Θεωρία Αριθμών
και εφαρμογές

Γιάννης Αντωνιάδης
Αριστείδης Κοντογεώργης

Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα
www.kallipos.gr

HEALLINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Θεωρία Αριθμών και εφαρμογές

Συγγραφή
Ιωάννης Αντωνιάδης
Αριστείδης Κοντογεώργης

Κριτικός αναγνώστης
Θεοδώρα Θεοχάρη-Αποστολίδου

Συντελεστές Έκδοσης
ΓΛΩΣΣΙΚΗ ΕΠΙΜΕΛΕΙΑ : Δημήτριος Καλλιάρας
ΓΡΑΦΙΣΤΙΚΗ ΕΠΙΜΕΛΕΙΑ : Αριστείδης Κοντογεώργης
ΤΕΧΝΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ : Αριστείδης Κοντογεώργης

ISBN: 978-618-82124-5-9

Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
Εθνικό Μετσόβιο Πολυτεχνείο
Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

http://www.kallipos.gr

Στη μνήμη των πατέρων μας, Αντώνη και Ιωάννη

Θεωρία Αριθμών και Εφαρμογές

Γιάννης Α. Αντωνιάδης, Αριστείδης Κοντογεώργης

10 Νοεμβρίου 2016

Περιεχόμενα

Κατάλογος Σχημάτων

Εισαγωγή

Η Θεωρία Αριθμών είναι ένας από τους αρχαιότερους κλάδους των Μαθηματικών. Το παρόν πόνημα αποτελεί μια εισαγωγή στην περιοχή. Αποτελείται από δύο μέρη. Το πρώτο αναφέρεται στην Αριθμητική των ρητών αριθμών. Το δεύτερο στην Αριθμητική των τετραγωνικών αρρήτων.

Η ύλη που περιέχεται σ' αυτό υπερκαλύπτει τις απαιτήσεις διδασκαλίας του αντίστοιχου μαθήματος σε όλα τα Τμήματα Μαθηματικών των Πανεπιστημίων και των Πολυτεχνείων της Χώρας.

Δεν χρειάζονται προαπαιτούμενα πέρα από τις βασικές γνώσεις μαθηματικών που διδάσκονται στο Λύκειο. Επομένως, είναι προσιτό και στους ενδιαφερόμενους μαθητές του Λυκείου.

Οι βασικές αρχές που επικράτησαν κατά τη συγγραφή παρουσιάζονται εν συντομία:

• Όπως προαναφέρθηκε δεν χρειάζονται προαπαιτούμενα. Θεωρούμε ότι αυτή είναι η φυσιολογική πορεία προσέγγισης της περιοχής. Αρκετά από τα αποτελέσματα έχουν γενικευτεί στην Άλγεβρα. Έτσι, αυτός που έχει παρακολουθήσει ένα μάθημα Άλγεβρας, μπορεί να συνάγει αντίστοιχα αποτελέσματα της Θεωρίας Αριθμών ως ειδική περίπτωση. Για τον αρχάριο όμως θεωρούμε ότι η επαγωγική μέθοδος είναι προτιμητέα.

Εξάλλου το πρώτο εισαγωγικό μάθημα Θεωρίας Αριθμών διδάσκεται, συνήθως, στο πρώτο ή δεύτερο εξάμηνο σπουδών, ενώ η Άλγεβρα κατά το τρίτο ή τέταρτο.

• Θεωρούμε επίσης ότι η ιστορική προσέγγιση των θεμάτων είναι η παιδαγωγικά σωστή. Έτσι το κείμενο εμπλουτίζεται σε κάθε του κεφάλαιο με ιστορικά στοιχεία. Δεν πρόκειται βέβαια για μια ανάπτυξη της Ιστορίας της Θεωρίας των Αριθμών, αλλά για αναφορά σε ιστορικά στοιχεία. Πιστεύουμε ότι αυτό αυξάνει το ενδιαφερόν του μελετητή. Εξάλλου η προσέγγιση αυτή είναι απόλυτα συμβατή με τη διεθνή βιβλιογραφία.

• Όπως έχει ήδη αναφερθεί, το περιεχόμενό του είναι ένα εισαγωγικό κείμενο στην περιοχή της Θεωρίας Αριθμών. Είναι λοιπόν αυτονόητο ότι τα περισσότερα από τα βασικά αποτελέσματα είναι αποτελέσματα περασμένων αιώνων. Όμως, ο κλάδος της Θεωρίας των Αριθμών είναι ένας από τους πιο δραστήριους ερευνητικά κλάδους των Μαθηματικών. Θα ήταν επομένως παράδοξο να μην αναφερθούν τα πρόσφατα αποτελέσματα της περιοχής. Φυσικά είναι αδύνατο να αποδειχθούν όλα αυτά. Όμως η Θεωρία των Αριθμών έχει επί του προκειμένου ένα ασύγκριτο πλεονέκτημα. Η διατύπωση των προτάσεων είναι κατανοητή από τον καθένα. Το πλεονέκτημα αυτό μας έχει επιτρέψει τη δυνατότητα αναφοράς πληθώρας προσφάτων και εξαιρετικά σημαντικών αποτελεσμάτων του κλάδου. Αυτό πιστεύουμε ότι θα κινήσει το ενδιαφέρον πολλών αναγνωστών για περαιτέρω εμβάθυνση στην περιοχή.

• Ο κλάδος της Θεωρίας Αριθμών ήταν για χιλιετηρίδες ένας κλάδος των λεγόμενων Θεω-

ρητικών Μαθηματικών, χωρίς άμεσες εφαρμογές στην καθημερινότητά μας. Τα αποτελέσματα αποτελούσαν ικανοποίηση του ανθρωπίνου πνεύματος, όπως έλεγε και ο Jacobi. Αυτό έκανε τον Hardy επίσης ευτυχισμένο, όπως αναφέρει στο έργο του «Η Απολογία ενός Μαθηματικού».

Όμως, κατά την τελευταία τεσσαρακονταετία η Θεωρία Αριθμών απέκτησε και πρακτικό «πεδίον δόξης λαμπρόν». Αιτία είναι η κατά τα τελευταία έτη, ραγδαία αναπτυσσόμενη Κρυπτογραφία. Δεν νοείται σήμερα βιβλίο Θεωρίας Αριθμών χωρίς αναφορά στους κρυπτογραφικούς αλγορίθμους. Αυτή την πρακτική ακολουθήσαμε και εμείς. Και εδώ επεκτεινόμαστε τόσο, ώστε οι αλγόριθμοι να είναι απλοί και κατανοητοί. Για περισσότερα στοιχεία παραπέμπουμε στο βιβλίο «Πεπερασμένα Σώματα και Κρυπτογραφία» των ίδιων συγγραφέων.

Στο βιβλίο δεν περιέχεται η θεωρία των πολλαπλασιαστικών συναρτήσεων εκτός από ειδικές περιπτώσεις όπως η ϕ-συνάρτηση του Euler. Ο λόγος είναι ότι προγραμματίζουμε την έκδοση ενός δεύτερου τόμου ο οποίος θα περιέχει την Αναλυτική Θεωρία Αριθμών, καθώς και στοιχεία υπερβατικής και προσθετικής Αριθμοθεωρίας. Σε αυτόν τον τόμο οι πολλαπλασιαστικές συναρτήσεις θα αναπτυχθούν πλήρως.

Στη συνέχεια θα αναφερθούμε με συντομία στο περιεχόμενο κάθε κεφαλαίου του πρώτου μέρους. Στο πρώτο κεφάλαιο αναπτύσονται βασικές έννοιες διαιρετότητας, πρώτων αριθμών και το θεμελιώδες θεώρημα της αριθμητικής. Στο δεύτερο κεφάλαιο μελετώνται διάφορες κλάσεις διοφαντικών εξισώσεων. Στο τρίτο κεφάλαιο ακολουθεί η μελέτη επώνυμων ακεραίων όπως φίλοι, τέλειοι, πολυγωνικοί και ισοδύναμοι αριθμοί. Για πρώτη φορά εισάγωνται έννοιες και τεχνικές κρυπτογραφίας και παραγοντοποίησης ακεραίων. Το τέταρτο κεφάλαιο είναι αφιερωμένο στη θεωρία των ισοδυναμίων (συχνά χρησιμοποιείται και ο όρος ισοτιμία). Μελετάται πληθώρα εφαρμογών κυρίως στην παραγοντοποίηση ακεραίων και στην κρυπτογραφία. Τέλος, στο πέμπτο κεφάλαιο μελετάται η θεωρία των τετραγωνικών υπολοίπων, αρχικών ριζών και δεικτών. Το περιεχόμενο των κεφαλαίων του δευτέρου μέρους περιγράφεται στην εισαγωγή του δεύτερου μέρους.

Θα θέλαμε να ευχαριστήσουμε το πρόγραμμα «Κάλλιπος», το οποίο ήταν το κίνητρο για να ολοκληρωθεί το βιβλίο. Επίσης, θερμές ευχαριστίες στην Καθηγήτρια του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης κα Θ. Θεοχάρη για τις παρατηρήσεις και τα σχόλιά της ως κριτική αναγνώστρια του κειμένου. Πολλές ευχαριστίες στους φοιτητές Αθανάσιο Τασόπουλο, Γιάννη Καρασαρίνη και Γιάννη Μπέκα (φοιτητές ΕΚΠΑ 2015) και Μανόλη Καπνόπουλο (φοιτητή Π.Κ. 2015) όπως και στον μεταπτυχιακό φοιτητή Πέτρο Πανταβό για τις διορθώσεις που πρότειναν. Τέλος θερμές ευχαριστίες στον γλωσσικό επιμελητή-φιλόλογο κ. Δημήτρη Καλλιάρα για όλες τις διορθώσεις του.

Μέρος Ι

ΑΡΙΘΜΟΘΕΩΡΙΑ ΤΩΝ ΡΗΤΩΝ ΑΡΙΘΜΩΝ

1

Διαιρετότητα και πρώτοι αριθμοί

1.1 Το σύνολο των ακέραιων

Η (στοιχειώδης) Θεωρία Αριθμών ασχολείται κυρίως με τη μελέτη των ιδιοτήτων του συνόλου των *ακέραιων αριθμών*

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

Με $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ θα συμβολίζουμε το σύνολο των *θετικών ακέραιων* και με

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

το σύνολο των *φυσικών αριθμών* .

Υποθέτουμε ότι ο αναγνώστης γνωρίζει τις βασικές ιδιότητες των πράξεων στα παραπάνω σύνολα.

Στα επόμενα, πάρα πολύ συχνά θα χρειαζόμαστε τις παρακάτω δύο προτάσεις - αξιώματα του συνόλου $\mathbb{N}$.

Αξίωμα 1.1.1 (Αξίωμα της μαθηματικής επαγωγής)**.** *Αν S μη κενό υποσύνολο του $\mathbb{N}$ με τις ιδιότητες:*

1. *$0 \in S$, και*
2. *για κάθε $s \in S$, έπεται ότι και $s + 1 \in S$,*

τότε το $S = \mathbb{N}$.

Αξίωμα 1.1.2 (Αρχή του ελαχίστου)**.** *Κάθε μη κενό σύνολο S, υποσύνολο του συνόλου των φυσικών αριθμών, έχει ελάχιστο στοιχείο.*

Αυτό σημαίνει ότι υπάρχει $a \in S$ τέτοιο, ώστε να ισχύει $a \leq s$ για κάθε $s \in S$.

Η αρχή του ελαχίστου είναι συνέπεια του αξιώματος της μαθηματικής επαγωγής. Η απόδειξη θα δοθεί στο Παράρτημα 1. Μπορεί να αποδειχθεί και το αντίστροφο. Αυτό σημαίνει ότι οι δύο προτάσεις είναι μεταξύ τους ισοδύναμες. Μία λοιπόν από τις δύο θεωρείται αξίωμα και η άλλη αποδεικνύεται. Άμεση συνέπεια της αρχής του ελαχίστου 1.1.2 είναι το

Αξίωμα 1.1.3 (Δεύτερη μορφή της μαθηματικής επαγωγής)**.** *Υποθέτουμε ότι $P(n)$ είναι μια πρόταση που αναφέρεται στον φυσικό αριθμό n. Αν*

1. *η $P(0)$ είναι αληθής*

2. *από την ισχύ της $P(m)$ για όλους τους φυσικούς $m < n$ έπεται η ισχύς της $P(n)$,*

τότε η $P(n)$ ισχύει για όλους τους φυσικούς αριθμούς.

Απόδειξη. Θεωρούμε το σύνολο

$$M := \{n \in \mathbb{N} | P(n) \text{ είναι ψευδής}\}$$

Το M είναι υποσύνολο του συνόλου $\mathbb{N}$. Αν $M \neq \emptyset$ τότε, σύμφωνα με την αρχή του ελαχίστου, το M έχει ελάχιστο στοιχείο, έστω m_0.

Η $P(0)$ είναι αληθής. Επομένως $m_0 > 0$. Από τον ορισμό του m_0 έχουμε ότι n πρόταση $P(m)$ είναι αληθής για κάθε $m < m_0$. Σύμφωνα με την υπόθεση θα είναι αληθής και η $P(m_0)$, άτοπο. Επομένως $M = \emptyset$, δηλαδή η $P(n)$ είναι αληθής για *κάθε* φυσικό αριθμό n. □

Ανάλογα αποδεικύεται και η

Πρόταση 1.1.4. *Υποθέτουμε ότι $P(n)$ είναι μια πρόταση που αναφέρεται στον φυσικό αριθμό n. Αν η $P(n_0)$ είναι αληθής για κάποιο φυσικό αριθμό $n_0 > 0$ και για κάθε φυσικό αριθμό m, $m \geq n_0$, n αλήθεια της $P(m)$, συνεπάγεται την αλήθεια της $P(m+1)$, τότε η $P(n)$ είναι αληθής για κάθε φυσικό αριθμό $n \geq n_0$.*

Η απόδειξη αφήνεται ως άσκηση στον αναγνώστη.

Παράδειγμα 1.1.5. Να αποδειχθεί ότι, για κάθε $n \in \mathbb{N}$ ισχύει:

$$0 + 1 + 2 + \cdots + (n-1) + n = \frac{1}{2}(n+1)n.$$

Απόδειξη. Για $n = 0$ είναι φανερό ότι η προηγούμενη σχέση ισχύει.

Υποθέτουμε ότι ισχύει για $n = m$, δηλαδή ότι

$$0 + 1 + \cdots + (m-1) + m = \frac{1}{2}(m+1)m$$

Θα αποδείξουμε ότι ισχύει και για $n = m + 1$.

Πράγματι,

$$0 + 1 + \cdots + (m-1) + m + (m+1) = \frac{1}{2}(m+1)m + (m+1) =$$

$$= (m+1)(\frac{m}{2} + 1) = \frac{(m+1)(m+2)}{2}.$$

Επομένως ισχύει για όλους τους φυσικούς αριθμούς n □

Παράδειγμα 1.1.6. Να αποδειχθεί ότι για κάθε φυσικό αριθμό n ισχύει:

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Απόδειξη. Για $n = 0$, έχουμε

$$\sum_{i=0}^{n} \binom{n}{i} = \binom{0}{0} = 0! = 1 = 2^0.$$

Υποθέτουμε ότι ισχύει για $n = m$, δηλαδή ότι $\sum_{i=0}^{m} \binom{m}{i} = 2^m$

Θα αποδείξουμε ότι ισχύει και για $n = m + 1$, δηλαδή ότι $\sum_{i=0}^{m+1} \binom{m+1}{i} = 2^{m+1}$.

Έχουμε

$$\binom{m+1}{0} = 1, \binom{m+1}{m+1} = 1$$

και

$$\binom{m+1}{k} = \binom{m}{k-1} + \binom{m}{k},$$

όπως εύκολα παρατηρεί κανείς υπολογίζοντας και τα δύο μέρη της εξίσωσης.

Συνεπώς,

$$\begin{aligned}
\sum_{i=0}^{m+1} \binom{m+1}{i} &= 2 + \sum_{i=1}^{m} \binom{m+1}{i} \\
&= 2 + \sum_{i=1}^{m} \binom{m}{i-1} + \binom{m}{i} \\
&= 2 + \sum_{i=0}^{m-1} \binom{m}{i} + \sum_{i=1}^{m} \binom{m}{i} \\
&= \sum_{i=0}^{m} \binom{m}{i} + \sum_{i=0}^{m} \binom{m}{i} \\
&= 2 \cdot \sum_{i=0}^{m} \binom{m}{i} = 2 \cdot 2^m = 2^{m+1}
\end{aligned}$$

Επομένως ισχύει για κάθε φυσικό αριθμό n. □

Παράδειγμα 1.1.7. Να αποδείξουμε ότι για κάθε φυσικό αριθμό $n \neq 0$ ισχύει:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

Απόδειξη. Για $n = 1$ ισχύει.

Υποθέτουμε ότι ισχύει για $m \geq 1$, δηλαδή ότι

$$\sum_{i=1}^{m} \frac{1}{i(i+1)} = \frac{m}{m+1} \tag{1.1.1}$$

Θα αποδείξουμε ότι ισχύει και για $m + 1$, δηλαδή ότι ισχύει

$$\sum_{i=1}^{m+1} \frac{1}{i(i+1)} = \frac{m+1}{m+2}.$$

Πράγματι,

$$\sum_{i=1}^{m+1} \frac{1}{i(i+1)} = \sum_{i=1}^{m} \frac{1}{i(i+1)} + \frac{1}{(m+1)(m+2)}$$

$$\overset{(1.1.1)}{=} \frac{m}{m+1} + \frac{1}{(m+1)(m+2)} = \frac{m(m+2)+1}{(m+1)(m+2)} =$$

$$= \frac{(m+1)^2}{(m+1)(m+2)} = \frac{m+1}{m+2}$$

Επομένως ισχύει για κάθε φυσικό αριθμό n, $n \neq 0$. □

Παράδειγμα 1.1.8. Να αποδείξετε ότι $n! > n^2$ για κάθε φυσικό αριθμό $n \geq 4$.

Απόδειξη. Αυτό είναι ένα παράδειγμα απόδειξης με επαγωγή η οποία ξεκινάει από το $n = 4$. Πράγματι, η πρόταση για $n = 4$ δίνει ότι $4! = 24 > 16 = 4^2$ η οποία είναι αληθής. Υποθέτουμε ότι ισχύει $n! > n^2$ και θα πρέπει να δείξουμε ότι $(n+1)! > (n+1)^2$. Πολλαπλασιάζουμε τη σχέση $n! > n^2$ με $n+1$ για να πάρουμε

$$(n+1)! > n^2(n+1) > (n+1)^2.$$

Αφήνεται στον αναγνώστη ως άσκηση να αποδείξει ότι $n^2 > n+1$ για $n \geq 2$. □

Παράδειγμα 1.1.9. Να αποδείξετε ότι κάθε φυσικός αριθμός είναι ίσος με τον επόμενό του.

Απόδειξη. Υποθέτουμε ότι η πρόταση ισχύει για m, δηλαδή ότι

$$m = m + 1$$

Προσθέτουμε και στα δύο μέλη το 1 και έχουμε

$$m + 1 = m + 2,$$

δηλαδή ισχύει και για $m + 1$. Επομένως ισχύει για κάθε φυσικό αριθμό n. □

Συμπέρασμα. Όλοι οι φυσικοί αριθμοί είναι ίσοι! Πού βρίσκεται το λάθος;

Σημείωση. Το τελευταίο παράδειγμα μάς δείχνει ότι θα πρέπει να είμαστε προσεκτικοί και να εφαρμόζουμε σωστά την επαγωγή.

1.1.1 Ασκήσεις

Α Ομάδα (Σωστό ή Λάθος) Να απαντήσετε αν οι παρακάτω προτάσεις είναι σωστές ή λάθος και να δικαιολογήσετε τις απαντήσεις σας.

1. Κάθε φυσικός είναι ακέραιος. **Σωστό Λάθος**
2. Κάθε ακέραιος είναι φυσικός. **Σωστό Λάθος**
3. Υπάρχουν αριθμοί που δεν είναι ακέραιοι. **Σωστό Λάθος**
4. Αν $x, y \in \mathbb{R}$ και $n \in \mathbb{N}$, $n \geq 1$ τότε ισχύει η

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

Β Ομάδα (Ασκήσεις κατανόησης)

1. Να αποδείξετε ότι για κάθε φυσικό αριθμό ισχύει $n < 2^n$.

2. Να αποδείξετε ότι για κάθε φυσικό αριθμό n, ο αριθμός

$$3 \cdot 7^n + 2 \cdot 2^n$$

είναι πολλαπλάσιο του 5.

3. Για κάθε φυσικό αριθμό n, $n \geq 1$, ισχύει

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

4. Ομοίως για κάθε $n \geq 1$ ισχύει

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Να συμπεράνετε ότι ο n^3 για κάθε φυσικό αριθμό n, $n \geq 1$ γράφεται ως διαφορά δύο τετραγώνων.

Γ Ομάδα (Ασκήσεις εμπέδωσης)

1. Να αποδείξετε ότι δεν υπάρχουν ακέραιοι μεταξύ 0 και 1.

2. Να αποδείξετε ότι για κάθε ακέραιο n ο αριθμός $3n^5 + 5n^3 + 7n$ διαιρείται με 15.

3. (Ανισότητα του Bernoulli) Αν $x \in \mathbb{R}$ με $1 + x > 0$ να αποδείξετε ότι για $n \geq 1$

$$(1 + x)^n \geq 1 + nx.$$

Γ Ομάδα (Ασκήσεις εμβάθυνσης)

1. Έστω $P(n)$ μία πρόταση η οποία εξαρτάται από τον φυσικό αριθμό n. Υποθέτουμε ότι η $P(0)$ είναι αληθής. Επίσης, αν $P(k)$ αληθής τότε και η $P(k+2)$ αληθής.

   Μπορούμε να συμπεράνουμε τότε ότι η $P(n)$ είναι αληθής για κάθε φυσικό αριθμό n; Αν όχι τι πρέπει να προσθέσουμε έτσι ώστε να ισχύει για κάθε φυσικό n·

2. Εδώ θα αποδείξουμε ότι όλες οι γυναίκες έχουν το ίδιο χρώμα ματιών. Πράγματι σε κάθε μονοσύνολο γυναικών όλες έχουν το ίδιο χρώμα ματιών, δηλαδή ισχύει για $n = 1$.

   Υποθέτουμε ότι σε κάθε σύνολο γυναικών πλήθους n, όλες έχουν το ίδιο χρώμα ματιών. Θεωρούμε ένα τυχαίο σύνολο γυναικών πλήθους $n+1$ έστω $\{1, 2, \ldots, n, n+1\}$. Το χωρίζουμε σε δύο σύνολα $\{1, 2, \ldots, n\}$ και $\{2, 3, \ldots, n, n+1\}$.

   Σύμφωνα με την υπόθεση της μαθηματικής επαγωγής, οι γυναίκες κάθε συνόλου έχουν το ίδιο χρώμα ματιών και επειδή έχουν κοινά στοιχεία τελικά και το σύνολο των γυναικών $\{1, 2, \ldots, n, n+1\}$ έχει το ίδιο χρώμα ματιών. Επομένως κάθε σύνολο γυναικών έχει το ίδιο χρώμα ματιών. Πού είναι το λάθος;

1.2 Διαιρετότητα

Το σύνολο των ακέραιων είναι εφοδιασμένο με δύο πράξεις, πρόσθεσης και πολλαπλασιασμού. Το άθροισμα, η διαφορά και το γινόμενο δύο ακέραιων είναι πάντα ακέραιος αριθμός. Το πηλίκο τους όμως *δεν* είναι πάντοτε ακέραιος. Δεν υπάρχει ακέραιος αριθμός a τέτοιος ώστε να ισχύει $2a = 1$, ενώ υπάρχει ακέραιος αριθμός b τέτοιος ώστε $2b = -4$.

Εντελώς φυσιολογικός επομένως είναι ο ακόλουθος ορισμός:

Ορισμός 1.2.1. Δίνονται δύο ακέραιοι αριθμοί a, b με $b \neq 0$. Θα λέμε ότι *ο b διαιρεί του a* όταν υπάρχει ακέραιος c τέτοιος ώστε $a = b \cdot c$.

Ισοδύναμα χρησιμοποιούνται και οι εκφράσεις «ο b είναι ένας διαιρέτης του a», «ο a είναι (ένα) πολλαπλάσιο του b», «ο a είναι διαιρετός από τον b». Αν ο b διαιρεί τον a γράφουμε $b|a$, αν όχι γράφουμε $b \nmid a$.

Άμεση συνέπεια του ορισμού είναι οι ακόλουθες ιδιότητες διαιρετότητας:

Πρόταση 1.2.2. *Στα παρακάτω τα a, b, c είναι ακέραιοι.*

1. *Για κάθε ακέραιο a, $a \neq 0$, ισχύει $a|0$ και $a|a$, δηλαδή ο a διαιρεί το μηδέν και τον εαυτό του.*
2. *Για κάθε ακέραιο a ισχύει $1|a$, δηλαδή ο 1 διαιρεί κάθε ακέραιο.*
3. *Αν $c|b$ και $b|a$, τότε και $c|a$.*
4. *Αν $c|a$ και $c|b$, τότε και $c|ka + lb$ για οποιουσδήποτε ακέραιους k, l.*
5. *Αν $b|a$ τότε και $bk|ak$ για οποιωνδήποτε ακέραιο $k \neq 0$. Αντιστρόφως, αν $bk|ak$ τότε και $b|a$ (Παρατηρήστε ότι $k \neq 0$ αφού δεν έχουμε ορίσει το $0 \mid 0$).*
6. *Αν $b|a$ και $a \neq 0$, τότε $|b| \leq |a|$.*
7. *Αν $b|a$ και $a|b$, τότε $a = \pm b$.*
8. *Αν $b|a$ και $a \neq 0$, τότε και $(a/b)|a$.*
9. *Αν $b_1|a_1$ και $b_2|a_2$, τότε και $b_1 b_2 | a_1 a_2$.*

Απόδειξη. Έχουμε:

1. $0 = a \cdot 0$ και $a = 1 \cdot a$
2. $a = 1 \cdot a$
3. $b = c \cdot k$ και $a = b \cdot l$, άρα $a = c(k \cdot l)$
4. $a = c\,a'$, $b = c\,b'$, οπότε $k\,a + l\,b = c(k\,a' + l\,b')$
5. $a\,k = (b\,k) \cdot c = (b\,c)\,k$, άρα $(a - b\,c)\,k = 0$ οπότε και $a = b\,c$, αφού $k \neq 0$
6. $a = b \cdot c$, άρα $|a| = |b| \cdot |c|$ $c \neq 0$, αφού $a \neq 0$. Επομένως $|b| \leq |a|$.
7. Από τον ορισμό της διαιρετότητας έπεται ότι $a \neq 0$ και $b \neq 0$. Λόγω της 6, $|b| \leq |a|$ και $|a| \leq |b|$.

   Συνεπώς $|a| = |b|$, δηλαδή $a = \pm b$.

8. $a = bc$. Επειδή $a \neq 0$ έπεται ότι και $c \neq 0$, άρα $c|a$.

9. $a_1 = b_1 c_1$ και $a_2 = b_2 c_2$, άρα $a_1 a_2 = (b_1 b_2)(c_1 c_2)$.

□

Παρατήρηση. Από την 6. ιδιότητα της Πρότασης (1.2.2) έπεται ότι το πλήθος των διαιρετών ακέραιου αριθμού είναι πάντοτε πεπερασμένο.

Θεώρημα 1.2.3 (Θεώρημα της διαίρεσης με υπόλοιπο)**.** *Αν a, b ακέραιοι και $b \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε*

$$a = bq + r \text{ και } 0 \leq r < |b|.$$

Απόδειξη. Γεωμετρικά, στον πραγματικό άξονα, η πρόταση είναι προφανής. Το σύνολο $M := \{a - bx | x \in \mathbb{Z}\}$ περιέχει φυσικούς αριθμούς. Πράγματι, αν $b > 0$ τότε ο αριθμός $a - b(-|a|)$ είναι φυσικός αριθμός και στοιχείο του M. Αν πάλι $b < 0$ τότε ο αριθμός $a - b|a|$ είναι φυσικός αριθμός και στοιχείο του M. Επομένως το σύνολο

$$S := M \cap \mathbb{N}$$

είναι μη κενό υποσύνολο του $\mathbb{N}$.

Σύμφωνα με την αρχή του ελαχίστου, το S έχει ελάχιστο στοιχείο, έστω r. Ο r έχει τη μορφή $r = a - bq$ για κάποιο $q \in \mathbb{Z}$, δηλαδή

$$a = bq + r.$$

Θα αποδείξουμε ότι $r < |b|$. Αν υποθέσουμε ότι $r \geq |b|$, τότε ο αριθμός

$$r - |b| = \begin{cases} a - bq - b = a - b(q+1), & \text{αν } b > 0 \\ a - bq + b = a - b(q-1), & \text{αν } b < 0 \end{cases}$$

ανήκει στο S και είναι μικρότερος του r, άτοπο. Συνεπώς $0 \leq r < |b|$

Αν τώρα $a = bq + r = bq' + r'$ και $0 \leq r, r' < |b|$, τότε

$$|r' - r| = |b(q - q')|.$$

Επειδή τα r, r' βρίσκονται στο διάστημα $[0, |b|)$ έπεται ότι $|r' - r| < |b|$. Αν λοιπόν $q \neq q'$ θα είχαμε $|r' - r| < |b| < |b(q - q')| = |r' - r|$, άτοπο.

Συνεπώς $q = q'$ και, κατ' ακολουθία,

$$r = a - bq = a - bq' = r'.$$

□

Μερικές φορές χρήσιμη είναι και η ακόλουθη μορφή.

Πόρισμα 1.2.4. *Αν a, b ακέραιοι και $b \neq 0$, υπάρχουν μοναδικοί ακέραιοι q, r τέτοιοι ώστε*

$$a = bq + r$$

και

$$-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|.$$

Απόδειξη. Σύμφωνα με το Θεώρημα 1.2.3 υπάρχουν μοναδικοί ακέραιοι q_0, r_0 ώστε να ισχύει $a = b\,q_0 + r_0$ και $0 \leq r_0 < |b|$. Αν $0 \leq r_0 \leq \frac{1}{2}|b|$, τότε παίρνουμε $q := q_0$ και $r := r_0$.

Αν $\frac{1}{2}|b| < r_0 < |b|$, Τότε παίρνουμε

$$r := r_0 - |b| < 0 \text{ και } q := \begin{cases} q_0 + 1, & \text{αν } b > 0 \\ q_0 - 1, & \text{αν } b < 0. \end{cases}$$

Έστω τώρα ότι $a = b\,q + r = b\,q' + r'$ με

$$-\frac{1}{2}|b| < r,\ r' \leq \frac{1}{2}|b|.$$

Ισχύει, $0 \leq |r' - r| < |b|$. Η υπόθεση $q \neq q'$ μας οδηγεί και πάλι στο άτοπο

$$0 \leq |r' - r| < |b| < |b(q - q')| = |r' - r|.$$

Επομένως $q = q'$ και $r = r'$. □

Παράδειγμα 1.2.5. Αν $a = 145$ και $b = 23$, τότε $q = 6$ και $r = 7$. Αν $a = 61$ και $b = -7$ τότε $q = -9$ και $r = -2$. Αν $a = -59$ και $b = 9$ τότε $q = -7$ και $r = 4$.

Παρατηρήσεις.

1. Από το Θεώρημα 1.2.3 προκύπτει αμέσως ότι $b|a$ ακριβώς τότε όταν $r = 0$.

2. Σύμφωνα με το Θεώρημα 1.2.3 κάθε ακέραιος αριθμός διαιρούμενος με δοθέντα φυσικό αριθμό $m > 1$, δίνει υπόλοιπο $r \in \{0, 1, 2, \ldots, m-1\}$.

   Αυτό σημαίνει ότι κάθε ακέραιος a γράφεται σε μία από τις μορφές

   $$m\,l,\ m\,l + 1, \ldots, m\,l + (m-1)$$

   για κάποιο μονοσήμαντα ορισμένο ακέραιο l.

   Πρόκειται για μια από τις πιο σημαντικές συνέπειες του Θεωρήματος 1.2.3.

3. Στην περίπτωση που το $m = 2$ οι ακέραιοι αριθμοί χωρίζονται σε δύο υποσύνολα. Στους (άρτιους) που γράφονται στη μορφή $2l$ και στους (περιττούς) αυτούς που γράφονται στη μορφή $2l + 1$ ($l \in \mathbb{Z}$).

4. Για $m = 3$, έχουμε ότι κάθε ακέραιος αριθμός a γράφεται σε μία από τις μορφές

   $$3l,\ 3l + 1,\ 3l + 2\ (l \in \mathbb{Z})$$

   Επομένως το $a^2 = 9l^2 = 3k$ ή $a^2 = 9l^2 + 6l + 1 = 3s + 1$ ή $a^2 = 9l^2 + 12k + 4 = 3t + 1$.

   Συνεπώς *δεν* υπάρχει ακέραιος αριθμός της μορφής $3l + 2 (l \in \mathbb{Z})$ ο οποίος να είναι τέλειο τετράγωνο.

   Παράδειγμα 1.2.6. Ο αριθμός $3l^2 - 1$, για οποιοδήποτε ακέραιο l *δεν* είναι τέλειο τετράγωνο.

5. Για $m = 4$ έχουμε ότι κάθε ακέραιος a γράφεται σε μία από τις μορφές

$$4l,\ 4l+1,\ 4l+2,\ 4l+3$$

για κάποιο, συγκεκριμένο ακέραιο l.

Εύκολα, όπως στο (3), συμπεραίνουμε ότι $a^2 = 4k$ ή $4k+1$.

Επομένως, *δεν* υπάρχει ακέραιος αριθμός της μορφής $4l+2$ ή $4l+3\,(l \in \mathbb{Z})$, ο οποίος να είναι τέλειο τετράγωνο.

Παράδειγμα 1.2.7. Κανένας από τους αριθμούς

$$11,\ 111,\ 1111,\ 11111, \ldots$$

δεν είναι τέλειο τετράγωνο ακέραιου.

Αυτό ισχύει διότι *όλοι* αυτοί οι αριθμοί γράφονται στη μορφή $4l+3$.

Πράγματι, $11 = 4{\cdot}2{+}3$, $111 = 4{\cdot}25{+}4{\cdot}2{+}3 = 4{\cdot}27{+}3$, $1111 = 4{\cdot}250{+}4{\cdot}27{+}3 = 4{\cdot}277{+}3$ και ούτω καθεξής.

Επίσης $a^2 = 4l$ ή $4l+1\,(l \in \mathbb{Z})$ και $b^2 = 4s$ ή $4s+1\,(s \in \mathbb{Z})$,

έχουμε ότι το άθροισμα των τετραγώνων δύο ακέραιων αριθμών είναι ακέραιος αριθμός της μορφής $4t$ ή $4t+1$ ή $4t+2$ $(t \in \mathbb{Z})$

Επομένως, κανένας ακέραιος της μορφής $4k+3 (k \in \mathbb{Z})$ *δεν* γράφεται ως άθροισμα δύο τετραγώνων ακέραιων αριθμών.

6. Για $m = 10$ έχουμε ότι κάθε ακέραιος a γράφεται στη μορφή

$$a = 10q + r,\ 0 \le r < 10$$

Επομένως $a^2 = 100q^2 + 20q + r^2$.

Αυτό σημαίνει ότι ο a^2 και ο r^2 έχουν το *ίδιο* ψηφίο μονάδων.

Τα τετράγωνα των αριθμών 0 έως 9 δίνουν ψηφίο μονάδων $0, 1, 4, 5, 6, 9$. Συνεπώς το τελευταίο ψηφίο του τετραγώνου ακέραιου αριθμού είναι $0, 1, 4, 5, 6, 9$.

7. Αν a, b ακέραιοι και $b > 0$, από το Θεώρημα 1.2.3 προκύπτει ότι $a = bq + r$, $0 \le r < b$. Επομένως,
$$\frac{a}{b} = q + \frac{r}{b}, 0 \le \frac{r}{b} < 1.$$

Ορισμός 1.2.8. Αν x πραγματικός αριθμός, το *ακέραιο* μέρος του x ορίζεται ως ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του x και συμβολίζεται με $[x]$. Επομένως $q = \left[\frac{a}{b}\right]$.

1.2.1 Ασκήσεις

Ομάδα Α Σωστό ή Λάθος

1. Κάθε φυσικός αριθμός m διαιρεί το γινόμενο οποιωνδήποτε m διαδοχικών ακέραιων. **Σωστό Λάθος**

2. Αν $n, m \in \mathbb{N}$, $n \geq m > 0$, το πλήθος των φυσικών αριθμών $\leq n$ οι οποίοι διαιρούνται με m είναι $\left[\frac{n}{m}\right] + 1$ **Σωστό Λάθος**

3. Για κάθε φυσικό $n > 0$, ισχύει $(a+1) \mid (a^{2n-1}+1)$ **Σωστό Λάθος**

4. Το πλήθος των φυσικών μεταξύ 10 και 1000 οι οποίοι δεν είναι διαιρετοί δια του 23 είναι 956. **Σωστό Λάθος**

Ομάδα Β (Ασκήσεις κατανόησης)

1. Πόσοι ακέραιοι ανάμεσα στο 100 και το 500 διαιρούνται με 7 και πόσοι με 49;

2. Να αποδείξετε ότι το γινόμενο δύο περιττών ακέραιων είναι περιττός ακέραιος, ενώ το γινόμενό τους είναι άρτιος αν ένας τουλάχιστον από τους δύο είναι άρτιος.

3. Να αποδείξετε ότι ο κύβος οποιουδήποτε ακέραιου έχει τη μορφή 9ℓ, $9\ell+1$ ή $9\ell+8$, $\ell \in \mathbb{Z}$.

4. Αν ένας ακέραιος a διαιρεί τους $12n+5$ και $4n+2$ για κάποιο ακέραιο n τότε $a = \pm 1$.

5. Να αποδείξετε ότι δεν υπάρχει ακέραιος της μορφής $8\ell+7$, $\ell \in \mathbb{Z}$ ο οποίος να γράφεται ως άθροισμα τριών τετραγώνων.

6. Αν οι a, b είναι περιττοί ακέραιοι και $b \nmid a$, τότε υπάρχουν ακέραιοι k, ℓ τέτοιοι ώστε $a = bk + \ell$, όπου ℓ είναι περιττός και $|\ell| < b$.

7. Αν a ακέραιος, τότε ένας από τους a, $a+2$, $a+4$ διαιρείται με 3.

Ομάδα Γ (Ασκήσεις εμπέδωσης)

1. Να αποδείξετε ότι για κάθε ακέραιο ℓ, υπάρχει ένας ακέραιος n τέτοιος ώστε $5 \mid n^3 + \ell$. Να ελέγξετε αν ισχύει το ίδιο αν αντικαταστήσουμε το 5 με το 7.

2. Αν ο ακέραιος a δεν διαιρείται με 2 ούτε με 3, τότε ο a^2+23 διαιρείται με 24.

3. Να αποδείξετε ότι για κάθε θετικό ακέραιο n ισχύει $2 \mid 3^n - 1$, $3 \mid 4^n - 1$, $4 \mid 5^n - 1, \ldots$

4. Να βρεθούν όλοι οι θετικοί ακέραιοι n για τους οποίους ο $3 \mid 2^n + 1$.

5. Να αποδείξετε ότι για κάθε φυσικό αριθμό n ισχύουν:
$$3 \mid n^3 - n, 5 \mid n^5 - n, 7 \mid n^7 - n.$$
Μπορούμε να συμπεράνουμε ότι για κάθε περιττό k και κάθε φυσικό n ισχύει $k \mid n^k - n$;

6. Από το σύνολο $\{1, 2, \ldots, 2n\}$ επιλέγουμε τυχαία $n+1$ αριθμούς. Να αποδείξετε ότι ανάμεσά τους υπάρχει τουλάχιστον ένα ζευγάρι όπου ο ένας διαιρεί τον άλλο.

Ομάδα Δ (Ασκήσεις εμβάθυνσης)

1. Να αποδείξετε ότι για κάθε θετικό ακέραιο n ισχύει:
$$(1 + 2 + \cdots + n) \mid 3(1^2 + 2^2 + \cdots n^2).$$

2. Να βρείτε όλους τους ακέραιους a, $a \neq 3$, για τους οποίους ισχύει:
$$a - 3 \mid a^3 - 3.$$

3. Αν x, y, z θετικοί ακέραιοι για τους οποίους ισχύει $x^2 + y^2 = z^2$, τότε ένας τουλάχιστον διαιρείται με 3.

4. Αν $S := \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, όπου n φυσικός, $n > 1$, τότε ο S δεν είναι ακέραιος.

1.3 Πρώτοι Αριθμοί

Κάθε ακέραιος αριθμός $a \neq 0$ έχει διαιρέτες τουλάχιστον τους αριθμούς ± 1 και $\pm a$.

Ορισμός 1.3.1. Ένας ακέραιος αριθμός p διάφορος των $0, \pm 1$ λέγεται *πρώτος* όταν έχει ως διαιρέτες του μόνο τους ± 1 και $\pm p$.

Ένας ακέραιος διάφορος του $0, \pm 1$ που *δεν* είναι πρώτος λέγεται *σύνθετος*.

Για παράδειγμα, οι ± 3 και ± 19 είναι πρώτοι, ενώ οι ± 6, ± 18 σύνθετοι.

Επειδή ο ακέραιος αριθμός a είναι πρώτος ακριβώς τότε όταν ο $-a$ είναι πρώτος, από εδώ και πέρα κάθε αναφορά σε πρώτους αριθμούς θα αφορά *θετικούς* πρώτους. Το σύνολο των πρώτων αριθμών θα το συμβολίζουμε με $\mathbb{P}$.

Κατ' αρχήν αποδεικνύουμε την

Πρόταση 1.3.2. *Κάθε φυσικός αριθμός n, $n > 1$, έχει τουλάχιστον έναν πρώτο διαιρέτη.*

Απόδειξη. Θεωρούμε το σύνολο

$$M = \{m \in \mathbb{N} \text{ ώστε } m|n \text{ και } m > 1\}.$$

Το M είναι υποσύνολο του συνόλου $\mathbb{N}$ και είναι διάφορο του κενού, διότι $n \in M$.

Σύμφωνα με την αρχή του ελαχίστου (Αξίωμα 1.1.2), το M έχει ένα ελάχιστο στοιχείο, έστω p. Ο p είναι πρώτος διαιρέτης του n.

Πράγματι, αν δεν ήταν πρώτος θα είχε τουλάχιστο μια ανάλυση της μορφής $p = a \cdot b$ με $a, b \in \mathbb{N} \setminus \{1\}$. Αυτό σημαίνει ότι ο $a \in \mathbb{N}$, $a > 1$ και $a|n$ (αφού $a|p$ και $p|n$), δηλαδή ότι a θα ήταν στοιχείο του M και ότι $a < p$, άτοπο. □

Ιστορικά 1.3.1

Οι πρώτοι που άρχισαν να αφηγούνται ιστορίες σχετικά με τους πρώτους αριθμούς, ήταν οι αρχαίοι Έλληνες. Αυτοί αναγνώρισαν την ισχύ των αποδείξεων στη χάραξη μόνιμων διόδων προς τα όρη του μαθηματικού κόσμου [14].
Η πρόταση 1.3.2 είναι η πρόταση 32, του βιβλίου VII των «Στοιχείων» του Ευκλείδη:
«Ἅπας ἀριθμός ἤτοι πρῶτος ἔστιν ἢ ὑπό πρώτου τινός ἀριθμοῦ μετρεῖται.»
Στην πρόταση 20, βιβλίο Θ', των «Στοιχείων» του ο Ευκλείδης εξηγεί και αποδεικνύει μια απλή αλλά θεμελιώδη αλήθεια σχετικά με τους πρώτους αριθμούς: ότι είναι άπειροι.
«Οἱ πρῶτοι ἀριθμοί πλείους εἰσί παντός τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν»,

Εφαρμογές 1.3.1

Μια οικογένεια τζιτζικιών στις ανατολικές ΗΠΑ περνάει 13 ή 17 χρόνια κάτω από τη γη ως νύμφες. Μετά από 13 ή 17 έτη εμφανίζεται μαζικά και σε πολύ μεγάλους αριθμούς για να ζευγαρώσει και να γεννήσει τα αυγά της. Οι βιολόγοι πιστεύουν ότι ο χρόνος που περνούν ως νύμφες είναι πρώτος αριθμός προκειμένου να αποφύγουν πληθυσμούς που τρέφονται με αυτές και έχουν επίσης έναν περιοδικό κύκλο ζωής. Αν το τζιτζίκι είχε έναν κύκλο ζωής 12 χρόνια θα συναντούσε τους κυνηγούς του που έχουν περίοδο ζωής 2,3,4,6,12 χρόνια σίγουρα.

Πρόταση 1.3.3 (Ύπαρξη άπειρων πρώτων)**.** *Το σύνολο των πρώτων αριθμών $\mathbb{P}$ είναι άπειρο.*

Σχήμα 1.3.1: Τζιτζίκι Magicada Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Δημιουργός: Bruce Marlin, Πηγή: Wikimedia Commons `https://upload.wikimedia.org/wikipedia/commons/2/20/Magicicada_species.jpg`

Απόδειξη πρώτη (Ευκλείδη)

Υποθέτουμε ότι το σύνολο $\mathbb{P}$ είναι πεπερασμένο,

$$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$$

Θεωρούμε τον φυσικό αριθμό

$$N := p_1 p_2 \ldots p_n + 1$$

Επειδή $N > 1$, από την πρόταση 1.3.2 προκύπτει ότι ο N έχει έναν τουλάχιστο πρώτο διαιρέτη, έστω p. Όμως $p \notin \mathbb{P}$, διότι αν $p = p_i$, για κάποιο $i \in 1, 2, \ldots, n$ θα είχαμε και $p | N - p_1 p_2 \ldots p_n = 1$, άτοπο.

Καταλήξαμε σε άτοπο επειδή υποθέσαμε ότι το $\mathbb{P}$ είναι πεπερασμένο. Άρα το $\mathbb{P}$ είναι άπειρο.

□

Ιστορικά 1.3.2

«Ήταν ένα πολύ όμορφο επιχείρημα. Ο Ευκλείδης δεν διέθετε κάποιον τρόπο παραγωγής πρώτων αριθμών. Είχε όμως αποδείξει ότι η πηγή τους δεν κινδύνευε να στερέψει...»
Marcus du Sautoy *Η μουσική των πρώτων αριθμών* [14].

Απόδειξη δεύτερη (T.J. Stieltjes)

Υποθέτουμε ότι το σύνολο $\mathbb{P}$ είναι πεπερασμένο και έστω

$$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$$

Γράφουμε το γινόμενο των πρώτων $p_1 \cdot p_2 \cdots p_n = A \cdot B$, ως γινόμενο δύο παραγόντων A και B. Κάθε πρώτος αριθμός p_i διαιρεί τον A ή τον B, αλλά όχι συγχρόνως και τους δύο. Θα αποδείξουμε αργότερα ότι αν $p \mid A \cdot B$ τότε $p \mid A$ ή $p \mid B$. Αυτό σημαίνει ότι $p_i \nmid (A + B)$ για κάθε $i = 1, \ldots, n$. Όμως ο $A + B > 1$ έχει έναν τουλάχιστον πρώτο διαιρέτη p, $p \neq p_i$ για κάθε $i = 1, \ldots, n$.

Όπως και στην πρώτη απόδειξη, καταλήξαμε σε άτοπο, επειδή υποθέσαμε ότι το $\mathbb{P}$ είναι πεπερασμένο. Άρα το $\mathbb{P}$ είναι άπειρο.

□

Παρατηρήσεις

1. Η απόδειξη του Ευκλείδη, προκύπτει από την απόδειξη του Stieltjes για $A = 1$.

2. Και οι δύο αποδείξεις χρησιμοποιούν την ίδια ιδέα που είναι η απαγωγή στο άτοπο.

3. Υπάρχουν πολλές αποδείξεις του Θεωρήματος του Ευκλείδη. Παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο [1] το οποίο περιλαμβάνει έξι αποδείξεις και στο [12] το οποίο περιλαμβάνει έντεκα. Η πιο πρόσφατη απόδειξη είναι του Filip Saidak [7].

   Έστω n φυσικός αριθμός > 1. Είναι φανερό ότι οι αριθμοί n και $n + 1$ δεν έχουν κοινό πρώτο παράγοντα. Επομένως ο αριθμός $N_2 = n(n + 1)$ έχει τουλάχιστο δύο διαφορετικούς μεταξύ τους πρώτους παράγοντες. Όμοια και οι φυσικοί αριθμοί $n(n + 1)$ και $n(n + 1) + 1$ δεν έχουν κοινό πρώτο παράγοντα. Επομένως ο

   $$N_3 = n(n + 1)(n(n + 1) + 1)$$

   θα έχει τουλάχιστο τρεις διαφορετικούς μεταξύ τους πρώτους παράγοντες. Η διαδικασία αυτή μπορεί να συνεχιστεί επ' άπειρο, δηλαδή το πλήθος των πρώτων είναι άπειρο.

Η απόδειξη του Saidak είναι ακόμη πιο απλή από την απόδειξη του Ευκλείδη αφού δεν χρησιμοποιεί την «απαγωγή στο άτοπο». Επίσης δεν χρησιμοποιεί την ιδιότητα ότι αν ένας πρώτος p διαιρεί το γινόμενο ab τότε θα διαιρεί τουλάχιστον ένα από τους a, b (δες πόρισμα 1.5.6 το οποίο χρησιμοποιείται σε πολλές άλλες αποδείξεις του Θεωρήματος του Ευκλείδη, 1.3.3). Τέλος, είναι με κάποια έννοια κατασκευαστική αφού μας δίνει θετικούς ακέραιους με οσοδήποτε μεγάλο πλήθος πρώτων παραγόντων.

Πρόταση 1.3.4. *Αν ο φυσικός αριθμός n είναι σύνθετος, τότε έχει έναν πρώτο παράγοντα p, $p \leq \sqrt{n}$.*

Απόδειξη. Αφού ο n είναι σύνθετος, έχει τουλάχιστον μία ανάλυση της μορφής:

$$n = a \cdot b\,, \text{με } 1 < a \leq b < n.$$

Ένα τουλάχιστον από τα a, b είναι μικρότερο ή ίσο της $\sqrt{n}$, διότι αν $a > \sqrt{n}$ και $b > \sqrt{n}$ θα είχαμε $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, άτοπο. Επειδή το $a > 1$ έχει, σύμφωνα με την πρόταση 1.3.2 ένα τουλάχιστον πρώτο διαιρέτη p.

Ο πρώτος αυτός είναι διαιρέτης του n και $p \leq a \leq \sqrt{n}$. □

Η Πρόταση 1.3.4 μας δίνει ένα κριτήριο ελέγχου πρώτων αριθμών.

Παράδειγμα 1.3.5. Ο φυσικός αριθμός $n = 179$ είναι πρώτος. Αν ήταν σύνθετος θα είχε έναν πρώτο διαιρέτη $p \leq \sqrt{179} < 14$. Οι πρώτοι οι μικρότεροι του 14 είναι οι 2, 3, 5, 7, 11 και 13. Κανένας τους δεν διαιρεί το 179. Συνεπώς ο 179 δεν είναι σύνθετος, άρα είναι πρώτος.

Φυσικά το κριτήριο δεν είναι εφαρμόσιμο για μεγάλους φυσικούς αριθμούς.

Παρατήρηση 1.3.6. Αν γνωρίζαμε ότι ένας σύνθετος αριθμός n περιέχει ℓ-το πλήθος διαιρέτες, τότε ένας τουλάχιστον από αυτούς θα είναι μικρότερος από την $\sqrt[\ell]{n}$. Σε διαφορετική περίπτωση, αν δηλαδή και οι ℓ διαιρέτες ήταν γνήσια μεγαλύτεροι του $\sqrt[\ell]{n}$, τότε το γινόμενο θα ήταν γνήσια μεγαλύτερο του n.

Η κρυπτογραφία βασίζεται στη δυσκολία να παραγοντοποιήσουμε έναν σύνθετο αριθμό σε γινόμενο πρώτων. Από την παραπάνω παρατήρηση προκύπτει ότι δυσκολεύουμε περισσότερο την παραγοντοποίηση του αριθμού n αν αυτός είναι γινόμενο δύο πρώτων που είναι περίπου ίδιου μεγέθους κοντά στη $\sqrt{n}$. Από την άλλη το να είναι το n γινόμενο δύο πρώτων παραγόντων είναι η «κερκόπορτα» του αλγορίθμου Fermat, όπως θα δούμε στην πρόταση 3.4.1.

Δυστυχώς, δεν υπάρχει αποτελεσματική μέθοδος πιστοποίησης ενός δοθέντος φυσικού αν είναι πρώτος ή όχι. Στο θέμα αυτό θα επανέλθουμε αργότερα.

Σχήμα 1.3.2: Ερατοσθένης ο Κυρηναίος 276-194 πχ. Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Portrait_of_Eratosthenes.png`

Πρώτος, ο Ερατοσθένης ο Κυρηναίος επινόησε μια τεχνική γνωστή σήμερα ως «Κόσκινο του Ερατοσθένη» για να βρίσκει πρώτους αριθμούς. Σύμφωνα με τη μέθοδο αυτή, αν θέλουμε να βρούμε όλους τους πρώτους μέχρι τον φυσικό αριθμό n, γράφουμε όλους τους ακέραιους από το 2 μέχρι τον φυσικό αριθμό n και διαγράφουμε διαδοχικά όλα τα πολλαπλάσια του 2 του 3, του 5 κλπ. Οι αριθμοί που απομένουν είναι πρώτοι.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	60
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Παρατήρηση 1.3.7. 1. Η μέθοδος αυτή του Ερατοσθένη έγινε γνωστή σε έμας μέσα από το έργο του Νικόμαχου του Γερασηνού «Αριθμητική Εισαγωγή» [16].

2. Ενδιαφέρον παρουσιάζει η ιστοσελίδα

`http://www.utm.edu/research/primes`

του C. Caldwell με τίτλο "The prime pages".

Σχήμα 1.3.3: Euler, Δημιουργός: J.E. Handmann (1718-1781), Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Leonhard_Euler_2.jpg`

Το πρόβλημα του ακριβούς προσδιορισμού της θέσης του n-στου πρώτου αριθμού αποδείχτηκε μέχρι σήμερα ένα άπιαστο όνειρο. Φάινεται ότι στον «πίνακα των πρώτων δεν επικρατεί ούτε νόμος ούτε τάξη», όπως έλεγε και ο Euler. Φυσικό είναι να αναρωτηθούμε αν υπάρχει κάποιο μικρό διάστημα μέσα στο οποίο να ανήκει ο p_n.

Η επόμενη πρόταση μας δίνει ένα άνω φράγμα του p_n το οποίο δεν είναι ικανοποιητικό.

Πρόταση 1.3.8. *Αν p_n είναι ο n-στος πρώτος αριθμός ($n \geq 1$), τότε ισχύει*

$$p_n \leq 2^{2^{n-1}}.$$

Απόδειξη. Για $n = 1$, $p_1 = 2 = 2^{2^{1-1}}$, ισχύει.

Υποθέτουμε ότι ισχύει για όλους τους φυσικούς αριθμούς m, $1 \leq m < n$. Θα αποδείξουμε ότι ισχύει και για n.

Έστω p ένας πρώτος διαιρέτης του αριθμού

$$p_1 p_2 \cdots p_{n-1} + 1.$$

Επειδή ο $p \neq p_i$ $i = 1, 2, \ldots, n-1$ έπεται ότι

$$\begin{aligned} p_n &\leq p \leq p_1 p_2 \cdots p_{n-1} + 1 \leq 2^{2^{1-1}} 2^{2^{2-1}} \cdots 2^{2^{(n-1)-1}} + 1 \\ &= 2 \cdot 2^2 \cdots 2^{2^{n-2}} + 1 \leq 2^{2^{n-1}} \end{aligned}$$

□

Αν p πρώτος, $p \neq 2$ τότε ο p θα είναι περιττός. Επόμένως ο $(p+1)$ θα είναι άρτιος άρα όχι πρώτος. Άρα η ελάχιστη διαφορά μεταξύ δύο διαδοχικών περιττών πρώτων είναι μεγαλύτερη ή ίση του 2.

Ορισμός 1.3.9. Δύο διαδοχικοί περιττοί αριθμοί οι οποίοι είναι πρώτοι, θα λέγονται *δίδυμοι*.

Παράδειγμα 1.3.10. Οι 3 και 5 είναι δίδυμοι, ομοίως οι 29 και 31, 71 και 73, 4967 και 4969.

Το ερώτημα είναι πόσα ζευγάρια διδύμων υπάρχουν.

Η *εικασία των διδύμων πρώτων* είναι ότι υπάρχουν *άπειροι* πρώτοι αριθμοί p τέτοιοι ώστε και ο $p+2$ να είναι πρώτος. Η εικασία είναι *ανοιχτή* μέχρι σήμερα.

Σταχυολογούμε μερικά σχετικά αποτελέσματα. Είναι γνωστό σε όλους ότι η σειρά

$$\sum_{n=1}^{\infty} \frac{1}{n} \text{ αποκλίνει.}$$

Στα 1737 απέδειξε ο Euler κάτι πολύ ισχυρότερο, ότι και η σειρά

$$\sum_{p\in\mathbb{P}} \frac{1}{p} \text{ επίσης αποκλίνει}$$

Το αποτέλεσμα του Euler αποτελεί μια ακόμη απόδειξη ότι υπάρχουν άπειροι πρώτοι αριθμοί (Αν ήταν πεπερασμένοι, η σειρά θα συνέκλινε!).

Ιστορικά 1.3.3

Στα 1849 ο A. Prince de Polignac διατύπωσε την εικασία ότι για κάθε άρτιο φυσικό n υπάρχουν άπειροι πρώτοι αριθμοί p τέτοιοι, ώστε και ο $p+n$ να είναι πρώτος. Η εικασία του Polignac για $n=2$ είναι η εικασία των διδύμων πρώτων.

Στα 1919 ο Viggo Brun απέδειξε ότι, όταν το p διατρέχει όλους τους δίδυμους πρώτους, τότε η σειρά

$$\sum_{p,\ \text{δίδυμος πρώτος}} \frac{1}{p} \text{ συγκλίνει.}$$

Αυτό βέβαια σημαίνει ότι υπάρχουν «πολύ λιγότεροι» δίδυμοι πρώτοι από ότι πρώτοι αριθμοί. Δεν μπορούμε όμως να συμπεράνουμε ότι το πλήθος τους είναι πεπερασμένο!

Ο P. Clement [11] μας έδωσε, στα 1949, ένα κριτήριο ελέγχου των διδύμων πρώτων.

Το ζευγάρι $(n,\ n+2)$ είναι ζευγάρι διδύμων πρώτων, τότε και μόνο τότε, όταν ο $(n+2)$ διαιρεί τον

$$[4((n-1)!+1)+n].$$

Δυστυχώς, όμως, το κριτήριο δεν έχει ουσιαστικά καμία πρακτική σημασία. Στα 1966, ο Chen Jingrun απέδειξε ότι υπάρχουν άπειρου πλήθους πρώτοι p τέτοιοι ώστε ο $p+2$ να είναι πρώτος ή γινόμενο δύο πρώτων.

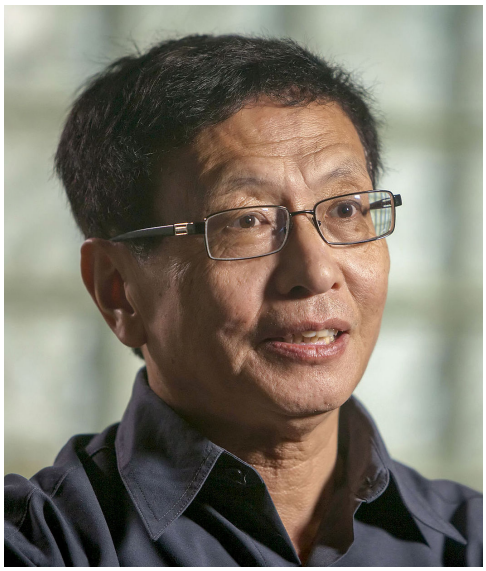
Στα 2004 ο Arenstorf δημοσίευσε μια «απόδειξη» της εικασίας των διδύμων πρώτων.`http://archiv.org/abs/math.NT/0405509`

Δυστυχώς η απόδειξη περιέχει ένα σοβαρό λάθος και αποσύρθηκε. (Δείτε, Eric W. Weisstein "Twin, Prime Proof Proffered"
(`http://mathworld.wolfram.com/news/2004-06-9/twinprimes/`.)

Σημειώστε ότι οι πρώτοι αριθμοί 1000000000061 και 1000000000063 είναι δίδυμοι. Το μεγαλύτερο γνωστό ζευγάρι διδύμων πρώτων μέχρι σήμερα (Μάρτιος 2015) είναι

$$3756801695685 \cdot 2^{666669} \pm 1.$$

Μερικοί συγγραφείς αποκαλούν ζευγάρια πρώτων της μορφής $(p,\ p+4)$ ή $(p,\ p+6)$ *ξαδέρφια* και *sexy πρώτους* αντίστοιχα.



Σχήμα 1.3.4: Yitang Zhang, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons https://en.wikipedia.org/wiki/File:Zhang_2014_hi-res-download_3.jpg

Διάσημοι μαθηματικοί, όπως οι Hardy και Wright ήταν πεπεισμένοι για την ύπαρξη άπειρου πλήθους διδύμων πρώτων. Σημείωναν όμως με έμφαση «is at present beyond the resources of mathematics». Κατά τον Daniel Shanks "the evidence is overwhelming".

1.3.1 Πρόσφατα αποτελέσματα στα κενά των πρώτων

Ο Yitang Zhang, σε μια εργασία του, το 2013 η οποία προκάλεσε αίσθηση, απέδειξε ότι υπάρχει ένας αριθμός N μικρότερος από 70 εκατομμύρια ώστε να υπάρχουν άπειρα ζευγάρια πρώτων που να απέχουν N. Για ένα κατατοπιστικό, ελάχιστα τεχνικό άρθρο ο αναγνώστης μπορεί να δει στο περιοδικό Quanta[1].

Η ιστορία όμως συνεχίστηκε. Ομάδες μαθηματικών μελέτησαν το άρθρο του Zhang και το φράγμα των 70 εκατομμυρίων βελτιωνόταν συνεχώς σε διαδοχικές εργασίες. Τον Ιούλιο του 2013 το φράγμα είχε πέσει στο $N = 4680$. Ακόμα καλύτερα αποτελέσματα εμφανίστηκαν στην εργασία του James Maynard όπου το φράγμα έπεσε στο $N = 600$. Για το θέμα δημιουργήθηκε ένα polymath project, όπου πολλοί μαθηματικοί εργάζονται ταυτόχρονα και ανταλλάσσουν ιδέες με τη βοήθεια του διαδικτύου. Σχετικά με τη συνεργασία αυτή ο αναγνώστης μπορεί να διαβάσει το σχετικό άρθρο στο περιοδικό Quanta. [2]

Αυτή τη στιγμή (31 Μαρτίου 2014), το καλύτερο φράγμα είναι το $N = 6$ κάνοντας χρήση της (γενικευμένης) εικασίας Elliott-Halberstam. Χωρίς τη χρήση της εικασίας αυτής το φράγμα είναι $N = 252$.

[1] https://www.simonsfoundation.org/quanta/
https://www.quantamagazine.org/20130519-unheralded-mathematician-bridges-the-prime-gap/

[2] https://www.simonsfoundation.org/quanta/20131119-together-and-alone-closing-the-prime-gap/

1.3.2 Εικασία του Goldbach

Ο Christian Goldbach (1690-1764), ήταν ένας ερασιτέχνης Γερμανός μαθηματικός ο οποίος ζούσε στη Μόσχα και εργαζόταν στο Υπουργείο Εξωτερικών. Αλληλογραφούσε με τον Leonard Euler, ο οποίος την περίοδο εκείνη ήταν μέλος της Ακαδημίας Επιστημών στην Αγία Πετρούπολη. Την 7η Ιουνίου του 1742 έστειλε επιστολή στον Euler στην οποία του εμπιστεύθηκε την εικασία του ότι

«Κάθε ακέραιος μεγαλύτερος του 2 γράφεται ως άθροισμα τριών πρώτων αριθμών».

("Es scheint wenigstens, dass jede Zahl, die größer ist als 2, ein aggregatum trium primorum sey".)

Ο Goldbach θεωρούσε και το 1 πρώτο αριθμό. Σήμερα η είκασια του Goldbach θα έπρεπε να διατυπωθεί ως εξής:

«Κάθε φυσικός αριθμός μεγαλύτερος του 5 γράφεται ως άθροισμα τριών πρώτων.»

Ο Euler έδειξε ενδιαφέρον για το πρόβλημα και απάντησε στον Goldbach ότι το πρόβλημα ήταν ισοδύναμο με την εικασία ότι, «κάθε άρτιος μεγαλύτερος του 2 γράφεται ως άθροισμα δύο πρώτων».

Η τελευταία εικασία λέγεται *ισχυρή εικασία του Goldbach*.

Η εικασία, ότι *όλοι οι περιττοί ακέραιοι οι μεγαλύτεροι του* 9 γράφονται ως *άθροισμα τριών περιττών πρώτων*, ονομάζεται *ασθενής εικασία του Goldbach*.

Ιστορικά 1.3.4

Ο N. Pipping επαλήθευσε, το 1938, την (ισχυρή) εικασία του Goldbach για $n \leq 10^5$. Επίσης ο Chen Jingrun απέδειξε το 1966 ότι κάθε *άρτιος* $n \geq 4$ είναι άθροισμα δύο αριθμών $p+a$, όπου ο πρώτος αριθμός και a πρώτος ή γινόμενο δύο πρώτων. (Δημοσιεύτηκε στο *Sci. Scinica 16(1973), 157-176)*.
Πρόκειται όμως ακόμη για πολύ μεγάλο αριθμό και είναι αδύνατο να καλυφθεί το ενδιάμεσο διάστημα με τη βοήθεια ηλεκτρονικού υπολογιστή.
Στα 1995, ο Oliver Ramaré απέδειξε ότι κάθε άρτιος $n \geq 4$ γράφεται ως άθροισμα έξι το πολύ πρώτων.
Το 2002, οι R. Heath-Brown και J.G. Puchta (*The Asian Journal of Mathematics*, 6(2002), 535-565), απέδειξαν ότι κάθε «αρκετά μεγάλος» άρτιος αριθμός γράφεται ως άθροισμα δύο πρώτων και ακριβώς 13 δυνάμεις του 2. Ο αριθμός 13 ελαττώθηκε στον αριθμό 8 από τους Pintz και Ruzsa το 2003.
Τέλος σχετικά με την ασθενή εικασία του Goldbach υπάρχει ο ισχυρισμός για μια πλήρη απόδειξη από τον Harald Helfgott το 2013. Τα άρθρα της απόδειξης βρίσκονται εδώ: ArXiV 1305.2897 ArXiV 1205.5252.
Επίσης ο James Maynard (University of Oxford) απέδειξε ότι κάθε περιττός φυσικός μεγαλύτερος ή ίσος του 7 γράφεται ως άθροισμα τριών πρώτων. Την εργασία αυτή την ανακοίνωσε στην 29η Journées Arithmétiques στην οποία ανέφερε ότι την απόδειξη την ολοκλήρωσε το 2013.
Για μια μυθιστορηματική προσέγγιση του θέματος παραπέμπουμε στο διεθνές best seller του Απόστολου Δοξιάδη «Ο Θείος Πέτρος και η εικασία του Goldbach».

Στη συνέχεια θα εξετάσουμε υποσύνολα του συνόλου των φυσικών αριθμών $\mathbb{N}$ και θα ελέγξουμε το πλήθος των πρώτων που υπάρχουν σ' αυτά.

Κάθε ακέραιος a γράφεται σε μία από τις μορφές:

$$4l,\ 4l+1,\ 4l+2,\ 4l+3 \,|\, l \in \mathbb{Z}.$$

Δεν υπάρχει πρώτος αριθμός της μορφής $4l$, αφού όλοι διαιρούνται με 4. Ο 2 είναι ο μόνος πρώτος της μορφής $4l+2$ (για $l=0$), αφού όλοι είναι άρτιοι.

Υπάρχουν πρώτοι αριθμοί της μορφής

$$4l+1, \text{ π.χ. } 5, 13, 17, \ldots$$

Επίσης υπάρχουν πρώτοι αριθμοί της μορφής $4l+3$, π.χ. $3, 7, 11, 19, \ldots$.

Το ερώτημα είναι πόσοι πρώτοι υπάρχουν σε κάθε κλάση.

Πρόταση 1.3.11. *Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής* $4l+3$.

Απόδειξη. Θα υποθέσουμε ότι υπάρχουν *πεπερασμένου* πλήθους πρώτοι αριθμοί της μορφής $4l+3$ και θα καταλήξουμε σε άτοπο.

Έστω λοιπόν ότι *όλοι* οι πρώτοι της μορφής $4l+3$ είναι οι $q_1, q_2, \ldots, q_5$. Ο φυσικός αριθμός $N : 4q_1 q_2 \ldots q_5 - 1 > 0$, έχει έναν τουλάχιστο πρώτο διαιρέτη της μορφής $4l+3$. (Αν όλοι οι πρώτοι διαιρέτες ήταν της μορφής $4l+1$, τότε και το γινόμενό τους θα ήταν της ίδιας μορφής, δηλαδή και ο N).

□

Πρόταση 1.3.12. *Υπάρχουν άπειροι πρώτοι της μορφής* $4l+1$.

Η προτάση 1.3.12 θα αποδειχθεί αργότερα.

Ας προσπαθήσουμε τώρα να γενικεύσουμε. Δίνονται ο φυσικός m, $m > 1$ και ο ακέραιος a, $0 \le a \le m-1$. Θεωρούμε το σύνολο των αριθμών της μορφής $ml+a$, όπου $l \in \mathbb{Z}$.

Αν υποθέσουμε ότι οι m και a *δεν* έχουν κοινό διαιρέτη μεγαλύτερο του ένα, τότε ισχύει το

Θεώρημα 1.3.13 (Θεώρημα του Dirichlet για αριθμητικές προόδους)**.** *Υπάρχουν άπειροι πρώτοι της μορφής* $ml+a$ *όπου* $l \in \mathbb{Z}$.

Το θεώρημα αποδείχθηκε το 1837 από τον L. J. Dirichlet. Η ειδική περίπτωση για $a=1$ είχε διατυπωθεί ως εικασία το 1775 από τον Euler. Ο Legendre διατύπωσε την εικασία γενικά, για κάθε a, το 1785. Προσπάθησε να το αποδείξει αλλά χωρίς πλήρη επιτυχία.

Η απόδειξη του θεωρήματος χρησιμοποιεί προχωρημένα εργαλεία ανάλυσης, και σηματοδοτεί την αρχή της λεγόμενης Αναλυτικής Αριθμοθεωρίας.

Ο ενδιαφερόμενος αναγνώστης μπορεί να βρει την απόδειξη στο: L-σειρές Γιάννη Αντωνιάδη, [15].

Παράδειγμα 1.3.14. Σύμφωνα με το Θεώρημα 1.3.13, το σύνολο

$$A := \{77, 177, 277, \ldots\}$$

περιέχει άπειρο πλήθος πρώτων.

Παρατήρηση 1.3.15. Κάθε κλάση ακέραιων της μορφής $ml+a$ όπου $l \in \mathbb{Z}$, περιέχει και *άπειρο* πλήθος *σύνθετων* ακέραιων.

Πράγματι, αν $a + m \cdot l_0 = p \in \mathbb{P}$ για κάποιο ακέραιο $l_0 \in \mathbb{Z}$, θεωρούμε την ακολουθία

$$l_k = l_0 + k \cdot p \text{ όπου } k = 1, 2, 3, \ldots$$

Για κάθε $k \geq 1$ ισχύει

$$\begin{aligned} m \cdot l_k + a &= m(l_0 + k \cdot p) + a = \\ &= (ml_0 + a) + p(km) = \\ &= p(km + 1), \end{aligned}$$

δηλαδή οι $m \cdot l_k + a | k = 1, 2, \ldots$ είναι σύνθετοι. Αυτό σημαίνει ότι δεν υπάρχει αριθμητική πρόοδος της οποίας όλοι οι όροι να είναι πρώτοι αριθμοί.

1.3.3 Πρώτοι αριθμοί ως διαδοχικοί όροι αριθμητικής προόδου

Στη συνέχεια θα ασχοληθούμε με το ερώτημα της ύπαρξης πρώτων αριθμών ως διαδοχικών όρων αριθμητικής προόδου. Δίνεται ένας φυσικός αριθμός $n > 2$. Υπάρχει πρώτος αριθμός p και φυσικός αριθμός d τέτοιοι ώστε οι n διαδοχικοί όροι της αριθμητικής ακολουθίας

$$p, p + d, \ldots, p + (n - 1)d$$

να είναι όλοι τους πρώτοι αριθμοί;

Έστω $n = 3$. Αν $d = 2$ τότε η μοναδική τριάδα είναι η $3, 5, 7$. Κάθε άλλη τριάδα της μορφής $p, p + 2, p + 4$ έχει έναν όρο διαιρετό με το 3 και διάφορο του 3. Φυσικά και υπάρχουν τριάδες για άλλα d. Έτσι έχουμε μια τριάδα για $d = 6$ την $p = 47, 53, 59$. Το ερώτημα είναι πόσες αριθμητικές πρόοδοι φυσικών αριθμών υπάρχουν οι οποίες να περιέχουν διαδοχικές τριάδες πρώτων αριθμών. Η απάντηση είναι άπειρες. Το αποτέλεσμα αυτό αποδείχθηκε από τον van der Copurt [5], S. Chowla [4] και ως πόρισμα γενικότερης θεωρίας από τον Heath-Brown [13].

Η πιο μικρή τετράδα πρώτων αριθμών η οποία να αποτελεί διαδοχικούς όρους αριθμητικής πρόοδου φυσικών αριθμών είναι αυτή με $p = 5$ και $d = 6$, δηλαδή η $5, 11, 17, 23$.

Το ερώτημα είναι και πάλι πόσες αριθμητικές πρόοδοι φυσικών αριθμών υπάρχουν οι οποίες να περιέχουν κάποια τετράδα διαδοχικών πρώτων. Φυσικά μπορούμε να γενικεύσουμε το ερώτημα αυτό για κάθε φυσικό $n \geq 4$. Η απάντηση δόθηκε πρόσφατα το 2006 από τους B. Green και T. Tao [2].

Θεώρημα 1.3.16 (Διαδοχικοί πρώτοι σε αριθμητικές προόδους)**.** *Για κάθε $n \geq 4$ υπάρχουν άπειρες αριθμητικές πρόοδοι οι οποίες να περιέχουν ως διαδοχικούς όρους n πρώτους αριθμούς.*

Η απόδειξη είναι πολύ δύσκολη και αρκετά πρωτότυπη. Χάρισε μάλιστα το Fields medal στον Tao, το οποίο του απονεμήθηκε στο Διεθνές Συνέδριο Μαθηματικών που έγινε στη Μαδρίτη τον Αύγουστο του 2006. Δυστυχώς όμως το θεώρημα έχει υπαρξιακό χαρακτήρα και δεν μας δίνει συγκεκριμένα παραδείγματα. Έτσι, για τον υπολογισμό παραδειγμάτων τον λόγο έχει ο ηλεκτρονικός υπολογιστής.

Σχήμα 1.3.5: T. Tao, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://en.wikipedia.org/wiki/File:Ttao2006.jpg`

Το μεγαλύτερο n για το οποίο υπάρχει συγκεκριμένη αριθμητική πρόοδος διαδοχικών πρώτων αριθμών μέχρι σήμερα είναι το $n = 24$. Ανακαλύφθηκε από τον Jaroslaw Wroblewski στις 17 Ιανουαρίου του 2007 και είναι η αριθμητική πρόοδος για $p = 468395662504823$ και $d = 205619 \cdot 23$ με $p + d\ell$, $\ell = 0, 1, \ldots, 23$. Στην προσπάθεια εύρεσης αυτής της αριθμητικής προόδου χρησιμοποιήθηκαν 75 ηλεκτρονικοί υπολογιστές.

Θα τελειώσουμε με ένα θεωρητικό αποτέλεσμα. Πρόκειται για μια πρόταση του M. Cantor (1861) [6, τόμος I. σελ. 425].

Πρόταση 1.3.17. *Έστω $d \geq 2$ και $a, a+d, \ldots, a+(n-1)d$ για $n > 2$ πρώτοι αριθμοί, διαδοχικοί όροι αριθμητικής προόδου και q ο μεγαλύτερος πρώτος με $q \leq n$. Τότε ο φυσικός αριθμός*

$$\left(\prod_{p \leq q} p\right) \text{ διαιρεί τον } d$$

ή $p = q$ και $\left(\prod_{p<q} p\right)$ διαιρεί τον d.

Απόδειξη. Αν $r \in \mathbb{P}$ ο οποίος δεν διαιρεί τον d, τότε οι πρώτοι αριθμοί

$$a, a+d, \ldots, a+(r-1)d$$

αφήνουν διαφορετικά υπόλοιπα modulo r, και ο r διαιρεί ακριβώς έναν από αυτούς. Πράγματι αν οι αριθμοί $a+id$ και $a+jd$ αφήνουν το ίδιο υπόλοιπο, αν διαιρεθούν με το r για $i, j \in \{0, 1, \ldots, r-1$, τότε $r \mid d(i-j)$ και επειδή $(d, r) = 1$ έπεται ότι $r \mid (i-j)$. Όμως $0 \leq |i-j| \leq r-1$. Συνεπώς θα πρέπει $i = j$. Επειδή το πλήθος τους είναι r, ένας ακριβώς από αυτούς θα διαιρείται με r.

Στη συνέχεια υποθέτουμε ότι ο $\prod_{p \leq q} p \nmid d$. Αυτό σημαίνει ότι υπάρχει πρώτος $p \leq n$ ο οποίος δεν διαιρεί τον d. Έστω p_0 ο μικρότερος με αυτή την ιδιότητα. Σύμφωνα με τα παραπάνω, υπάρχει ένα j_0, $0 \leq j_0 \leq p_0 - 1$ για το οποίο ισχύει: $p_0 \mid (a + j_0 d)$. Επειδή εξ υποθέσεως, ο $a + j_0 d$ είναι πρώτος, $p_0 = a + j_0 d$. Ο a είναι πρώτος αριθμός. Αν $a \neq a + j_0 d = p_0$ τότε ο a θα διαιρεί τον $d = a\ell$, $\ell \in \mathbb{Z}$, αφού ο p_0 ο ελάχιστος πρώτος με την ιδιότητα $p_0 \nmid d$. Επομένως, $a \mid (a + j_0 d) = a + j_0 a\ell = p_0$. Από τα παραπάνω συμπεραίνουμε ότι $a = p_0$, άτοπο αφού $a \mid d$ ενώ $p_0 \nmid d$. Συνεπώς $a = a + j_0 d = p_0$, δηλαδή $j_0 = 0$ και $a = p_0$.

Αν $p_0 < q \leq n$ τότε $p_0 \leq n-1$ και συνεπώς ο p_0 διαιρεί τον $a + p_0 d$ οπότε και πάλι $p_0 = a + p_0 d = p_0 + p_0 d = p_0(1+d)$, άτοπο.

Αποδείξαμε ότι όταν το γινόμενο $\prod_{p \leq q} p$ δεν διαιρεί το d, τότε ο $q = p_0 = a$ και ότι το γινόμενο $\prod_{p<q} p$ διαιρεί τον d. □

Αν τώρα θεωρήσουμε τους ακέραιους της μορφής $m \cdot l + a$ ως τιμές του πολυωνύμου $f(x) = mx + a$, για $x = l \in \mathbb{Z}$, είναι φυσικό να θεωρήσουμε και πολυώνυμα ανωτέρου βαθμού.

Ας πάρουμε το πολυώνυμο

$$f(x) = x^2 + 1.$$

Για όλα τα $x = 1, \ldots, 40$, το παραπάνω πολυώνυμο δίνει τιμές πρώτους. Έτσι για παράδειγμα υπολογίζουμε ότι:

Για $x = 1$, δίνει $f(1) = 2 \in \mathbb{P}$,
Για $x = 2$, δίνει $f(2) = 5 \in \mathbb{P}$,
Για $x = 4$, δίνει $f(4) = 17 \in \mathbb{P}$,
Για $x = 6$, δίνει $f(6) = 37 \in \mathbb{P}$
για $x = 40$, δίνει $f(40) = 1601 \in \mathbb{P}$.

Εικασία 1.3.18 ((N^2+1)- εικασία)**.** Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής (N^2+1).

Η εικασία μέχρι σήμερα είναι *ανοιχτή*. Το καλύτερο γνωστό σχετικό αποτέλεσμα είναι του Hendrik Iwaniec, από το 1978 [8]:

«Υπάρχουν άπειρες τιμές του N για τις οποίες ο N^2+1 είναι πρώτος ή γινόμενο δύο πρώτων».

Εάν επιθυμούμε να μελετήσουμε το ανάλογο πρόβλημα και για άλλα πολυώνυμα δευτέρου ή ανωτέρου βαθμού, θα πρέπει κατ' αρχήν να περιοριστούμε σε πολυώνυμα με ακέραιους συντελεστές με τον περιορισμό ότι *δεν* υπάρχει *πρώτος*, αριθμός p τέτοιος ώστε να διαιρεί όλες τις τιμές $f(n)$ όπου $n \in \mathbb{Z}$.

Στην περίπτωση αυτή απέδειξε ο H.-E. Richert [3, σελ. 140] το 1968 ότι «υπάρχουν άπειρες τιμές $n \in \mathbb{N}$ για τις οποίες το $f(n)$ είναι γινόμενο το πολύ $(\deg(f)+1)$- πρώτων». (όχι κατ' ανάγκη διαφορετικών μεταξύ τους).

Παρατήρηση 1.3.19. Το αποτέλεσμα του Richert εξασφαλίζει απειρία τιμών $n \in \mathbb{N}$ για τις οποίες το $f(x) = x^2+1$ είναι γινόμενο το πολύ τριών πρώτων, ενώ του Iwaniec για το πολύ δύο πρώτων, αλλά είναι ειδικά μόνο για το συγκεκριμένο πολυώνυμο.

Ιστορικά 1.3.5

Για αιώνες οι μαθηματικοί έψαχναν να ανακαλύψουν έναν απλό τύπο ο οποίος να μας δίνει όλους τους πρώτους αριθμούς, ή τουλάχιστον έναν απλό τύπο που να μας δίνει μόνο πρώτους αριθμούς. Έψαχναν λοιπόν να βρουν μια συνάρτηση

$$f : \begin{bmatrix} \mathbb{N} & \longrightarrow & \mathbb{P} \\ n & \longmapsto & f(n) \in \mathbb{P} \end{bmatrix}$$

Φυσικά θα ήταν πολύ ωραίο αν αυτή η συνάρτηση ήταν πολυώνυμο.
Στα 1772 ο Euler παρατήρησε ότι το πολυώνυμο

$$f(x) = x^2 + x + 17$$

δίνει τιμές *πρώτους* αριθμούς για $x = 1, 2, \ldots, 15$, αλλά όχι για 16. Το ίδιο έτος ο Euler και ο Legendre απέδειξαν ότι το πολυώνυμο

$$f(x) = x^2 + x + 41$$

δίνει τιμές πρώτους αριθμούς για $-41 \leq x < 40$ αλλά όχι για $x = 40$. Πράγματι $f(40) = 40 \cdot 41 + 41 = 41^2$.
Ακόμη, $f(41) = 41 \cdot 42 + 41 = 41 \cdot 43$. Όμως $f(42) = 1847 \in \mathbb{P}$, πρώτος αριθμός. Το πολυώνυμο αυτό θα το ονομάζουμε πολυώνυμο του Euler. Για τις πρώτες 100 τιμές του n δίνει 86 πρώτους αριθμούς. Μέχρι σήμερα όμως δεν είναι γνωστό αν για άπειρο πλήθος n δίνει τιμές πρώτους αριθμούς. Όταν ο $n \leq 10^6$, το πολυώνυμο του Euler δίνει 261081 τιμές πρώτους αριθμούς.
Δεν είναι σήμερα γνωστό αν το πολυώνυμο αυτό δίνει τιμή πρώτο αριθμό για άπειρες ακέραιες τιμές της μεταβλητής x.
Στα 1899 ο E.B. Escott, απέδειξε ότι το πολυώνυμο

$$f(x) = x^2 + 79x + 1601$$

δίνει τιμές *πρώτους* αριθμούς για $x = 0, 1, \ldots, 79$, όχι όμως για $x = 80$.
Το πολυώνυμο του Escott δίνει για τις πρώτες 100 τιμές του n, 95 πρώτους αριθμούς.
Αυτονόητα ανακύπτει το ερώτημα αν υπάρχει πολυώνυμο με ακέραιους συντελεστές το οποίο να δίνει τιμές πρώτους αριθμούς όταν η μεταβλητή x διατρέχει όλους τους φυσικούς αριθμούς. Θα ήταν πολύ ωραίο για να είναι αληθινό!

Πρόταση 1.3.20 (Euler, Goldbach)**.** *Δεν υπάρχει πολυώνυμο*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,\ n \geq 1$$

με συντελεστές ακέραιους αριθμούς τέτοιο ώστε, οι τιμές $f(m)$ να είναι, για κάθε $m \in \mathbb{N}$, πρώτοι αριθμοί.

Απόδειξη. Ας υποθέσουμε ότι υπάρχει ένα τέτοιο πολυώνυμο και θα καταλήξουμε σε άτοπο. Για κάποια τιμή του m, έστω m_0, έχουμε $f(m_0) = p$ πρώτος αριθμός.

Για κάθε ακέραιο t, θεωρούμε την

$$\begin{aligned} f(m_0 + t \cdot p) &= a_n(m_0 + t \cdot p)^n + \cdots + a_1(m_0 + t \cdot p) + a_0 \\ &= (a_n m_0^n + \cdots + a_1 m_0 + a_0) + p \cdot F(t) \end{aligned}$$

όπου $F(t)$ πολυώνυμο του t με ακέραιους συντελεστές.

Επομένως $f(m_0 + t \cdot p) = f(m_0) + p \cdot F(t) = p \cdot (1 + F(t))$.

Επειδή $p | f(m_0 + t \cdot p)$ και οι τιμές του $f(x)$ είναι πρώτοι αριθμοί, έπεται ότι $f(m_0 + t \cdot p) = p$ για *κάθε* ακέραιο t, άτοπο, διότι *κάθε* πολυώνυμο βαθμού n παίρνει μια συγκεκριμένη τιμή το πολύ n-φορές. □

Ας ψάξουμε για συνάρτηση δύο μεταβλητών.

Η συνάρτηση

$$f(x, y) = \frac{1}{2}(y - 1)\left[|A^2 - 1| - (A^2 - 1)\right] + 2,$$

όπου $A = x(y+1) - (y!+1)$ δίνει, όταν τα X και Y διατρέχουν τους φυσικούς, εικόνα, η οποία *περιέχει όλους τους πρώτους αριθμούς*.

Η συνάρτηση δίνει ως εικόνα το 2 άπειρες φορές, ενώ κάθε περιττό πρώτο μόνο μία φορά [9].

Δυστυχώς και πάλι η συνάρτηση δίνει τιμές και σύνθετους ακέραιους.

Ιστορικά 1.3.6

Στα 1976, ο Ρώσος μαθηματικός Matijsevič ανακάλυψε μία πολυωνυμική συνάρτηση με 26 μεταβλητές (όλα τα γράμματα του λατινικού αλφαβήτου). Δίνουμε ακέραιες τιμές στις μεταβλητές και υπολογίζουμε, με τη βοήθεια του υπολογιστή το αποτέλεσμα. Αν το αποτέλεσμα είναι θετικό, τότε είναι πρώτος αριθμός. Κανένας πρώτος δεν διαφεύγει από αυτόν τον τύπο. Και πάλι, δυστυχώς, για κάποιες τιμές των μεταβλητών, δίνει τιμή αρνητικό αριθμό. Μάλιστα οι περισσότερες τιμές που παίρνει η εξίσωση είναι αρνητικές. Στην παραγματικότητα είναι πρακτικώς άχρηστη [14, σελ. 312-313].
Μήπως υπάρχει κάποια άλλη συνάρτηση, όχι κατ' ανάγκη πολυωνυμική η οποία να "παράγει" μόνο πρώτους αριθμούς;
Ο W.H. Mills απέδειξε στα 1947 ότι υπάρχει $\beta \in \mathbb{R}_+$, τέτοιο ώστε $[\beta^{3^n}] \in \mathbb{P}$, για *κάθε* φυσικό n. ([ ], είναι η συνάρτηση ακέραιο μέρος).
Δυστυχώς και αυτό το θεώρημα είναι πρακτικά άχρηστο, διότι ουδείς γνωρίζει την ακριβή τιμή του β!
Ανάλογα αποτελέσματα μπορεί να δει κανείς στις εργασίες των R. Ernvall, *A formula for the least Prime greater than a given integer* , Elem. Math 30(1975) , 13-14 και S. Regimbal, *An Explicit Formula for the Prime Number*, Math. Mag. 48(1975), 230-232.

Αφού δεν τα καταφέραμε να βρούμε μια «μηχανή» η οποία να παράγει πρώτους αριθμούς, είναι φυσικό να αναρωτηθούμε αν μπορούμε να εκτιμήσουμε το πλήθος των πρώτων μέσα σε συγκεκριμένα διαστήματα. Η επόμενη πρόταση μας αποδεικνύει ότι υπάρχουν μεγάλα κενά πρώτων στο σύνολο των φυσικών αριθμών.

Πρόταση 1.3.21. *Υπάρχουν διαστήματα φυσικών αριθμών οσοδήποτε μεγάλα τα οποία δεν περιέχουν κανέναν πρώτο αριθμό.*

Απόδειξη. Έστω $n \in \mathbb{N}$. Κανένας από τους διαδοχικούς φυσικούς αριθμούς $(n+1)!+2$, $(n+1)!+3, \ldots, (n+1)!+(n+1)$ δεν είναι πρώτος, διότι ο $(n+1)!+m$, διαιρείται με m για κάθε $m = 2, 3, \ldots, (n+1)$. □

Παρατήρηση: Για να αποδείξουμε την παραπάνω πρόταση χρειάστηκε να πάμε «αρκετά μακριά» στο σύνολο των φυσικών. π.χ. για $n = 100$, οι αριθμοί $n!+2, \ldots$ είναι πολύ μεγάλοι.

Υπάρχουν όμως διαστήματα στα οποία να εξασφαλίζεται η ύπαρξη πρώτων αριθμών;

Πρόταση 1.3.22 (Αξίωμα του Bertrand)**.** *Για κάθε φυσικό ακέραιο $n > 1$ υπάρχει τουλάχιστο ένας πρώτος p,*

$$n < p < 2n.$$

Απόδειξη. Θα το αποδείξουμε στην παράγραφο 1.4 □

Ιστορικά 1.3.7

Αναφέρεται ως αξίωμα, ίσως διότι ήταν εικασία του Bertrand (1845). Πρωτοαποδείχτηκε από τον Tchebychef στα 1852.
Από το αξίωμα συνεπάγεται ότι το πλήθος των πρώτων είναι άπειρο. Αν ήταν πεπερασμένο και έστω p ο μεγαλύτερος από όλους, τότε στο διάστημα μεταξύ των $p+1$ και $2(p+1)$ θα υπήρχε κάποιος πρώτος q, $p<q$, άτοπο.
Η απόδειξη της πρότασης 1.3.22 απλοποιήθηκε αργότερα από τους Ramanujan και το 1931 από τον δεκαοκτάχρονο τότε P. Erdös.
Πρώτος ο Gauß είχε την ιδέα να εξετάσει αν υπήρχε τρόπος να προβλέψει πόσοι πρώτοι υπάρχουν μικρότεροι από το 100, μικρότεροι από το 1000 και ούτω καθεξής.
Αν $x \in \mathbb{R}_+$, θα προσπαθήσουμε να μετρήσουμε τους πρώτους που είναι $\leq x$.
Τη συνάρτηση αυτή θα την ονομάζουμε $\pi(x)$.

$$\pi(x) := \{p \in \mathbb{P} | p \leq x\} = \sum_{p\in\mathbb{P}\ p\leq x} 1.$$

Έτσι π.χ. έχουμε: $\pi(10) = 4$, αφού οι πρώτοι οι μικρότεροι το 10 είναι οι 2,3,5 και 7. Ομοίως $\pi(100) = 25$ και $\pi(1000) = 168$. Έτσι ενώ μέχρι το 10, ένας στους 2.5 είναι πρώτος, μέχρι το 100 είναι ένας στους 4 και μέχρι το 1000 ένας στους 6.
Ας φτιάξουμε έναν πίνακα.

x	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8
$\pi(x)$	4	25	168	1229	9592	78468	664579	5761455
$\pi(x)/x$	0.4	0.25	0.168	0.1229	0.09592	0.0784	0.0664	0.05761

Βλέπουμε ότι το $\frac{\pi(x)}{x}$ φθίνει καθώς το x αυξάνει. Το ερώτημα είναι πόσο γρήγορα φθίνει.
Το $x/\pi(x)$ στον παραπάνω πίνακα είναι

$$2.5, 4.0, 8.1, 10.4, 12.7, 15.0$$

Ο Gauß λοιπόν παρατήρησε ότι κάθε φορά που πολλαπλασίαζε το x επί 10 έπρεπε να προσθέτει στη μέση απόσταση ανάμεσα σε δύο πρώτους αριθμούς περίπου 23, δηλαδή κάτι πολύ κοντά στο l. Έτσι οδηγήθηκε στην εικασία ότι από 1 μέχρι N υπάρχουν περίπου $ln(N)$ πρώτοι.
Συνεπώς μια καλή προσέγγιση για το $\pi(x)$ είναι x/lnx.
Ο Gauss δεν δημοσίευσε, ως συνήθως, τα αποτελέσματά του. Μερικά χρόνια αργότερα στην ίδια εικασία, με μία επιπλέον σταθερά στον παρονομαστή ως διορθωτικό όρο, οδηγήθηκε ο Legendre.
Η απόδειξη της εικασίας του Gauss άργησε λιγάκι.
Στα 1896 οι Jacques Hadamard και Ch. de la Vallée Poussin κατάφεραν, με χρήση μεθόδων της μιγαδικής ανάλυσης, να αποδείξουν ανεξάρτητα ο ένας από τον άλλο, το Θεώρημα των πρώτων αριθμών.

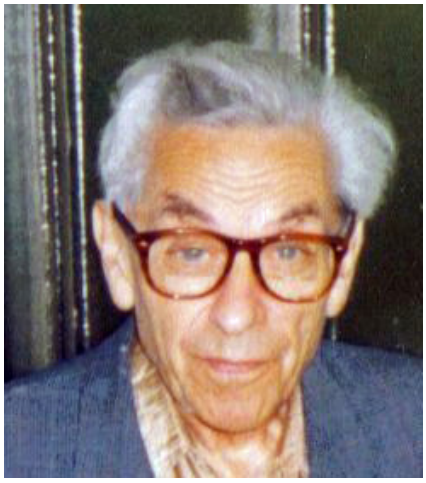
Θεώρημα 1.3.23 (Θεώρημα των πρώτων αριθμών)**.** *Για μεγάλο x η συνάρτηση $\pi(x)$ προσεγγίζει την $x/\log x$, δηλαδή*

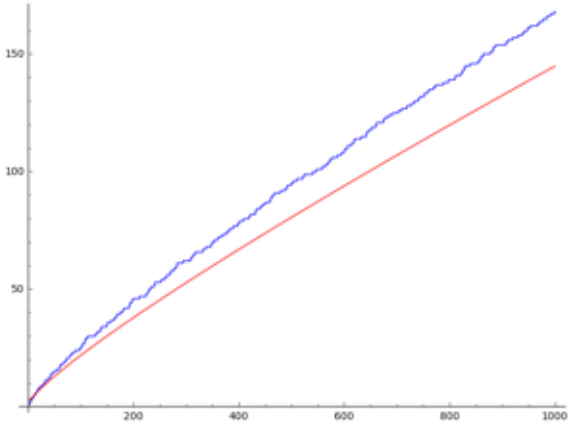
$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Μισό αιώνα αργότερα, το 1948, δόθηκε μια *στοιχειώδης απόδειξη* του θεωρήματος, από τους Paul

Erdös και Alte Selberg, και πάλι ανεξάρτητα ο ένας από τον άλλο.

Σχήμα 1.3.6: P. Erdos και A. Selberg. Το παρόντα έργα αποτελούν κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://en.wikipedia.org/wiki/File:Erdos_head_budapest_fall_1992.jpg` και `https://en.wikipedia.org/wiki/File:Atle_Selberg.jpg`





Σχήμα 1.3.7: Γραφική παράσταση της $\pi(x)$ (μπλέ) και της $x/\log(x)$ (κόκκινο) μέχρι το 1000

Όταν λέμε «στοιχειώδης» απόδειξη, όμως, δεν εννοούμε «απλή». Απλώς, δεν γίνεται χρήση μεθόδων της μιγαδικής ανάλυσης αλλά μόνο απειροστικού λογισμού.

Το αποτέλεσμα αυτό χάρισε στον Alte Selberg το 1950 το βραβείο Fields.

Για περισσότερες πληροφορίες σχετικά με το Θεώρημα των πρώτων αριθμών, παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στις εργασίες.

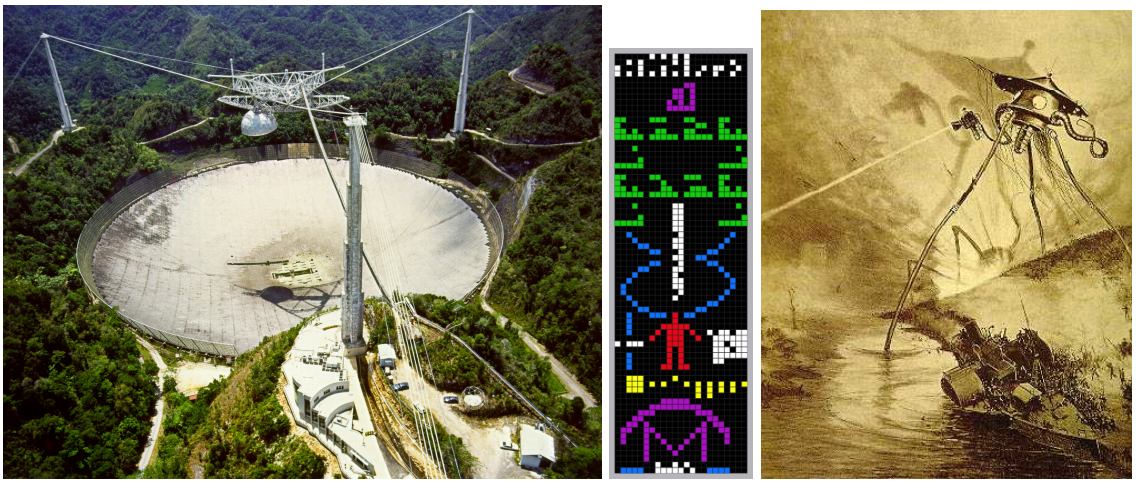
- Μελετία Αλεβυζάκη, *Το θεώρημα των πρώτων αριθμών*, Διπλωματική εργασία, Ηράκλειο 1999.

- N. Levinson, "A motivated account of an elementary proof of the prime number theorem", *American Mathematical Monthly* 76 (1969), 225-245 .

- H. G. Diamond, "Elementary methods in the study of the distribution of prime numbers", *Bull. Amer. Math. Soc.* 7(1982), 553-589 και
- Paul T. Bateman and Harold G. Diamond "A Hundred Years of Prime Numbers" *Amer. Math Monthly* 103 (1996), 729-741.

Εφαρμογές 1.3.2

Το μήνυμα του Arecibo. Είναι μια καλή ιδέα να χρησιμοποιήσουμε τους πρώτους αριθμούς ως βάση επικοινωνίας με εξωγήινους πολιτισμούς. Το παραπάνω μήνυμα είναι ένα σήμα το όποιο σχεδιάστηκε από τον ραδιοαστρόνομο Frank Drake και τον αστροφυσικό Carl Sagan το οποίο αποτελείται από 1679 bits και στάλθηκε με το ομώνυμο ραδιοτηλεσκόπιο στο διάστημα. Ο εξωγήινος πολιτισμός που θα το λάβει θα πρέπει να αναγνωρίσει ότι $1679 = 23 \times 73$ και να «ανάψει» τα bits θέτοντάς τα σε γραμμές και στήλες, οπότε θα σχηματιστεί μια εικόνα που θα περιέχει τους αριθμούς 1-10, ατομικούς αριθμούς των στοιχείων που σχηματίζουν το DNA, στοιχεία σχετικά με τα νουκλεοτίδια του DNA, το σχήμα της διπλής έλικας, τη μορφή ενός ανθρώπου και τον πληθυσμό της γης, όπως και σχεδιαγράμματα του ηλιακού συστήματος και του δίσκου του ραδιοτηλεσκοπίου.
Η ίδια ιδέα εμφανίζεται και στην ταινία «Επαφή», όπου ένα σήμα αναγνωρίζεται ως προϊόν εξωγήινης νοημοσύνης, αφού αποτελείται από ακολουθία πρώτων αριθμών



Σχήμα 1.3.8: Το ραδιοτηλεσκόπιο του Arecibo, το σήμα του Arecibo, και παράσταση εξωγήινου από την Γαλλική έκδοση από του βιβλίου του H.G. Wells, «ο πόλεμος των κόσμων». Τα παρόντα έργα αποτελούν κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://en.wikipedia.org/wiki/File:Arecibo_Observatory_Aerial_View.jpg` Δημιουργός H. Schweiker και `https://en.wikipedia.org/wiki/File:Arecibo_message.svg` και Δημιουργός: A. Correa `https://en.wikipedia.org/wiki/File:War-of-the-worlds-tripod.jpg`

1.3.4 Ασκήσεις

Α Ομάδα (Σωστό ή Λάθος)

1. Το πλήθος των πρώτων είναι υπεραριθμήσιμο.

2. Το πλήθος των άρτιων πρώτων είναι άπειρο.

3. Το πλήθος των περιττών πρώτων είναι αριθμήσιμο.

4. Υπάρχουν άπειροι δίδυμοι πρώτοι.

5. Η ακολουθία
$$99,\ 199,\ 299,\ \ldots,999,\ 1099,\ldots$$
περιέχει άπειρο πλήθος πρώτων.

6. (Εικασία του Tartaglia (1556))

   Τα αθροίσματα

   $1+2+4$
   $1+2+4+8$
   $1+2+4+8+16,$
   είναι διαδοχικά πρώτοι και σύνθετοι αντίστοιχα.

Β Ομάδα (Ασκήσεις Κατανόησης)

1. Αν $(p,\ p+2)$ είναι ένα ζευγάρι διδύμων πρώτων και $p>3$ τότε να αποδείξετε ότι $6|(p+1)$

2. Αν $p\in\mathbb{P},\ p\geq 5$, τότε ο p^2+2 είναι σύνθετος.

3. Κάθε φυσικός αριθμός της μορφής n^4+4 με $n>1$ είναι σύνθετος.

4. Κάθε φυσικός αριθμός $n>11$ μπορεί να γράφει ως άθροισμα δύο σύνθετων (θετικών) ακέραιων.

5. Αν ο φυσικός αριθμός n^3+1 είναι πρώτος, τότε $n=1$.

6. Να αποδείξετε ότι η μοναδική τριάδα πρώτων της μορφής $p,\ p+2$ και $p+4$ είναι 3, 5 και 7.

7. Για ποιούς πρώτους αριθμούς $p,\ 0\,17p+1$ είναι τέλειο τετράγωνο ;

8. Αν ο ελάχιστος πρώτος p που διαιρεί τον n είναι $p>n^{1/3}$, τότε ο άλλος παράγοντας του n θα πρέπει να είναι πρώτος.

9. Να αποδείξετε ότι το πολυώνυμο
$$f(x)=x^2+x+11$$
δίνει τιμές πρώτους αριθμούς για $x=1,\ 2,\cdots,\ 9$ αλλά όχι πρώτο για $x=10$.

Γ Ομάδα (Ασκήσεις Εμπέδωσης)

1. Έστω n ακέραιος, $n \geq 1$ και p πρώτος αριθμός. Αν l είναι η μεγαλύτερη δύναμη του p που διαιρεί το $n!$, δηλάδη $p^l | n!$, ενώ $p^{l+1} \nmid n!$, τότε το l γράφεται

$$l = \sum_{r=1}^{\infty} \left[\frac{n}{p^r} \right]$$

2. Αν $m_1, m_2, \ldots, m_n$ ακέραιοι ≥ 1, να αποδείξετε ότι ο αριθμός

$$\frac{(m_1 + m_2 + \cdots + m_n)!}{m_1!\, m_2! \cdots m_n!}$$

είναι ακέραιος.

Δ Ομάδα (Ασκήσεις Εμβάθυνσης)

1. Να αποδείξετε ότι για κάθε φυσικό αριθμό n ο

$$2^{2^n} + 2^{2^{n-1}} + 1$$

έχει *τουλάχιστον* n διαφορετικούς μεταξύ τους πρώτους διαιρέτες. Στη συνέχεια να συμπεράνετε ότι το πλήθος των πρώτων είναι άπειρο.

1.4 Το αξίωμα του Bertrand

Αν $n > 0$, υπάρχει πάντα πρώτος p τέτοιος ώστε $n < p \leq 2n$

Σημείωση Αν είχα $n > 1$ τότε $n < p < 2n$. Για $n = 1$, $1 < p \leq 2 \cdot 1 \Rightarrow p = 2$ χρειάζεται την ισότητα.

Παρατήρηση Συνήθως η απόδειξη είναι αναλυτικής μορφής και αποτελεί μέρος της απόδειξης του prime number theorem [10]. Εδώ θα δώσουμε μία απόδειξη περισσότερο συνδυαστική, η οποία οφείλεται στον Erdös.

Λήμμα 1.4.1. *Αν $n \geq 1$, τότε:*

1. $2^n \leq \binom{2n}{n} < 2^{2n}$.
2. $\prod_{n<p\leq 2n} p$ *διαιρεί το* $\binom{2n}{n}$.
3. *Αν $r(p)$ ο εκθέτης του p, έτσι ώστε*
$$p^{r(p)} \leq 2n < p^{(r(p)+1)}$$
τότε $\binom{2n}{n} \mid \prod_{p\leq 2n} p^{r(p)}$.
4. *Αν $n > 2$ και $\frac{2n}{3} < p \leq n$, τότε $p \nmid \binom{2n}{n}$.*
5. $\prod_{p\leq n} p < 4^n$.

Απόδειξη. 1. $2n - k \geq 2(n - k)$ για κάθε k, $0 \leq k < n$.

Επομένως $2^n \leq \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{n} = \binom{2n}{1}$. Από την άλλη μεριά, ο αριθμός $\binom{2n}{n}$ είναι ο μεγαλύτερος συντελεστής του $(1+1)^{2n}$, $\binom{2n}{n} < (1+1)^{2n} = 2^{2n}$.

2. $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. Για κάθε $p \in \mathbb{P}$, $n < p \leq 2n$ ισχύει ότι $p \mid (2n)!$ αλλά
$$p \nmid n! \Rightarrow \prod_{n<p\leq 2n} p \mid \binom{2n}{n}.$$

3. Ο εκθέτης του p στο $n!$ είναι $\sum_{j=1}^{r(p)} \left[\frac{n}{p^j}\right]$ (θα το δούμε, στις ασκήσεις).

Επομένως, ο εκθέτης του p στο $\binom{2n}{n}$ είναι
$$\sum_{j=1}^{r(p)} \left\{\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right\} \leq \sum_{j=1}^{r(p)} 1 = r(p)$$

Εδώ χρησιμοποιούμε την ιδιότητα
$$[x] + [y] \leq [x + y]$$
$$2\left[\frac{n}{p^j}\right] = \left[\frac{n}{p^j}\right] + \left[\frac{n}{p^j}\right] \leq \left[\frac{2n}{p^j}\right]$$

και

$$\left\{\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right\} = 0 \text{ ή } 1$$

και συνεπώς

$$\prod_{p\le 2n} p^{r(p)} \ge \binom{2n}{n}.$$

4. Αν $\frac{2n}{3} < p \le n$ τότε το p εμφανίζεται μια φορά στην παραγοντοποίηση του $n!$ και δύο φορές, αφού $3p > 2n$, στην παραγοντοποίηση του $(2n)!$. Επομένως, αφού $n > 2$ και $p > 2$, ισχύει

$$\frac{2n}{3} < p \Rightarrow p \nmid \binom{2n}{n}.$$

5. Έστω $P(n)$ η προς απόδειξη πρόταση

   $P(1)$ $0 \le 4^1$, ισχύει

   $P(2)$ $2 < 4^2$, ισχύει

   $P(3)$ $3 < 4^3$, ισχύει

   Τώρα, αν $m > 1$, Τότε $P(2m-1) \Rightarrow P(2m)$. Πράγματι,

$$\prod_{p\le 2m} p = \prod_{p\le 2m-1} p < 4^{2m-1} < 4^{2m}.$$

   Επομένως, μπορούμε να υποθέσουμε ότι $n = 2m+1$, όπου $m \ge 2$. Για κάθε $p \in \mathbb{P}$, $m+2 \leqq p \le 2m+1$, έχουμε $p \mid \binom{2m+1}{m}$. Αν λοιπόν υποθέσουμε ότι η $P(m+1)$ ισχύει, τότε:

$$\prod_{p\le 2m+1} p \le \binom{2m+1}{m} \prod_{p\le m+1} p < \binom{2m+1}{m} 4^{m+1}.$$

   Αλλά $\binom{2m+1}{m}$ είναι ο (κεντρικός) συντελεστής του αναπτύγματος $(1+1)^{2m+1}$ οπότε

$$\binom{2m+1}{m} < \frac{1}{2}(1+1)^{2m+1} = 4^m.$$

   Συνεπώς αποδείξαμε ότι $P(m+1) \Rightarrow P(2m+1)$. Χρησιμοποιώντας την αλήθεια της πρότασης για $1, 2, 3$ και την αλήθεια των συνεπαγωγών $P(2m-1) \Rightarrow P(2m)$ και $P(m+1) \Rightarrow P(2m+1)$ διαπιστώνουμε την αλήθεια της πρότασης για κάθε φυσικό αριθμό.

□

Απόδειξη. (του αξιώματος του Bertrand). Το αξίωμα ισχύει για $n \le 3$ αφού για $n = 1$, $1 < 2 \le 2$, και για $n = 2$, $2 < 3 \le 4$, για $n = 3$, $3 < 5 \le 6$.

Θα υποθέσουμε ότι είναι λάθος για $n > 3$ και θα καταλήξουμε σε άτοπο.

Από το (4) του λήμματος 1.4.1 όλοι οι πρώτοι παράγοντες p του $\binom{2n}{n}$ επαληθεύουν την ανισότητα

$$p \le \frac{2n}{3}.$$

Έστω $s(p)$, η πιο μεγάλη δύναμη του p η οποία διαιρεί το $\binom{2n}{n}$. Από το (3) του λήμματος 1.4.1 έχουμε:

$$p^{s(p)} \mid \binom{2n}{n} \mid \prod_{p\le 2n} p^{r(p)} \Rightarrow s(p) \le r(p)$$

και καταλήγουμε στην ανισότητα

$$p^{s(p)} \le p^{r(p)} \le 2n. \tag{1.4.1}$$

Επομένως, αν $s(p) > 1$ τότε $p \le \sqrt{2n}$. Συνεπώς δεν υπάρχουν περισσότεροι από $[\sqrt{2n}]$ πρώτοι διαιρέτες του $\binom{2n}{n}$ με εκθέτη > 1. Αυτό έχει ως συνέπεια λόγω της (1.4.1) ότι

$$\binom{2n}{n} \le (2n)^{[\sqrt{2n}]} \prod_{p\le \frac{2n}{3}} p. \tag{1.4.2}$$

Όμως

$$\binom{2n}{n} > \frac{4^n}{2n+1}, \tag{1.4.3}$$

(Εδώ $\binom{2n}{n}$ είναι ο μεγαλύτερος συντελεστής του $(1+1)^{2n} = 4^n$, το οποίο ανάπτυγμα έχει $(2n+1)$-όρους). Από τις εξισώσεις (1.4.2), (1.4.3) και το (5) του λήμματος 1.4.1 έχουμε:

$$\frac{4^n}{2n+1} < (2n)^{[\sqrt{2n}]} \prod_{p\le \frac{2n}{3}} p < 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{2n}}.$$

Προφανώς $2n+1 < (2n)^2$, οπότε απλοποιώντας με $4^{2n/3}$ έχουμε

$$4^{n/3} < (2n)^{2+\sqrt{2n}}.$$

Λογαριθμίζουμε, $\frac{n\ln 4}{3} < (2+\sqrt{2n})\ln 2n$. Αυτό όμως δεν ισχύει για μεγάλα n.

Για παράδειγμα για $n = 750$ έχουμε (χρησιμοποιούμε τις ανισότητες $1,\ 3 < \ln 4$ και $\ln 1500 < 7.5$

$$325 = \frac{750\cdot 1.3}{3} < (2+\sqrt{1500})\ln 1500 < 41\cdot 7.5 < 308, \text{ άτοπο}$$

Συνεπώς το αξίωμα ισχύει για $n \ge 750$. Για $n < 750$ ισχύει επίσης, αφού οι πρώτοι $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 751$ είναι, κάθε φορά, ο καθένας τους 2 φορές του προηγούμενού του. □

1.5 Μ.Κ.Δ. και Ε.Κ.Π.

Έστω a, b ακέραιοι αριθμοί από τους οποίους ένας τουλάχιστον είναι διάφορος του μηδενός. Ένας ακέραιος αριθμός d λέγεται *κοινός διαιρέτης* των a, b όταν $d|a$ και $d|b$.

Θεωρούμε το σύνολο των θετικών ακέραιων που είναι κοινοί διαιρέτες των a και b:

$$S = \{d \in \mathbb{N} \,|\, d|\, a,\ d|b \text{ και } d \ge 1\}.$$

Είναι φανερό ότι $S \neq \emptyset$, αφού $1 \in S$. Αν $d \in S$ τότε $d \le |a|$. Συνεπώς το σύνολο S είναι πεπερασμένο. Το μεγαλύτερο στοιχείο του συνόλου S λέγεται *μέγιστος κοινός διαιρέτης* των a και b και συμβολίζεται ως (a, b).

Ορισμός 1.5.1. Αν a, b ακέραιοι από τους οποίους ένας τουλάχιστον είναι διάφορος του μηδενός. Ο θετικός ακέραιος d λέγεται *μέγιστος κοινός διαιρέτης* των a, b όταν:

1. $d|a$ και $d|b$
2. Αν $d'|a$ και $d'|b$, τότε $d' \leq d$.

Παρατηρήσεις

1. Είναι φανερό ότι $(0, b) = |b|$ και ότι $(a, 0) = |a|$.
2. Αν $a = 0$ και $b = 0$ τότε το σύνολο των κοινών διαιρετών των a, b είναι άπειρο και συνεπώς ο μέγιστος κοινός διαιρέτης δεν ορίζεται. Για λόγους όμως που θα εξηγήσουμε παρακάτω, μπορούμε να ορίσουμε $(0, 0) = 0$.
3. Επειδή οι διαιρέτες του $-a$ συμπίπτουν με τους διαιρέτες του a, μπορούμε στα επόμενα να περιοριστούμε στον μέγιστο κοινό διαιρέτη θετικών ακέραιων.

Παραδείγματα

1. Έστω $a = 15$ και $b = 18$. Ο θετικοί διαιρέτες του a είναι 1, 3, 5, 15. Οι θετικοί διαιρέτες του b, 1, 2, 3, 6, 9, 18. Επομένως, $(15, 18) = 3 = (-1) \cdot 15 + 1 \cdot 18$.
2. Έστω $a = 76$ και $b = 190$. Οι θετικοί διαιρέτες του a είναι 1, 2, 4, 19, 38, 76. Οι θετικοί διαιρέτες του b είναι 1, 2, 5, 10, 19, 38, 95, 190. Επομένως, $(76, 190) = 38$.
3. Έστω $a = 14$ και $b = 55$. Οι θετικοί διαιρέτες του a, είναι 1, 2, 7, 14. Οι θετικοί διαιρέτες του b είναι 1, 5, 11, 55. Επομένως, $(14, 55) = 1$.

   Η εύρεση των διαιρετών ενός ακέραιου δεν είναι εύκολη υπόθεση όταν οι a και b είναι μεγάλοι. Θα πρέπει επομένως να προσπαθήσουμε να χαρακτηρίσουμε τον μέγιστο κοινό διαιρέτη δύο ακέραιων με άλλους τρόπους και να βρούμε πιο γρήγορες δυναμικές μεθόδους υπολογισμού του.

   Παρατηρούμε ότι στα παραδείγματα έχουμε:

   $(76, 190) = 38 = 190 - 2 \cdot 76 = 1 \cdot 190 + (-2) \cdot 76$

   $(14, 55) = 1 = -55 + 4 \cdot 14 = (-1) \cdot 55 + 4 \cdot 14$

Ορισμός 1.5.2. Αν a, b ακέραιοι, τότε κάθε παράσταση της μορφής $ka + lb$, όπου k, l ακέραιοι λέγεται *γραμμικός συνδυασμός* των a και b.

Πρόταση 1.5.3. *Αν a, b ακέραιοι, όχι και οι δύο ίσοι με μηδέν, τότε υπάρχουν ακέραιοι x_0, y_0 τέτοιοι ώστε*

$$d := (a, b) = ax_0 + by_0$$

και μάλιστα ο d είναι ο ελάχιστος θετικός ακέραιος με αυτή την ιδιότητα.

Απόδειξη. Έστω $S := \{ax + by | x, y$ ακέραιοι και $ax + by > 0\}$. Το σύνολο S είναι υποσύνολο του $\mathbb{N}$ και είναι διάφορο του κενού. Πράγματι, αν $a \neq 0$, τότε αν $a > 0$ το $a \in S$, για $x = 1$ και $y = 0$ ενώ αν $a < 0$, τότε $-a \in S$ για $x = -1$ και $y = 0$. Ομοίως αν $b \neq 0$.

Επομένως, από 1.1.2, έχουμε ότι το σύνολο S περιέχει ένα ελάχιστο στοιχείο, έστω d. Αφού $d \in S$, έπεται ότι υπάρχουν ακέραιοι x_0 και y_0 τέτοιοι ώστε

$$d = ax_0 + by_0 > 0.$$

Σύμφωνα με την Πρόταση 1.2.2, υπάρχουν ακέραιοι q και r έτσι ώστε να ισχύει

$$a = d \cdot q + r,\ 0 \leq r < d.$$

Το υπόλοιπο της διαίρεσης γράφεται

$$r = a - d \cdot q = a - (ax_0 + by_0)q = a(1 - qx_0) + b(-y_0 \cdot q).$$

Αν $r > 0$, τότε θα είχαμε ότι $r \in S$ το οποίο όμως είναι άτοπο, διότι το ελάχιστο στοιχείο του S είναι το d, ενώ $r < d$. Επομένως $r = 0$, δηλαδή $d|a$.

Εντελώς όμοια αποδεικνύεται ότι και $d|b$. Από τον ορισμό 1.5.1 προκύπτει

$$d \leq (a,\ b) \tag{1.5.1}$$

Τέλος, ο $(a,\ b)$ αφού διαιρεί τα a και b θα διαιρεί και το $d = ax_0 + by_0$, οπότε θα ισχύει και

$$(a,\ b) \leq d. \tag{1.5.2}$$

Από τις (1.5.1) και (1.5.2) έχουμε $d = (a,\ b)$. □

Άμεση συνέπεια της 1.5.3 είναι ότι ένας ισοδύναμος ορισμός του μέγιστου κοινού διαιρέτη δύο ακέραιων $a,\ b$, $(a,\ b) \neq (0,\ 0)$, είναι ο εξής:

Ο $d = (a,\ b)$ όταν:

1. $d|a$ και $d|b$ και
2. Αν $d' \in \mathbb{N}$, $d'(\geq 1)$ τέτοιο ώστε $d'|a$ και $d'|b$ τότε $d'|d$

(Η 1. είναι ταυτόσημη με την (1) του Ορισμού 1.5.1. Αν ισχύει η 2., τότε $d' \leqq d$, αφού $d'|d$, δηλαδή ισχύει η (2) του ορισμού 1.5.1.

Αν ισχύει η (2) του ορισμού 1.5.1 τότε επειδή $d'|a$ και $d'|b$ έπεται ότι $d'|ax_0 + by_0 = d$)

Ορισμός 1.5.4. Δύο ακέραιοι αριθμοί $a,\ b$ θα λέγονται *πρώτοι μεταξύ τους* όταν $(a,\ b) = 1$.

Στη συνέχεια θα μελετήσουμε μερικές βασικές ιδιότητες του μέγιστου κοινού διαιρέτη.

Πρόταση 1.5.5. $a,\ b,\ c,\ d,\ q, b_i \in \mathbb{Z}$.

1. *Ο* $(a,\ b) = 1$ *ακριβώς τότε όταν υπάρχουν ακέραιοι* $x_0,\ y_0$ *για τους οποίους να ισχύει:*

$$ax_0 + by_0 = 1.$$

2. *Αν* $a|bc$ *και* $(a,\ b) = 1$, *τότε* $a|c$.
3. *Αν* $a = bq + c$, *τότε* $(a,\ b) = (a,\ c)$.
4. *Αν* m *θετικός ακέραιος τότε* $(ma,\ mb) = m\,(a,\ b)$.
5. *Αν* $d|a$ *και* $d|b$ *τότε*

$$\left(\frac{a}{d},\ \frac{b}{d}\right) = \frac{(a,\ b)}{|d|}$$

6. *Αν* $(a,\ b_i) = 1$ *για κάθε* $i = 1,\ 2,\ \ldots,\ n$ *τότε* $(a,\ b_1 b_2 \ldots b_n) = 1$.
7. *Αν* $a|c$, $b|c$ *και* $(a,\ b) = 1$ *τότε* $ab|c$.

Θα αποδείξουμε πρώτα την 1. Αν ο $(a, b) = 1$ τότε από 1.5.3 προκύπτει ότι υπάρχουν ακέραιοι x_0, y_0:

$$ax_0 + by_0 = 1.$$

Αν τώρα $ax_0 + by_0 = 1$ και $d = (a, b)$ επειδή $d|a$ και $d|b$, θα έχουμε ότι και $d|ax_0 + by_0 = 1$. Επειδή d θετικός ακέραιος, $d = 1$.

Τώρα θα αποδείξουμε την 2. Λόγω της πρότασης 1.5.3 η υπόθεση ότι $(a, b) = 1$, μας εξασφαλίζει την ύπαρξη δύο ακέραιων x_0, y_0 τέτοιων ώστε

$$ax_0 + by_0 = 1.$$

Πολλαπλασιάζουμε και τα δύο μέλη της τελευταίας ισότητας με c,

$$(ac)x_0 + (bc)y_0 = c.$$

Η υπόθεση ότι το $a \mid bc$ μας εξασφαλίζει ότι το $a \mid (ac)x_0 + (bc)y_0 = c$.

Πόρισμα 1.5.6. *Αν p πρώτος αριθμός, τότε ισχύουν:*

1. *Αν $p \mid ab$, τότε έχουμε $p \mid a$ είτε $p \mid b$*
2. *Αν ο p διαιρεί το γινόμενο των ακέραιων $a_1 a_2 \dots a_n$ $(n \geq 2)$, τότε θα διαιρεί τουλάχιστον έναν από τους a_i.*
3. *Αν p διαιρεί το γινόμενο πρώτων $p_1 p_2 \dots p_n$ τότε ταυτίζεται με κάποιον p_i.*

Απόδειξη του πορίσματος:

1. Αν $p|a$ δεν έχουμε να αποδείξουμε τίποτα. Έστω ότι $p \nmid a$. Επειδή p πρώτος, $(p, a) = 1$. Η (2) της πρότασης 1.5.5 ($p|ab$ και $(p, a) = 1$) μας δίνει $p|b$.

2. Εφαρμόζουμε επαγωγή ως προς n.

   Για $n = 2$, ισχύει, λόγω της 1. Έστω ότι ισχύει για $(n - 1)$. Θα αποδείξουμε ότι ισχύει και για n. Το $p|a_1 a_2 \dots a_{n-1} a_n = (a_1 a_2 \dots a_{n-1})a_n$. Λόγω της 1. έχουμε $p|(a_1 a_2 \dots a_{n-1})$ είτε $p|a_n$.

   Η υπόθεση της μαθηματικής επαγωγής μας δίνει:

   Από $p|(a_1 a_2 \dots a_{n-1})$ έπειται ότι $p|a_i$ για κάποιο $i \in \{1, 2, \dots, n-1\}$. Άρα ισχύει και για n.

3. Λόγω της 2. το $p \mid p_i$ για κάποιο i, $1 \leq i \leq n$. Επειδή p, p_i πρώτοι, κατ' ανάγκη, $p = p_i$.

Με τα παραπάνω ολοκληρώσαμε την απόδειξη του πορίσματος. Συνεχίζουμε να αποδείξουμε το 3. της πρότασης.

Κάθε κοινός διαιρέτης των a, b διαιρεί και το $a + b(-q) = c$, δηλαδή είναι και κοινός διαιρέτης των b, c. Επίσης κάθε κοινός διαιρέτης των b, c διαιρεί και το $a = bq + c$, δηλαδή είναι κοινός διαιρέτης των a, b.

Τώρα θα αποδείξουμε το 4. Έστω $d_1 := (a, b)$. Υπάρχουν ακέραιοι x_1, y_1 : $d_1 = ax_1 + by_1$. Επομένως, $md_1 = (ma)x_1 + (mb)y_1$. Αν $d_2 := (ma, mb)$, θα έχουμε $d_2|ma$ και $d_2|mb$ οπότε

$$d_2|md_1. \tag{1.5.3}$$

Επίσης υπάρχουν ακέραιοι x_2, y_2 τέτοιοι ώστε

$$d_2 = (ma)x_2 + (mb)y_2 = m(ax_2 + by_2)$$

Επειδή $d_1|a$ και $d_1|b$, προκύπτει ότι $d_1|ax_2 + by_2$. Επομένως

$$md_1|d_2. \tag{1.5.4}$$

Από τις σχέσεις (1.5.3) και (1.5.4), έχουμε $d_2 = md_1$.

Προχωρούμε στην απόδειξη της 5. Είναι φανερό ότι οι $\frac{a}{d}$ και $\frac{b}{d}$ είναι ακέραιοι αριθμοί. Επομένως, η τελευταία παρατήρηση δίνει:

$$\left(d\frac{a}{d},\ d\cdot\frac{b}{d}\right) = |d|\cdot\left(\frac{a}{d},\ \frac{b}{d}\right),$$

δηλαδή το ζητούμενο.

Τώρα θα αποδείξουμε την 6. Υποθέτουμε ότι

$$d := (a,\ b_1b_2\cdots b_n) > 1.$$

Λόγω της πρότασης 1.3.2 ο d έχει τουλάχιστο έναν πρώτο διαιρέτη, έστω p. Ο $p|d|a$ και $p|d|b_1b_2\ldots b_n$. Όμως το πόρισμα 1.5.6 (2), μας δίνει ότι $p|b_{i_0}$ για $i_0 \in \{1,\ 2,\ldots,\ n\}$. Αυτό σημαίνει ότι $p|(a,\ b_{i_0}) = 1$, άτοπο. Άρα $d = 1$.

Θα τελειώσουμε με την απόδειξη της 7. Αφού $a|c$, υπάρχει ακέραιος r τέτοιος ώστε $c = ar$ Ομοίως, αφού $b|c$, Υπάρχει ακέραιος τέτοιος ώστε $c = bs$. Επομένως $ar = bs$, δηλαδή $b|ar$. Η (2) της πρότασης 1.5.5, $((a,\ b) = 1)$ μας δίνει $b|r$. Συνεπώς $r = bt$, για κάποιο ακέραιο t. Τελικά

$$c = ar = a(bt) = (ab)t,\ \text{δηλαδή } ab|c.$$

Η απόδειξη της πρότασης έχει ολοκληρωθεί.

Παρατήρηση 1.5.7. Αν $m \in \mathbb{Z}$ τότε

$$(ma,\ mb) = |m|\cdot(a,\ b).$$

Παρατήρηση 1.5.8. Στην ειδική περίπτωση που $d =(a,\ b)$, έχουμε

$$\left(\frac{a}{d},\ \frac{b}{d}\right) = \frac{(a,b)}{d} = \frac{d}{d} = 1.$$

Σημείωση 1.5.9. Η πρόταση (1) του πορίσματος 1.5.6, λέγεται και «Λήμμα του Ευκλείδη». Περιέχεται στα «Στοιχεία», βιβλίο VII, πρόταση 30.

« Ἐὰν δύο ἀριθμοὶ πολλαπλασιάσαντες ἀλλήλους ποιῶσί τινά, τὸν δὲ γενόμενον ἐξ αὐτῶν μετρῇ τις πρῶτος ἀριθμός, καὶ ἕνα τῶν ἐξ ἀρχῆς μετρήσει»

Τέλος, ας σημειώσουμε ότι η (2) της πρότασης 1.5.5, *δεν* ισχύει αν $(a,\ b) > 1$, π.χ. $6|3\cdot 4$ ενώ $6 \nmid 3$ και $6 \nmid 4$.

Ορισμός 1.5.10. Οι ακέραιοι αριθμοί

$$a_1,\ a_2\cdots,\ a_n$$

θα λέγονται *πρώτοι μεταξύ τους ανά δύο*, όταν ο $(a_i,\ a_j) = 1$, για *κάθε* $i, j \in \{1,\ 2,\ldots,\ n\}$, $i \neq j$.

Στη συνέχεια μπορούμε να διατυπώσουμε και αποδείξουμε την ακόλουθη

Πρόταση 1.5.11. *Αν οι πρώτοι μεταξύ τους ανά δύο ακέραιοι $m_1, m_2, \ldots, m_n$ διαιρούν τον ακέραιο a, τότε και το γινόμενό τους $m := m_1 m_2 \ldots m_n$ διαιρεί επίσης τον a.*

Απόδειξη. Επαγωγικά ως προς n.

Για $n = 1$, είναι φανερό ότι ισχύει. Έστω ότι ισχύει n. Θα αποδείξουμε ότι ισχύει και για $n + 1$.

Από την υπόθεση, συμπεραίνουμε ότι ο $(m_{n+1}, m_j) = 1$, για κάθε $j = 1, 2, \ldots, m$. Λόγω της Πρότασης 1.5.5, (6) έχουμε

$$(m_{n+1}, m_1 m_2 \ldots m_n) = 1$$

Η υπόθεση της μαθηματικής επαγωγής δίνει $m'|a$, όπου $m' := m_1 m_2 \ldots m_n$. Από το (7) της πρότασης (1.5.5) έπεται ότι

$$m' m_{n+1}|a \text{ δηλαδή } m_1 m_2 \ldots m_n m_{n+1}|a$$

□

Στη συνέχεια θα αναφερθούμε σε μία παράλληλη έννοια προς αυτήν του μέγιστου κοινού διαιρέτη, αυτή του *ελαχίστου κοινού* πολλαπλάσιου.

Αν a, b ακέραιοι οι οποίοι διαιρούν τον ακέραιο m, τότε θα λέμε ότι ο m είναι ένα κοινό πολλαπλάσιο των a και b. Επειδή η διαίρεση με το 0 είναι αδύνατη, αυτό σημαίνει ότι υποθέτουμε αυτόματα ότι $a \neq 0$ και $b \neq 0$. Τα γινόμενα $a \cdot b$ και $-a \cdot b$ είναι κοινά πολλαπλάσια των a και b ένα από τα δύο είναι θετικός ακέραιος.

Επομένως το σύνολο

$$S_{a,b} := \{m \in \mathbb{N} | m > 0, \text{ κοινό πολλαπλάσιο των } a \text{ και } b\} \subseteq \mathbb{N}$$

και *δεν* είναι κενό.

Από το αξίωμα του ελαχίστου 1.1.2, έπεται ότι υπάρχει ελάχιστο στοιχείο στο σύνολο $S_{a,b}$.

Ορισμός 1.5.12. Το *ελάχιστο κοινό πολλαπλάσιο* δύο, μη-μηδενικών, ακέραιων a, b ορίζεται ως ελάχιστος θετικός ακέραιος $m := [a, b]$, με τις ιδιότητες

1. $a|[a, b]$ και $b|[a, b]$
2. Αν $a|c$ και $b|c$, c ακέραιος, $c > 0$ τότε $[a, b] \leq c$.

Παράδειγμα 1.5.13.

1. Αν $a = -3$ και $b = 5$ το $[-3, 5] = 15$.
2. Αν $a = 4$ και $b = 6$, το $[4, 6] = 12$.

Αν τώρα ο ακέραιος m είναι ένα κοινό πολλαπλάσιο των a, b τότε το $c := [a, b]|m$. Αυτό είναι ισοδύναμο με την πρόταση ότι το σύνολο

$$M = \{0, \pm c, \pm 2c, \ldots\}$$

περιέχει όλα τα κοινά πολλαπλάσια των a, b. Πράγματι, διαιρούμε το m με το c. Το θεώρημα 1.2.3 μας δίνει,

$$m = cq + r,\ q \in \mathbb{Z},\ r \in \mathbb{Z},\ 0 \leq r < c.$$

Θα αποδείξουμε ότι $r = 0$. Αν υποθέσουμε ότι $r \neq 0$, τότε ($a|m$ και $a|c$) μας δίνει $a|r$. Ομοίως $b|r$. Επομένως το r είναι κοινό πολλαπλάσιο των a και b και είναι θετικός ακέραιος μικρότερος του c, άτοπο. Άρα $r = 0$, οπότε και $c|m$.

Άμεση συνέπεια των παραπάνω είναι ότι ένας ισοδύναμος ορισμός του ΕΚΠ είναι ο εξής:

Ο $e = [a, b]$ τότε και μόνο τότε όταν (i) $a|e$ και $b|e$ (ii) αν $a|c$ και $b|c (c \in \mathbb{Z}_+)$, τότε $e|c$. Αλλά ποια σχέση έχει ο (a, b) με το $[a, b]$;

Πρόταση 1.5.14. *Αν a, b ακέραιοι, $ab \neq 0$ τότε ισχύει $(a, b)[a, b] = |ab|$.*

Απόδειξη. Έστω $d := (a, b)$. Επειδή $d|a$ και $d|b$ έχουμε, $a = dr$ και $b = ds$, $r, s \in \mathbb{Z}$. Αν $m := \frac{|ab|}{d} = \frac{d^2|rs|}{d} = |r \cdot ds| = |rb|$ και $m = |dr \cdot s| = |as|$. Από τις τελευταίες δύο σχέσεις έχουμε $a|m$ και $b|m$. Στη συνέχεια υποθέτουμε ότι $a|c$ και $b|c$, $(c \in \mathbb{Z})$. Επομένως, $c = au = bv$, $(u, v \in \mathbb{Z})$, οπότε $dru = dsv$, δηλαδή $ru = sv$.

Συνεπώς $r|sv$, και επειδή $(r, s) = 1$, έπεται ότι $r|v$, υπάρχει λοιπόν ακέραιος t, τέτοιος ώστε $v = rt$.

Αυτό σημαίνει ότι, $c = bv = brt = \pm m \cdot l$ δηλαδή $m|c$. Συνεπώς $m = [a, b]$. □

Πόρισμα 1.5.15. *Ισχύει $[a, b] = |ab|$ ακριβώς τότε, όταν $(a, b) = 1$.*

Τους ορισμούς του ΜΚΔ και του ΕΚΠ δύο ακέραιων μπορούμε να τους γενικεύσουμε για πεπερασμένου πλήθους ακέραιους αριθμούς.

Ορισμός 1.5.16. Ως ΜΚΔ των ακέραιων $a_1, a_2, \ldots, a_n$ ορίζεται ο θετικός ακέραιος d για τον οποίο ισχύουν:

1. $d|a_1$, $d|a_2, \ldots, d|a_n$ και
2. αν $d'|a_1$, $d'|a_2, \ldots d'|a_n$, τότε $d'|d$.

Ως ΕΚΠ των ακέραιων $a_1, a_2, \ldots, a_n$ ορίζεται ο θετικός ακέραιος c για τον οποίο ισχύουν:

1. $a_1|c$, $a_2|c, \ldots, a_n|c$ και
2. αν $a_1|s$, $a_2|s, \ldots a_n|s$, τότε $c|s$

Παρατηρήσεις

1. Για το πεπερασμένο πλήθος ακέραιων ισχύει πρόταση, ανάλογη της 1.5.3. Συγκεκριμένα $d := (a_1, a_2, \ldots, a_n)$, ακριβώς τότε όταν υπάρχουν ακέραιοι $x_1, x_2, \ldots x_n$ τέτοιοι ώστε $d = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ και μάλιστα ο d είναι ο ελάχιστος θετικός ακέραιος με αυτή την ιδιότητα.
2. Οι ακέραιοι $a_1, a_2, \ldots, a_n$ θα λέγονται *πρώτοι μεταξύ τους* τότε και μόνο τότε όταν
$$(a_1, a_2, \ldots, a_n) = 1.$$
3. Οι έννοιες *πρώτοι μεταξύ τους* και πρώτοι μεταξύ τους ανά δύο δεν συμπίπτουν.
4. Ισχύουν.

   (α') $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$ και

(β΄) $[a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_{n-1}], a_n]$

5. Η πρόταση 1.5.14 *δεν* ισχύει εν γένει για $n > 2$.

   Πράγματι, $(2, 4, 6) = 2$, $[2, 4, 6] = 12$ $(2, 4, 6)\cdot [2, 4, 6] = 2 \cdot 12 = 24 \neq 2 \cdot 4 \cdot 6 = 48$

6. Υπάρχουν βέβαια σχέσεις μεταξύ ΜΚΔ και ΕΚΠ περισσότερων των δύο ακέραιων. Παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο P. Bundschuch, *Einführung in die Zahlentheorie* 2η έκδοση 1992, σελίδες 26 και 27. Συγκεκριμένα ισχύουν:

Πρόταση 1.5.17. *Αν $n_1, n_2, \ldots, n_\ell$, $n'_1, n'_2, \ldots, n'_\ell$ και n ακέραιοι διάφοροι του μηδενός για τους οποίους ισχύουν $n_i \cdot n'_i = n$ $(i = 1, \ldots, \ell)$ τότε*

$$[n_1, n_2, \ldots, n_\ell](n'_1, \ldots, n'_\ell) = |n|.$$

Στο πρόγραμμα sage ο αλγόριθμος του Ευκλείδη υλοποιείται ως εξής:

```
sage: d,u,v = xgcd(1200,1334)
sage: print u,v
219 -197
sage: d == u*12 + v*15
True
```

1.5.1 Ασκήσεις

Α Ομάδα (Σωστό ή Λάθος)

1. Ο $(10, -15) = -5$
2. $(-40, -60) = (-10)(4, 6)$
3. Ο $(2437, 51329) = 1$, διότι $51329(-978) + 2437 \cdot 20599 = 1$
4. Ο $(963, 657) = 18$, αφού $657 \cdot 44 + 963(-30) = 18$
5. Αν $a|bc$ τότε $a|b$ είτε $a|c$.

Β Ομάδα (Ασκήσεις Κατανόησης)

1. Αν $a \in \mathbb{Z}$ και $n \in \mathbb{Z}_+$, τότε $(a, a + n)|n$
2. Αν $(a, b) = 1$ Και $c|a + b$, τότε $(a, c) = (b, c) = 1$
3. Να αποδειχθεί ότι $a|b$ ακριβώς τότε όταν $[a, b] = |b|$
4. Να αποδειχθεί ότι $[9n + 8, 6n + 5] = 54n^2 + 93n + 40$, για κάθε φυσικό αριθμό $n > 0$
5. Αν $(a, b) = 1$, τότε $(a + b, a - b) = 1$ ή 2
6. Αν $d|mn$ και $(m, n) = 1$ να αποδειχθεί ότι $d = d_1 d_2$ όπου $d_1|m$, $d_2|m$ και $(d_1, d_2) = 1$
7. Αν $m > 0$, να αποδειχθεί ότι $[md, mb] = m[a, b]$ Στη συνέχεια να αποδείξετε ότι αν για τους *θετικούς* ακέραιους a, b, c ισχύει $(a, b, c) = 1$, τότε $[ab, bc, ca] = abc$
8. Να αποδείξετε ότι $a|b \cdot c$ ακριβώς τότε όταν $\frac{a}{(a,b)}|c$.
9. Αν $(a, b) = 1$ τότε $(a^n, b^n) = 1$
10. Αν $a^n|b^n$ τότε $a|b$
11. Αν a και b θετικοί ακέραιοι, τότε $(a, b) = [a, b]$ ακριβώς τότε, όταν $a = b$
12. Να αποδειχθεί ότι για κάθε φυσικό αριθμό n το κλάσμα

$$\frac{21n + 4}{14n + 3}$$

είναι ανάγωγο.

Γ Ομάδα (Ασκήσεις Εμπέδωσης)

1. Αν $a, b, c, d \in \mathbb{Z}$, $b > 0$, $d > 0$, $(a, b) = (c, d) = 1$ και $\frac{a}{b} + \frac{c}{d} \in \mathbb{Z}$ τότε $b = d$
2. Αν $(a, b) = r$, $(a, c) = s$ και $(b, c) = 1$ να αποδειχθεί ότι $(a, bc) = rs$. Δώστε ένα αντιπαράδειγμα, όταν $(b, c) > 1$

3. Αν a, b, c θετικοί ακέραιοι και $a|bc$, $a \nmid b$ και $a \nmid c$ τότε ο αριθμός

$$d = \frac{b}{(b, \frac{bc}{a})}|a$$

και μάλιστα $1 < d < a$ (Δηλαδή ο a είναι σύνθετος!)

4. Αν $(a, b, c) = 1$ και $\frac{1}{q} + \frac{1}{b} = \frac{1}{c}$ τότε ο $a + b$ είναι τέλειο τετράγωνο. (64ος Πανελλήνιος Διαγωνισμός στα Μαθηματικά «Ο Θαλής», 1-11-2003).

Δ Ομάδα (Ασκήσεις Εμβάθυνσης)

1. Αν $m \geq 1$ και $a > 1$ τότε
$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m).$$

2. Αν a, m, n θετικοί ακέραιοι και $m \neq n$ τότε
$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{όταν } a \text{ άρτιος} \\ 2, & \text{όταν } a \text{ περιττός} \end{cases}$$

3. Αν m, n θετικοί ακέραιοι και m περιττός τότε
$$(2^m - 1 + 2^n + 1) = 1.$$

1.6 Ο αλγόριθμος του Ευκλείδη

Ο ορισμός του ΜΚΔ δύο ακέραιων δεν βοηθάει στην εύρεσή του, ιδιαίτερα όταν οι ακέραιοι είναι μεγάλοι.

Η πιο αποτελεσματική γνωστή μέθοδος υπολογισμού του ΜΚΔ δύο ακέραιων είναι ο *αλγόριθμος του Ευκλείδη*. Αλγόριθμός είναι μια πεπερασμένη επαναληπτική διαδικασία.

Ας πάρουμε π.χ. $a = 224$ και $b = 35$ εφαρμόζουμε το θεώρημα της διαίρεσης με υπόλοιπο, $a = b \cdot q_1 + r_1$, $224 = 35 \cdot 6 + 14$.

Στη συνέχεια θεωρούμε τους ακέραιους $b = 35$ και $r = 14$ και ξανακάνουμε το ίδιο $b = r_1 q_2 + r_2$ $35 = 14 \cdot t_2 + 7$, και συνεχίζουμε μέχρι που το υπόλοιπο της διαίρεσης να είναι μηδέν. $r_1 = r_2 q_3 + r_3$ $14 = 7 \cdot 2 + 0$.

Ο μέγιστος κοινός διαιρέτης των a και b είναι το τελευταίο μη- μηδενικό υπόλοιπο.

$$(224, 35) = 7.$$

Η γενική μέδοθος είναι η εξής:

Εφαρμόζουμε διαδοχικά το θεώρημα της διαίρεσης με υπόλοιπο:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < |b| \\ b &= r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1} \\ &\text{και} & r_{n-1} = r_n q_{n+1} \end{aligned}$$

Η ακολουθία των υπολοίπων $\{r_i\}_{i\in\mathbb{N}}$ είναι μια γνησίως φθίνουσα ακολουθία μη αρνητικών ακέραιων. Άρα υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $r_{n+1} = 0$.

Ο $(a, b) = r_n$. Πράγματι, ο $r_n | r_{n-1}$, οπότε $r_n | r_{n-2}, \ldots, r_n | b$ και $r_n | a$. Επίσης, αν $d' | a$ και $d' | b$ τότε $d' | r_1$, $d' | r_2, \ldots, d' | r_n$.

Παράδειγμα. $a = 288$, $b = 51$

$$\begin{array}{ll} 288 = 51 \cdot 5 + 33 & | \ (288, 51) = \\ 51 = 33 \cdot 1 + 18 & | \ (51, 33) = \\ 33 = 18 \cdot 1 + 15 & | \ (33, 18) = \\ 18 = 15 \cdot 1 + 3 & | \ (18, 15) = \\ 15 = 3 \cdot 5 & | \ (15, 3) = 3 \end{array}$$

Αν θέλουμε να υπολογίσουμε τους ακέραιους x_0, y_0 τέτοιο ώστε $d = ax_0 + by_0$, ακολουθούμε την αντίστροφη πορεία. Έτσι στο τελευταίο παράδειγμα έχουμε:

$$\begin{aligned} 3 = 18 - 15 &= 18 - (33 - 18) = 2 \cdot 18 - 33 = \\ &= 2(51 - 33) - 33 = 2 \cdot 51 - 33 \cdot 3 = \\ &= 2 \cdot 51 - 3(288 - 5 \cdot 51) = \\ &= 288(-3) + 51 \cdot 17 \end{aligned}$$

Επομένως, $3 = 288(-3) + 51 \cdot 17$

Αν βέβαια τα βήματα εύρεσης του (a, b) είναι πολλά, η αντίστροφη πορεία είναι αρκετά επίπονη.

Στα 1740, ο Καθηγητής του Πανεπιστήμιου του Cambridge, Nicholas Saunderson, διατύπωσε έναν αρκετά πιο απλοποιημένο αλγόριθμο.

Έστω a, b ακέραιοι, $a \geq b > 0$, $d := (a, b) = r_n$, δηλαδή $r_{n+1} = 0$ και $r_i = r_{i+1}q_{i+2} + r_{i+2}$ για $i = 1, 2, \ldots, n$.

Ας ονομάσουμε $r_{-1} := a$ και $r_0 = b$. Ορίζουμε $x_0 = 0$, $x_1 = 1, y_0 = 1$, $y_1 = q_1$ και $x_i = x_{i-2} + x_{i-1}q_i$, $y_i = y_{i-2} + y_{i-1}q_i$.

Πρόταση 1.6.1. *Αν a, b ακέραιοι, $a \geq b > 0$ και $d := (a, b)$ τότε*

$$d = a(-1)^{n-1}x_n + b(-1)^n y_n.$$

Απόδειξη. Θα αποδείξουμε επαγωγικά ότι ισχύει η

$$P(n): \qquad ax_n - by_n = (-1)^{n-1}r_n.$$

Πράγματι, για $n = 0$, ισχύει

$$ax_0 - by_0 = 0 - b = -b \text{ και } (-1)^{-1}r_0 = -b.$$

Επίσης ισχύει και για $n = 1$, δηλαδή

$$ax_1 - by_1 = a \cdot 1 - b \cdot q_1 = r_1.$$

Υποθέτουμε ότι ισχύει για όλους τους φυσικούς $k, 0 \leq k < n$. Θα αποδείξουμε ότι ισχύει και για $k + 1$.

$$P(k+1): \qquad ax_{k+1} - by_{k+1} = (-1)^k r_{k+1}$$

Πράγματι,

$$\begin{aligned} ax_{k+1} - by_{k+1} &= a(x_{k-1} + x_k q_{k+1}) - b(y_{k-1} + y_k q_{k+1}) \\ &= (ax_{k-1} - by_{k-1}) + q_{k+1}(ax_k - bg_k) \end{aligned}$$

Από την υπόθεση της μαθηματικής επαγωγής, προκύπτει ότι

$$\begin{aligned} ax_{k+1} - by_{k+1} &= (-1)^{k-2} r_{k-1} + q_{k+1}(-1)^{k-1} r_k = \\ &= (-1)^k (r_{k-1} - q_{k+1} r_k) = (-1)^k r_{k+1} \end{aligned}$$

Επομένως ισχύει

$$\begin{aligned} d = r_n &= (-1)^{n-1}(ax_n - by_n) \\ &= a(-1)^{n-1} x_n + b(-1)^n y_n. \end{aligned}$$

□

Παράδειγμα. Έστω $a = 455$ και $b = 255$ Εφαρμόζουμε τον ευκλείδειο αλγόριθμο.

$$\begin{aligned} 455 &= 255 \cdot 1 + 200 \quad | \quad a = bq_1 + r_1 \\ 255 &= 200 \cdot 1 + 55 \quad | \quad b = r_1 q_2 + r_2 \\ 200 &= 55 \cdot 3 + 35 \quad | \quad r_1 = r_2 q_3 + r_3 \\ 55 &= 35 \cdot 1 + 20 \quad | \quad r_2 = r_3 q_4 + r_4 \\ 35 &= 20 \cdot 1 + 15 \quad | \quad r_4 = r_5 q_6 + r_6 \\ 15 &= 5 \cdot 3 \quad | \\ (455, 255) &= 5 \quad | \quad r_5 = r_6 q_7 \end{aligned}$$

i	0	1	2	3	4	5	6	7	
q_i		1	1	3	1	1	1	3	
x_i	0	1	1	4	5	9	14	51	
y_i	1	1	2	7	9	16	25	91	

Επομένως $d = (-14) \cdot 455 + 25 \cdot 255$
Παρατηρήσεις:

1. Ο ευκλείδειος αλγόριθμος περιγράφεται στα «Στοιχεία» Κεφάλαιο VII, Πρόταση 2 «Δύο ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν.»

2. Το ερώτημα πώς να υπολογίσουμε τον ΜΚΔ τριών ακέραιων απαντήθηκε επίσης από τον Ευκλείδη στα «Στοιχεία» του Κεφαλαίου VII, Πρόταση 3. «Τριῶν ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν.»

   Εδώ χρησιμοποιούμε την ιδιότητα του ΜΚΔ, οπότε υπολογίζουμε τον ΜΚΔ των δύο πρώτων και αυτού με τον τρίτο.

   Όμοια εργαζόμαστε για τον υπολογισμό του ΜΚΔ περισσοτέρων ακέραιων.

3. Στο ερώτημα πόσο γρήγορος είναι ο ευκλείδειος αλγόριθμος. Μία, πολύ χοντρική, εκτίμηση είναι ότι θα σταματήσει το πολύ μετά από $|b|$-βήματα. Εύκολα αποδεικνύεται ότι για τα διαδοχικά υπόλοιπα

   $$b = r_0,\ r_1,\ r_2, \ldots$$

   ισχύει $r_{i+2} < \frac{1}{2} r_i$, για κάθε $i = 1, 2, \ldots$.

Από αυτή παρατήρηση αυτή *έπεται ότι* ο αλγόριθμος περατούται (σταματάει) μετά από το πολύ $2\log_2(|b|)$-βήματα, από το οποίο προκύπτει ότι χρειάζεται το πολύ $6,65$-φορές τον αριθμό των ψηφίων του b για να σταματήσει.

Ιστορικά 1.6.1

Ο Γάλλος μαθηματικός Gabriel Lamé απέδειξε στα 1845 ότι ο αριθμός των βημάτων είναι μικρότερος από το 5-πλάσιο του αριθμού των ψηφίων του b.
Στα 1970, ο Καναδός μαθηματικός John Dixon καλυτέρευσε το παραπάνω αποτέλεσμα του Lamé (John Dixon, "The number of steps in the Euclidean algorithm" J. Number Theory 2(1970) 414-422).

Από τα παραπάνω γίνεται φανερό πόσο αποτελεσματικός είναι ο αλγόριθμος.

4. Δεν χρειάζεται το θεώρημα της διαίρεσης με υπόλοιπο για τον υπολογισμό των διαδοχικών πηλίκων q_1, $q_2, \ldots$

   Γνωρίζουμε ήδη ότι αυτό είναι το ακέραιο μέρος του πηλίκου του διαιρετέου προς τον διαιρέτη. Με ένα κομπιουτεράκι κάνουμε τη διαίρεση και «ξεχνούμε» το δεκαδικό κομμάτι του αριθμού που βρίσκουμε. Αυτό είναι το αντίστοιχο πηλίκο q. Το αντίστοιχο υπόλοιπο υπολογίζεται εύκολα από
   $$r = \Delta - \delta q$$

5. Το θεώρημα του Saunderson σχετίζεται με τη θεωρία των συνεχών κλασμάτων, κλάδο της θεωρίας αριθμών τον οποίο θα αναπτύξουμε αργότερα.

Ασκήσεις στον Ευκλείδιο Αλγόριθμο

1. Να υπολογίσετε τον (15540, 19980) και να τον γράψετε ως γραμμικό συνδυασμό αυτών των δύο ακέραιων. Στη συνέχεια να κάνετε το ίδιο για το (6660, 15540, 19980)

2. Πόσα βήματα χρειάζεται ο αλγόριθμος του Ευκλείδη για να υπολογίσει τον (a, b), όπου

$$a = \frac{2^n - (-1)^n}{3},\ b = \frac{2(2^{n-1} - (-1)^{n-1})}{3}$$

   και n θετικός ακέραιος

3. Να υπολογίσετε το ΕΚΠ (5040, 7700).

4. Αν a, m, n $(a > 1)$ θετικοί ακέραιοι, να αποδειχθεί ότι

$$(a^m - 1,\ a^n - 1) = a^{(m,n)} - 1.$$

5. Αν m, n θετικοί ακέραιοι και m περιττός, τότε $(2^m - 1,\ 2^n + 1) = 1$.

1.7 Το θεμελιώδες θεώρημα της Αριθμητικής

Ένα από τα πιο σημαντικά θεωρήματα της Θεωρίας Αριθμών είναι το θεμελιώδες θεώρημα της Αριθμητικής . Σύμφωνα με αυτό οι πρώτοι αριθμοί είναι οι «δομικοί λίθοι» του «οικοδομήματος» των φυσικών αριθμών. Έτσι, αν «γνωρίζουμε» όλους τους πρώτους, «γνωρίζουμε» και όλους τους φυσικούς και τις ιδιότητές τους.

Η αυστηρή διατύπωση του θεωρήματος είναι η εξής:

Θεώρημα 1.7.1 (Θεμελιώδες θεώρημα της Αριθμητικής)**.** *Κάθε φυσικός αριθμός $n > 1$ αναλύεται σε γινόμενο πρώτων παραγόντων. Η ανάλυση αυτή είναι μονοσήμαντη.*

Σημείωση: Όταν λέμε «γινόμενο πρώτων» δεν εννοούμε ότι οι πρώτοι παράγοντες είναι μεταξύ τους διαφορετικοί π.χ. $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. Επίσης όταν λέμε ότι η παράσταση είναι "μονοσήμαντη" εννοούμε ότι δεν ξεχωρίζουμε δύο αναλύσεις που διαφέρουν μόνο στη σειρά των παραγόντων, π.χ. οι αναλύσεις του $18 = 2 \cdot 2 \cdot 3$ και $18 = 2 \cdot 3 \cdot 2$ *δεν* είναι μεταξύ τους διαφορετικές.

Απόδειξη. Η απόδειξη θα γίνει σε δύο βήματα.

Βήμα 1ο: Απόδειξη της ύπαρξης μιας τουλάχιστον παραγοντοποίησης. Η απόδειξη του βήματος θα γίνει επαγωγικά ως προς n.

Για $n = 2$, ισχύει αφού ο 2 είναι πρώτος. Υποθέτουμε ότι ισχύει για *όλους* τους φυσικούς $2 \leq i \leq n - 1$.

Θα αποδείξουμε ότι ισχύει και για n. Αν ο n είναι πρώτος, δεν έχουμε τίποτε να αποδείξουμε. Υποθέτουμε λοιπόν ότι ο n είναι σύνθετος. Έστω p_1 ο *ελάχιστος* πρώτος διαιρέτης του n.

Ο n γράφεται, $n = p_1 \cdot m$, όπου m φυσικός, $1 < m \leq n - 1$. Σύμφωνα με την υπόθεση της μαθηματικής επαγωγής ο m αναλύεται σε γινόμενο πρώτων παραγόντων, $m = p_2 p_3 \dots p_l (p_i \in \mathbb{P}$ για κάθε $i = 2, 3, \dots l)$ Επομένως, $n = p_1 p_2 p_3 \dots p_l$, δηλαδή ισχύει και για n, άρα για κάθε φυσικό n, $n > 1$

Βήμα 2ο Υποθέτουμε ότι ο n έχει δύο παραγοντοποιήσεις:

$$n = p_1 p_2 \dots p_l = q_1 q_2 \dots q_s$$

Θα αποδείξουμε ότι οι παραγοντοποιήσεις συμπίπτουν.

Πράγματι, $p_1|n = q_1 q_2 \dots q_s$. Από πόρισμα 1.5.6 3 προκύπτει ότι $p_1 = q_1$ $i \in \{1, 2, \dots, s\}$. Μπορούμε, αλλάζοντας αν χρειαστεί την αρίθμηση ότι $i = 1$, $p_1 = q_1$. Επομένως έχουμε $p_2\, p_3 \dots p_l = q_2\, q_3 \dots q_s$. Εργαζόμαστε όπως παραπάνω και έχουμε $p_2 = q_2$ και $p_3 \dots p_l = q_3\, q_4 \dots q_s$. Συνεχίζουμε όμοια μέχρι να εξαντληθούν όλοι οι πρώτοι από κάποιο μέλος. Αν $l < s$ έχουμε $1 = q_{l+1} \dots q_s$, άτοπο.

Άρα $l = s$ και $p_i = q_i$. □

Παρατηρήσεις

1. Εδώ φαίνεται γιατί αποκλείσαμε το 1 από τους πρώτους αριθμούς. Αν το 1 ελογίζετο μεταξύ των πρώτων *δεν* θα είχαμε *μονοσήμαντη* ανάλυση.

2. Υπάρχει και άλλη απόδειξη η οποία αποφεύγει τη χρήση της (3) του πορίσματος 1.5.6 δηλαδή αποφεύγει τη χρήση της έννοιας του ΜΚΔ και κατ' επέκταση της προσθετικής δομής του $\mathbb{N}$. Οφείλεται στον Γερμανό μαθηματικό E. Zermelo.

3. Το θεμελιώδες θεώρημα της Αριθμητικής δεν ευρίσκεται διατυπωμένο με σαφήνεια σε κάποια πρόταση των «Στοιχείων» του Ευκλείδη, παρά το ότι υπάρχουν προτάσεις που είναι σχεδόν ισοδύναμες με αυτό. Στο βιβλίο IX, πρόταση 1.4 αναφέρεται:

   «Ἐάν ἐλάχιστος ἀριθμός ὑπό πρώτων ἀριθμῶν μετρῆται, ὑπ' ὐυδενός ἄλλου πρώτου ἀριθμοῦ μετρηθήσεται παρέξ τῶν ἐξ ἀρχῆς μετρούντων.»

   Πολλοί ισχυρίζονται ότι θα πρέπει να ήταν γνωστό στον Ευκλείδη. Ούτε στο έργο του A.M. Legendre εμφανίζεται ξεκάθαρα. Η πρώτη σαφής διατύπωσή του εμφανίζεται στο έργο του Gauss "Disquisitiones Arithmeticae" (1801) άρθρο (πρόταση) 16 "THEOREMA. Numerus compositus quicunque unico tantum modo in factores unico resolvi potest."

   Θεώρημα 1.7.2. *Κάθε σύνθετος φυσικός αριθμός αναλύεται μονοσήμαντα σε γινόμενο πρώτων.*

4. Παραθέτουμε σχετικό απόσπασμα από τη σελίδα 43 του βιβλίου «Η μουσική των πρώτων αριθμών» του Marcus Du Sautoy.

   «Οι αρχαίοι Έλληνες ήταν οι πρώτοι που ανακάλυψαν κατά τον 4ο αιώνα π.χ., τη δυναμική των πρώτων αριθμών, ως δομικών λίθων για όλους τους αριθμούς. Διαπίστωσαν ότι κάθε αριθμός μπορεί να δημιουργηθεί από τον πολλαπλασιασμό μεταξύ πρώτων αριθμών. Ενώ πίστευαν λανθασμένα ότι ο αέρας, η φωτιά, το νερό και η γη είναι οι δομικοί λίθοι της ύλης, είχαν πολύ μεγαλύτερη επιτυχία όταν τέθηκε το θέμα του προσδιορισμού των ατόμων της Αριθμητικής. Επί πολλούς αιώνες οι χημικοί αγωνίστηκαν για να προσδιορίσουν τα βασικά συστατικά του αντικειμένου τους, και η ελληνική διαίσθηση βρήκε επιτέλους τη θέση της στον περιοδικό πίνακα του Dimitri Mendeleev, που αποτελεί μία πλήρη περιγραφή των στοιχείων της Χημείας. Αντιθέτως, ενώ οι Έλληνες έκαναν μια καλή αρχή εντοπίζοντας τους δομικούς λίθους της Αριθμητικής, οι μαθηματικοί προσπαθούν ακόμη να κατανοήσουν τη δομή του πίνακα των πρώτων αριθμών.»

5. Υπάρχει κάποιο βιβλίο-μυθιστόρημα το οποίο αναφέρεται στο πώς θα αντιλαμβανόμασταν τον τρισδιάστατο ευκλείδειο χώρο, αλλά ζούσαμε στον διδιάστατο. Το βιβλίο αυτό είναι του E.A. Abbott, Flatland: *A Romance of Many Dimensions*, Dover, New York 1952. Ας

κάνουμε και εμείς για λίγο το ίδιο και ας θεωρήσουμε ότι ο κόσμος των φυσικών αριθμών είναι «άρτιος» δηλαδή αποτελείται μόνο από τους άρτιους ακέραιους.

$$\mathbb{A} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

Είναι φανερό ότι το άθροισμα, η διαφορά και το γινόμενο άρτιων είναι επίσης άρτιος. Θα λέμε ότι ο αριθμός m του $\mathbb{A}$ *διαιρεί* τον αριθμό n αυτού ακριβώς τότε όταν υπάρχει $k \in \mathbb{A}$ τέτοιο ώστε $n = mk$.

Προσοχή: Το 4 *διαιρεί* το 8 στο $\mathbb{A}$ όχι όμως το 12, διότι $12 = 4 \cdot 3$ ενώ ο 3 είναι περιττός και $3 \notin \mathbb{A}$. Ο $p \in \mathbb{A}$ θα λέγεται $\mathbb{A}$-*πρώτος* αν δεν διαιρείται από κανέναν αριθμό του $\mathbb{A}$. (Οι $\mathbb{A}$-ακέραιοι *δεν* διαιρούνται με τον εαυτό τους!).

Οι αριθμοί $2, 6, 10, \ldots$ είναι $\mathbb{A}$- πρώτοι. Μάλιστα όλοι οι $\mathbb{A}$-πρώτοι είναι οι ακέραιοι της μορφής $2k | k \in \mathbb{Z} - 2\mathbb{Z}$.

Μία βασική ιδιότητα των πρώτων αριθμών είναι η (Αν $p|a \cdot b$ τότε $p|a$ είτε $p|b$) (βλ. πόρισμα 1.5.6 (1)).

Η ιδιότητα αυτή δεν ισχύει στους $\mathbb{A}$-ακέραιους. Ο $\mathbb{A}$-ακέραιος 10 που είναι $\mathbb{A}$-πρώτος, διαιρεί το γινόμενο $30 \cdot 50 = 1500$ *δεν* διαιρεί όμως ούτε το 30 ούτε το 50!.

Είναι εύκολο να αποδειχθεί ότι κάθε $\mathbb{A}$- ακέραιος είναι γινόμενο $\mathbb{A}$-πρώτων *δεν* ισχύει όμως το *μονοσήμαυτο*.

π.χ. $1500 = 30 \cdot 50 = 6 \cdot 250$, και οι 30, 50, 6, 250 είναι $\mathbb{A}$- πρώτοι.

Αυτό δείχνει ότι το μονοσήμαντο της παραγοντοποίησης δεν είναι καθόλου προφανές! Αλλά σ' αυτό το θέμα θα επανέλθουμε στο δεύτερο μέρος του βιβλίου.

Καιρός όμως να επιστρέψουμε πίσω στο θεμελιώδες θεώρημα της αριθμητικής. Αν n φυσικός, $n > 1$, αναλύεται μονοσήμαντα σε γινόμενο πρώτων παραγόντων. Αν συμπτύξουμε τους πρώτους παράγοντες σε δυνάμεις και τους διατάξουμε σε αύξουσα ακολουθία έχουμε, $n = p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$, $p_i \in \mathbb{P}$ για $i = 1, 2, \ldots, s$, $p_1 < p_2 < \cdots < p_s$ και οι n_i είναι *θετικοί* ακέραιοι.

Συχνά είναι χρήσιμη και η εξής παράσταση, $n = \prod_{p \in \mathbb{P}} p^{n_p}$, όπου οι εκθέτες είναι φυσικοί αριθμοί *σχεδόν όλοι μηδέν*.

(Αυτό σημαίνει ότι όλοι εκτός από πεπερασμένο πλήθος είναι ίσοι με μηδέν). Η ανάλυση αυτή λέγεται *κανονική* ανάλυση του n. Από το θεμελιώδες θεώρημα της Αριθμητικής προκύπτει ότι ο εκθέτης n_p ορίζεται μονοσήμαντα από τον φυσικό αριθμό n και τον πρώτο p. Συχνά θα τον συμβολίζουμε με $\vartheta_p(n)$.

Αφού κάθε ακέραιος $a \notin \{0, \pm 1\}$, γράφεται στη μορφή $a = \varepsilon \cdot n$, όπου $\varepsilon \in \{+1, -1\}$ και n φυσικός, $n > 1$, έχουμε:

Κάθε ακέραιος a, $a \notin \{0, \pm 1\}$, γράφεται μονοσήμαντα στη μορφή

$$a = \varepsilon \prod_{p \in \mathbb{P}} p^{\vartheta_p(a)} \ , \vartheta_p(a) \geq 0$$

σχεδόν όλοι ίσοι με μηδέν.

Μπορούμε να θεωρήσουμε ότι και ο 1 έχει μια τέτοια παράσταση με όλους τους εκθέτες $\vartheta_p(1) = 0$ για κάθε $p \in \mathbb{P}$.

Αν τώρα $a \in \mathbb{Q}$, $a \neq 0$, αυτός γράφεται $a = \varepsilon \frac{m}{n}$ όπου $\varepsilon \in \{\pm 1\}$ και m, n φυσικοί, $mn \neq 0$.

Αν $m = \prod_{p \in \mathbb{P}} p^{\vartheta_p(m)}$ και $n = \prod_{p \in \mathbb{P}} p^{\vartheta_p(n)}$ οι κανονικές αναλύσεις των m, n αντίστοιχα, έχουμε

$$a = \varepsilon \prod_{p \in \mathbb{P}} p^{\vartheta_p(m) - \vartheta_p(n)} = \varepsilon \prod_{p \in \mathbb{P}} p^{\vartheta_p(a)}$$

όπου $\vartheta_p(a)$ *ακέραιοι* αριθμοί σχεδόν όλοι μηδέν.

Εύκολα αποδεικνύεται ότι η ανάλυση είναι *μονοσήμαντη*.

Επομένως, ο *ρητός* a, $a \neq 0$ είναι *ακέραιος* ακριβώς τότε όταν $\vartheta_p(a) \geq 0$ για κάθε $p \in \mathbb{P}$.

Στη συνέχεια αποδεικνύουμε την

Πρόταση 1.7.3. *Αν a, b ακέραιοι αριθμοί, διάφοροι του μηδενός, τότε $b|a$ ακριβώς τότε όταν $\vartheta_p(b) \leq \vartheta_p(a)$, για κάθε $p \in \mathbb{P}$*

Απόδειξη. Ο b διαιρεί τον a ακριβώς τότε όταν ο ρητός $\frac{a}{b}$ είναι ακέραιος. Αν $a = \varepsilon_a \prod_{p\in\mathbb{P}} p^{\vartheta_p(a)}$ και $b = \varepsilon_b \prod_{p\in P} p^{\vartheta_p(b)}$ οι κανονικές αναλύσεις των a και b η κανονική ανάλυση του ρητού a/b είναι

$$\frac{a}{b} = \varepsilon' \prod_{p\in\mathbb{P}} p^{\vartheta_p(a)-\vartheta_p(b)} \qquad (\varepsilon' = \varepsilon_a\, \varepsilon_b)$$

Ο αριθμός αυτός είναι ακέραιος ακριβώς τότε όταν $\vartheta_p(a) - \vartheta_p(b) \geq 0$, για κάθε $p \in \mathbb{P}$, δηλαδή όταν $\vartheta_p(a) \geq \vartheta_p(b)$ για κάθε πρώτο p. □

Προκειμένου να ισχύει το κριτήριο και στις περιπτώσεις που $a = 0$ ή $b = 0$ εισάγουμε μια τυπική κανονική ανάλυση και για το μηδέν. Επειδή κάθε ακέραιος b διαιρεί το μηδέν, θα πρέπει, αν $0 = \prod_{p\in\mathbb{P}} p^{\vartheta_p(0)}$, να ισχύει $\vartheta_p(b) \leq \vartheta_p(0)$ για *κάθε* πρώτο p και *κάθε* ακέραιο $b (b \neq 0)$.

Για να ισχύει αυτό θα πρέπει να ορίσουμε $\vartheta_p(0) = \infty$, για *κάθε* $p \in \mathbb{P}$. Επομένως ορίζουμε, εντελώς τυπικά,

$$0 = \prod_{p\in\mathbb{P}} p^{\infty}.$$

Σημείωση: Το κριτήριο διαιρετότητας με τον παραπάνω ορισμό ισχύει και όταν $b = 0$ (τότε $a \neq 0$) διότι $0|a$ ισχύει μόνο όταν $a = 0$, οπότε έχουμε $b|a$.

$$\begin{aligned} \Leftrightarrow \infty \leq \vartheta_p(a) &\Leftrightarrow \vartheta_p(a) = \infty \ \forall p \in \mathbb{P} \\ &\Leftrightarrow a = 0 \end{aligned}$$

Η επόμενη πρόταση εκφράζει τον ΜΚΔ και το ΕΚΠ δύο ακέραιων υπο το φως των καινούργιων δεδομένων

Πρόταση 1.7.4. *Αν a, b μη-μηδενικοί ακέραιοι και*

$$a = \varepsilon_a \prod_{p\in\mathbb{P}} p^{\vartheta_p(a)} \quad b = \varepsilon_b \prod_{p\in\mathbb{P}} p^{\vartheta_p(b)}$$

οι κανονικές αναλύσεις τους, τότε

$$(a,\, b) = \prod_{p\in\mathbb{P}} p^{\min\{\vartheta_p(a),\, \vartheta(b)\}} \ \textit{και}\ [a,\, b] = \prod_{p\in\mathbb{P}} p^{\max\{\vartheta_p(a),\, \vartheta(b)\}}$$

Απόδειξη. Η απόδειξη είναι απλή επαλήθευση των απαιτήσεων του ορισμού των ΜΚΔ και ΕΚΠ αντίστοιχα. □

Η πρόταση 1.7.4 είναι χρήσιμη για την απόδειξη ιδιοτήτων του ΜΚΔ και του ΕΚΠ. Για παράδειγμα η πρόταση 1.5.14 αποδεικνύεται αμέσως αφού $\vartheta_p(|a\, b|) = \vartheta_p(a) + \vartheta_p(b) = \min\{\vartheta_p(a),\, \vartheta_p(b)\} + \max\{\vartheta_p(a),\, \vartheta_p(b)\}$ για κάθε $p \in \mathbb{P}$.

Δεν είναι όμως *πρακτική* αφού προϋποθέτει την δυνατότητα εύρεσης της παραγοντοποίησης, κάτι το οποίο είναι εξαιρετικά δύσκολο, όπως θα δούμε παρακάτω.

Τέλος είμαστε σε θέση να αποδείξουμε αυτό που έχουμε ήδη υποσχεθεί.

Πρόταση 1.7.5. *Υπάρχουν άπειροι πρώτοι της μορφής* $4l+3$, $l \in \mathbb{Z}$

Απόδειξη. Η μέθοδος είναι και πάλι η απαγωγή στο άτοπο.

Έστω ότι υπάρχουν πεπερασμένου πλήθους, $p_1, p_2, \ldots, p_s$. Σχηματίζουμε τον φυσικό αριθμό

$$n := 4p_1p_2\ldots p_s - 1$$

Ο αριθμός αυτός, σύμφωνα με την πρόταση 1.7.1, αναλύεται μονοσήμαντα σε γινόμενο πρώτων παραγόντων.

Ισχυρίζομαστε ότι ένας τουλάχιστο από τους παράγοντες είναι της μορφής

$$4l+3.$$

Αν ήταν της μορφής $4l+1$, τότε και το γινόμενό τους θα ήταν αριθμός της μορφής $4l+1$, δηλαδή και ο n, άτοπο. Έστω λοιπόν p πρώτος, $p|n$ και p της μορφής $4l+3$. Ο p θα είναι κάποιος από τους p_i, $i \in \{1, 2, \ldots, s\}$. Επομένως $p|4p_1p_2\ldots p_s$ και $p|n = 4p_1p_2\ldots p_s - 1$. Τελικά ο $p|1$, άτοπο.

Συνεπώς υπάρχουν άπειροι πρώτοι της μορφής $4l+3$, $l \in \mathbb{Z}$.

Σημείωση: Η παραπάνω ιδέα δεν μπορεί να εφαρμοστεί για να μας δώσει την ύπαρξη απειρίας πρώτων της μορφής

$$4l+1,\ l \in \mathbb{Z}.$$

Αυτό διότι το γινόμενο δύο ακέραιων της μορφής $4l+3$ είναι αριθμός της μορφής $4l+1$.

Την περίπτωση αυτή θα την εξετάσουμε αργότερα. □

Πρόταση 1.7.6. *Αν a, b και c θετικοί ακέραιοι με $(b, c) = 1$ και $a^n = bc$, για κάποιον φυσικό $n > 1$ τότε υπάρχουν ακέραιοι a_1, a_2, πρώτοι μεταξύ τους όπου $a = a_1a_2$ και τέτοιοι ώστε $b = a_1^n$ και $c = a_2^n$.*

Απόδειξη. Αν $b = 1$ είτε $c = 1$ η πρόταση είναι φανερή. Επομένως, ας υποθέσουμε ότι $b > 1$ και $c > 1$. Τότε και $a > 1$. Γράφουμε τη μονοσήμαντη ανάλυση σε γινόμενο πρώτων των b, c.

Λόγω της υπόθεσης ότι $(b, c) = 1$ οι αριθμοί b, c δεν έχουν κοινό πρώτο παράγοντα.

$$b = p_1^{b_1}p_2^{b_2}\ldots p_s^{b_s},\ c = q_1^{c_1}q_2^{c_2}\ldots q_l^{c_l}$$

($p_i \neq q_j\ \forall_i = 1, 2, \ldots, s$ και $\forall_j = 1, 2, \ldots, l$)

Η υπόθεση ότι $a^n = bc$ και το μονοσήμαντο της ανάλυσης σε γινόμενο πρώτων μας δίνουν ότι

$$a = p_1^{r_1}\ldots p_s^{r_s}q_1^{s_1}q_2^{s_2}\ldots q_l^{s_l}$$

και ότι

$$p_1^{nr_1}p_2^{nr_2}\ldots p_s^{nr_s}q_1^{ns_1}q_2^{ns_2}\ldots q_l^{ns_l} = p_1^{b_1}p_2^{b_2}\ldots p_s^{b_s}q_1^{c_1}q_2^{c_2}\ldots q_l^{c_l},$$

δηλαδή $b_i = nr_i$ για $i = 1, 2, \ldots s$ και $c_i = ns_i$ για $i = 1, 2, \ldots, l$. Συνεπώς, αν $a_1 = p_1^{r_1}\ldots p_s^{r_s}$ και $a_2 = q_1^{s_1}\ldots q_l^{s_l}$ τότε $a = a_1a_2$ και $b = a_1^n$, $c = a_2^n$. □

Άμεση συνέπεια της πρότασης είναι το ακόλουθο

Πόρισμα 1.7.7. *Έστω $m \geq 2$ και $b_1, b_2, \ldots, b_m$ θετικοί ακέραιοι πρώτοι μεταξύ τους ανά δύο και $a \in \mathbb{Z}$ ώστε*

$$a^n = b_1b_2\cdots b_m.$$

Τότε υπάρχουν m ακέραιοι c_i για τους οποίους ισχύει $b_i = c_i^n$ για κάθε $i = 1, 2, \ldots, m$.

Απόδειξη. Επαγωγικά ως προς m.

Για $m = 2$ ισχύει από την προηγούμενη πρόταση. Έστω ότι ισχύει για $m-1$. Θα αποδείξουμε ότι ισχύει και για m. Πράγματι αν

$$a^n = b_1 b_2 \cdots b_{m-1} b_m,$$

επειδή $(b_m, b_1 b_2 \cdots b_{m-1}) = 1$ έπεται ότι

$$b_m = c_m^n \text{ και } b_1 b_1 \cdots b_{m-1} = d^n \quad (a = c_m d).$$

Λόγω της υπόθεσης της μαθηματικής επαγωγής $b_i = c_i^n$ για $i = 1, 2, \ldots, m-1$. Συνεπώς $b_i = c_i^n$, για $i = 1, 2, \ldots, m-1, m$. □

1.7.1 Ασκήσεις

1. Αν n φυσικός αριθμός $n > 1$ και
$$n = \prod_{i=1}^{n} p_i^{n_i},$$
$n_i > 0$ η κανονική παράσταση αυτού, να αποδείξετε ότι ο n είναι τέλειο τετράγωνο ακριβώς όταν $2 \mid n_i$, για κάθε $i = 1, 2, \ldots, s/$

2. Αν $p \in \mathbb{P}$ να αποδείξετε ότι $p \mid \binom{p}{k}$ για κάθε $k = 1, 2, 3, \ldots, p-1$.

3. Αν $p \mid a^p - b^p$, $p \in \mathbb{P}$ να αποδείξετε ότι τότε $p^2 \mid a^p - b^p$.

4. Αν $n \in \mathbb{N}$, $n > 1$, πόσα ζευγάρια θετικών ακέραιων υπάρχουν ώστε $[a, b] = n$;

5. Αν k, ℓ, m θετικοί ακέραιοι να αποδειχτεί ότι:
$$\max k, \ell, m = k + \ell + m - \min(k, \ell) - \min(k, m) - \min(\ell, m) + \min(k, \ell, m).$$
Συμπεράνετε ότι
$$[k, \ell, n] = \frac{k\ell m[k, \ell, m]}{[k, \ell][k, m][\ell, m]}.$$

6. Αν a, m, n θετικοί ακέραιοι, $a > 1$ να αποδειχτεί ότι
$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

Βιβλιογραφία

[1] Aigner, G.M. Ziegler, and and K.H. Hofmann: *Proofs from the Book*. Springer, Berlin, 2014.

[2] Ben Green, Terence Tao: *The primes contain arbitrarily long arithmetic progressions*. Ann. of Math., 167(2):481–547, 2008.

[3] Bundschuh: *Einführung in die Zahlentheorie*. 2002.

[4] Chowla, S.: *There exists an infinity of 3-combinations of primes in A. P.* Proc. Lahore Philos. Soc., 6(2):15–16, 1944.

[5] der Corput, J. G. van: *Über Summen von Primzahlen und Primzahlquadraten*. Math. Ann., 116(1):1–50, 1939.

[6] E. Dickson: *History of the Theory of Numbers*. 1, 1999.

[7] Filip Saidak: *A new proof of Euclid's theorem*. Am. Math. Mon., 113(10):937–938, 2006.

[8] H. Iwaniec: *Almost-primes represented by quadratic polynomials*. Inv. Math., 47:171–188, 1978.

[9] James J. Tattersall: *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, second edition, 2005.

[10] M. Niven and H.S. Zuckerman and H.L. Montgomery: *An introduction to the theory of numbers*. J. Wiley, 1991.

[11] P. Clement: *Congruences for sets of primes*. Am. Math. Monthly, 96:23–25, 1949.

[12] Paulo Ribenboim: *The Little Book of Bigger Primes*. Springer, 2004.

[13] R. Heath-Brown, D.: *The ternary Goldbach problem*. Rev. Mat. Iberoamericana, 1(1):45–59, 1985.

[14] Marcus du Sautoy: *Η μουσική των πρώτων αριθμών, το μεγαλύτερο ανεπίλυτο μυστήριο των μαθηματικών*. 2005.

[15] Αντωνιάδης, Γιάννης Α.: *Θεωρία Αριθμών ΙΙ, L-σειρές.* Ηράκλειο, 1999.

[16] Σπανδάγου, Ευάγγελου: *Ἡ Ἀριθμητική Εἰσαγωγή τοῦ Νικομάχου, τοῦ Γερασηνοῦ.* 2001.

2

Διοφαντικές Εξισώσεις

2.1 Εισαγωγή

Διοφαντική εξίσωση θα λέγεται κάθε πολυωνυμική εξίσωση της μορφής

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{2.1.1}$$

όπου $f(x_1, x_2, \ldots, x_n)$ πολυώνυμο με συντελεστές *ακέραιους αριθμούς*.

Κάθε n-άδα *ακέραιων* $(x_1, x_2, \ldots, x_n)$ η οποία επαληθεύει την (2.1.1) θα λέγεται *μία λύση* της (2.1.1).

Λύση της εξίσωσης (2.1.1), θα λέγεται η εύρεση *όλων των ακέραιων λύσεων* αυτής.

Βέβαια, δεν είναι πάντοτε δυνατή η λύση μιας διοφαντικής εξίσωσης. Συχνά τίθενται ασθενέστερα ερωτήματα όπως:

1. Έχει η εξίσωση (2.1.1), λύση ή όχι;
2. Αν έχει λύσεις, είναι το πλήθος αυτών πεπερασμένο ή άπειρο;
3. Αν το σύνολο των λύσεων είναι άπειρο, μπορεί να δοθεί παραμετρικά;
4. Αν το σύνολο των λύσεων είναι πεπερασμένο, τότε μπορεί να βρεθεί ένα ανώτερο φράγμα πέρα από το οποίο δεν υπάρχουν λύσεις, ή ο ακριβής αριθμός των λύσεων ή, ακόμη καλύτερα, όλες οι λύσεις;

Στη συνέχεια θα εξετάσουμε μερικές απλές διοφαντικές εξισώσεις.

Σημείωση 2.1.1. Ο χαρακτηρισμός των εξισώσεων ως «διοφαντικές» αποτελεί απόδοση τιμής στο μαθηματικό Διόφαντο που έζησε κατά τον 3ο μ.Χ. αιώνα. Θεωρείται ο πατέρας της Άλγεβρας. Το σημαντικότερο έργο του είναι τα «Αριθμητικά» του. Το έργο του χωρίζεται σε δεκατρία βιβλία. Περιέχουν 189 προβλήματα. Ο Διόφαντος αναπτύσσει τη μεθοδολογία του λύνοντας συγκεκριμένα αριθμητικά προβλήματα. Κατά τον 15ο αιώνα τα «Αριθμητικά» μεταφράστηκαν στα Λατινικά. Πάνω σε ένα τέτοιο αντίγραφο, δίπλα στο περιθώριο των σελίδων του σημείωνε ο Fermat τις παρατηρήσεις του, κάτι που σηματοδοτεί τη γένεση της Θεωρίας Αριθμών στους νεώτερους χρόνους.

Στα νέα Ελληνικά έχουν εκδοθεί από τον Ευάγγελο Σταμάτη, «Διοφάντου Αριθμητικά» Οργανισμός Εκδόσεων Διδακτικών Βιβλίων, Εν Αθήναις 1953.

Σχήμα 2.2.1: Διόφαντος ο Αλεξανδρεύς, Το παρόν έργο αποτελεί κοινό κτήμα λόγω παρέλευσης 70 ετών από τον θάνατο του δημιουργού.

Πάρα πολύ ευχάριστα διαβάζεται και το βιβλίο της Isabella Grigoryevna Bashmakova, *Diophantus and Diophantine Equations* [3] (μετάφραση από τα ρωσικά του A. Shenitzer, *The Mathematical Association of America*, 1997. Του βιβλίου αυτού υπάρχει μετάφραση και στα γερμανικά. Μάλιστα σύντομα θα κυκλοφορήσει και στα Ελληνικά.)

Τέλος, θα πρέπει να σημειώσουμε ότι πριν από περίπου 30 χρόνια βρέθηκαν τέσσερα από τα χαμένα βιβλία των αριθμητικών στα αραβικά. Αγγλική μετάφραση τους περιέχεται στο *Sesiano J. Books IV to VII of Diophantus Arithmetica: In the Arabic Translation attributed to Qustâ Ibn Lûqâ*, Springer, New York 1982.

2.2 Γραμμικές διοφαντικές εξισώσεις

Η γενική γραμμική διοφαντική εξίσωση έχει τη μορφή,

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{2.2.1}$$

όπου $a_1, a_2, \ldots, a_n, c$ ακέραιοι αριθμοί.

Θα ξεκινήσουμε από ένα πρόβλημα που πρότεινε ο Euler στα 1770.

«Να αναλυθεί ο αριθμός 100 σε αθροίσματα δύο θετικών προσθετέων a και b τέτοιων ώστε ο ένας να είναι διαιρετός με 7 και ο άλλος με 11»

Θα πρέπει, ο $a = 7x$, $x \in \mathbb{Z}$, ≥ 1 και $b = 11y$, $y \geq 1$. Δηλαδή θα πρέπει να βρούμε τις λύσεις της γραμμικής διοφαντικής εξίσωσης

$$7X + 11Y = 100$$

φυσικά με τους περιορισμούς $x \geq 1$, $y \geq 1$.

Πρώτα απ' όλα θα μελετήσουμε την ειδική περίπτωση, για $n = 2$. Το ερώτημα είναι, πότε η διοφαντική εξίσωση

$$aX + bY = c \tag{2.2.2}$$

έχει λύση;

Έστω $d := (a, b)$. Αν (x, y) μία λύση της (2.2.2) τότε επειδή $d|a$ και $d|b$ έπεται ότι

$$d|ax + by = c$$

Επομένως, αν η εξίσωση (2.2.2) έχει λύση τότε κατ' ανάγκη $d|c$. Ισχύει και το αντίστροφο.
Αν $d = (a, b)|c$, τότε $c = ds$, $s \in \mathbb{Z}$.
Λόγω της (1.5.3), υπάρχουν ακέραιοι x_0, y_0 τέτοιοι ώστε $d = ax_0 + by_0$. Επομένως,

$$c = ds = (ax_0 + by_0)s = a(x_0 s) + b(y_0 s)$$

δηλαδή η (2.2.2) έχει τη λύση $X = x_0 s$ και $Y = y_0 s$.

Συνεπώς, έχουμε αποδείξει ότι

Πρόταση 2.2.1. *Η διοφαντική εξίσωση (2.2.2) έχει λύση ακριβώς τότε όταν ο* $(a, b)|c$.

Αν η εξίσωση (2.2.2) έχει μία λύση, τότε πόσες και ποιες είναι οι λύσεις αυτής;

Πρόταση 2.2.2. *Αν* (x_0, y_0) *λύση της (2.2.2), τότε η εξίσωση έχει άπειρες λύσεις οι οποίες δίνονται από τους τύπους*

$$x_k = x_0 + (b/d)k, \;\; y_k = y_0 - (a/d)k, \;\; k \in \mathbb{Z}.$$

Απόδειξη. Αν (x', y') οποιαδήποτε άλλη λύση θα έχουμε $ax_0 + by_0 = c$ και $ax' + by' = c$. Επομένως, $a(x' - x_0) = b(y' - y_0)$. Αν $d = (a, b)$ και γράψουμε $a = da'$ και $b = db'$, $a', b' \in \mathbb{Z}$, τότε $(a', b') = 1$.

Επομένως, έχουμε $a'(x' - x_0) = b'(y' - y_0)$ και συνεπώς, από (1.5.5-2) $a'|(y_0 - y')$, δηλαδή υπάρχει ακέραιος k τέτοιος ώστε $y_0 - y' = a'k$. Η παραπάνω σχέση γράφεται $x' - x_0 = b'k$, $x' = x_0 + b'k$ οπότε και $y' = y_0 - a'k$.

Αποδείξαμε ότι η λύση (x', y'), γράφεται στη μορφή

$$\left[\begin{array}{l} x' = x_0 + \left(\frac{b}{d}\right)k \\ \\ y' = y_0 - \left(\frac{a}{d}\right)k \end{array} \right]$$

για *κάποιο* ακέραιο k, τέλος παρατηρούμε ότι για *κάθε* ακέραιο k το (x_k, y_k) είναι λύση της (2.2.2). □

Πόρισμα 2.2.3. *Αν* $(a, b) = 1$ *η (2.2.2) έχει πάντοτε λύση και αν* (x_0, y_0) *μία λύση αυτής, τότε όλες οι λύσεις δίνονται από*

$$\left[\begin{array}{l} x_k = x_0 + b_k \\ \\ y_k = y_0 - a_k \end{array} \right], k \in \mathbb{Z}$$

Απομένει, μέχρι στιγμής, αναπάντητο το ερώτημα, πώς θα βρούμε μια λύση (x_0, y_0) της εξίσωσης (2.2.2). Η απάντηση όμως είναι εύκολη. Γράφουμε τον $(a, b) = ax_1 + by_1$, οπότε

$$\left(x_0 = x_1 \cdot \frac{c}{d}, \;\; y_0 = y_1 \cdot \frac{c}{d}\right)$$

είναι η ζητούμενη λύση.

Ας γυρίσουμε τώρα στο αρχικό μας παράδειγμα. $(7, 11) = 1$, άρα η εξίσωση έχει λύση. $11 = 7+4$, $7 = 4+3$, $4 = 3+1$, $3 = 1\cdot 3+0$, $1 = 4-3 = 4-(7-4) = 2\cdot 4-1 = 2(11-7)-7 = 2\cdot 11-3\cdot 7$. Επομένως, $x = -3$ και $y = 2$, δηλαδή $(x_0 = -300,\ y_0 = 200)$ είναι μία λύση.

Όλες οι λύσεις είναι,

$$x_k = -300 + 11k \qquad y_k = +200 - 7k.$$

Εξετάζουμε ποιες από αυτές τις λύσεις είναι θετικές.

$$-300 + 11k > 0 \text{ και } 200 - 7k > 0.$$

Το σύστημα αυτό των ανισοτήτων δίνει:

$$27 + \frac{3}{11} < k < 28 + \frac{4}{7}$$

Η μόνη ακέραια τιμή του k, στο διάστημα αυτό είναι $k = 28$ η οποίας μας δίνει τη λύση

$$x = 8 \text{ και } y = 4$$

Συνεπώς η λύση στο πρόβλημα του Euler είναι ($7 \cdot 8 = 56$ και $4 \cdot 11 = 44$).

Παρατηρήσεις

1. Η παραμετρικοποίηση των λύσεων δεν είναι μονοσήμαντη. Αν στη λύση του παραδείγματος θέσουμε $k = 28 - l$ βρίσκουμε $x_l = 8 - 11l$ και $y_l = 4 + 7l$, $l \in \mathbb{Z}$.

2. Ανάλογα αποδεικνύεται ότι η εξίσωση (2.2.1) έχει ακέραια λύση ακριβώς τότε όταν ο $(a_1,\ a_2, \ldots, a_n) | c$. Το αποτέλεσμα αυτό ανάγεται [4, σελ. 184] στον Gauss (1801).

3. Η εύρεση των λύσεων μιας εξίσωσης της μορφής (2.2.1), για $n > 2$, ανάγεται σε επίλυση εξίσωσης δύο μεταβλητών και μελετάται στην επόμενη παράγραφο.

4. Πλήρη λύση της εξίσωσης (2.2.2) εμφανίζεται για πρώτη φορά στο έργο των Ινδών αστρονόμων Aryabhata και Brahmagupta τον 6ο μ.Χ. αιώνα. Η μέθοδός τους στηρίζεται στον αλγόριθμο του Ευκλείδη.

   Κατά παράδοξο τρόπο δεν αναφέρεται ούτε στον Ευκλείδη ούτε στον Διόφαντο, παρά το ότι και οι δύο έχουν ασχοληθεί με πολύ πιο δύσκολες εξισώσεις (ανώτερου βαθμού).

2.2.1 Γραμμικές Διοφαντικές εξισώσεις n-μεταβλητών.

Πρόταση 2.2.4. *Αν $a_1, a_2, \ldots, a_n (n \geq 2)$, μη-μηδενικοί ακέραιοι και b ακέραιος, τότε η γραμμική διοφαντική εξίσωση*

$$a_1X_1 + a_2X_2 + \cdots + a_nX_n = b$$

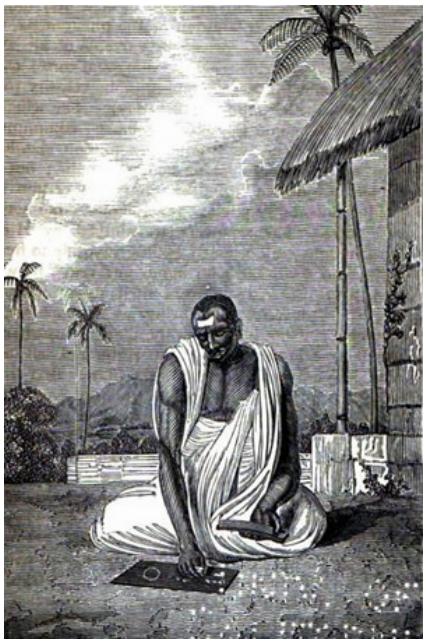
έχει λύση, ακριβώς τότε όταν ο $d := (a_1, a_2, \ldots, a_n) \mid b$. Όταν έχει λύση, το πλήθος των λύσεων είναι άπειρο και μάλιστα δίνεται μέσω $(n-1)$-παραμέτρων.

Απόδειξη. Αν $(x_1, x_2, \ldots, x_n)$ μια λύση της εξίσωσης, τότε από τη σχέση

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

και το γεγονός ότι $d \mid a_i$ για κάθε $i = 1, 2, \ldots, n$ έπεται ότι $d \mid b$. Επομένως, αν $d \nmid b$, τότε η εξίσωση δεν έχει λύση.

Σχήμα 2.2.2: Aryabhata και Brahmagupta Copyright:Public Domain, Τα παρόντα έργα αποτελούν κοινό κτήμα (public domain). Πηγή: Wikimedia Commons https://commons.wikimedia.org/wiki/File:2064_aryabhata-crp.jpg και https://commons.wikimedia.org/wiki/File:Brahmagupta.jpg



Στην συνέχεια θα αποδείξουμε ότι αν $d \mid b$ τότε η εξίσωση επιδέχεται $(n-1)$-παραμετρική απειρία λύσεων. Η απόδειξη θα γίνει επαγωγικά ως προς n.

Η πρόταση ισχύει για $n = 2$ από την πρόταση 2.2.2.

Υποθέτουμε ότι η πρόταση ισχύει για κάθε γραμμική διοφαντική εξίσωση n-αγνώστων. Θεωρούμε τη γραμμική διοφαντική εξίσωση $(n+1)$-αγνώστων

$$a_1X_1 + a_2X_2 + \cdots + a_nX_n + a_{n+1}X_{n+1} = b$$

και υποθέτουμε ότι ο $d := (a_1, a_2, \ldots, a_n, a_{n+1}) \mid b$. Αν $d_1 := (a_1, a_2)$, τότε το σύνολο των γραμμικών συνδυασμών

$$\{a_1x_1 + a_2x_2 | x_1 \in \mathbb{Z}, x_2 \in \mathbb{Z}\} = \{d_1 \cdot y | y \in \mathbb{Z}\},$$

Επομένως η αρχική διοφαντική εξίσωση ανάγεται στην

$$d_1y + a_3X_3 + \cdots + a_nX_n + a_{n+1}X_{n+1} = 0.$$

Ο $(d_1, a_3, \ldots, a_n, a_{n+1}) = ((a_1, a_2), a_3, \ldots, a_n, a_{n+1}) = (a_1, a_2, \ldots, a_n, a_{n+1}) \mid b$. Επομένως, σύμφωνα με την υπόθεση της μαθηματικής επαγωγής, η τελευταία εξίσωση επιδέχεται $(n-1)$-παραμετρική απειρία λύσεων. Συνεπώς και η αρχική επιδέχεται n-παραμετρική απειρία λύσεων.

Πρακτικά, για να λύσουμε τη διοφαντική εξίσωση, εφαρμόζουμε τη διαδικασία της απόδειξης. □

Παράδειγμα. Να επιλυθεί η διοφαντική εξίσωση

$$5X_1 + 6X_2 + 3X_3 + 4X_4 = 15.$$

Υπολογίζουμε $(5,6) = 1$. Θεωρούμε τη διοφαντική εξίσωση

$$5X_1 + 6X_2 = y, \qquad y \in \mathbb{Z}.$$

Οι λύσεις αυτής είναι:

$$X_1 = -y + 6t, X_2 = y - 5t, t \in \mathbb{Z}.$$

Από την αρχική εξίσωση προκύπτει

$$Y + 3X_3 + 2X_4 = 15.$$

Θέτουμε $Y + 3X_3 =: Z$. Η επίλυση αυτής μας δίνει

$$\begin{aligned} y &= 4z + 3u \\ x_3 &= -z - u, \quad u \in \mathbb{Z}. \end{aligned}$$

Η αρχική μετασχηματίζεται στη συνέχεια στην

$$Z + 2X_4 = 15,$$

της οποίας οι λύσεις είναι

$$\begin{aligned} z &= -15 + 2\phi \\ x_4 &= 15 - \phi, \qquad \phi \in \mathbb{Z} \end{aligned}$$

Τελικά έχουμε:

$$\begin{aligned} x_1 &= 6y - 3z - 8\phi + 60 \\ x_2 &= -5y + 3z + 8\phi - 60 \\ x_3 &= 15 - z - 2\phi \\ x_4 &= 15 - \phi, \qquad\qquad y, z, \phi \in \mathbb{Z}. \end{aligned}$$

Ισοδύναμα

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 60 \\ -60 \\ 15 \\ 15 \end{pmatrix} + \begin{pmatrix} 6 \\ -5 \\ 0 \\ 0 \end{pmatrix} y + \begin{pmatrix} -3 \\ 3 \\ -1 \\ 0 \end{pmatrix} z + \begin{pmatrix} -8 \\ 8 \\ -2 \\ -1 \end{pmatrix} \phi, y, z, \phi \in \mathbb{Z}.$$

Παρατήρηση 2.2.5. 1. Πολύ πιο εύκολα θα μπορούσαμε να λύσουμε την εξίσωση ως εξής:
Από

$$2X_4 = 15 - 5X_1 - 6X_2 - 3X_3$$

έπεται ότι

$$X_4 = 7 - 2X_1 - 3X_2 - X_3 + \frac{1 - X_1 - X_3}{2}.$$

Επειδή $X_4 \in \mathbb{Z}$, έπεται ότι

$$1 - X_1 - X_3 = 2y, \qquad y \in \mathbb{Z}.$$

Επομένως,

$$\begin{aligned} X_1 &= 1 - X_3 - 2y \\ X_2 &= X_2 \\ X_3 &= X_3 \\ X_4 &= 5 + X_3 - 3X_2 + 5y, \qquad X_2, X_3, y \in \mathbb{Z} \end{aligned}$$

ή

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 5 \end{pmatrix} + \begin{pmatrix} -2 \\ 0 \\ 0 \\ 5 \end{pmatrix} y + \begin{pmatrix} 0 \\ 1 \\ 0 \\ -3 \end{pmatrix} X_2 + \begin{pmatrix} -1 \\ 0 \\ 1 \\ 1 \end{pmatrix} X_3 \qquad y, X_2, X_3 \in \mathbb{Z}.$$

2. Για την επίλυση γραμμικών διοφαντικών εξισώσεων και συστημάτων εφαρμόζονται συχνά μέθοδοι της Γραμμικής Άλγεβρας. Τον ενδιαφερόμενο αναγνώστη παραπέμπουμε στα [5, σελ. 140-141] και [5, σελ. 178-181] και [6, σελ. 214-230]

2.3 Πυθαγόρειες τριάδες

Σε όλους είναι γνωστό το Πυθαγόρειο θεώρημα. Αν x, y, z είναι μήκη των πλευρών ορθογωνίου τριγώνου τότε επαληθεύουν την εξίσωση

$$X^2 + Y^2 = Z^2 \tag{2.3.1}$$

Η διοφαντική εξίσωση (2.3.1), είναι δευτέρου βαθμού. Για προφανείς λόγους μας ενδιαφέρουν μόνο θετικές ακέραιες λύσεις.

Είναι φανερό ότι μια τέτοια λύση είναι η (3, 4, 5).

Ορισμός. Τριάδες θετικών ακέραιων (x, y, z) οι οποίες επαληθεύουν την (2.3.1) θα λέγονται *πυθαγόρειες τριάδες*.

Αν (x, y, z) πυθαγόρεια τριάδα και $d \in Z$, τότε και η (dx, dy, dz) είναι επίσης πυθαγόρεια τριάδα, αφού $(dx)^2 + (dy)^2 = (dz)^2$.

Επομένως και οι τριάδες (6, 8, 10) (9, 12, 15), . . . είναι επίσης πυθαγόρειες.

Αν γνωρίζουμε όλες τις πυθαγόρειες τριάδες (a, b, c) για τις οποίες $(a, b, c) = 1$, τότε γνωρίζουμε και *όλες* τις λύσεις της (2.3.1).

Ορισμός. Μία πυθαγόρεια τριάδα (a, b, c) θα λέγεται *πρωταρχική* ή *πρωτογενής* (primitive) όταν

$$(a, b, c) = 1$$

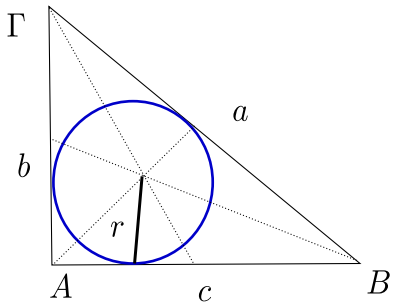
Η (3, 4, 5) λοιπόν είναι πρωταρχική. Υπάρχουν και άλλες; Η απάντηση είναι «ναι».

Οι πυθαγόρειες τριάδες (5, 12, 13), (8, 5, 17), (7, 24, 25), (9, 40, 41) είναι πρωταρχικές.

Αν (x, y, z) πρωταρχική πυθαγόρεια τριάδα, τότε ένας ακριβώς από τους x, y θα είναι άρτιος και ο άλλος περιττός.

Πράγματι, αν x και y άρτιοι, τότε και z άρτιος, οπότε $(x, y, z) \geq 2$, άτοπο.

Αν πάλι x και y περιττοί τότε $x^2 = 1 + 4l$, $l \in \mathbb{Z}$ και $y^2 = 1 + 4m$, $m \in \mathbb{Z}$, οπότε $z^2 = x^2 + y^2 = 2 + 4t, t \in \mathbb{Z}$. Αυτό όμως είναι αδύνατο, αφού το τετράγωνο ακέραιου είναι πάντοτε της μορφής $4l$ ή $4l + 1$, $l \in \mathbb{Z}$.



Σχήμα 2.3.1: Περιγεγραμμένος Κύκλος

Απάντηση στο πρόβλημα της εύρεσης όλων των πρωταρχικών πυθαγορείων τριάδων μας δίνει n ακόλουθη.

Πρόταση 2.3.1. *Οι θετικοί ακέραιοι x, y, z αποτελούν πρωταρχική πυθαγόρεια τριάδα με y άρτιο ακριβώς τότε όταν υπάρχουν θετικοί ακέραιοι r, s με $r > s$, $(r, s) = 1$ ένας εκ των οποίων είναι άρτιος και ο άλλος περιττός (ετερότυποι), τέτοιοι ώστε*

$$(x = r^2 - s^2,\ y = 2rs,\ z = r^2 + s^2)$$

Απόδειξη. Αφού y άρτιος, τα x και z θα είναι περιττοί. Επομένως $z + x$ και $z - x$ θα είναι άρτιοι. Αν ονομάζουμε $k := \frac{z+x}{2} \in \mathbb{Z}$ και $l := \frac{z-x}{2} \in \mathbb{Z}$ έχουμε

$$k \cdot l = \frac{(z+x)(z-x)}{4} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = \left(\frac{y}{2}\right)^2.$$

Ο $(k, l) = 1$, διότι αν $d := (k, l) > 1$ θα είχαμε $d|k = z + x$ και $d|l = z - x$, δηλαδή $d|(k + l) = z$ και $d|(k - l) = x$, οπότε $(x, z) \geq d > 1$, άτοπο.

Επομένως, από την πρόταση 1.7.6 προκύπτει ότι $k = r^2$, $l = s^2$ και $(r, s) = 1$, (αφού $(k, l) = 1$). Συνεπώς $x = r^2 - s^2$, $y = 2rs$ και $z = r^2 + s^2$.

Τέλος, ο ένας από τους r και s είναι άρτιος και ο άλλος περιττός. Αυτό ισχύει διότι δεν είναι δυνατό να είναι και οι δύο άρτιοι αφού $(r, s) = 1$, αλλά ούτε και οι δύο περιττοί αφού τότε οι x, y, z θα ήταν άρτιοι και η πυθαγόρεια τριάδα *δεν* θα ήταν πρωταρχική.

Αντίστροφα, υποθέτουμε ότι τα x, y, z έχουν τη σωστή μορφή και θα αποδείξουμε ότι αποτελούν πρωταρχική πυθαγόρεια τριάδα.

Πρώτα απ' όλα είναι φανερό ότι $x^2 + y^2 = z^2$, δηλαδή ότι (x, y, z) πυθαγόρεια τριάδα.

Αν $d := (x, y, z) > 1$ και $p \in \mathbb{P}$ τέτοιος ώστε $p|d$ τότε $p|x$, $p|y$ και $p|z$. Το $p \neq 2$, διότι x περιττός.

Από $p|x$ και $p|z$, έπεται ότι $p|(z + x)$ και $p|(z - x)$ δηλαδή $p|2r^2$ και $p|2s^2$, οπότε $p|(2r^2, 2s^2) = 2(r, s) = 2$, άτοπο.

Συνεπώς η τριάδα (x, y, z) είναι πρωταρχική πυθαγόρεια τριάδα. □

Ένα ορθογώνιο τρίγωνο με μήκη πλευρών *ακέραιους* θα λέγεται *πυθαγόρειο τρίγωνο*.

Ως μια πρώτη εφαρμογή της Πρότασης 2.3.1 αποδεικνύουμε ότι,

Πόρισμα 2.3.2. *Η ακτίνα r του εγγεγραμμένου κύκλου ενός πυθαγόρειου τριγώνου έχει μήκος ακέραιο αριθμό.*

Απόδειξη. Το εμβαδόν του τριγώνου $AB\Gamma$, υπολογιζόμενο με δύο διαφορετικούς τρόπους, δίνει:

$$bc = r(a+b+c)$$

Από την Πρόταση (2.3.1), έχουμε

$$c = l(r^2 - s^2),\ b = 2rsl,\ a = l(r^2+s^2),\ l, r, s \in \mathbb{Z},\ l \geq 1, r > s, (r,s) = 1, r \not\equiv s \bmod 2.$$

Επομένως και «κατάλληλα» r, s

$$\rho = \frac{bc}{a+b+c} = \frac{2l^2rs(r^2-s^2)}{2lr^2+2lrs} = \frac{ls(r-s)(r+s)}{(r+s)} = ls(r-s) \in \mathbb{Z}.$$

□

Ιστορικά 2.3.1

Κατά τον Μεσαίωνα τα μαθηματικά των αρχαίων Ελλήνων και φυσικά και η θεωρία αριθμών ξεχάστηκαν. Πάρα πολύ αργότερα τον 17ο αιώνα η Θεωρία Αριθμών ξαναγεννήθηκε. Αφορμή αποτέλεσε η έκδοση των «Αριθμητικών» του Διοφάντου στο πρωτότυπο ελληνικό κείμενο με μετάφραση στα Λατινικά και σχόλια από τον Bachet.
Ένα αντίτυπο της έκδοσης αυτής έπεσε στα χέρια του J.P. Fermat (1601-1665). Ο Fermat μελέτησε συστηματικά το έργο του Διόφαντου. Δίπλα στο περιθώριο του προβλήματος 8, Βιβλίο II των Αριθμητικών του Διοφάντου, το οποίο αναφέρεται στις Πυθαγόρειες τριάδες: «Τόν ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους.»
(Να αναλύσετε δοθέν τέλειο τετράγωνο σε (άθροισμα) δύο τέλειων τετραγώνων) ο Fermat συμπλήρωσε, στα Λατινικά, τα ακόλουθα:
" Cubum in duos cubos aut quadro-quadratum in duos quadro-quadratos et generaliter nullam in infinitum, ultra quadratum, potestam in duas ejusdem nominis fas est dividere. Cujus rei demonstrationem mirabilem sone detexi, hanc marginis exiguitas non caperet."
Μετάφραση: « Δεν είναι δυνατόν να αναλύσουμε έναν κύβο σε άθροισμα δύο κύβων, ούτε μια τέταρτη δύναμη σε (άθροισμα) δύο τετάρτων δυνάμεων και γενικά μια δύναμη μεγαλύτερη του δύο σε άθροισμα δύο δυνάμεων με τον ίδιο εκθέτη. Έχω ανακαλύψει μια καταπληκτική απόδειξη αυτού, αλλά το περιθώριο (του βιβλίου) είναι πολύ μικρό για να τη χωρέσει. »
Οι σημειώσεις του Fermat στο αντίτυπο των Αριθμητικών δημοσιεύτηκαν για πρώτη φορά από τον Samuel Fermat στα 1670. Σε γερμανική μετάφραση έχουν δημοσιευθεί στο Pierre de Fermat, *Bemerkungen zu Diophant*, μετάφραση από τα λατινικά του Max Miller, *Akademische Verlagsgesellschaft*, Leipzig 1932.

Σύμφωνα λοιπόν με τα παραπάνω, ο Fermat διατύπωσε την εικασία του

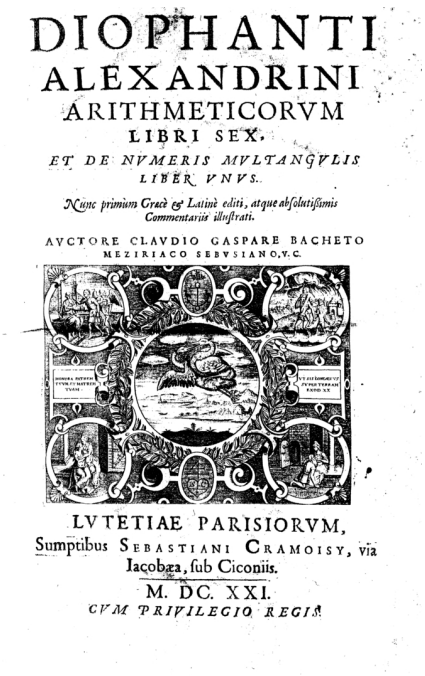
2.3.1 Εικασία του Fermat

Η διοφαντική εξίσωση

$$X^n + Y^n = Z^n,\ n \geq 3$$

δεν έχει, μη- τετριμμένη, δηλαδή για $xyz \neq 0$ ακέραια λύση.

Ισχυρίστηκε μάλιστα ότι έχει μια καταπληκτική απόδειξη η οποία όμως δεν χωράει στο περιθώριο του βιβλίου.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

Σχήμα 2.3.2: Εξώφυλλο της έκδοσης των «αριθμητικών» του 1621. Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Diophantus_-_Aritmeticorum_libri_6.,_1670_-_842640.jpeg`

Τη «χαμένη αυτή αλήθεια» έψαχναν για αιώνες οι μαθηματικοί.

Τελικά, η εικασία αποδείχθηκε πλήρως το 1995 [2], [8]. Δεν επιθυμούμε να αναφερθούμε σ' όλη την πορεία της πραγματικά γιγαντιαίας αυτής προσπάθειας απόδειξης της εικασίας. Στο τελικό στάδιο σημαντικότατη ήταν η συνεισφορά των Gerhard Frey, Jean-Pierre Serre, Kenech Ribet, Andrew Wiles και Richard Taylor.

Ο ίδιος ο Fermat απέδειξε την εικασία του για $n = 4$ ότι δηλαδή η $X^4 + Y^4 = Z^4$ δεν έχει, μη-τετριμμένη ακέραια λύση.

Επίσης απέδειξε ότι *δεν* υπάρχει τρίγωνο με μήκη πλευρών πυθαγόρεια τριάδα τέτοια ώστε το εμβαδόν του να είναι τέλειο τετράγωνο. Μία ισοδύναμη έκφραση αυτής της πρότασης, είναι ότι η διοφαντική εξίσωση

$$X^4 - Y^4 = Z^2$$

δεν έχει, μη-τετριμμένες, ακέραιες λύσεις.

Η απόδειξη της τελευταίας πρότασης γράφηκε στο περιθώριο των «Αριθμητικών» δίπλα στην άσκηση 20 του Βιβλίου *VI*.

Ο Fermat χρησιμοποιεί την Πρόταση (2.3.1) (πυθαγόρειες τριάδες) και τη συνδυάζει με μια δικής του εμπνεύσεως μέθοδο. Πρόκειται και πάλι για απαγωγή στο άτοπο. Αν υποθέσουμε ότι υπάρχει τουλάχιστον μια μη-μηδενική, λύση στο σύνολο των θετικών ακέραιων, τότε από το σύνολο των λύσεων διαλέγουμε εκείνη η οποία έχει ελάχιστη τιμή σε έναν από τους αγνώστους. Στη συνέχεια αποδεικνύουμε ότι υπάρχει και άλλη, μη-μηδενική, λύση με μικρότερη τιμή, άτοπο. Άρα η αρχική εξίσωση *δεν* έχει μη-τετριμμένη λύση.

Ο ίδιος ο Fermat «βάφτισε» τη μέθοδό του. Σε ένα γράμμα του προς τον P. De Carcavi (1659), γράφει:

«...Μίας και οι γνωστές μέθοδοι (επιλύσεως διοφαντικών εξισώσεων) της βιβλιογραφίας δεν αρκούν για την απόδειξη τόσο δύσκολων προτάσεων βρήκα έγω έναν πέρα για πέρα δικό μου δρόμο..... την αποδεικτική αυτή μέθοδο ονόμασα άπειρη κάθοδο (la descente in finie)...»

Η εικασία του Fermat υπήρξε η ατμομηχανή ανάπτυξης της Θεωρίας Αριθμών από τον 17ο αιώνα μέχρι σήμερα.

Πρόταση 2.3.3. *Η διοφαντική εξίσωση*

$$X^4 + Y^4 = Z^2$$

δεν έχει θετικές ακέραιες λύσεις.

Απόδειξη. Υποθέτουμε ότι η εξίσωση έχει τουλάχιστον μια θετική ακέραια λύση, έστω (x, y, z). Αν διαιρέσουμε τα x, y, z με τον μέγιστο κοινό τους διαιρέτη βρίσκουμε μια πρωταρχική λύση της εξίσωσης. Θα τη συμβολίζουμε και πάλι με (x, y, z).

Συνεπώς η (x^2, y^2, z) είναι μια πρωταρχική πυθαγόρεια τριάδα. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι το y^2 είναι άρτιος. Επομένως έχουμε

$$x^2 = s^2 - t^2, \quad y^2 = 2st, \quad z = s^2 + t^2,$$

με $(s, t) = 1$, $s > t$ ο ένας άρτιος και ο άλλος περιττός. Η πρώτη από τις παραπάνω ισότητες γράφεται $x^2 + t^2 = s^2$. Αυτό σημαίνει ότι η (x, t, s) είναι επίσης πυθαγόρεια τριάδα. Επειδή $(s, t) = 1$, έπεται ότι η (x, t, s) είναι πρωταρχική επειδή ο x είναι περιττός και ο t θα είναι κατ' ανάγκη άρτιος. Επομένως,

$$x = u^2 - v^2, \quad t = 2uv, \text{ και } s = u^2 + v^2,$$

όπου $(u, v) = 1$, $u > v$ ο ένας άρτιος και ο άλλος περιττός. Το y^2 τώρα γράφεται

$$y^2 = 2st = 4uv(u^2 + v^2).$$

Οι $u, v, u^2 + v^2$ είναι ανά δύο πρώτοι μεταξύ τους. Σύμφωνα λοιπόν με το πόρισμα 1.7.7 έχουμε

$$u = x_1^2, v = y_1^2 \text{ και } u^2 + v^2 = z_1^2,$$

δηλαδή

$$x_1^4 + y_1^4 = z_1^2.$$

Αυτό σημαίνει ότι (x_1, y_1, z_1) είναι επίσης μια θετική λύση της εξίσωσης $x^4 + y^4 = z^2$. Αφού η λύση (x_1, y_1, z_1) είναι θετική έπεται ότι $z_1 > 1$.

Επομένως,

$$z_1 < z_1^4 = (u^2 + v^2)^2 = s^2 < s^2 + t^2 = z.$$

Εδώ η μέθοδος έχει δυο (ισοδύναμες) παραλλαγές. Ή θα υποθέσουμε ότι η (x, y, z) είναι μια λύση με τον ελάχιστο φυσικό αριθμό z και καταλήξαμε σε άτοπο, άρα δεν υπάρχει λύση ή συνεχίζουμε και κατασκευάζουμε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών αριθμών

$$z > z_1 > z_2 > \cdots > z_n > z_{n+1} > \cdots$$

το οποίο αντιβαίνει στην αρχή του ελαχίστου. □

Πόρισμα 2.3.4. *Η «εικασία» του Fermat είναι αληθής για $n = 4$.*

Απόδειξη. Αν υπήρχε θετική λύση (x, y, z) της $x^4 + y^4 = z^4$ τότε η (x, y, z^2) θα ήταν θετική λύση της $x^4 + y^4 = z^2$, άτοπο. □

Παρατήρηση 2.3.5. Αν $4 \mid n$ και η διοφαντική εξίσωση $X^n + Y^n = Z^n$ είχε θετική λύση τότε θα είχε και η $X^4 + Y^4 = Z^4$, άτοπο.

Με την μέθοδο της καθόδου μπορούμε ακόμα να αποδείξουμε

Πρόταση 2.3.6. *Η διοφαντική εξίσωση*

$$X^4 - Y^4 = Z^2$$

δεν έχει θετική ακέραια λύση.

Απόδειξη. Υποθέτουμε ότι έχει θετικές λύσεις. Επιλέγουμε μία (x, y, z) με το μικρότερο x. Δεν χάνουμε τίποτα αν υποθέσουμε ότι $(x, y) = 1$. Επομένως η (x^2, z, y^2) είναι μια πρωταρχική πυθαγόρεια τριάδα. Ξεχωρίζουμε δύο περιπτώσεις: Αν ο y είναι περιττός τότε

$$y^2 = s^2 - t^2, \quad z = 2st, \quad x^2 = s^2 + t^2,$$

με s, t πρώτοι μεταξύ τους, ο ένας άρτιος ο άλλος περιττός. Επομένως,

$$s^4 - t^4 = (xy)^2,$$

δηλαδή η τριάδα (s, t, xy) αποτελεί λύση της εξίσωσης με $s < x$, άτοπο.

Αν ο y είναι άρτιος τοτε

$$y^2 = 2st, \quad z = s^2 - t^2, x^2 = s^2 + t^2,$$

με s, t πρώτοι μεταξύ τους, ο ένας άρτιος και ο άλλος περιττός. Αν ο t είναι περιττός, τότε $(2s, t) = 1$. Επομένως $2s = (2u)^2$ και $t = v^2$ αφού $y = 2st$. Συνεπώς,

$$x^2 = 4u^4 + v^4,$$

από την οποία σχέση συμπεραίνουμε ότι η τριάδα $(2u^2, v^2, x)$ είναι μια πρωταρχική πυθαγόρεια τριάδα.

Άρα $2u^2 = 2ml$, $v^2 = m^2 - l^2$, $x = m^2 + l^2$, όπου m, l πρώτοι μεταξύ τους, ο ένας άρτιος και ο άλλος περιττός. Η σχέση $u^2 = ml$ συνεπάγεται ότι $m = a^2$, $l = b^2$, δηλαδή $a^4 - b^4 = v^2$ λύση της εξίσωσης με $a < x$, άτοπο.

Αν τώρα ο t είναι άρτιος, τότε ο $(s, 2t) = 1$, επομένως $s = u^2$, $2t = (2v)^2$ και όπως παραπάνω $x^2 = u^4 + 4v^4$, δηλαδή ο $(u^2, 2v^2, x)$ πρωταρχική πυθαγόρεια τριάδα. Επομένως,

$$u^2 = m^2 - l^2, \quad 2v^2 = 2ml \text{ και } x = m^2 + l^2,$$

με m, l πρώτους μεταξύ τους ο ένας άρτιος ο άλλος περιττός. Επειδή $v^2 = ml$ και $(m, l) = 1$ έπεται ότι $m = a^2, l = b^2$ και συνεπώς $a^4 - b^4 = u^2$, δηλαδή και πάλι έχουμε λύση της εξίσωσης (a, b, u) με $a < x$, άτοπο. □

Πόρισμα 2.3.7. *Δεν υπάρχει πυθαγόρειο τρίγωνο με εμβαδό τέλειο τετράγωνο.*

Απόδειξη. Πράγματι, αν υποθέσουμε ότι υπάρχουν θετικοί ακέραιοι x, y, z για τους οποίους να ισχύει:

$$x^2 + y^2 = z^2 \text{ και } xy = 2m^2, \quad m \in \mathbb{Z}, m \geq 1$$

τότε $(x+y)^2 = z^2 + 4m^2$ και $(x-y)^2 = z^2 - 4m^2$. Επομένως, $z^4 - (2m)^4 = ((x+y)(x-y))^2$, δηλαδή η εξίσωση

$$X^4 - Y^4 = Z^2,$$

έχει θετική ακέραια λύση άτοπο λόγω της αλήθειας της πρότασης 2.3.6. □

Η εικασία του Fermat για $n = 3$ αποδείχθηκε από τον Euler. Η απόδειξη του δημοσιεύτηκε στα 1770.

Ο Euler διατύπωσε την εικασία ότι ούτε η εξίσωση

$$X^4 + Y^4 + Z^4 = W^4$$

έχει, μη-τετριμμένη ακέραια λύση.

Μάλιστα τη γενίκευσε στην

Εικασία του Euler . Για κάθε ακέραιο n, $n > 0$ το άθροισμα $(n-1)$ n-στων δυνάμεων *δεν* είναι n-στη δύναμη ακέραιου.

Ο ίδιος ο Euler γράφει: «...Σε πολλούς Γεωμέτρες θεωρήθηκε ότι το θεώρημα αυτό (το τελευταίο θεώρημα του Fermat) θα μπορούσε ίσως να γενικευτεί. Όπως ακριβώς δεν υπάρχουν δύο κύβοι των οποίων το άθροισμα ή η διαφορά να είναι ένας κύβος, είναι αδύνατον να εκφραστεί το άθροισμα τριών διτετράγωνων αριθμών ως ένας διτετράγωνος αριθμός. Αλλά ότι τουλάχιστον τέσσερις διτετράγωνοι απαιτούνται για να είναι δυνατόν να είναι το άθροισμα τους διτετράγωνος αριθμός, παρά το ότι μέχρι σήμερα κανείς δεν έδωσε ένα ανάλογο παράδειγμα. Ανάλογα φαίνεται ότι είναι αδύνατον να εκφραστεί το άθροισμα τεσσάρων πέμπτων δυνάμεων ακέραιων ως μια πέμπτη δύναμη και το αντίστοιχο για μεγαλύτερες δυνάμεις.»

Από την εποχή του Euler δεν σημειώθηκε καμμία πρόοδος σχετικά με την εικασία μέχρι το 1911 όταν ο R. Norrie απέδειξε ότι

$$30^4 + 120^4 + 272^4 + 315^4 = 353^4.$$

Στα 1966 οι Lander και Parkin απέδειξαν ότι η Εικασία του Euler *δεν* ισχύει για $n = 5$. Μια, μη-τετριμμένη λύση είναι η (27, 84, 110, 133, 144).

Το 1986 ο Elkies [7] απέδειξε ότι ούτε για $n = 4$ ισχύει. Απέδειξε μάλιστα ότι έχει *άπειρες* λύσεις. Όμως, μέχρι σήμερα μόνο 7 λύσεις είναι γνωστές.

Η λύση που βρήκε ο N. Elkies ήταν

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

Την ίδια χρονιά ο Roger Frye υπολόγισε την πιο μικρή λύση:

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

Η εικασία του Euler δεν ισχύει για $n = 4$ αποδείχτηκε και από τον Don Zagier. Σε πρόσφατο άρθρο του [1] εξηγεί με χιουμοριστικό τρόπο γιατί δεν υποβλήθηκε για δημοσίευση το 1986 και γιατί αποφάσισε να την δημοσιεύσει το 2013.

Για $n \geq 6$ η εικασία είναι μέχρι σήμερα ανοιχτή.

2.3.2 Εικασία του Catalan

Στα 1844 ο Βέλγος μαθηματικός Eugène Catalan διατύπωσε την εικασία, ότι οι μόνοι διαδοχικοί ακέραιοι οι οποίοι είναι τέλειες δυνάμεις είναι το 8 και το 9. Με άλλα λόγια ότι η διοφαντική εξίσωση

$$X^m - Y^n = 1 \qquad (m > 1, n > 1)$$

έχει μοναδική μη τετριμμένη λύση $x^m = 3^2, y^n = 2^3$. Η εικασία αποδείχθηκε πρόσφατα το 2003 σε μια σειρά εργασιών του P. Mihailescu. Για μια παρουσίαση της απόδειξης δες και την πτυχιακή εργασία της Ε. Συρράκου «Η απόδειξη της εικασίας του Catalan» Μεταπτυχιακή εργασία, Ηράκλειο 2007.

Παρατηρήσεις

1. Ας ονομάσουμε το εμβαδόν ενός (πρωταρχικού) πυθαγόρειου τριγώνου, *πυθαγόρειο αριθμό*.

   Αν, δύο πυθαγόρειες τριάδες έχουν τον ίδιο πυθαγόρειο αριθμό και ίσες υποτείνουσες, τότε οι τριάδες συμπίπτουν.

   Πράγματι, έστω (x_1, y_1, z_1) και (x_2, y_2, z_2) δύο πυθαγόρειες τριάδες με $z_1 = z_2$ και $x_1 y_1 = x_2 y_2$, τότε n σχέσεις $x_1^2 + y_1^2 = z_1^2$ και $x_2^2 + y_2^2 = z_2^2$ μας δίνουν $(x_1 - y_1)^2 = (x_2 - y_2)^2$ και $(x_1 + y_1)^2 = (x_2 + y_2)^2$.

   Συνεπώς, αν υποθέσουμε ότι $x_1 \geq y_1$ και $x_2 \geq y_2$ (χωρίς περιορισμό της γενικότητας), έχουμε $x_1 = x_2$ και $y_1 = y_2$.

   Όμως υπάρχουν (πρωταρχικές) πυθαγόρειες τριάδες, με διαφορετικές υποτείνουσες που έχουν το ίδιο εμβαδό.

   π.χ. (21, 20, 29) και (35, 12, 37).

   Ο Fermat μάλιστα απέδειξε ότι για κάθε φυσικό αριθμό n, $n > 1$ υπάρχουν n *πυθαγόρειες τριάδες* (όχι κατ' ανάγκη πρωταρχικές) οι οποίες έχουν διαφορετικές διακρίνουσες και τον ίδιο πυθαγόρειο αριθμό [9, σελ. 49 Θεωρ. 2].

2. Είναι εύκολο να υπολογίσουμε όλες τις πυθαγόρειες τριάδες των οποίων ο πυθαγόρειος αριθμός είναι ίσος με την περίμετρό του.

   Πράγματι, από το σύστημα των δύο σχέσεων

   $$x^2 + y^2 = z^2 \qquad x + y + z = \frac{1}{2}xy$$

   προκύπτει $(x - 4)(y - 4) = 8$, άρα $(x - 4)|8$. Αποκλείουμε την περίπτωση $x - 4 < 0$, οπότε έχουμε $x - 4 = 1, 2, 4, 8$, δηλαδή

   $$x = 5, 6, 8 \text{ ή } 12.$$

   Για τις τιμές αυτές υπολογίζουμε το αντίστοιχο $y = 12, 8, 6$ ή 5. Επομένως οι τιμές αυτές δίνουν τις πυθαγόρειες τριάδες

   $$(5, 12, 13) \text{ και } (6, 8, 10)$$

3. Η πυθαγόρεια τριάδα

   $$(9999, 137532, 137895)$$

   είναι ασυνήθιστη, διότι ο πυθαγόρειος αριθμός είναι

   $$687591234$$

   και περιέχει όλα τα ψηφία, πλην του μηδενός.

2.3.3 Μια διαφορετική προσέγγιση του θέματος των πυθαγόρειων τριάδων.

Αν (x, y, z) Πυθαγόρεια τριάδα, έχουμε

$$x^2 + y^2 = z^2$$

Αν τώρα, υποθέσουμε ότι $z \neq 0$ και διαιρέσουμε και τα δύο μέλη με z, έχουμε

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

Αυτό σημαίνει ότι οι *ρητοί* αριθμοί $u = \frac{x}{z}$ και $v = \frac{y}{z}$ είναι λύση της διοφαντικής εξίσωσης

$$U^2 + V^2 = 1 \tag{2.3.2}$$

Αν πάλι $(u, v) \in \mathbb{Q}^2$, λύση της (2.3.2) και γράψουμε τα κλάσματα ομώνυμα $u = \frac{x}{z}$, $v = \frac{y}{z}$, $z \neq 0$, τότε έχουμε

$$x^2 + y^2 = z^2$$

δηλαδή μια πυθαγόρεια τριάδα

$$(x, y, z) \text{ με } z \neq 0$$

Θα λύσουμε τώρα την εξίσωση (2.3.2) στο σώμα των ρητών αριθμών.

Η μέθοδος είναι περισσότερο γεωμετρική και η ιδέα της ανάγεται στον Διόφαντο.

Ο Διόφαντος εφαρμόζει τη μέθοδο αυτή για να λύσει τα προβλήματα 8 και 9 του Βιβλίου ΙΙ των «Αριθμητικών» του.

Τα προβλήματα αυτά είναι: *«Του ἐπιταχθέντα τετραγώνου διελεῖν εἰς δύο τετραγώνους»*

και

«Του δοθέντα ἀριθμόν ὅς σύγκειται ἐκ δύο τετραγώνων μεταδιελεῖν δύο ἑτέρους τετραγώνους». [3], [10]

Παρατηρούμε κατ' αρχήν ότι η εξίσωση (2.3.2) είναι η εξίσωση του μοναδιαίου κύκλου. Ένα ρητό σημείο της είναι αυτό με συντεταγμένες $(0, -1)$.

Αν (u, v) τυχαίο σημείο του κύκλου, $(u, v) \neq (-1, 0)$. Η ευθεία η οποία περνάει από τα δύο σημεία $(-1, 0)$ και (u, v) έχει κλίση t και εξίσωση $V = t(U + 1)$.

Το σημείο (u, v) είναι λύση του συστήματος

$$\begin{aligned} U^2 + V^2 &= 1 \\ V &= t(U + 1) \end{aligned} \tag{2.3.3}$$

Με απαλοιφή του V στο σύστημα (2.3.3) προκύπτει η εξίσωση

$$(1 + t^2)U^2 + 2t^2U + (t^2 - 1) = 0.$$

Η εξίσωση αυτή έχει ρίζες $u = \frac{1-t^2}{1+t^2}$ και $u = -1$

Η δεύτερη λύση αντιστοιχεί στο σημείο $(-1, 0)$. Για $u = \frac{1-t^2}{1+t^2}$ η αντίστοιχη τιμή για το v είναι, $v = \frac{2t}{1+t^2}$.

Παρατηρούμε ότι αν η κλίση $t \in \mathbb{Q}$ τότε $(u, v) \in \mathbb{Q}^2$ και αντιστρόφως, η ευθεία που συνδέει δύο *ρητά* σημεία έχει *ρητή κλίση*.

Επομένως, έχουμε αποδείξει ότι ισχύει η ακόλουθη:

Πρόταση 2.3.8. *Όλες οι ρητές λύσεις της εξίσωσης* $U^2 + V^2 = 1$, *εκτός του σημείου* $(-1, 0)$, *δίνονται από τον τύπο*

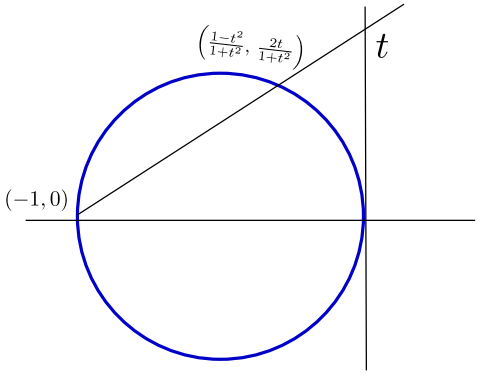
$$(U, V) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right),$$

όπου το t *διατρέχει όλους τους ρητούς. (Το σημείο* $(-1, 0)$ *προκύπτει από τον παραπάνω τύπο για* $t \to \infty$*).*

Αν θέσουμε $t = \frac{r}{s}$, *με* $r, s \in \mathbb{Z}$, $s \neq 0$, *τότε η λύση* (u, v) *γράφεται στη μορφή*

$$(u, v) = \left(\frac{s^2 - r^2}{s^2 + r^2}, \frac{2rs}{s^2 + r^2}\right)$$

και αντιστοιχεί στην (όχι κατ' ανάγκη πρωταρχική) πυθαγόρεια τριάδα $(x, y, z) = (s^2 - r^2, 2rs, s^2 + r^2)$ *με* $z = s^2 + r^2 \neq 0$.



Σχήμα 2.3.3: Γεωμετρική Προσέγγιση Πυθαγόρειων Τριάδων

Στο πρόγραμμα sage μπορούμε να υπολογίσουμε πυθαγόριες τριάδες με ωμή βία ως εξής:

```
SquaresL=[i^2 for i in range(1,50)]
CP=CartesianProduct(range(1,50),range(1,50))
PT=[ [a[0],a[1],sqrt(a[0]^2+a[1]^2)] for a in CP if \
 a[0]^2+a[1]^2 in SL]
PT
[3,4,5], [4,3,5], [5,12,13], [6,8,10], [7,24,25], [8,6,10],\
[8,15,17], [9,12, 15], [9,40,41], [10,24,26], [12,5,13], \
[12,9,15], [12,16, 20], [12,35,37], [15,8,17], [15,20,25], \
[15,36,39], [16,12, 20], [16,30,34], [18,24,30], [20,15,25], \
[20,21,29], [21,20, 29], [21,28,35], [24,7,25], [24,10,26], \
[24,18,30], [24,32, 40], [27,36,45], [28,21,35], [30,16,34], \
[32,24,40], [35,12, 37], [36,15,39], [36,27,45], [40,9,41]]
```

2.3.4 Ασκήσεις

1. Κάποιος είχε στο πορτοφόλι του χαρτονομίσματα των 20, 50, 100 ευρώ σε σύνολο χαρονομισμάτων 15. Το συνολικό ποσό ήταν 690 ευρώ. Πόσα χαρτονομίσματα είχε από κάθε είδος;

2. Μια ομάδα 41 ανθρώπων, αντρών, γυναίκών και παιδιών δειπνουν σε κάποια ταβέρνα. Ο λογαριασμός είναι 400 ευρώ. Κάθε άντρας πληρώνει 40 ευρώ κάθε γυναίκα 30 ευρώ και κάθε τριάδα παιδιών πληρώνει 10 ευρώ. Πόσοι άνδρες, γυναίκες και παιδιά πήραν μέρος στο δείπνο; (Bachet)

3. Να λύσετε το διοφαντικό σύστημα

$$x + y + z = 30, \quad \frac{x}{3} + \frac{y}{2} + 2z = 30$$

(Fibonacci, 1228.)

4. Ένας έμπορος αγόρασε τρία είδη εμπορευμάτων και πλήρωσε 4000 ευρώ για συνολικά 100 κομμάτια. Κάθε κομμάτι από το πρώτο είδος κοστίζει 120 ευρώ, από το δεύτερο 50 ευρώ και απο το τρίτο 25 ευρώ. Αν ο έμπορος αγόρασε τουλάχιστον ένα κομμάτι από κάθε είδος τότε πόσα κομμάτια από κάθε είδος είχε αγοράσει;

5. Ένας ταχυδρομικός υπάλληλος έχει γραμματόσημα μόνο των 42 λεπτών και των 63 λεπτών. Ποιους συνδιασμούς πρέπει να κάνει για να πουλήσει ένα πακέτο ποσού ακριβώς

   (α′) $10,50$ ευρώ·

   (β′) $12,00$ ευρώ·

   (γ′) $23,31$ ευρώ·

6. Αν το άθροισμα δύο διαδοχικών ακέραιων είναι τέλειο τετράγωνο να αποδείξετε ότι ο μικρότερος είναι κάθετος πλευρά και ο μεγαλύτερος υποτείνουσα ορθογωνίου τριγώνου.

7. Να αποδείξετε ότι η πυθαγόρεια τριάδα $(3, 4, 5)$ είναι η μοναδική πρωτογενής πυθαγόρεια τριάδα στην οποία οι πλευρές του ορθογωνίου τριγώνου είναι διαδοχικοί ακέραιοι.

8. Αν (x, y, z) είναι πρωτογενής πυθαγόρεια τριάδα, τότε τουλάχιστον ένα από τα x, y, z διαιρείται με 5.

9. Να βρεθούν όλα τα πυθαγόρεια τρίγωνα των οποίων το εμβαδό είναι ίσο με την περίμετρό τους.

10. Να λύσετε τη διοφαντική εξίσωση

$$x^2 + 2y^2 = z^2.$$

Βιβλιογραφία

[1] A. Malter, D. Schleicher D. Zagier: *New looks and old number theory*. Am. Math. Monthly, 120:243–264, 2013.

[2] A. Wiles: *Modular Elliptic Curves and Fermat's Last Theorem*. Annals of Mathematics, 141:443–551, 1995.

[3] Isabella Grigoryevna Bashmakova: *Diophantus and Diophantine Equations, A, Shenitzer (translator)*. The Mathematical Association of America, 1997.

[4] James J. Tattersall: *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, second edition, 2005.

[5] Kenneth H. Rosen: *Elementary Number Theory*. 2011.

[6] M. Niven and H.S. Zuckerman and H.L. Montgomery: *An introduction to the theory of numbers*. J. Wiley, 1991.

[7] Noam Elkies: *On* $a^4 + B^4 + C^4 = D^4$. Mathematics of Computation, 51:825–835, 1988.

[8] R. Taylor, A. Wiles: *Ring-theoretic properties of certain Hecke algebras*. Annals of Mathematics, 141:553–572, 1995.

[9] W.Sierpinski: *Elementary Theory of Numbers*. P.W.N. Warsawa, 1964.

[10] Σταμάτη, Ευάγγελου: *Διοφάντου Αριθμητικά*. 1953.

3

Επώνυμοι ακέραιοι, κρυπτογραφία και κωδικοποίηση

Στο κεφάλαιο αυτό θα μελετήσουμε μερικές κλάσεις ακέραιων με ιδιαίτερες ιδιότητες. Μερικές από αυτές έχουν ενδιαφέρον για λόγους ιστορικούς, κάποιες μάλιστα θεωρούνται κληρονομιά της αριθμολογίας, και άλλες παρουσιάζουν ιδιαίτερο επιστημονικό ενδιαφέρον.

Τέλος, θα αναφερθούμε στο πρόβλημα της παραγοντοποίησης, τη σημασία του στην Κρυπτογραφία και θα αναπτύξουμε μερικές σχετικές μεθόδους.

3.1 Φίλοι αριθμοί

Για κάθε θετικό ακέραιο n, ορίζουμε μια συνάρτηση $\sigma(n)$, το άθροισμα των θετικών διαιρετών του n.

Έτσι, $\sigma(1) = 1$, $\sigma(2) = 1+2 = 3$, $\sigma(3) = 1+3 = 4$, $\sigma(4) = 1+2+4 = 7$. Για κάθε $n \geq 2$, ισχύει $\sigma(n) \geq n+1$. Αν $n = \prod_{p|n} p^{\vartheta_p(n)}$ η (μονοσήμαντη) ανάλυση του n σε γινόμενο πρώτων παραγόντων, τότε κάθε θετικός διαιρέτης $d|n$ θα έχει τη μορφή

$$d = \prod_{p|n} p^{a_p}, \text{ όπου } 0 \leq a_p \leq \vartheta_p(n)$$

για κάθε $p \in \mathbb{P}$, $p|n$.

Επομένως,

$$\sigma(n) = \sum_{d|n} d = \prod_{p|n} \sum_{a_p=0}^{\vartheta_p(n)} p^{a_p}$$

Το εσωτερικό άθροισμα, είναι άθροισμα όρων γεωμετρικής προόδου και συνεπώς

$$\sum_{a_p=0}^{\vartheta_p(n)} p^{a_p} = \frac{p^{\vartheta_p(n)+1} - 1}{p-1}.$$

Άρα

$$\sigma(n) = \prod_{p|n} \frac{p^{\vartheta_p(n)+1} - 1}{p-1}$$

Παράδειγμα. Αν $n = 120 = 2^3 \cdot 3 \cdot 5$ οι διαιρέτες του είναι $d = 2^a \cdot 3^b \cdot 5^c$ $0 \leq a \leq 3$, $0 \leq b, c \leq 1$ και $\sigma(n) = \frac{2^4-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 15 \cdot 4 \cdot 6 = 360$.

Πρόταση 3.1.1. *Αν n, m θετικοί ακέραιοι και $(m, n) = 1$, τότε $\sigma(nm) = \sigma(n)\sigma(m)$.*

Απόδειξη.

$$\sigma(nm) = \prod_{p|nm} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1} = \prod_{p|n} \frac{p^{\vartheta_p(n)+1} - 1}{p-1} \prod_{p|m} \frac{p^{\vartheta_p(m)+1} - 1}{p-1} = \sigma(n)\sigma(m).$$

□

Ορισμός. Δύο θετικοί ακέραιοι m, n θα λέγονται *φίλοι* όταν

$$\sigma(m) - m = n$$

και

$$\sigma(n) - n = m,$$

δηλαδή όταν $\sigma(m) = m + n = \sigma(n)$.

Το μικρότερο ζευγάρι γνωστών φίλων αριθμών αναφέρεται στο έργο του Ιάμβλιχου «Περί τῆς Νικομάχου Ἀριθμητικῆς Εἰσαγωγῆς» και είναι το $(220, 284)$. Αποδίδεται μάλιστα στον Πυθαγόρα και στους μαθητές του. Ονομάστηκαν έτσι, επειδή έχουν τη «δύναμη» ο ένας να «παράγει» τον άλλο και αντιστρόφως, κάτι που συμβολίζει την «αμοιβαία αρμονία» την «τέλεια φιλία». Όταν κάποτε ο Πυθαγόρας ρωτήθηκε

«Τί ἐστί φίλος;», απάντησε «Ἕτερος ἐγώ». %ερασε

Σχήμα 3.1.1: Ιάμβλιχος, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Iamblichus.jpg`

Μερικά άλλα ζευγάρια φίλων είναι: $(1184, 1210)$, $(2620, 2924)$, $(5020, 5564)$, $(6232, 6368)$, $(10744, 10856)$, $(12285, 14595)$, $(17296, 18416)$.

Το 1636 ο Fermat και το 1638 ο Descartes βρήκαν το $(9363584, 9437056)$. Τα δύο τελευταία αποτελέσματα ήταν ήδη γνωστά στους Άραβες. Ο Euler ανακάλυψε το 1747, 30 νέα ζευγάρια φίλων αριθμών και στη συνέχεια επεξέτεινε τα αποτελέσματά του σε 64 ζευγάρια (δύο από τα

Σχήμα 3.1.2: Thabit ibn Qurra Το παρόν έργο αποτελεί κοινό κτήμα (public domain), λόγω παρέλευσης 70 ετών από τον Θάνατο του δημιουργού.

οποία ήταν λάθος). Αξιοσημείωτο είναι ότι το ζευγάρι (1184, 1210) διέλαθε της προσοχής όλων, ακόμη και του Euler και πρωτοανακαλύφθηκε από τον 16χρονο Nicolo Papagini στα 1866.

Το 1946 ήταν γνωστά μόνο 390 ζευγάρια, ενώ σήμερα (αποτελέσματα του 2007) - με χρήση υπολογιστή - είναι γνωστά περίπου $12 \cdot 10^6$ ζευγάρια.

Το ερώτημα αν υπάρχει κάποιος κανόνας υπολογισμού ζευγαριών φίλων αριθμών, απαντήθηκε θετικά κατά τον 9ο μ.Χ. αιώνα από τον Άραβα μαθηματικό Thabit ibn Kuwah (ή, κατ' άλλους Qurra)

Πρόταση 3.1.2. *Αν $n > 1$ και οι αριθμοί $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ και $r = 9 \cdot 2^{2n-1} - 1$ είναι πρώτοι τότε οι $2^n \cdot p \cdot q$ και $2^n \cdot r$ είναι φίλοι.*
Παράδειγμα. Για $n = 2$, $p = 5$, $q = 11$, $r = 71$ έχουμε $2^2 \cdot 5 \cdot 11 = 220$ και $2^2 \cdot 71 = 284$. Δυστυχώς δεν προκύπτουν όλα τα ζευγάρια φίλων κατ' αυτό του τρόπο, π.χ. το ζευγάρι (6232, 6368). Αργότερα, το αποτέλεσμα αυτό γενικεύθηκε από τον Euler.

Παρατήρηση

1. Δεν υπάρχει γνωστό ζευγάρι φίλων στο οποίο ένας τουλάχιστον να είναι τέλειο τετράγωνο.

2. Υπάρχουν ζευγάρια φίλων οι οποίοι να έχουν ίσα αθροίσματα ψηφίων, π.χ. (69615, 87633). Στα πρώτα 5000 427 είναι τέτοια.

   Υπάρχουν ζευγάρια φίλων στα οποία κάθε φίλος διαιρείται με το άθροισμα των ψηφίων του, π.χ. (2620, 2924).

3. Σ' όλα τα γνωστά ζευγάρια φίλων μέχρι τη δεκαετία του '60 οι περιττοί φίλοι αριθμοί διαιρούνταν με 3. Έτσι οι Bratley και Mc Kay (1968) διατύπωσαν την εικασία ότι αυτό ισχύει για *όλα* τα ζευγάρια περιττών φίλων. Η εικασία αυτή αποδείχθηκε λανθασμένη 20 χρόνια αργότερα από τους Battiato και Borho (1988).

   Το αντιπαράδειγμα με τους πιο μικρούς φίλους είναι:

   $$(42262694537514864075544955198125, 42405817271188606697466971841875)$$

οι οποίοι είναι αριθμοί με 32 ψηφία.

3.2 Τέλειοι αριθμοί

Είναι φανερό ότι $\sigma(n) \geq 1 + n$, για κάθε θετικό ακέραιο n, $n > 1$.

Η ισότητα ισχύει, όταν $n \in \mathbb{P}$. Μάλιστα ισχύει και το αντίστροφο. Αν $\sigma(n) = 1 + n$, τότε κατ' ανάγκη ο $n \in \mathbb{P}$.

Ορισμός. Ο θετικός ακέραιος n, $n > 1$ λέγεται

1. *Υπερτέλειος αριθμός* (abundant) όταν $\sigma(n) > 2n$
2. *τέλειος αριθμός* (perfect) όταν $\sigma(n) = 2n$
3. *ελλιπής αριθμός* (deficient) όταν $\sigma(n) < 2n$

Η ταξινόμηση αυτή ανάγεται στους Πυθαγόρειους.

Είναι φανερό ότι, για κάθε πρώτο p, $\sigma(p) = 1 + p < 2p$, άρα υπάρχουν άπειροι ελλιπείς ακέραιοι.

Επίσης αν $n = 2^k \cdot 3$, $k > 1$ τότε

$$\sigma(n) = \sigma(2^k)\sigma(3) = (2^{k+1} - 1) \cdot 4 = 2^{k+1} \cdot 4 - 4 = 2^{k+1} \cdot 3 + 2^{k+1} - 4 > 2^{k+1} \cdot 3 = 2n$$

Συνεπώς υπάρχουν και άπειροι υπερτέλειοι ακέραιοι.

Οι 4 πρώτοι (μικρότεροι) τέλειοι αριθμοί είναι:

- $6 = 1 + 2 + 3$
- $28 = 1 + 2 + 4 + 7 + 14$
- $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$ και
- $8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$

Και οι 4 ήταν γνωστοί στον Νικόμαχο τον Γερασηνό και αναφέρονται στο έργο «Ἀριθμητική Εἰσαγωγή».

Πρόταση 3.2.1. *(Ευκλείδη). Αν ο $2^n - 1$ είναι πρώτος αριθμός, $n \geq 2$, τότε ο $2^{n-1}(2^n - 1)$ είναι τέλειος.*

Απόδειξη. Αφού $2^n - 1$ πρώτος, έπεται ότι $\sigma(2^n - 1) = 1 + (2^n - 1) = 2^n$. Έστω $m := 2^{n-1}(2^n - 1)$. Επίσης $(2^{n-1}, 2^n - 1) = 1$, επομένως $\sigma(m) = \sigma(2^{n-1}(2^n - 1)) = \sigma(2^{n-1})\sigma(2^n - 1) = 2^n \sum_{k=0}^{n-1} 2^k =$ $2^n(2^n - 1) = 2m$. Συνεπώς ο m είναι τέλειος. □

Παρατήρηση Η παραπάνω πρόταση εμπεριέχεται στα «Στοιχεία» του Ευκλείδη. (Βιβλίο IX, πρόταση 36)

«Ἐάν ἀπό μονάδος ὁποσοῖον ἀριθμοί ἐξῆς ἐκτεθῶσιν ἐν τῇ διπλασίονι ἀναλογία, ἕως οὗ ὁ σύμπας συντεθείς πρῶτος γένηται, καί ὁ σύμπας ἐπί τον ἔσχατον πολλαπλασιασθείς ποιῇ τινα, ὁ γενόμενος τέλειος ἔσται.»

(Αν $1 + 2 + 2^2 + \cdots + 2^{n-1}$ είναι πρώτος αριθμός τότε ο $2^{n-1}(1 + 2 + \cdots + 2^{n-1})$ είναι τέλειος.)

Παράδειγμα.

Σχήμα 3.2.1: Νικόμαχος ο Γερασηνός, Το παρόν έργο αποτελεί κοινό κτήμα (public domain) λόγω παρέλευσης 70 ετών από τον θάνατο του δημιουργού.

1. $1 + 2 = 3 \in \mathbb{P}$. Επομένως, ο $2 \cdot 3 = 6$ είναι τέλειος.
2. $1 + 2 + 4 = 7 \in \mathbb{P}$. Συνεπώς ο $4 \cdot 7 = 28$ είναι τέλειος
3. $1 + 2 + 4 + 8 + 16 = 31 \in \mathbb{P}$, άρα ο $16 \cdot 31 = 496$ είναι τέλειος.
4. $1 + 2 + 4 + 8 + 16 + 32 = 127 \in \mathbb{P}$, οπότε ο $64 \cdot 127 = 8128$ είναι τέλειος.

Έχοντας ως βάση τη γνώση αυτών των τεσσάρων τέλειων αριθμών ο Νικόμαχος ο Γερασηνός, διατύπωσε πέντε εικασίες. Στο έργο του Νικομάχου αναφέρονται ως «αποτελέσματα» χωρίς την παραμικρή αναφορά σε αποδείξεις.

1. Ο n-οστός τέλειος έχει n ψηφία.
2. Όλοι οι τέλειοι είναι άρτιοι.
3. Οι τέλειοι αριθμοί έχουν ψηφίο μονάδων 6 ή 8 και μάλιστα εναλλάξ.
4. Η πρόταση του Ευκλείδη (πρόταση 3.2.1) μας δίνει όλους τους τέλειους αριθμούς.
5. Υπάρχουν άπειροι τέλειοι αριθμοί.

Στη συνέχεια θα εξετάσουμε τι είναι μέχρι σήμερα γνωστό σχετικά με τις *εικασίες* του Νικομάχου.

Στα 1747 ο Euler απέδειξε ότι ισχύει και το αντίστροφο της πρότασης του Ευκλείδη με τον περιορισμό όμως στους *άρτιους* αριθμούς. Συγκεκριμένα

Πρόταση 3.2.2 (Euler)**.** *Αν ο άρτιος φυσικός αριθμός m είναι τέλειος, τότε έχει κατ' ανάγκη τη μορφή $m = 2^{n-1}(2^n - 1)$, για κάποιο φυσικό αριθμό $n \geq 2$.*

Απόδειξη. Αφού ο m είναι άρτιος, γράφεται στη μορφή $m = 2^{n-1} \cdot l$ όπου $n > 1$ και l περιττός.

Συνεπώς $(2^{n-1}, l) = 1$ οπότε η πρόταση 3.1.1 μας δίνει

$\sigma(m) = \sigma(2^{n-1} \cdot l) = \sigma(2^{n-1})\sigma(l) = (2^n - 1)\sigma(l)$.

Ο m όμως είναι και τέλειος, συνεπώς

$$\sigma(m) = 2m = 2^n \cdot l$$

Επομένως $2^n l = (2^n - 1)\sigma(l)$, δηλαδή $(2^n - 1)|2^n l$ και, επειδή $(2^n - 1,\ 2^n) = 1$, έχουμε $(2^n - 1)|l$, $l = (2^n - 1)t$, για κάποιο $t \in \mathbb{Z}$.

Αντικαθιστούμε το l στην προηγούμενη σχέση και απλοποιώντας, με το $2^n - 1$ βρίσκουμε

$$2^n \cdot t = \sigma(l).$$

Αλλά το l και το t είναι διαιρέτες του l ($t < l$). Επομένως $l + t \leq \sigma(l) = 2^n \cdot t$. Επίσης $l + t = (2^n - 1)t + t = 2^n \cdot t$ άρα $\sigma(l) = l + t$. Αυτό μας δείχνει ότι ο l έχει ακριβώς δύο διαιρέτες τους l και t. Άρα θα πρέπει ο l να είναι πρώτος, ($l \in \mathbb{P}$) και ο $t = 1$. Καταλήξαμε στο συμπέρασμα ότι $l = (2^n - 1) \in \mathbb{P}$, δηλαδή ότι $m = 2^{n-1}(2^n - 1)$. □

Παρατήρηση Άμεση συνέπεια της πρότασης 3.2.2 είναι ότι η εικασία (4) είναι σωστή αν δεχθούμε την ορθότητα της εικασίας (2).

Από την πρόταση 3.2.2 προκύπτει ότι είναι ενδιαφέρον το ερώτημα πότε ένας φυσικός αριθμός της μορφής $2^n - 1$ είναι πρώτος;

Προτού ασχοληθούμε όμως με το ερώτημα αυτό θα εξετάσουμε πότε ένας ακέραιος της μορφής

$$a^n - 1,\ a > 1,\ n > 1$$

είναι πρώτος.

Πρόταση 3.2.3. *Αν ο $a^n - 1$, $a > 1$, $n > 1$ είναι πρώτος, τότε κατ' ανάγκη $a = 2$ και n πρώτος αριθμός*

Απόδειξη. Είναι γνωστή η παραγοντοποίηση

$$(a^n - 1) = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Ο δεύτερος παράγοντας είναι μεγαλύτερος του 1. Επειδή $a^n - 1$, πρώτος, έπεται ότι $a - 1 = 1$, δηλαδή $a = 2$.

Αν τώρα n είναι σύνθετος, $n = m \cdot l$, $m > 1$, $l > 1$ τότε

$$2^n - 1 = 2^{ml} - 1 = (2^m)^l - 1 = (2^m - 1)((2^m)^{l-1} + \cdots + 2^m + 1).$$

Αμφότεροι οι παράγοντες του δεξιού μέλους είναι μεγαλύτεροι του 1, δηλαδή ο $2^n - 1$ είναι σύνθετος.

Συνεπώς θα πρέπει ο n να είναι πρώτος. □

Παρατήρηση: Από την πρόταση 3.2.3 προκύπτει αμέσως ότι αναγκαία συνθήκη για να είναι ένας αριθμός της μορφής $2^n - 1$ πρώτος, είναι να είναι ο n πρώτος. Βέβαια, το αντίστροφο *δεν* ισχύει, π.χ. για $p = 11 \in \mathbb{P}$ ο $2^p - 1 = 2^{11} - 1 = 2047 = 23 \cdot 89$ *δεν* είναι πρώτος.

Τελικά για να βρούμε *όλους* τους *άρτιους τέλειους* αριθμούς θα πρέπει να γνωρίζουμε όλους τους πρώτους της μορφής $2^p - 1$, $p \in \mathbb{P}$.

Ας ξαναγυρίσουμε όμως για λίγο πίσω στην ιστορία ανακάλυψης τέλειων αριθμών. Άγνωστος μαθηματικός απέδειξε το 1496 ότι ο $2^{13} - 1 = 8191$ είναι πρώτος, επομένως ο $2^{12}(2^{13} - 1) = 33550336$ είναι ο 5ος τέλειος αριθμός.

Επομένως η πρώτη εικασία του Νικομάχου είναι λάθος (ο 5ος τέλειος αριθμός έχει 8 ψηφία).

Στα 1555 ο Schebyl καί, λίγο αργότερα, στα 1588 ο Piedro Antonio Cataldi απέδειξαν ότι οι $2^{17}-1 = 131071$ και $2^{19}-1 = 524287$ είναι πρώτοι και έτσι ανακάλυψαν τους επόμενους δύο τέλειους αριθμούς 8589869056, 137438691328.

Παρατήρηση: Αμφότεροι οι διαδοχικοί τέλειοι 5ος και 6ος έχουν ψηφίο μονάδων το 6. Άρα δεν ισχύει το εναλλάξ στην εικασία (3).

Το υπόλοιπο της εικασίας (3) όμως είναι σωστό. Αποδείχθηκε από τον Euler.

Πρόταση 3.2.4. *Το ψηφίο των μονάδων ενός άρτιου τέλειου φυσικού αριθμού m είναι 6 ή 8.*

Απόδειξη. Σύμφωνα με την πρόταση 3.2.2 ο $m = 2^{n-1}(2^n-1)$ και ο $2^n-1 =: p$ είναι πρώτος.

Σύμφωνα με την πρόταση 3.2.3 θα πρέπει ο n να είναι πρώτος, $n =: q \in \mathbb{P}$. Αν $q = 2$, τότε $m = 2\cdot 3 = 6$, ισχύει.

Έστω τώρα $q > 2$. Ξεχωρίζουμε δύο περιπτώσεις.

Περίπτωση 1: Ο q είναι της μορφής $4l+1$. Στην περίπτωση αυτή ο m γράφεται

$$m = 2^{4l}(2^{4l+1}-1) = 2^{8l+1} - 2^{4l} = 2\cdot 16^{2l} - 16^l.$$

Επαγωγικά αποδεικνύεται ότι ο 16^l, γράφεται πάντα στη μορφή $10\cdot s + 6$.

Πραγματικά, για $l = 1$, ισχύει. Έστω ότι ισχύει για $l = k$, δηλαδή ότι $16^k = 10s + 6$. Για $l = k+1$, $16^{k+1} = 16^k\cdot 16 = (10s+6)16 = 160s + 96 = 10t + 6$ όπου $(t = 16s + 9)$.

Επομένως, ο

$$m = 2(10s_1+6) - (10s_2+6) = 10(2s_1 - s_2) + 6.$$

Περίπτωση 2: Ο q είναι της μορφής $4l+3$. Τότε $m = 2^{4l+2}(2^{4l+3}-1) = 2^{8l+5} - 2^{4l+2} = 2\cdot 16^{2l+1} - 4\cdot 16^l = 2(10t_1+6) - 4(10t_2+6) = 10(2t_1 - 4t_2) - 12 = 10(2t_1 - 4t_2 - 2) + 8$

□

Παρατήρηση 3.2.5. Θα μπορούσε μάλιστα κανείς να αποδείξει ότι τα τελικά ψηφία άρτιου τέλειου αριθμού είναι το 6 ή το 28 [3].

3.2.1 Πρώτοι αριθμοί Mersenne και Fermat

Ορισμός. Οι πρώτοι αριθμοί της μορφής

$$M_p := 2^p - 1,\ p \in \mathbb{P}$$

λέγονται *πρώτοι αριθμοί (του) Mersenne*.

Μέχρι σήμερα (Νοέμβριος 2014), είναι γνωστοί συνολικά 48 πρώτοι αριθμοί του Mersenne και, συνεπώς, 48 άρτιοι τέλειοι αριθμοί.

Παρατηρήσεις

1. Είναι μέχρι σήμερα άγνωστο αν υπάρχουν άπειροι τέλειοι αριθμοί, αφού δεν είναι γνωστό αν υπάρχουν άπειροι πρώτοι αριθμοί Mersenne. Σύμφωνα με τον M. de Sautoy [12, σελ. 326], ο P. Erdös κατέταξε το πρόβλημα μεταξύ των μεγαλυτέρων ανοιχτών προβλημάτων της Θεωρίας Αριθμών. Όποιος βρει έναν πρώτο αριθμό Mersenne με περισσότερα από 10.000.000 δεκαδικά ψηφία θα πάρει 100.000 δολλάρια. `http://primes.utm.edu/Mersenne`.

2. Μέχρι σήμερα δεν είναι γνωστός κανείς *περιττός τέλειος* αριθμός. Τα μέχρι τώρα γνωστά αποτελέσματα δείχνουν ότι, αν υπάρχει κάποιος θα πρέπει να είναι «αρκετά» μεγάλος.

Σε αναλογία προς την πρόταση 3.2.4 μπορούμε να θεωρήσουμε ακέραιους της μορφής $a^n + 1$.

Πρόταση 3.2.6. *Αν ο φυσικός αριθμός*

$$a^n + 1,\ a > 1,\ n > 0$$

είναι πρώτος τότε κατ΄ ανάγκη ο a είναι άρτιος και ο $n = 2^l$, $l \in \mathbb{N}$.

Απόδειξη. Αν ο a ήταν περιττός, τότε ο $a^n + 1 \geq 4$ θα ήταν άρτιος, δηλαδή όχι πρώτος, άτοπο.

Αν ο n δεν ήταν δύναμη του 2 θα είχε κάποιον περιττό πρώτο παράγοντα, έστω q, $n = mq$.

Τότε όμως θα είχαμε

$a^n + 1 = a^{mq} + 1 = (a^m + 1)(a^{m(q-1)} - a^{m(q-2)} + \cdots - a^m + 1)$.

Επειδή $q \geq 3$, οι παράγοντες του δεξιού μέλους είναι αμφότεροι μεγαλύτεροι του 1 και άρα ο $a^n + 1$ δεν είναι πρώτος. Συνεπώς $n = 2^r$, $r \in \mathbb{N}$. □

Ο Fermat θεώρησε την ειδική περίπτωση που $a = 2$, δηλαδή αριθμούς της μορφής $F_n := 2^{2^n} + 1$.

Για $n = 0, 1, 2, 3, 4$ οι αριθμοί αυτοί είναι πρώτοι. Πράγματι

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537.$$

Η εικασία του ήταν ότι όλοι οι αριθμοί αυτής της μορφής είναι πρώτοι. Εδώ όμως ο Fermat στάθηκε άτυχος. Αν είχε κάνει ένα βήμα ακόμη θα είχε διαπιστώσει το λάθος του.

Πράγματι, ο F_5 διαιρείται από το 641.

$$F_5 = 4294967297 = 641 \cdot 60417.$$

Βέβαια η διαπίστωση αυτή έγινε έναν αιώνα αργότερα από τον Euler (1732).

Ορισμός. Κάθε *πρώτος* αριθμός της μορφής $F_n := 2^{2^n} + 1$, θα λέγεται *πρώτος αριθμός Fermat*.

Μέχρι σήμερα οι μόνοι γνωστοί πρώτοι αριθμοί Fermat είναι οι F_0, F_1, F_2, F_3 και F_4.

Οι αριθμοί αυτοί σχετίζονται με τη δυνατότητα κατασκευής κανονικού πολυγώνου.

Στα 1796 ο 19ετής Gauss απέδειξε ότι ένα κανονικό n-γώνο είναι κατασκευάσιμο με κανόνα και διαβήτη. Τότε ο n θα είναι κατ΄ ανάγκη της μορφής

$$n = 2^\ell p_1 p_2 \cdots p_s$$

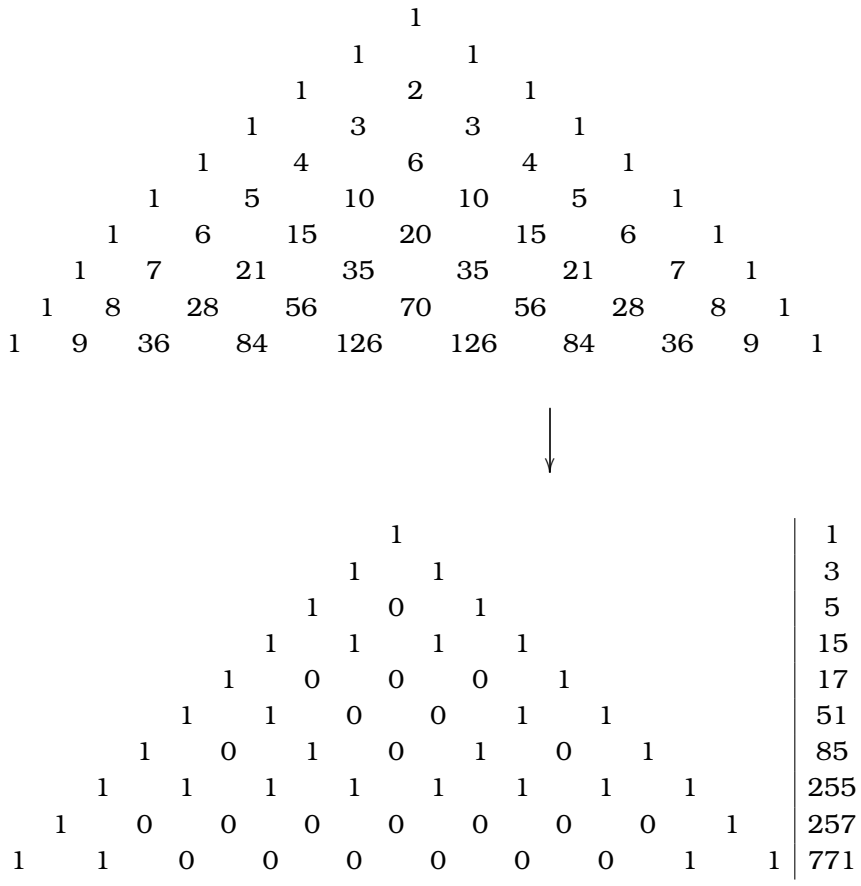
όπου $\ell \in \mathbb{N}$ και p_i $(1 \leq i \leq s)$ διακεκριμένοι μεταξύ τους πρώτοι αριθμοί Fermat. Η απόδειξή του περιέχεται στα άρθρα (προτάσεις) 365 και 366 του [1]. Ισχυρίσθηκε μάλιστα ότι ισχύει και το αντίστροφο αλλά η πρώτη πλήρης απόδειξη δημοσιεύτηκε από τον Wantzel στα 1837. Με έμφαση πάντως παρατηρεί ότι από τους χρόνους του Ευκλείδη κατά τους οποίους δόθηκε η κατασκευή ισόπλευρου τριγώνου και κανονικού πενταγώνου με την βοήθεια κανόνα και διαβήτη μέχρι την εποχή του, τίποτε άλλο σχετικό δεν είχε γίνει.

Η πρώτη εγγραφή του στο ημερολόγιό του η οποία έχει ημερομηνία 30 Μαρτίου 1796 αναφέρεται στα θεμέλια στα οποία στηρίζεται η διαμέριση του κύκλου (σε ίσα μέρη και στη διαίρεση γεωμετρικά σε 17 μέρη)

"Principia quibus innitur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes?"

Οι M. Gardner και W. Watkins παρατήρησαν ανεξάρτητα ο ένας από τον άλλο ότι, αν θεωρήσουμε τις πρώτες 32 γραμμές του τριγώνου του Pascal, αντικαταστήσουμε τους άρτιους αριθμούς κάθε γραμμής με 0 και τους περιττούς με 1 και θεωρήσουμε κάθε γραμμή που σχηματίζεται

ως έναν αριθμό γραμμένο στη δυαδική μορφή, αυτοί παριστούν περιττούς φυσικούς που είναι κατασκευάσιμοι με κανόνα και διαβήτη.



3.2.2 Πολυγωνικοί Αριθμοί

Οι αρχαίοι Έλληνες όρισαν επίσης τους *πολυγωνικούς αριθμούς*. Κατά τον Heath [13, σελ. 100], η θεωρία των πολυγωνικών αριθμών ανάγεται στον Πυθαγόρα.

Οι πολυγωνικοί αριθμοί συνδέονται με κανονικά πολύγωνα και αποτελούν μέρος του συνδέσμου μεταξύ Γεωμετρίας και Θεωρίας Αριθμών.

Οι αριθμοί $1, 3, 6, 10, \ldots$ λέγονται *τρίγωνοι* αριθμοί. Πρόκειται για τους αριθμούς της μορφής $1 + 2 + \cdots + +n = \frac{n(n+1)}{2}$.

Οι αριθμοί $1, 4, 9, 16, \ldots$ λέγονται *τετράγωνοι*. Πρόκειται για τους αριθμούς της μορφής n^2.

Οι αριθμοί $1, 5, 12, 22, \ldots$ λέγονται *πεντάγωνοι αριθμοί*. Πρόκειται για αριθμούς της μορφής

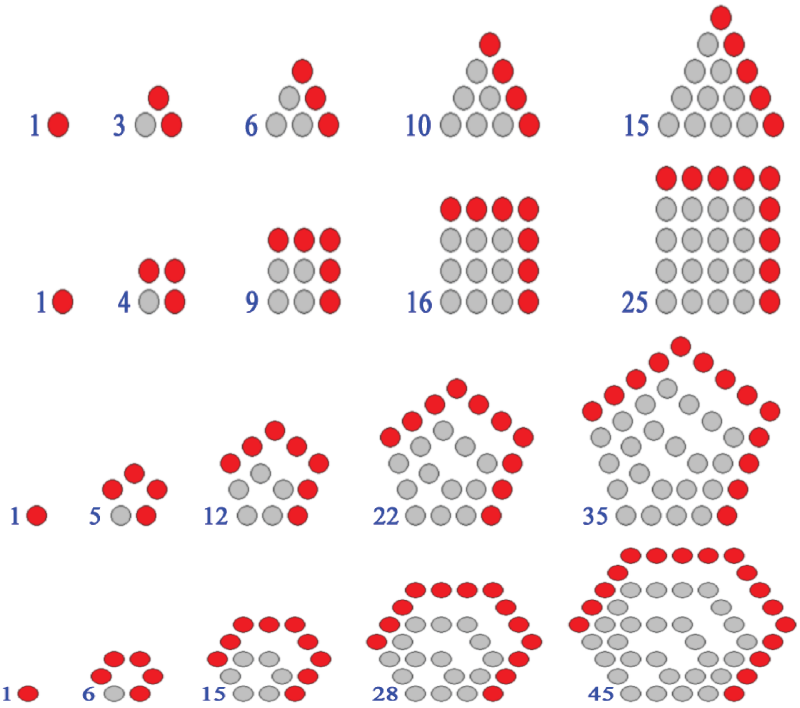
$$3\frac{t^2-1}{2} + t | t \geq 1$$

Γενικά, οι *n-πολυγωνικοί* αριθμοί ορίζονται ως $(n-2)\frac{t^2-t}{2} + t | t \geq 1$.

Οι ιδιότητές τους μελετήθηκαν από τον Πυθαγόρα και τους μαθητές του (6ος αιώνας π.Χ.,), τον Νικόμαχο τον Γερασηνό στην «Ἀριθμητική Ἐισαγωγή» του (1ος αιώνας μ.Χ.) και τον Διόφαντο, στο ομώνυμο έργο του. (3ος αιώνας μ.Χ.).

Στην 18η σημείωσή του στο περιθώριο του αντιτύπου των *Αριθμητικών* ο Fermat [10] διατυπώνει την εικασία ότι:

«Κάθε θετικός ακέραιος είναι άθροισμα το πολύ n n-πολυγωνικών αριθμών».



Σχήμα 3.2.2: Πολυγωνικοί Αριθμοί, Το παρόν σχήμα αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Polygonal_Number_3.gif`

Προσθέτει μάλιστα ότι σκοπεύει να γράψει ένα βιβλίο σχετικά με το θέμα, κάτι το οποίο όμως δεν έγινε ποτέ.

Η σημείωση του Fermat, έχει γραφεί δίπλα στο πρόβλημα 29 του βιβλίου IV του Διόφαντου.

«Εὑρεῖν τέσσαρας ἀριθμούς «τετραγώνους» οἵ συντεθέντες καί προσλαβόντας τάς ἰδίας πλευράς συντεθείσας ποιοῦσι δοθέντα ἀριθμόν»

Δηλαδή να βρεθούν 4 τετράγωνοι αριθμοί των οποίων το άθροισμα συν το άθροισμα των τετραγωνικών ριζών τους μας δίνουν δοσμένο ακέραιο αριθμό.

Εδώ ο Bachet παρατηρεί ότι κάθε θετικός ακέραιος ή είναι τέλειο τετράγωνο ή αλλιώς μπορεί να γραφεί ως άθροισμα 2,3 ή 4 τετραγώνων. Ο Bachet παρατηρεί ότι αυτό ισχύει για τους φυσικούς από 1 ως 125 και συμπεραίνει ότι αυτό ισχύει για κάθε θετικό ακέραιο. [10].

Για τριγωνικούς αριθμούς η εικασία αποδείχθηκε από τον Gauss, ο οποίος στις 10 Ιουλίου του 1796 σημειώνει στο ημερολόγιό του, ως άλλος Αρχιμήδης [14],[2]:

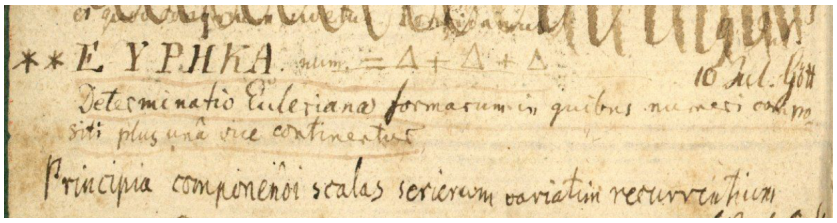
«ΕΥΡΗΚΑ! *num*[*erus*] = Δ + Δ + Δ»

Για τετράγωνους αποδείχθηκε από τον J-L. Lagrange, στα 1798. Πλήρη απόδειξη της εικασίας, έδωσε ο Cauchy στα 1813.

Παρατηρήσεις

1. Για μια σύντομη ιστορική εισαγωγή παραπέμπουμε στο βιβλίο του Tattersall [5, σελ. 1-23].

2. Αν τεθεί το πρόβλημα του «τετραγωνισμού του τριγώνου», της εύρεσης δηλαδή τετραγώνων αριθμών οι οποίοι είναι και τρίγωνοι, τότε βλέπουμε ότι υπάρχουν τέτοιοι, ο πιο μικρός είναι ο $36 = 6^2 = \frac{8\cdot 9}{2}$ και ότι η εύρεση όλων ανάγεται στην εύρεση των λύσεων της διοφαντικής εξίσωσης $X^2 - 2Y^2 = 1$. [6, κεφ. 28]



Σχήμα 3.2.3: Η σημείωση του Gauss, Το παρόν έργο αποτελεί κοινό κτήμα (public domain), λόγω παρέλευσης 70 ετών από τον Θάνατο του δημιουργού.

Εξισώσεις της μορφής $X^2 - Dy^2 = 1$, $D > 1$, $D \neq \square$ λέγονται *εξισώσεις του Pell*

3. Άλλες σχετικές προτάσεις που οδηγούν σε κυβικές διοφαντικές εξισώσεις μπορεί να βρεί ο ενδιαφερόμενος αναγνώστης στο βιβλίο των Kazuya Kato, Nobushgo Kurokawa, Takeshi Saito [7].

3.2.3 Ισοδύναμοι Αριθμοί

Αν (x, y, z) είναι πυθαγόρεια τριάδα τότε το εμβαδόν του αντίστοιχου ορθωγωνίου τριγώνου είναι φυσικός αριθμός. Άραβες μαθηματικοί κατά τον 10ο αιώνα γενίκευσαν το ερώτημα:

«Ποιοι φυσικοί αριθμοί είναι εμβαδόν ορθογωνίου τριγώνου με πλευρές ρητούς αριθμούς;»

Ορισμός 3.2.7. Οι φυσικοί αριθμοί που προκύπτουν ως εμβαδόν ορθογωνίου τριγώνου με πλευρές ρητούς λέγονται ισοδύναμοι αριθμοί (congruent numbers).

Παρατήρηση 3.2.8. Ο πιο μικρός ισοδύναμος αριθμός ο οποίος προκύπτει από πυθαγόρεια τριάδα είναι ο 6. Είναι το εμβαδόν ορθογωνίου τριγώνου με μήκη πλευρών 3,4,5.

Όμως και ο 5 είναι ισοδύναμος αριθμός. Πράγματι, αντιστοιχεί στην τριάδα $(3/2, 20/3, 41/6)$ αφού

$$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2 \text{ και } E = \frac{3/2 \cdot 20/3}{2} = 5.$$

Η τριάδα αυτή ανακαλύφθηκε από τον Leonardo Pisano (Fibonacci) (1220) [8, προτ. 17]

Μια ισοδύναμη μορφή του παραπάνω ορισμού των ισοδύναμων αριθμών είναι:

Πρόταση 3.2.9. *Ο θετικός ακέραιος n είναι ισοδύναμος τότε και μόνο τότε όταν το σύστημα των διοφαντικών εξισώσεων*

$$\begin{aligned} X^2 + nY^2 &= S^2 \\ X^2 - nY^2 &= T^2 \end{aligned} \tag{3.2.1}$$

έχει ακέραια λύση (x, y, s, t) με $y \neq 0$.

Απόδειξη. Αν ο n είναι ισοδύναμος, τότε υπάρχει τριάδα ρητών (a, b, c), ώστε $a^2 + b^2 = c^2$ και $n = \frac{ab}{2}$. Επομένως

$$(a \pm b)^2 = a^2 \pm 2ab + b^2 = c^2 \pm 4n,$$

δηλαδή το σύστημα (3.2.1) έχει την ακέραια λύση $(x, y, s, t) = (c, 2, a + b, a - b)$.

Αντίστροφα, αν (x, y, s, t) μία ακέραια λύση του διοφαντικού συστήματος (3.2.1) με $y \neq 0$, τότε η ρητή τριάδα

$$(a, b, c) = \left(\frac{s-t}{y}, \frac{s+t}{y}, \frac{2x}{y}\right)$$

επαληθεύει την

$$a^2 + b^2 = \left(\frac{s-t}{y}\right)^2 + \left(\frac{s+t}{y}\right)^2 = \left(\frac{2x}{y}\right)^2 = c^2$$

και επιπλέον

$$\frac{s-t}{y}\frac{s+t}{y} = \frac{s^2-t^2}{2y^2} = \frac{2ny^2}{2y^2} = n,$$

δηλαδή ο n είναι ισοδύναμος. □

Παρατήρηση 3.2.10. Άμεση συνέπεια της πρότασης είναι ότι ο θετικός ακέραιος n είναι ισοδύναμος ακριβώς τότε όταν υπάρχει ρητός αριθμός x τέτοιος ώστε οι $x^2 - n$ και $x^2 + n$ να είναι τέλεια τετράγωνα ρητών.

Σε αυτή την μορφή δόθηκε το πρόβλημα στον Fibonacci από τον Johann Panormitanus of Palermo:

«Να βρεθεί ένας ρητός αριθμός x ώστε $x^2 \pm 5$ να είναι τετράγωνο ρητών.»

Το οποίο μάλιστα αποτέλεσε αφορμή να γράψει ο Fibonacci ένα ολόκληρο βιβλίο σχετικό με το θέμα το «Liber Quadratorum»

Παρατήρηση 3.2.11. Ο 1 δεν είναι ισοδύναμος αριθμός. Αν ήταν, σύμφωνα με την πρόταση 3.2.9 το σύστημα

$$\begin{aligned} X^2 + Y^2 &= S^2 \\ X^2 - Y^2 &= T^2 \end{aligned}$$

θα είχε ακέραια λύση (x, y, s, t) με $y \neq 0$ και συνεπώς και η διοφαντική εξίσωση

$$X^4 - Y^2 = Z^2$$

θα είχε ακέραια, μη τετριμμένη λύση. Αυτό όμως είναι άτοπο σύμφωνα με την 2.3.6

Παρατήρηση 3.2.12. Είναι φανερό ότι ο θετικός ακέραιος n είναι ισοδύναμος αν, και μόνο αν, και ο nm^2 είναι ισοδύναμος. Πράγματι, στη ρητή τριάδα (a, b, c) με $a^2 + b^2 = c^2$ και $n = \frac{ab}{2}$ αντιστοιχεί η (ma, mb, mc) με $(ma)^2 + (mb)^2 = (mc)^2$ και $nm^2 = \frac{m^2ab}{2}$. Αυτό σημαίνει ότι ούτε ο 4 είναι ισοδύναμος και ότι αρκεί να περιοριστούμε μόνο σε ελεύθερους τετραγώνου αριθμούς n.

Παρατήρηση 3.2.13. Για διάφορα ιστορικά στοιχεία παραπέμπουμε στο [4, κεφ. XVI]. Επίσης μια σύντομη περιγραφή θα βρει ο αναγνώστης στο [11, D 27].

Θα μπορούσε να αναρωτηθεί κανείς πώς βρήκαμε την απάντηση για $n = 5$. Εφαρμόζουμε τον αλγόριθμο:

1. Θεωρούμε δύο θετικούς ακέραιους s, t με $(s, t) = 1$ όπου ο ένας είναι άρτιος και ο άλλος περιττός. Η πυθαγόρεια τριάδα $(x = s^2 - t^2, y = 2st, z = s^2 + t^2)$ μας δίνει τρίγωνο εμβαδού $E = \frac{xy}{2}$.

2. Αν $E = m^2 n$ τότε ο n είναι ισοδύναμος αφού είναι το εμβαδόν τριγώνου με πλευρές $(x/m, y/m, z/m)$. Έτσι για $s = 5, t = 4$ έχουμε $(x, y, z) = (9, 40, 41)$ με $E = xy/2 = 180 = 6^2 \cdot 5$. Συνεπώς το 5 είναι ισοδύναμος και το ορθογώνιο τρίγωνο με εμβαδόν 5 έχει πλευρές $(9/6, 40/6, 41/6) = (3/2, 20/3, 41/6)$.

Ο παραπάνω αλγόριθμος παρουσιάζει δύο σοβαρά μειονεκτήματα:

1. Δεν γνωρίζουμε πόσα βήματα πρέπει να κάνουμε για να αποφασίσουμε τελικά αν ο δοσμένος θετικός είναι ισοδύναμος ή όχι. Μετά από αρκετές δοκιμές, αν δεν βρούμε πυθαγόρεια τριάδα με εμβαδόν $m^2 n$ για κάποιον n, τότε πιθανόν ο n να μην είναι ισοδύναμος αλλά μπορεί να είναι ισοδύναμος και να μην πήραμε αρκετές τιμές των s, t. Συχνά,για αρκετά μικρές τιμές του n χρειάζεται να πάρουμε μεγάλες τιμές των (s, t). Έτσι, για $n = 157$ η πιο μικρή λύση είναι:

$$\begin{aligned} X &= \frac{157841 \cdot 4947203 \cdot 526771095761}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441} \\ Y &= \frac{2^2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 526771095761} \\ Z &= \frac{20085078913 \cdot 1185369214457 \cdot 942545825502442041907480 1}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 526771095761} \end{aligned}$$

   το αποτέλεσμα αυτό υπολογίστηκε από τον D. Zagier.

2. Αν ο n δεν είναι ισοδύναμος, τότε ο αλγόριθμός δεν σταματάει ποτέ.

Το πρόβλημα λοιπόν παραμένει.

Δίνεται ο ελεύθερος τετραγώνου θετικός ακέραιος n. Θα μπορούσαμε να βρούμε κάποιο κριτήριο ελέγχου για το αν ο n είναι ισοδύναμος ή όχι. Η απάντηση δίνεται από το ακόλουθο:

Θεώρημα 3.2.14. *Ο αριθμός n είναι ισοδύναμος τότε και μόνο τότε όταν η καμπύλη*

$$E_n : Y^2 = X^3 - n^2 X,$$

έχει άπειρο πλήθος ρητών σημείων.

Δυστυχώς όμως το θεώρημα αυτό μεταφέρει ένα πολύ δύσκολο πρόβλημα σε ένα αλλο εξίσου δύσκολο πρόβλημα με το αρχικό. Το μόνο πλεονέκτημα είναι ότι το δεύτερο πρόβλημα αποτελεί μέρος μιας καλά δομημένης θεωρίας. Έτσι, με χρήση σημαντικών θεωρημάτων της αριθμητικής αυτών των καμπυλών κατάφερε ο J. Tunnel (1983) να αποδείξει ένα πολύ πιο πρακτικό κριτήριο, το οποίο όμως και πάλι έχει το μειονεκτήμα η μία του κατεύθυνση να στηρίζεται σε μια αναπόδεικτη μέχρι σήμερα εικασία, την εικασία των Birch Swinnerton-Dyer.

Το πρόβλημα των ισοδύναμων αριθμών αποτέλεσε το κίνητρο συγγραφής του [9], στο οποίο αναπτύσεται όλη σχεδόν η απαιτούμενη θεωρία για την απόδειξη του θεωρήματος του Tunnel.

3.3 Κατάλογος Sloane

Ο Neil Sloane ξεκίνησε το 1964 να καταγράφει συστηματικά ακολουθίες φυσικών αριθμών και η εργασία του αυτή οδήγησε σήμερα στον κατάλογο που είναι γνωστός ως The On-Line Encyclopedia of Integer Sequences `https://oeis.org`. Τα προγράμματα υπολογιστικής άλγεβρας έχουν πρόσβαση σε αυτό τον κατάλογο. Για παράδειγμα η ακολουθία των τέλειων αριθμών είναι καταλογογραφημένη ως A000396ηττπσ://οεις.οργ/A000396 ενώ για να δούμε και να επεξεργαστούμε τους πρώτους 10 πρώτους όρους της στο sage δίνουμε

```
sage: a=sloane.A000396;a
Perfect numbers: equal to sum of proper divisors.
sage: L=[a[i] for i in range(1,10)];L
[6,
 28,
 496,
 8128,
 33550336,
 8589869056,
 137438691328,
 2305843008139952128,
 2658455991569831744654692615953842176]
```

Αξίζει να σημειωθεί ότι ο κατάλογος του Sloane παρέχει τη δυνατότητα αντίστροφης αναζήτησης.

```
sloane_find([2,3,5,7], 2)       # optional - internet
Searching Sloane's online database...
[[40, 'The prime numbers.', [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109,
113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191,
193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271]],
[41, 'a(n) = number of partitions of n (the partition numbers).', [1, 1,
2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, 135, 176, 231, 297, 385,
490, 627, 792, 1002, 1255, 1575, 1958, 2436, 3010, 3718, 4565, 5604,
6842, 8349, 10143, 12310, 14883, 17977, 21637, 26015, 31185, 37338,
44583, 53174, 63261, 75175, 89134]]]
```

Παρατηρήστε ότι το κομμάτι $2, 3, 5, 7$ περιέχεται σε δύο γνωστές ακολουθίες και η αναζήτηση τις επέστρεψε και τις δύο. Είναι σαφές ότι μια πεπερασμένη ακολουθία αριθμών δεν περιέχει αρκετή πληροφορία για να περιγράψει πλήρως μια άπειρη ακολουθία αριθμών.

3.4 Παραγοντοποίηση και Κρυπτογραφία

Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής, κάθε φυσικός αριθμός n, $n > 1$ γράφεται μονοσήμαντα ως γινόμενο πρώτων αριθμών.

Ένα σημαντικό πρόβλημα είναι η παραγοντοποίηση δοσμένου φυσικού αριθμού n. Πρόκειται για αρκετά δύσκολο πρόβλημα. Τα τελευταία χρόνια έχουν αναπτυχθεί διάφορες μέθοδοι παραγοντοποίησης. Πέρα από θεωρητικό ενδιαφέρον, η παραγοντοποίηση απέκτησε και πρακτικό ενδιαφέρον, διότι παίζει σημαντικό ρόλο στην κρυπτολογία.

Στην παράγραφο αυτή θα ασχοληθούμε με μερικές απλές μεθόδους παραγοντοποίησης και με μικρή αναφορά στην Κρυπτογραφία. Θα επανέλθουμε στο θέμα και στα επόμενα κεφάλαια.

3.4.1 Παραγοντοποίηση Fermat

Πρόταση 3.4.1. *Για κάθε περιττό φυσικό αριθμό n, $n > 1$ υπάρχει μία αμφιμονοσήμαντη αντιστοιχία μεταξύ των παραγοντοποιήσεων του n, σε γινόμενο δύο θετικών ακεραίων $n = ab$, $a \geq b > 0$ και παραστάσεων του n, ως διαφορά τετραγώνων $n = t^2 - s^2$, όπου s και t φυσικοί αριθμοί.*

Η αντιστοιχία δίνεται από τις ισότητες

$$t = \frac{a+b}{2},\ s = \frac{a-b}{2}\quad a = t+s,\ b = t-s.$$

Απόδειξη. Αν $n = a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = t^2 - s^2$. Αν πάλι $n = t^2 - s^2 = (t-s)(t+s) = a \cdot b$, όπου $a = t - s$ και $b = t + s$, δηλαδή $t = \frac{a+b}{2}$ και $s = \frac{a-b}{2}$ □

Η ιδέα του Fermat ήταν, αν $n = a \cdot b$ και a, b δύο περιττοί ακέραιοι, περίπου του ίδιου μεγέθους, τότε ο $s = \frac{a-b}{2}$ είναι σχετικά μικρός και ο t λίγο μεγαλύτερος της $\sqrt{n}$. Επομένως, θα μπορούσαμε να υπολογίσουμε τους a και b δοκιμάζοντας διάφορες τιμές του t στις $[\sqrt{n}] + 1$, $[\sqrt{n}] + 2, \ldots$, μέχρι να βρούμε κάποιο t για το οποίο το $t^2 - n = s^2$, είναι τέλειο τετράγωνο.

Παράδειγμα. Να παραγοντοποιηθεί ο φυσικός αριθμός $n = 200819$.

Ο $[\sqrt{n}] + 1 = [\sqrt{200819}] + 1 = 449$. Για $t = 449$ υπολογίζουμε $449^2 - 200819 = 782$, το οποίο *δεν* είναι τέλειο τετράγωνο.

Παίρνουμε $t = 450$, $450^2 - 200819 = 1681 = 41^2$. Επομένως $200819 = 450^2 - 41^2 = (450 + 41)(450 - 41) = 491 \cdot 409$.

Αν οι ακέραιοι a και b δεν είναι του ίδιου μεγέθους για κάθε παραγοντοποίηση του $n = ab$ τότε είναι πιθανόν η μέθοδος Fermat να ανακαλύψει τους παράγοντες a, b μετά από αρκετές δοκιμές. Στην περίπτωση είναι πιο βολικό να χρησιμοποιούμε την ακόλουθη γενίκευση:

Επιλέγουμε ένα μικρό φυσικό αριθμό k και θέτουμε $t = k[\sqrt{n}] + 1$, $k[\sqrt{n}] + 2, \ldots$ μέχρι να επιτύχουμε παράσταση της μορφής $t^2 - k \cdot n$ η οποία είναι τέλειο τετράγωνο,

$$t^2 - k \cdot n = s^2$$

Όταν το επιτύχουμε αυτό έχουμε $(t+s)(t-s) = kn$. Αυτό σημαίνει ότι οι $t+s$ και n έχουν κάποιο, μη-τετριμμένο, κοινό παράγοντα ο οποίος ευρίσκεται από τον υπολογισμό του $(t + s,\ n)$.

Παράδειγμα. Να παραγοντοποιηθεί ο 14167.

Αν προσπαθήσουμε με την κλασική παραγοντοποίηση Fermat, θα πρέπει να θέσουμε $t = 377, 378, \ldots$ και να ...κουραστούμε θέτοντας διάφορες τιμές του t. Αν όμως θέσουμε $t = [\sqrt{3n} + 1] = 652, 653, 654, 655$, βρίσκουμε

$$655^2 - 3 \cdot 141467 = 68^2$$

και υπολογίζουμε τον $(655 + 68,\ 141467) = 241$.

Τελικά μια παραγοντοποίηση του αριθμού 14167 είναι $241 \cdot 587$.

Η απάντηση στο ερώτημα γιατί δούλεψε η μέθοδος για $k = 3$ είναι ότι στην παραγοντοποίηση του $n = a \cdot b = 241 \cdot 587$ το $b = 587$ είναι κοντά στο $3a = 3 \cdot 241 = 723$.

Από τα παραπάνω φαίνεται ότι χρειαστήκαμε 4 μόνο τιμές του t, ενώ αν εφαρμόζαμε τη μέθοδο για $k = 1$ θα χρειαζόμασταν 38 τιμές του t

Δύο λέξεις για την Κρυπτογραφία

Το κύριο αντικείμενο της *κρυπτογραφίας* είναι η μελέτη μεθόδων επικοινωνίας μεταξύ δύο ανθρώπων, τους οποίους θα ονομάζουμε Αλίκη και Βασιλάκη, μέσω κάποιου επισφαλούς μέσου

(καναλιού), κατά τέτοιο τρόπο ώστε ο οποιοσδήποτε ανεπιθύμητος τρίτος, να μην είναι σε θέση να κατανοήσει το περιεχόμενο του μηνύματος.

Συνήθως χρειάζεται ένα «κλειδί» κρυπτογράφησης μέσω του οποίου ο αποστολέας μετατρέπει το μήνυμα σε «ακατανόητη» μορφή και, φυσικά και ο παραλήπτης χρειάζεται ένα αντίστοιχο «κλειδί» αποκρυπτογράφησης του μηνύματος. Φυσικά για τον ανεπιθύμητο τρίτο, αναπτυχθήκαν μέθοδοι οι οποίες να επιτρέπουν το «σπάσιμο» του κώδικα επικοινωνίας. Η διαδικασία αυτή λέγεται *κρυπτοανάλυση*. Η κρυπτογραφία αναπτύχθηκε από πολύ παλιά κυρίως για στρατιωτικούς σκοπούς και τη διπλωματία. Οι Σπαρτιάτες ήταν αυτοί που πρώτοι χρησιμοποίησαν στρατιωτική κρυπτογραφία.

Θα αναρωτηθεί τώρα ο αναγνώστης τι σχέση έχει η κρυπτογραφία με τη Θεωρία Αριθμών. Αυτό θα το δούμε αργότερα στα επόμενα κεφάλαια. Προς το παρόν θα παραμείνουμε (αρκεστούμε) στο έργο του G.H. Hardy *Η απολογία ενός μαθηματικού*, Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 1991, σελίδα 82:

«Τόσο ο Gauss όσο και μικρότερου βεληνεκούς μαθηματικοί μπορούν δικαιολογημένα να χαίρονται που υπάρχει- όπως και να'χει το θέμα - μια επιστήμη (εννοεί τη Θεωρία Αριθμών), που η απόστασή της από τις συνήθεις ανθρώπινες δραστηριότητες πρέπει να την κρατήσει ευγενή και καθαρή».

Σχήμα 3.4.1: H. Hardy, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Ghhardy@72.jpg`

Βιβλιογραφία

[1] C. F. Gauss: *Untersuchungen über höhere Arithmetik*. Chelsea Publishing Company, Second Edition, New York, 1981.

[2] C. F. Gauss: *Mathematisches Tagebuch*. Ostwalds Klassiker der exacten Wissenschaften 256, Akademische Verlangsgesellschaft, Leipzig, 1985.

[3] Damvid, M, Burton: *Elementary Number Theory*. UBS New Delhi, 1998. second edition.

[4] E. Dickson: *History of the Theory of Numbers*. 1, 1999.

[5] James J. Tattersall: *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, second edition, 2005.

[6] J.Silverman: *A friendly Introduction to Number Theory*. Prentice Hall, 2012.

[7] Kazuya Kato, Nobushgo Kurokawa, Takeshi Saito: volume 186. 2009.

[8] Leonardo Fibonacci: *The Book of Squares*. Academic Press, Boston, 1987. An Annotated Translation Into Modern English by L. E. Singler.

[9] Neal Koblitz: *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag New York, 1993. Second Edition.

[10] Pierre De Fermat: *Bemerkungen zu Diophant*. Klassiker der Exakten Wissenshaften, Akademic Verlaggesellschaft M.B. U. Leipzig, 1932. Aus Dem Lateinischen übersetzt und mit Anmerkungen herausgegeben von Max Miller Ostwald's.

[11] R. Guy: *Unsolved problems in Number Theory*. Springer Verlag New York, 1994. Second edition.

[12] Marcus du Sautoy: *Η μουσική των πρώτων αριθμών, το μεγαλύτερο ανεπίλυτο μυστήριο των μαθηματικών*. 2005.

[13] Sir Thomas L. Heath: *Ιστορία των Ελληνικών Μαθηματικών*. Κ.Ε.ΕΠ.ΕΚ., Αθήνα, 2001.

[14] W.S. Anglin: *The Queen of Mathematics: An Introduction to Number Theory*. Kluwer Academic Publishers, Dordrecht, 1995.

4

Ισοδυναμίες

4.1 Εισαγωγή (Ορισμός και πρώτες ιδιότητες)

Είδαμε μέχρι στιγμής ότι η διαιρετότητα παίζει σημαντικό ρόλο στη Θεωρία Αριθμών. Χάρη στο έργο των Euler, Lagrange, Legendre και Gauss, η Θεωρία Αριθμών αναγνωρίσθηκε ως κλάδος των Μαθηματικών και όχι ως μια συλλογή ενδιαφερόντων προβλημάτων.

Στα 1801 ο 24-ετής Gauss δημοσίευσε το μνημειώδες έργο του

"Disquistiones Arithmeticae" (Αριθμητικές Έρευνες).

Στο έργο του αυτό εισάγει, για πρώτη φορά, έναν εύχρηστο και δυναμικό συμβολισμό έκφρασης της διαιρετότητας, αυτόν της ισοδυναμίας (congruence).

Ορισμός. Αν a, b ακέραιοι αριθμοί και m φυσικός $m \geq 2$ τότε οι δύο ακέραιοι a και b θα λέγονται *ισοδύναμοι με μέτρο* m (ή ισοδύναμοι modulo m) όταν η διαφορά τους διαιρείται με m.

Ο Gauss αρχίζει το έργο του ως εξής:

«Si numerus a numeromur b, c defferentiam metitur b et c secundum a congrui dicuntur, sin minus incongrui: ipsum a modulum appelamus»

«Αν ο αριθμός a διαιρεί τη διαφορά των αριθμών b, c τότε τα b και c θα λέγονται ισοδύναμοι ως προς a, αλλιώς (θα λέγονται) μη-ισοδύναμοι το ίδιο το a θα το λέμε μέτρο.»

Στο δεύτερο άρθρο του (χρησιμοποιεί την αρίθμηση σε «άρθρα»), αναφέρει:

«numero congruentiam hoc signo, ≡, in postero denotabimus, modulum ubi opus erit in clausulis adiungentes»

«Την ισοδυναμία αριθμών τη συμβολίζουμε με ≡, αν είναι αναγκαίο επισυνάπτουμε το μέτρο σε παρένθεση»

Επομένως $a \equiv b$ modm, σημαίνει $m|(a-b)$.

Σε υποσημείωση του δεύτερου άρθρου του προσθέτει:

«Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam invenitur adoptavimus»

«Έχουμε επιλέξει τον συμβολισμό αυτόν λόγω της υφιστάμενης μεγάλης ομοιότητας μεταξύ ισότητας και ισοδυναμίας.»

Είναι λοιπόν πολύ εύχρηστος συμβολισμός και προσομοιάζει τη θεωρία της διαιρετότητας μ' αυτήν των εξισώσεων.

Στη συνέχεια ο Gauss αναπτύσσει μια πλούσια θεωρία των ισοδυναμιών η οποία αποτελεί συστατικό στοιχείο της θεωρίας αριθμών μέχρι σήμερα.

"...Μια από τις σημαντικότερες ανακαλύψεις των νεανικών χρόνων του Gauss, υπήρξε και ο ωρολογιακός υπολογιστής. Ήταν περισσότερο μια ιδέα παρά αληθινή μηχανή, που έδινε τη δυνατότητα των πράξεων με αριθμούς οι οποίοι στο παρελθόν είχαν χαρακτηριστεί ιδιαιτέρως δύσχρηστοι. Ο ωρολογιακός υπολογιστής δουλεύει ακριβώς με την ίδια αρχή που ακολουθεί κι ένα συμβατικό ρολόι. Αν ένα ρολόι δείχνει 9 και προσθέσουμε 4 ώρες, ο ωροδείκτης θα μετακινηθεί και θα δείχνει 1. Συνεπώς, ο ωρολογιακός υπολογιστής του Gauss θα έδινε την απάντηση 1 αντί για την απάντηση 13. Αν ο Gauss επιθυμούσε να κάνει πιο περίπλοκους υπολογισμούς, όπως το 7×7, ο ωρολογιακός υπολογιστής θα έδινε ως αποτέλεσμα το υπόλοιπο της διαίρεσης του $49(= 7 \times 7)$ δια 12. Δηλαδή, το αποτέλεσμα θα ήταν και πάλι 1.

Η ισχύς και η ταχύτητα του ωρολογιακού υπολογιστή του Gauss φαίνεται όταν θέλουμε να υπολογίσουμε την τιμή $7 \times 7 \times 7$. Αντί να πολλαπλασιάσουμε ξανά το 49 επί 7, θα πολλαπλασιάσουμε το αποτέλεσμα της τελευταίας πράξης ($7 \times 7 : 12$, που ήταν 1) επί 7, και θα βρούμε 7. Έτσι, χωρίς να χρειαστεί να υπολογίσουμε το $7 \times 7 \times 7$ (που παρεμπιπτόντως κάνει 343), με πολύ μικρότερη προσπάθεια βρίσκουμε ότι το υπόλοιπο της διαίρεσης του διά 12, είναι 7. Ο ωρολογιακός υπολογιστής άρχισε να αποδίδει καρπούς όταν ο Gauss προχώρησε στη διερεύνηση αριθμών τόσο μεγάλων, που ήταν πέρα από τις υπολογιστικές του δυνάμεις. Αν και δεν είχε την παραμικρή ιδέα πόσο κάνει 7^{99}, ο ωρολογιακός υπολογιστής του τον πληροφορούσε ότι το υπόλοιπο της διαίρεσής του δια 12 είναι 7.

Ο Gauss συνειδητοποίησε ότι τα ρολόγια με δώδεκα ώρες στο καντράν τους, δεν έχουν τίποτα το ιδιαίτερο. Εισήγαγε την ιδέα της ωρολογιακής αριθμητικής (που συχνά αποκαλείται αριθμητική των υπολοίπων - modular arithmetic) με οποιονδήποτε αριθμό ωρών στο καντράν. Έτσι, για παράδειγμα, ο αριθμός 11 σ' έναν ωρολογιακό υπολογιστή χωρισμένο σε 4 ώρες ισούται με 3, αφού το υπόλοιπο της διαίρεσης του 11 δια 4 είναι 3. Η εισαγωγή αυτού του νέου τύπου αριθμητικής στο γύρισμα του δέκατου ένατου αιώνα επέφερε επαναστατικές αλλαγές στα Μαθηματικά. Ακριβώς, όπως το τηλεσκόπιο έδωσε στους αστρονόμους τη δυνατότητα να παρατηρήσουν νέους κόσμους, η ανάπτυξη του ωρολογιακού υπολογιστή βοήθησε τους μαθηματικούς να ανακαλύψουν στον κόσμο των αριθμών νέες κανονικότητες, που παρέμεναν μέχρι τότε στο σκοτάδι. Ακόμα και σήμερα τα ρολόγια του Gauss παίζουν κεντρικό ρόλο στην ασφάλεια του διαδικτύου το οποίο χρησιμοποιεί ωρολογιακούς υπολογιστές που φέρουν στο καντράν τους περισσότερες ώρες από όσα άτομα περιλαμβάνει ολόκληρο το παρατηρήσιμο σύμπαν..." [19, σελ. 40-41].

Αν, σύμφωνα με το θεώρημα 1.2.3, γράψουμε τον ακέραιο a στη μορφή $a = mq + r$, $0 \leq r < m$ τότε είναι φανερό ότι $a \equiv r \bmod m$.

Ορισμός 4.1.1. Ο r θα λέγεται *ελάχιστο* υπόλοιπο του $a \bmod m$.

Έυκολα προκύπτει ότι δύο ακέραιοι a, b είναι ισοδύναμα ως προς το μέτρο m, ακριβώς τότε όταν έχουν το ίδιο ελάχιστο υπόλοιπο $\bmod m$. Πράγματι αν

$$a = qm + r, \ 0 \leq r < m$$

και

$$b = q'm + r', \ 0 \leq r' < m$$

τότε $a \equiv b \bmod m$ τότε και μόνο τότε όταν $m|a - b = (q - q')m + r - r'$, δηλαδή ακριβώς τότε όταν $m|(r - r')$. Επειδή $0 \leq |r - r'| < m$, η τελευταία σχέση ισχύει ακριβώς τότε όταν $r = r'$.

Επίσης, η σχέση «≡» στο σύνολο των ακέραιων είναι μια σχέση ισοδυναμίας. Αυτό σημαίνει ότι ισχύουν οι τρεις παρακάτω ιδιότητες.

Το m είναι, όπως παραπάνω, φυσικός αριθμός, $m \geq 2$, $a, b, c \in \mathbb{Z}$.

1. $a \equiv a \bmod m$, για κάθε ακέραιο a.

2. Αν $a \equiv b \mathrm{mod} m$, τότε και $b \equiv a \mathrm{mod} m$.

3. Αν $a \equiv b \mathrm{mod} m$ και $b \equiv c \mathrm{mod} m$, τότε $a \equiv c \mathrm{mod} m$

(Η απόδειξη αφήνεται ως άσκηση στον αναγνώστη).

Επομένως, το σύνολο των ακέραιων διαμερίζεται σε *κλάσεις* ισοδυναμίας. Το πλήθος των κλάσεων είναι όσα και τα δυνατά ελάχιστα υπόλοιπα $\mathrm{mod} m$. Επειδή αυτά είναι τα $0, 1, 2, \ldots, (m-1)$, έπεται ότι το σύνολο των ακέραιων διαμερίζεται σε ακριβώς m κλάσεις. Η κλάση του αριθμού a, συμβολίζεται

$$k_a := \{b \in \mathbb{Z} / b \equiv a \mathrm{mod} m\}.$$

Ορισμός. Το σύνολο $\{0, 1, \ldots, m-1\}$ θα λέγεται *ελάχιστο πλήρες σύστημα αντιπροσώπων των κλάσεων υπολοίπων* $\mathrm{mod} m$ και θα το συμβολίζουμε ως $\mathcal{S}(m)$

Στη συνέχεια θα αποδείξουμε μερικές βασικές ιδιότητες των ισοδυναμιών.

Πρόταση 4.1.2. *Αν a_i, $b_i (i \in \{1, 2, \ldots, n\})$ ακέραιοι και $a_i \equiv b_i \mathrm{mod} m$, για $i = 1, 2, \ldots, n$ τότε*

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \mathrm{mod} m$$

και

$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \mathrm{mod} m$$

Απόδειξη. Η υπόθεση ($a_i \equiv b_i \mathrm{mod} m$ για κάθε $i = 1, 2, \ldots, n$) είναι ισοδύναμη με $(m | (a_i - b_i)$, για κάθε $i = 1, 2, \ldots, n)$. Επομένως, υπάρχουν ακέραιοι ℓ_i, $i = 1, 2, \ldots, n$ τέτοιοι ώστε

$$a_i - b_i = m\ell_i \text{ για κάθε } i = 1, 2, \ldots, n.$$

Συνεπώς

$$\begin{aligned} \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i &= \sum_{i=1}^{n} (a_i - b_i) \\ &= \sum_{i=1}^{n} m\ell_i = m\left(\sum_{i=1}^{n} \ell_i\right) \end{aligned}$$

δηλαδή

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \mathrm{mod} m$$

Η απόδειξη θα γίνει επαγωγικά.

Για $n = 1$ προφανώς ισχύει. Υποθέτουμε ότι ισχύει για n, δηλαδή ότι

$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \mathrm{mod} m$$

Θα αποδείξουμε ότι ισχύει και για $n+1$. Έστω λοιπόν ότι

$$a_i \equiv b_i \mathrm{mod} m \text{ για } i = 1, 2, \ldots, n+1$$

Απο την υπόθεση της μαθηματικής επαγωγής έχουμε

$$\prod_{i=1}^{n} a_i - \prod_{i=1}^{n} b_i = m\ell \text{ για κάποιο } \ell \in \mathbb{Z}.$$

Συνεπώς

$$\begin{aligned}\prod_{i=1}^{n+1} a_i - \prod_{i=1}^{n+1} b_i &= \prod_{i=1}^{n+1} a_i - b_{n+1}\prod_{i=1}^{n} a_i + b_{n+1}\prod_{i=1}^{n} a_i - \prod_{i=1}^{n+1} b_i \\ &= (a_{n+1} - b_{n+1})\prod_{i=1}^{n} a_i + b_{n+1}\left(\prod_{i=1}^{n} a_i - \prod_{i=1}^{n} b_i\right) \\ &= mk + m\ell b_{n+1} = m(k + \ell b_{n+1}),\end{aligned}$$

δηλαδή ισχύει και για $n+1$ και συνεπώς για κάθε φυσικό n, $n \geq 1$. □

Άμεση συνέπεια της πρότασης 4.1.2 είναι το ακόλουθο:

Πόρισμα 4.1.3. *Έστω m φυσικός, $m \geq 2$, $a, b, c \in \mathbb{Z}$ και $n \in \mathbb{Z}$. Αν $a \equiv b \bmod m$ τότε*

1. $a \pm c \equiv b \pm c \bmod m$
2. $ac \equiv bc \bmod m$
3. $a^n \equiv b^n \bmod m$

Από τα παραπάνω προκύπτει ότι μπορούμε να προσθαφαιρούμε και να πολλαπλασιάζουμε ισοδυναμίες άφοβα.

Τι γίνεται όμως με τη δυνατότητα απλοποίησης; Το ότι αυτό δεν είναι πάντοτε σωστό προκύπτει αμέσως από το εξής αντιπαράδειγμα:

$$2 \cdot 6 \equiv 2 \cdot 3 \bmod 6$$

ενώ $6 \not\equiv 3 \bmod 6$. Ισχύει όμως η

Πρόταση 4.1.4. *Αν $ac \equiv bc \bmod m$ τότε*

$$a \equiv b \bmod \frac{m}{d},$$

όπου $d = (c, m)$.

Απόδειξη. Αφού $ac \equiv bc \bmod m$, έπεται ότι υπάρχει $\ell \in \mathbb{Z}$ τέτοιο ώστε

$$(a - b)c = ac - bc = m\ell.$$

Διαιρούμε και τα δύο μέλη με d και έχουμε

$$\frac{(a-d)c}{d} = \frac{m\ell}{d}.$$

Αν $m = dM$ και $c = dC$ ($M, C \in \mathbb{Z}$) τότε η παραπάνω ισότητα γράφεται

$$(a - b)C = M\ell.$$

Επειδή $(M, C) = 1$, έπεται ότι $M \mid (a - b)$ δηλαδή ότι

$$a \equiv b \bmod \frac{m}{d}.$$

□

Πόρισμα 4.1.5. *Αν* $ac = bc \bmod m$ *και* $(c, m) = 1$ *τότε*

$$a \equiv b \bmod m$$

Απόδειξη. Άμεση συνέπεια της πρότασης 4.1.4. □

Φυσικά αν $c \neq 0$ και $ac \equiv bc \bmod mc$ τότε $a \equiv b \bmod m$. Αυτό γιατί από $ac \equiv bc \bmod mc$, έπεται ότι υπάρχει $\ell \in \mathbb{Z}$ ώστε $ac - bc = (m\ell)c$ άρα $(a - b - ml)c = 0$ και αφού $c \neq 0$ καταλήγουμε στο $a \equiv b \bmod m$.

4.2 Το (μικρό) θεώρημα του Fermat, η φ-συνάρτηση και το θεώρημα του Euler

Προσπαθούμε να βρούμε έναν τρόπο να υπολογίζουμε δυνάμεις ακέραιων ως προς κάποιο μέτρο m, όπου m φυσικός $m > 1$.

Για λόγους ευκολίας, θα περιοριστούμε στην περίπτωση που ο m είναι πρώτος αριθμός, $m = p \in \mathbb{P}$. Θα ξεκινήσουμε με ένα παράδειγμα. Ας πάρουμε $p = 5$. Για $a = 1, 2, 3, 4$ υπολογίζουμε τις δυνάμεις modulo 5.

Αν $a = 1$, όλες οι δυνάμεις είναι ισοδύναμες με το $1 \bmod 5$.
Αν $a = 2$, $a^2 \equiv 4 \bmod 5$, $a^3 \equiv 3 \bmod 5$, $a^4 \equiv 1 \bmod 5$
Αν $a = 3$, $a^2 \equiv 4 \bmod 5$, $a^3 \equiv 2 \bmod 5$, $a^4 \equiv 1 \bmod 5$
Αν $a = 4$, $a^2 \equiv 1 \bmod 5$, $a^3 \equiv 4 \bmod 5$, $a^4 \equiv 1 \bmod 5$
Παρατηρούμε ότι για κάθε a, $1 \leq a < 5$ ισχύει

$$a^4 \equiv 1 \bmod 5$$

Αν θεωρήσουμε τώρα την περίπτωση $p = 11$, εύκολα μπορούμε να διαπιστώσουμε ότι για κάθε a, $1 \leq a < 11$, ισχύει

$$a^{10} \equiv 1 \bmod 11$$

Παρατήρηση 4.2.1.

1. Ο περιορισμός των τιμών του a δεν βλάπτει τη γενικότητα (διότι αν $a_1 \equiv a_2 \bmod p$ τότε $a_1^n \equiv a_2^n \bmod p$ για κάθε $n \in \mathbb{N}$)
2. Αν $a \equiv 0 \bmod p$, τότε $a^n \equiv 0 \bmod p$

Το ερώτημα αν η ισοδυναμία ισχύει γενικά, για κάθε πρώτο αριθμό p, δέχεται καταφατική απάντηση.

Πρόταση 4.2.2 (Μικρό θεώρημα του Fermat)**.** *Για κάθε πρώτο* p *και κάθε ακέραιο* a *για τον οποίο* $p \nmid a$*, ισχύει*

$$a^{p-1} \equiv 1 \bmod p$$

Πόρισμα 4.2.3. *Για κάθε πρώτο* p *και κάθε ακέραιο* a*, ισχύει*

$$a^p \equiv a \bmod p$$

Απόδειξη του πορίσματος:

Αν $p \nmid a$ τότε, λόγω της πρότασης 4.2.2, έχουμε

$$a^{p-1} \equiv 1 \mathrm{mod} p$$

Πολλαπλασιάζουμε την ισοδυναμία με a και έχουμε

$$a^p \equiv a(\mathrm{mod} p)$$

Αν $p|a$ τότε $a \equiv 0(modp)$ και $a^p \equiv 0(modp)$, δηλαδή και πάλι $a^p \equiv a \mathrm{mod} p$.

Παρατήρηση 4.2.4. Αν δεχθούμε την αλήθεια του πορίσματος 4.2.3 μπορούμε να συμπεράνουμε την αλήθεια της πρότασης 4.2.2

Πράγματι, αν $a^p \equiv a \mathrm{mod} p$ και $p \nmid a$, λόγω πορίσματος 4.2.3 έχουμε $a^{p-1} \equiv 1 \mathrm{mod} p$. Αν επομένως δώσουμε μια ανεξάρτητη της πρότασης απόδειξη του πορίσματος θα έχουμε αποδείξει και το μικρό θεώρημα του Fermat.

Απόδειξη. Η απόδειξη θα γίνει επαγωγικά.

Για $a = 0$, ισχύει.

Υποθέτουμε ότι ισχύει για τον φυσικό $a \geq 0$, δηλαδή ότι

$$a^p \equiv a \mathrm{mod} p$$

Θα αποδείξουμε ότι ισχύει και για $(a + 1)$.

Πράγματι

$$(a+1)^p = \sum_{j=0}^{p} \binom{p}{j} a^j$$

και επειδή $p|\binom{p}{j}, \forall j = 1, 2, \ldots, (p-1)$, $(a+1)^p \equiv a + 1 \mathrm{mod} p$ (**Άσκηση**.)

Η απόδειξη της ισοδυναμίας για ένα πλήρες σύστημα αντιπροσώπων $modp$ συνεπάγεται την ισχύ της για κάθε ακέραιο a □

Στη συνέχεια θα δώσουμε και μία απόδειξη της πρότασης 4.2.2. Ας δούμε την ιδέα της σε ένα παράδειγμα.

Για να αποδείξουμε ότι $5^{12} \equiv 1 \mathrm{mod} 13$ σχηματίζουμε τον πίνακα.

$a \mathrm{mod} 13$	1	2	3	4	5	6	7	8	9	10	11	12
$5a \mathrm{mod} 13$	5	10	2	7	12	4	9	1	6	11	3	8

Παρατηρούμε ότι οι αριθμοί από 1 έως 13 εμφανίζονται ακριβώς μια φορά και στη δεύτερη γραμμή, με διαφορετική φυσικά σειρά.

Αν λοιπόν πολλαπλασιάσουμε όλους τους αριθμούς της δεύτερης σειράς έχουμε:

$(5 \cdot 1)(5 \cdot 2) \ldots (5 \cdot 12) \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 12 \mathrm{mod} 13$,

δηλαδή $5^{12} \cdot 12! \equiv 12! \mathrm{mod} 13$

Επειδή $(12!, 13) = 1$, έχουμε $5^{12} \equiv 1 \mathrm{mod} 13$

Απόδειξη. Απόδειξη της πρότασης 4.2.2. Οι αριθμοί $a, 2a, \ldots, (p-1)a \mathrm{mod} p$ είναι οι ίδιοι με τους

$$1, 2, \ldots, (p-1) \mathrm{mod} p$$

με πιθανόν διαφορετική σειρά.

Πράγματι το πλήθος τους είναι $(p-1)$, κανείς τους δεν διαιρείται με p και αν $ka \equiv la \mathrm{mod} p$ για $k, l \in \{1, 2, \ldots, (p-1)\}$, έχουμε $p|a(k-l)$. Επειδή $p \nmid a$, έπεται ότι $p|(k-l)$, δηλαδή $k \equiv l \mathrm{mod} p$. Όμως $1 \leq k, l \leq p-1$. Επομένως $|k-l| < p-1$. Συνεπώς $k-l=0$, δηλαδή $k=l$. Αποδείξαμε ότι οι αριθμοί είναι $(p-1)$ διαφορετικοί μεταξύ τους και διάφοροι του μηδενός $\mathrm{mod} p$. Συνεπώς ταυτίζονται με τους $1, 2, \ldots, (p-1) \mathrm{mod} p$, με διαφορετική ίσως σειρά.

Από τα παραπάνω συμπεραίνουμε ότι $a \cdot (2a) \ldots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \mathrm{mod} p$ και, ισοδύναμα, ότι $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mathrm{mod} p$

Είναι φανερό ότι $p \nmid (p-1)!$.

Τελικά ισχύει $a^{p-1} \equiv 1 \mathrm{mod} p$ □

Παράδειγμα. Να αποδειχθεί ότι $7|111^{333} + 333^{111}$.

Εφαρμόζουμε το μικρό θεώρημα του Fermat. Ο $p=7$ είναι πρώτος και $7 \nmid 111$ καθώς και $7 \nmid 333$. Επομένως, $111^6 \equiv 1 \mathrm{mod} 7$ και $333^6 \equiv 1 \mathrm{mod} 7$. Το $333 = 6 \cdot 55 + 3$ και το $111 = 6 \cdot 18 + 3$.

Συνεπώς $111^{333} = 111^{6 \cdot 55+3} = (111^6)^{55} \cdot 111^3 \equiv 1^5 \cdot 111^3 = 111^3 \mathrm{mod} 7$ και, επειδή $111 = 7 \cdot 15 + 6$, $111^3 \equiv 6^3 \mathrm{mod} 7 \equiv (-1)^3 \equiv (-1) \equiv 6 \mathrm{mod} 7$

Επίσης $333^{111} = 333^{6 \cdot 18+3} = (333^6)^{18} \cdot 333^3 \equiv 1^{18} \cdot 333^3 \equiv 333^3 \mathrm{mod} 7$ και επειδή $333 = 7 \cdot 47 + 4$, $333^3 \equiv 4^3 \equiv 1 \mathrm{mod} 7$.

Προσθέτοντας κατά μέλη τις δύο ισοδυναμίες προκύπτει

$111^{333} + 333^{111} \equiv 6 + 1 \equiv 0 \mathrm{mod} 7$, δηλαδή ότι $7|111^{333} + 333^{111}$.

Παράδειγμα. Να υπολογιστεί το υπόλοιπο της διαίρεσης του αριθμού 2^{160677} με 73.

Το 73 είναι πρώτος. Από το θεώρημα του Fermat έπεται ότι $2^{72} \equiv 1 \mathrm{mod} 73$, $(2, 73) = 1$. Ο εκθέτης γράφεται στη μορφή

$$160677 = 72 \cdot 2231 + 45.$$

Συνεπώς $2^{160677} \equiv 2^{45} \mathrm{mod} 73$. Ένας εύκολος τρόπος για να υπολογίσουμε την τελευταία δύναμη είναι να γράψουμε το 45 στη δυαδική του μορφή.

$$45 = (101101)_2 \quad (= 2^5 + 2^3 + 2^2 + 1 = 32 + 8 + 4 + 1).$$

Γραφουμε $2^1 \equiv 2 \mathrm{mod} 73$ και υψώνουμε κάθε φορά και τα δύο μέλη της ισοδυναμίας στο τετράγωνο:

$$\begin{aligned} 2^1 &\equiv 2 \mathrm{mod} 73 \\ 2^2 &\equiv 4 \mathrm{mod} 73 \\ 2^4 &\equiv 16 \mathrm{mod} 73 \\ 2^8 &\equiv 37 \mathrm{mod} 73 \\ 2^{16} &\equiv 55 \mathrm{mod} 73 \\ 2^{32} &\equiv 32 \mathrm{mod} 73 \end{aligned}$$

Επομένως, $2^{45} \equiv 2^{32+8+4+1} \equiv 2^{32} \cdot 2^8 \cdot 2^4 \cdot 2 \equiv 32 \cdot 37 \cdot 16 \cdot 2 = 74 \cdot 32 \cdot 16 \equiv 1 \cdot 512 \equiv 1 \mathrm{mod} 73$

Το πρόγραμμα sage μας δίνει τη δυνατότητα να κάνουμε πράξεις με ισοδυναμίες mod73:

```
for i in range(1,6):
    i,2^(2^i), Mod(2^(2^i),73)

(1, 4, 4)
(2, 16, 16)
```

(3, 256, 37)
(4, 65536, 55)
(5, 4294967296, 32)

Στη δεύτερη στήλη εμφανίζεται η τιμή 2^{2^i} ως ακέραιος αριθμός, ενώ στην τρίτη στήλη η τιμή της mod73.

Ας θεωρήσουμε τώρα τη γενική περίπτωση όπου m φυσικός, $m > 1$. Είναι σαφές ότι το μικρό θεώρημα του Fermat δεν ισχύει για m σύνθετο.

Παράδειγμα: $2^{11} \equiv 8 \mathrm{mod} 12$

Το ερώτημα λοιπόν είναι αν, δοθέντος του m και κάποιου ακέραιου a, υπάρχει εκθέτης του a, έστω s, τέτοιος ώστε $a^s \equiv 1 \mathrm{mod} m$. Το παραπάνω παράδειγμα μας δείχνει ότι αυτό δεν είναι πάντοτε δυνατό.

Αν κάποια δύναμη του a, $a^s \equiv 1 \mathrm{mod} m$ τότε $a^s - km = 1$, για κάποιο $k \in \mathbb{Z}$, δηλαδή $(a, m) = 1$. Όταν $m = p$, τότε για κάθε $a \in \mathbb{Z}$ με $p \nmid a$ έχουμε $(a, p) = 1$. Δηλαδή όλες οι κλάσεις $a \mathrm{mod} p$ με $a = 1, 2, \ldots, p-1$ είναι υποψήφιες.

Για m τυχαίο φυσικό, $m > 1$, θα πρέπει να αναζητήσουμε ακέραιους a για τους οποίους $(a, m) = 1$, δηλαδή στο σύνολο

$$\{a \in \mathbb{Z} | 1 \leq a < m \text{ και } (a, m) = 1\}$$

Το σύνολο αυτό για $m = p \in \mathbb{P}$ έχει $(p-1)$ στοιχεία και ο αριθμός αυτός έπαιξε κάποιο ρόλο στο μικρό θεώρημα του Fermat.

Είναι λοιπόν φυσικό να ορίσουμε τον αριθμό

$$\varphi(m) := \#\{a \in \mathbb{Z} | 1 \leq a < m \text{ και } (a, m) = 1\}$$

Έτσι ορίσαμε μια συνάρτηση για κάθε φυσικό αριθμό m.

Ορισμός 4.2.5. Η συνάρτηση αυτή λέγεται η φ-συνάρτηση του Euler . Ας δούμε μερικές τιμές της.

Αν $p \in \mathbb{P}$, $\varphi(p) = p - 1$. Επομένως $\varphi(2) = 1$, $\varphi(3) = 2$. Επίσης $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(9) = 6$, $\varphi(10) = 4$, $\varphi(12) = 4$.

Μία κλάση $a \mathrm{mod} m$ *θα λέγεται πρώτη κλάση υπολοίπων* $\mathrm{mod} m$ *όταν ο* $(a, m) = 1$

Το σύνολο όλων των πρώτων κλάσεων υπολοίπων $\mathrm{mod} m$, να λέγεται *πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων* υπολοίπων $\mathrm{mod} m$ με $\mathcal{R}(m)$. Θα συμβολίζουμε το σύνολο $\mathcal{R}(m) = \{a \in \mathcal{S}(m) | (a, m) = 1\}$

Πρόταση 4.2.6. *Αν* $\{a_1, a_2, \ldots a_{\varphi(m)}\}$ *ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων* $\mathrm{mod} m$ *και* $b \in \mathbb{Z}$ *τέτοιο ώστε* $(b, m) = 1$ *τότε και το σύνολο* $\{ba_1, ba_2, \ldots, ba_{\varphi(m)}\}$ *είναι επίσης πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων* $\mathrm{mod} m$.

Απόδειξη. Επειδή $(a_i, m) = 1$ και $(b, m) = 1$, έπεται ότι $(ba_i, m) = 1$, δηλαδή ότι οι κλάσεις των αντιπροσώπων ba_i είναι πρώτες κλάσεις. Αρκεί να αποδείξουμε ότι είναι μεταξύ τους ανά δύο διαφορετικές.

Έστω $ba_i \equiv ba_j \mathrm{mod} m$. Συνεπώς $m | b(a_i - a_j)$ και επειδή $(b, m) = 1$ έπεται ότι $m | (a_i - a_j)$, δηλαδή ότι $a_i \equiv a_j \mathrm{mod} m$. Η τελευταία ισοδυναμία ισχύει μόνο για $i = j$. □

Άμεση συνέπεια της πρότασης 4.2.6 είναι το:

Πρόταση 4.2.7 (Euler). *Για κάθε ακέραιο a με $(a, m) = 1$ ισχύει*

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Απόδειξη. Η απόδειξη είναι ανάλογη αυτής του μικρού θεωρήματος του Fermat.

Πράγματι, λόγω της πρότασης 4.2.6 έπεται ότι

$$\{a_1 \bmod m,\ a_2 \bmod m, \ldots, a_{\varphi(m)} \bmod m\} =$$

$$= \{aa_1 \bmod m,\ aa_2 \bmod m,\ \ldots\ , aa_{\varphi(m)} \bmod m\}$$

Επομένως,

$$(aa_1)(aa_2)\ldots(aa_{\varphi(m)}) \equiv a_1 a_2 \ldots a_{\varphi(m)} \bmod m$$

Συνεπώς $a^{\varphi(m)} \cdot (a_1 a_2 \cdots a_{\varphi(m)}) \equiv a_1 a_2 \cdots a_{\varphi(m)} \bmod m$

Η υπόθεση $(a_i, m) = 1$, για κάθε $i = 1, 2, \ldots \varphi(m)$ μας δίνει

$$(a_1 a_2 \ldots a_{\varphi(m)},\ m) = 1$$

οπότε από την παραπάνω ισοδυναμία προκύπτει

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

□

Παρατήρηση 4.2.8.

1. Επειδή για $m = p \in \mathbb{P}$, $\varphi(m) = p - 1$, το θεώρημα του Fermat προκύπτει ως ειδική περίπτωση του θεωρήματος του Euler.

2. Μία γενίκευση του θεωρήματος του Euler αποτελεί το ακόλουθο αποτέλεσμα του L. Redei (1948): Για κάθε φυσικό αριθμό $m > 1$ και οποιονδήποτε ακέραιο a ισχύει:

   $$m | (a^m - a^{m-\varphi(m)}).$$

   Εύκολα διαπιστώνεται ότι το θεώρημα του Euler αποτελεί ειδική περίπτωση του θεωρήματος του L. Redei. Πράγματι, $m | a^{m-\varphi(m)}(a^{\varphi(m)} - 1)$. Επειδή $(a, m) = 1$ έπεται ότι $(a^{m-\varphi(m)}, m) = 1$. Συνεπώς $m | (a^{\varphi(m)} - 1)$, δηλαδή το θεώρημα του Euler. Θα πρέπει όμως να επισημάνουμε ότι στην απόδειξη του θεωρήματος του Redei, γίνεται χρήση του θεωρήματος του Euler. Δεν μας είναι γνωστή απόδειξη ανεξάρτητη της χρήσης του θεωρήματος του Euler.

Παράδειγμα. 3^{100}.

Θα πρέπει να υπολογίσουμε το ελάχιστο θετικό υπόλοιπο του $3^{100} \bmod 100$.

Γράφουμε και πάλι το 100 στο 2-αδικό σύστημα

$$100 = (1100100) = 2^6 + 2^5 + 2^2$$

$3^{100} = 3^{2^6+2^5+2^2} = 3^{2^6} \cdot 3^{2^5} \cdot 3^{2^4} = 3^{64} \cdot 3^{32} \cdot 3^4$

$3^1 \equiv 3 \bmod 100$

$3^2 \equiv 9 \bmod 100$

$3^4 \equiv 81 \bmod 100$

$3^8 \equiv 61 \bmod 100$

$3^{16} \equiv 21 \bmod 100$

$3^{32} \equiv 41 \bmod 100$

$3^{64} \equiv 81 \mathrm{mod} 100$

Επομένως $3^{100} \equiv 81 \cdot 41 \cdot 81 \mathrm{mod} 100 \equiv 21 \cdot 81 \mathrm{mod} 100 \equiv 01 \mathrm{mod} 100$.

Άρα τα δύο τελευταία ψηφία του αριθμού είναι 01. Αν βέβαια ήταν εύκολο να υπολογίσουμε το $\varphi(100)$, θα ήταν σίγουρα πολύ πιο εύκολος ο υπολογισμός. Το πρόβλημά μας λοιπόν είναι ο υπολογισμός του $\varphi(m)$, όταν γνωρίζουμε φυσικά το m.

Σε λίγο θα αποδείξουμε ότι $\varphi(100) = 40$.

Συνεπώς $3^{100} \equiv 3^{20} \equiv 21 \cdot 81 \equiv 01 \mathrm{mod} 100$.

Ο υπολογισμός είναι σχετικά εύκολος όταν το m είναι δύναμη του p, έστω $m = p^l$. Οι ακέραιοι a, $1 \leq a < m$, οι οποίοι *δεν* είναι πρώτοι προς τον p είναι οι

$$p,\ 2p,\ 3p, \ldots,\ (p^{l-1}-2)p,\ (p^{l-1}-1)p,\ p^l$$

δηλαδή σε πλήθος p^{l-1}.

Επομένως $\varphi(p^l) = p^l - p^{l-1}$

Μερικά παραδείγματα: $\varphi(6) = 2$, $\varphi(2) = 1$, $\varphi(3) = 2$. Επομένως $\varphi(6) = \varphi(2)\varphi(3)$. Επίσης $\varphi(12) = 4$ και $\varphi(3)\varphi(4) = 2 \cdot 2 = 4$, δηλαδή και πάλι $\varphi(12) = \varphi(3)\varphi(4)$. Όμως $\varphi(12) = 4 \neq \varphi(2)\varphi(6) = 1 \cdot 2 = 2$.

Από τα παραπάνω, και άλλα παραδείγματα που μπορεί να υπολογίσει ο ενδιαφερόμενος αναγνώστης, μπορούμε ίσως να διατυπώσουμε την εικασία:

Πρόταση 4.2.9.

αν $(m, n) = 1$ *τότε* $\varphi(m \cdot n) = \varphi(m)\varphi(n)$.

Πράγματι, η εικασία μας ισχύει. Θα δώσουμε στην πορεία διάφορες αποδείξεις.

Η ιδέα της πρώτης απόδειξης θα δοθεί με ένα παράδειγμα.

Έστω $m = 5$ και $n = 8$, $m \cdot n = 5 \cdot 8 = 40$. Θα σχηματίσουμε ένα ορθογώνιο παραλληλόγραμμο με τους φυσικούς από 1 έως 40 διατεταγμένους σε γραμμές και στήλες ως εξής:

1	6	*11*	16	*21*	26	*31*	36
2	*7*	12	*17*	22	*27*	32	*37*
3	8	*13*	18	*23*	28	*33*	38
4	*9*	14	*19*	24	*29*	34	*39*
5	10	15	20	25	30	35	40

Το $\varphi(5) = 5 - 1 = 4$. Υπάρχουν ακριβώς 4 γραμμές που περιέχουν ακέραιους πρώτους προς το 5, οι τέσσερις πρώτες. Το $\varphi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$. Σε κάθε μια απο τις τέσσερις γραμμές υπάρχουν ακριβώς 4 αριθμοί οι οποίοι είναι πρώτοι προς το 8. Συνεπώς υπάρχουν $4 \cdot 4 = 16$ φυσικά, πρώτοι προς το 40, $\varphi(40) = 16 = 4 \cdot 4 = \varphi(5)\varphi(8)$.

Απόδειξη της πρότασης 4.2.9

Τοποθετούμε τους φυσικούς από 1 έως $m \cdot n$ κατά το ακόλουθο σχήμα:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \ldots & (n-1)m+3 \\
\vdots & \vdots & & & \\
r & m+r & 2m+r & \ldots & (n-1)m+r \\
\vdots & \vdots & & & \\
m & 2m & 3m & & (n-1)m+m = m \cdot n
\end{array}$$

Υποθέτουμε ότι ο $(m, r) =: d > 1$. Κανένα στοιχείο της r-στης γραμμής δεν είναι πρώτο προς το m, αφού είναι της μορφής

$$km + r \text{ όπου } 0 \leq k \leq n-1$$

και $d|(km + r)$.

Επομένως οι φυσικοί από 1 έως $m \cdot n$ που είναι πρώτοι προς το m ανήκουν στις r-στες γραμμές για τις οποίες $(m, r) = 1$.

Αν τώρα $(m, r) = 1$ και $1 \leq r \leq m$ θα πρέπει τώρα να υπολογίσουμε πόσοι πρώτοι προς τον $m \cdot n$ υπάρχουν στην r-στη γραμμή.

Πρώτα από όλα είναι φανερό ότι όλοι οι όροι της r-στης γραμμής είναι πρώτοι προς το m.

$$(km + r, m) = (m, r) = 1.$$

Επίσης οι n φυσικοί της r-στης γραμμής αποτελούν ένα πλήρες σύστημα των κλάσεων υπολοίπων mod$n$. Επομένως ακριβώς $\varphi(n)$ από αυτούς είναι πρώτοι προς το n. Επειδή όλοι της γραμμής είναι πρώτοι προς το m, έπεται ότι η γραμμή περιέχει ακριβώς $\varphi(n)$ πρώτους το $m \cdot n$, και επειδή οι γραμμές είναι $\varphi(m)$ συνολικά οι πρώτοι προς το $m \cdot n$ είναι $\varphi(m) \cdot \varphi(n)$, δηλαδή

$$\varphi(m \cdot n) = \varphi(m)\varphi(n).$$

Πρόταση 4.2.10. *Αν $n = \prod_{i=1}^{s} p_i^{n_i}$ η κανονική ανάλυση του φυσικού n, $(n > 1)$ σε γινόμενο πρώτων παραγόντων τότε*

$$\varphi(n) = \prod_{i=1}^{s} p_i^{n_i - 1}(p_i - 1) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Απόδειξη. Ο

$$\left(\prod_{i=1}^{s-1} p_i^{n_i},\ p_s^{n_s}\right) = 1.$$

Συνεπώς,

$$\varphi(n) = \varphi\left(\prod_{i=1}^{s-1} p_i^{n_i}\right)\varphi\left(p_s^{n_s}\right)$$

και, επαγωγικά,

$$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{n_i})$$

Τέλος, από τη σχέση $\varphi(p_i^{n_i}) = p_i^{n_i} - p_i^{n_i - 1} = p_i^{n_i}\left(1 - \frac{1}{p_i}\right)$ έχουμε το ζητούμενο αποτέλεσμα. □

Πρόταση 4.2.11. *Για κάθε φυσικό αριθμό n, $n > 2$ ο $\varphi(n)$ είναι άρτιος.*

Απόδειξη. Ξεχωρίζουμε δύο περιπτώσεις:

1. Αν ο n είναι δύναμη του 2, $n = 2^l$ με $l > 1$ τότε $\varphi(n) = \varphi(2^l) = 2^{l-1}$, δηλαδή άρτιος.
2. Αν ο n δεν είναι δύναμη του 2, θα έχει κάποιο περιττό πρώτο διαιρέτη, έστω p. Επομένως ο n θα γράφεται στη μορφή $n = p^l \cdot m (l \geq 1)$ όπου $p \nmid m$.

   Επομένως $\varphi(n) = \varphi(p^l)\varphi(m) = p^{l-1}(p-1)\varphi(m)$.

   Ο $(p-1)$ είναι άρτιος διαιρέτης του $\varphi(n)$ συνεπώς ο $\varphi(n)$ είναι άρτιος.

□

Παρατήρηση 4.2.12. 1. Πιο μπροστά αναφερθήκαμε στον υπολογισμό του

$$\varphi(100) = \varphi\left(2^2 \cdot 5^2\right) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

2. Ο Fermat ανακοίνωσε το αποτέλεσμα που φέρει το όνομά του σε ένα γράμμα του προς τον Frènicle de Bessy με ημερομηνία 18 Οκτωβρίου 1640. Ονομάστηκε «μικρό θεώρημα του Fermat» (σε αντιδιαστολή με το «Θεώρημα του Fermat» ή «εικασία του Fermat» στο οποίο έχουμε αναφερθεί πιο πριν, το οποίο απολάμβανε τον τίτλο του θεωρήματος χωρίς να έχει αποδειχθεί).

   Φαίνεται ότι ο Fermat δεν το είχε αποδείξει. Στο γράμμα του προς τον Frènicle γράφει: «Θα σου έστελνα την απόδειξη αν δεν φοβόμουνα ότι θα ήταν ή θα γινόταν υπερβολικά μακροσκελής» («I would send you the demonstration, if I did not fear its being too long»).

   Κάπου μεταξύ 1676 και 1680 αποδείχτηκε από τον Leibniz, αλλά η απόδειξή του βρέθηκε πολύ αργότερα στα αδημοσίευτα χειρόγραφά του. Έτσι, χάθηκε η ευκαιρία να συνδεθεί το όνομά του με την απόδειξη του θεωρήματος.

   Η πρώτη δημοσιευμένη απόδειξη ήταν αυτή του Euler, περίπου έναν αιώνα αργότερα, το 1736. Η απόδειξή του στηρίζεται στον διωνυμικό τύπο. [4, σελ. 189].

   Η δεύτερη απόδειξη δόθηκε από τον Euler στα 1750 και η γενίκευσή της στα 1760 [4, σελ. 57].

   Χωρίς να χρησιμοποιήσει τον συμβολισμό $\varphi(n)$, ο Euler είναι ο πρώτος που εισάγει τη συνάρτηση αυτή. Αργότερα χρησιμοποιεί τον συμβολισμό $\pi(n)$. Πρώτος που χρησιμοποιεί τον συμβολισμό $\varphi(n)$ είναι ο Gauss [6, Άρθρο 38].

4.2.1 Ασκήσεις

1. Να αποδείξετε ότι για $n \in \mathbb{N}$, $n \geq 1$

$$5^n \equiv 1 + 4n \mathrm{mod} 16$$

2. Αν a, b θετικοί ακέραιοι και $(a, b) = 1$ να αποδείξετε ότι

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mathrm{mod} ab$$

3. Να αποδείξετε ότι το

$$7 \mid 1941^{1963} + 1963^{1991}$$

4. Ποια είναι τα δύο τελευταία ψηφία του 3^{1000};

5. Να αποδείξετε ότι για κάθε ακέραιο a ισχύει $2730 \mid a^{13} - a$.

6. Αν $n \in \mathbb{N}$, $n > 2$ τότε να αποδείξετε ότι το άθροισμα των φυσικών που είναι μικρότεροι του n και πρώτοι προς το n και πρώτοι προς το n είναι $\frac{n\varphi(n)}{2}$.

7. Να αποδείξετε ότι ο αριθμός
$$\frac{1}{5}a^5 + \frac{1}{3}a^3 + \frac{7}{15}a$$
είναι πάντοτε ακέραιος, για κάθε ακέραιο a.

8. Αν ο n είναι περιττός να αποδείξετε ότι
$$\varphi(2n) = \varphi(n).$$
Αν ο n είναι άρτιος να αποδείξετε ότι
$$\varphi(2n) = 2\varphi(n)$$
Να αποδείξετε ότι
$$\varphi(3n) = 3\varphi(n) \Leftrightarrow 3 \mid n$$

9. Αν $a \in \mathbb{Z}$ και $(a, 10) = 1$, τότε τα τελευταία τρία δεκαδικά ψηφία των a^{2001} και a σημπίπτουν.

4.3 Γραμμικές ισοδυναμίες και συστήματα

Αν $f(X) = c_nX^n + \cdots + c_2X + c$ πολυώνυμο (μίας μεταβλητής) n-στού βαθμού με ακέραιους συντελεστές και $m \in \mathbb{N}$, $m > 1$, τότε η ισοδυναμία
$$f(X) \equiv \mathrm{mod} m \tag{4.3.1}$$
θα λέγεται *ισοδυναμία* n-στού βαθμού.

Ο ακέραιος a θα λέγεται *λύση* της ισοδυναμίας όταν $f(a) \equiv 0 \mathrm{mod} m$.

Είναι εύκολο να αποδειχθεί ότι αν $a \equiv b \mathrm{mod} m$ τότε $f(a) \equiv f(b) \mathrm{mod} m$.

Απόδειξη. Από το Πόρισμα 4.1.3 προκύπτει ότι $a^l \equiv b^l \mathrm{mod} m$ για κάθε $l = 0, 1, 2, \ldots, n$.

Επομένως, πόρισμα 4.1.3(ii) και $c_la^l \equiv c_lb^l \mathrm{mod} m$ για κάθε $l = 0, 1, 2, \ldots, n$, οπότε Πρόταση 4.1.2 και $\sum_{l=0}^{n} c_la^l \equiv \sum_{l=0}^{n} c_lb^l \mathrm{mod} m$, δηλαδή $f(a) \equiv f(b) \mathrm{mod} m$. □

Επομένως αν a λύση της ισοδυναμίας (4.3.1), όλοι οι ακέραιοι b, $b \equiv a \mathrm{mod} m$ είναι επίσης λύση. Όλη η κλάση θα θεωρείται ως *μία* λύση. Άρα, δύο λύσεις a_1 και a_2 θα είναι διαφορετικές όταν $a_1 \not\equiv a_2 \mathrm{mod} m$.

Από τα παραπάνω προκύπτει ότι για να βρούμε όλες τις λύσεις θα πρέπει να ελέγξουμε ποιοι από τους αντιπροσώπους ενός πλήρους συστήματος αντιπροσώπων των κλάσεων υπολοίπων $\mathrm{mod} m$, επαληθεύουν την ισοδυναμία. Για παράδειγμα μπορούμε να θεωρήσουμε το σύστημα $\{0, 1, 2, \ldots, m-1\}$.

Μια ισοδυναμία θα λέγεται *ισοδυναμία πρώτου βαθμού* ή γραμμική , όταν $n = 1$. Μία γραμμική ισοδυναμία θα είναι, επομένως, της μορφής
$$ax \equiv b \mathrm{mod} m$$

Έχει πάντοτε μια γραμμική ισοδυναμία λύση (λύσεις);

Η απάντηση είναι όχι. Για παράδειγμα, η ισοδυναμία $3x \equiv 5 \mathrm{mod} 9$ δεν έχει λύση.

(Αν x_0 ήταν λύση, τότε θα είχαμε $3x_0 - 9k = 5$ δηλαδή $3|5$, άτοπο Αν έχει (τουλάχιστον) μια λύση, τότε πόσες και συνακόλουθα ποιες είναι οι λύσεις της; Για παράδειγμα η ισοδυναμία:

$$5x \equiv 7 \mathrm{mod} 12$$

έχει λύση την κλάση $x \equiv 11 \mathrm{mod} 12$. Πώς βρήκαμε τη λύση; Γράφουμε το $(5, 12) = 1$ ως γραμμικό συνδιασμό των 12 και 5,

$$5 \cdot 5 + (-2)12 = 1.$$

Πολλαπλασιάζουμε με 7, $5 \cdot 35 + (-14) \cdot 12 = 7$. Επομένως η κλάση $x \equiv 35 \equiv 11 \mathrm{mod} 12$, είναι λύση.

Πρόταση 4.3.1. *Η ισοδυναμία $ax \equiv b \mathrm{mod} m$ έχει λύση ακριβώς τότε όταν ο $d := (a, m) \mid b$. Αν έχει λύση, τότε το πλήθος των λύσεων είναι ακριβώς d.*

Απόδειξη. Αν $d \mid b$, τότε υπάρχει $\ell \in \mathbb{Z}$ τέτοιο ώστε $b = d\ell$. Όμως $d = (a, m)$. Συνεπώς υπάρχουν ακέραιοι $r, s \in \mathbb{Z}$ τέτοιοι ώστε $d = ar + ms$. Επομένως,

$$b = d\ell = (ar + ms)\ell = a(r\ell) + m(s\ell),$$

δηλαδή το $x_0 \equiv (r\ell) \mathrm{mod} m$, είναι λύση της ισοδυναμίας.

Ας υποθέσουμε τώρα ότι η ισοδυναμία έχει κάποια λύση x_0, $ax_0 \equiv b \mathrm{mod} m$. Αυτό σημαίνει ότι

$$ax_0 - b = mk, \text{ για κάποιο } k \in \mathbb{Z}.$$

Ο $d = (a, m)$, διαιρεί τα a και m. Άρα $d \mid b$. Στη συνέχεια θα αποδείξουμε ότι το πλήθος των λύσεων είναι ακριβώς d.

Αν x_0 λύση της ισοδυναμίας και $k \in \mathbb{Z}$, τότε και για $x_0 + k\frac{m}{d}$ είναι επίσης λύση. Πράγματι,

$$a\left(x_0 + k\frac{m}{d}\right) = ax_0 + km\frac{a}{d} \equiv ax_0 \equiv b \mathrm{mod} m.$$

Επίσης αν x_0, x_1 λύσεις, τότε

$$ax_0 \equiv b \equiv ax_1 \mathrm{mod} m.$$

Επειδή $d = (a, m)$, έπεται ότι

$$x_1 \equiv x_0 \mathrm{mod} \frac{m}{d},$$

και συνεπώς

$$x_1 = x_0 + k\frac{m}{d}, k \in \mathbb{Z},$$

δηλαδή κάθε λύση είναι της μορφής αυτής. Οι λύσεις

$$x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$$

είναι διαφορετικές $\mathrm{mod} m$, διότι για $k_1, k_2 \in \{1, 2, \ldots, d-1\}$ ισχύει

$$x_0 + k_1\frac{m}{d} = x_0 + k_2\frac{m}{d} \mathrm{mod} m \Leftrightarrow m \mid (k_1 - k_2)\frac{m}{d} \Leftrightarrow d \mid (k_1 - k_2) \Leftrightarrow k_1 = k_2,$$

διότι $0 \leq |k_1 - k_2| < d$.

Τέλος, κάθε λύση είναι ισοδύναμη με μία από τις παραπάνω. Πράγματι αν $x_0 + k\frac{m}{d}$, $k \in \mathbb{Z}$ λύση και γράψουμε $k = qd + r$, $0 \leq r < d$ έχουμε

$$x_0 + k\frac{m}{d} \equiv x_0 + \frac{(qd + r)m}{d} = x_0 + qm + r\frac{m}{d} \equiv x_0 + r\frac{m}{d} \mathrm{mod} m$$

για $0 \leq r < d$. □

Πόρισμα 4.3.2. *Αν* $(a, m) = 1$, *τότε η ισοδυναμία*

$$ax \equiv b \bmod m$$

έχει πάντοτε ακριβώς μια λύση.

Σημείωση Η ισοδυναμία $5x \equiv 7 \bmod 12$ έχει ακριβώς μια λύση, την $x \equiv 11 \bmod 12$.
Παράδειγμα. Να λυθεί η ισοδυναμία

$$27x \equiv 18 \bmod 105.$$

Ο μέγιστος κοινός διαιρέτης $(27, 105) = 3 \mid 18$. Επομένως η ισοδυναμία έχει ακριβώς 3 λύσεις $\bmod 105$. Γράφουμε τον $(27, 105)$ ως γραμμικό συνδυασμό των $27, 105$:

$$3 = 27 \cdot 4 + 105 \cdot (-1).$$

Πολλαπλασιάζουμε με 6,

$$18 = 27 \cdot 24 + 105 \cdot (-6).$$

Επομένως μία λύση της ισοδυναμίας είναι η

$$x_0 \equiv 24 \bmod 105.$$

Οι άλλες δύο λύσεις είναι:

$$x_1 = x_0 + \frac{m}{d} = 24 + \frac{105}{3} \equiv 59 \bmod 105$$

και

$$x_2 = x_0 + \frac{2m}{d} = 24 + 12\frac{105}{3} \equiv 94 \bmod 105.$$

Παρατήρηση 4.3.3. Ο τύπος του Georgi Voromi [10, σελ. 69]. Αν $(a, m) = 1$, η λύση της ισοδυναμίας

$$ax \equiv 1 \bmod m$$

δίνεται από τον τύπο

$$x \equiv \left(3 - 2a + 6\sum_{k=1}^{a-1}\left[\frac{mk}{a}\right]^2\right) \bmod m$$

Ο τύπος είναι αρκετά βολικός όταν ο a είναι αρκετά μικρός αφού τότε θα έχουμε λίγους προσθετέους.

Στη συνέχεια θα δούμε ότι το πρόβλημα της επίλυσης ισοδυναμίας ανωτέρου βαθμού ανάγεται στην επίλυση ενός γραμμικού συστήματος μιας ισοδυναμίας μέτρου δύναμης πρώτου αριθμού.

Πρόταση 4.3.4. *Υποθέτουμε ότι ο φυσικός αριθμός m, $(m > 1)$ αναλύεται σε γινόμενο*

$$m = \prod_{i=1}^{r} m_i,$$

όπου $(m_i, m_j) = 1$ για κάθε $i,j \in \{1, 2, \ldots, r\}$ και $i \neq j$. Κάθε λύση της ισοδυναμίας

$$f(x) \equiv 0 \mathrm{mod} m$$

είναι συγχρόνως και λύση του συστήματος ισοδυναμιών

$$\begin{aligned} f(x) &\equiv 0 \mathrm{mod} m_1 \\ f(x) &\equiv 0 \mathrm{mod} m_2 \\ &\vdots \quad\quad \vdots \\ f(x) &\equiv 0 \mathrm{mod} m_r \end{aligned} \tag{4.3.2}$$

και αντιστρόφως.

Απόδειξη. Αν $x_0 \in \mathbb{Z}$ λύση της ισοδυναμίας, θα έχουμε $f(x_0) \equiv 0 \mathrm{mod} m$. Επειδή για κάθε $i \in \{1, 2, \ldots, m\}$, $m_i \mid m$, έπεται ότι

$$f(x_0) \equiv 0 \mathrm{mod} m_i, \quad i \in \{1, 2, \ldots, r\}.$$

Αντίστροφα, αν x_0 κοινή λύση του συστήματος (4.3.2) θα έχουμε

$$f(x_0) \equiv 0 \mathrm{mod} m_i, \text{ για κάθε } i \in \{1, 2, \ldots, r\}.$$

Επομένως, $m_i \mid f(x_0)$ για κάθε $i \in \{1, 2, \ldots, r\}$. Συνεπώς $m = \prod_{i=1}^{r} m_i \mid f(x_0)$, δηλαδή ότι $f(x_0) \equiv 0 \mathrm{mod} m$. □

Αν λοιπόν μπορούσαμε να λύσουμε κάθε ισοδυναμία $f(x) \equiv 0 \mathrm{mod} m_i$, $i \in \{1, 2, \ldots, r\}$ χωριστά και να βρούμε κάποια λύση x_i,

$$f(x_i) \equiv 0 \mathrm{mod} m_i,$$

τότε θα μπορούσαμε στη συνέχεια να λύσουμε ένα σύστημα γραμικών ισοδυναμιών της μορφής:

$$\begin{aligned} x &\equiv x_1 \mathrm{mod} m_1 \\ x &\equiv x_2 \mathrm{mod} m_2 \\ &\vdots \quad\quad \vdots \\ x &\equiv x_r \mathrm{mod} m_r \end{aligned} \tag{4.3.3}$$

και κάθε λύση του συστήματος (4.3.3), έστω x_0 θα είναι και λύση του αρχικού συστήματος ισοδυναμιών (4.3.2), αφού

$$f(x_0) \equiv f(x_i) \equiv 0 \mathrm{mod} m_i$$

για κάθε $i \in \{1, 2, \ldots, r\}$.

Πρόταση 4.3.5 (Κινέζικό θεώρημα Υπολοίπων)**.** *Αν $m_1, m_2, \ldots, m_r$ φυσικοί αριθμοί $m_i > 1$ για κάθε $i \in \{1, 2, \ldots, r\}$ πρώτοι μεταξύ τους ανά δύο και $a_i \in \mathbb{Z}$, τότε το σύστημα ισοδυναμιών:*

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \quad\quad \vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

έχει μοναδική λύση $\bmod m$, $m = \prod_{i=1}^{r} m_i$. *Η απόδειξη της πρότασης υποδεικνύει και τον τρόπο υπολογισμού της λύσης.*

Απόδειξη. Για κάθε $i \in \{1, 2, 3, \ldots, r\}$, θέτουμε

$$M_i = \frac{m}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} m_{i+2} \cdots m_r.$$

Επειδή οι m_i είναι πρώτοι μεταξύ τους ανά δύο έπεται ότι $(m_i, M_i) = 1$. Επομένως για κάθε $i \in \{1, 2, \ldots, n\}$ η ισοδυναμία

$$M_i x \equiv 1 \bmod m_i$$

έχει μοναδική $\bmod m_i$ λύση. Ας την ονομάσουμε b_i. Ο ακέραιος αριθμός

$$x_0 \equiv \sum_{i=1}^{r} a_i M_i b_i$$

είναι λύση του συστήματος. Πράγματι, για κάθε $i \in \{1, 2, \ldots, r\}$, έχουμε

$$a_i M_i b_i \equiv a_i \bmod m_i$$

και για κάθε $j \in \{1, 2, \ldots, r\}, j \neq i$ ισχύει

$$a_j M_j b_j \equiv 0 \bmod m_i$$

δηλαδή

$$x_0 \equiv a_i \bmod m_i.$$

Θα αποδείξουμε ότι αυτή η λύση είναι μοναδική $\bmod m$. Αν x_1 μια άλλη λύση, τότε ισχύει

$$x_1 \equiv a_i \equiv x_0 \bmod m_i \text{ για κάθε } i \in \{1, 2, \ldots, r\}.$$

Συνεπώς $m_i \mid x_1 - x_0$ και επειδή οι m_i είναι πρώτοι μεταξύ τους ανά δύο, έπεται ότι

$$m = \prod_{i=1}^{r} m_i \mid (x_1 - x_0), \text{ δηλαδή } x_1 \equiv x_0 \bmod m.$$

□

Παρατήρηση 4.3.6. 1. Η πρόταση 2.2.2 θα μπορούσε να αποδειχθεί και με χρήση της 4.3.1.

Πράγματι η ύπαρξη λύσης της διοφαντικής εξίσωσης

$$aX + bY = c$$

είναι ισοδύναμη με την ύπαρξη λύσης της ισοτιμίας

$$aX \equiv c \bmod b$$

είτε της ισοτιμίας

$$bY \equiv c \bmod a.$$

Οι ισοτιμίες όμως έχουν λύση ακριβώς τότε όταν ο $d = (a, b)|c$. Επιπλέον αν x_0 κάποια λύση της ισοτιμίας

$$aX \equiv c \bmod b,$$

όλες οι λύσεις της είναι

$$x_k = x_0 + \frac{kb}{d}, \qquad k \in \mathbb{Z}.$$

Από την $aX + bY = c$, υπολογίζουμε το $y_0 = \frac{c-ax_0}{b}$ και στη συνέχεια τα

$$y_k = \frac{c - ax_k}{b} = \frac{c - a\left(x_0 + \frac{kb}{d}\right)}{b} = \frac{c - ax_0}{b} - \frac{a\frac{kb}{d}}{b} = y_0 - \frac{ka}{d}, \qquad k \in \mathbb{Z}.$$

2. Η πρόταση 4.3.5 χρωστά το όνομά της στον Sun-Tsu, Κινέζο συγγραφέα του πρώτου μ.Χ. αιώνα (κατ' άλλους θα πρέπει να έχει ζήσει μεταξύ του 200 και 470), ο οποίος στο έργο του Suan-ching «Εγχειρίδιο Αριθμητικής» έθεσε το ακόλουθο πρόβλημα:

   « Υποθέτουμε ότι έχουμε έναν άγνωστο αριθμό αντικειμένων. Όταν τα μετρούμε ανά τρία περισσεύουν δύο, όταν τα μετρούμε ανά πέντε περισσεύουν τρία, ενώ όταν τα μετρούμε ανά επτά περισσεύουν δυό. Πόσα αντικείμενα έχουμε;» Η λύση του προβλήματος, δηλαδή η λύση του συστήματος γραμμικών ισοτιμιών:

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

   παρά το ότι αφορά μια ειδική περίπτωση ο Sun-Tsu έδωσε ακριβώς τη μέθοδο απόδειξης της πρότασης 4.3.5. Πρώτα υπολογίζει βοηθητικούς ακέραιους $70, 21$ και 15 οι οποίοι είναι τα γινόμενα $5 \cdot 7$, $3 \cdot 7$ και $3 \cdot 5$ αντίστοιχα. Στη συνέχεια υπολογίζει το άθροισμα $270 + 321 + 215 = 233$, αυτή είναι μια λύση. Για να βρει την ελάχιστη αφαιρεί πολ/σια του 105 και βρίσκει 25. Φυσικά εδώ πρέπει να παρατηρήσουμε ότι οι $70, 21$ και 15 διαιρούμενοι με $3, 5$ και 7 αφήνου υπόλοιπο ένα.

   Δυστυχώς υπάρχει διχογνωμία σχετικά με το πότε έζησε ο Shun-Tsu. Μερικοί συγγραφείς όπως ο R. Dickson(1919), υποστηρίζουν ότι έζησε τον πρώτο μετά μ.Χ. αιώνα, ενώ άλλοι, όπως A. Wylie (1897), αλλά και ο L. Wang (1964), κάπου μεταξύ τρίτου και πέμπτου μ.Χ. αιώνα.

   Το αποτέλεσμα συμπεριελήφθηκε κατά τον 13ο αιώνα στο έργο του Qin Jushao Shushu Jiuzhan *Μαθηματική πραγματεία σε εννέα παραγράφους* [1] (1247), από όπου και διαδόθηκε στους νεότερους χρόνους.

[1] Παράφραση του παραπάνω τίτλου χρησιμοποιήσε ο J. Tattersall ως τίτλο του βιβλίου του *Elementary Number Theory in Nine chapters*

3. Το ίδιο ακριβώς πρόβλημα και λύση εμφανίζεται στην έκδοση του R. Hoche (1866) του έργου του Νικόμαχου του Γερασηνού, μαθηματικού του 1ου μ.Χ. αιώνα, « Ἀριθμητική εἰσαγωγή». Δεν ανήκει όμως στο σώμα του κυρίως κειμένου αλλά ακολουθεί ένα παράρτημα με τίτλο «Προβλήματα Αριθμητικά» και είναι το πέμπτο πρόβλημα με τίτλο: «Μέθοδος, δι' ἧς ἀστείως εὑρήσεις, οἷον ἀριθμόν ἔχει τις ἐπί νοῦν».

   Έτσι δεν είναι σίγουρο ότι είναι του Νικόμαχου. Εικάζεται ότι είναι του Ιωάννη του Φιλόπονου, 6ου μ.Χ. αιώνα ο οποίος συνέγραψε σχόλιο με τίτλο «Ἰωάννου Γραμματικοῦ Ἀλεξανδρέως (του Φιλοπόνου) εἰς το πρῶτον και δεύτερον τῆς Νικομάχου Ἀριθμητικής εἰσαγωγής». Παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στα [20], [25], [21], [18], [23].

4. Η απόδειξη της πρότασης 4.3.5 οφείλεται στον Gauss [6, άρθρο 36].

Η πρόταση 4.3.5 γενικεύθηκε γύρω στα 700 μ.Χ. από τον βουδιστή Μοναχό Yi Xing.

Πρόταση 4.3.7. *Το σύστημα ισοδυναμιών*

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \quad\quad \vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

έχει λύση ακριβώς τότε όταν $(m_i, m_j)|(a_i - a_j)$ για κάθε i,j, $i \neq j$. Αν υπάρχει λύση τότε αυτή είναι μοναδική modulo m όπου $m = [m_1, \ldots, m_r]$.

Απόδειξη. Αν το σύστημα έχει λύση τότε $m_i \mid (x - a_i)$ για κάθε $i = 1, \ldots, r$. Ας ονομάσουμε $m_{ij} = (m_i, m_j)$ για $i \neq j$, τότε $m_{ij} \mid (x - a_i)$ και $m_{ij} \mid (x - a_j)$ οπότε $m_{ij} \mid (x - a_i) - (x - a_j) = a_j - a_i$ για κάθε $i \neq j$.

Αντιστρόφως, υποθέτουμε ότι $m_{ij} \mid (a_i - a_j)$ για κάθε ζευγάρι $i,j \in \{1, 2, \ldots, r\}$, $i \neq j$. Η ιδέα είναι να αντικαταστήσουμε το δοθέν σύστημα με άλλο ισοδύναμο στο οποίο μπορούμε να εφαρμόσουμε το κινέζικο θεώρημα.

Σύμφωνα με την ανάλυση του φυσικού αριθμού $m = p_1^{n_1} p_2^{n_2} \cdot p_s^{n_s}$ τότε η ισοδυναμία $x \equiv a \bmod m$ είναι ισοδύναμη με το σύστημα των γραμμικών ισοδυναμιών

$$\begin{aligned} x &\equiv a \bmod p_1^{n_1} \\ x &\equiv a \bmod p_2^{n_2} \\ &\vdots \quad\quad \vdots \\ x &\equiv a \bmod p_s^{n_s} \end{aligned}$$

Αν το εφαρμόσουμε στο αρχικό σύστημα θα προκύψει σύστημα ισοδύναμο προς το αρχικό του οποίου κάθε ισοδυναμία θα έχει μέτρο δύναμη πρώτου. Βέβαια, τα μέτρα αυτά δεν είναι όλα κατ' ανάγκη πρώτα μεταξύ τους, αφού είναι δυνατόν κάποιες δυνάμεις πρώτου να εμφανίζονται στην κανονική ανάλυση των m_i για διάφορα m_i. Για κάποιο δοσμένο p αν διαλέξουμε τον δείκτη $i \in \{1, 2, \ldots, r\}$, για τον οποίο ο p εμφανίζεται στην κανονική ανάλυση του m_i με τον μεγαλύτερο εκθέτη (σε σχέση με τους εκθέτες στην ανάλυση του m_j).Έστω ότι αυτή η δύναμη είναι p^e. Αν τώρα $p^f \mid m_j$, τότε κατ' ανάγκη $f \leq e$ και $p^f \mid m_{ij} = (m_i, m_j) \mid a_i - a_j$. Επομένως προκύπτει ότι $a_i \equiv a_j \bmod p^f$. Αυτό σημαίνει ότι, αν η ισοδυναμία $x \equiv a \bmod p^e$ έχει λύση, τότε έχει λύση και η $x \equiv a_j \bmod p^f$.

Δηλαδή μπορούμε να διαγράψουμε από το σύστημα όλες τις ισοδυναμίες $x \equiv a_j \mathrm{mod} p^f$ και να αφήσουμε μόνο την $x \equiv a_i \mathrm{mod} p^e$ αυτή με τον μεγαλύτερο εκθέτη του p.

Αν το κάνουμε αυτό για κάθε πρώτο p θα έχουμε ένα σύστημα ισοδυναμιών με μέτρα δυνάμεις πρώτων οι οποίοι θα είναι ανά δύο διαφορετικοί. Το κινέζικο θεώρημα υπολοίπων μας εξασφαλίζει την ύπαρξη μοναδικής λύσης η οποία αυτόματα είναι και λύση του αρχικού. □

Παραδείγματα ισοδυναμιών:

(1) Να λυθεί το σύστημα:

$$\begin{aligned} 2x &\equiv 1 \mathrm{mod} 5 \\ 3x &\equiv 2 \mathrm{mod} 7 \\ 4x &\equiv 5 \mathrm{mod} 9 \end{aligned}$$

Κάθε ισοτιμία ξεχωριστά έχει μοναδική λύση. Η πρώτη $x \equiv 3 \mathrm{mod} 5$, η δεύτερη $x \equiv 3 \mathrm{mod} 7$ και η η τρίτη $x \equiv 8 \mathrm{mod} 9$. Επομένως, αρκεί να λύσουμε το σύστημα:

$$\begin{aligned} x &\equiv 3 \mathrm{mod} 5 \\ x &\equiv 3 \mathrm{mod} 7 \\ x &\equiv 8 \mathrm{mod} 9 \end{aligned}$$

Συνεπώς, $a_1 = 3$, $a_2 = 3$, $a_3 = 8$, $m = 5 \cdot 7 \cdot 9 = 315$, $M_1 = 63$, $M_2 = 45$ και $M_3 = 35$. Οι ισοτιμίες $M_i x \equiv 1 \mathrm{mod} m_i$, $i = 1, 2, 3$. $63x \equiv 1 \mathrm{mod} 5$, $45x \equiv 1 \mathrm{mod} 7$ και $35x \equiv 1 \mathrm{mod} 9$ έχουν λύσεις $b_1 \equiv 2 \mathrm{mod} 5$, $b_2 \equiv 5 \mathrm{mod} 7$ και $b_3 \equiv 8 \mathrm{mod} 9$ αντίστοιχα. Επομένως, η μοναδική λύση του αρχικού συστήματος είναι

$$x_0 \equiv (a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3) \mathrm{mod} 315$$

δηλαδή

$$x_0 = 143 \mathrm{mod} 315.$$

(2) Να λυθεί το σύστημα:

$$\begin{aligned} x &\equiv 13 \mathrm{mod} 40 \\ x &\equiv 5 \mathrm{mod} 44 \\ x &\equiv 38 \mathrm{mod} 275 \end{aligned}$$

Επειδή $a_1 = 13$, $a_2 = 5$, $a_3 = 38$, $m_1 = 40$, $m_2 = 44$, $m_3 = 275$ και $(40, 44) = 4 | 13 - 5 = 8$, $(40, 275) = 5 | 13 - 38 - -25$, $(44, 275) = 11 | 5 - 38 = -33$, έπεται ότι το σύστημα έχει μοναδική λύση $\mathrm{mod} m$, όπου $m = [40, 44, 275] = 2200$.

Για να βρούμε τη λύση διασπούμε τις ισοτιμίες σε ισοδύναμα συστήματα με μέτρα δυνάμεις πρώτων αριθμών. Έτσι η πρώτη ισοδυναμία γράφεται:

$$\begin{aligned} x &\equiv 13 \mathrm{mod} 2^3 \\ x &\equiv 13 \mathrm{mod} 5 \end{aligned}$$

η δεύτερη

$$\begin{aligned} x &\equiv 5 \mathrm{mod} 2^2 \\ x &\equiv 5 \mathrm{mod} 11 \end{aligned}$$

και η τρίτη

$$\begin{aligned} x &\equiv 38 \bmod 5^2 \\ x &\equiv 38 \bmod 11 \end{aligned}$$

Από αυτές επιλέγουμε μόνο εκείνες που έχουν μέτρο με τον μεγαλύτερο εκθέτη και σχηματίζουμε το σύστημα

$$\begin{aligned} x &\equiv 5 \bmod 8 \\ x &\equiv 13 \bmod 25 \\ x &\equiv 5 \bmod 11 \end{aligned}$$

Λύνουμε το τελευταίο σύστημα σύμφωνα με το κλασικό θεώρημα υπολοίπων του Κινέζου και βρίσκουμε

$$x \equiv 1413 \bmod 2200.$$

Μπορούμε να λύσουμε το παραπάνω σύστημα στο sage δίνοντας τις εντολές:

```
sage: CRT_list([13,5,38],[40,44,275])
1413
```

Θα μπορούσαμε να αντιμετωπίσουμε το παραπάνω πρόβλημα με ωμή βία, αλλά αυτό θα καθυστερούσε πολύ περισσότερο:

```
for i in range(1,8*25*11):
    if (Mod(i,8) == Mod(5,8)) and (Mod(i,25) == Mod(13,25)) \
    and (Mod(i,11) == Mod(5,11)):
        i
1413
```

Στο παραπάνω πρόγραμμα ζητήσαμε από τον υπολογιστή να δοκιμάσει όλους τους αριθμούς από το 1 μέχρι το $2200 = 8 \cdot 25 \cdot 11$ και να βρει τη λύση.

Παρατήρηση 4.3.8. Μπορούμε να δόσουμε μια διαφορετική απόδειξη του θεωρήματος του Κινέζου κάνοντας χρήση του θεωρήματος του Euler 4.2.6. Όπως και στην πρώτη απόδειξη του θεωρήματος θέτουμε $m = \prod_{i=1}^{r} m_i$ και $M_i = \frac{m}{m_i}$, $i = 1, 2, \ldots, r$.

Ο ακέραιος αριθμός

$$x_0 = \sum_{i=1}^{r} a_i M_i^{\varphi(m_i)}.$$

είναι λύση του συστήματος ισοτιμιών. Πράγματι, επειδή

$$M_j \equiv 0 \bmod m_i \text{ για κάθε } j \neq i$$

έχουμε $x_0 = a_i M_i^{\varphi(m_i)} \bmod m_i$. Όμως, επειδή $(M_i, m_i) = 1$, σύμφωνα με το θεώρημα του Euler, έχουμε

$$M_i^{\varphi(m_i)} \equiv 1 \bmod m_i.$$

Συνεπώς $x_0 = a_i \bmod m_i$ για κάθε $i = 1, 2, \ldots, r$.

Παρατήρηση 4.3.9. Με τη βοήθεια του Κινέζικου θεωρήματος υπολοίπων μπορούμε να δώσουμε μια διαφορετική απόδειξη του ότι η ϕ συνάρτηση είναι πολλαπλασιαστική.

Υποθέτουμε ότι m_1, m_2 είναι δύο θετικοί ακέραιοι πρώτοι μεταξύ τους. Αν $m = m_1 m_2$ και a ακέραιος με $(a, m) = 1$. Υπάρχει μοναδικό $a_1 \in \mathcal{S}(m_1)$ τέτοιο ώστε $a \equiv a_1 \mathrm{mod} m_1$. Αρκεί να πάρουμε το $a \mathrm{mod} m_1$. Ομοίως υπάρχει $a_2 \in \mathcal{S}(m_2)$ ώστε $a \equiv a_2 \mathrm{mod} m_2$. Είναι φανερό ότι $(a, m_1) = 1$ για $i = 1, 2$. Επομένως και $(a_i, m_i) = 1$ για $i = 1, 2$. Από τα παραπάνω συμπεραίνουμε ότι σε κάθε $a \in \mathcal{R}(m)$ αντιστοιχεί ένα ζευγάρι $(a_1, a_2) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2)$. Αντίστροφα, αν μας δοθεί ένα ζευγάρι $(a_1, a_2) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2)$, τότε σύμφωνα με το Κινέζικο θεώρημα υπολοίπων, υπάρχει ένα μοναδικό $x \in \mathcal{S}(m)$ τέτοιο ώστε

$$\begin{aligned} x &\equiv a_1 \mathrm{mod} m_1 \\ x &\equiv a_2 \mathrm{mod} m_2 \end{aligned}$$

Επειδή $(a_i, m_i) = 1$ για $i = 1, 2$ έπεται ότι και $(x, m_i) = 1$, δηλαδή ότι $(x, m) = 1$, που σημαίνει ότι $x \in \mathcal{R}(m)$.

Επομένως αποδείξαμε ότι υπάρχει αμφιμονοσήμαντη αντιστοιχία ανάμεσα στα σύνολα $\mathcal{R}(m)$ και $\mathcal{R}(m_1) \times \mathcal{R}(m_2)$. Τα σύνολα αυτά έχουν τον ίδιο αριθμό στοιχείων δηλαδή $\phi(m) = \phi(m_1)\phi(m_2)$.[2]

4.3.1 Ασκήσεις

1. Να λύσετε τις ισοδυναμίες:

   (α΄) $25x \equiv 15 \mathrm{mod} 29$

   (β΄) $6x \equiv 15 \mathrm{mod} 21$

   (γ΄) $34x \equiv 60 \mathrm{mod} 98$

2. Ομοίως να λυθούν τα συστήματα:

   (α΄)

   $$\begin{aligned} x &\equiv 4 \mathrm{mod} 11 \\ x &\equiv 14 \mathrm{mod} 29 \\ x &\equiv 7 \mathrm{mod} 31 \end{aligned}$$

   (β΄)

   $$\begin{aligned} 2x &\equiv 1 \mathrm{mod} 5 \\ 3x &\equiv 6 \mathrm{mod} 9 \\ x &\equiv 3 \mathrm{mod} 17 \end{aligned}$$

3. Να βρείτε έναν ακέραιο ο οποίος διαιρούμενος με $2, 3, 6$ και 12 να δίνει υπόλοιπο $1, 2, 5$ και 5 αντίστοιχα.

4. Τρεις γεωργοί μοιράζονται εξ ίσου το ρύζι που παράγουν όλοι μαζί. Επισκέπτονται διαφορετικές αγορές ο καθένας. Στην πρώτη αγορά μονάδα μέτρησης είναι τα 83 κιλά, στη δεύτερη τα 110 κιλά και στη τρίτη τα 135 κιλά. Ο καθένας πούλησε όσο πιο πολλά μπορούσε και όταν γύρισαν σπίτι, ο πρώτος επέστρεψε 32 κιλά, ο δεύτερος 70 κιλά και ο τρίτος 30 κιλά. Πόσα κιλά ρύζι παρήγαγαν και οι τρεις μαζί; (Αρχαίο κινέζικο πρόβλημα).

[2] Στο δεύτερο μέρος του βιβλίου θα δώσουμε μια απόδειξη η οποία είναι κατά βάθος ίδια με την παρούσα αλλά χρησιμοποιεί ορολογία Θεωρίας Ομάδων.

4.4 Εφαρμογές των ισοδυναμιών

4.4.1 g-αδική παράσταση θετικών ακέραιων

Στην παράγραφο αυτή θα ασχοληθούμε με μερικές εφαρμογές των ισοδυναμιών.

Πρόταση 4.4.1 (*g*-αδική παράσταση θετικών ακέραιων)**.** *Αν $g \in \mathbb{Z}$, $g > 1$ τότε κάθε θετικός ακέραιος n γράφεται μονοσήμαντα στη μορφή*

$$n = a_m g^m + a_{m-1} g^{m-1} + \cdots + a_2 g^2 + a_1 g + a_0,$$

όπου a_i $i = 0, 1, 2, \ldots m$ ακέραιοι τέτοιοι ώστε $0 \leq a_i < g$ για κάθε $i = 0, 1, 2, \ldots, m$.

Απόδειξη. Θα αποδείξουμε πρώτα την ύπαρξη. Σύμφωνα με το θεώρημα της διαίρεσης με υπόλοιπο 1.2.3 έχουμε

$$n = q_1 g + a_0, \qquad 0 \leq a_0 < g.$$

Αν $q_1 \geq g$ τότε, πάλι λόγω της 1.2.3 έχουμε $q_1 = q_2 g + a_1$, $0 \leq a_1 < g$, οπότε

$$n = (q_2 g + a_1) g + a_0 = q_2 g^2 + a_1 g + a_0.$$

Αν $q_2 \geq g$, συνεχίζουμε κατά τον ίδιο τρόπο, $q_2 = q_3 g + a_2$, $0 \leq a_2 < g$,

$$n = q_3 g^3 + a_2 g^2 + a_1 g + a_0.$$

Συνεχίζουμε όσο το επόμενο πηλίκο είναι $\geq g$ (επαγωγικά). Επειδή

$$n > q_1 > q_2 > \cdots \geq 0,$$

αυστηρά φθίνουσα ακολουθία θετικών ακέραιων έπεται ότι μετά από πεπερασμένο πλήθος βημάτων θα γίνει σταθερά. Αν αυτό γίνει στο $(m-1)$-στο βήμα θα έχουμε

$$q_{m-1} = q_m g + a_{m-1}, 0 \leq a_{m-1} < g \text{ και } 0 \leq q_m < g.$$

Αν $a_m := q_m$, τότε

$$n = a_m g^m + a_{m-1} g^{m-1} + \cdots + a_1 g + a_0.$$

Θα αποδείξουμε τώρα τη μοναδικότητα της παράστασης. Υποθέτουμε ότι ο n έχει δύο, διαφορετικές μεταξύ τους παραστάσεις:

$$\begin{aligned} n &= a_m g^m + \cdots + a_1 g + a_0 \\ n &= b_m g^m + \cdots + b_1 g + b_0, \end{aligned}$$

όπου $0 \leq a_i, b_j < g$ για κάθε $i, j \in \{0, 1, 2, \ldots, m\}$. Χρησιμοποιούμε και στις δύο εκφράσεις τον ίδιο εκθέτη m διότι μπορούμε να συμπληρώσουμε, αν χρειάζεται, όρους με συντελεστή 0.

Αφαιρούμε τις δύο παραπάνω σχέσεις κατά μέλη και έχουμε

$$0 = c_m g^m + \cdots + c_1 g + c_0, \text{ όπου } c_i = a_i - b_i, \quad i = 0, 1, 2, \ldots, m. \tag{4.4.1}$$

Επειδή οι δύο παραστάσεις είναι διαφορετικές μεταξύ τους, έπεται ότι υπάρχει ένας τουλάχιστον δείκτης $i \in \{0, 1, 2, \ldots, m\}$ τέτοιος ώστε $c_i = a_i - b_i \neq 0$. Αν

$$\ell := \min \{i \in \{0, 1, 2, \ldots, m\} | c_i \neq 0\},$$

τότε η σχέση (4.4.1) γράφεται

$$0 = c_m g^m + \cdots + c_\ell g^\ell \qquad c_\ell \neq 0.$$

Επομένως $c_\ell = -g\left(c_m g^{m-\ell-1} + \cdots + c_{\ell+1}\right)$ συνεπώς $g \mid c_\ell$. Από τις ανισότητες $0 \leq a_\ell < g$ και $0 \leq b_\ell < g$ προκύπτει: $-g < a_\ell - b_\ell < g$, δηλαδή $-g < c_\ell < g$ δηλαδή $|c_\ell| < g$ το οποίο όμως μαζί με το $g \mid c_\ell$ δίνει ότι $c_\ell = 0$, άτοπο. Συνεπώς αποδείξαμε και το μονοσήμαντο. □

Συνήθως χρησιμοποιούμε τον συμβολισμό

$$n = (a_m a_{m-1} \ldots a_2 a_1 a_0)_g$$

και θα λέμε ότι αυτή είναι η παράσταση του n *ως προς τη βάση* g. Οι συνηθισμένες βάσεις είναι $g = 10$ (δεκαδικό) και $g = 2$ (δυαδική). Η απόδειξη της ύπαρξης μας δίνει και τη μέθοδο (αλγόριθμο) της εύρεση της παράστασης του δοθέντος n ως προς κάποια δοθείσα βάση g.

Για παράδειγμα ο αριθμός $n = 1785$ (δεκαδικός) γράφεται με βάση το 2 (δυαδικό σύστημα)

$$\begin{aligned}
1785 &= 2 \cdot 892 + 1 = 2(2 \cdot 446) + 1 = \\
&= 2^2 \cdot 446 + 1 = 2^2(2 \cdot 223) + 1 = 2^3 \cdot 223 + 1 \\
&= 2^3(2 \cdot 111 + 1) + 1 = 2^4 \cdot 111 + 2^3 \cdot 1 + 1 \\
&= 2^4(2 \cdot 55 + 1) + 2^3 + 1 = \\
&= 2^5 \cdot 55 + 2^4 + 2^3 + 1 = 2^5(2 \cdot 27 + 1) + 2^4 + 2^3 + 1 \\
&= 2^6 \cdot 27 + 2^5 + 2^4 + 2^3 + 1 = \\
&= 2^6(2 \cdot 13 + 1)2^5 + 2^4 + 2^3 + 1 = 2^7(2 \cdot 6 + 1) + 2^5 + 2^4 + 2^3 + 1 = \\
&= 2^8 \cdot 6 + 2^7 + 2^5 + 2^4 + 2^3 + 1 = 2^8(2 \cdot 3) + 2^7 + 2^5 + 2^4 + 2^3 + 1 = \\
&= 2^9(2 + 1) + 2^7 + 2^5 + 2^4 + 2^3 + 1 = \\
&= 2^{10} + 2^9 + 2^7 + 2^5 + 2^4 + 2^3 + 1 = (11010111001)_2.
\end{aligned}$$

Ιδιαίτερα ως προς βάση το $g = 2$, επειδή τα ψηφία της παράστασης είναι 0 και 1 από την πρόταση 4.4.1, έπεται ότι κάθε φυσικός αριθμός έχει μοναδική παράσταση ως άθροισμα διαφορετικών μεταξύ τους δυνάμεων του 2 με εκθέτες φυσικούς αριθμούς.

Τέλος στο ερώτημα πόσο είναι το πλήθος των ψηφίων του n ως προς τη βάση g, η απάντηση είναι εύκολη. Επειδή

$$g^m \leq n < g^{m+1},$$

συνεπάγεται ότι $m \log g \leq \log n < (n+1) \log g$,

$$m \leq \frac{\log n}{\log g} < m + 1.$$

Επομένως

$$m = \left[\frac{\log n}{\log g}\right]$$

και επειδή τα ψηφία είναι $m + 1$ έχουμε $\left[\frac{\log n}{\log g}\right] + 1$ το πλήθος ψηφία. Φυσικά αν θεωρήσουμε και τον λογάριθμό ως προς βάση g, τότε το πλήθος των ψηφίων είναι $[\log_g n] + 1$. Συχνά ο αριθμός αυτός συμβολίζεται και $\lceil \log_g n \rceil$ και ονομάζεται *οροφή* του $\log_g n$.

4.4.2 Κριτήρια διαιρετότητας

Αν $\sum_{i=0}^{n} a_i 10^i$ είναι η δεκαδική παράσταση του θετικού ακέραιου m, $s = \sum_{i=0}^{n} a_i$, $t = \sum_{i=0}^{n} (-1)^i a_i$, τότε

1. $2 \mid m$ ακριβώς τότε όταν $2 \mid a_0$, αφού $10^k \equiv 0 \mathrm{mod} 2$ για κάθε $k \geq 1$.

2. $5 \mid m$ ακριβώς τότε όταν $5 \mid a_0$, αφού $10^k \equiv 0 \mathrm{mod} 5$ για κάθε $k \geq 1$.

3. $4 \mid m$ ακριβώς τότε όταν $4 \mid 10a_1 + a_0$, αφού $10^k \equiv 0 \mathrm{mod} 4$ για κάθε $k \geq 2$.

4. $25 \mid m$ ακριβώς τότε όταν $25 \mid 10a_1 + a_0$ αφού $10^k \equiv 0 \mid 25$ για κάθε $k \geq 2$.

5. 3 ή $9 \mid m$ ακριβώς τότε όταν 3 ή $9 \mid s$, αφού $10^k \equiv 1 \mathrm{mod} 9$ ή $10^k \equiv 1 \mathrm{mod} 3$ για κάθε $k \geq 1$.

6. $11 \mid m$ ακριβώς τότε όταν $11 \mid t$ αφού $10^k \equiv (-1)^k \mathrm{mod} 11$ για κάθε $k \geq 1$.

7. $7 \mid m$ ακριβώς τότε όταν $7 \mid b - 2a_0$, όπου $b = a_m 10^{m-1} + \cdots + a_2 10 + a_1$. Πράγματι, $m = 10b + a_0$ Επομένως $7 \mid m$ αν και μόνο αν $7 \mid 3b + a_0 = 3b + 7a_0 - 6_a 0$ αν και μόνο αν $7 \mid 3(b - 2a_0)$ αν και μόνο αν $7 \mid b - 2a_0$.

8. $13 \mid m$ ακριβώς τότε όταν $13 \mid (b + 4a_0)$ όπου $b = a_m 10^{m-1} + \cdots + a_2 10 + a_1$. Πράγματι, $13 \mid m$ αν και μόνο αν $13 \mid 10b + a_0$ αν και μόνο αν $13 \mid (13b - 3b + 13a_0 - 12a_0)$ αν και μόνο αν $13 \mid 3(b + 4a_0)$ αν και μόνο αν $13 \mid b + a_0$.

9. Ο m διαιρείται συγχρόνως με $7, 11$ και 13 ακριβώς τότε όταν το $7, 11$ και 13 διαιρούν τον

   $$100a_2 + 10a_1 + a_0 - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - (100a_{11} + 10a_{10} + a_9).$$

   Πράγματι παρατηρούμε ότι $7 \cdot 11 \cdot 13 = 1001$ και ότι για ℓ άρτιο

   $$10^{3\ell} \equiv 1 \mathrm{mod} 1001, 10^{3\ell+1} \equiv 10 \mathrm{mod} 1001, 10^{3\ell+2} \equiv 100 \mathrm{mod} 1001$$

   ενώ για ℓ περιττό

   $$10^{3\ell} \equiv -1 \mathrm{mod} 10001, 10^{3\ell+1} \equiv -10 \mathrm{mod} 1001, 10^{3\ell+2} \equiv -100 \mathrm{mod} 1001.$$

4.4.3 Η ημέρα της εβδομάδας

Αν

- k είναι η μέρα του μήνα
- m είναι ο μήνας (η αρίθμηση αρχίζει από τον μήνα Μάρτιο)
- N είναι το έτος (αν είναι Ιανουάριος ή Φεβρουάριος είναι το προηγούμενο έτος)
- C είναι ο αιώνας
- Y είναι το έτος μέσα στον αιώνα ($N = 100C + Y$).

τότε

$$W = k + [2,6 \cdot m - 0,2] - 2 \cdot C + Y + \left[\frac{Y}{4}\right] + \left[\frac{C}{4}\right] \mathrm{mod} 7$$

Παράδειγμα. Τι μέρα ήταν η 5η Σεπτεμβρίου του 1951;

$$k = 5, m = 7, N = 1951, C = 19, Y = 51$$

$$\begin{aligned} W &= 5 + [2,6 \cdot 7 - 0,2] - 2 \cdot 19 + 51 + \left[\frac{51}{4}\right] + \left[\frac{19}{4}\right] \\ &= 5 + 18 - 38 + 51 + 12 + 4 \mathrm{mod} 7 \equiv 52 \equiv 3 \mathrm{mod} 7. \end{aligned}$$

Επομένως ήταν ημέρα Τετάρτη (Κυριακή αντιστοιχεί στο 0 και το Σάββατο στο 6). [12, σελ. 166-170]

Παράδειγμα. Σήμερα 7η Δεκεμβρίου 2014 έχουμε $k = 7$, $m = 10$, $C = 20$, $Y = 14$. Επομένως $W = 7 + [2,6 \cdot 10 - 0,2] - 2 \cdot 20 + 14 + [14/4] + [20/4] = 7 + 25 - 40 + 14 + 3 + 5 \equiv 0 \mathrm{mod} 7$. Άρα είναι μέρα Κυριακή!

4.4.4 Υπολογισμός του Ορθοδόξου Πάσχα

Ο υπολογισμός της ημέρας του Πάσχα βασίζεται και αυτός στις ιδιότητες των ισοτιμιών. Αν συμβολίσουμε με (b, a) το υπόλοιπο της διαίρεσης του ακέραιου b με τον ακέραιο a και για το έτος X ορίσουμε

$$a = (X, 19), b = (X, 4), c = (X, 7), A = (19a + 16, 30), B = (4c + 2b + 6a, 7),$$

τότε η ημέρα του Πάσχα $E(X)$ του έτους X θα είναι

$$E(X) = A + B + 3 \text{ «ημέρες Απριλίου»}$$

Σημείωση: Αν $E(Q) \leq 30$, τότε αναφέρεται σε ημέρες Απριλίου ενώ αν $E(X) \geq 30$, τότε αυτό σημαίνει την $(E(X) - 30)$-στή ημέρα του Μαΐου. Ο παραπάνω τύπος οφείλεται στον Gauss.

Παράδειγμα. Για $X = 2007$ $a = 12, b = 3, c = 5, A = 4, B = 1$. $E(X) = A + B + 3 = 4 + 1 + 3 = 8$ ημέρες Απριλίου. Πράγματι, το 2007 το Πάσχα ήταν στις 8 Απριλίου.

Παράδειγμα. Το έτος $Q = 2015$ το Πάσχα θα είναι $a = (X, 19) = 1$, $b = (X, 4) = 3$, $c = (X, 7) = 6$, $A = (19a+16, 30) = (35, 30) = 5$, $B = (4c+2b+6A, 7) = (60, 7 = 4)$. Επομένως $E(X) = 5+4+3 = 12$ Απριλίου. [10].

4.5 Ύψωση σε δύναμεις και εύρεση ρίζας $\mathrm{mod} m$

Θέλουμε να υπολογίσουμε το

$$7^{345678912} \mathrm{mod} 18165151.$$

Το πρώτο που θα έπρεπε να γνωρίζουμε είναι η παραγοντοποίηση του αριθμού 18165151 για να εφαρμόσουμε το θεώρημα του Euler.

Πράγματι με μεθόδους που θα αναπτύξουμε παρακάτω έχουμε

$$18165151 = 3931 \cdot 4621.$$

Η ϕ-συνάρτηση του Euler μας δίνει

$$\phi(18165151) = (3931 - 1)(4621 - 1) = 18156600.$$

Ο μέγιστος κοινός διαιρέτης $(7, 181651551) = 1$. Επομένως από το θεώρημα του Euler,

$$7^{18156600} \equiv 1 \mathrm{mod} 18165151.$$

Επειδή, $345678912 = 18156600 \cdot 19 + 541043$, έχουμε

$$7^{18156600} \equiv 7^{541043} \mathrm{mod} 18165151.$$

Γράφουμε τον εκθέτη 541043 σε δυαδική μορφή. Αυτό γίνεται πολύ εύκολα σύμφωνα με τον ακόλουθο αλγόριθμο:

$$n = \sum_{i=0}^{r} \varepsilon_i 2^{r-i}, \varepsilon_i \in \{0, 1\}.$$

Αν m περιττός $\varepsilon_0 = 1$, αλλιώς $\varepsilon_0 = 0$. Αντικαθιστούμε το n με το $\left[\frac{n}{2}\right]$ και συνεχίζουμε όμοια μέχρι να φτάσουμε στο 0.

Το

$$a^n = a^{\sum_{i=0}^{r} \varepsilon_i 2^i} = \prod_{e_i=1} a^{2^i} \mathrm{mod} n.$$

Στο παράδειγμά μας,

$$541043 = (11001110100000100001)_2$$

Στη συνέχεια εφαρμόζουμε τη μέθοδο των διαδοχικών υψώσεων στο τετράγωνο.

$$\begin{array}{rcrl}
7 & = & 7 & \mathrm{mod} 18165151 \\
7^2 & = & 49 & \mathrm{mod} 18165151 \\
7^{2^3} & = & 2401 & \mathrm{mod} 18165151 \\
7^{2^4} & = & 5764801 & \mathrm{mod} 18165151 \\
7^{2^5} & = & 4796913 & \mathrm{mod} 18165151 \\
7^{2^6} & = & 14438188 & \mathrm{mod} 18165151 \\
7^{2^7} & = & 16179105 & \mathrm{mod} 18165151 \\
7^{2^8} & = & 15991127 & \mathrm{mod} 18165151 \\
7^{2^9} & = & 7879037 & \mathrm{mod} 18165151 \\
7^{2^{10}} & = & 2156379 & \mathrm{mod} 18165151 \\
7^{2^{11}} & = & 543208 & \mathrm{mod} 18165151 \\
7^{2^{12}} & = & 218420 & \mathrm{mod} 18165151 \\
7^{2^{13}} & = & 5609874 & \mathrm{mod} 18165151 \\
7^{2^{14}} & = & 16317151 & \mathrm{mod} 18165151 \\
7^{2^{15}} & = & 1116547 & \mathrm{mod} 18165151 \\
7^{2^{16}} & = & 2890079 & \mathrm{mod} 18165151 \\
7^{2^{17}} & = & 2214629 & \mathrm{mod} 18165151 \\
7^{2^{18}} & = & 9002792 & \mathrm{mod} 18165151 \\
7^{2^{19}} & = & 12145310 & \mathrm{mod} 18165151 \\
7^{2^{20}} & = & 8503586 & \mathrm{mod} 18165151
\end{array}$$

Το ζητούμενο αποτέλεσμα προκύπτει πολλαπλασιάζοντας τις δυνάμεις που εμφανίζονται με 1 στο δυαδικό ανάπτυγμα:

$$7 \cdot 7^{2^5} \cdot 7^{2^{11}} \cdot 7^{2^{13}} \cdot 7^{2^{14}} \cdot 7^{2^{15}} \cdot 7^{2^{18}} \cdot 7^{2^{19}} = 13883771.$$

Ας έρθουμε στο αντίστροφο πρόβλημα. Γνωρίζουμε ότι

$$x^n \equiv a \bmod m,$$

τα m, a και n είναι δεδομένα. Ζητούμε να βρούμε το x.

Για παράδειγμα υποθέτουμε ότι $x^{157} \equiv 1078 \bmod 2724$. Επιθυμούμε να υπολογίσουμε το x. Ο 2747 είναι μικρός ακέραιος. Παραγοντοποιείται εύκολα, $2747 = 41 \cdot 67$. Επομένως $\phi(2747) = \phi(41)\phi(67) = 40 \cdot 66 = 2640$. Λύνουμε τη διοφαντική εξίσωση

$$157b - 2640c = 1$$

και βρίσκουμε μια λύση $b = 1093$ και $c = 65$. Σύμφωνα με το θεώρημα του Euler,

$$x^{2640} \equiv 1 \bmod 2747.$$

Επομένως,

$$\begin{aligned} \left(x^{157}\right)^{1095} &= x^{157 \cdot 1093} = x^{1+65 \cdot 65 \cdot 2640} \\ &= x \cdot \left(x^{2640}\right)^{65} \equiv x \bmod 2747 \end{aligned}$$

Επειδή $x^{157} \equiv 1078 \bmod 2747$, έπεται ότι $x \equiv 1078^{1093} \bmod 2747$. Εφαρμόζουμε και πάλι τη μέθοδο των διαδοχικών υψώσεων στο τετράγωνο και βρίσκουμε

$$x \equiv 1415 \qquad \bmod 2747$$

Παρατηρούμε ότι τελικά η διαδικασία είναι εύκολη. Προϋποθέτει όμως τη γνώση της τιμής της συνάρτησης του Euler στο μέτρο 2747 κάτι το οποίο εξαρτάται από την παραγοντοποίηση του μέτρου. Αυτό βέβαια δεν είναι πάντοτε δυνατό, ιδιαίτερα όταν το μέτρο είναι μεγάλο και έχει μόνο μεγάλους πρώτους παράγοντες. Αλλά «κάθε εμπόδιο για καλό» που λέει και ο λαός. Το «καλό» είναι η χρήση της Θεωρίας Αριθμών στην Κρυπτογραφία.

4.6 Κρυπτογραφία

Ένα κρυπτοσύστημα είναι μια διατεταγμένη πεντάδα (P, C, K, E, D) όπου:

- P (plaintext) είναι το σύνολο των μηνυμάτων που θέλουμε να στείλουμε
- C (ciphertext) είναι το σύνολο όλων των κωδικοποιημένων μηνυμάτων.
- K (key space) ο χώρος των κλειδιών κωδικοποίησης.
- E ο χώρος των συναρτήσεων κωδικοποίησης. Για κάθε κλειδί $k \in K$ υπάρχει μια συνάρτηση $\varepsilon_k \in E$ τέτοια ώστε $\varepsilon_k : P \to C$.
- D ο χώρος των συναρτήσεων αποκωδικοποίησης. Για κάθε κλειδί $k \in K$ υπάρχει μια συνάρτηση $d_k : C \to P$ τέτοια ώστε

$$d_k(e_k(x)) = x, \text{ για κάθε } x \in P.$$

Από πλευράς μεθοδολογίας η κρυπτογραφία χωρίζεται σε δύο μεγάλες κατηγορίες, στη *συμμετρική* και στην *ασύμμετρη* κρυπτογραφία.

4.6.1 Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία η κρυπτογράφηση και η αποκρυπτογράφηση γίνεται με το ίδιο κλειδί.

Αντιστοιχούμε σε κάθε γράμμα του αγγλικού αλφαβήτου τους αριθμούς από 0 μέχρι 25 και εργαζόμαστε mod26. Ακολουθούν μερικά παραδείγματα συμμετρικών κρυπτοσυστημάτων.

Το κρυπτοσύστημα της μεταφοράς (shift cipher)

Εδώ $P = C = K = \mathbb{Z}_{26}$. Αν $k \in K = \mathbb{Z}_{26}$ η $e_k(x) \equiv (x + k) \text{mod} 26$ και η $d_k(y) \equiv (y - k) \text{mod} 26$.

Η ειδική περίπτωση για $k = 3$ λέγεται κρυπτοσύστημα του Καίσαρα (Caesar cipher). Για παράδειγμα η Αλίκη επιθυμεί να στείλει στον Βασιλάκη το μήνυμα:

I LOVE YOU

Μετατρέπει τα γράμματα σε αριθμούς. (Λέγεται ότι αυτό ήταν επινόηση του Πολύβιου.)

$$8, 11, 14, 21, 4, 24, 14, 20$$

Αυτό κωδικοποίειται (προσθέτουμε το 3 σε κάθε αριθμό εργαζόμενοι mod26) στο

$$11, 14, 17, 24, 7, 1, 17, 23$$

Στην αποκωδικοποίηση αφαιροούμε 3 από κάθε αριθμό και βρίσκουμε πάλι το αρχικό μήνυμα.

Παρατήρηση: Το κρυπτοσύστημα έχει ένα σοβαρό μειονέκτημα: έχει πολύ μικρό αριθμό κλειδιών μόνο 26. Θα μπορούσε να δοκιμάσει κανείς όλα τα δυνατά κλειδιά μέχρι που να προκύψει κείμενο που έχει νόημα και έτσι να το αποκρυπτογραφήσει.

Το κρυπτοσύστημα της αντικατάστασης (substitution cipher)

Στο κρυπτοσύστημα της αντικατάστασης $P = C = \mathbb{Z}_{26}$ αλλά το K είναι το σύνολο των μεταθέσεων των 26 στοιχείων δηλαδή $\#K = 26!$.

Δυστυχώς και πάλι το σύστημα δεν είναι ασφαλές. Υπάρχουν πίνακες οι οποίοι μας δίνουν τη συχνότητα εμφάνισης ενός γράμματος σε κείμενο της αγγλικής γλώσσας. Αυτό βοηθάει πολύ στην αποκρυπτογράφηση του συστήματος από τον ανεπιθύμητο τρίτο.

Το αφινικό κρυπτοσύστημα

Στο αφινικό κρυπτοσύστημα $P = C = \mathbb{Z}_{26}$ και

$$K := \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : (a, 26) = 1\}.$$

Το πλήθος των κλειδιών είναι $\phi(26) \cdot 26 = 312$. Για κάθε κλειδί $k = (a, b) \in K$ η συνάρτηση κωδικοποίησης $e_k(x) = (ax + b) \text{mod} 26$ και η συνάρτηση αποκωδικοποίησης

$$d_k(y) = a^{-1}(y - b) \text{mod} 26$$

όπου a^{-1} είναι το αντίστροφο του $a \text{mod} 26$ δηλαδή η λύση της ισοδυναμίας

$$ax \equiv 1 \text{mod} 26$$

Σημείωση: Αν με τη βοήθεια του ευκλείδειου αλγορίθμου, γράψουμε

$$as + 26t = 1$$

τότε το s είναι το a^{-1}.
Παράδειγμα. Έστω $K = (a, b) = (3, 7)$. Η συνάρτηση κωδικοποίησης είναι

$$e_k(x) \equiv 7x + 3 \mathrm{mod} 26$$

Η ισοδυναμία $7x \equiv 1 \mathrm{mod} 26$, έχει λύση την $x \equiv 15 \mathrm{mod} 26$, δηλαδή $a^{-1} = 15$. Η συνάρτηση αποκωδικοποίησης είναι η

$$d_k(y) \equiv 15(y - 3) \equiv 15y - 19 \mathrm{mod} 26$$

Κωδικοποιούμε τη λέξη ΗΟΤ

$H \mapsto 7$	$e_k(7) \equiv 0$	mod26	$0 \mapsto A$
$O \mapsto 14$	$e_k(14) \equiv 23$	mod26	$23 \mapsto X$
$T \mapsto 19$	$e_k(19) \equiv 6$	mod26	$6 \mapsto G$

Το κωδικοποιημένο μήνυμα είναι AXG. Η αποκωδικοποίηση:

$A \mapsto 0$	$d_k(0) \equiv 7$	mod26	$7 \mapsto H$
$X \mapsto 23$	$d_k(23) \equiv 14$	mod26	$14 \mapsto O$
$G \mapsto 6$	$d_k(6) \equiv 19$	mod26	$19 \mapsto T$

Υπάρχουν και άλλα πιο πολύπλοκα και αρκετά πιο ασφαλή συμμετρικά κρυπτοσυστήματα. Όλα όμως έχουν δύο βασικά μειονεκτήματα. Το πρώτο είναι ότι δεν υπάρχει ασφαλής τρόπος μεταφοράς του κλειδιού ανάμεσα στα επικοινωνούντα μέλη. Το δεύτερο, ο μεγάλος αριθμός κλειδιών που χρειαζόμαστε. Αν για παράδειγμα 1000 άνθρωποι επικοινωνούν με διαφορετικό κλειδί ανα δύο τότε χρειάζονται $\binom{1000}{2} = 299 \cdot 1000/2 = 499500$ διαφορετικά κλειδιά.

Αυτό που χρειαζόμαστε είναι να κατασκευάσουμε τέτοια κρυπτοσυστήματα ώστε η συνάρτηση e_kνα είναι εύκολα υπολογίσιμη για να μπορούμε να στέλνουμε τα μηνύματα εύκολα και γρήγορα, ενώ η d_k να είναι αδύνατο να υπολογιστεί ακόμη και όταν η e_k είναι γνωστή. Σε αυτή την περίπτωση θα μπορούσαμε να δημοσιοποιήσουμε το κλειδί k χωρίς να κινδυνεύει να αποκρυπτογραφηθεί το μήνυμά μας από ανεπιθύμητους τρίτους. Σε αυτή την απλή ιδέα στηρίζεται η

4.6.2 Μη συμμετρική Κρυπτογραφία

Μια πρώτη ιδέα ήταν ότι ο πολλαπλασιασμός ακέραιων είναι, ιδιαίτερα για τον υπολογιστή, μια πάρα πολύ εύκολη πράξη. Ειδική περίπτωση είναι η ύψωση σε δύναμη. Η αντίστροφή της θα ήταν η παραγοντοποίηση δοθέντως φυσικού αριθμού n. Αυτό είναι σχεδόν αδύνατο όταν ο φυσικός αριθμός n έχει μεγάλο πλήθος ψηφίων. Η ιδέα ανήκει στους Diffie και Hellman (1976), και το πρώτο κρυπτοσύστημα που στηρίχθηκε σ' αυτή την ιδέα δόθηκε από τους Rivest-Shamir-Adlemann (1978) [17] και ονομάστηκε

RSA κρυπτοσύστημα

Ακολουθούμε τα ακόλουθα βήματα:

1. Επιλέγουμε δύο μεγάλους πρώτους αριθμούς
2. Υπολογίζουμε το γινόμενο $n = p \cdot q$
3. Υπολογίζουμε το
$$\varphi(n) = p \cdot q\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$$
4. Βρίσκουμε δύο ακέραιους a, b τέτοιους, ώστε το $ab - 1$να είναι πολλαπλάσιο του $\varphi(n)$.
5. Δημοσιοποιούμε τα n και b.
6. Τα a και τα p, q δεν δημοσιοποιούνται
7. Κωδικοποιούμε το x στο $x^b \mathrm{mod} n$, δηλαδή $e_k(x) = x^b \mathrm{mod} n$
8. Αποκωδικοποιούμε το y στο $y^a \mathrm{mod} n$, δηλαδή $d_k(y) \equiv y^d \mathrm{mod} n$.

Παρατήρηση 4.6.1. Στο βήμα (4), όταν επιλέξουμε κάποιο b, για να υπάρχει a τέτοιο ώστε $ba \equiv 1 \mathrm{mod} \varphi(n)$ πρέπει η ισοδυναμία

$$bx \equiv 1 \mathrm{mod} \varphi(n)$$

να έχει λύση, δηλαδή πρέπει $(b, \varphi(n)) = 1$. Συνεπώς επιλέγουμε ένα τέτοιο b και λύνουμε το κρυπτοσύστημα.

Θα πρέπει να αποδείξουμε ότι πράγματι είναι κρυπτοσύστημα, δηλαδή ότι

$$d_k(e_k(x)) = x \qquad \text{για κάθε } x \in \mathbb{Z}_n.$$

Αν $(x, n) = 1$, τότε ισχύει το Θεώρημα του Euler

$$x^{\varphi(n)} \equiv 1 \mathrm{mod} n.$$

Επομένως

$$d_k(e_k(x)) \equiv d_k(x^b) = x^{ab} \mathrm{mod} n.$$

Γράφουμε $ab = 1 + \varphi(n)t$ με $t \in \mathbb{Z}$ οπότε

$$d_k(e_k(x)) \equiv x^{1+\varphi(n)t} \equiv x(x^{\varphi(n)})^t \equiv x \mathrm{mod} n.$$

Θα αποδείξουμε ότι αυτό ισχύει και για κάθε x όταν $(x, n) > 1$. Επειδή $n = pq$ αν $(x, n) > 1$ τότε $x = p$ ή $x = q$ $(x < pq = n)$. Δεν χάνουμε τίποτε αν υποθέσουμε ότι $x = \alpha \cdot p$, με $(\alpha, p) = 1$. Θα αποδείξουμε λοιπόν ότι

$$p^{ab} = p \mathrm{mod} pq.$$

Η τελευταία ισοδυναμία ισχύει ακριβώς τότε όταν

$$p^{ab-1} \equiv 1 \mathrm{mod} q$$

δηλαδή ακριβώς τότε όταν

$$p^{\varphi(n)t} \equiv 1 \bmod q.$$

Η τελευταία όμως ισχύει διότι

$$p^{q-1} \equiv 1 \bmod q$$

οπότε και

$$\left(p^{q-1}\right)^{(p-1)t} \equiv 1 \bmod q.$$

Σημείωση: Η σχέση αυτή δεν ισχύει εν γένει αν ο n δεν είναι γινόμενο δύο, διαφορετικών μεταξύ τους πρώτων αριθμών.
Παράδειγμα. $n = 3 \cdot 4 = 12$, $\varphi(n) = 4$. Αν $b = 3$, $(3,4) = 1$ η ισοδυναμία

$$3x \equiv 1 \bmod 4$$

έχει λύση $a = 3$. Ας πάρουμε $x = 2$, $(2,12) = 2 > 1$, $(2^3)^3 \equiv 2^9 \not\equiv 2 \bmod 12$, αφού $2^9 \equiv 8 \bmod 12$.

Παραδείγματα RSA-κρυπτογράφησης

1. Ας πάρουμε $p = 3$ και $q = 11$, $n = pq = 33$.

$$\varphi(n) = \varphi(33) = (3-1)(11-1) = 20.$$

Επιλέγουμε $b = 3$, όπου $(3,20) = 1$. Η ισοδυναμία

$$3x \equiv 1 \bmod 20,$$

έχει λύση $a = 7$. Η Αλίκη κωδικοποιεί και στέλνει στον Βασιλάκη το μήνυμα

$$13, 31, 11, 11, 5$$

Ο Βασιλάκης αποκωδικοποιεί

$$\begin{aligned} 13 &\mapsto 13^7 = 33 \cdot \pi_1 + 7 \\ 31 &\mapsto 31^7 = 33 \cdot \pi_2 + 4 \\ 11 &\mapsto 11^7 = 33 \cdot \pi_3 + 11 \\ 5 &\mapsto 5^7 = 33 \cdot \pi_4 + 14 \end{aligned}$$

Το αποκωδικοποιούμε

7	4	11	11	14
↓	↓	↓	↓	↓
H	E	L	L	0

2. Ας πάρουμε $p = 47$ και $q = 59$.

$$n = p \cdot q = 47 \cdot 59 = 2773, \quad \varphi(n) = 2668.$$

Επιλέγουμε $b = 17$, $(17, 2668) = 1$. Λύνουμε την ισοδυναμία

$$17x \equiv 1 \bmod 2668$$

και βρίσκουμε $a = 157$. Υποθέτουμε ότι θέλουμε να κρυπτογραφήσουμε το μήνυμα “Its all go”. Το χωρίζουμε σε ζευγάρια. (Αν κρυπτογραφούμε ένα-ένα τα γράμματα τότε μπορεί το 0 ή το 1 να μας ... προδώσουν!

IT	S ∅	AL	L ∅	GO
0920	1900	0112	1200	0715

Κωδικοποίηση

$$0920^{17} \equiv 0948 \mathrm{mod} 2713$$

Αποκρυπτογράφηση

$$948^{157} \equiv 920 \mathrm{mod} 2273$$

και το 920 αντιστοιχεί στο IT. Ομοίως και τα υπόλοιπα.

ISBN και Θεωρία της Κωδικοποίησης

Όλα τα βιβλία στο πίσω μέρος του εξωφύλλου τους έχουν τον συμβολισμό ISBN ο οποίος σημαίνει International Standard Book Number και ακολουθείται από έναν δεκαψήφιο αριθμό χωριζόμενο σε τέσσερα μέρη από τρεις παύλες ¨-¨.

Ο αριθμός αυτός χαρακτηρίζει τη συγκεκριμένη έκδοση. Το πρώτο μέρος χαρακτηρίζει τη χώρα έκδοσης. Για τις ΗΠΑ είναι το μηδέν για τη Γερμανία το τρία, την Ινδία το 81 κοκ. Το δεύτερο μέρος χαρακτηρίζει τον εκδοτικό οίκο. Έτσι ο διεθνούς φημισμένος οίκος έκδοσης μαθηματικών βιβλίων ο Springer χαρακτηρίζεται από τον αριθμό 540. Το τρίτο μέρος χαρακτηρίζει τη συγκεκριμένη έκδοση. Για παράδειγμα το βιβλίο των Martin Aigner και Günter M. Ziegler, *Proofs from the Book*, χαρακτηρίζεται από τον αριθμό 40460.

Τι παριστάνει όμως το τέταρτο μέρος το αριθμού; Πρόκειται για ένα ψηφίο ελέγχου της ορθότητας των προηγουμένων.

Αν τα πρώτα 9 ψηφία του αριθμού είναι τα a_1, a_2, ..., a_9, τότε το a_{10} ορίζεται από την ισοδυναμία:

$$\sum_{i=1}^{10} i a_i \equiv 0 \mathrm{mod} 11$$

ή ισοδύναμα

$$a_{10} \equiv \sum_{i=1}^{9} i a_i \mathrm{mod} 11.$$

Αν, για παράδειγμα, τα πρώτα 9 ψηφία του αριθμού είναι 3-540-40460-□, τότε το τελευταίο ψηφίο ελέγχου θα είναι

$$\begin{aligned} a_{10} &\equiv 13 + 2 \cdot 5 + 3 \cdot 4 + 4 \cdot 0 + 5 \cdot 4 + 6 \cdot 0 + 7 \cdot 4 + 8 \cdot 6 + 9 \cdot 0 \\ &\equiv 3 + 10 + 12 + 5 + 54 + 7 + 18 \equiv 0 \mathrm{mod} 11. \end{aligned}$$

Άρα $a_{10} = 0$.

Αν τώρα έχουμε τον αριθμό $3 - 540 - 19102$ τότε

$$\begin{aligned} a_{10} &\equiv 1 \cdot 3 + 2 \cdot 5 + 3 \cdot 4 + 4 \cdot 0 + 5 \cdot 1 + 6 \cdot 9 + 7 \cdot 1 + 8 \cdot 0 + 9 \cdot 2 \\ &= 3 + 10 + 12 + 5 + 54 + 7 + 18 \equiv 10 \mathrm{mod} 11 \end{aligned}$$

Επειδή ο 10 είναι διψήφιος στην τελευταία θέση του ISBN μπαίνει το γράμμα «X», ISBN 3-540-19102-X.

Αν υποθέσουμε ότι κατά την εκτύπωση στο ISBN έχει γίνει ακριβώς ένα λάθος, τότε αυτό εύκολα ανιχνεύεται, αφού αν υποθέσουμε ότι στη θέση του a_j μπήκε κάποιο άλλο ψηφίο a'_j, τότε αν γράψουμε $a'_j = a_j + b$, $(-9 \leq b \leq)$, έχουμε

$$\sum_{\substack{i=1 \\ i\neq j}} ia_i + ja'_j = \sum_{i=1}^{10} ia_i + jb \equiv jb \bmod 11.$$

Επειδή $11 \nmid j$, $11 \nmid b$ έπεται ότι

$$\sum_{\substack{i=1 \\ i\neq j}} a_i + ja'_i \not\equiv 0 \bmod 11.$$

το οποίο σημαίνει ότι το λάθος έχει ανιχνευθεί.

Παρατηρήσεις:

1. Είμαστε σε θέση να ανιχνεύσουμε ένα το πολύ λάθος, δεν είμαστε όμως σε θέση να το διορθώσουμε.
2. Εύκολα βλέπουμε επίσης ότι μπορούμε να ανιχνεύσουμε την ύπαρξη αντιμετάθεσης μεταξύ δύο διαφορετικών μεταξύ τους ψηφίων του ISBN (άσκηση).
3. Το ISBN αποτελεί ένα απλό παράδειγμα ενός γενικότερου κλάδου των Μαθηματικών ο οποίος ασχολείται με την ανίχνευση και διόρθωση λαθών τα οποία δημιουργούνται κυρίως κατά τη μεταφορά ενός μηνύματος μέσω ενός καναλιού και λέγεται «Θεωρία της Κωδικοποίησης».
4. Υπάρχει και ISBN για την ηλεκτρονική έκδοση βιβλίων το οποίο αρχίζει με 978 και έχει συνολικά 13 ψηφία.

4.7 Ισοδυναμίες ανωτέρου βαθμού

Σύμφωνα με τα προηγούμενα, για να μελετήσουμε ισοδυναμίες ανωτέρου βαθμού, αρκεί να μελετήσουμε ισοδυναμίες της μορφής

$$f(x) \equiv 0 \bmod p^\ell,$$

όπου $f(x)$ πολυώνυμο με ακέραιους συντελεστές βαθμού $\deg f(x) \geq 2$, $p \in \mathbb{P}$ και $\ell \geq 1$.

Η παράγωγος του πολυωνύμου

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

ορίζεται ως εξής:

$$f'(x) = \sum_{k=0}^{n} k a_k x^{k-1}.$$

Στα επόμενα χρήσιμη θα είναι η ακόλουθη:

Πρόταση 4.7.1. *Αν $a, b \in \mathbb{Z}$ τότε*

$$f(a+b) = f(a) + bf'(a) + b^2 m,$$

για κάποιο $m \in \mathbb{Z}$, $m = m(a, b, n)$.

Απόδειξη. Από το διωνυμικό τύπο για $k > 1$ προκύπτει ότι

$$(a+b)^k = a^k + ka^{k-1}b + b^2 m_k$$

με $m_k = \sum_{i=2}^{k} \binom{k}{i} a^{k-i} b^{i-2} \in \mathbb{Z}$.

Επομένως

$$\begin{aligned} f(a+b) &= \sum_{k=0}^{n} a_k (a+b)^k \\ &= \sum_{k=2}^{n} a_k (a^k + kba^{k-1} + b^2 m_k) + a_1(a+b) + a_0 \\ &= \sum_{k=0}^{n} a_k a^k + b \sum_{k=1}^{n} k a_k a^{k-1} + b^2 \sum_{k=2}^{n} a_k m_k \\ &= f(a) + bf'(a) + b^2 \cdot m, \text{ με } m = \sum_{k=2}^{n} a_k m_k \in \mathbb{Z}. \end{aligned}$$

□

Το επόμενο θεώρημα μας δείχνει πώς από την γνωστή λύση της ισοδυναμίας

$$f(x) \equiv 0 \bmod p$$

προκύπτουν διαδοχικά οι λύσεις της

$$f(x) \equiv 0 \bmod p^i$$

για $i = 2, 3, \ldots, \ell$.

Πρόταση 4.7.2. *Το x_0 είναι λύση της ισοδυναμίας*

$$f(x) \equiv 0 \bmod p^\ell, \quad \ell \geq 2$$

ακριβώς τότε όταν

$$x_0 = \alpha + y_0 p^{\ell-1},$$

όπου α λύση της

$$f(x) \equiv 0 \bmod p^{\ell-1}$$

και y_0 λύση της

$$\frac{f(\alpha)}{p^{\ell-1}} + yf'(\alpha) \equiv 0 \bmod p$$

(τα α και y_0 μπορούν να επιλεγούν έτσι ώστε $0 \leq \alpha < p^{\ell-1}$ και $0 \leq y_0 < p$)

Απόδειξη. Κάθε λύση x_0 της ισοδυναμίας $f(x) \equiv 0 \bmod p^\ell$ είναι και λύση της $f(x) \equiv 0 \bmod p^{\ell-1}$. Συνεπώς, $x_0 = \alpha + y_0 p^{\ell-1}$, όπου α λύση της ισοδυναμίας $f(x) \equiv 0 \bmod p^{\ell-1}$, $0 \leq \alpha < p^{\ell-1}$ και $y_0 \in \mathbb{Z}$.

Επειδή σύμφωνα με την πρόταση 4.7.1

$$f(\alpha + y_0 p^{\ell-1}) = f(\alpha) + y_0 p^{\ell-1} f'(\alpha) + (y_0 p^{\ell-1})^2 \cdot m$$

έπεται ότι

$$f(\alpha + y_0 p^{\ell-1}) \equiv 0 \bmod p^{\ell}$$

ακριβώς τότε όταν

$$f(\alpha) + y_0 p^{\ell-1} f'(\alpha) \equiv 0 \bmod p^{\ell}$$

(Παρατηρήστε $p^{2\ell-2} \geq p^{\ell}$ για $\ell \geq 2$).

Επειδή $f(a) \equiv 0 \bmod p^{\ell-1}$, η τελευταία ισοδυναμία γράφεται (ισοδύναμα) στη μορφή:

$$\frac{f(\alpha)}{p^{\ell-1}} + y_0 f'(\alpha) \equiv 0 \bmod p.$$

Επομένως, ο $\alpha + y_0 \cdot p^{\ell-1}$ είναι λύση της ισοδυναμίας $f(x) \equiv 0 \bmod p^{\ell}$ ακριβώς τότε όταν το y_0 είναι λύση της

$$\frac{f(\alpha)}{p^{\ell-1}} + y f'(\alpha) \equiv 0 \bmod p.$$

Η τελευταία γραμμική ισοδυναμία έχει

- ακριβώς p λύσεις $\bmod p$ αν και μόνο αν $p \mid f'(\alpha)$ και $p^{\ell} \mid f(\alpha)$.
- ακριβώς μία λύση $\bmod p$ αν και μόνο αν $p \nmid f'(\alpha)$
- καμία λύση $\bmod p$ αν και μόνο αν $p \mid f'(\alpha)$ και $p^{\ell} \nmid f(\alpha)$

Τέλος, αν y_0 λύση της ισοδυναμίας

$$\frac{f(\alpha)}{p^{\ell-1}} + y f'(\alpha) \equiv 0 \bmod p$$

και $y_0 + sp$, $s \in \mathbb{Z}$ είναι επίσης λύση. Επίσης ισχύει,

$$\alpha + (y_0 + sp)p^{\ell-1} = \alpha + y_0 p^{\ell-1} + sp^{\ell} \equiv \alpha + y_0 p^{\ell-1} \bmod p^{\ell}.$$

Αυτό σημαίνει ότι η $y_0 + sp$ δίνει την ίδια λύση $\bmod p^{\ell}$ με αυτήν που δίνει και η y_0 δηλαδή μπορούμε να επιλέξουμε το y_0 έτσι ώστε να ισχύει $0 \leq y_0 < p$. □

Παράδειγμα. Να λυθεί η ισοδυναμία:

$$f(x) := x^3 + x + 1 \equiv 0 \bmod 27$$

Λύση: Θα πρέπει να βρούμε διαδοχικά τις λύσεις των ισοδυναμιών

$$f(x) \equiv 0 \bmod 3 \tag{4.7.1}$$
$$f(x) \equiv 0 \bmod 3^2 \tag{4.7.2}$$
$$f(x) \equiv 0 \bmod 3^3 \tag{4.7.3}$$

Για την εξίσωση 4.7.1 παρατηρούμε: Επειδή $f(0) = 1 \not\equiv 0 \bmod 3$, $f(1) \equiv 3 \equiv 0 \bmod 3$ και $f(2) = 11 \equiv 2 \not\equiv 0 \bmod 3$, έπεται ότι η μοναδική λύση της (4.7.1) είναι η $a = 1$.

$f(1) = 3$ $f'(1) = 4$. Η ισοδυναμία

$$\frac{f(1)}{3} + y f'(1) \equiv 0 \bmod 3$$

γράφεται ισοδύναμα

$$1 + 4y \equiv 0 \mathrm{mod} 3$$

που έχει λύση $y \equiv 2 \mathrm{mod} 3$. Θέτουμε $y_0 = 2$, επομένως ο

$$x_0 = a + y_0 p^{\ell - 1} = 1 + 2 \cdot 3^{2-1} = 7$$

είναι η μοναδική λύση της (4.7.2).

Ο $a = 7$ είναι λύση της ισοδυναμίας (4.7.2). υπολογίζουμε ότι $f(7) = 351$, $f'(7) = 148$. Η ισοδυναμία

$$\frac{f(7)}{9} + y f'(7) \equiv 0 \mathrm{mod} 3$$

η οποία ισοδύναμα γράφεται

$$y \equiv 0 \mathrm{mod} 3$$

και έχει μοναδική λύση $y_0 = 3$. Επομένως η μοναδική λύση της (4.7.3) είναι η

$$x_0 = 7 \mathrm{mod} 27.$$

Παράδειγμα. Να λυθεί η ισοδυναμία:

$$x^3 + x + 1 \equiv 0 \mathrm{mod} 25$$

Λύση: $f(x) := x^3 + x + 1$. $f(0) = 1 \not\equiv 0 \mathrm{mod} 5$, $f(1) = 3 \not\equiv 0 \mathrm{mod} 5$, $f(2) = 11 \not\equiv 0 \mathrm{mod} 5$, $f(3) = f(-2) = -9 \not\equiv 0 \mathrm{mod} 5$, $f(4) \equiv f(-1) = -1 \not\equiv 0 \mathrm{mod} 5$. Δεν έχουμε ρίζα, άρα ούτε η αρχική έχει.

Παράδειγμα. Να λυθεί η ισοδυναμία

$$x^3 + x + 1 \equiv 0 \mathrm{mod} 121$$

Λύση $f(x) := x^3 + x + 1$. Η $f(x) \equiv 0 \mathrm{mod} 11$ έχει μοναδική λύση $a = 2$. Επίσης, $f(2) = 11$, $f'(2) = 13$. Η ισοδυναμία

$$\frac{f(2)}{11} + y f'(2) \equiv 0 \mathrm{mod} 11,$$

γράφεται $2y \equiv 10 \mathrm{mod} 11$ και έχει μοναδική λύση την $y_0 = 5$. Επομένως η μοναδική λύση της ισοδυναμίας

$$x^3 + x + 1 \equiv 0 \mathrm{mod} 121$$

είναι η $x_0 \equiv a + y_0 \cdot 11 = 2 + 5 \cdot 11 \equiv 57 \mathrm{mod} 121$.

Παράδειγμα. Να λυθεί η ισοδυναμία:

$$f(x) = x^3 + x + 1 \mathrm{mod} 3267.$$

Λύση: Αναλύουμε το μέτρο σε γινόμενο παραγόντων $3267 = 3^3 \cdot 11^2$. Αρκεί επομένως να λύσουμε το σύστημα

$$\begin{aligned} f(x) &\equiv 0 \mathrm{mod} 27 \\ f(x) &\equiv 0 \mathrm{mod} 121 \end{aligned}$$

Η πρώτη ισοδυναμία έχει λύση $x \equiv 7 \bmod 27$ ενώ η δεύτερη $x \equiv 57 \bmod 121$. Επομένως πρέπει να λύσουμε το σύστημα

$$\begin{aligned} x &\equiv 7 \bmod 27 \\ x &\equiv 57 \bmod 121 \end{aligned}$$

Ο μέγιστος κοινός διαιρέτης $(27, 121) = 1$, άρα υπάρχει μοναδική λύση $\bmod 3267$ την οποία την υπολογίζουμε κατά τα γνωστά ως $2356 \bmod 3267$.

Παράδειγμα. Να λυθούν οι ισοδυναμίες

$$\begin{aligned} x^3 - x^2 + 7x + 1 &\equiv 0 \bmod 8 \\ x^3 - x^2 + 7x + 1 &\equiv 0 \bmod 25 \\ x^3 - x^2 + 7x + 1 &\equiv 0 \bmod 200 \end{aligned}$$

Λύση: Εφαρμόζουμε την παραπάνω μέθοδο και βρίσκουμε ότι η πρώτη έχει τις λύσεις

$$x \equiv 1, 3, 5, 7 \bmod 8$$

και η δεύτερη τη λύση

$$x \equiv 23 \bmod 25.$$

Επομένως οι λύσεις της τρίτης ισοδυναμίας προκύπτουν ως οι λύσεις των τεσσάρων συστημάτων

$$\begin{array}{cccc} x \equiv 1 \bmod 8 & x \equiv 3 \bmod 8 & x \equiv 5 \bmod 8 & x \equiv 7 \bmod 8 \\ x \equiv 23 \bmod 25 & x \equiv 23 \bmod 25 & x \equiv 23 \bmod 25 & x \equiv 23 \bmod 25 \end{array}$$

και αυτές είναι οι $x \equiv 23, 73, 123, 173 \bmod 200$. Από τα παραπάνω είναι φανερό είναι ότι η λύση κάθε πολυωνυμικής ισοδυναμίας

$$f(x) \equiv \bmod m$$

ανάγεται τελικά στη λύση ισοδυναμιών της μορφής

$$f(x) \equiv 0 \bmod p$$

όπου p πρώτος αριθμός. Στα προηγούμενα παραδείγματα βοηθούσε το γεγονός ότι οι πρώτοι αριθμοί ήταν μικροί οπότε δοκιμάζαμε όλες τις δυνατές περιπτώσεις $x \bmod p$ για να βρούμε τις ρίζες.

Αλλά τι μπορούμε να πούμε στη γενική περίπτωση;

Η πρώτη παρατήρηση είναι ότι μας φτάνει να ελέγξουμε πολυωνυμικές ισοδυναμίες

$$f(x) \equiv 0 \bmod p$$

για πολυώνυμα $f(x)$ βαθμού $\deg f(x) < p$.

Θα λέμε ότι δυο ισοδυναμίες (ισοτιμίες) $f(x) \equiv 0 \bmod m$ και $g(x) \equiv 0 \bmod m$ είναι ισοδύναμες όταν έχουν ακριβώς τις ίδιες λύσεις.

Πρόταση 4.7.3. *Κάθε ισοδυναμία (ισοτιμία)*

$$f(x) \equiv 0 \bmod p$$

όπου $\deg f(x) \geq p$ *και* p *πρώτος αριθμός, είναι ισοδύναμη προς μια ισοτιμία*

$$r(x) \equiv 0 \bmod p$$

με $\deg r(x) < p$.

Απόδειξη. Στο $\mathbb{Z}[x]$ ισχύει η ευκλείδια διαίρεση με υπόλοιπο[3]. Διαιρούμε το πολυώνυμο $f(x)$ με το $\pi(x) := x^p - x$. Υπάρχουν πολυώνυμα $q(x) \in \mathbb{Z}[x]$ και $r(x) \in \mathbb{Z}[x]$ τέτοια ώστε

$$f(x) = q(x)\pi(x) + r(x)$$

με $\deg r(x) < \deg \pi(x) = p$ ή $r(x) = 0$. Σύμφωνα με το θεώρημα του Fermat έχουμε $a^p \equiv a \mathrm{mod} p$ για κάθε $a \in \mathbb{Z}$. Συνεπώς για κάθε $a \in \mathbb{Z}$

$$f(a) \equiv r(a) \mathrm{mod} p$$

Άρα οι ισοτιμίες $f(x) \equiv 0 \mathrm{mod} p$ και $r(x) \equiv 0 \mathrm{mod} p$ είναι ισοδύναμες. □

Από την Άλγεβρα του σχολείου γνωρίζουμε ότι η πολυωνυμική εξίσωση

$$f(x) = 0,$$

έχει το πολύ n ρίζες, όπου $n = \deg(f)$ ο βαθμός του πολυωνύμου $f(x)$.

Με τις ισοτιμίες δεν ισχύει το ίδιο. Η ισοτιμία

$$3x \equiv 6 \mathrm{mod} 9$$

είναι γραμμική αλλά έχει τρεις λύσεις. Στο προηγούμενο παράδειγμα, οι ισοτιμίες είναι κυβικές αλλά έχουν $4, 1$ και 4 λύσεις αντίστοιχα. Όταν όμως το μέτρο της ισοδυναμίας είναι πρώτος αριθμός τότε ισχύει το

Πρόταση 4.7.4 (Lagrange). *Αν $f(x) = \sum_{i=0}^{n} a_i x^i$ πολυώνυμο βαθμού $n \geq 1$ με ακέραιους συντελεστές και $a_n \not\equiv 0 \mathrm{mod} p$, τότε η ισοτιμία*

$$f(x) \equiv 0 \mathrm{mod} p$$

έχει το πολύ n-λύσεις mod$p$.

Απόδειξη. Επαγωγικά ως προς n. Για $n = 1$ $f(x) = a_1 x + a_0$ με $a_1 \not\equiv 0 \mathrm{mod} p$. Είναι γνωστό οτι η ισοτιμία έχει ακριβώς μία λύση, αφού το a_1 είναι αντιστρέψιμο mod$p$.

Υποθέτουμε ότι η πρόταση ισχύει για όλα τα πολυώνυμα $f(x)$ βαθμού $n \geq 1$ για τα οποία ισχύει $a_n \not\equiv 0 \mathrm{mod} p$.

Θα αποδείξουμε ότι ισχύει για όλα τα πολυώνυμα βαθμού $n + 1$. Ας υποθέσουμε ότι υπάρχει ένα πολυώνυμο $f(x)$, βαθμού $n + 1$ με $a_{n+1} \not\equiv 0 \mathrm{mod} p$ και τουλάχιστο $(n + 2)$-λύσεις mod$p$.

Αν a μια λύση αυτού, τότε υπάρχουν ένα πολυώνυμο $q(x)$ με ακέραιους συντελεστές και βαθμού n και ένας ακέραιος r, τέτοιοι ώστε

$$f(x) = (x - a)q(x) + r.$$

Ο συντελεστής του x^n στο $q(x)$ είναι ο a_{n+1} για τον οποίο ισχύει $a_{n+1} \not\equiv 0 \mathrm{mod} p$. Σύμφωνα με την υπόθεση της μαθηματικής επαγωγής το $q(x)$ έχει το πολύ n λύσεις mod$p$.

Επειδή

$$f(a) \equiv 0 \mathrm{mod} p$$

έπεται ότι $r \equiv 0 \mathrm{mod} p$ από την οποία προκύπτει[4]

$$f(x) \equiv (x - a)q(x) \mathrm{mod} p.$$

[3] Αυτό ισχύει γιατί ο συντελεστής του μεγιστοβάθμιου όρου του πολυωνύμου είναι 1

[4] Δύο πολυώνυμα $f(x), g(x)$ είναι ισοδύναμα mod$p$ ακριβώς τότε αν έχουν το ίδιο βαθμό και οι αντίστιχοι ομόβαθμοι συντελεστές είναι ισότιμοι mod$p$.

Αν b κάποια άλλη λύση $b \not\equiv a \bmod p$ τότε $f(b) \equiv 0 \bmod p$, οπότε $(b-a)q(b) \equiv 0 \bmod p$. Επειδή $b \not\equiv a \bmod p$ έπεται ότι $q(b) \equiv 0 \bmod p$, δηλαδή ότι το b είναι λύση της ισοδυναμίας $q(x) \equiv 0 \bmod p$. Αποδείξαμε ότι κάθε λύση b της $f(x) \equiv 0 \bmod p$ είναι και λύση της $q(x) \equiv 0 \bmod p$. Αυτό σημαίνει ότι η $q(x) \equiv 0 \bmod p$ έχει τουλάχιστον $(n+1)$-λύσεις το όποιο είναι άτοπο. Συνεπώς η $f(x) \equiv 0 \bmod p$ έχει το πολύ $(n+1)$-λύσεις. □

Για μια διαφορετική απόδειξη της πρότασης δες [24, σελ. 72-73] και [14, πρόταση 2.15].

Σύμφωνα με το θεώρημα του Fermat η εξίσωση $x^p - x$ έχει ακριβώς p-λύσεις $\bmod p$, άρα το παραπάνω φράγμα των λύσεων είναι βέλτιστο.

Άμεση συνέπεια της παραπάνω πρότασης είναι το ακόλουθο:

Πόρισμα 4.7.5. *Αν η ισοτιμία $f(x) \equiv 0 \bmod p$, όπου $f(x) = \sum_{i=0}^{n} a_i x^i$ και p πρώτος αριθμός που έχει περισσότερες από n λύσεις τότε όλοι οι συντελεστές του πολυωνύμου διαιρούνται με p.*

Απόδειξη. Αν υπάρχει κάποιος συντελεστής που δεν διαιρείται με p, τότε η πολυωνυμική ισοδυναμία

$$f(x) \equiv 0 \bmod p$$

έχει βαθμό φυσικό αριθμό μικρότερο ή ίσο του n. Σύμφωνα με το θεώρημα Lagrange, η ισοτιμία έχει το πολύ n λύσεις $\bmod p$, άτοπο, □

Μια δεύτερη εφαρμογή είναι το

Πόρισμα 4.7.6. *Αν $d \mid (p-1)$ τότε η ισοτιμία*

$$x^d \equiv 1 \bmod p$$

έχει ακριβώς d-λύσεις.

Απόδειξη. Σύμφωνα με το θεώρημα του Lagrange η ισοτιμία έχει το πολύ d λύσεις. Θα αποδείξουμε ότι έχει ακριβώς d.

Λόγω της υπόθεσης ότι $d \mid (p-1)$ έπεται ότι υπάρχει $\ell \in \mathbb{Z}$ τέτοιο ως $d\ell = p-1$. Επομένως

$$x^{p-1} - 1 = (x^d - 1)f(x),$$

όπου

$$f(x) = x^{d(\ell-1)} + x^{d(\ell-2)} + \cdots + x^d + 1.$$

Από το θεώρημα του Lagrange και πάλι προκύπτει ότι η ισοτιμία

$$f(x) \equiv 0 \bmod p$$

δεν μπορεί να έχει περισσότερες από $(p-1-d)$-λύσεις. Επομένως αν η ισοτιμία είχε λιγότερες από d, τότε και η ισοτιμία

$$x^{p-1} \equiv 1 \bmod p$$

θα είχε λιγότερες από $p-1$, άτοπο αφού η τελευταία ισοτιμία έχει ακριβώς $(p-1)$-λύσεις, τις $x = 1, 2, \ldots, p-1 \bmod p$. □

Σαν τρίτη εφαρμογή του θεωρήματος του Lagrange παρουσιάζουμε μια αξιοσημείωτη ιδιότητα των πρώτων αριθμών, γνωστή στη βιβλιογραφία ως

Θεώρημα 4.7.7 (Wilson)**.** *Για κάθε πρώτο αριθμό ισχύει:*

$$(p-1)! \equiv -1 \mathrm{mod} p.$$

Απόδειξη. Θεωρούμε το πολυώνυμο

$$\begin{aligned} f(X) &= \prod_{i=1}^{p-1}(X-i) - (X^{p-1}-1) \\ &= a_{p-2}X^{p-2} + a_{p-3}X^{p-3} + \cdots + a_1 X + a_0. \end{aligned}$$

Η ισοδυναμία $f(X) \equiv 0 \mathrm{mod} p$ έχει $(p-1)$-λύσεις $\mathrm{mod} p$, τις $1, 2, \ldots, (p-1)$. Ο βαθμός του πολυωνύμου είναι $(p-2)$. Επομένως, σύμφωνα με το πόρισμα 4.7.5 ισχύει

$$a_{p-2} \equiv a_{p-1} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \mathrm{mod} p.$$

Για $X = p$ η ισοδυναμία γίνεται

$$\prod_{i=1}^{p-1}(p-i) \equiv (p^{p-1}-1) \mathrm{mod} p,$$

δηλαδή

$$(p-1)! \equiv -1 \mathrm{mod} p$$

□

Παρατήρηση 4.7.8. Ισχύει και το αντίστροφο

Πρόταση 4.7.9. *Αν n φυσικός, $n \geq 1$ τέτοιος ώστε $(n-1)! \equiv -1 \mathrm{mod} n$, τότε ο n είναι πρώτος.*

Απόδειξη. Αν ο n δεν ήταν πρώτος, τότε θα υπήρχε p πρώτος $p < n$, $p \mid n$. Αλλά τότε $p \mid (n-1)!$, αφού $p < n$. Επομένως θα είχαμε $p \mid n$ και $p \mid (n-1)!$, δηλαδή $p \mid 1$, άτοπο. □

Παρατήρηση 4.7.10. Από το θεώρημα του Wilson προκύπτει ότι υπάρχει άπειρο πλήθος σύνθετων ακέραιων της μορφής $n! + 1$. Δεν είναι, μέχρι σήμερα γνωστό, αν υπάρχει και άπειρο πλήθος πρώτων της μορφής αυτής.

Το θεώρημα του Wilson μας δίνει ένα όμορφο αλλά όχι πρακτικό κριτήριο ελέγχου πρώτων αριθμών. Στο θέμα αυτό θα επανέλθουμε στις επόμενες δύο παραγράφους.

Ακολουθούν δύο ακόμα εφαρμογές του θεωρήματος του Wilson:

Πρόταση 4.7.11 (Wolstenholme 1862)**.** *Αν p περιττός πρώτος, τότε ο αριθμητής του κλάσματος (εννοείται σε ανάγωγη μορφή)*

$$\mathcal{K} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

διαιρείται με p και αν $p > 3$ διαιρείται με p^2.

Απόδειξη. Κάνουμε τα κλάσματα ομώνυμα

$$\mathcal{K} = \frac{b_1 + b_2 + \cdots b_{p-1}}{(p-1)!},$$

όπου $b_i = \frac{(p-1)!}{i}$. Λόγω του θεωρήματος Wilson 4.7.7 το $p \nmid (p-1)!$. Θεωρούμε το πολυώνυμο

$$f(X) = \prod_{i=1}^{p-1}(X-i) - (X^{p-1}-1) = a_{p-2}X^{p-2} + a_{p-3}X^{p-3} + \cdots + a_2X^2 + a_1X + a_0.$$

Όπως και στο θεώρημα του Wilson, το πολυώνυμο αυτό έχει $(p-1)$-ρίζες, τους αριθμούς $1, 2, \ldots, (p-1)$ και βαθμό $p-2$. Επομένως όλοι οι συντελεστές αυτού $a_i \equiv 0 \bmod p$ για κάθε $i = 0, \ldots, p-2$. Από τις σχέσεις ριζών συντελεστών έχουμε ότι ο συντελεστής a_1 είναι ο αντίθετος του αθροίσματος όλων των γινομένων των $(p-1)$-ριζών ανά $p-2$. Επομένως

$$a_1 = -(b_1 + b_2 + \cdots + b_{p-1}).$$

Επειδή $p \mid a_1$, έπεται ότι p διαιρεί τον αριθμητή του κλάσματος $\mathcal{K}$, $b_1+b_2+\cdots+b_{p-1}$. Παρατηρούμε ότι

$$f(p) = (p-1)! + 1 - p^{p-1} = a_{p-2}p^{p-2} + \cdots + a_2p^2 + a_1p + a_0$$

και ότι $a_0 = (p-1)! + 1$. Επομένως, $-p^{p-1} = a_{p-2}p^{p-2} + \cdots + a_2p^2 + a_1p$. Απλοποιούμε με p και έχουμε

$$a_1 = -p^{p-2} - a_{p-2}p^{p-3} - \cdots a_2p,$$

το οποίο διαιρείται με p^2, αφού $p \mid a_2$. □

Πρόταση 4.7.12. *Υποθέτουμε ότι $n \geq 2$. Οι φυσικοί αριθμοί $n, n+2$ αποτελούν ζευγάρι δίδυμων ακριβώς τότε όταν*

$$4[(n-1)! + 1] + n \equiv 0 \bmod n(n+2).$$

Απόδειξη. Υποθέτουμε ότι $n \in \mathbb{P}$ και $n+2 \in \mathbb{P}$. Είναι φανερό ότι $n \neq 2$. Από το θεώρημα του Wilson, έπεται ότι

$$(n-1)! + 1 \equiv 0 \bmod n \text{ και } (n+1)! + 1 \equiv 0 \bmod (n+2)$$

Επομένως

$$4[(n-1)! + 1] + n \equiv 0 \bmod n$$

και από την $(n+1)! + 1 \equiv 0 \bmod (n+2)$ προκύπτει ότι

$$(n-1)!n(n+1) + 1 \equiv 0 \bmod (n+2).$$

Το $n(n+1) = (n+2)(n-1) + 2$. Άρα, έχουμε

$$2(n-1)! + 1 \equiv 0 \bmod n+2$$

Επειδή $n, n+2$ πρώτοι έχουμε $(n, n+2) = 1$ και συνεπώς το ζητούμενο.

Αντίστροφα, προφανώς η ισοτιμία δεν ισχύει για $n = 2, 4$. Άρα $n \neq 2, 4$. Επομένως, ισχύει $(n-1)! + 1 \equiv 0 \bmod n$, οπότε από το αντίστροφο του Θεωρήματος Wilson έχουμε $n \in \mathbb{P}$.

Επίσης

$$4(n-1)! + 4 + n \equiv 4(n-1)! + 2 \bmod (n+2)$$

Επομένως $4(n-1)! + 2 \equiv 0 \bmod (n+2)$. Πολλαπλασιάζουμε με $n(n+1)$ και καταλήγουμε

$$4(n+1)! + 2n(n+1) \equiv 0 \bmod (n+2)$$

άρα

$$4[(n+1)! + 1] + 2n^2 + 2n - 4 \equiv 0 \bmod n(n+2)$$

επομένως $(n+1)! + 1 \equiv 0 \bmod (n+2)$. Από το αντίστροφο του Θεωρήματος Wilson έπεται $n+1 \in \mathbb{P}$, δηλαδή οι n και $n+2$ δίδυμοι πρώτοι. □

Ιστορικά 4.7.1

Όταν ο Euler εγκατέλειψε το Βερολίνο στο 1766 για να αποδεχτεί τη θέση στην Ακαδημία της Αγίας Πετρούπολης που του πρόσφερε η Αικατερίνη η Μεγάλη, ο Φρειδερίκος ο Μέγας κάλεσε στην Πρωσική Ακαδημία τον Lagrange (1736-1813). Η πιο παραγωγική περίοδος του Lagrange η σχετική με θέματα Θεωρίας Αριθμών είναι η από το 1766 μέχρι το 1787, ο χρόνος που έμενε στο Βερολίνο. Στο διάστημα αυτό απέδειξε και το ομώνυμο θεώρημα.

Ιστορικά 4.7.2

Ορόσημο στην πορεία της εξέλιξης της Θεωρίας Αριθμών απετέλεσε η έκδοση του «Meditationes Arithmeticae (1770)» του Άγγλου μαθηματικού Edward Waring (1741-1793). Στο βιβλίο του αυτό ανακοινώνει διάφορα αποτελέσματα Θεωρίας Αριθμών. Ένα από αυτά είναι και η εικασία που έθεσε ο μαθητής του John Wilson ότι αν p πρώτος τότε

$$(p-1)! \equiv -1 \mathrm{mod} p.$$

Ο Waring πρόσεθεσε ότι: «Θεωρήματα αυτού του είδους είναι δύσκολο να αποδειχτούν λόγω έλλειψης συμβολισμού έκφρασης των πρώτων αριθμών...»
«...Theorems of this kind will be very hard to prove, because of the absense of a notation to express prime numbers..»
Χειρόγραφα του Leibniz αποδεικνύουν ότι το θεώρημα θα πρέπει να ήταν γνωστό στον ίδιο από το 1683.
Η πρώτη απόδειξη δημοσιεύτηκε από τον Lagrange στα 1771. Αργότερα ο Gauss σκέφτηκε μια απόδειξη μέσε σε πέντε λεπτά στον δρόμο προς το σπίτι του. Η απόδειξη του Gauss περιέχεται στην πρόταση 77 των Disquisitiones Arithmiticae και είναι η εξής: Η πρόταση ισχύει για $p = 2$, αφού $(2-1)! \equiv 1 \equiv -1 \mathrm{mod} 2$. Επίσης ισχύει για $p = 3$ αφού $(3-1)! = 2! = 2 \equiv -1 \mathrm{mod} 3$. Υποθέτουμε ότι $p > 5$. Αν a οποιοσδήποτε από τους αντιπροσώπους $1, 2, 3, \ldots, p-1$, η ισοδυναμία $ax \equiv 1 \mathrm{mod} p$ έχει μοναδική λύση. Επομένως υπάρχει μοναδικό a', $1 \leq a' \leq p-1$ τέτοιο ώστε $aa' \equiv 1 \mathrm{mod} p$. Αντίστροφα, αν μας δοθεί το a', τότε σε αυτό αντιστοιχεί μονοσήμαντα ο a, $1 \leq a \leq p-1$ για τον οποίο ισχύει $aa' \equiv 1 \mathrm{mod} p$. Άρα φτιάχνουμε ζευγαράκια (a, a'). Το ερώτημα είναι πότε $a = a'$; Αν $a = a'$, έχουμε $a^2 \equiv 1 \mathrm{mod} p$, δηλαδή $p \mid (a-1)(a+1)$. Επομένως $a = a'$ ακριβώς τότε όταν $a = 1$ ή $a = p-1$. Οι υπόλοιποι ακέραιοι σχηματίζουν ζευγαράκια (a, a'), $a \neq a'$ και $aa' \equiv 1 \mathrm{mod} p$. Πολλαπλασιάζουμε κατά μέλη αυτές τις ισοδυναμίες και έχουμε

$$2 \cdot 3 \cdots (p-2) \equiv 1 \mathrm{mod} p$$

δηλαδή $(p-2)! \equiv 1 \mathrm{mod} p$ από όπου το ζητούμενο προκύπτει με πολλαπλασιασμό κατά μέλη με $p-1$.
Η παρατήρηση τέλος του Gauss στο παραπάνω σχόλιο του Warring ήταν:
«Οι αποδείξεις πρέπει να οδηγούνται από ιδέες (έννοιες) και όχι από συμβολισμούς»

Ιστορικά 4.7.3

Θεωρείται ότι το θεώρημα ήταν γνωστό στον Ali al-Hasan ibn al-Haytam (964-1040), 750 χρόνια πριν τον Wilson [9, σελ. 32].

4.8 Κριτήρια ελέγχου πρώτων αριθμών και παραγοντοποίηση

Στην προηγούμενη παράγραφο αναφερθήκαμε στο κριτήριο του Wilson. Όμως είναι πάρα πολύ δύσκολο να υπολογίσουμε παραγοντικά. Αυτός είναι ο λόγος για τον οποίο το κριτήριο αυτό είναι πρακτικά άχρηστο (δύσχρηστο).

Πολύ πιο εύκολος είναι ο υπολογισμός δυνάμεων. Δυνάμεις εμφανίζονται στο Θεώρημα του Fermat, στο οποίο το μέτρο είναι πρώτος αριθμός. Άμεση συνέπεια του θεωρήματος είναι ότι:

Αν n φυσικός αριθμός και υπάρχει ακέραιος a, τέτοιος ώστε

$$a^n \not\equiv a \bmod n,$$

τότε ο n είναι σύνθετος.

Παράδειγμα. Υπολογίζουμε ότι $2^{10} \equiv 4 \bmod n$. Επομένως $2^{10} \not\equiv 2 \bmod 10$ και συνεπώς το 10 είναι σύνθετος. Ομοίως ο 63 είναι σύνθετος, αφού $2^{68} \equiv 8 \bmod 63$.

Σημείωση: Στα παραραδείγματα έχουμε επιλέξει $a = 2$. Ο λόγος είναι ότι ο $a = 2$ είναι ο πιο μικρός διαθέσιμος ακέραιος.

Στα 1680 ο Leibniz διατύπωσε την εικασία ότι αν ο n δεν είναι πρώτος τότε δεν διαιρεί τον $2^n - 2$. Η εικασία αυτή αποδείχθηκε λάθος από τον F. Sarrus, ο οποίος απέδειξε ότι δεν ισχύει για $n = 341$.

Πράγματι $341 = 11 \cdot 31$. Εφαρμόζουμε το θεώρημα του Fermat για τους πρώτους 11 και 31 και έχουμε

$$2^{10} \equiv 1 \bmod 11,$$

άρα

$$2^{340} \equiv \left(2^{10}\right)^{34} \equiv 1 \bmod 11$$

και συνεπώς $2^{341} \equiv 2 \bmod 11$. Όμοιως $2^{30} \equiv 1 \bmod 31$, άρα $2^{330} \equiv 1 \bmod 31$. Όμως $2^5 \equiv 32 \equiv 1 \bmod 32$ δηλαδή

$$2^{340} \equiv 1 \bmod 31$$

και επομένως

$$2^{341} \equiv 2 \bmod 31.$$

Τώρα $11 \mid 2^{341} - 2$ και $31 \mid 2^{341} - 2$ και $(11, 31) = 1$. Συνεπώς

$$11 \cdot 31 = 341 \mid 2^{341} - 2.$$

Σημείωση:

1. Ο 341 είναι ο μικρότερος αριθμός με αυτή την ιδιότητα.
2. Διάφοροι συγγραφείς υποστηρίζουν ότι η εικασία του Leibniz ανάγεται σε αρχαίους κινέζους μαθηματικούς [7, σελ. 117], [1, σελ. 72].

Ορισμός 4.8.1. Αν a θετικός ακέραιος και n σύνθετος θετικός ακέραιος τέτοιος ώστε

$$a^n \equiv a \bmod n$$

θα λέμε ότι ο n είναι *ψευδοπρώτος* ως προς τη βάση a.

Συνήθως παραλείπουμε τον όρο «ως προς τη βάση a» όταν $a = 2$.

Οι ψευδοπρώτοι αριθμοί είναι αραιότεροι των πρώτων στο σύνολο των φυσικών αριθμών. Για παράδειγμα, πρώτοι αριθμοί μικρότεροι ενός εκατομμυρίου υπάρχουν 78492 ενω ψευδοπρώτοι μόνο 245. Οι επόμενοι του 341 είναι οι $561, 645, 1105$. Ο μικρότερος άρτιος ψευδοπρώτος είναι ο 1610038. D. Lehmer, 1950.

Είναι εύκολο να αποδειχτεί ότι υπάρχουν άπειροι ψευδοπρώτοι αριθμοί.

Πρόταση 4.8.2. *Υπάρχουν άπειροι ψευδοπρώτοι αριθμοί.*

Απόδειξη. Θα αποδείξουμε ότι αν n ψευδοπρώτος τότε και ο $2^n - 1$ είναι επίσης ψευδοπρώτος. Είναι φανερό ότι αν το αποδείξουμε αυτό τότε η απόδειξη της πρότασης έχει τελειώσει, αφού $2^n - 1 > n$ και μπορούμε να ξεκινήσουμε για $n = 341$.

Πρώτα από όλα ο n είναι σύνθετος, $n = a \cdot b$, $1 < a < n$, $1 < b < n$. Ο $2^a - 1 > 1$ και $2^a - 1 \mid 2^n - 1$, οπότε και ο $(2^n - 1)$ είναι σύνθετος. Επίσης ισχύει

$$2^{2^n-1} \equiv 2 \mathrm{mod}(2^n - 1).$$

Πράγματι, αφού ο n είναι ψευδοπρώτος,

$$2^n \equiv 2 \mathrm{mod} n.$$

Επομένως υπάρχει ακέραιος ℓ τέτοιος ώστε

$$2^n - 2 = \ell n.$$

Γράφουμε τη γνωστή ταυτότητα

$$X^m - 1 = (X - 1)(X^{m-1} + X^{m-2} + \cdots + X + 1)$$

η οποία για $X = 2^n$ και $m = \ell$ και εχουμε

$$2^n - 1 \mid 2^{n\ell} - 1 \Rightarrow 2^{n\ell} \equiv 1 \mathrm{mod}(2^n - 1),$$

οπότε

$$2^{2^n-1} = 2^{n\ell+1} \equiv 2 \mathrm{mod}(2^n - 1).$$

□

Κατά καιρούς έχουν τεθεί διάφορα ερωτήματα για τους ψευδοπρώτους, ανάλογα με αυτά που έχουν τεθεί για τους πρώτους. Έτσι αποδείχθηκε το 1963 [3] ότι κάθε αριθμητική προόδος $an + b, (a, b) = 1, n \in \mathbb{Z}$ περιέχει άπειρους ψευδοπρώτους.

Παρατήρηση 4.8.3. Για τους αριθμούς Fermat, $F_n = 2^{2^n} + 1$, $n \geq 0$ ισχύει $2^{F_n} \equiv 2 \mathrm{mod} F_n$.

Απόδειξη. Αν m άρτιος

$$X^m - 1 = (X + 1)(X^{m-1} - X^{m-2} + \cdots - 1) \Rightarrow X + 1 \mid X^m - 1,$$

Για $X = 2^{2^n}$ και $m = 2^{2^n-n}$, έχουμε

$$F_n = 2^{2^n} + 1 \mid \left(2^{2^n}\right)^{2^{2^n-n}} - 1 = 2^{2^n \cdot 2^{2^n-n}} - 1 = 2^{2^{2^n}} - 1.$$

Επομένως $2^{2^n} \equiv 1 \mathrm{mod} F_n$, οπότε

$$2^{F_n} = 2^{2^{2^n}+1} \equiv 2 \mathrm{mod} F_n.$$

□

Αυτό σημαίνει ότι όλοι οι αριθμοί του Fermat που δεν είναι πρώτοι είναι ψευδοπρώτοι. Τώρα το θεώρημα του Fermat ισχύει για όλους τους ακέραιους a. Αν επομένως έχουμε $2^n \equiv 2 \mathrm{mod} n$ μπορούμε να επιλέξουμε ως βάση το 3 και να ελέγξουμε αν

$$3^n \equiv 3 \mathrm{mod} n$$

ή όχι. Αν δεν ισχύει η τελευταία ισοδυναμία τότε και πάλι συμπεραίνουμε ότι ο n είναι σύνθετος.

Μπορούμε για παράδειγμα να αποδείξουμε ότι

$$3^{441} \equiv 3 \mathrm{mod} 11$$

και $3^{341} \equiv 13 \mathrm{mod} 31$. Συνεπώς $3^{341} \not\equiv 3 \mathrm{mod} 341$ και επομένως η ισοδυναμία δεν ισχύει.

Έτσι απέδειξε ο G.A. Paxson [8] το 1961 ότι

$$3^{F_{13}} \not\equiv 3 \mathrm{mod} F_{13}$$

και κατέληξε στο συμπέρασμα ότι ο F_{13} είναι σύνθετος.

Αν είχαμε βρει $3^{341} \equiv 3 \mathrm{mod} 341$ θα παίρναμε $a = 4$ και ούτω καθεξης. Είναι φυσικό ότι αν η ισοδυναμία συνεχίζει να ισχύει για διάφορες τιμές της βάσης a αυξάνονται οι πιθανότητες ο αριθμός μας να είναι πρώτος. Θα μπορούσε να ελπίζει κανείς ότι αν ο αριθμός n είναι σύνθετος, ίσως υπάρχει πάντα κάποια βάση a για την οποία να ισχύει

$$a^n \not\equiv a \mathrm{mod} n.$$

Οι ελπίδες αυτές όμως παρέμειναν φρούδες. Ο λόγος είναι ότι ο R.C. Carmichael απέδειξε στα 1909 ότι υπάρχουν σύνθετοι ακέραιοι n για τους οποίους ισχύει η ισοδυναμία

$$a^n \equiv a \mathrm{mod} n$$

για όλους τους ακέραιους a.

Ο μικρότερος από αυτούς είναι ο 561.

Ορισμός 4.8.4. Ο σύνθετος ακέραιος n, $n > 1$ θα λέγεται *αριθμός Carmichael* όταν

$$a^n \equiv a \mathrm{mod} n$$

για κάθε ακέραιο a, $(a, n) = 1$.

Σημείωση: Είναι προφανές ότι αρκεί να ελέγξουμε την ισοδυναμία για όλους τους a, $1 < a < n$, ή ισοδύναμα για όλους τους $1 < a < n$ με $(a, n) = 1$ ισχύει

$$a^{n-1} \equiv 1 \mathrm{mod} n.$$

Πρόταση 4.8.5. *Ο αριθμός* 561 *είναι αριθμός Carmichael.*

Απόδειξη. Υπολογίζουμε ότι $n = 561 = 3 \cdot 11 \cdot 17$. Αρκεί να αποδείξουμε ότι για κάθε ακέραιο a ισχύουν:

$$\begin{aligned} a^{561} &\equiv a \mathrm{mod} 3 \\ a^{561} &\equiv a \mathrm{mod} 11 \\ a^{561} &\equiv a \mathrm{mod} 17. \end{aligned}$$

Έστω ότι $(a, 561) = 1$. Αυτό σημαίνει ότι $(a, 3) = (a, 11) = (a, 17) = 1$. Εφαρμόζουμε το θεώρημα Fermat:

$$\begin{aligned} a^2 \equiv 1 \mathrm{mod} 3 &\Rightarrow a^{561} \equiv a \mathrm{mod} 3 \\ a^{10} \equiv 1 \mathrm{mod} 11 &\Rightarrow a^{561} \equiv a \mathrm{mod} 11 \\ a^{16} \equiv 1 \mathrm{mod} 17 &\Rightarrow a^{561} \equiv a \mathrm{mod} 17, \end{aligned}$$

δηλαδή το ζητούμενο. □

Εντελώς φυσικά προκύπτει το ερώτημα αν υπάρχει κάποια πρόταση η οποία να χαρακτηρίζει τους αριθμους Carmichael. Η απάντηση στο ερώτημα είναι θετική.

Πρόταση 4.8.6. *Αν n σύνθετος, ελεύθερος τετραγώνου δηλαδή $n = p_1 p_2 \cdots p_s$, με $p_i \neq p_j$ για κάθε $i \neq j$, και $p_{i-1} \mid (n-1)$ για κάθε $i = 1, 2, \ldots, s$ τότε και μόνο τότε αν ο n είναι αριθμός Carmichael.*

Απόδειξη. Αν a ακέραιος και $(a, n) = 1$, τότε $(a, p_i) = 1$ για κάθε $i = 1, 2, \ldots, s$. Επομένως από το θεώρημα Fermat $p_i \mid a^{p_i - 1} - 1$ για κάθε $i = 1, 2, \ldots, s$, οπότε και $a^{p_i} \equiv a \mathrm{mod} p_i$ για κάθε ακέραιο a.

Επειδή $(p_i - 1) \mid (n-1)$, έπεται ότι $p_i \mid a^{n-1} - 1$, οπότε και $a^n \equiv a \mathrm{mod} p_i$ για κάθε ακέραιο a. Τελικά $n = p_1 p_2 \cdots p_s \mid a^n - a$.

Σημείωση Το ικανό θα αποδειχθεί αργότερα. □

Με βάση το κριτήριο μπορούμε πολύ εύκολα να αποδείξουμε ότι ο 561 είναι αριθμός Carmichael. Πράγματι, $561 = 3 \cdot 11 \cdot 17$, ελεύθερος τετραγώνου και σύνθετος. Επιπλέον

$$\begin{aligned} 3 - 1 = 2 \mid 561 - 1 = 560 \\ 11 - 1 = 10 \mid 561 - 1 = 560 \\ 17 - 1 = 16 \mid 561 - 1 = 560 = 16 \cdot 35. \end{aligned}$$

Πόσοι όμως αριθμοί Carmichael υπάρχουν; Ο ίδιος ο Carmichael διατύπωσε την εικασία ότι υπάρχουν άπειροι ομώνυμοι αριθμοί.

Η εικασία αυτή αποδείχθηε στα 1994 από τους W.R. Alford, A. Granville και C. Pomerance «There are infinitely many Carmichael numbers» [22].

Πιο συγκεκριμένα αυτό που απέδειξαν οι Alford, Granville και Pomerance ήταν ότι

$$\#\{n \in \mathbb{N} : n \leq x, n \text{ αριθμός Carmichael}\} > x^{2/7}$$

για αρκετά μεγάλο x ($x \to \infty$). Η απόδειξη ξεπερνάει τα όρια και τον σκοπό του παρόντος.

Με βάση τα παραπάνω μπορούμε πλέον να διατυπώσουμε το πιθανοθεωρητικό κριτήριο ελέγχου πρώτων αριθμών στηριζόμενο στο θεώρημα του Fermat.

Θέτουμε n από 3 μέχρι ας πούμε 10^{10}. Αν το $2^n \equiv 2 \mathrm{mod} n$, τότε ο n είναι πολύ πιθανό να είναι πρώτος, αλλιώς ο n είναι σύνθετος. (Αν $2^n \not\equiv 2 \mathrm{mod} n$, τότε ο n είναι σύνθετος.)

Αν λάβουμε υπόψη τον αριθμό των ψευδοπρώτων στο διάστημα από 1 μέχρι $2,5 \cdot 10^{10}$ ο οποίος μας είναι γνωστός, τότε η πιθανότητα να είναι ο n σύνθετος και να ισχύει $2^n \equiv 2 \mathrm{mod} n$ είναι ένα προς πενήντα χιλιάδες.

Το τελευταίο γνωστό αποτέλεσμα στους συγγραφείς είναι αυτό του R. Pinch, ο οποίος υπολόγισε ότι μέχρι το 10^{21} υπάρχουν 20138200 αριθμοί Carmichael.

Στη συνέχεια θα περιγράψουμε ένα κριτήριο ελέγχου πρώτων που αποτελεί βελτίωση του προηγούμενου. Είναι το κριτήριο Miller-Rabin. Πρώτα από όλα παρατηρούμε ότι, αν p πρώτος

αριθμός, τότε $x^2 \equiv 1 \mod p$ ακριβώς τότε όταν $x \equiv \pm 1 \mod p$. Αν τώρα n όχι πρώτος μπορούμε να έχουμε και άλλες λύσεις. Για παράδειγμα, αν $n = 35$ η $x^2 \equiv 1 \mod 35$ έχει λύση και το $x = 6$. Τέτοιες λύσεις θα λέγονται *μη-τετριμμένες τετραγωνικές ρίζες του* $1 \mod n$.

Είναι και πάλι φανερό ότι:

Αν η ισοδυναμία $x^2 \equiv 1 \mod n$, έχει μη-τετριμμένη ρίζα, τότε ο n είναι σύνθετος.

Αν τώρα ο περιττός φυσικός αριθμός n, $n > 1$ γραφεί στη μορφή

$$n - 1 = 2^k \cdot m,$$

όπου m περιττός και $k \geq 1$ τότε τα βήματα του *κριτηρίου του Miller-Rabin* είναι τα εξής:

1. Επιλέγουμε τυχαία έναν ακέραιο $a \in \mathbb{Z}$, $1 \leq a \leq n - 1$.

2. Υπολογίζουμε το $b := a^m \mod n$. Αν $b \equiv 1 \mod n$, τότε η απάντηση είναι: «ο n είναι πρώτος» και σταματάμε.

3. Αλλιώς υπολογίζουμε διαδοχικά τις δυνάμεις

$$b, b^2 = a^{2m}, b^4 = a^{2^2 m}, \ldots, b^{2^{k-1} m} \mod n$$

Αν σε κάποιο βήμα βρούμε ότι $a^{2^i m} \equiv -1 \mod n$ τότε και πάλι απαντούμε ότι «ο n είναι πρώτος». Αν δεν βρούμε ποτέ $a^{2^i m} \equiv -1 \mod n$ απαντούμε ότι « ο n είναι σύνθετος».

Θα αποδείξουμε ότι η απάντηση για τον n ότι είναι σύνθετος είναι σίγουρη, ενώ η απάντηση ότι είναι πρώτος είναι επισφαλής. Υπάρχουν, σύνθετοι ακέραιοι που μασκαρεύονται σε πρώτους.

Τέτοιοι αλγόριθμοι λέγονται αλγόριθμοι Monte-Carlo.

Ορισμός 4.8.7. Ένας αλγόριθμος Monte-Carlo είναι ένας πιθανοθεωρητικός αλγόριθμος του οποίου η απάντηση «Ναι» σε κάποιο πρόβλημα είναι πάντα σωστή, αλλά η απάντηση «όχι» μπορεί να είναι και λάθος.

Θα λέμε ότι ο αλγόριθμος Monte-Carlo έχει πιθανότητα λάθους ε, όταν σε περιπτώσεις που η απάντηση θα έπρεπε να είναι είναι «ναι» ο αλγόριθμος δίνει τη λάθος απάντηση με πιθανότητα το πολύ ε.

Πρόταση 4.8.8. *Ο αλγόριθμος Miller-Rabin είναι ένας Monte-Carlo αλγόριθμος στον οποίο η απάντηση «ναι» σημαίνει ότι ο n είναι σύνθετος.*

Απόδειξη. Θα υποθέσουμε ότι ο αλγόριθμός δίνει απάντηση «Ναι, ο n είναι σύνθετος» για κάποιο πρώτο αριθμό n και θα καταλήξουμε σε άτοπο.

Από την απάντηση που πήραμε συμπεραίνουμε ότι

$$a^m \not\equiv 1 \mod n.$$

Επίσης ο αλγόριθμος ελέγχει τις τιμές

$$a^m, a^{2m}, \ldots, a^{2^{k-1} m} \mod n.$$

Και πάλι, αφού η απάντηση είναι ότι «ο n είναι σύνθετος» έχουμε

$$a^{2^i m} \not\equiv -1 \mod n,$$

για κάθε $i = 0, 1, 2, \ldots, k-1$. Όμως έχουμε υποθέσει ότι ο n είναι πρώτος, οπότε σύμφωνα με το θεώρημα του Fermat

$$a^{n-1} \equiv 1 \bmod n,$$

δηλαδή

$$a^{2^{kq}m} \equiv 1 \bmod n$$

Αν $x := a^{2^{k-1}m}$ η ισοδυναμία γράφεται

$$x^2 \equiv 1 \bmod n.$$

Λόγω της υπόθεσης ότι ο n είναι πρώτος, έπεται ότι η ισοδυναμία έχει μοναδικές λύσεις $x = \pm 1 \bmod n$. Εμείς όμως έχουμε

$$x = a^{2^{k-1}m} \not\equiv -1 \bmod n.$$

Επομένως, αναγκαστικά θα ισχύει

$$x = a^{2^{k-1}m} \equiv 1 \bmod n.$$

Αν τώρα $y := a^{2^{k-2}m}$, έχουμε

$$y^2 \equiv 1 \bmod n,$$

οπότε, όπως και παραπάνω, καταλήγουμε στο συμπέρασμα ότι

$$y = a^{2^{k-2}m} \equiv 1 \bmod n.$$

Συνεχίζουμε επαγωγικά και καταλήγουμε στο συμπέρασμα ότι και

$$a^m \equiv 1 \bmod n,$$

άτοπο. Άρα ο n είναι σύνθετος. □

Ορισμός 4.8.9. Αν ο σύνθετος n περάσει ανέπαφος από τα «γρανάζια» του test των Miller-Rabin ως προς τη βάση b τότε λέμε ότι ο n είναι *ισχυρός ψευδο-πρώτος* ως προς τη βάση b.

Υπάρχουν άπειροι ισχυροί ψευδοπρώτοι ως προς βάση το 2 [11, Θ. 6.6 σελ. 226]. Δεν υπάρχει ανάλογο των αριθμών Carmichael για ισχυρούς ψευδο-πρώτους. Πράγματι ισχύει [11, Θ. 6.10]

Πρόταση 4.8.10. *Αν n σύνθετος θετικός ακέραιος τότε ο n περνάει το Miller-Rabin test το πολύ για $\frac{n-1}{4}$-βάσεις b, $1 \leq b \leq n-1$.*

Επομένως, αν ένας φυσικός περάσει το test για περισσότερες από $\frac{n-1}{4}$ βάσεις, τότε είναι πρώτος.

Παρατήρηση 4.8.11. Ο πιο μικρός σύνθετος που περνάει το test ελέγχου πρώτων αριθμών μασκαρεμένος σε πρώτο ενώ είναι σύνθετος είναι ο $2047 = 23 \cdot 89$. Εδώ $2047 - 1 = 2046 = 2 \cdot 1023$ και

$$2^{1023} \equiv 1 \bmod 2047$$

καθώς και $2^{2046} \equiv 1 \bmod 2047$. Οι τελευταίες ισοδυναμίες υπολογίζονται εύκολα αφού $2^{11} \equiv 2048 \equiv 1 \bmod 2047$. Ισχύει $2046 = 11 \cdot 86$, $1023 = 11 \cdot 93$.

Παρατήρηση 4.8.12. Αποδεικνύεται ότι η πιθανότητα λάθους του αλγορίθμου είναι το πολύ $\varepsilon = \frac{1}{4}$, αλλά θα παραλείψουμε την απόδειξη αυτή.

Παρατήρηση 4.8.13. Κατά τον Mollin [2, σελ. 161] το κριτήριο θα έπρεπε να ονομάζεται Miller-Selfidge-Rabin γιατί το χρησιμοποίησε ο Selfridge το 1974 πριν από τη δημοσίευση του Miller.

Παρατήρηση 4.8.14. Εάν επιλέξουμε k διαφορετικούς ακέραιους $\leq n$ ως βάση εκτέλεσης του αλγόριθμου, τότε η πιθανότητα λάθους είναι $< \frac{1}{2^{2k}}$.

Παρατήρηση 4.8.15. Παρατηρούμε ότι τα ντετερμινιστικά κριτήρια είναι όμορφα αλλά όχι πρακτικά ενώ τα πιθανοθεωρητικά έχουν το μειονέκτημα ότι δεν δίνουν πάντοτε τη σωστή απάντηση, αλλά είναι πρακτικά. Βέβαια το 2002, δημοσιεύτηκε το άρθρο των M. Agrawal, N. Kayal και N. Saxena [13] το οποίο διαπραγματεύται έναν σχεδόν ντετερμινιστικό αλγόριθμο ελέγχου.

Υπάρχει ένα πολύ καλό βιβλίο που διαπραγμετεύται το θέμα [15] καθώς και στα ελληνικά η πτυχιακή του Μάνου Καμαριανάκη (δες την ιστοσελίδα του Γιάννη Αντωνιάδη `http://www.math.uoc.gr/~antoniad/`».

4.9 Αλγόριθμοί παραγοντοποίησης ακέραιων αριθμών

4.9.1 Αλγόριθμος παραγοντοποίησης του Dixon

Πρόταση 4.9.1. *Αν x, y ακέραιοι και $x^2 \equiv y^2 \bmod n$ και $x \not\equiv \pm y$ τότε ο φυσικός $d = (x-y, n)$ είναι μη-τετριμμένος παράγοντας του n.*

Απόδειξη. Έχουμε $n \mid x^2 - y^2 = (x-y)(x+y)$, ενώ $n \nmid (x-y)$ και $n \nmid (x+y)$. Είναι φανερό ότι $d \mid n$. Θα αποδείξουμε ότι $1 < d < n$.

Αν $d = n$ θα είχαμε $n \mid (x-y)$, άτοπο. Αν $d = 1$ τότε αφού $n = (x+y)(x-y)$ και $(x-y, n) = 1$ έπεται ότι $n \mid (x+y)$, πάλι άτοπο. □

Παράδειγμα. Υπολογίζουμε ότι $10^2 \equiv 32^2 \bmod 77$, $10 \not\equiv 32 \bmod 77$, $10 \not\equiv -32 \bmod 77$. Επομένως ο 77 και ένας γνήσιος παράγοντας αυτού είναι ο $(10-32, 77) = 11$.

4.9.2 Ο p-1-αλγόριθμος παραγοντοποίησης του Pollard

Υποθέτουμε ότι μας δίνεται ο φυσικός αριθμός n για τον οποίο υποψιαζόμαστε ότι είναι σύνθετος και θέλουμε να τον παραγοντοποίησουμε. Επιλέγουμε έναν ακέραιο B, ως φράγμα εργασίας.

- Θέτουμε $a = 2$
- Υπολογίζουμε τις δυνάμεις $\alpha = a^j \bmod n$ για $j = 2, 3, \ldots, B$
- Υπολογίζουμε το $d = (\alpha - 1, n)$
- Αν $1 < d < n$ τότε ο d είναι ένας γνήσιος παράγοντας του n (επιτυχία), αλλιώς δεν βρήκαμε γνήσιο παράγοντα του n (αποτυχία).

Αν τώρα p πρώτος διαιρέτης του n και υποθέτουμε ότι κάθε δύναμη πρώτου διαιρέτη του $p-1$, έστω q, είναι μικρότερη ή ίση του B θα έχουμε $(p-1) \mid B!$

Για το τελικό α που θα βρούμε στο δεύτερο βήμα του αλγορίθμου ισχύει

$$\alpha \equiv 2^{B!} \bmod n$$

και κατ' επέκταση

$$\alpha \equiv 2^{B!} \bmod p,$$

για όλους τους διαιρέτες του n. Επειδή $(p-1) \mid B!$ έπεται ότι $B! = (p-1)t$ με $t \in \mathbb{Z}$ και συνεπώς

$$2^{B!} \equiv (2^{p-1})^t \mathrm{mod} p$$

Επειδή $2^{p-1} \equiv 1 \mathrm{mod} p$, τελικά προκύπτει ότι $\alpha \equiv 2^{B!} \equiv 1 \mathrm{mod} p$.

Επειδή $p \mid (\alpha - 1)$ και $p \mid n$, έπεται ότι $p \mid (\alpha - 1, n) =: d$ και συνεπώς $1 < p \leq d$. Αν $d = n$, θα είχαμε $n \mid (\alpha - 1)$. Όμως το $\alpha - 1 < n$ οπότε θα έπρεπε $\alpha = 1$. Επομένως βρίσκουμε έναν μη-τετριμμένο παράγοντα d του n και συνεχίζουμε την προσπάθεια παραγοντοποίησης των d και n/d.

Παρατήρηση 4.9.2. Μπορούμε να εργαστούμε με το ελάχιστο κοινό πολλαπλάσιο $[1, 2, \ldots, B]$ αντί του $B!$ αφού είναι πιο μικρός γενικά ακέραιος.

Παράδειγμα. Θεωρούμε τον φυσικό $n = 540143$. Επιλέγουμε $B = 8$. Επομένως $k := [1, 2, \ldots, 8] = 840$. Θέτουμε $a = 2$ και υπολογίζουμε

$$2^{840} \equiv 53047 \mathrm{mod} n$$

Επίσης $(53047, n) = 421$ συνεπώς $540143 - 421 \cdot 1283$.

Παρατήρηση 4.9.3. Αν το B που επιλέξαμε δεν αρκεί για το σκοπό του επιλέγουμε κάποιο άλλο μεγαλύτερο του αρχικού και επαναλαμβάνουμε τη διαδικασία.

Μερικές φορές ο αλγόριθμος δεν λειτουργεί για $a = 2$, οπότε μπορούμε να δοκιμάσουμε για $a = 3$ και αν πάλι δεν λειτουργεί να δοκιμάσουμε με μεγαλύτερες τιμές του a.
Παράδειγμα. Επιθυμούμε να παραγοντοποιήσουμε τον $n = 187$. Επιλέγουμε $B = 15$. Επομένως $k = [1, 2, \ldots, 15] = 360360$. Για $a = 2$ ο $(2^{360360} - 1, 187) = 187$ και δεν καταφέρνουμε να τον παραγοντοποιήσουμε.

Για $a = 3$ έχουμε $3^{360360} - 1 \equiv 66 \mathrm{mod} 187$ και επομένως $(3^{360360} - 1, 187) = (66, 187) = 11$. Συνεπώς $187 = 11 \cdot 17$.

Για μια ντετερμινιστική προσέγγιση του αλγόριθμου παραπέμπουμε στο άρθρο του Bartosz Zraler [5].

4.9.3 Ο αλγόριθμος παραγοντοποίησης ρ του Pollard

Η ιδέα του αλγόριθμου αυτού είναι η εξής:

Έστω n σύνθετος ακέραιος και p ο ελάχιστος πρώτος παράγοντας του n. Αν μπορούμε να βρούμε ακέραιους

$$x_0, x_1, x_2, \ldots, x_\ell$$

τέτοιους ώστε για κάποιους δείκτες $i, j \in \{0, 1, 2, \ldots, \ell\}$ να ισχύουν

$$x_i \equiv x_j \mathrm{mod} p \text{ και } x_i \not\equiv x_j \mathrm{mod} n$$

τότε ο $(x_i - x_j, n)$ είναι ένας γνήσιος διαιρέτης του n αφού $p \mid (x_i - x_j, n) \mid n$ και $(x_i - x_j, n) \neq n$.

Τα ερωτήματα που προκύπτουν είναι πώς θα επιλέξουμε τα x_i και στη συνέχεια με ποιον σύντομο τρόπο θα διαπιστώσουμε την ύπαρξη ενός κατάλληλου ζευγαριού με τις παραπάνω ιδιότητες. Είναι φανερό ότι ο υπολογισμός του $(x_i - x_j, n)$ για όλους τους δείκτες $0 \leq i, j \leq \ell$ είναι μια αρκετά χρονοβόρα διαδικασία.

Η ακολουθία $x_0, x_1, \ldots, x_\ell$ θα πρέπει να είναι κατά το δυνατόν τυχαία (random) ακολουθία. Επιλέγουμε τυχαία το $x_0 = 2$ και μια πολυωνυμική συνάρτηση $f(x)$ με ακέραιους συντελεστές και υπολογίζουμε αναδρομικά τους υπόλοιπους όρους της ακολουθίας

$$x_{i+1} \equiv f(x_i) \bmod n, 0 \leq x_{i+1} < n.$$

Για να επαναλαμβάνονται οι όροι της ακολουθίας (mod$p$) μετά από λογικό αριθμό βημάτων θα πρέπει να επιλέξουμε κατάλληλη πολυωνυμική συνάρτηση $f(x)$. Δεν θέλουμε να υπάρχει κάποιος ακέραιος $a \bmod p$ τέτοιος ώστε η ακολουθία

$$x_1 = f(a), x_2 = f(x_1) = f(f(a)) = f^{(2)}(a), \ldots, x_\ell = f^{(\ell)}(a)$$

να δίνει για μεγάλο ℓ διαφορετικές τιμές mod$p$.

Ας ονομάσουμε «ρ-αριθμό» μιας τέτοιας ακολουθίας x_i ως προς τον πρώτο αριθμό p τον μεγαλύτερο ακέραιο m για τον οποίο υπάρχει ένα $a \bmod p$ τέτοιο ώστε όλοι οι όροι της ακολουθίας

$$f(a), \ldots, f^{(m)}(a)$$

να είναι ανά δύο διαφορετικοί mod$p$. Εμείς θέλουμε ακολουθίες με μικρό ρ-αριθμό. Επομένως δεν μπορούμε να επιλέξουμε πρωτοβάθμια πολυωνυμική συνάρτηση

$$f(x) = aX + b.$$

Αυτό διότι όταν $a \not\equiv 1 \bmod p$, τότε ο «ρ-αριθμός» είναι η τάξη του $a \bmod p$ και αυτός είναι συνήθως ένας μεγάλος διαιρέτης του $p - 1$.

Αν $a \equiv 1 \bmod p$ και $b \not\equiv 0 \bmod p$, τότε $f(X) = X + b$ και ο «ρ-αριθμός» είναι ακριβώς p, αφού $f(x_1) \equiv f(x_2) \bmod p$ αν και μόνο αν $x_1 \equiv x_2 \bmod p$.

Θα πρέπει επομένως να επιλέξουμε μία πολυωνυμική συνάρτηση δευτέρου βαθμού. Φαίνεται ότι μια καλή επιλογή είναι η πολυωνυμική συνάρτηση $f(X) = X^2 + 1$.

Τώρα είναι φανερό ότι αν $x_i \equiv x_j \bmod p$ τότε και $x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1} \bmod p$. Αυτό σημαίνει ότι η ακολουθία γίνεται από ένα σημείο και πέρα, περιοδική (mod$p$) με περίοδο $(i - j)$. Συνεπώς, αν $r \geq i, t \geq i$, και $r \equiv t \bmod (i - j)$ τότε

$$x_r \equiv x_t \bmod p.$$

Αν λοιπόν s είναι το ελάχιστο πολλαπλάσιο του $(i - j)$ το οποίο είναι $\geq i$, έχουμε

$$x_{2s} \equiv x_s \bmod p.$$

Υπολογίζουμε επομένως πολύ λιγότερους μέγιστους κοινούς διαιρέτες από τους συνδυασμούς ανά δύο. Συγκεκριμένα υπολογίζουμε τους

$$(x_{2s} - x_s, n) \text{ με } s = 1, 2, 3, \ldots$$

μέχρι να βρούμε κάποιον διάφορο του 1 και του n.

Παράδειγμα. Έστω $n = 2047$. Για $x_0 = 2$ και $f(x) = x^2 + 1$ υπολογίζουμε τους όρους της ακολουθίας

$$x_{i+1} = f(x_i) \bmod n$$

$$\begin{array}{ccccc} x_0 = 2 & x_1 = 5 & x_2 = 26 & x_3 = 677 & \\ x_4 = 1849 & x_5 = 312 & x_6 = 1136 & x_7 = 887 & \\ x_8 = 722 & x_9 = 1347 & x_{10} = 768 & x_{11} = 289 & x_{12} = 1642 \end{array}$$

Στη συνέχεια υπολογίζουμε τους

$$(x_{2s} - x_s, n), \text{ για } s = 1, 2, 3, 4, 5, 6$$

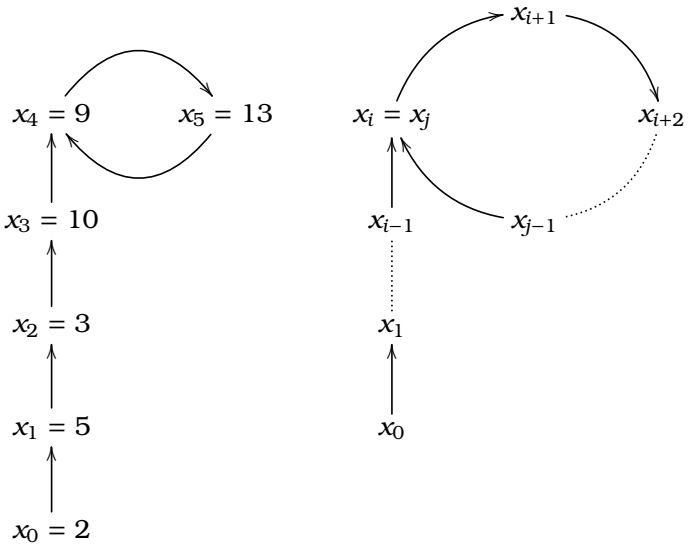
$$\begin{aligned}(26 - 5, 2047) &= 1\\ (1849 - 26, 2047) &= 1\\ (1136 - 677, 2047) &= 1\\ (722 - 1842, 2047) &= 1\\ (768 - 312, 2047) &= 1\\ (1642 - 1136, 2047) &= 23\end{aligned}$$

Επομένως $2047 = 23 \cdot 89$.

Παρατήρηση 4.9.4. Η μέθοδος προτάθηκε από τον J. Pollard στα 1975. Ονομάστηκε ρ-μέθοδος γιατί οι τιμές mod$p$ στην αρχή κάνουν μία «ουρά» μέχρι το σημείο που αρχίζει η περιοδικότητα και στη συνέχεια έναν κύκλο, δηλαδή συνολικά το γράμμα ρ.

Στο παράδειγμά μας έχουμε

$$\begin{array}{lll} x_1 \equiv 5 \bmod 23 & x_2 \equiv 3 \bmod 23 & x_3 \equiv 10 \bmod 23\\ x_4 \equiv 9 \bmod 23 & x_5 \equiv 13 \bmod 23 & x_6 \equiv 9 \bmod 23\\ x_7 \equiv 13 \bmod 23 & x_8 \equiv 9 \bmod 23 & x_9 \equiv 13 \bmod 23\\ x_{10} \equiv 9 \bmod 23 & x_{11} \equiv 13 \bmod 23 & x_{12} \equiv 9 \bmod 23 \end{array}$$



Παρατήρηση 4.9.5. Η μέθοδος έχει εφαρμοστεί από τους R. P. Brent και J. Pollard (1981) [16] για την παραγοντοποίηση του αριθμού Fermat F_8. Επειδή όμως κάθε πρώτος παράγοντας p του F_m έχει τη μορφή

$$p \equiv 1 \bmod 2^{2^{m+2}},$$

η πολυωνυμική συνάρτηση που χρησιμοποιήθηκε ήταν η $f(x) = x^{2^{m+2}} + 1$.

Παρατήρηση 4.9.6. Όταν γνωρίζουμε το x_i προκειμένου να υπολογίσουμε το x_{2i} δεν χρειάζεται να υπολογίσουμε όλους τους ενδιάμεσους όρους

$$x_{i+1}, x_{i+2}, \ldots, x_{2i-1}, x_{2i}.$$

Αν $y_i = x_{2i}$ παρατηρούμε ότι

$$y_1 = x_2 = f(x_1) = f(f(x_0)) = f(f(y_0)),$$

$$y_2 = x_4 = f(x_3)f(f(x_2)) = f(f(y_1))$$

και γενικότερα

$$y_i = x_{2i} = f(f(y_{i-1})).$$

Επομένως σε κάθε βήμα υπολογίζουμε

$$\begin{aligned} x_i &= f(x_{i-1}) \mathrm{mod} n \\ y_i &= f(f(y_{i-1})) \mathrm{mod} n \end{aligned}$$

Παρατήρηση 4.9.7. Υπάρχουν αρκετοί αλγόριθμοι παραγοντοποίησης. Ενδεικτικά αναφέρουμε

- Ο $(p+1)$-αλγόριθμος του Williams.
- Ο αλγόριθμος συνεχών κλασμάτων.
- Ο αλγόριθμος του τετραγωνικού κόσκινου.
- Ο αλγόριθμος των ελλειπτικών καμπυλών.
- Ο αλγόριθμος του κοσκίνου αλγεβρικών σωμάτων αριθμών.

Με μερικούς από αυτούς θα ασχοληθούμε στη συνέχεια.

Βιβλιογραφία

[1] A. Jones, J. M. Jones: *Elementary number theory*. Springer N. York, 1998.

[2] A. Mollin: *Fundamental Number Theory with applications*. Chapman & Hall, 2008. second Edition.

[3] A. Rotkiewicz: *Sur les nombres pseudopremiers de la forme ax + b*. C. R. Acad. Sci. Paris, 257:2601–2604, 1963.

[4] A. Weil: *Number theory, an approach through history, from Hammurapi to Legendere*. Birkhäuser Boston, 1983.

[5] Bartosz Zraler: *A deterministic version of Pollard's p − 1-algorithm*. arXiv:0707.4102v2 30.7.2007. Math. of Comp., 79:513–533, 2010.

[6] C.F. Gauss: *Disquisitiones Arithmeticae*. Yale University Press, 1965.

[7] Damvid, M, Burton: *Elementary Number Theory*. UBS New Delhi, 1998. second edition.

[8] G. A. Paxson: *The compositeness of the 13-th Fermat number*. Math. of Computation, 15:420, 1961.

[9] Graham Everest, Thomas Ward: *An Introduction to Number Theory*, volume 232 of *Graduate Texts in Mathematics*. Springer-Verlag London, 2005.

[10] James J. Tattersall: *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, second edition, 2005.

[11] Keneth H.Rosen: *Elementary Number Theory*. 2011.

[12] K.H. Rosen: *Elementary Number Theory and Its Applications*. Addison-Wesley Longman, Limited, 2000.

[13] M. Agrawal, N. Kayal, N. Saxena: *Primes is in p*. Annals of Mathematics 160, pages 781–793, 2004.

[14] M. Niven and H.S. Zuckerman and H.L. Montgomery: *An introduction to the theory of numbers*. J. Wiley, 1991.

[15] Martin Dietzfelbinger: *Primality Testing in Polynomial Time, from Randomized Algorithms to "Primis in P"*. Springer-Verlag, 2004.

[16] R. P. Brent, J. Pollard: *Factorization of the 8th Fermat number*. Math. Comp., 36:627–630, 1981.

[17] R. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*. Comm. ACM, 21:120–126, 1978.

[18] Tarán: *Nicomachus of Gerasa*. Biography in Dictionary of Scientific Biography, (New York), 1970-1990.

[19] Marcus du Sautoy: *Η μουσική των πρώτων αριθμών, το μεγαλύτερο ανεπίλυτο μυστήριο των μαθηματικών*. 2005.

[20] Richardus Hoche: *Νικομάχου Γερασηνού Πυθαγορικού, Αριθμητική Εισαγωγή*. 1866.

[21] Sir Thomas L. Heath: *Ιστορία των Ελληνικών Μαθηματικών*. Κ.Ε.ΕΠ.ΕΚ., Αθήνα, 2001.

[22] W. R. Alford, A. Granville, C. Pomerance: *There are infinitely many Carmichael numbers*. Annals of Math., 140:703–722, 1994.

[23] Ζαχαρίου, Α. και Ε.: *Νικόμαχος ο Γερασηνός, άρθρο στην Μεγάλη Σοβιετική Εγκυκλοπαίδεια*.

[24] Λάκκης, Κ.: *Θεωρία Αριθμών*. Εκδόσεις Ζήτη, 1990.

[25] Σπανδάγου, Ευάγγελου: *῾Η Ἀριθμητική Εἰσαγωγή τοῦ Νικομάχου, τοῦ Γερασηνοῦ*. 2001.

5

Τετραγωνικά Υπόλοιπα, αρχικές ρίζες, δείκτες και εφαρμογές

5.1 Ισοτιμίες δευτέρου βαθμού

Στο κεφάλαιο αυτό θα μελετήσουμε ισοτιμίες της μορφής:

$$f(x) \equiv 0 \bmod p, \tag{5.1.1}$$

όπου p πρώτος αριθμός, $p \neq 2$ και $f(x)$ ένα πολυώνυμο δευτέρου βαθμού

$$f(x) = ax^2 + bx + c, a, b, c \in \mathbb{Z} \text{ και } p \nmid a.$$

Η λύση ισοτιμιών δευτέρου βαθμού είναι πολύ πιο δύσκολο πρόβλημα από αυτό των γραμμικών. Χρειάστηκαν μακροχρόνιες προσπάθειες διακεκριμένων μαθηματικών για να φτάσουμε σε ένα ικανοποιητικό αποτέλεσμα.

Επειδή $(4a, p) \neq 1$, έπεται ότι η ισοτιμία (5.1.1) είναι ισοδύναμη προς την

$$4af(x) \equiv 0 \bmod p \tag{5.1.2}$$

Η τελευταία ισοτιμία γράφεται

$$(2ax + b)^2 \equiv (b^2 - 4ac) \bmod p \tag{5.1.3}$$

Η λύση της ισοτιμίας αυτής ανάγεται στη λύση μιας ισοτιμίας της μορφής

$$Y^2 \equiv D \bmod p, \tag{5.1.4}$$

όπου $D := b^2 - 4ac$, και μιας γραμμικής ισοτιμίας

$$2ax + b = y_0 \bmod p, \tag{5.1.5}$$

όπου y_0 λύση της (5.1.4).

Η ισοτιμία (5.1.5) έχει πάντοτε μοναδική λύση, αφού $p \nmid 2a$, και η διαδικασία εύρεσης της λύσης μας είναι γνωστή.

Από τα παραπάνω συμπεραίνουμε ότι θα πρέπει να μελετήσουμε την ύπαρξη λύσεων ισοτιμιών της μορφής

$$x^2 \equiv a \bmod p \tag{5.1.6}$$

Αν $p \mid a$, τότε η (5.1.6) έχει μοναδική λύση $x_0 \equiv 0 \bmod p$.

Στη συνέχεια θα μελετήσουμε την τετραγωνική ισοτιμία

$$\boxed{x^2 \equiv a \bmod p \;\; a \in \mathbb{P}, p \neq 2, \text{ και } p \nmid a} \tag{5.1.7}$$

Ορισμός 5.1.1. Ο ακέραιος a θα λέγεται ότι είναι τετραγωνικό υπόλοιπο mod$p$, όταν η ισοτιμία (5.1.7) έχει λύση και ότι δεν είναι τετραγωνικό υπόλοιπο mod$p$, όταν η ισοτιμία (5.1.7) δεν έχει λύση.

Για τη μελέτη των τετραγωνικών υπολοίπων εισήγαγε ο Legendre στο έργο του «Essai sur la Théorie des Nombres» το 1798 το ομώνυμο σύμβολο.

Ορισμός 5.1.2 (Σύμβολο του Legendre)**.** Αν $a \in \mathbb{Z}$ και $p \in \mathbb{P}$, $p \neq 2$, τότε το σύμβολο του Legendre $\left(\frac{a}{p}\right)$ ορίζεται:

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{όταν ο } a \text{ είναι τετραγωνικό υπόλοιπο mod}p \\ -1, & \text{όταν ο } a \text{ δεν είναι τετραγωνικό υπόλοιπο mod}p \end{cases}$$

Παρατήρηση 5.1.3. Η τιμή του συμβόλου εξαρτάται από την κλάση του $a \bmod p$. Πράγματι, αν $a, b \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \neq 2$ και

$$a \equiv b \bmod p \text{ τότε } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Το $\left(\frac{a}{p}\right) = 1$ ακριβώς τότε όταν η ισοτιμία

$$x^2 \equiv a \bmod p$$

έχει λύση. Όμως η τελευταία ισοτιμία έχει λύση ακριβώς τότε όταν η ισοτιμία

$$x^2 \equiv b \bmod p$$

έχει λύση, δηλαδή όταν $\left(\frac{b}{p}\right) = 1$.

Επομένως για να ελέγξουμε αν κάποιος ακέραιος αριθμός a είναι τετραγωνικό υπόλοιπο mod$p$, αρκεί να θεωρήσουμε ένα πλήρες σύστημα αντιπροσώπων mod$p$ -για παράδειγμα το $0, 1, \ldots, p-1$ (ή το $0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$)- και να ελέγξουμε αν ο a είναι ισότιμος προς κάποιον από τα τετράγωνα αυτών.

Παράδειγμα. Θα ελέγξουμε αν ο 2 είναι τετραγωνικό υπόλοιπο mod7. Υπολογίζουμε τα τετράγωνα:

$$\begin{array}{rcccccccc} x & \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 \mod 7 \\ x^2 & \equiv & 0 & 1 & 4 & 2 & 2 & 4 & 1 \mod 7 \end{array}.$$

Επομένως το 2 είναι τετραγωνικό υπόλοιπο mod7. Μάλιστα η ισοτιμία $x^2 \equiv 2 \bmod 7$ έχει δύο λύσεις $x \equiv 3 \bmod 7$ και $x \equiv 4 \bmod 7$.

Παράδειγμα. Είναι το 2 τετραγωνικό υπόλοιπο mod11; Υπολογίζουμε

$$\begin{array}{rcccccccc} x & \equiv & 0 & \pm 1 & \pm 2 & \pm 3 & \pm 4 & \pm 5 & \mod 11 \\ x^2 & \equiv & 0 & 1 & 4 & 9 & 5 & 3 & \mod 11 \end{array}.$$

Επομένως το 2 δεν είναι τετραγωνικό υπόλοιπο mod11.

Παράδειγμα. Είναι φανερό ότι το 1 είναι πάντοτε τετραγωνικό υπόλοιπο mod$p$, για κάθε (περιττό) πρώτο αριθμό p. Το ίδιο ισχύει και για κάθε τέλειο τετράγωνο ακέραιου αριθμού.

Εύκολα διαπιστώνεται από τα παραπάνω παραδείγματα, ότι το αντίστροφο της πρότασης που αναφέραμε στην παραπάνω παρατήρηση δεν ισχύει, για παράδειγμα, ενώ $\left(\frac{5}{11}\right) = \left(\frac{3}{11}\right)$, ισχύει $5 \not\equiv 3 \bmod 11$

Στα παραπάνω παραδείγματα παρατηρούμε ότι παίρνουμε όλα τα τετραγωνικά υπόλοιπα $\bmod p$ από τα τετράγωνα των αντιπροσώπων των κλάσεων $1, 2, \ldots, \frac{p-1}{2}$ και στη συνέχεια τα τετράγωνα των $\frac{p+1}{2}, \ldots, (p-1)$ μας ξαναδίνουν τα ίδια αλλά με αντίστροφη σειρά. Αυτό ισχύει γενικά

Πρόταση 5.1.4. *Για κάθε περιττό πρώτο p υπάρχουν ακριβώς $\frac{p-1}{2}$ μη-ισοδύναμα τετραγωνικά υπόλοιπα $\bmod p$ και συνεπώς ακριβώς $\frac{p-1}{2}$ που δεν είναι τετραγωνικά υπόλοιπα $\bmod p$.*

Απόδειξη. Αν η ισοτιμία $x^2 \equiv a \bmod p$, έχει λύση έστω x_0 τότε $p \nmid x_0$ αφού $p \nmid a$. Επομένως θα πρέπει να θεωρήσουμε τις κλάσεις $1, 2, \ldots, p-1 \bmod p$. Όμως επειδή

$$(p-x)^2 \equiv x^2 \bmod p$$

αρκεί να περιοριστούμε στο σύνολο των κλάσεων

$$\left\{1, 2, \ldots, \frac{p-1}{2} \bmod p\right\}.$$

Απομένει να δείξουμε ότι τα τετράγωνα

$$1^2, 2^2, \ldots, \frac{(p-1)^2}{4} \bmod p$$

είναι ανά δύο, μη ισοδύναμα $\bmod p$. Πράγματι, υποθέτουμε ότι υπάρχουν $b, c \in \left\{1, 2, \ldots, \frac{p-1}{2} \bmod p\right\}$ τέτοιοι ώστε $b^2 = c^2 \bmod p$. Επομένως

$$p \mid (c^2 - b^2) = (b-c)(b+c).$$

Επειδή $2 \leq b + c \leq p-1$, έπεται ότι $p \nmid (b+c)$. Συνεπώς $p \mid (b-c)$, και αφού $|b-c| \leq \frac{p-1}{2}$, συμπεραίνουμε ότι $b = c$. □

Παρατήρηση 5.1.5. Άμεση συνέπεια της πρότασης 5.1.4 είναι ότι

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

5.2 Ο τετραγωνικός νόμος αντιστροφής

Το σύμβολο του Legendre μπορεί να ιδωθεί ως συνάρτηση κατά δύο διαφορετικούς τρόπους. Ο ένας είναι να κρατήσουμε το p σταθερό και να θεωρήσουμε το $\left(\frac{a}{p}\right)$ ως συνάρτηση του a:

$$\chi_p(a) = \left(\frac{a}{p}\right).$$

Το ερώτημα λοιπόν είναι ποιοι ακέραιοι αριθμοί είναι τετραγωνικά υπόλοιπα $\bmod p$ όπου p δοσμένος πρώτος αριθμός p.

Μπορούμε όμως να θεωρήσουμε ότι μας δίνεται ο a και ότι το σύμβολο του Legendre είναι συνάρτηση του (περιττού) πρώτου αριθμού p

$$\psi_a(p) := \left(\frac{a}{p}\right).$$

Το ερώτημα εδώ είναι ως προς ποιους πρώτους p είναι ο δοσμένος ακέραιος a τετραγωνικό υπόλοιπο mod$p$.

Ποιά σχέση όμως υπάρχει ανάμεσα στα δύο ερωτήματα;

Προφανώς καμμία! Αυτή είναι βέβαια μια επιπόλαια απάντηση. Θα δούμε ότι υπάρχει σχέση και ότι η σχέση αυτή είναι πολύ σημαντική για τη Θεωρία Αριθμών.

Στο πρώτο ερώτημα θα λέγαμε ότι έχουμε ήδη έτοιμη την απάντηση. Αρκεί να θεωρήσουμε τις κλάσεις

$$1, 2, \ldots, \frac{p-1}{2} \mathrm{mod} p$$

και να υπολογίσουμε τα τετράγωνά τους

$$1^2, 2^2, \ldots, \frac{(p-1)^2}{4} \mathrm{mod} p$$

Όταν όμως ο p είναι αρκετά μεγάλος θα πρέπει να ψάξουμε να βρούμε άλλο τρόπο. Ας ξαναγυρίσουμε για λίγο στο θεώρημα του Fermat. Λόγω της υπόθεσης $p \nmid a$ έχουμε

$$a^{p-1} \equiv 1 \mathrm{mod} p$$

Ο $p-1$ είναι άρτιος, άρα $\frac{p-1}{2} \in \mathbb{Z}$. Επομένως η ισοτιμία γράφεται

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mathrm{mod} p$$

Συνεπώς

$$a^{\frac{p-1}{2}} \equiv \pm 1 \mathrm{mod} p$$

Πότε όμως είναι $+1$ και πότε -1; Αν $p = 7$ και $a = 2$ τότε $a^{\frac{p-1}{2}} = 2^{\frac{7-1}{2}} \equiv 1 \mathrm{mod} 7$ και $\left(\frac{a}{p}\right) = \left(\frac{2}{7}\right) = 1$, αφού το 2 είναι τετραγωνικό υπόλοιπο mod7. Αν $a = 3$ $a^{\frac{p-1}{2}} = 3^3 \equiv -1 \mathrm{mod} 7$ και $\left(\frac{3}{7}\right) = -1$. Ομοίως για $p = 11$ και $a = 2$, $a^{\frac{p-1}{2}} = 2^{\frac{11-1}{2}} \equiv -1 \mathrm{mod} 11$ και $\left(\frac{2}{11}\right) = -1$.

Η συσχέτιση του $a^{\frac{p-1}{2}} \mathrm{mod} p$ με την τιμή του συμβόλου του Legendre δεν είναι τυχαία. Διαπιστώθηκε και αποδείχτηκε για πρώτη φορά από τον Euler. Η επόμενη λοιπόν πρόταση είναι γνωστή προς τιμήν του στη βιβλιογραφία ως *κριτήριο του Euler*.

Πρόταση 5.2.1 (κριτήριο του Euler)**.** *Αν $a \in \mathbb{Z}$ και p περιττός πρώτος $p \nmid a$ τότε*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mathrm{mod} p$$

Απόδειξη. Για κάθε b, $1 \leq b \leq p-1$, η ισοτιμία $bx \equiv a \mathrm{mod} p$ έχει μοναδική λύση. Έστω c, $1 \leq c \leq p-1$ η λύση αυτή. Αν ο a δεν είναι τετραγωνικό υπόλοιπο mod$p$ τότε $b \neq c$. Επίσης αν $b_1 \neq b_2$ τότε $c_1 \neq c_2$. Επομένως, οι αριθμοί $1, 2, \ldots, p-1$ μπορούν να διαμεριστούν σε δύο ομάδες από $\frac{p-1}{2}$ αριθμούς η καθεμία, τους b_i και τους c_i για τους οποίους ισχύει

$$b_i c_i \equiv a \mathrm{mod} p \quad i = 1, 2, \ldots, \frac{p-1}{2}.$$

Το γινόμενο των ισοτιμιών αυτών δίνει

$$(p-1)! \equiv a^{\frac{p-1}{2}} \mathrm{mod} p$$

Λόγω του θεωρήματος του Wilson, $(p-1)! \equiv -1 \mathrm{mod} p$, άρα $\left(\frac{a}{p}\right) = -1$, δηλαδή

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mathrm{mod} p$$

Αν πάλι ο a είναι τετραγωνικό υπόλοιπο mod$p$ τότε για ένα ζευγάρι (b_0, c_0) έχουμε $b_0 = c_0$ και

$$b_0^2 \equiv a \mathrm{mod} p$$

Η ισοτιμία $x^2 \equiv a \mathrm{mod} p$ έχει λύση την $b_0 \mathrm{mod} p$ και την $(p - b_0) \mathrm{mod} p$. Σύμφωνα με το θεώρημα του Lagrange δεν υπάρχουν άλλες λύσεις.

Οι υπόλοιποι $(p-3)$ από τους αριθμούς $1, 2, \ldots, (p-1)$ διαμερίζονται και πάλι σε δύο ομάδες και όπως και προηγουμένως, διαμερίζονται σε δύο ομάδες όπου

$$b_i c_i \equiv a \mathrm{mod} p, \quad i = 1, 2, \ldots, \frac{p-3}{2}.$$

Πολλαπλασιάζουμε τις ισοτιμίες κατά μέλη και έχουμε

$$-1 \equiv (p-1)! \equiv b_0(p-b_0) a^{\frac{p-3}{2}} = -b_0^2 a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \mathrm{mod} p$$

Επομένως $a^{\frac{p-1}{2}} \equiv 1 \mathrm{mod} p$ και $\left(\frac{a}{p}\right) = 1$ δηλαδή και πάλι

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mathrm{mod} p$$

□

Πόρισμα 5.2.2. *1. Ισχύει* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

2. Αν $a = \prod_{i=1}^{s} a_i$ *και* $p \nmid a_i$ *για κάθε* $i = 1, 2, \ldots, s$ *τότε*

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{s} \left(\frac{a_i}{p}\right)$$

Απόδειξη. Για το πρώτο: Σύμφωνα με το κριτήριο του Euler $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mathrm{mod} p$. Επειδή είναι αδύνατο να ισχύει $-1 \equiv 1 \mathrm{mod} p$ (ο p είναι περιττός), έπεται ότι $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Για το δεύτερο: Λόγω του κριτηρίου του Euler και πάλι

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{s} a_i^{\frac{p-1}{2}} \equiv \prod_{i=1}^{s} \left(\frac{a_i}{p}\right) \mathrm{mod} p$$

Επομένως υπάρχει ακέραιος ℓ τέτοιος ώστε

$$\left(\frac{a}{p}\right) - \prod_{i=1}^{s} \left(\frac{a_i}{p}\right) = \ell \cdot p.$$

Οι δυνατές τιμές του αριστερού μέλους είναι $2, -2$ ή 0. Επειδή p περιττός πρώτος θα έχουμε $\ell = 0$, δηλαδή το ζητούμενο

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{s}\left(\frac{a_i}{p}\right).$$

□

Παρατήρηση 5.2.3. Το κριτήριο δημοσιεύθηκε με απόδειξη από τον Euler γύρω στα 1760. Ο ίδιος το είχε ανακοινώσει περισσότερα από δέκα χρόνια πριν. Εννοείται χωρίς την έκφραση μέσω του συμβόλου του Legendre, το οποίο δεν υπήρχε την εποχή του Euler.

Παρατήρηση 5.2.4. Η απόδειξη που δώσαμε είναι του Dirichlet. Αργότερα, μετά την επόμενη παράγραφο θα το ξαναποδείξουμε.

Παρατήρηση 5.2.5. Από το πόρισμα 5.2.2.2 προκύπτει ότι η συνάρτηση $\chi_p(\cdot)$ είναι πολλαπλασιαστική:

$$\chi_p(a \cdot b) = \chi_p(a)\chi_p(b).$$

Επομένως, αν συμβολίσουμε την έννοια του τετραγωνικού υπολοίπου με τη συντομογραφία QR και αυτή του μη-τετραγωνικού υπολοίπου με NQR, έχουμε τον ακόλουθο πίνακα πολλαπλασιασμού:

$$\begin{aligned} \mathrm{QR} \times \mathrm{QR} &= \mathrm{QR} \\ \mathrm{QR} \times \mathrm{NQR} &= \mathrm{NQR} \\ \mathrm{NQR} \times \mathrm{NQR} &= \mathrm{QR} \end{aligned}$$

Παρατήρηση 5.2.6. Μπορούμε να επεκτείνουμε το σύμβολο του Legendre και για ακέραιους a οι οποίοι διαιρούνται με p θέτοντας

$$\left(\frac{a}{p}\right) = 0, \text{ όταν } p \mid a.$$

Οι ιδιότητες, αν $a \equiv b \bmod p$ τότε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ και $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ συνεχίζουν να ισχύουν. Επίσης, το πλήθος των λύσεων της ισοτιμίας δίνεται από τον τύπο

$$\#\left\{x \bmod p : x^2 \equiv a \bmod p\right\} = 1 + \left(\frac{a}{p}\right).$$

Τέλος ισχύει

$$\sum_{a=0}^{p-1}\left(\frac{a}{p}\right) = 0.$$

Παρατήρηση 5.2.7. Στο ερώτημα πόσο πρακτικό είναι το κριτήριο του Euler απάντηση έδωσε ο ίδιος ο Gauss: «In praxi nullun fere usum habeat» δηλαδή «στην πράξη έχει μηδενική αξία», Disquisitiones Arithmeticae άρθρο 106.

Παρατήρηση 5.2.8. Αν $a = \varepsilon_a \prod_{i=1}^{s} p_i^{v_p(a)}$, η μονοσήμαντη ανάλυση του a σε γινόμενο πρώτων παραγόντων, $\varepsilon_a \in \{\pm 1\}$, τότε σύμφωνα με το πόρισμα 5.2.2.2

$$\left(\frac{a}{p}\right) = \left(\frac{\varepsilon_a}{p}\right)\prod_{i=1}^{s}\left(\frac{p_i}{p}\right).$$

Επομένως θα μπορούσαμε να υπολογίσουμε το σύμβολο του Legendre, αν γνωρίζαμε πώς να υπολογίσουμε το $\left(\frac{q}{p}\right)$, $q \in \mathbb{P}$. Για τον σκοπό μας αυτό σε πρώτο βήμα θα αποδείξουμε το παρακάτω

Πρόταση 5.2.9 (λήμμα του Gauss). *Έστω p περιττός πρώτος και a ακέραιος, $p \nmid a$. Έστω S το ελάχιστο σύστημα των αντιπροσώπων των κλάσεων υπολοίπων* $\mathrm{mod}p$ *των ακέραιων*

$$a, 2a, \ldots, \frac{1}{2}(p-1)a.$$

Αν r είναι το πλήθος των στοιχείων του S που είναι μεγαλύτερα από $\frac{p}{2}$ τότε

$$\left(\frac{a}{p}\right) = (-1)^r,$$

Απόδειξη. Αν $s = \frac{p-1}{2} - r$, $s + r = \frac{p-1}{2}$ και διαμερίσουμε τα στοιχεία του S σε δύο σύνολα

$$S_1 = \{a_1, a_2, \ldots, a_s\} \text{ και } S_2 = \{b_1, b_2, \ldots, b_r\}$$

όπου $a_i < \frac{p}{2}$ και $b_j > \frac{p}{2}$, τότε

$$\prod_{i=1}^{s} a_i \prod_{j=1}^{r} b_j \equiv \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \mathrm{mod}p \tag{5.2.1}$$

Οι ακέραιοι $a_1, a_2, \ldots, a_s, p-b_1, p-b_2, \ldots, p-b_r$ είναι όλοι στο διάστημα $[1, \frac{p-1}{2}]$, πλήθους $s + r = \frac{p-1}{2}$ και ανά δύο μη-ισότιμοι $\mathrm{mod}p$.

Πράγματι, αν ήταν $a_i = p - b_j$ για κάποια i, j, τότε θα υπήρχαν ακέραιοι k_i, ℓ_j $1 \le k_i, \ell_j \le \frac{p-1}{2}$ τέτοιοι ώστε

$$a_i \equiv k_i a \mathrm{mod}p \text{ και } b_j \equiv \ell_j a \mathrm{mod}p$$

οπότε θα είχαμε

$$(k_i + \ell_j)a \equiv a_i + b_j \equiv 0 \mathrm{mod}p$$

το οποίο όμως είναι άτοπο αφού $1 < k_i + \ell_j \le p - 1$.

Επομένως αποτελούν μια μετάθεση του συνόλου $\{1, 2, \ldots, \frac{p-1}{2}\}$. Άρα,

$$\left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{s} a_i \prod_{j=1}^{r} (p - b_j) \equiv (-1)^r \prod_{i=1}^{s} a_i \prod_{j=1}^{r} b_j \equiv (-1)^r \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \mathrm{mod}p.$$

Επειδή $p \nmid \left(\frac{p-1}{2}\right)!$ έπεται ότι

$$1 \equiv (-1)^r a^{\frac{p-1}{2}} \mathrm{mod}p$$

συνεπώς

$$(-1)^r \equiv a^{\frac{p-1}{2}} \mathrm{mod}p$$

και λόγω του κριτηρίου του Euler

$$\left(\frac{a}{p}\right) \equiv (-1)^r \mathrm{mod}p$$

Και πάλι οι δυνατές τιμές της παράστασης $\left(\frac{a}{p}\right) - (-1)^r$ είναι $2, 0, -2$ και επείδη ο p περιττός έχουμε

$$\boxed{\left(\frac{a}{p}\right) = (-1)^r}$$

□

Παράδειγμα. Αν $p = 17$ και $a = 7$ τότε $\frac{p-1}{2} = 8$ και

$$S = \left\{7, \boxed{14}, 4, \boxed{11}, 1, 8, \boxed{15}, 5\right\}.$$

Συνεπώς $r = 3$ και επομένως $\left(\frac{7}{17}\right) = (-1)^3 = -1$.

Παράδειγμα. Αν $a = 2$ θα εξετάσουμε ως προς ποιους πρώτους p είναι τετραγωνικό υπόλοιπο. Σύμφωνα με το λήμμα του Gauss θα πρέπει να υπολογίσουμε τους άρτιους ανάμεσα στο $\frac{p}{2}$ και το p. Αρκεί να υπολογίσουμε το πλήθος των ακέραιων στο διάστημα $\left(\frac{p}{4}, \frac{p}{2}\right)$. Γράφουμε τον p στη μορφή $8k + \ell$, $\ell = 1, 3, 5$ ή 7. Επομένως, θα πρέπει να ελέγξουμε αν το πλήθος των ακέραιων στο διάστημα

$$\left(2k + \frac{\ell}{4}, 4k + \frac{\ell}{2}\right),$$

είναι άρτιο ή περιττό. Στο υποδιάστημα $\left(2k + \frac{\ell}{4}, 4k + \frac{\ell}{4}\right)$ υπάρχει άρτιο πλήθος ακέραιων (αυτό είναι $2k$, επομένως αρκεί να υπολογίσουμε το πλήθος των ακέραιων στο διάστημα $\left(4k + \frac{\ell}{4}, 4k + \frac{\ell}{2}\right)$ ή στο διάστημα $\left(\frac{\ell}{4}, \frac{\ell}{2}\right)$. Αν $\ell = 1$, τότε $r = 0$, αν $\ell = 3$ τότε $r = 1$ αν $\ell = 5$ τότε $r = 1$ και αν $\ell = 7$ τότε $r = 2$. Επομένως έχουμε δείξει ότι:

Πόρισμα 5.2.10.

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{όταν } p \equiv \pm 1 \bmod 8 \\ -1 & \text{όταν } p \equiv \pm 3 \bmod 8 \end{cases}$$

Το πόρισμα αυτό μπορεί να διατυπωθεί και ως εξής:

$$\boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}}$$

Πράγματι, ο εκθέτης $\frac{p^2-1}{8}$ γράφεται

$$\frac{1}{2}\frac{(p-1)}{2}\frac{(p+1)}{2}$$

Οι $p-1$ και $p+1$ είναι διαδοχικοί άρτιοι. Άρα μόνο ο ένας διαιρείται με 4. Επομένως ο εκθέτης είναι άρτιος όταν ο παράγοντας αυτός διαιρείται με 8 δηλαδή όταν $p \equiv \pm 1 \bmod 8$ και περιττός, όταν δεν διαιρείται με 8, δηλαδή όταν $p \equiv \pm 3 \bmod 8$.

Με τη βοήθεια του λήμματος του Gauss θα αποδείξουμε την ακόλουθη:

Πρόταση 5.2.11. *Αν p περιττός πρώτος και a ακέραιος, $p \nmid a$ τότε*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}$$

Απόδειξη. Θεωρούμε τους αριθμούς

$$a, 2a, \ldots, \frac{1}{2}(p-1)a$$

τους οποίους διαιρούμε με p και έχουμε για k, $1 \le k \le \frac{p-1}{s}$:

$$ka = pq_k + v_k \text{ με } q_k, v_k \in \mathbb{Z} \text{ και } 0 \le v_k \le p-1.$$

Επομένως,

$$\frac{ka}{p} = q_k + \frac{v_k}{p} \text{ με } 0 \leq \frac{v_k}{p} < 1,$$

το οποίο σημαίνει ότι

$$q_k = \left[\frac{ka}{p}\right] \text{ και } ka = p\left[\frac{ka}{p}\right] + v_k.$$

Υποθέτουμε ότι $a_1, a_2, \ldots, a_s$ είναι οι τιμές των v_k οι οποίες είναι μικρότερες του $p/2$ και $b_1, b_2, \ldots, b_r$ αυτές που είναι μεγαλύτερες του $p/2$. Αν $C = \sum_{i=1}^{s} a_i$, $D = \sum_{j=1}^{r} b_j$ τότε

$$C + D = \sum_{k=1}^{\frac{p-1}{2}} v_k \tag{5.2.2}$$

Σύμφωνα με το λήμμα του Gauss $\left(\frac{a}{p}\right) = (-1)^r$. Οι ακέραιοι $a_1, a_2, \ldots, a_s, p-b_1, p-b_2, \ldots, p-b_r$ αποτελούν μια μετάθεση του $\{1, 2, \ldots, \frac{p-1}{2}\}$. Επομένως,

$$C + rp - D = \sum_{i=1}^{s} a_i + \sum_{j=1}^{r}(p - b_j) = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8}. \tag{5.2.3}$$

Επίσης,

$$p\sum_{k=1}^{\frac{p-1}{2}} q_k + C + D = \sum_{k=1}^{\frac{p-1}{2}}(pq_k + v_k) = \sum_{k=1}^{\frac{p-1}{2}} ka = \frac{p^2-1}{8}a \tag{5.2.4}$$

Αφαιρούμε την (5.2.3) από την (5.2.4) και έχουμε

$$p\sum_{k=1}^{\frac{p-1}{2}} q_k + 2D - rp = \frac{p^2-1}{8}(a-1). \tag{5.2.5}$$

Μέχρις εδώ πουθενά δεν χρησιμοποιήσαμε την υπόθεση ότι ο a είναι περιττός. Επειδή $\frac{p^2-1}{8}$ ακέραιος και a, p περιττός η (5.2.5) μας δίνει

$$\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv r \bmod 2 \tag{5.2.6}$$

δηλαδή

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]}$$

□

Παράδειγμα. Να υπολογισθεί το σύμβολο του Legendre $\left(\frac{23}{47}\right)$.

Θα πρέπει να υπολογίσουμε το άθροισμα

$$\sum_{k=1}^{23}\left[\frac{23k}{47}\right] \bmod 2$$

Επειδή κάθε φορά το ακέραιο μέρος παίρνει την ίδια τιμή για ακριβώς δύο τιμές του k, το παραπάνω άθροισμα μέχρι την τιμή $k = 22$ είναι άρτιο. Για $k = 23$ $\left[\frac{23\cdot 23}{47}\right] = 11$. Επομένως,

$$\sum_{k=1}^{23}\left[\frac{23k}{47}\right] \equiv 1 \bmod 2$$

και συνεπώς $\left(\frac{23}{47}\right) = -1$.

Το επόμενο θεώρημα, είναι ένα από τα πιο σημαντικά αποτελέσματα της Θεωρίας Αριθμών και σίγουρα το σημαντικότερο της κλασικής Αριθμοθεωρίας. Αυτό, όχι μόνο διότι μας επιτρέπει να υπολογίζουμε πολύ εύκολα τα τετραγωνικά υπόλοιπα, αλλά και για το θεωρητικό του βάθος. Η πρώτη πλήρης απόδειξη δόθηκε από τον Gauss στα 1795 λίγο πριν συμπληρώσει το 18ο έτος της ηλικίας του. Αργότερα θα επανέλθουμε με περισσότερα ιστορικά στοιχεία.

Θεώρημα 5.2.12 (Νόμος τετραγωνικής αντιστροφής)**.** *Αν p, q περιττοί πρώτοι $p \neq q$, τότε*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

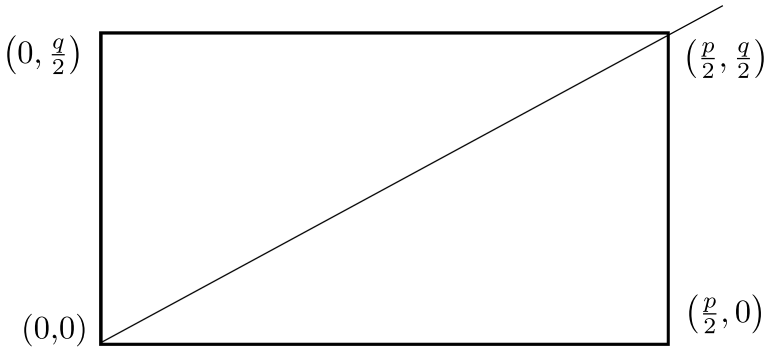
Απόδειξη. Εφαρμόζουμε την πρόταση 5.2.11 δύο φορές, για το $\left(\frac{p}{q}\right)$ και το $\left(\frac{q}{p}\right)$ και έχουμε:

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right]} \text{ και } \left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kq}{p}\right]}.$$

Επομένως αρκεί να αποδείξουμε ότι

$$\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right] + \sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kq}{p}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}. \tag{5.2.7}$$

Η απόδειξη της σχέσης αυτής θα γίνει γεωμετρικά. Θεωρούμε το ορθογώνιο παραλληλόγραμμο με κορυφές $(0,0), \left(\frac{p}{2}, 0\right), \left(\frac{p}{2}, \frac{q}{2}\right), \left(0, \frac{q}{2}\right)$. Η ευθεία που συνδέει τα σημεία $(0,0)$ και $\left(\frac{p}{2}, \frac{q}{2}\right)$ είναι η



Σχήμα 5.2.1: Γεωμετρική απόδειξη τετραγωνικής αντιστροφής

$$y = \frac{q}{p}x,$$

η οποία χωρίζει το ορθογώνιο σε δύο ίσα μέρη. Πάνω στην ευθεία αυτή δεν υπάρχουν σημεία με ακέραιες συντεταγμένες για

$$x = 1, 2, \ldots, \frac{p-1}{2}.$$

Για $x = j \in \mathbb{Z}$ φέρνουμε την ευθεία που είναι κάθετη στον άξονα των x στο σημείο $(j, 0)$. Αυτή τέμνει τη διαγώνιο $y = \frac{q}{p}x$ στο σημείο $\left(j, \frac{q}{p}j\right)$. Το πλήθος των σημείων με ακέραιες συντεταγμένες μέχρι εκεί είναι $\left[\frac{q}{p}j\right]$. Συνολικά λοιπόν στο κάτω τρίγωνο του παραλληλογράμμου υπάρχουν $\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{q}{p}j\right]$ σημεία με ακέραιες συντεταγμένες, ενώ στο πάνω τρίγωνο τα σημεία είναι $\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{p}{q}k\right]$. Συνολικά όμως τα σημεία με ακέραιες συντεταγμένες στο ορθογώνιο είναι $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Συνεπώς η σχέση (5.2.7) έχει αποδειχθεί. □

Οι παρακάτω εξισώσεις αποτελούν τον νόμο τετραγωνικής αντιστροφής p, q περιττοί πρώτοι $p \neq q$.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{I}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{II}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{III}$$

Η (I) λέγεται πρώτο συμπλήρωμα της (III) και η (II) δεύτερο συμπλήρωμα αυτής.

Παρατήρηση 5.2.13. Ο τετραγωνικός νόμος αντιστροφής (III) μπορεί να γραφεί και στη μορφή:
Αν p, q περιττοί πρώτοι και $p \neq q$ τότε

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{όταν } p \equiv 1 \bmod 4 \text{ ή } q \equiv 1 \bmod 4 \\ -1 & \text{όταν } p \equiv q \equiv 3 \bmod 4 \end{cases} \tag{IIIα}$$

καθώς επίσης και στη μορφή:
Αν p, q περιττοί πρώτοι και $p \neq q$ τότε

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{όταν } p \equiv 1 \bmod 4 \text{ ή } q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & \text{όταν } p \equiv q \equiv 3 \bmod 4 \end{cases} \tag{III β}$$

Με βάση τον τετραγωνικό νόμο αντιστροφής μπορούμε να ελέγξουμε αν η τετραγωνική ισοτιμία

$$x^2 \equiv a \bmod p, p \in \mathbb{P}, p \neq 2$$

έχει λύση ή όχι. Αρκεί να ακολουθήσουμε τον εξής αλγόριθμο.

1. Αναλύουμε τον a σε γινόμενο παραγόντων. Το $\left(\frac{a}{p}\right)$ γράφεται ως γινόμενο συμβόλων του Legendre της μορφής $\left(\frac{q}{p}\right)$ όπου $q \in \text{ιι} \in \mathbb{P}$, $q \neq 2$, $\left(\frac{-1}{p}\right)$ και $\left(\frac{2}{p}\right)$.

2. Υπολογίζουμε τα $\left(\frac{-1}{p}\right)$ και $\left(\frac{2}{p}\right)$ μέσω των (I) και (II) και εφαρμόζουμε τον νόμο αντιστροφής (III) για τα σύμβολα $\left(\frac{p}{q}\right)$ αντικαθιστώντας τα με $\left(\frac{q}{p}\right) - \left(\frac{q}{p}\right)$.

3. Ανάγουμε το $p \bmod q$ και επαναλαμβάνουμε τη διαδικασία.

Παράδειγμα. Να εξετασθεί αν η ισοτιμία

$$x^2 \equiv 23 \bmod 47,$$

έχει λύση.

Οι αριθμοί 23 και 47 είναι περιττοί πρώτοι. Επομένως

$$\left(\frac{23}{47}\right) = (-1)^{\frac{23-1}{2}\frac{47-1}{2}}\left(\frac{47}{23}\right) = (-1)\left(\frac{1}{47}\right) = -1.$$

Άρα η ισοτιμία μας δεν έχει λύση.

Παράδειγμα. Να εξετασθεί αν η ισοτιμία

$$x^2 \equiv -154 \mathrm{mod} 163$$

έχει λύση. Ο 163 είναι πρώτος αριθμός ενώ το -154 αναλύεται σε γινόμενο πρώτων παραγόντων $-154 = (-1)\cdot 2\cdot 7\cdot 11$. Επομένως

$$\left(\frac{-154}{163}\right) = \left(\frac{-1}{163}\right)\left(\frac{2}{163}\right)\left(\frac{7}{163}\right)\left(\frac{11}{163}\right)$$

Τώρα

$$\left(\frac{-1}{163}\right) = (-1)^{\frac{163-1}{2}} = (-1)^{81} = -1.$$

Επειδή $163 \equiv 3 \mathrm{mod} 8$, έχουμε $\left(\frac{2}{163}\right) = -1$. Επίσης αφού $7 \equiv 1 \mathrm{mod} 4$

$$\left(\frac{7}{163}\right) = -\left(\frac{163}{7}\right) = -\left(\frac{2}{7}\right) = (-1)(+1) = -1.$$

Αφού $11 \equiv 3 \mathrm{mod} 4$

$$\left(\frac{11}{163}\right) = -\left(\frac{163}{11}\right) = -\left(\frac{9}{11}\right) = -\left(\frac{3}{11}\right)^2 = -1.$$

Τελικά έχουμε

$$\left(\frac{-154}{163}\right) = (-1)(-1)(-1)(-1) = +1$$

και συνεπώς η ισοτιμία έχει λύση.

Παράδειγμα. Να εξετασθεί αν η ισοτιμία

$$x^2 \equiv -42 \mathrm{mod} 61$$

έχει λύση.

Εργαζόμενοι όπως παραπάνω υπολογίζουμε το σύμβολο του Legendre $\left(\frac{-42}{61}\right) = 1$ και επομένως η ισοτιμία έχει λύση.

Παράδειγμα. Για ποιους περιττούς πρώτους αριθμούς p η ισοτιμία

$$x^2 \equiv 5 \mathrm{mod} p$$

έχει λύση;

Η ισοτιμία έχει λύση ακριβώς τότε όταν $\left(\frac{5}{p}\right) = 1$. Τώρα $\left(\frac{5}{p}\right) = 1$ αν και μόνο αν $\left(\frac{p}{5}\right) = 1$. Αν $p \equiv 1, 4 \mathrm{mod} 5$ τότε $\left(\frac{p}{5}\right) = 1$.

Αν $p \equiv 2, 3 \mathrm{mod} 5$ τότε $\left(\frac{p}{5}\right) = -1$.

Συνεπώς έχει λύση ακριβώς τότε όταν

$$p \equiv \pm 1 \mathrm{mod} 5.$$

Η παραπάνω διαδικασία είναι ένας πολύ αποτελεσματικός αλγόριθμος από τον οποίο παίρνουμε απάντηση σε περίπου τόσα βήματα όσα ο αριθμός των ψηφίων του p. Το πιο δύσκολο στάδιο είναι η παραγοντοποίηση του a και του αντιπροσώπου του $p \mathrm{mod} q$ κάθε φορά που εφαρμόζουμε τον νόμο αντιστροφής στο $\left(\frac{q}{p}\right)$.

5.2.1 Το σύμβολο του Jacobi

Το σύμβολο του Jacobi ορίζεται μέσω του συμβόλου του Legendre και αποτελεί γενίκευση αυτού.

Αν b περιττός ακέραιος $b = \varepsilon p_1 p_2 \cdots p_s$, η ανάλυση αυτού σε γινόμενο πρώτων παραγόντων p_i ($i = 1, 2, \ldots, s$) όχι κατ' ανάγκη διαφορετικών μεταξύ τους ($\varepsilon = \pm 1$) και a ακέραιος πρώτος προς τον b, τότε το σύμβολο του Jacobi ορίζεται

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right).$$

Οι ιδιότητες του συμβόλου του Jacobi είναι ανάλογες αυτών του συμβόλου του Legendre.

1. $$\left(\frac{a}{b}\right) = \left(\frac{a}{|b|}\right)$$

2. $$\left(\frac{1}{b}\right) = 1$$

3. Αν $a_1 = a_2 \bmod |b|$, τότε
$$\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$$

4. Αν $(a_i, b) = 1$ για κάθε $i = 1, 2, \ldots, n$ τότε
$$\left(\frac{a_1 a_2 \cdots a_n}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)\cdots\left(\frac{a_n}{b}\right)$$

5. Αν $b_1, b_2, \ldots, b_n$ περιττοί ακέραιοι και a ακέραιος με $(a, b_1 b_2 \cdots b_n) = 1$, τότε
$$\left(\frac{a}{b_1 b_2 \cdots b_n}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)\cdots\left(\frac{a}{b_n}\right)$$

6. $$\left(\frac{-1}{b}\right) = (-1)^{\frac{|b|-1}{2}}$$

7. $$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

8. $$\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2} + \frac{\operatorname{sgn} a - 1}{2}\cdot\frac{\operatorname{sgn} b - 1}{2}} \left(\frac{a}{b}\right)$$

Υπενθυμίζουμε ότι το πρόσημο $\operatorname{sgn}(a)$ ενός πραγματικού αριθμού a ορίζεται ως:

$$\operatorname{sgn}(a) = \begin{cases} +1 & \text{αν } a > 0 \\ 0 & \text{αν } a = 0 \\ -1 & \text{αν } a < 0 \end{cases}$$

Τέλος, αν ο a είναι τετραγωνικό υπόλοιπο $\bmod |b|$, δηλαδή αν η ισοτιμία

$$x^2 \equiv a \bmod |b|$$

έχει λύση τότε και οι ισοτιμίες

$$x^2 \equiv a \bmod p_i$$

θα έχουν λύση για κάθε πρώτο διαιρέτη p_i του b. Συνεπώς θα έχουμε $\left(\frac{a}{p_i}\right) = 1$ οπότε και $\left(\frac{a}{b}\right) = 1$.

Προσοχή Το αντίστροφο δεν ισχύει. Για παράδειγμα $\left(\frac{1}{15}\right) = 1$ και η $x^2 \equiv 1 \bmod 15$ είναι επιλύσιμη, ενώ $\left(\frac{2}{15}\right) = 1$ και η $x^2 \equiv 2 \bmod 15$ δεν είναι επιλύσιμη.

Από τα παραπάνω συμπεραίνουμε ότι αν $\left(\frac{a}{b}\right) = -1$, τότε η ισοτιμία $x^2 \equiv a \bmod |b|$ δεν έχει λύση.

Η χρήση του συμβόλου του Jacobi μας απαλλάσσει από το «καθήκον» της παραγοντοποίησης, μιας πραγματικά χρονοβόρας και για μεγάλους ακέραιους, δύσκολης διαδικασίας στην οποία είμαστε υποχρεωμένοι να καταφύγουμε, όταν χρησιμοποιούμε το σύμβολο του Legendre. Αυτά που πρέπει μόνο να ελέγξουμε είναι ότι ο b είναι περιττός και ότι ο a είναι πρώτος προς τον b.

Στη συνέχεια θα αναφερθούμε σε έναν αλγόριθμο υπολογισμού του συμβόλου Jacobi γνωστού στη βιβλιογραφία ως ο «κανόνας του Eisenstein» [32, σελ. 329-333], [17, σελ. 132-133], [20, σελ. 362-364], σύμφωνα με τον οποίο ο υπολογισμός είναι τόσο γρήγορος όσο και ο ευκλείδειος αλγόριθμος υπολογισμού του μέγιστου κοινού διαιρέτη.

Έστω a και b πρώτοι μεταξύ τους θετικοί ακέραιοι με $a > b$. Συμβολίζουμε με $A_0 := a$ και $A_1 := b$. Εφαρμόζουμε το θεώρημα διαίρεσης με πηλίκο αλλά συγχρόνως παραγοντοποιούμε το υπόλοιπο σε δύναμη του 2 και περιττό ακέραιο. Έτσι έχουμε

$$A_0 = A_1 q_1 + 2^{\ell_1} A_2, \quad \ell_1 \geq 0, 0 < A_2 < A_1.$$

Συνεχίζουμε, κάνοντας το ίδιο μεταξύ των A_1, A_2 κ.ο.κ

$$\begin{aligned}
A_1 &= A_2 q_2 + 2^{\ell_2} A_3, \quad \ell_2 \geq 0, 0 < A_3 < A_2 \\
A_2 &= A_3 q_3 + 2^{\ell_3} A_4, \quad \ell_3 \geq 0, 0 < A_4 < A_3 \\
&\dots \\
A_{n-3} &= A_{n-2} q_{n-2} + 2^{\ell_{n-2}} A_{n-1}, \quad \ell_{n-2} \geq 0, 0 < A_{n-1} < A_{n-2} \\
A_{n-2} &= A_{n-1} q_{n-1} + 2^{\ell_{n-1}} \cdot 1
\end{aligned}$$

Πρόταση 5.2.14. *Αν a, b θετικοί ακέραιοι, $a > b$ πρώτοι μεταξύ τους και b περιττός τότε*

$$\left(\frac{a}{b}\right) = (-1)^{\ell_1 \frac{A_1^2-1}{2} + \dots + \ell_{n-1} \frac{A_{n-1}^2-1}{2} + \frac{A_1-1}{2} \cdot \frac{A_2-1}{2} + \dots + \frac{A_{n-2}}{2} \cdot \frac{A_{n-1}-1}{2}}$$

Απόδειξη. Εφαρμόζουμε τις ιδιότητες του συμβόλου Jacobi

$$\left(\frac{a}{b}\right) = \left(\frac{A_0}{A_1}\right) = \left(\frac{2^{\ell_1} A_2}{A_1}\right) = \left(\frac{2}{A_1}\right)^{\ell_1} \left(\frac{A_2}{A_1}\right) =$$

$$= (-1)^{\ell_1 \frac{A_1^2-1}{8}} \cdot (-1)^{\frac{A_1-1}{2} \cdot \frac{A_2-1}{2}} \left(\frac{A_1}{A_2}\right) =$$

$$(-1)^{\ell_1 \frac{A_1-1}{8} + \frac{A_1-1}{2} \cdot \frac{A_2-1}{2}} \cdot \left(\frac{2^{\ell_2}}{A_2}\right)\left(\frac{A_3}{A_2}\right)$$

και συνεχίζουμε ανάλογα. □

Παράδειγμα. Να υπολογιστεί το σύμβολο του Jacobi $\left(\frac{1105}{231}\right)$.

Επαληθεύουμε ότι οι a, b είναι πρώτοι μεταξύ τους. Σύμφωνα με την πρόταση 5.2.14, έχουμε

$$\begin{array}{rcll} 1105 & = & 231 \cdot 4 + 181, & A_1 = 251, \quad \ell_1 = 0 \\ 231 & = & 181 \cdot 1 + 2 \cdot 25, & A_2 = 185, \quad \ell_2 = 1 \\ 181 & = & 25 \cdot 7 + 2 \cdot 3, & A_3 = 25, \quad \ell_3 = 1 \\ 25 & = & 3 \cdot 8 + 1, & A_4 = 3, \quad \ell_4 = 0 \end{array}$$

Επομένως το σύμβολο του Jacobi

$$\left(\frac{1105}{231}\right) = (-1)^m,$$

όπου

$$m = 0 \cdot \frac{231^2-1}{8} + \frac{181^2-1}{8} + 1 \cdot \frac{25^2-1}{8} + 0 \cdot \frac{3^2-1}{8} + \frac{231-1}{2} \cdot \frac{181-1}{2} + \frac{181-1}{2} \frac{25-1}{2} + \frac{25-1}{2} \cdot \frac{3-1}{2}.$$

Ο μόνος περιττός προσθετέος του εκθέτη m είναι ο $1 \cdot \frac{181^2-1}{8}$ Άρα $m \equiv 1 \mathrm{mod} 2$ και

$$\left(\frac{1105}{231}\right) = -1.$$

Θεωρούμε και πάλι δύο περιττούς θετικούς ακέραιους a, b πρώτους μεταξύ τους. Σύμφωνα με το θεώρημα της διαίρεσης με υπόλοιπο, υπάρχουν μοναδικοί ακέραιοι q, r τέτοιοι ώστε

$$a = bq + r, \quad 1 \leq r < b.$$

Μπορούμε να γράψουμε τη σχέση και ως εξής:

$$a = b(q+1) + (b-r), \quad 1 \leq b - r < b.$$

Επειδή $(b-r) + r = b$ είναι περιττός ακέραιος, ένας ακριβώς από τους $r, b-r$ είναι άρτιος και ο άλλος περιττός.

Άρα ο a γράφεται μονοσήμαντα στη μορφή

$$a = bq + \varepsilon \cdot r,$$

όπου $\varepsilon = \pm 1$ και r περιττός $1 \leq r < b$. Παρατηρούμε ότι ο q θα πρέπει να είναι άρτιος, διότι αλλιώς ο $a \pm r$ θα ήταν περιττός.

Επομένως, υπάρχουν μονοσήμαντα ορισμένοι ακέραιοι q_1 και r_1, r_1 περιττός $1 \leq r_1 < b$ ώστε να ισχύει

$$a = 2q_1 b + \varepsilon_1 r_1, \text{ με } \varepsilon_1 = \pm 1.$$

Εφαρμόζουμε διαδοχικά την παραπάνω σχέση γράφοντας $A_0 = b$ και $A_i = r_i$ και έχουμε

$$\begin{array}{rcl} a & = & 2q_1 A_0 + \varepsilon_1 A_1, A_1 \text{ περιττός } 1 \leq A_1 < A_0, \varepsilon_1 = \pm 1 \\ A_0 & = & 2q_2 A_1 + \varepsilon_2 A_2, A_2 \text{ περιττός } 1 \leq A_2 < A_1, \varepsilon_2 = \pm 1 \\ A_1 & = & 2q_3 A_2 + \varepsilon_3 A_3, A_3 \text{ περιττός } 1 \leq A_2 < A_2, \varepsilon_3 = \pm 1 \\ \ldots & & \\ A_{n-3} & = & 2q_{n-1} A_{n-2} + \varepsilon_{n-1} A_{n-1}, A_{n-1} \text{ περιττός }, 1 \leq A_{n-1} < A_{n-2} \\ A_{n-2} & = & 2q_n A_{n-1} + \varepsilon_n A_n, \text{ με } A_n = 1 \text{ και } \varepsilon_n = \pm 1. \end{array}$$

Η ακολουθία των $(A_i)_{i \in \mathbb{N}}$ είναι γνήσια φθίνουσα ακολουθία φυσικών αριθμών. Άρα μετά από πεπερασμένο πλήθος βημάτων θα έχουμε $A_n = 1$.

Το σύμβολο Jacobi.

$$\left(\frac{a}{b}\right)=\left(\frac{a}{A_0}\right)=\left(\frac{\varepsilon_1 A_1}{A_0}\right)=\left(\frac{\varepsilon_1}{A_0}\right)\left(\frac{A_1}{A_0}\right).$$

Το $\left(\frac{\varepsilon_1}{A_0}\right)=(-1)^{\frac{A_0-1}{2}\frac{1=\varepsilon_1}{2}}$. Πράγματι, αν $\varepsilon_1=1$ τότε

$$\left(\frac{\varepsilon_1}{A_0}\right)=1=(-1)^{\frac{A_0-1}{2}\frac{1-e_1}{2}}.$$

Αν πάλι $\varepsilon_1=-1$, τότε

$$\left(\frac{\varepsilon_1}{A_0}\right)=(-1)^{\frac{A_0-1}{2}}=(-1)^{\frac{A_0-1}{2}\frac{1-e_1}{2}}.$$

Συνεπώς,

$$\left(\frac{a}{b}\right)=\left(\frac{a}{A_0}\right)=(-1)^{\frac{A_0-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{A_0-1}{2}\cdot\frac{A_1-1}{2}}\left(\frac{A_0}{A_1}\right).$$

Αν τώρα λάβουμε υπόψη ότι $\varepsilon_1^2=1$ και ότι $(-1)^{a/\varepsilon_1}=(-1)^a$ για κάθε ακέραιο a, έχουμε

$$\frac{A_0-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{A_0-1}{2}\cdot\frac{A_1-1}{2}=\frac{A_0-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{A_0-1}{2}\cdot\frac{A_1-\varepsilon_1}{2}$$

$$=\frac{A_0-1}{2}\cdot\frac{\varepsilon_1A_1-\varepsilon_1^2}{2\varepsilon_1}=\frac{A_0-1}{2}\cdot\frac{\varepsilon_1A_1-1}{2\varepsilon_1}$$

και

$$(-1)^{\frac{A_0-1}{2}\cdot\frac{\varepsilon_1A_1-1}{2\varepsilon_1}}\left(\frac{A_0}{A_1}\right).$$

Επαναλαμβάνουμε διαδοχικά τη διαδικασία και έχουμε:

$$\left(\frac{A_0}{A_1}\right)=(-1)^{\frac{A_1-1}{2}\cdot\frac{e_2A_2-1}{2}}\left(\frac{A_1}{A_2}\right)$$

$$\left(\frac{A_{n-3}}{A_{n-2}}\right)=(-1)^{\frac{A_{n-2}-1}{2}\cdot\frac{e_{n-1}A_{n-1}-1}{2}}\left(\frac{A_{n-2}}{A_{n-1}}\right)$$

$$\left(\frac{A_{n-2}}{A_{n-1}}\right)==\left(\frac{\varepsilon_n}{A_{n-1}}\right)=(-1)^{\frac{A_{n-1}-1}{2}\cdot\frac{e_nA_{n-1}-1}{2}}=(-1)^{\frac{A_n-1}{2}\cdot\frac{\varepsilon_nA_n-1}{2}}.$$

Από τα παραπάνω συμπεραίνουμε ότι

$$\left(\frac{a}{b}\right)=(-1)^{\ell}$$

με

$$\ell:=\sum_{i=1}^{n}\frac{A_{i-1}-1}{2}\cdot\frac{\varepsilon_iA_i-1}{2}$$

και $A_n=1$.

Ένας προσθετέος του ℓ

$$\frac{A_{i-1}-1}{2}\cdot\frac{\varepsilon_iA_i-1}{2}$$

είναι περιττός ακριβώς τότε όταν

$$A_{i-1}\equiv 3\text{mod}4 \text{ και } \varepsilon_iA_i\equiv 3\text{mod}4$$

Πρόταση 5.2.15 (Κανόνας του Eisenstein)**.** *Αν a, b περιττοί θετικοί ακέραιοι πρώτοι μεταξύ τους τότε*

$$\left(\frac{a}{b}\right) = (-1)^m,$$

όπου

$$m = \#\{(A_{i-1}, \varepsilon_i A_i) : A_{i-1} \equiv 3\text{mod}4 \text{ και } \varepsilon_i A_i \equiv 3\text{mod}4, \quad i = 1, 2, \ldots, n-1\}.$$

Παράδειγμα. Να υπολογιστεί το σύμβολο του Jacobi $\left(\frac{335}{2999}\right)$.

Ελέγχουμε πρώτα από όλα ότι $(335, 2999) = 1$. Γράφουμε

$335 = 2999 \cdot 0 + 335$	$A_0 = 2999$	$\varepsilon_1 = 1, A_1 = 335$
$2999 = 8 \cdot 335 + 319$	$\varepsilon_2 = 1$	$A_2 = 319$
$335 = 2 \cdot 319 + (-1) \cdot 283$	$\varepsilon_3 = -1$	$A_3 = 283$
$319 = 2 \cdot 283 + (-1)247$	$\varepsilon_4 = -1$	$A_4 = 247$
$283 = 2 \cdot 247 + (-1)211$	$\varepsilon_5 = -1$	$A_5 = 211$
$247 = 2 \cdot 211 + (-1)175$	$\varepsilon_6 = -1$	$A_6 = 175$
$211 = 2 \cdot 175 + (-1)139$	$\varepsilon_7 = -1$	$A_7 = 139$
$175 = 2 \cdot 139 + (-1)103$	$\varepsilon_8 = -1$	$A_8 = 103$
$139 = 2 \cdot 103 + (-1)67$	$\varepsilon_9 = -1$	$A_9 = 67$
$103 = 2 \cdot 67 + (-1)31$	$\varepsilon_{10} = -1$	$A_{10} = 31$
$67 = 2 \cdot 31 + 5$	$\varepsilon_{11} = 1$	$A_{11} = 5$
$31 = 6 \cdot 5 + 1$	$\varepsilon_{12} = 1$	$A_{12} = 1$

Σχηματίζουμε τα ζευγάρια

$$\begin{aligned}
(A_0, \varepsilon_1 A_1) &= (2999, 335)\\
(A_1, \varepsilon_2 A_2) &= (335, 319)\\
(A_2, \varepsilon_3 A_3) &= (319, -283)\\
(A_3, \varepsilon_4 A_4) &= (283, -247)\\
(A_4, \varepsilon_5 A_5) &= (247, -211)\\
(A_5, \varepsilon_6 A_6) &= (211, -175)\\
(A_6, \varepsilon_7 A_7) &= (175, -103)\\
(A_7, \varepsilon_8 A_8) &= (139, 335)\\
(A_8, \varepsilon_9 A_9) &= (103, -67)\\
(A_9, \varepsilon_{10} A_{10}) &= (67, -31)\\
(A_{10}, \varepsilon_{11} A_{11}) &= (31, 5)\\
(A_{11}, \varepsilon_{12} A_{12}) &= (5, 1)
\end{aligned}$$

Επομένως $m = 2$ και $\left(\frac{335}{2999}\right) = 1$.

Παρατήρηση 5.2.16. Επειδή στο παράδειγμά μας ο 2999 είναι πρώτος το σύμβολο του Jacobi είναι και σύμβολο του Legendre. Συνεπώς η ισοτιμία

$$x^2 \equiv 335\text{mod}2999$$

έχει λύση.

Παρατήρηση 5.2.17. Ο κανόνας του Eisenstein αποδείχθηκε κάπως μακροσκελής στο συγκεκριμένο παράδειγμα. Ας δοκιμάσουμε κατ' ευθείαν με χρήση του νόμου αντιστροφής του Jacobi.

$$\left(\frac{335}{2999}\right) = -\left(\frac{2999}{335}\right) = -\left(\frac{319}{335}\right) = -\left(\frac{-16}{319}\right) = -1\left(\frac{-1}{319}\right) = -(-1) = +1.$$

Παρατήρηση 5.2.18. Να υπολογισθεί το σύμβολο του Jacobi

$$\left(\frac{514}{1573}\right) = \left(\frac{2\cdot 257}{1573}\right) = \left(\frac{2}{1573}\right)\left(\frac{257}{1573}\right).$$

Επειδή $1573 \equiv 5 \bmod 8$ έχουμε $\left(\frac{2}{1573}\right) = -1$.

$257 = 1573 \cdot 0 + 257$	$A_0 = 1573,$	$\varepsilon_1 = 1, A_1 = 257$
$1573 = 6 \cdot 257 + 31$	$\varepsilon_1 = 1$	$A_2 = 31$
$257 = 8 \cdot 31 + 9$	$\varepsilon_3 = 1$	$A_3 = 9$
$31 = 4 \cdot 9 + (-1)5$	$\varepsilon_4 = -1$	$A_4 = 5$
$9 = 2 \cdot 5 + (-1)1$	$\varepsilon_5 = -1$	$A_5 = 1$

Σχηματίζουμε τα ζευγάρια $(1573, 257), (257, 31), (31, 9), (9, -5), (5, -1)$ και καταλήγουμε στο $m = 0$ και $\left(\frac{514}{1573}\right) = (-1)(-1)^0 = -1$.

5.2.2 Εύρεση των λύσεων

Είδαμε ότι τελικά είναι σχετικά εύκολη η διαπίστωση της ύπαρξης η μή λύσεων της ισοτιμίας

$$x^2 \equiv a \bmod p$$

Εάν τώρα διαπιστώσουμε την ύπαρξη λύσεων τότε πώς θα βρούμε τις λύσεις;

Αν στην $x^2 \equiv a \bmod p$ έχουμε $p \equiv 3 \bmod 4$ και $\left(\frac{a}{p}\right) = +1$ τότε μια λύση είναι η $x_0 \equiv a^{\frac{p+1}{4}} \bmod p$ αφού

$$x_0^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}+1} \equiv a^{\frac{p-1}{2}} \cdot a \equiv \left(\frac{a}{p}\right) a \equiv a \bmod p$$

Η άλλη ρίζα είναι προφανώς η $x_0 \equiv -a^{\frac{p+1}{4}} \bmod p$.

Αν τώρα $p \equiv 1 \bmod 4$, δεν είναι γνωστός ο ντετερμινιστικός αλγόριθμος (πολυωνυμικού χρόνου) ο οποίος να μας δίνει τις λύσεις τις ισοτιμίας.

Θα περιγράψουμε έναν πιθανοθεωρητικό αλγόριθμο.

Έστω $z \bmod p$ κάποια τυχαία επιλεγείσα κλάση $1 \le z \le p-1$ και έστω

$$u + vx := (1 + zx)^{\frac{p-1}{2}}.$$

Αν $v \neq 0$, τότε οι λύσεις της ισοδυναμίας x_0, x_0' υπολογίζονται ως εξής:

Ο $u + vx_0 := (1 + zx_0)^{\frac{p-1}{2}}$ είναι μία $\frac{p-1}{2}$-δύναμη $\bmod p$. Επομένως ισούται με $0, 1$ ή $-1 \bmod p$. Συνεπώς $x_0 \equiv -\frac{u}{v}, \frac{1-u}{v}$, ή $-\frac{1+u}{v} \bmod p$.

Γνωρίζουμε τα u, v. Δοκιμάζουμε αν τα $-\frac{u}{v}, \frac{1-u}{v}$ και $-\frac{1+u}{v}$ είναι τετραγωνικά υπόλοιπα $\bmod p$.

Παράδειγμα. Να λυθεί η

$$x^2 \equiv 69 \bmod 389$$

Είναι $p = 389 \equiv 1 \bmod 4$. Επιλέγουμε $z \equiv 24 \bmod 389$ και υπολογίζουμε

$$(1 + 24x)^{194} = -1 = u + vx.$$

Όμως $v = 0$ το οποίο δεν μας κάνει.

Επιλέγουμε ξανά $z = 51 \bmod 389$ και υπολογίζουμε

$$(1 + 51x)^{194} = 239x = u + vx.$$

Άρα $u = 0$, $v = 239$ και $\frac{1}{v} = 153 \bmod 389$. Επομένως $-\frac{u}{v} = 0$, $\frac{1-u}{v} = 153$, $-\frac{1-u}{u} = -153$. Συνεπώς, οι λύσεις της ισοδυναμίας είναι οι

$$153, -153 \bmod 289.$$

Στη συνέχεια θα αποδείξουμε μια χρήσιμη ισοδύναμη μορφή του τετραγωνικού νόμου αντιστροφής. Εδώ θεωρούμε το σύμβολο του Legendre ως συνάρτηση του (περιττού) πρώτου αριθμού p, $\psi_a(p)$ και θα αποδείξουμε την

Πρόταση 5.2.19. *Υποθέτουμε ότι p, q είναι περιττοί πρώτοι και $a \geq 1$. Ο τετραγωνικός νόμος αντιστροφής είναι ισοδύναμος προς την πρόταση*

$$\text{Αν } p \equiv \pm q \bmod 4a, \text{ τότε } \psi_a(p) = \psi_a(q). \tag{5.2.8}$$

Απόδειξη. Δεχόμαστε τον τετραγωνικό νόμο αντιστροφής. Αρκεί να αποδείξουμε την (5.2.8) για a οποιοδήποτε περιττό πρώτο, $a \neq p, q$.

Πράγματι, αν a τυχαίος ακέραιος $a \geq 1$ και

$$a = 2^t \prod_{i=1}^{s} p_i^{a_i}$$

η ανάλυση αυτού σε γινόμενο πρώτων παραγόντων. Τότε

$$\psi_a(p) = \left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^t \prod_{i=1}^{s} \left(\frac{p_i}{p}\right)^{a_i} = \left(\frac{2}{q}\right)^t \prod_{i=1}^{s} \left(\frac{p_i}{q}\right) = \left(\frac{a}{q}\right) = \psi_a(q).$$

Αν $p \equiv q \bmod 4a$ τότε $\left(\frac{p}{a}\right) = \left(\frac{q+4a\ell}{a}\right) = \left(\frac{q}{a}\right)$. Επομένως

$$\left(\frac{a}{p}\right) = (-1)^{\frac{(p-1)(a-1)}{4}} \left(\frac{p}{a}\right) = (-1)^{\frac{(p-1)(a-1)}{4}} \left(\frac{q}{a}\right)$$

$$= (-1)^{\frac{(p-1)(a-1)}{4}} (-1)^{\frac{q-1}{2}\frac{a-1}{2}} \left(\frac{a}{q}\right) = (-1)^{\frac{(a-1)(b+q-2)}{4}} \left(\frac{a}{q}\right) =$$

$$= (-1)^{\frac{(a-1)(q-1+2a\ell)}{2}} \left(\frac{a}{q}\right) = \left(\frac{a}{q}\right),$$

αφού q-περιττός.

Αν $p \equiv -q \bmod 4a$ αποδεικνύεται ανάλογα.

Στη συνέχεια υποθέτουμε ότι η (5.2.8) ισχύει για κάθε ακέραιο $a \geq 1$ και θα αποδείξουμε τον τετραγωνικό νόμο αντιστροφής. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $p > q$.

Αν $p \equiv q \bmod 4$, γράφουμε το $p = q + 4a$, $a \geq 1$. Επομένως,

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p \cdot q}{}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right).$$

Αν τώρα $p \equiv 1 \bmod 4$, τότε και $q \equiv 1 \bmod 4$ και έχουμε $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Αν $p \equiv 3 \bmod 4$ τότε $q \equiv 3 \bmod 4$ και $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, δηλαδή ισχύει ο τετραγωνικός νόμος αντιστροφής (στη μορφή IIa).

Αν ισχύει η ισοτιμία $p \equiv -q \bmod 4$, τότε έχουμε $p + q = 4a$, για κάποιο a, $a \geq 1$. Συνεπώς

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{q}{p}\right).$$

□

Η τελευταία πρόταση μαζί με τον τετραγωνικό νόμο αντιστροφής μας επιτρέπουν να χαρακτηρίσουμε τους πρώτους p για τους οποίους δοσμένος ακέραιος είναι (ή δεν είναι) τετραγωνικό υπόλοιπο mod$p$.

Παράδειγμα. Για ποιους πρώτους είναι ο $a = 3$ τετραγωνικό υπόλοιπο mod$p$;

Έχουμε $4a = 4 \cdot 3 = 12$. Επομένως η ισοτιμία $p \equiv \pm q \bmod 12$ συνεπάγεται $\left(\frac{3}{p}\right) = \left(\frac{3}{q}\right)$. Για $q = 5, 7, 11$ και 13 έχουμε

$$\left(\frac{3}{p}\right) = \left(\frac{3}{5}\right) = -1, \left(\frac{3}{p}\right) = \left(\frac{3}{7}\right) = -1, \left(\frac{3}{p}\right) = \left(\frac{3}{11}\right) = 1 \text{ και } \left(\frac{3}{p}\right) = \left(\frac{3}{13}\right) = 1$$

Άρα

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \bmod 12$$

Παράδειγμα. Για ποιους πρώτους είναι ο $a = 5$ τετραγωνικό υπόλοιπο mod$p$;

Υπολογίζουμε $4a = 4 \cdot 20$. Επομένως η ισοτιμία $p \equiv \pm q \bmod 20$ συνεπάγεται ότι $\left(\frac{5}{p}\right) = \left(\frac{5}{q}\right)$.

Βρίσκουμε πρώτους αντιπροσώπους των κλάσεων

$$1, 3, 7, 9, 11, 13, 17, 19 \bmod 20$$

τους

$$41, 3, 7, 29, 11, 13, 17, 19$$

Υπολογίζουμε το σύμβολο του Legendre

$$\left(\frac{5}{41}\right) = \left(\frac{1}{5}\right) = +1, \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1, \left(\frac{5}{7}\right) = \left(\frac{2}{5}\right) = -1$$

$$\left(\frac{5}{29}\right) = \left(\frac{4}{5}\right) = +1, \left(\frac{5}{11}\right) = \left(\frac{1}{5}\right) = 1, \left(\frac{5}{13}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{5}{17}\right)\left(\frac{2}{5}\right) = -1, \left(\frac{5}{19}\right) = \left(\frac{4}{5}\right) = +1$$

Επομένως $\left(\frac{5}{p}\right) = 1$, αν και μόνο αν, $p \equiv 1, 9, 11, 19 \bmod 20$. Παρατηρούμε όμως ότι το 20 δεν είναι ένα καλό μέτρο, αφού μπορούμε να γράψουμε

$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \bmod 5$$

Ο λόγος είναι ότι η πρόταση που αποδείξαμε δεν είναι βέλτιστη. Μάλιστα απαιτεί $a \geq 1$. Τι γίνεται αν θέλουμε να χαρακτηρίσουμε τους πρώτους p για τους οποίους το -3 ή το -5 είναι τετραγωνικό υπόλοιπο mod$p$;

Ισχύει το εξής: Αν η ανάλυση του ακέραιου a είναι

$$a = (-1)^{\alpha} \prod_{i=1}^{s} q_i^{a_i}$$

και ορίσουμε το $k(a) = (-1)^{\alpha} \prod_{a_i \equiv 1 \bmod 2}^{s} q_i$, τότε το ελάχιστο μέτρο είναι το

$$m(a) := \begin{cases} |k(a)| & \text{αν } k(a) \equiv 1 \bmod 4 \\ 4|k(a)| & \text{αν } k(a) \not\equiv 1 \bmod 4 \end{cases}$$

[17, σελ. 109], [23, σελ. 139] Εδώ φαίνεται γιατί στο πρώτο παράδειγμα $a = 3$ το ελάχιστο μέτρο είναι το 12, ενώ για $a = 5$ είναι το 5.

Είναι φανερό ότι αν ο ακέραιος a είναι τέλειο τετράγωνο ακέραιου τότε η ισοτιμία $x_0^2 \equiv a \bmod p$ έχει λύση για κάθε πρώτο p. (Αν $a = b^2$, μία λύση είναι η $x_0 \equiv b \bmod p$.)

Θα αποδείξουμε και το αντίστροφο.

Πρόταση 5.2.20. *Αν για τον ακέραιο a η ισοτιμία*

$$x^2 \equiv a \bmod p$$

έχει λύση για κάθε πρώτο αριθμό p, τότε ο a είναι τέλειο τετράγωνο ακέραιου.

Απόδειξη. Αν ο a δεν είναι τέλειο τετράγωνο ακέραιου θα βρούμε ότι υπάρχει τουλάχιστον ένας πρώτος p για τον οποίο ισχύει $\left(\frac{a}{p}\right) = -1$. Επομένως για αυτόν τον πρώτο, η ισοτιμία

$$x^2 \equiv a \bmod p$$

δεν έχει λύση, άτοπο.

Λόγω της πολλαπλασιαστικότητας του συμβόλου του Jacobi, αρκεί να αποδείξουμε ότι υπάρχει ένας περιττός θετικός ακέραιος ℓ τέτοιος ώστε $\left(\frac{a}{\ell}\right) = -1$. Επειδή υποθέσαμε ότι ο a δεν είναι τέλειο τετράγωνο έπεται ότι θα έχουμε μία από τις ακόλουθες τρεις δυνατότητες:

1. $a = -b^2$ για κάποιο $b \in \mathbb{Z}$. Στην περίπτωση αυτή αν $c \in \mathbb{Z}$, $c > 0$ με $c \equiv 3 \bmod 4$ και $(b, c) = 1$, τότε
$$\left(\frac{a}{c}\right) = \left(\frac{-b^2}{c}\right) = \left(\frac{-1}{c}\right) = (-1)^{\frac{c-1}{2}} = -1.$$

2. $a = \pm 2^t b$, όπου $t, b \in \mathbb{Z}$ περιττοί θετικοί ακέραιοι. Στην περίπτωση αυτή το σύστημα
$$\begin{aligned} x &\equiv 5 \bmod 8 \\ x &\equiv 1 \bmod b \end{aligned}$$
έχει λύση αφού $(8, b) = 1$. Αν λοιπόν $c \in \mathbb{Z}$, $c > 0$ λύση του παραπάνω συστήματος (αν $b = 1$ τότε παίρνουμε $c = 5$) έχουμε
$$\left(\frac{2^t}{c}\right) = \left(\frac{-2^t}{c}\right) = \left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}} = -1$$
και
$$\left(\frac{b}{c}\right) = \left(\frac{c}{b}\right) = \left(\frac{1}{b}\right) = 1,$$
συνεπώς $\left(\frac{a}{c}\right) = -1$.

3. $a = \pm 2^{2s} q^t b$, όπου b, t περιττοί θετικοί ακέραιοι και $(q, b) = 1$, $2 \neq q \in \mathbb{P}$. Στην περίπτωση αυτή θεωρούμε το σύστημα

$$\begin{aligned} x &\equiv 1 \bmod 4b \\ x &\equiv d \bmod q \end{aligned}$$

για οποιονδήποτε ακέραιο d, έχει λύση αφού $(4b, q) = 1$.

Έστω $d > 0$ κάποιο μη-τετραγωνικό υπόλοιπο $\bmod q$ και $\ell > 0$, $\ell \equiv 1 \bmod 4b$, $\ell \equiv d \bmod q$.

Είναι φανερό ότι

$$\left(\frac{2^{2s}}{\ell}\right) = \left(\frac{-2^{2s}}{\ell}\right) = 1$$

και

$$\left(\frac{b}{\ell}\right) = (-1)^{\frac{b-1}{2}\frac{\ell-1}{2}} \left(\frac{\ell}{b}\right) = \left(\frac{\ell}{b}\right) = \left(\frac{1}{b}\right) = 1.$$

Επίσης,

$$\left(\frac{q^t}{\ell}\right) = \left(\frac{q}{\ell}\right) = \left(\frac{\ell}{q}\right) = \left(\frac{d}{q}\right) = -1.$$

Επομένως και σε αυτή την περίπτωση $\left(\frac{a}{\ell}\right) = -1$.

□

Παράδειγμα. Όταν μια ισοτιμία $x^2 \equiv a \bmod p$ έχει λύση για κάποιον πρώτο p θα λέμε ότι έχουμε τοπική επιλυσιμότητα της ισοτιμίας ως προς τον πρώτο αυτό p. Όταν η εξίσωση $x^2 \equiv a$ έχει λύση στο $\mathbb{Z}$ θα λέμε ότι έχουμε γενική επιλυσιμότητα. Βλέπουμε λοιπόν ότι από τη τελευταία πρόταση προκύπτει ότι η τοπική επιλυσιμότητα για κάθε πρώτο p συνεπάγεται τη γενική επιλυσιμότητα.

Το φαινόμενο αυτό λέγεται τοπικό-γενικό αξίωμα (local-global principle) και θα το συναντήσουμε και σε άλλες περιπτώσεις αργότερα.

Πάντως δεν ισχύει εν γένει για ισοτιμίες μεγαλύτερου βαθμού (δέστε πρόταση 5.3.7 του παρόντος κεφαλαίου).

Μια άλλη ενδιαφέρουσα εφαρμογή του συμβόλου του Jacobi είναι το ακόλουθο αποτέλεσμα:

Πρόταση 5.2.21. *Αν $a \in \mathbb{Z}$, όχι τέλειο τετράγωνο ακέραιου, υπάρχουν άπειροι πρώτοι p για τους οποίους $\left(\frac{a}{p}\right) = -1$.*

Απόδειξη. Αν $a = -1$, τότε $\left(\frac{-1}{p}\right) = -1$ αν και μόνο αν $p \equiv 3 \bmod 4$. Έχουμε όμως αποδείξει ότι υπάρχουν άπειροι πρώτοι της μορφής $4m + 3$.

Αν $a = \pm 2$, τότε

$$\left(\frac{a}{5}\right) = \left(\frac{\pm 2}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Υποθέτουμε ότι υπάρχουν πεπερασμένου πλήθους πρώτοι, έστω $p_1, p_2, \ldots, p_\ell$ μεγαλύτεροι του 3 για τους οποίους ισχύουν $\left(\frac{a}{p_i}\right) = -1$ για κάθε $i = 1, 2, \ldots, \ell$.

Θέτουμε $A := 8 p_1 p_2 \cdots p_3 \pm 3$, όπου τα πρόσημα αντιστοιχούν στο $a = \pm 2$. Είναι φανερό ότι $3 \nmid A$ καθώς επίσης ότι και $p_i \nmid A$. Επειδή $A \equiv \pm 3 \bmod 8$, έπεται ότι $\left(\frac{2}{A}\right) = -1$ και $\left(\frac{a}{A}\right) = \left(\frac{\pm 2}{A}\right) = -1$.

Αν $A = q_1 q_2 \cdots q_n$ η ανάλυση του A σε γινόμενο πρώτων παραγόντων (όχι κατ' ανάγκην διακεκριμένων μεταξύ τους) τότε

$$\left(\frac{a}{A}\right) = \left(\frac{a}{q_1}\right) \cdots \left(\frac{a}{q_n}\right) = -1.$$

Άρα ένα τουλάχιστον από τα $\left(\frac{a}{q_j}\right) = -1$ για κάποιο j. Το $q_j \mid A$, $q_j > 3$. Επομένως, $q_j \notin \{p_1, \ldots, p_\ell\}$, άτοπο.

Ας περάσουμε τώρα στη γενική περίπτωση. Δεν χάνουμε τίποτα, αν υποθέσουμε ότι ο a είναι ελεύθερος τετραγώνου (square-free). Επομένως ο a αναλύεται στη μορφή:

$$a = \varepsilon_a 2^t q_1 q_2 \cdots q_s, \quad \varepsilon_a \in \{\pm 1\}, t \in \{0, 1\},$$

q περιττοί πρώτοι και $q_i \neq q_j$ για $i \neq j$. Το $s \geq 1$ γιατί αλλιώς έχουμε τις δυνατότητες που ήδη μελετήσαμε.

Έστω $\{p_1, p_2, \ldots, p_m\}$ ένα πεπερασμένο σύνολο περιττών πρώτων, διαφορετικών των πρώτων q_i, $i = 1, 2, \ldots, s$. Ως γνωστό υπάρχουν $\frac{q_1-1}{2}$ μη τετραγωνικά υπόλοιπα $\bmod q_1$. Έστω c ένα από αυτά, δηλαδή $\left(\frac{c}{q_1}\right) = -1$.

Το γραμμικό σύστημα ισοτιμιών

$$\begin{aligned} x &\equiv 1 \bmod 8 \\ x &\equiv 1 \bmod p_i \quad i = 1, 2, \ldots, m \\ x &\equiv c \bmod q_1 \\ x &\equiv 1 \bmod q_j \quad j = 2, 3, \ldots, s \end{aligned}$$

έχει λύση, αφού τα μέτρα είναι πρώτα μεταξύ τους ανά δύο. Έστω $x = b$ μία λύση αυτού. Επομένως ο b δεν διαιρείται από κανέναν από τους πρώτους $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_s$. Επειδή $b \equiv 1 \bmod 8$ έπεται ότι $\left(\frac{-1}{b}\right) = \left(\frac{2}{b}\right) = 1$. Επίσης

$$\left(\frac{q_j}{b}\right) = (-1)^{\frac{q_j-1}{2}\frac{b-1}{2}} \left(\frac{b}{q_j}\right) = \left(\frac{b}{q_j}\right)$$

για κάθε $j = 1, 2, \ldots, s$. Επομένως,

$$\left(\frac{a}{b}\right) = \left(\frac{\varepsilon_a}{b}\right)\left(\frac{2}{b}\right)^t \left(\frac{q_1}{b}\right)\left(\frac{q_2}{b}\right)\cdots\left(\frac{q_s}{b}\right) = \left(\frac{b}{q_1}\right)\cdots\left(\frac{b}{q_s}\right) =$$

$$\left(\frac{c}{q_1}\right)\left(\frac{1}{q_2}\right)\cdots\left(\frac{1}{q_s}\right) = \left(\frac{c}{q_1}\right) = -1.$$

Τελικά υπάρχει κάποιος πρώτος παράγοντας του b, έστω q τέτοιος ώστε $\left(\frac{a}{q}\right) = -1$.

Αν λοιπόν υποθέσουμε ότι το σύνολο $\{p_1, p_2, \ldots, p_m\}$ είναι όλοι οι πρώτοι για τους οποίους $\left(\frac{a}{p_i}\right) = -1$, εμείς βρήκαμε ακόμα έναν, τον q, και συνεπώς καταλήξαμε σε άτοπο. Άρα υπάρχει και σε αυτή την περίπτωση άπειρο πλήθος πρώτων q ώστε $\left(\frac{a}{q}\right) = -1$. □

Επίσης υπάρχουν άπειροι πρώτοι ώστε $\left(\frac{a}{p}\right) = +1$ [17, σελ. 176-177]

Αν θεωρήσουμε κάποιον περιττό πρώτο p, τότε τίθεται το ερώτημα πώς κατανέμονται τα τετραγωνικά υπόλοιπα και πώς τα τετραγωνικά μη-υπόλοιπα στο διάστημα $[0, p]$;

Το πρόβλημα αυτό είναι αρκετά δύσκολο. Σε καμμία περίπτωση δεν μπορεί να θεωρηθεί ότι βρισκόμαστε σε ικανοποιητικό επίπεδο γνώσης. Δεν θα αναφερθούμε σε επιμέρους αποτελέσματα. Θα περιοριστούμε μόνο στο ερώτημα: Πόσο μακριά πρέπει να πάμε για να «συναντήσουμε» σίγουρα ένα τουλάχιστον μη-τετραγωνικό υπόλοιπο $\bmod p$;

Η απάντηση δίνεται από την ακόλουθη:

Πρόταση 5.2.22. *Έστω p περιττός πρώτος. Αν a είναι το ελάχιστο θετικό τετραγωνικό μη-υπόλοιπο* mod$p$*, τότε* $a < 1 + \sqrt{p}$.

Απόδειξη. Έστω b ο ελάχιστος φυσικός τέτοιος ώστε $ab > p$. Επομένως $a(b-1) \leq p$. Επειδή το 1 είναι πάντοτε τετραγωνικό υπόλοιπο mod$p$ έπεται ότι $a \geq 2$. Επίσης $b > 1$, διότι αν $b = 1$ θα είχαμε $a > p$, άτοπο, αφού υπάρχουν $\frac{p-1}{2}$ μη-τετραγωνικά υπόλοιπα mod$p$. Επομένως, αφού p περιττός πρώτος, ισχύει

$$a(b-1) < p \Rightarrow 0 < ab - p < a.$$

Συνεπώς, εξ ορισμού του a, έπεται ότι

$$\left(\frac{ab-p}{p}\right) = 1 \Rightarrow \left(\frac{ab}{p}\right) = 1 \Rightarrow \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1 \Rightarrow \left(\frac{b}{p}\right) = -1.$$

Το b είναι και αυτό τετραγωνικό ανισοϋπόλοιπο mod$p$, το a όμως είναι το ελάχιστο μ' αυτή την ιδιότητα. Άρα $b \geq a$, οπότε

$$(a-1)^2 < (a-1)a \leq (b-1)a < p.$$

Επομένως $a - 1 < \sqrt{p}$, δηλαδή $a < 1 + \sqrt{p}$. □

Σημείωση: Για αρκετά μεγάλο p αποδεικνύεται ότι

$$a < \sqrt{p}.$$

Απόδειξη της πρότασης αυτής και σχετικές εικασίες μπορούμε να δούμε στο [13, σελ. 69].

5.2.3 Πρώτοι σε αριθμητικές προόδους

Με τη βοήθεια του τετραγωνικού νόμου αντιστροφής μπορούμε να αποδείξουμε την ύπαρξη άπειρου πλήθους πρώτων σε αριθμητικές ακολουθίες τις οποίες δεν μπορούσαμε να διαπραγματευτούμε πριν.

Πρόταση 5.2.23. *Υπάρχουν άπειροι πρώτοι της μορφής* $4m + 1$, $m \in \mathbb{N}$.

Απόδειξη. Αν $n \in \mathbb{N}$, $n \geq 1$ ορίζουμε τον

$$\mathcal{N} := (n!)^2 + 1.$$

Ο $\mathcal{N}$ είναι φυσικός μεγαλύτερος του 1. Θα έχει κάποιο πρώτο διαιρέτη p, $p \mid \mathcal{N}$. Ο $p > n$, διότι αν $p \leq n$ θα είχαμε $p \mid \mathcal{N}$ και $p \mid n!$, δηλαδή $p \mid 1$, άτοπο.

Αφού $p \mid \mathcal{N}$, έπεται ότι

$$(n!)^2 \equiv -1 \bmod p.$$

Αυτό σημαίνει ότι η ισοτιμία

$$x^2 \equiv -1 \bmod p$$

έχει λύση, δηλαδή ισχύει $\left(\frac{-1}{p}\right) = 1$ που σημαίνει ότι $p \equiv 1 \bmod 4$.

Έχουμε αποδείξει ότι για κάθε φυσικό n υπάρχει πρώτος p, $p > n$ με $p \equiv 1 \bmod 4$.

Συνεπώς υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $4m + 1$. □

Σημείωση: Προσπαθήστε να δώσετε μία απόδειξη ανάλογη αυτής του Ευκλείδη για την ύπαρξη άπειρων πρώτων.

Πρόταση 5.2.24. *Υπάρχουν άπειροι πρώτοι της μορφής* $5m-1$, $m \in \mathbb{N}$.

Απόδειξη. Έστω $n \in \mathbb{N}$, $n > 1$. Ορίζουμε τον φυσικό αριθμό

$$\mathcal{N} := 5(n!)^2 - 1.$$

Ο $\mathcal{N}$, είναι περιττός και έχει έναν τουλάχιστον πρώτο διαιρέτη p ($p \neq 2, p \neq 5$), ο οποίος δεν είναι της μορφής $5\ell + 1$.

Ο p είναι μεγαλύτερος του n. Επειδή $p \mid \mathcal{N}$, έπεται ότι

$$5(n!)^2 = +1 \bmod p.$$

Επομένως,

$$\left(\frac{5}{p}\right) = \left(\frac{5(n!)^2}{p}\right) = \left(\frac{1}{p}\right) = 1.$$

Ο τετραγωνικός νόμος αντιστροφής δίνει

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) = 1.$$

Ο p θα έχει τη μορφή $5\ell \pm 1$ ή $5\ell \pm 2$. Αν ήταν όμως $p = 5\ell \pm 2$ θα είχαμε

$$\left(\frac{p}{5}\right) = \left(\frac{\pm 2}{5}\right) = -1,$$

άτοπο. Επειδή έχουμε αποκλείσει και την περίπτωση $5\ell + 1$, έπεται ότι κατ' ανάγκην ο $p = 5\ell - 1$, $\ell \in \mathbb{N}$. Συνεπώς υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $5m - 1$. □

Σημείωση:

1. Προσπαθήστε και πάλι με τη μέθοδο του Ευκλείδη.
2. Αν p πρώτος της μορφής $5m-1$, ο m θα είναι κατ' ανάγκη άρτιος, αλλιώς ο p θα ήταν άρτιος πρώτος > 2. Επομένως ο p θα είναι της μορφής $10m - 1$. Άμεση συνέπεια της πρότασης 5.2.24 είναι ότι υπάρχουν άπειροι πρώτοι που έχουν ως τελευταίο ψηφίο 9.

Πρόταση 5.2.25. *Υπάρχουν άπειροι πρώτοι της μορφής* $8m-1$, $m \in \mathbb{N} - \{0\}$.

Απόδειξη. Υποθέτουμε ότι υπάρχουν πεπερασμένου πλήθους πρώτοι αριθμοί της μορφής $8m - 1$ και αυτοί είναι οι

$$S := \{p_1, p_2, \ldots, p_n\}.$$

Ο ακέραιος $\mathcal{N} = (4p_1p_2 \cdots p_n)^2 - 2$ έχει τουλάχιστον έναν περιττό πρώτο διαιρέτη, $p \mid \mathcal{N}$.

Επομένως, $(4p_1p_2 \cdots p_n)^2 \equiv 2 \bmod p$, δηλαδή το 2 είναι τετραγωνικό υπόλοιπο $\bmod p$. Αυτό σημαίνει ότι $\left(\frac{2}{p}\right) = 1$, δηλαδή ότι

$$p \equiv \pm 1 \bmod 8.$$

Αν όλοι οι πρώτοι διαιρέτες του $\mathcal{N}$ ήταν της μορφής $8k + 1$, τότε ο $\mathcal{N}$ θα ήταν της μορφής $\mathcal{N} = 2(8k + 1) = 16k + 2$, άτοπο αφού έχει τη μορφή $16k - 2$.

Άρα ο $\mathcal{N}$ έχει έναν πρώτο διαιρέτη p της μορφής $p = 8k - 1$ και συνεπώς $p = p_i$ για κάποιο $i \in \{1, 2, \ldots, n\}$. Έχουμε $p \mid \mathcal{N}$ και $p \mid (4p_1 \cdots p_n)^2$ άρα $p \mid 2$, άτοπο. Αποδείξαμε δηλαδή ότι υπάρχει ένας ακόμα, άρα υπάρχουν άπειροι. □

Σημείωση: Θεωρήστε τον $\mathcal{N} := 2(n!)^2 - 1$ και εφαρμόστε τη μέθοδο των δύο προηγούμενων προτάσεων.

Πρόταση 5.2.26. *Υπάρχουν άπειροι πρώτοι της μορφής* $8m+3$, $m \in \mathbb{N}$.

Απόδειξη. Έστω $n \in \mathbb{N}$, $n > 1$. Αν με p_m συμβολίζουμε τον m-στο πρώτο αριθμό και $a := p_2 p_3 \cdot p_n$ ορίζουμε τον

$$\mathcal{N} := a^2 + 2 > 1.$$

Ο a είναι περιττός, επομένως ο a^2 είναι της μορφής $8m+1$ και συνεπώς ο $\mathcal{N}$ είναι φυσικός αριθμός της μορφής $8m+3$. Αν όλοι οι πρώτοι διαιρέτες του $\mathcal{N}$ ήταν της μορφής $8m \pm 1$, τότε και ο $\mathcal{N}$ θα ήταν της ίδιας μορφής. Επομένως υπάρχει πρώτος αριθμός p, $p \mid N$ ο οποίος θα είναι της μορφής $8m \pm 3$.

Η ισοτιμία $x^2 \equiv -2 \bmod p$ έχει λύση $x_0 = a$ συνεπώς

$$\left(\frac{-2}{p}\right) = +1.$$

Συνεπώς ο p θα είναι της μορφής $8m+3$. Τέλος, $p > p_n$, διότι αλλιώς $p \mid 2$, άτοπο.

Άρα για κάθε φυσικό αριθμό $n > 1$ υπάρχει πρώτος p της μορφής $8m+3$, $p > p_n$ και υπάρχουν άπειροι πρώτοι αυτής της μορφής. □

Πρόταση 5.2.27. *Υπάρχουν άπειροι πρώτοι της μορφής* $8m+5$, $m \in \mathbb{N}$.

Απόδειξη. Έστω $n \in \mathbb{N}$, $n > 1$ και

$$a := p_2 p_3 \cdots p_n$$

Ο a είναι περιττός, συνεπώς ο

$$\mathcal{N} := a^2 + 4$$

είναι της μορφής $8m+5$. Ο $\mathcal{N}$ περιέχει τουλάχιστον έναν πρώτο παράγοντα της μορφής $8m \pm 3$. Όμως $\left(\frac{-4}{p}\right) = 1$, άρα p της μορφής $8m+5$, $p > p_n$, συνεπώς υπάρχουν άπειροι πρώτοι της μορφής $8m+5$. □

Πρόταση 5.2.28. *Αν* $p \in \mathbb{P} - \{2\}$ *και* $k \in \mathbb{N} - \{0\}$, *τότε υπάρχουν άπειροι πρώτοι αριθμοί της μορφής* $1 + 2p^k m$, $m \in \mathbb{N}$.

Απόδειξη. Ονομάζουμε $x := 2^{p^{k-1}}$. Αν q πρώτος διαιρέτης του

$$x^{p-1} + x^{p-2} + \cdots + x + 1,$$

τότε

$$q \mid x^p - 1 = (x-1)(x^p + \cdots + x + 1)$$

συνεπώς $x^p \equiv 1 \bmod q$. Το $x^p = (2^{p^{k-1}}) = 2^{p^k}$. Θα αποδείξουμε ότι δεν υπάρχει δύναμη του 2, έστω ℓ μικρότερη του p^k για την οποία να ισχύει η ισοτιμία $2^\ell \equiv 1 \bmod q$.

Φυσικά αρκεί να το ελέγξουμε μόνο για δυνάμεις του p, $\ell = p^t$, $t < k$.

Αρκεί επομένως να αποδείξουμε ότι

$$2^{p^{k-1}} \not\equiv 1 \bmod q.$$

Αν υποθέσουμε ότι $2^{p^{k-1}} \equiv 1 \bmod q$, δηλαδή $x \equiv 1 \bmod q$, τότε $x^{p-1} + \cdots + x + 1 \equiv p \bmod q$. Όμως $x^{p-1} + \cdots + x + 1 \equiv 0 \bmod q$ άρα $p \equiv 0 \bmod q$, δηλαδή $p = q$. Θα αποδείξουμε ότι αυτό είναι άτοπο.

Το θεώρημα του Fermat δίνει $2^p \equiv 2 \bmod p$ και επαγωγικά $2^{p^{k-1}} \equiv 2 \bmod p$. Αυτή, αν συνδυαστεί με την $2^{p^{k-1}} \equiv 1 \bmod q$ δίνει $2 \equiv 1 \bmod p$, άτοπο.

Επομένως η τάξη του $x = 2^{p^{k-1}}$ είναι p^k, συνεπώς $p^k \mid \varphi(q) = q-1$. Είναι φανερό ότι $2 \mid (q-1)$, q-περιττός. Άρα $2p^k \mid (q-1)$, συνεπώς υπάρχει $m \in \mathbb{Z}$ ώστε $q = 1 + 2p^k m$.

Αποδείξαμε την ύπαρξη ενός πρώτου της μορφής αυτής. Θα αποδείξουμε ότι είναι άπειροι.

Αν $n \in \mathbb{N}$, $n > 5$, υπάρχει πρώτος q της μορφής

$$q = 1 + 2p^n m.$$

Επειδή, $p^n > n$ και $q > n$ ο q γράφεται στη μορφή

$$q = 1 + 2p^k(p^{n-k})m = 1 + 2p^n m$$

και συνεπώς υπάρχουν άπειροι πρώτοι της μορφής $1 + 2p^k m$. □

Υπενθυμίζουμε (χωρίς απόδειξη) το θεώρημα του Dirichlet. Αν m φυσικός > 1 και a ακέραιος με $(a, m) = 1$, τότε υπάρχουν άπειροι πρώτοι της μορφής $m\ell + a$, $\ell \in \mathbb{N}$.

Η εικασία στην ειδική περίπτωση $a = 1$, διατυπώθηκε για πρώτη φορά από τον Euler στα 1775. Στη γενική της μορφή διατυπώθηκε για πρώτη φορά από τον Legendre το 1785.

Είναι φανερό ότι μια τέτοια πρόταση είναι αδύνατο να αποδειχθεί με μεθόδους και τεχνικές που αναφέραμε εδώ. Χρειάζεται μια νέα μεγαλειώδη ιδέα. Η πρόταση αποδείχθηκε από τον Dirichlet στα 1837 με αναλυτικές μεθόδους [33].

Ας θεωρήσουμε τώρα την

Πρόταση 5.2.29. *Αν $(a, m) = 1$, τότε η αριθμητική πρόοδος $m\ell + a$, $\ell \in \mathbb{Z}$, έχει τουλάχιστον έναν πρώτο.*

Είναι φανερό ότι το θεώρημα του Dirichlet συνεπάγεται την αλήθεια της πρότασης 5.2.29.

Ισχύει και το αντίστροφο. Πράγματι, υπάρχει ένας ακέραιος ℓ_1, τέτοιος ώστε ο $m\ell_1 + a$ να είναι πρώτος αριθμός. Επειδή $(a, m\ell_1 + a) = 1$ θα υπάρχει κάποιος ακέραιος ℓ_2 τέτοιως ώστε ο $m\ell_2 + (m\ell_1 + a) = m(\ell_2 + \ell_1) + a$ να είναι πρώτος. Συνεχίζοντας τη διαδικασία αποδεικνύουμε ότι ο $m\ell + a$ είναι πρώτος για άπειρο πλήθος τιμών του ℓ.

5.2.4 Παρατηρήσεις - Ιστορικά στοιχεία

1. Το γεγονός ότι δεν υπάρχει ακέραιος ο οποίος να είναι ισότιμος προς $\equiv 3 \bmod 4$ ο οποίος να γράφεται ως άθροισμα τετραγώνων ήταν φαίνεταο γνωστό στον Διόφαντο (Βιβλίο V πρόβλημα 9).

Ο πρώτος που ξεκίνησε τη μελέτη των νόμων αντιστροφής ήταν ο Fermat. Σε κάποιο γράμμα του στον Mersenne διατύπωσε την πρόταση:

« Tout nombre premiere, qui surpasse de l'unite un multiple du quaternaire, est une seul fois la somme des deux carres »

«κάθε πρώτος ο οποίος είναι κατά ένα μεγαλύτερος του 4 είναι κατά μοναδικό τρόπο άθροισμα δύο τετραγώνων»

Σε επόμενο κεφάλαιο θα μελετήσουμε την παράσταση ακέραιων μέσω τετραγωνικών μορφών. Εκεί θα δούμε εύκολα ότι αν $p \in \mathbb{P} - \{2\}$ ισχύει η ισοδυναμία

(ο p είναι άθροισμα δύο τετραγώνων ακέραιων) αν και μόνο αν ($p \equiv 1 \bmod 4$) αν και μόνο αν (η ισοτιμία $x^2 \equiv -1 \bmod p$ έχει λύση)

Το πρώτο θεώρημα του Euler που σχετίζεται με τον τετραγωνικό νόμο αντιστροφής ήταν το ομώνυμο κριτήριο. Η απόδειξη που δώσαμε εμείς εδώ οφείλεται στον Dirichlet (Crelle 3 (1828) 390-393).

Ο Euler διατύπωσε ένα θεώρημα το οποίο είναι ισοδύναμο με τον τετραγωνικό νόμο αντιστροφής, στα 1744. Αυτό βέβαια έγινε γνωστό πολύ αργότερα από το άρθρο του Kronecker "Bemerkungen zur Geschichte des quadratischen Reciprocitätgesetzes" Berl. Monatber. (1872) 846-848.

Μια ειδική περίπτωση του νόμου τετραγωνικής αντιστροφής είχε ήδη ανακοινωθεί από τον Euler με γράμμα του προς τον Goldbach ήδη στα 1742.

Η δουλειά του Lagrange στη Θεωρία Αριθμών κατά τη διετία 1773/75, ο οποίος βρισκόταν στο Βερολίνο, ενώ ο Euler είχε επιστρέψει στην Αγία Πετρούπολη, παρακίνησε τον Euler να ασχοληθεί και πάλι με τη Θεωρία Αριθμών. Την περίοδο αυτή ανακάλυψε πλήρως τον τετραγωνικό νόμο αντιστροφής, δεν κατάφερε όμως να τον αποδείξει. Η εργασία του αυτή δημοσιεύθηκε μετά τον θάνατό του, στα 1783.

Ο A. M. Legendre ήταν ο πρώτος που δημοσίευσε, στα 1788 (η εργασία παρουσιάστηκε στην Ακαδημία των Παρισίων στα 1785) τον τετραγωνικό νόμο αντιστροφής σε μορφή πολύ κοντινή στη σημερινή του έκφραση. Στα 1798 ανακοίνωσε τον τετραγωνικό νόμο αντιστροφής, αφού πρώτα εισήγαγε το ομώνυμο σύμβολο (σύμβολο Legendre). Για την απόδειξη διέκρινε διάφορες περιπτώσεις. Μερικές από αυτές κατάφερε να τις αποδείξει πλήρως. Κάπου όμως παρουσιάστηκαν ανυπέρβλητες για τον ίδιο δυσκολίες και διαπίστωσε ότι χρειάζεται μια βοηθητική πρόταση για την οποία επίσης ήταν πεπεισμένος ότι είναι σωστή την οποία όμως, ούτε αυτή, μπορούσε να αποδείξει. Η εικασία του Legendre δεν ήταν τίποτε άλλο από το θεώρημα του Dirichlet για αριθμητικές προόδους ! Τα αποτελέσματα του περιέχονται στις διάφορες εκδόσεις του βιβλίου του "Essai sur la théorie des nombres" Παρίσι 1798, 1808, 1830 και (1955!). Τελικά, κατάφερε να περιοριστεί σε μία μόνο αναπόδεικτη υπόθεση: (Αν $p \in \mathbb{P}, p \equiv 1 \bmod 4$, τότε υπάρχει ένας τουλάχιστον πρώτος $q \equiv 3 \bmod 4$ τέτοιος ώστε $\left(\frac{p}{q}\right) = -1$) αλλά, παρά τις προσπάθειές του, δεν κατάφερε ποτέ να αποδείξει πλήρως τον τετραγωνικό νόμο αντιστροφής.

Ο πρώτος που απέδειξε πλήρως τον τετραγωνικό νόμο αντιστροφής ήταν ο 18-ετής Gauss. Η απόδειξη περιέχεται στο έργο του "Disquisitiones Arithmeticae" προτάσεις 131-144. Όπως αναφέρει ο ίδιος [5], «το θεώρημα αυτό ταλαιπωρούσε για έναν ολόκληρο χρόνο τη σκέψη μου και αντιστεκόταν στις επίμονες προσπάθειές μου μέχρι που κατάφερα να δώσω την απόδειξη στο τέταρτο μέρος του έργου μου».

"Ein ganzes Jahr quälte mich dieser Satz und entzog sich den angestregtesten Bemühungen, bis ich endlich den in vierten Abschnitt jenes Werkes gegebenen Beweis erlangte".

Μάλιστα, όπως μας βεβαιώνει ο ίδιος δεν είχε ιδέα από τα επιμέρους αποτελέσματα των Euler και Legendre.

"Es möge nur zur Bestätigung des im vorigen Paragraphen Behaupteten gestattet sein, auf meine eigenen Versuche Bezug zu nehmen. Auf den Satz selbst kam ich völlig selbständig im Jahre 1795, zu einer Zeit, da ich mich in völliger Unkenntniss über Alles befand, was in der höheren Arithmetik bereits erreicht worden war, und zugleich nicht die mindesten litterarischen Hilfsmittel besass"

«Για την επιβεβαίωση τών ισχυρισμών της προηγουμένης παραγράφου, ας επιτραπεί να αναφερθώ στις δικές μου προσπάθειες. Το θεώρημα το ανακάλυψα εντελώς ανεξάρτητα το έτος 1795, σε μία εποχή κατά την οποία βρισκόμουν σε πλήρη άγνοια όλων των, ως τότε, αποτελεσμάτων της ανώτερης Αριθμητικής και δεν είχα την παραμικρή πρόσβαση στη σχετική βιβλιογραφία.»

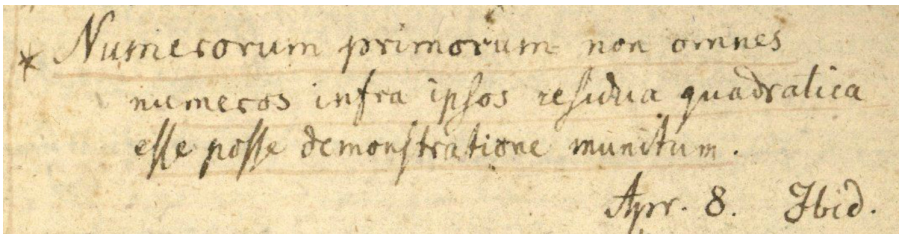
Πώς κατάφερε ο Gauss να διατυπώσει και να αποδείξει πλήρως τον τετραγωνικό νόμο αντιστροφής;

Με επιδεξιότητα και αντοχή κατασκεύασε έναν πίνακα στον οποίο υπολόγιζε ποιοι από τους πρώτους τους μικρότερους του 1000 είναι τετραγωνικά υπόλοιπα και ποιοι όχι ως προς τους πρώτους από το 3 ως το 503. Έπρεπε να εξετάσει 16000 περιπτώσεις αν είναι τετραγωνικά υπόλοιπα ή όχι.

Στην απόδειξη και ο ίδιος είχε τις δυσκολίες του. Η (πρώτη του) απόδειξη έμοιαζε με αυτή του Legendre. Χρειάστηκε και ο ίδιος έναν «βοηθητικό πρώτο» και όταν τον βρήκε το ημερολόγιο έγραφε:

8 Απριλίου του 1796

"Numerorum primorum non omnes numeros infra ipsos residua quadratica esse posse demonstratione munitum"



Σχήμα 5.2.2: Ημερολόγιο Gauss, το έργο αποτελεί κοινό κτήμα λόγω παρέλευσης 70 ετών από τον θάνατο του δημιουργού.

Ο Legendre ονόμασε το θεώρημα «Loi le reciprocite», νόμο αντιστροφής». Ο Gauss «Theorema fundamentale theorie residuorum quadraticorum, θεμελιώδες θεώρημα της θεωρίας των τετραγωνικών υπολοίπων» και το κατέτασσε στις «ύψιστες αλήθειες της ανώτερης Αριθμητικής», «Zu den höchsten Wahrheiten der höheren Arithmetik zu rechnen ist»

Η πρώτη απόδειξη του Gauss δεν θεωρήθηκε ιδιαίτερα κομψή. Χρησιμοποιεί διπλή επαγωγή. Εκτός από το «Disquisitiones Arithmeticae», η απόδειξη περιέχεται και στο [1]. Αξίζει να αναφερθεί και το άρθρο του Ezra Brown, "The First proof of quadratic reciprocity Law", [14] στο οποίο η επαγωγή μετατρέπεται σε ένα είδος «άπειρης καθόδου».

Πάρα πολύ σύντομα, στις 27 Ιουνίου του 1796, ακολούθησε η δεύτερη απόδειξη του Gauss [άρθρο 262][7], στην οποία θα αναφερθούμε αργότερα. Σ' αυτήν χρησιμοποιεί τη θεωρία των τετραγωνικών μορφών. Ακολούθησαν άλλες έξι, σύνολο οκτώ, αποδείξεις του.

Καιρός να πούμε δύο λόγια για την απόδειξη που δώσαμε. Το επόμενο σημαντικό βήμα, μετά το κριτήριο του Euler, ήταν το λήμμα του Gauss. Αυτό αποδείχθηκε στα 1807 και αποτελούσε μέρος της τρίτης απόδειξης του τετραγωνικού νόμου αντιστροφής που έδωσε ο ίδιος. Τέλος, το τελικό βήμα της απόδειξης είναι του Eisenstein (1844), μαθητή του Gauss. Εδώ για πρώτη φορά χρησιμοποιούνται γεωμετρικές μέθοδοι. Μετρούμε τα ακέραια σημεία του ορθογωνίου κατά δύο διαφορετικούς τρόπους. Η κατεύθυνση αυτή αναπτύχθηκε αργότερα από τον Minkowski και ονομάστηκε «Γεωμετρία» των Αριθμών. Πρόδρομος της θεωρίας αυτής μπορεί να θεωρηθεί ο Eisenstein.

Συνολικά έχουν δοθεί μέχρι σήμερα περισσότερες από 200 αποδείξεις. Βέβαια αρκετές από αυτές είναι μεταξύ τους σχεδόν όμοιες.

Στα 1963 ο M. Gesterhaber δημοσίευσε [22] την 152η απόδειξη του τετραγωνικού νόμου αντιστροφής. Είχε μετρήσει όλες τις προηγούμενες; Η απάντηση που έδωσε ο ίδιος είναι «Όχι»! Ακολούθησε την πρόταση του A. Weil σε ένα σεμινάριο στο Inst. for Advanced Studies του

Princeton ο οποίος είπε ότι γνωρίζει 50 αποδείξεις και για κάθε μία υπάρχουν άλλες δύο που δεν γνωρίζει. Έτσι συμπέρανε ότι θα πρέπει να είναι 150. Στη« συνέχεια επέστησε την προσοχή στην εργασία του Kubota η οποία θα πρέπει να ήταν η 151η απόδειξη. Επομένως η δικιά του θα έπρεπε να είναι η 152! Σύμφωνα με τον κατάλογο του Lemmermyer είναι η 149, δηλαδή δεν έπεσε καθόλου έξω ο A. Weil!

Ο αναγνώστης μπορεί να διαβάσει περισσότερα στη σχετική βιβλιογραφία:

1. Franz Lemmermeyer, *Reciprocity Laws from Euler to Eisenstein*, Springer Monographs in Mathematics, Springer, Berlin 2000 [16]

2. Herbert Piper *Variationen über ein zahlentheoretishen Thema von Carl Friedrich Gauss* [18] Περιέχει 14 αποδείξεις.

3. Horst Knörrerm Claus-Günther Schmidt, Joachim Schwermer, Peter Soloday *Mathematische Miniaturen Arithmetik und Geometrie* [19]

4. Winfried Scharlau, Hans Opolka, *From Fermat to Minkowski, Lectures on the theory of Numbers and its Historical Development* [31]

5. Andre Weil, *Number Theory An approach through history, from Hammurapi to Legendre* [2]

Η σημασία του τετραγωνικού νόμου αντιστροφής

Στη συνέχεια θα εξετάσουμε εν συντομία πόσο σημαντικός είναι ο τετραγωνικός νόμος αντιστροφής. Το γεγονός ότι δεν ήταν εύκολη η απόδειξή του καθώς και το ότι υπάρχουν περισσότερες από 200 αποδείξεις γνωστές είναι ασφαλώς μια ένδειξη.

Το σημαντικό είναι ότι ο τετραγωνικός νόμος αντιστροφής αποτέλεσε το κίνητρο για την εξέλιξη της Θεωρίας Αριθμών. Φυσικά και η εικασία του Fermat έπαιξε σημαντικότατο ρόλο. Υπάρχουν μάλιστα μαθηματικοί που υποστηρίζουν ότι η ιστορία των νόμων αντιστροφής έπαιξε πιο σημαντικό ρόλο ρόλο και από την εικασία του Fermat, [16].

Μετά την απόδειξη του τετραγωνικού νόμου αντιστροφής ο Gauss μελέτησε και κυβικές $x^3 \equiv a \mathrm{mod} p$ και διτετραγωνικές $x^4 \equiv a \mathrm{mod} p$ ισοτιμίες. Πείστηκε ότι δεν μπορεί κανείς να ελπίζει σε εύκολα αποτελέσματα αν παρέμεινε στους ακέραιους αριθμούς. Για το σκοπό του μελετά μιγαδικούς αριθμούς της μορφής

$$a + bi, \quad a, b \in \mathbb{Z},$$

οι οποίοι αργότερα ονομάστηκαν ακέραιοι του Gauss. Στα 1825 διατυπώνει τον νόμο της διτετραγωνικής αντιστροφής, [7, άρθρο 510-533,534-586].

Αποδείχθηκε αργότερα στα 1844 από τον μαθητή του Gauss, G. Eisenstein. Ο Jacobi διατυπώνει στα 1827 τον κυβικό νόμο αντιστροφής. Αποδειξη δίνει και πάλι την ίδια χρονια (1844) ο Eisenstein.

Στο διεθνές Μαθηματικό Συνέδριο των Παρισίων στα 1900, ο Hilbert προσκλήθηκε να δώσει μια διάλεξη με τίτλο «Mathematische Probleme». Η διάλεξη περιέχει 23 προβλήματα από όλους τους κλάδους των Μαθηματικών. Από αυτά το 9ο είναι η εύρεση του γενικού νόμου αντιστροφής σε οποιοδήποτε αλγεβρικό σώμα αριθμών. [9], [10].

Ακολουθούν σημαντικά αποτελέσματα των Takagi 1920, Hasse 1926, Artin 1928, Shafarevitch, Serre τα οποία απαντούν πλήρως στη λεγόμενη «αβελιανή περίπτωση». Η θεωρία ενός «μη-αβελιανού» νόμου αντιστροφής αρχίζει από τη δεκαετία του 1960 με τον Langlands και συνεχίζεται μέχρι σήμερα.

5.3 Τετραγωνικά υπόλοιπα ως προς μέτρο σύνθετο ακέραιο

Μέχρι τώρα, μελετήσαμε τετραγωνικες ισοτιμίες ως προς μέτρο περιττό πρώτο αριθμό. Τι γίνεται όμως όταν έχουμε ισοτιμίες της μορφής

$$x^2 \equiv a \bmod m \text{ όπου } m \in \mathbb{Z}, m \geq 1;$$

Σε πρώτο βήμα θα θεωρήσουμε την περίπτωση ισοτιμιών ως προς μέτρο δύναμη πρώτου αριθμού.

Πρόταση 5.3.1. *Αν $a \in \mathbb{Z}$ και p πρώτος, $p \neq 2$, $p \nmid a$ τότε η ισοτιμία*

$$x^2 \equiv a \bmod p^s, \quad s \geq 1$$

έχει λύση ακριβώς τότε όταν $\left(\frac{a}{p}\right) = 1$, δηλαδή ακριβώς τότε όταν η ισοτιμία

$$x^2 \equiv a \bmod p$$

έχει λύση.

Απόδειξη. Αν η ισοτιμία $x^2 \equiv a \bmod p^s$ έχει λύση, τότε αυτή είναι και λύση της $x^2 \equiv a \bmod p$. Επομένως $\left(\frac{a}{p}\right) = 1$.

Υποθέτουμε τώρα ότι $\left(\frac{a}{p}\right) = 1$, δηλαδή ότι η ισοτιμία $x^2 \equiv a \bmod p$ έχει λύση. Θα αποδείξουμε ότι και η ισοτιμία $x^2 \equiv a \bmod p^s$ για οποιοδήποτε ακέραιο $s \geq 1$ έχει επίσης λύση. Η απόδειξη θα γίνει επαγωγικά ως προς s. Για $s = 1$ ισχύει. Δεχόμαστε ότι ισχύει για $s = t \geq 1$ και θα αποδείξουμε ότι ισχύει για $s = t + 1$. Λόγω της υπόθεσης, η $x^2 \equiv a \bmod p^t$ έχει λύση. Επομένως υπάρχει ακέραιο x_0 ώστε

$$x_0^2 \equiv a \bmod p^t,$$

δηλαδή,

$$x_0^2 = a + \ell p^t$$

για κάποιο ακέραιο ℓ. Η ισοτιμία $2x_0 y \equiv -\ell \bmod p$ έχει μοναδική λύση $\bmod p$ αφού $(2x_0, p) = 1$. Αν y_0 η λύση αυτής, τότε $p \mid (2x_0 y_0 + \ell)$.

Ο ακέραιος $x_1 = x_0 + y_0 p^t$ είναι λύση της

$$x^2 \equiv a \bmod p^{t+1}.$$

Πράγματι,

$$\begin{aligned} x_1^2 &= x_0^2 + 2x_0 y_0 p^t + y_0 p^{2t} \\ &= a + \ell p^t + 2x_0 y_y p^t + y_0 p^{2t} \\ &= a + (\ell + 2x_0 y_0) p^t + y_0 p^{2t} \equiv a \bmod p^{t+1} \end{aligned}$$

Αν $\left(\frac{a}{p}\right) = 1$, η ισοτιμία $x^2 \equiv a \bmod p$ έχει δύο λύσεις $\bmod p$. Πόσες λύσεις $\bmod p$ έχει η ισοτιμία $x^2 \equiv a \bmod p^s$; Σύμφωνα με την πρόταση 5.3.1 έχει τουλάχιστον μια λύση έστω x_1. Ας υποθέσουμε ότι έχει και μια άλλη λύση, έστω x_2. Θα έχουμε

$$x_2^2 \equiv x_1^2 \bmod p^s \Rightarrow p^s \mid (x_2 - x_1)(x_2 + x_1).$$

Επομένως $p \mid (x_2 - x_1)(x_2 + x_1)$, δηλαδή $p \mid (x_2 - x_1)$ ή $p \mid (x_2 + x_1)$. Αν ισχύουν και οι δύο θα είχαμε $p \mid 2x_1$, άτοπο.

Από τα παραπάνω συμπεραίνουμε ότι ισχύει ακριβώς μια από τις ισοτιμίες

$$x_2 \equiv x_1 \bmod p^s \text{ ή } x_2 \equiv -x_1 \bmod p^s$$

δηλαδή η ισοτιμία $x^2 \equiv a \bmod p^s$ έχει ακριβώς δύο λύσεις. □

Το

$$\#\{x \bmod p^s : x^2 \equiv a \bmod p^s, p \in \mathbb{P}, p \neq 2, p \nmid a\} = 1 + \left(\frac{a}{p}\right).$$

Αν γνωρίζουμε τις λύσεις της $x^2 \equiv a \bmod p$ πώς θα βρούμε τις λύσεις της $x^2 \equiv a \bmod p^s$; Θα εφαρμόζουμε τη γενική θεωρία, πρόταση 4.7.2. Θα πρέπει βεβαίως σε κάθε βήμα να λύσουμε μια γραμική ισοτιμία. Στην ειδική περίπτωση των τετραγωνικών ισοτιμιών μπορούμε να εφαρμόσουμε τον ακόλουθο:

Αλγόριθμο Βρίσκουμε μια λύση x_0 της ισοτιμίας $x^2 \equiv a \bmod p$. Ορίζουμε δύο ακολουθίες ακέραιων $\{b_n\}_{n\geq 0}$ και $\{c_n\}_{n\geq 0}$ ως εξής: $b_0 = 1$, $c_0 = 0$,

$$\begin{aligned} b_s &:= x_0 \cdot b_{s-1} + a \cdot c_{s-1} \\ c_s &:= x_0 \cdot c_{s-1} \end{aligned}$$

για κάθε $s \geq 1$. Η λύση x_1 της γραμμικής ισοτιμίας

$$c_s \cdot x \equiv b_s \bmod p^s,$$

είναι λύση της $x^2 \equiv a \bmod p^s$. [34, σελ. 46],[11].

Παράδειγμα. Να υπολογιστούν οι λύσεις της ισοτιμίας

$$x^2 \equiv 51 \bmod 343 = 7^3.$$

Η ισοτιμία $x^2 \equiv 2 \bmod 7$ έχει δύο λύσεις, $3, 4 \bmod 7$. Για $x_0 = 3, a = 51$, έχουμε

$$\begin{aligned} b_1 &= 3 \cdot 1 + 51 \cdot 0 = 3 \\ c_1 &= 1 + 3 \cdot 0 = 1 \\ b_2 &= 3 \cdot 3 + 51 \cdot 1 = 60 \\ c_2 &= 3 + 3 \cdot 1 = 6 \\ b_3 &= 3 \cdot 60 + 51 \cdot 6 = 486 \\ c_3 &= 60 + 3 \cdot 6 = 78 \end{aligned}$$

Η ισοτιμία

$$78x \equiv 486 \bmod 342$$

ή

$$78x \equiv 143 \bmod 324$$

έχει λύση $x \equiv 59 \bmod 343$. Πράγματι $59^2 \equiv 3481 \equiv 51 \bmod 343$. Οι λύσεις της $x^2 \equiv 51 \bmod 343$ είναι οι $x \equiv 59, 284 \bmod 343$. Επεξήγηση στον αλγόριθμο: Εύκολα αποδεικνύεται ότι

$$b_s^2 - ac_s^2 = (x_0^2 - a)^s \tag{5.3.1}$$

$$b_s^2 - ac_s^2 \equiv 0 \bmod p^s \tag{5.3.2}$$

$$c_{s+1} \equiv (2x_0)^s \bmod p^s \tag{5.3.3}$$

$$\text{και} \quad p \nmid c_s \tag{5.3.4}$$

Επομένως, η $c_s x \mathrm{mod} b_s \mathrm{mod} p^s$ έχει μοναδική λύση, έστω x_1 $c_s x_1 \mathrm{mod} p^s$.

Αφού $(p^s, c_s) = 1$ αρκεί να αποδείξουμε ότι

$$c_s^2 x_1^2 \equiv a c_s^2 \mathrm{mod} p^s$$

Αλλά

$$c_s^2 x_1^2 \equiv b_s^2 \mathrm{mod} p^s$$

Αλλά

$$c_s^2 x_1^2 \equiv b_s^2 \mathrm{mod} p^s$$

και από (5.3.2)

$$b_s^2 \equiv a c_s^2 \mathrm{mod} p^s$$

Όμως τι γίνεται με τις δυνάμεις του ιδιότροπου (κατά Silverman "oddest") πρώτου αριθμού·[1]

Αν a περιττός ακέραιος τότε η ισοτιμία

$$x^2 \equiv a \mathrm{mod} 2$$

έχει πάντοτε μοναδική λύση, $x \equiv 1 \mathrm{mod} 2$.

Η $x^2 \equiv a \mathrm{mod} 4$ έχει λύση ακριβώς τότε όταν $a \equiv 1 \mathrm{mod} 4$. Ο x_0 θα πρέπει να είναι περιττός και το τετράγωνό του είναι πάντοτε της μορφής $4m + 1$. Αν $a \equiv 1 \mathrm{mod} 4$, τότε η ισοτιμία έχει ακριβώς δύο λύσεις $x \equiv 1, 3 \mathrm{mod} 4$.

Πρόταση 5.3.2. *Αν a περιττός ακέραιος η ισοτιμία*

$$x^2 \equiv a \mathrm{mod} 2^s$$

για $s \geq 3$ έχει λύση, ακριβώς αν $a \equiv 1 \mathrm{mod} 8$. Αν έχει λύση τότε το πλήθος των λύσεων είναι 4.

Απόδειξη. Αν η ισοτιμία έχει λύση, έστω x_0 τότε ο x_0 είναι περιττός και συνεπώς $x_0^2 \equiv 1 \mathrm{mod} 8$. Επομένως $a \equiv 1 \mathrm{mod} 8$.

Υποθέτουμε τώρα ότι $a \equiv 1 \mathrm{mod} 8$. Θα εφαρμόσουμε επαγωγή ως προς s. Αν $s = 3$ η ισοτιμία γράφεται $x^2 \equiv 1 \mathrm{mod} 8$ η οποία έχει 4 $x \equiv 1, 3, 5, 7 \mathrm{mod} 8$.

Υποθέτουμε ότι η ισοτιμία

$$x^2 \equiv a \mathrm{mod} 2^s$$

για κάποιον σταθερό s, $s \geq 3$ έχει λύση, έστω x_0. Θα αποδείξουμε ότι και η

$$x^2 \equiv a \mathrm{mod} 2^{s+1}$$

έχει επίσης λύση. Το $x_0^2 = a + \ell \cdot 2^s$, για κάποιο $\ell \in \mathbb{Z}$. Ο a είναι περιττός, επομένως και ο x_0 είναι περιττός. Θεωρούμε τη γραμμική ισοτιμία

$$x_0 y \equiv -\ell \mathrm{mod} 2$$

η οποία έχει μοναδική λύση, έστω y_0.

Ο αριθμός $x_1 = x_0 + y_0 2^{s-1}$ είναι λύση της ισοτιμίας $x^2 \equiv a \mathrm{mod} 2^{s+1}$. Πράγματι, ($2s - 2 \geq s + 1$ αφού $s \geq 3$)

$$x_1^2 = (x_0 + y_0 2^{s-1})^2 = x_0^2 + x_0 y_0 \cdot 2^s + y_0^2 2^{2s-2} =$$

[1] Ο Silverman κάνει λογοπαίγνιο με τη λέξη odd που σημαίνει ιδιότροπος αλλά και περιττός για τον άρτιο πρώτο 2.

$$= a + (\ell + x_0 y_0)2^s + y_0^2 2^{2s-2} \equiv a \bmod 2^{s+1}$$

Αν τώρα x_2 άλλη λύση, θα έχουμε

$$x_2^2 \equiv x_1^2 \bmod 2^s$$

και x_1, x_2 περιττοί. Επομένως $(x_2 + x_1)(x_2 - x_1) \equiv 0 \bmod 2^{s-2}$ και $x_2 + x_1$, $x_2 - x_1$ είναι άρτιοι. Γράφουμε την ισοτιμία στη μορφή

$$\frac{x_2 + x_1}{2} \cdot \frac{x_2 - x_1}{2} \equiv 0 \bmod 2^{s-2}$$

Αφού $s \geq 3$, έπεται ότι $2 \mid \frac{x_2+x_1}{2} \cdot \frac{x_2-x_1}{2}$. Το 2 δεν μπορεί να διαιρεί και τους δύο παράγοντες, διότι τότε θα διαιρούσε και τη διαφορά τους που είναι ο περιττός x_1.

Επομένως ισχύει ακριβώς μία από τις ισοτιμίες

$$\frac{x_2 + x_1}{2} \equiv 0 \bmod 2^{s-2} \text{ ή } \frac{x_2 - x_1}{2} \equiv 0 \bmod 2^{s-2}$$

από τις οποίες προκύπτει

$$x_2 \equiv \pm x_1 \bmod 2^{s-1}$$

Το x_2 γράφεται, $x_2 = \pm x_1 + \ell 2^{s-1}$ για κάποιο ακέραιο ℓ.

Αν ο ℓ είναι άρτιος, τότε $x_2 \equiv \pm x_1 \bmod 2^s$.

Αν ο ℓ είναι περιττός, τότε $x_2 \equiv \pm x_1 + 2^{s-1} \bmod 2^s$.

Βλέπουμε ότι το x_2 έχει αυτές τις τέσσερις δυνατότητες $x_1, -x_1, x_1 + 2^{s-1}, -x_1 + 2^{s-1}$. Οι τιμές αυτές είναι ανά-δύο ανισότιμες $\bmod 2^s$ και έχουμε ακριβώς τέσσερις λύσεις. □

Φυσικά τίθεται και πάλι το ερώτημα πώς θα βρούμε τις λύσεις. Θα εφαρμόσουμε τον ακόλουθο

Αλγόριθμο Αν $a \equiv 1 \bmod 8$ η ισοτιμία $x^2 \equiv a \bmod 2^s$ έχει μια λύση x_s τέτοια ώστε $x_3 = 1$ και

$$x_{t+2} \equiv x_t + \frac{1}{2}(x_t^2 - a) \bmod 2^{t+1}$$

Παράδειγμα. Να υπολογιστούν οι λύσεις της ισοτιμίας

$$x^2 \equiv 17 \bmod 32$$

$x_3 = 1$, $x_4 \equiv 1 + \frac{1}{2}(1^2 - 17) \bmod 2^4$, $x_4 \equiv -7 \bmod 2^4$.

$x_5 \equiv x_4 + \frac{1}{2}(x_4^2 - a) \bmod 2^5$ άρα $x_5 \equiv (-7) + \frac{1}{2}(49 - 17) \equiv -7 + \frac{1}{2}32 \equiv -7 + 16 \equiv 9 \bmod 2^5$.

Επομένως μια λύση είναι η $9 \bmod 2^5$ και συνεπώς οι άλλες είναι οι $\pm 9, \pm 9 + 2^4 \equiv \pm 7 \bmod 2^5$.

Επεξήγηση στον αλγόριθμό Αν $a \equiv 1 \bmod 8$ η $x^3 \equiv 1 \bmod 2^3$ έχει μία λύση $x_3 = 1$. Για $s > 3$ ισχύει: Υποθέτουμε λοιπόν ότι το x_s είναι μια λύση της $x^2 \equiv a \bmod 2^s$. Επομένως, $x_s^2 = a + \ell 2^s$ για κάποιο ακέραιο $\ell \in \mathbb{Z}$.

Αν ℓ άρτιος, $\ell = 2t$ έχουμε

$$x_{s+1} \equiv x_s + \frac{1}{2}(x_s^2 - a) \equiv x_s + t2^s \bmod 2^{s+1}$$

και

$$x_{s+1}^2 \equiv x_s^2 + t2^{s+1} + t^2 2^{2s} \equiv x_s^2 \equiv a + t2^{s+1} \equiv a \bmod 2^{s+1}$$

Αν πάλι ℓ περιττός, $\ell = 2t + 1$, τότε

$$x_{s+1} \equiv x_s + \frac{1}{2}(x_s^2 - a) \equiv x_s + \frac{1}{2}(2t + 1) \cdot 2^s \equiv x_s + 2^s t + 2^{s-1} \bmod 2^{s+1}$$

και, επειδή $s \geq 3$ και x_s περιττός

$$\begin{aligned} x_{s+1}^2 &\equiv x_s^2 + 2x_s(2^s t + 2^{s-1}) + (2^s t + 2^{s-1}) \mathrm{mod} 2^{s+1} \\ &\equiv x_s^2 + 2^s x_s \equiv a + 2^s(2t+1) + 2^s x_s \\ &\equiv a + 2^s(1 + x_s) \equiv a \mathrm{mod} 2^{s+1} \end{aligned}$$

Παρατήρηση 5.3.3. Στην επόμενη παράγραφο θα δούμε ότι κάθε περιττός $a \equiv 1 \mathrm{mod} 8$ είναι ισότιμος $\mathrm{mod} 2^s$ προς μία άρτια δύναμη του 5, έστω 5^{2t}. Αυτό σημαίνει ότι το 5^t είναι λύση της $x^2 \equiv a \mathrm{mod} 2^s$. Επομένως θα πρέπει να θεωρήσουμε τις δυνάμεις $5^2, 5^4, \ldots, 5^{2^{s-2}}$ και να δούμε ποιος είναι ισότιμος προς τον $a \mathrm{mod} 2^s$ για να βρούμε μία λύση.

Στο προηγούμενο παράδειγμα $5^4 \equiv 17 \mathrm{mod} 2^5$. Αλλά θα επανέλθουμε σύντομα.

Τέλος αν $m \in \mathbb{Z}$, $m > 1$ και

$$m = 2^{a_2} \prod_{i=1}^{t} p_i^{\ell_i}$$

η ανάλυση του m σε γινόμενο πρώτων παραγόντων, είναι γνωστό ότι η ισοτιμία $x^2 \equiv a \mathrm{mod} m$ έχει λύση ακριβώς τότε όταν το σύστημα των ισοτιμιών

$$\begin{aligned} x^2 &\equiv a \mathrm{mod} 2^{a_2} \\ x^2 &\equiv a \mathrm{mod} p_1^{\ell_1} \\ \ldots &\quad \ldots \\ x^2 &\equiv a \mathrm{mod} p_t^{\ell_t} \end{aligned}$$

έχει λύση.

Συνοψίζοντας τα παραπάνω έχουμε

Πρόταση 5.3.4. *Αν $a \in \mathbb{Z}$, $m \in \mathbb{N}$ και $(a, m) = 1$ τότε η*

$$x^2 \equiv a \mathrm{mod} m$$

έχει λύση τότε και μόνο τότε όταν ισχύουν

- $\left(\frac{a}{p_i}\right) = 1$ *για κάθε* $i = 1, 2, \ldots, t$
- $a \equiv 1 \mathrm{mod} 4$ *αν* $4 \| n$ *η* $a \equiv 1 \mathrm{mod} 8$ *αν* $8 | n$.

Αν έχει λύση το πλήθος, των λύσεων είναι

$$N(m) = 2^{f+t}, \text{ όπου } f = \begin{cases} 0 & \text{αν } 4 \nmid n \\ 1 & \text{αν } 4 \| n \\ 2 & \text{αν } 8 \mid n \end{cases}$$

Παρατήρηση 5.3.5. Η πρόταση μπορεί να διατυπωθεί κάπως πιο γενικά. Αν $a \in \mathbb{Z}$, $m \in \mathbb{N}$ $m > 1$ και $(a, m) = 1$ τότε η $x^2 \equiv a \mathrm{mod} m$ έχει

$$2^f \cdot \prod_{i=1}^{t} \left(1 + \left(\frac{a}{p_i}\right)\right)$$

το πλήθος λύσεις. Αν κάποιο $\left(\frac{a}{p_i}\right) = -1$, τότε το γινόμενο είναι 0 και η ισοτιμία δεν έχει λύσεις.

Παράδειγμα. Να βρεθούν οι λύσεις τις ισοτιμίας

$$x^2 \equiv 453 \mathrm{mod} 1236. \tag{5.3.5}$$

Επειδή $(453, 1236) = 3$ η ισοτιμία είναι ισοδύναμη προς την

$$3y^2 \equiv 151 \mathrm{mod} 412 \tag{5.3.6}$$

Η αντίστροφη της κλάσης $3 \mathrm{mod} 412$ είναι η $275 \mathrm{mod} 412$. Επομένως η ισοτιμία (5.3.6) είναι ισοδύναμη προς την

$$x^2 \equiv 151 \cdot 275 \equiv 325 \mathrm{mod} 412$$

Το $412 = 2^2 \cdot 103$ και $325 \equiv 1 \mathrm{mod} 4$. Επομένως η ισοτιμία έχει λύση ακριβώς τότε όταν $\left(\frac{325}{103}\right) = 1$. Πράγματι $\left(\frac{325}{103}\right) = \left(\frac{16}{103}\right) = +1$. Η ισοτιμία $x^2 \equiv 16 \mathrm{mod} 103$, δηλαδή έχουμε τέσσερις λύσεις $\pm 99, \pm 107 \mathrm{mod} 412$ οι οποίες μας δίνουν τις τέσσερις λύσεις της αρχικής $x \equiv \pm 297, \pm 321 \mathrm{mod} 1236$.

Πράγματι $f = 1$, $t = 1$, $a = 315$ και $p = 103$ το πλήθος των λύσεων είναι $2^1 \cdot \left(1 + \frac{315}{103}\right) = 2 \cdot 2 = 4$.

Παρατήρηση 5.3.6. Το παράδειγμα αυτο επεξεργάστηκα ο Gauss στο *Disiquisitiones Arithmeticae* άρθρο 146.

Πρόταση 5.3.7. *Αν $f(x) = (x^2 - 2)(x^2 + 7)(x^2 + 14)$, τότε η ισοτιμία*

$$f(x) \equiv 0 \mathrm{mod} n$$

έχει λύση για κάθε φυσικό αριθμό n, $n \geq 1$ παρά το ότι δεν έχει ακέραια λύση.

Απόδειξη. Σύμφωνα με το κινέζικο θεώρημα αρκεί να αποδείξουμε ότι η πρόταση ισχύει για $n = p^\ell$, όπου $p \in \mathbb{P}$ και $\ell \geq 1$.

Για να το αποδείξουμε αρκεί να αποδείξουμε ότι τουλάχιστον ένας από τους $2, -7$ και -14 είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p^\ell$.

Επειδή $-7 \equiv 1 \mathrm{mod} 8$, η ισοτιμία $x^2 \equiv 1 \mathrm{mod} 8$ έχει λύση για κάθε $\ell \geq 1$, πρόταση 5.3.2. Επίσης, αφού $\left(\frac{2}{7}\right) = +1$ η ισοτιμία $x^2 \equiv 2 \mathrm{mod} 7^\ell$ έχει λύση για κάθε $\ell \geq 1$, πρόταση 5.3.1. Αν τώρα p πρώτος $\neq 2, 7$ τότε επειδή $-14 \equiv 2 \cdot (-7)$, έχουμε $\left(\frac{-14}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-7}{p}\right)$.

Τουλάχιστον ένα από τα τρία σύμβολα του Legendre έχει τιμή 1, δηλαδή τουλάχιστον ένας από τους αριθμούς $2, -7, -14$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$ και συνεπώς η ισοτιμία $x^2 \equiv a \mathrm{mod} p^\ell$ έχει λύση για τουλάχιστον ένα $a \in \{2, -7, -14\}$,

Τέλος, είναι φανερό ότι η $f(x) = 0$ δεν έχει ακέραιες λύσεις. □

Παρατήρηση 5.3.8. Η πρόταση 5.3.7 μας δείχνει ότι για τη συγκεκριμένη ισοτιμία το τοπικό-γενικό αξίωμα δεν ισχύει.

5.4 n-στα υπόλοιπα, αρχικές ρίζες και δείκτες

Στις προηγούμενες δύο παραγράφους ασχοληθήκαμε με τετραγωνικές ισοτιμίες. Στην παράγραφο αυτή θα ασχοληθούμε γενικότερα με ισοτιμίες της μορφής

$$x^n \equiv a \mathrm{mod} m, \tag{5.4.1}$$

$n \geq 2$, $m \geq 2$ και $(a, m) = 1$.

Ορισμός 5.4.1. Θα λέμε ότι ο ακέραιος a είναι n-στο υπόλοιπο mod$m$ όταν η (5.4.1) έχει τουλάχιστον μία λύση.

Πότε όμως η ισοτιμία (5.4.1) είναι επιλύσιμη; Στην ειδική περίπτωση $a = 1$ και $n = \phi(m)$ η ισοτιμία $x^{\phi(m)} \equiv 1 \mathrm{mod} m$ είναι πάντα επιλύσιμη. Μάλιστα, κάθε ακέραιος a πρώτος προς τον m είναι μια λύση αυτής.

Επομένως για κάθε ακέραιο a πρώτο προς τον m υπάρχει κάποιος ελάχιστις φυσικός αριθμός $s := s(a, m)$ που εξαρτάται τόσο από το m όσο και από το a τέτοιος ώστε να ισχύει

$$a^s \equiv 1 \mathrm{mod} m \tag{5.4.2}$$

Ορισμός 5.4.2. Αν $a \in \mathbb{Z}, m \in \mathbb{N}$, $m \geq 2$ και $(a, m) = 1$, τότε ο ελάχιστος φυσικός αριθμός $s := s(a, m) \geq 1$ με την ιδιότητα (5.4.2) θα λέγεται τάξη του $a \mathrm{mod} m$ και θα τη συμβολίζουμε με $\mathrm{ord}_m(a)$.

Παράδειγμα.

1. Αν $m = 5$ και $a = 2$, τότε $s = 4$.
2. Αν $m = 5$ και $a = 3$, τότε $s = 4$
3. Αν $m = 12$ και $a = 5, 7$ ή 11 τότε $s = 2$.

Στη συνέχεια θα μελετήσουμε μερικές ιδιότητες της έννοιας της τάξης που μόλις ορίσαμε.

Πρόταση 5.4.3. *Αν $s := \mathrm{ord}_m(a)$ και ισχύει*

$$a^\ell \equiv 1 \mathrm{mod} m,$$

τότε $s \mid \ell$.

Απόδειξη. Σύμφωνα με το θεώρημα της διαίρεσης με υπόλοιπο ο ℓ γράφεται στη μορφή

$$\ell = sq + u, \quad 0 \leq u < s.$$

Επομένως

$$a^\ell = (a^s)^q a^u \equiv a^u \equiv 1 \mathrm{mod} m$$

Όμως s είναι ο ελάχιστος μη-μηδενικός φυσικός με αυτή την ιδιότητα. Συνεπώς $\upsilon = 0$, δηλαδή $s \mid \ell$. □

Παρατήρηση 5.4.4. Άμεση συνέπεια της πρότασης 5.4.3 και του θεωρήματος 4.2.7 του Euler είναι ότι πάντοτε ισχύει $s := \mathrm{ord}_m a \mid \phi(m)$. Μάλιστα, αν ο $m = p$ πρώτος αριθμός, τότε $s \mid (p - 1)$.

Πρόταση 5.4.5. *Αν $s := \mathrm{ord}_m(a)$, τότε οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:*

1. $a^k \equiv a^\ell \mathrm{mod} m$
2. $k \equiv \ell \mathrm{mod} s$

Απόδειξη. $1 \Rightarrow 2$. Υποθέτουμε ότι $a^k \equiv a^\ell \mathrm{mod} m$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $\ell < k$. Σύμφωνα με την πρόταση 1.5.5 $(a^\ell, m) = 1$ αφού $(a, m) = 1$. Επομένως a είναι αντιστρέψιμο και $a^{k-\ell} \equiv 1 \mathrm{mod} m$. Η πρόταση 5.4.3 δίνει $s \mid (k - \ell)$, δηλαδή

$$k \equiv \ell \mathrm{mod} s$$

$2 \Rightarrow 1$. Υποθέτουμε ότι $k \equiv \ell \mathrm{mod} s$. Επομένως υπάρχει ακέραιος t ώστε $k = \ell + t \cdot s$. Συνεπώς

$$a^k = a^{\ell+ts} = a^\ell (a^s)^t \equiv a^\ell \mathrm{mod} m.$$

□

Πρόταση 5.4.6.
- *Αν* $s := \mathrm{ord}_m(a)$ *τότε* $s' := \mathrm{ord}_m(a^\ell) = \frac{s}{d}$, *όπου* $d = (\ell, s)$.
- *Αν* $s_1 := \mathrm{ord}_m(a)$, $s_2 := \mathrm{ord}_m(b)$ *και* $(s_1, s_2) = 1$, *τότε* $s := \mathrm{ord}_m(ab) = s_1 s_2$.

Απόδειξη.
- Από τον ορισμό της τάξης έπεται ότι $a^s \equiv 1 \mathrm{mod} m$. Επομένως $(a^s)^{\ell/d} = (a^\ell)^{s/d} \equiv 1 \mathrm{mod} m$. Λόγω της πρότασης 5.4.3

$$\mathrm{ord}_m(a^\ell) \mid \frac{s}{d}, \quad s' \mid \frac{s}{d}.$$

Επίσης $(a^\ell)^{s'} \equiv 1 \mathrm{mod} m$, δηλαδή

$$a^{\ell s'} \equiv 1 \mathrm{mod} m$$

Επομένως, η πρόταση 5.4.3, $s \mid \ell s'$, δηλαδή $\frac{s}{d} \mid \frac{\ell}{d} s'$. Όμως $\left(\frac{s}{d}, \frac{\ell}{d}\right) = 1$, αφού $(s, \ell) = d$. Η 1.5.5 δίνει $\frac{s}{d} \mid s'$. Συνεπώς $s' = \frac{s}{d}$.

- Από τον ορισμό της τάξης, έπεται ότι

$$\begin{aligned} a^{s_1} &\equiv 1 \mathrm{mod} m \\ b^{s_2} &\equiv 1 \mathrm{mod} m \\ (ab)^s &\equiv 1 \mathrm{mod} m \end{aligned}$$

Άρα

$$b^{ss_1} = 1 b^{ss_1} \equiv (a^{s_1})^s b^{ss_1} \equiv (ab)^{ss_1} \equiv 1 \mathrm{mod} m$$

Συνεπώς, η πρόταση 5.4.3 $s_2 \mid ss_1$. Επειδή $(s_1, s_2) = 1$ 1.5.5 έχουμε $s_2 \mid s$. Ανάλογα αποδεικνύεται ότι $s_1 \mid s$. Συνεπώς $s_1 s_2 \mid s$.

Βέβαια

$$(ab)^{s_1 s_2} = (a^{s_1})^{s_2} (b^{s_2})^{s_1} \equiv 1 \cdot 1 \equiv 1 \mathrm{mod} m$$

και λόγω της πρότασης 5.4.3 $s \mid s_1 s_2$, συνεπώς $s = s_1 s_2$.

□

Παρατήρηση 5.4.7. Άμεση συνέπεια της πρότασης 5.4.6.1 είναι ότι αν η τάξη του $a \mathrm{mod} m$, $\mathrm{ord}_m(a) = st$, τότε η τάξη του $a^s \mathrm{mod} m$ είναι t, αφού $(s, st) = s$.

Επίσης, άμεση συνέπεια της πρότασης 5.4.6.2 είναι ότι αν $s := \mathrm{ord}_m(a)$ τότε

$$\mathrm{ord}_m(a^\ell) = s \Leftrightarrow (\ell, s) = 1.$$

Ορισμός 5.4.8. Έστω $a \in \mathbb{Z}$ και $m \in \mathbb{N}$, $m \geq 2$ με $(a, m) = 1$. Ο a θα λέγεται *αρχική ρίζα ή γεννήτορας* $\mathrm{mod}m$ όταν $\mathrm{ord}_m(a) = \varphi(m)$.

Από την παρακάτω πρόταση φαίνεται η χρησιμότητα της έννοιας.

Πρόταση 5.4.9. *Ο a είναι αρχική ρίζα* $\mathrm{mod}m$ *ακριβώς τότε όταν οι δυνάμεις*

$$a, a^2, \ldots, a^{\varphi(m)}$$

αποτελούν ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων $\mathrm{mod}m$.

Σημείωση: Όταν λέμε ότι ο a είναι αρχική ρίζα θα υπονοούμε πάντοτε και την υπόθεση $(a, m) = 1$.

Απόδειξη. Υποθέτουμε ότι το a είναι αρχική ρίζα $\mathrm{mod}m$. Είναι φανερό ότι $(a^i, m) = 1$ για κάθε $i = 1, 2, \ldots, \varphi(m)$ αφού $(a, m) = 1$, πρόταση 1.5.5.6. Επειδή το πλήθος των δυνάμεων του a είναι $\varphi(m)$, αρκεί να αποδείξουμε ότι οι δυνάμεις αυτές είναι ανά δύο διαφορετικές $\mathrm{mod}m$. Πράγματι, αν $a^k \equiv a^\ell \mathrm{mod}m$ $1 \leq k < \ell \leq \varphi(m)$ τότε (πρόταση 5.4.5) $k \equiv \ell \mathrm{mod}\varphi(m)$, δηλαδή $\varphi(m) \mid k - \ell$, άτοπο. Αντιστρόφως, υποθέτουμε ότι το σύνολο $\{a, a^2, \ldots, a^{\varphi(m)}\}$ αποτελεί ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων $\mathrm{mod}m$. Αυτό σημαίνει ότι $a^{\varphi(m)} \equiv 1 \mathrm{mod}m$, ενώ $a^\ell \not\equiv 1 \mathrm{mod}m$ για κάθε ℓ, $1 \leq \ell < \varphi(m)$, δηλαδή ότι ο a είναι αρχική ρίζα $\mathrm{mod}m$. □

Παράδειγμα. Να βρεθεί αν υπάρχει μια αρχική ρίζα mod43.

Για όλους τους ακέραιους $a \in \mathbb{Z}$, πρώτους προς το 43 ισχύει $\mathrm{ord}_{43}(a) \in \{1, 2, 3, 6, 7, 14, 21, 42\}$. Ο a είναι αρχική ρίζα mod43 αν και μόνο αν $\mathrm{ord}_{43}(a) = 42$.

Ας πάρουμε $a = 2$, $2^7 \equiv -1 \mathrm{mod}43$, άρα $2^{14} \equiv 1 \mathrm{mod}43$. Συνεπώς ο $a = 2$ δεν είναι αρχική ρίζα mod43. Ας δοκιμάσουμε το $a = 3$.

$$\begin{aligned} 3^7 &\equiv -6 \mathrm{mod}43 \\ 3^{14} &\equiv 36 \mathrm{mod}43 \\ 3^{21} &\equiv -1 \mathrm{mod}43 \\ 3^{42} &\equiv 1 \mathrm{mod}43 \end{aligned}$$

Επομένως ο $a = 3$ είναι αρχική ρίζα mod43.

Παράδειγμα. Να βρεθεί, αν υπάρχει, μία αρχική ρίζα mod47.

Αν $a = 2$,

$$\begin{aligned} 2^{12} &\equiv 4096 \equiv 7 \mathrm{mod}47 \\ 2^{24} &\equiv 2 \mathrm{mod}47 \\ 2^{23} &\equiv 1 \mathrm{mod}47 \end{aligned}$$

και ο 2 δεν είναι αρχική ρίζα mod47.

Επίσης για $a = -1$, $(-1)^2 \equiv 1 \mathrm{mod}47$. Επομένως $\mathrm{ord}_{47}(2) = 23$ και $\mathrm{ord}_{47}(-1) = 2$.

Από την πρόταση 5.4.6.3 προκύπτει ότι $\mathrm{ord}_{47}(-2) = 2 \cdot 23 = 46$. Συνεπώς ο 45 είναι αρχική ρίζα mod47.

Θεωρούμε αυτονόητα τα ακόλουθα ερωτήματα:

1. Υποθέτουμε ότι υπάρχει μια αρχική ρίζα $\mathrm{mod}m$. Υπάρχουν και άλλες; Πόσες είναι και πώς θα τις βρούμε;

2. Υπάρχει πάντοτε μια αρχική ρίζα mod$m$ για κάθε m; Εδώ η απάντηση είναι αρνητική. Για παράδειγμα δεν υπάρχει αρχική ρίζα mod12. Το ερώτημα τροποποιείται επομένως ως εξής:

3. Για ποιους $m \in \mathbb{Z}$, $m \geq 2$ υπάρχει αρχική ρίζα mod$m$;

4. Δίνεται ο $a \in \mathbb{Z}$. Για ποιους $m \in \mathbb{Z}$ είναι ο a αρχική ρίζα mod$m$;

Άμεση απάντηση στο πρώτο από το ερωτήματα μας δίνει το ακόλουθο πόρισμα της πρότασης 5.4.9:

Πόρισμα 5.4.10. *Αν υπάρχει αρχική ρίζα* mod$m$*, τότε το πλήθος των αρχικών ριζών* mod$m$ *είναι* $\phi(\phi(m))$.

Απόδειξη. Έστω a μια αρχική ρίζα mod$m$. Σύμφωνα με την πρόταση 5.4.9 κάθε άλλη αρχική ρίζα περιέχεται στο σύνολο $\{a, a^2, \ldots, a^{\phi(m)}\}$. Τα στοιχεία του συνόλου αυτού που έχουν τάξη $\phi(m)$ είναι οι δυνάμεις του a, a^ℓ με $\mathrm{ord}_m(a^\ell) = \phi(m)$. Αυτό όμως ισχύει ακριβώς τότε όταν $(\ell, \phi(m)) = 1$. Το πλήθος των ℓ, $1 \leq \ell \leq \phi(m)$ με $(\ell, \phi(m)) = 1$ είναι $\phi(\phi(m))$. □

Παράδειγμα. Για $m = 43$, $\phi(m) = 43 - 1 = 42$ και την αρχική ρίζα $a = 3$ έχουμε τις αρχικές ρίζες mod43.

$$a = 3, 3^5, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{25}, 3^{29}, 3^{31}, 3^{37}, 3^{41} \mathrm{mod} 43$$

Το πλήθος τους είναι $\phi(42) = \phi(2 \cdot 3 \cdot 7) = 12$ και είναι οι

$$a = 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34 \mathrm{mod} 43$$

Παρατήρηση 5.4.11. Εδώ υποθέσαμε ότι γνωρίζαμε ήδη την ύπαρξη της αρχικής ρίζας $a = 3$. Αυτή την υπολογίσαμε πιο πριν εύκολα αλλά γενικά η εύρεσή της δεν είναι ένα εύκολο πρόβλημα.

Στη συνέχεια θα περάσουμε στο (3) ερώτημα. Στο πρώτο μας βήμα θα αποδείξουμε ότι υπάρχουν αρχικές ρίζες mod$p$ για κάθε περιττό πρώτο αριθμό p. Η απόδειξη θα στηριχθεί στο ακόλουθο:

Λήμμα 5.4.12. *Αν p περιττός πρώτος, ℓ θετικός ακέραιος και q πρώτος τέτοιος ώστε*

$$q^\ell \mid (p-1)$$

τότε υπάρχει ακέραιος a του οποίου η τάξη mod$p$ *να είναι q^ℓ, $\mathrm{ord}_p(a) = q^\ell$.*

Απόδειξη. Σύμφωνα με το θεώρημα του Lagrange 4.7.4 η ισοτιμία

$$x^{\frac{p-1}{q}} \equiv 1 \mathrm{mod} p$$

έχει το πολύ $s = \frac{p-1}{q} \leq \frac{p-1}{2} < p-1$ λύσεις.

Αυτό σημαίνει ότι υπάρχει τουλάχιστον ένα $b \in \{1, 2, \ldots, p-1\}$ για το οποίο ισχύει

$$b^{\frac{p-1}{q}} \not\equiv 1 \mathrm{mod} p, \quad (b, p) = 1$$

Θα αποδείξουμε ότι η τάξη του στοιχείου $a := b^{\frac{p-1}{q^\ell}}$ είναι ακριβώς q^ℓ.

Πράγματι $a^{q^\ell} = b^{p-1} \equiv 1 \mathrm{mod} p$ που σημαίνει ότι (πρόταση 5.4.3), $t := \mathrm{ord}_p(a) \mid q^\ell$.

Αν $t = \mathrm{ord}_p(a) < q^\ell$ θα είχαμε $t \mid q^{\ell-1}$, οπότε

$$b^{\frac{q-1}{q}} = a^{q^{\ell-1}} \equiv 1 \mathrm{mod} p,$$

άτοπο. Συνεπώς $t = q^\ell$. □

Πρόταση 5.4.13. *Για κάθε πρώτο αριθμό p υπάρχει μία τουλάχιστον αρχική ρίζα* mod$p$.

Απόδειξη. Για $p = 2$ το $a = 1$ είναι αρχική ρίζα mod2.

Υποθέτουμε τώρα ότι ο p είναι περιττός πρώτος και έστω

$$p - 1 = \prod_{i=1}^{r} p_i^{\ell_i}$$

η ανάλυση του $p-1$ σε γινόμενο πρώτων παραγόντων. Σύμφωνα με το λήμμα 5.4.12 για κάθε $i = 1, 2, \ldots, r$ υπάρχουν ακέραιοι a_i οι οποίοι να έχουν τάξη $\mathrm{ord}_p(a_i) = p_i^{\ell_i}$. Ο ακέραιος $a := \prod_{i=1}^{r} a_i$ έχει τάξη (πρόταση 5.4.6.2)

$$\mathrm{ord}_p(a) = \prod_{i=1}^{r} \mathrm{ord}_p(a_i) = \prod_{i=1}^{r} p_i^{\ell_i} = p - 1.$$

Επομένως ο a είναι αρχική ρίζα mod$p$. □

Παρατήρηση 5.4.14. Άμεση συνέπεια της πρότασης 5.4.13 και του πορίσματος 5.4.10 είναι ότι για κάθε πρώτο p υπάρχουν ακριβώς $\phi(p-1)$ αρχικές ρίζες.

Αν και δεν συνδέεται άμεσα με τον προβληματισμό μας θα αποδείξουμε κάτι ισχυρότερο, ότι δηλαδή για κάθε διαιρέτη $d \mid (p-1)$ υπάρχουν ακριβώς $\phi(d)$ ανισότιμοι mod$p$ ακέραιοι οι οποίοι έχουν τάξη mod$p$ ίση με d. Πρώτα απ' όλα όμως θα αποδείξουμε μια βοηθητική για μας πρόταση.

Πρόταση 5.4.15. *Για κάθε θετικό ακέραιο $n \geq 1$, ισχύει*

$$n = \sum_{d \mid n} \phi(d)$$

Στο παραπάνω άθροισμα το d διατρέχει τους θετικούς διαιρέτες του n.

Απόδειξη. Θεωρούμε το σύνολο

$$S_d := \{m \in \mathbb{N} : 1 \leq m \leq n \text{ και } (m, n) = d\}.$$

Είναι γνωστό, πρόταση 1.5.5 ότι

$$(m, n) = d \Leftrightarrow \left(\frac{m}{d}, \frac{n}{d}\right) = 1.$$

Επομένως το πλήθος των στοιχείων του συνόλου S_d είναι ίσο με το πλήθος των θετικών ακέραιων $\leq \frac{n}{d}$ οι οποίοι είναι πρώτοι προς τον $\frac{n}{d}$, δηλαδή $\phi(n/d)$. Τα σύνολα S_d αποτελούν μια διαμέριση του συνόλου $\{1, 2, \ldots, n\}$, άρα $n = \sum_{d \mid n} \phi(n/d)$.

Όταν το d διατρέχει όλους τους θετικούς διαιρέτες του n, το ίδιο κάνει και το n/d δηλαδή

$$\sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(n),$$

συνεπώς

$$n = \sum_{d \mid n} \phi(d).$$

□

Πρόταση 5.4.16. *Αν p πρώτος αριθμός και d ένας θετικός διαιρέτης του $p-1$. Υπάρχουν $\phi(d)$ ανισότιμοι* mod$p$ *ακέραιοι οι οποίοι έχουν τάξη* mod$p$ *ίση με d.*

Απόδειξη. Αν το σύνολο S περιέχει ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων mod$p$, τότε για κάθε $a \in S$, $\mathrm{ord}_p(a) \mid (p-1)$.

Για κάθε θετικό διαιρέτη d του $p-1$ ορίζουμε

$$\psi(d) = \#\{a \in S : \mathrm{ord}_p(a) = d\}.$$

Είναι φανερό ότι

$$\sum_{d|(p-1)} \psi(d) = p-1.$$

Για το $\psi(d)$ έχουμε δύο δυνατότητες:

$$\psi(d) = 0 \text{ ή } \psi(d) \neq 0.$$

Αν $\psi(d) = 0$, τότε $\psi(d) \leq \phi(d)$.

Αν $\psi(d) \neq 0$, τότε υπάρχει ένα τουλάχιστον $a \in S$ με $\mathrm{ord}_p(a) = d$. Στην περίπτωση αυτή οι αριθμοί $a, a^2, \ldots, a^d$ είναι ανά δύο ανισότιμοι mod$p$ και όλοι τους είναι λύσεις της ισοτιμίας

$$x^d - 1 \equiv 0 \mathrm{mod} p$$

Σύμφωνα με το θεώρημα του Lagrange 4.7.4 αυτές είναι όλες οι λύσεις της ισοτιμίας. Επομένως, κάθε λύση της ισοτιμίας είναι ισότιμη με ακριβώς μία δύναμη του a, $a^\ell \mathrm{mod} p$, $\ell = 1, 2, \ldots, d$. Ιδιαίτερα αυτό θα ισχύει και για κάθε στοιχείο τάξης d. Αλλά τα στοιχεία τάξης d είναι ακριβώς τα a^ℓ με $(\ell, d) = 1$, δηλαδή έχουν πλήθος $\phi(d)$.

Συνεπώς, αν $\psi(d) \neq 0$, τότε $\psi(d) = \phi(d)$. Τελικά, για κάθε θετικό διαιρέτη του $p-1$ ισχύει

$$\psi(d) \leq \phi(d).$$

Σε συνδυασμό με την πρόταση 5.4.15 προκύπτει

$$p-1 = \sum_{d|(p-1)} \psi(d) \leq \sum_{d|(p-1)} \phi(d) = p-1,$$

από το οποίο συνάγεται ότι $\psi(d) = \phi(d)$ για κάθε θετικό διαιρέτη d του $p-1$. □

Επιστρέφουμε στο ερώτημα (3).

Πρόταση 5.4.17. *Αν $m, n \in \mathbb{Z}$ με $(m,n) = 1$, $m, n > 2$ τότε δεν υπάρχει αρχική ρίζα* modmn.

Απόδειξη. Αν $a \in \mathbb{Z}$ με $(a, mn) = 1$ τότε 1.5.5, $(a,m) = (a,n) = 1$. Σύμφωνα με το θεώρημα του Euler

$$a^{\phi(m)} \equiv 1 \mathrm{mod} m$$

Επειδή $n > 2$, έπεται ότι ο $\phi(n)$ είναι άρτιος. Επομένως

$$a^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \mathrm{mod} m$$

Ομοίως

$$a^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \mathrm{mod} n$$

Το θεώρημα του Euler και η πρόταση 1.5.5, μας δίνουν

$$a^{\frac{\phi(mn)}{2}} \equiv 1 \mathrm{mod} mn$$

Αυτό σημαίνει ότι $\mathrm{ord}_{mn}(a) < \phi(mn)$ και συνεπώς ο a δεν είναι αρχική ρίζα modmn. □

Παρατήρηση 5.4.18. Αν ο m διαιρείται από το γινόμενο δύο περιττών ακέραιων ή από το 4 και κάποιο περιττό ακέραιο, τότε δεν υπάρχει αρχική ρίζα mod$m$. Επομένως, αν υπάρχει αρχική ρίζα mod$m$, τότε ο m θα είναι της μορφής $m = 2^\ell p^a$, $a, \ell \in \mathbb{N}$, $\ell \in \{0, 1\}$.

Θα εξετάσουμε την περίπτωση $m = 2^\ell, (a = 0)$. Για $m = 2$ και $m = 4$ έχουμε αρχικές ρίζες $a = 1$ και $a = 3$ αντίστοιχα. Για $m = 2^3 = 8$ οι πρώτες κλάσεις υπολοίπων mod8 είναι $1, 3, 5$ και 7. Όλες έχουν τάξη ≤ 2, ενώ $\phi(8) = 4$, δηλαδή δεν υπάρχει αρχική ρίζα mod8.

Πρόταση 5.4.19. *Για κάθε $\ell \geq 3$ δεν υπάρχουν αρχικές ρίζες* mod2^ℓ.

Απόδειξη. Θα αποδείξουμε επαγωγικά ότι για κάθε περιττό ακέραιο a ισχύει

$$a^{2^{\ell-2}} \equiv 1 \mathrm{mod} 2^\ell$$

Για $\ell = 3$ ισχύει. Υποθέτουμε ότι η ισοτιμία ισχύει για $\ell \geq 3$ και θα αποδείξουμε ότι ισχύει και για $\ell + 1$. Εξ υποθέσεως λοιπόν έχουμε

$$a^{2^{\ell-2}} = 1 + 2^\ell t, \quad t \in \mathbb{Z}.$$

Επομένως,

$$a^{2^{\ell-1}} = (a^{2^{\ell-1}})^2 = (1 + 2\ell^t)^2 = 1 + t2^{\ell+1} + t^2 2^{2\ell}.$$

Επειδή $\ell \geq 3$, έπεται ότι $2\ell \geq \ell + 1$. Άρα

$$a^{2^{\ell-1}} \equiv 1 \mathrm{mod} 2^{\ell+1}.$$

Αποδείξαμε ότι

$$a^{\frac{\phi(2^\ell)}{2}} \equiv 1 \mathrm{mod} 2^m$$

για κάθε $\ell \geq 3$, δηλαδη $\mathrm{ord}_2(a) < \phi(2^\ell)$. Αυτό σημαίνει ότι ο a δεν είναι αρχική ρίζα mod2^ℓ. □

Παρατήρηση 5.4.20. Συνοψίζοντας τα μέχρι στιγμής αποτελέσματα:

Αν για κάποιο $m \in \mathbb{Z}, m \geq 2$ υπάρχει αρχική ρίζα mod$m$ τότε $m \in \{2, 4, p^\ell, 2p^\ell\}$. Απομένει ο έλεγχος των περιπτώσεων p^ℓ και $2p^\ell$.

Πρόταση 5.4.21. *Αν p περιττός πρώτος τότε υπάρχει αρχική ρίζα* modp^ℓ *για κάθε $\ell \geq 1$.*

Απόδειξη. Έχουμε ήδη αποδείξει ότι υπάρχει αρχική ρίζα mod$p$, πρόταση 5.4.13.

Έστω λοιπόν a μια αρχική ρίζα mod$p$. Σύμφωνα με το θεώρημα του Fermat

$$a^{p-1} \equiv 1 \mathrm{mod} p$$

Άρα υπάρχει $t \in \mathbb{Z}$ τέτοιος ώστε $a^{p-1} - 1 = tp$. Ορίζουμε τον ακέραιο b,

$$b := \begin{cases} a & \text{αν } p \nmid t \\ a + p & \text{αν } p \mid t \end{cases}.$$

Θα αποδείξουμε ότι ο b είναι μια αρχική ρίζα modp^ℓ για κάθε $\ell \geq 2$.

Αν $p \mid t$ τότε $a^{p-1} \equiv 1 \mathrm{mod} p^2$ οπότε

$$b^{p-1} = (a + p)^{p-1} \equiv a^{p-1} + (p - 1)pa^{p-2} \equiv 1 + (p - 1)pa^{p-2} \mathrm{mod} p^2$$

Συνεπώς $b^{p-1} = 1 + pm$ με $p \nmid m$. Το ίδιο ισχύει και όταν $p \nmid t$,

$$b^{p-1} = a^{p-1} = 1 + pt.$$

Αποδείξαμε ότι

$$b^{p-1} = 1 + pt_1 \text{ με } p \nmid t_1.$$

Αυτό σημαίνει ότι $b^{p-1} \not\equiv 1 \bmod p^2$, δηλαδή ότι $\mathrm{ord}_{p^s}(p) = p(p-1) = \phi(p^2)$ και συνεπώς το b είναι αρχική ρίζα $\bmod p^2$.

Επαγωγικά αποδεικνύεται ότι για κάθε $\ell \geq 1$ ισχύει

$$b^{(p-1)p^\ell} = 1 + p^\ell t_\ell, \text{ με } p \nmid t_\ell,$$

δηλαδή ότι

$$b^{(p-1)p^{\ell-1}} \not\equiv 1 \bmod p^{\ell+1}.$$

Αν $s_\ell := \mathrm{ord}_{p^\ell}(b)$ τότε $s_\ell \mid \phi(p^\ell) = p^\ell(p-1)$.

Επειδή $b^{s_\ell} \equiv 1 \bmod p^\ell$ έπεται ότι και $b^{s_\ell} \equiv 1 \bmod p$, συνεπώς $(p-1) \mid s_\ell$.

Αποδείξαμε ότι το s_ℓ θα εχει κατ' ανάγκη τη μορφή

$$s_\ell = (p-1)p^d, \quad 0 \leq d \leq \ell - 1.$$

Αν $s_\ell \neq (p-1)p^{\ell-1}$, τότε $s_\ell \mid (p-1)p^{\ell-2}$ και επομένως θα ίσχυε η ισοτιμία

$$b^{(p-1)p^{\ell-2}} \equiv 1 \bmod p^\ell$$

Όμως

$$b^{(p-1)p^{\ell-2}} = 1 + p^{\ell-1} t_{\ell-1}$$

με $p \nmid t_{\ell-1}$. Αυτό σημαίνει ότι

$$b^{(p-1)p^{\ell-2}} \not\equiv 1 \bmod p^\ell$$

Καταλήξαμε σε άτοπο γιατί υποθέσαμε $d < \ell - 1$. Συνεπώς, $d = \ell - 1$, $s_\ell = (p-1)p^{\ell-1} = \phi(p^\ell)$ και επομένως το b είναι αρχική ρίζα $\bmod p^\ell$.

Απόδειξη της μαθηματικής επαγωγής:

Για $\ell = 1$ ισχύει. Υποθέτουμε ότι ισχύει για $\ell \geq 1$. Θα αποδείξουμε ότι ισχύει και για $\ell + 1$. Ισχύει για ℓ:

$$b^{(p-1)p^{\ell-1}} = 1 + p^\ell t_\ell \text{ με } p \nmid t_\ell.$$

Υψώνουμε τα μέλη της τελευταίας ισότητας στην p-στη δύναμε και έχουμε

$$b^{(p-1)p^\ell} \equiv 1 + pp^\ell t_\ell \bmod p^{\ell+2}$$

Επομένως

$$b^{(p-1)p6^\ell} = 1 + p^{\ell+1} t_{\ell+1} \text{ με } p \nmid t_{\ell+1}.$$

□

Η απόδειξη για το $2p^\ell$ στηρίζεται στην πρόταση 5.4.21.

Πρόταση 5.4.22. *Για κάθε περιττό πρώτο p και κάθε ακέραιο $\ell \geq 1$ υπάρχει αρχική ρίζα $\bmod 2p^\ell$.*

Απόδειξη. Έστω b μια αρχική ρίζα $\mathrm{mod}p^\ell$ και

$$c := \begin{cases} b & \text{αν } b \text{ περιττός} \\ b + p^\ell & \text{αν } b \text{ άρτιος} \end{cases}$$

Και το $b + p^\ell$ είναι αρχική ρίζα $\mathrm{mod}p^\ell$. Από τον ορισμό του c προκύπτει αμέσως ότι $(c, 2p^\ell) = 1$. Αν $s_\ell := \mathrm{ord}_{2p^\ell}(c)$ τότε

$$s_\ell \mid \phi(2p^\ell) = \phi(2)\phi(p^\ell).$$

Επειδή $c^{s_\ell} \equiv 1 \mathrm{mod} 2p^\ell$ θα ισχύει και

$$c^{s_\ell} \equiv 1 \mathrm{mod} p^\ell$$

και συνεπώς $\phi(p^\ell) \mid s_\ell$. Άρα $s_\ell = \phi(2p^\ell)$. □

Συνοψίζουμε τα μέχρι τώρα αποτελέσματα:

Θεώρημα 5.4.23. *Αν m ακέραιος $m > 1$ τότε υπάρχει αρχική ρίζα $\mathrm{mod}m$ ακριβώς τότε όταν ο m έχει τη μορφή $2, 4, p^\ell, 2p^\ell$ για $\ell \geq 1$.*

Το πλήθος των αρχικών ριζών $\mathrm{mod}m$ είναι $\phi(\phi(m))$. Αν a είναι μια αρχική ρίζα $\mathrm{mod}m$ τότε όλες οι αρχικές ρίζες δίνονται από τις δυνάμεις του a^t, με $1 \leq t < \phi(m)$ και $(t, \phi(m)) = 1$.

Αν ο a είναι αρχική ρίζα $\mathrm{mod}p$ και $a^{p-1} - 1 = pt$ τότε ο

$$b := \begin{cases} a & \text{όταν } p \nmid t \\ a + p & \text{όταν } p \mid t \end{cases}$$

είναι αρχική ρίζα $\mathrm{mod}p^\ell$ για κάθε $\ell \geq 1$ και

$$c := \begin{cases} b & \text{αν } b \text{ περιττός} \\ b + p^\ell & \text{αν } b \text{ άρτιος} \end{cases}$$

είναι αρχική ρίζα $\mathrm{mod}2p^\ell$.

Παρατήρηση 5.4.24. Το θεώρημα 5.4.23 δίνει πλήρη απάντηση στο ερώτημα (3). Απαραίτητη προϋπόθεση φυσικά είναι η εύρεση μιας αρχικής ρίζας $\mathrm{mod}p$, p περιττός πρώτος. Ένας τρόπος είναι να ξεκινήσουμε να ελέγχουμε διαδοχικά τους ακέραιους

$$a = 2, 3, 5, 6, \ldots$$

με την ελπίδα να βρούμε σύντομα μια αρχική ρίζα $\mathrm{mod}p$. Δεν εξετάζουμε τους ακέραιους που είναι τέλειες δυνάμεις γιατί αν ο $b = a^\ell$ είναι αρχική ρίζα τότε είναι και ο a και έχει ήδη εξεταστεί.

Το ερώτημα είναι πόσο μακριά πρέπει να πάμε για να βρούμε αρχική ρίζα. Υπάρχει ένα αποτέλεσμα του Shoup, [30] σύμφωνα με το οποίο ο a φράσσεται από τον $(\log p)^6$ επί κάποια σταθερά. Δυστυχώς το αποτέλεσμα στηρίζεται σε μία αναπόδεικτη μέχρι σήμερα εικασία τη *Γενικευμένη εικασία του Riemann*.

Επίσης είναι γνωστή μια εικασία του E. Bach σύμφωνα με την οποία η ελάχιστη αρχική ρίζα $\mathrm{mod}p$ είναι $\log p \log\log p$ επί μία σταθερά [12]

Για να ελέγξουμε τώρα αν ο a που πήραμε είναι αρχική ρίζα θα πρέπει να παραγοντοποιήσουμε τον αριθμό $p - 1$ και να ελέγχουμε διαδοχικά αν

$$a^{\frac{p-1}{q}} \not\equiv 1 \mathrm{mod} p$$

για κάθε πρώτο διαιρέτη q του $p-1$. Αν σε κάποιο βήμα βρούμε $a^{\frac{p-1}{q}} \equiv 1 \bmod q$ τότε επιλέγουμε ένα άλλο a.

Ιστορικά 5.4.1

Ο πρώτος πίνακας αρχικών ριζών mod$p$ για $p < 1000$ δόθηκε από τον C.G. Jacobi το 1839 στο *Canon Arithmeticus*. Επανεκδόθηκε από τον εκδοτικό οίκο Akademie-Verlag Berlin το 1956.
Και ο R. Osborn στο "Tables of all primitive roots of odd primes less than 1000" Austin 1961 έκανε το ίδιο [3]. Οι A.E. Western και J.C.P. Miller [8] επεξέτειναν τους πίνακες για $p \leq 50021$.

Επιστρέφουμε στο ερώτημα (4). Ας πάρουμε $a = 2$ και $m = p$ πρώτος αριθμός. Για ποιους πρώτους p ο 2 είναι αρχική ρίζα mod$p$; Από τους πίνακες για 4000 αυτό συμβαίνει για τους πρώτους

$$p = 3, 5, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163173, 179, 181, 197,$$

$$211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, 509,$$

$$523, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709, 757, 773,$$

$$787, 797, 821, 827, 829, 853, 859, 877, 883, 907, 941, 947.$$

Μήπως υπάρχει κάποιος κανόνας; Άγνωστο. Ούτε ο Artin κατάφερε να βρει. Υπάρχουν 129 πρώτοι μικρότεροι του 1000. Από αυτούς, οι 67 έχουν ως αρχική ρίζα το 2. Με βάση παρόμοια δεδομένα ο Artin διατύπωσε την ομώνυμη εικασία:

Εικασία του Artin (1920) Υπάρχουν άπειροι πρώτοι p για τους οποίους ο 2 είναι αρχική ρίζα mod$p$.

Σύντομα μάλιστα τη γενίκευσε, αφού διαπίστωσε ότι το $a = 2$ δεν παίζει σημαντικό ρόλο. Αυτό έγινε σε κάποιο γράμμα του προς τον Hasse με ημερομηνία 27 Σεπτεμβρίου του 1927:

Γενικευμένη εικασία του Artin :

Κάθε ακέραιος a, $a \neq -1, 0$ και a όχι τέλειο τετράγωνο είναι αρχική ρίζα mod$p$ για άπειρο πλήθος πρώτων p.

Τι γνωρίζουμε μέχρι σήμερα για την εικασία του Artin;

Στα 1967 ο C. Holley απέδειξε ότι είναι αληθής [6] υπό την προϋπόθεση ότι ισχύει η γενικευμένη εικασία του Riemann.

Οι R. Gupta και M. Ram Murty [28] απέδειξαν, χωρίς τη χρήση καμμιάς υπόθεσης ότι η εικασία του Artin είναι αληθής για άπειρο πλήθος a. Λίγο αργότερα ο R. Heath- Brown [29] απέδειξε απέδειξε ότι υπάρχουν το πολύ δύο πρώτοι αριθμοί για τους οποίους η εικασία δεν ισχύει. Δυστυχώς από την απόδειξη δεν προκύπτει ποιοι είναι αυτοί. Έτσι γνωρίζουμε ότι από τους πρώτους $2, 3, 5$ για έναν τουλάχιστον ισχύει αλλά δεν γνωρίζουμε αν είναι για παράδειγμα ο 2.

Τέλος, ο Pieter Morre, [26] απέδειξε ότι για δοσμένο a υπάρχουνε άπειροι πρώτοι p για τους οποίος η τάξη $\mathrm{ord}_p(a)$ είναι διαιρετή από τον μεγαλύτερο πρώτο παράγοντα του $p-1$.

5.4.1 n-στα υπόλοιπα

Μπορούμε τώρα να επιστρέψουμε στα n-στα υπόλοιπα mod$m$. Αν $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $m > 1$ και $(a, m) = 1$, τότε:

Πότε είναι η ισοτιμία

$$x^n \equiv a \bmod m$$

επιλύσιμη για $n \geq 2$; Αν είναι επιλύσιμη πόσες λύσεις έχει; Πώς θα μπορούσαμε να τις βρούμε;

Προς το παρόν θα περιοριστούμε στην περίπτωση που ο m είναι ένας περιττός πρώτος. Θα τον συμβολίζουμε με p. Αν $n = 2$, ένας χαρακτηρισμός ύπαρξης λύσεων δίνεται μέσω του κριτηρίου του Euler:

Η ισοτιμία $x^2 \equiv a \bmod p$ είναι επιλύσιμη ακριβώς τότε όταν $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Παρατηρούμε ότι $2 = (p-1, 2)$. Αν υποθέσουμε ότι η

$$x^n \equiv a \bmod p$$

έχει λύση, έστω $b \bmod p$ τότε είναι φανερό ότι και $(b, p) = 1$. Αν $d := (n, p-1)$ τότε

$$a^{\frac{p-1}{d}} \equiv b^{\frac{p-1}{d} \cdot n} \equiv (b^{p-1})^{\frac{n}{d}} \equiv 1 \bmod p$$

Βλέπουμε δηλαδή αμέσως ότι η μία κατεύθυνση του κριτηρίου του Euler ισχύει γενικά για κάθε n, $n \geq 2$. Θα αποδείξουμε ότι ισχύει και το αντίστροφο. Σε πρώτο βήμα θα αποδείξουμε το ακόλουθο κριτήριο:

Πρόταση 5.4.25. *Υποθέτουμε ότι ο p είναι ένας περιττός πρώτος, $a \in \mathbb{Z}$, $p \nmid a$ και g μια αρχική ρίζα $\bmod p$. Η ισοτιμία*

$$x^n \equiv a \bmod p$$

είναι επιλύσιμη ακριβώς τότε όταν $a = g^{kd} \bmod p$, όπου $k \in \mathbb{Z}$ και $d = (p-1, n)$.

Απόδειξη. Σύμφωνα με την πρόταση 5.4.9 οι δυνάμεις

$$g, g^2, \ldots, g^{p-1}$$

αποτελούν ένα πλήρες σύστημα των πρώτων κλάσεων υπολοίπων $\bmod p$. Αφού $p \nmid a$ έπεται ότι

$$a \equiv g^{\ell} \bmod p, \quad 1 \leq \ell \leq p-1.$$

Αν $b \in \mathbb{Z}$ λύση της ισοτιμίας, τότε και $p \nmid b$ και συνεπώς το $b \equiv g^s \bmod p$ κάποιο $1 \leq s \leq p-1$. Επομένως η ισοτιμία έχει λύση ακριβώς τότε όταν υπάρχει $s \in \mathbb{N}$ έτσι ώστε να ισχύει

$$g^{sn} \equiv g^{\ell} \bmod p$$

Η ισοτιμία αυτή είναι ισοδύναμη (πρόταση 5.4.5) προς την

$$sn \equiv \ell \bmod (p-1) \tag{5.4.3}$$

Η τελευταία ισοτιμία έχει λύση τότε και μόνο τότε όταν $d = (p-1, n) \mid \ell$, δηλαδή όταν $\ell = d \cdot k$ για κάποιο $k \in \mathbb{Z}$. Μάλιστα η (5.4.3) έχει ακριβώς d λύσεις και συνεπώς και η αρχική,

$$x^n \equiv a \bmod p$$

□

Πρόταση 5.4.26 (Γενικευμένο κριτήριο Euler)**.** *Ισχύουν οι προϋποθέσεις της πρότασης 5.4.25. Η ισοτιμία*

$$x^n \equiv a \bmod p$$

είναι επιλύσιμη ακριβώς τότε όταν

$$a^{\frac{p-1}{d}} \equiv 1 \bmod p, \quad \text{όπου } d := (p-1, n).$$

Απόδειξη. Η κατεύθυνση " $\Rightarrow$ " έχει ήδη αποδειχθεί.

Για το αντίστροφο, υποθέτουμε ότι

$$a^{\frac{p-1}{d}} \equiv 1 \bmod p \;\; d := (p-1, n).$$

Αφού $p \nmid a$, υπάρχει $t \in \mathbb{Z}$ τέτοιος ώστε

$$a \equiv g^t \bmod p, \;\; g \text{ μια αρχική ρίζα } \bmod p$$

Επομένως

$$g^{\frac{t(p-1)}{d}} \equiv a^{\frac{p-1}{d}} \equiv 1 \bmod p$$

Το g είναι μια πρωταρχική ρίζα $\bmod p$. Επομένως

$$\mathrm{ord}_p(g) = (p-1) \mid (p-1)\frac{t}{d}.$$

Αυτό σημαίνει ότι $\frac{t}{d}$ είναι ακέραιος δηλαδή ότι $t = kd$, $k \in \mathbb{Z}$. Τότε όμως

$$a \equiv g^{kd} \bmod p$$

και συνεπώς (πρόταση 5.4.25) η $x^n \equiv a \bmod p$ είναι επιλύσιμη. □

Εφαρμογή: Η ισοτιμία

$$x^8 \equiv 16 \bmod p$$

έχει λύση για κάθε πρώτο αριθμό p.

Απόδειξη. Αν $p = 2$ η λύση $x_0 = 0$ είναι προφανής. Έστω $p \neq 2$. Αν $p \not\equiv 1 \bmod 8$ τότε ο $d = (p-1, n) = (p-1, 8) < 8$. Συνεπώς $d \in \{1, 2, 4\}$ και

$$a^{\frac{p-1}{d}} = 16^{\frac{p-1}{d}} = 2^{(p-1)k} \equiv 1 \bmod p$$

όπου $k = 4, 2, 1$ για $d = 1, 2, 4$ αντίστοιχα.

Σύμφωνα με το γενικευμένο κριτήριο του Euler (πρόταση 5.4.26) η $x^8 \equiv 16 \bmod p$ έχει λύση.

Αν τέλος $p \equiv 1 \bmod 8$, τότε το 2 είναι τετραγωνικό υπόλοιπο $\bmod p$ και αν y_0 μια λύση της ισοτιμίας $y^2 \equiv 2 \bmod p$, τότε μια λύση της $x^8 \equiv 16 \bmod p$ είναι η $x_0 = y_0^4$. □

Παρατήρηση 5.4.27. Η εξίσωση $x^8 = 16$ δεν έχει ακέραια λύση. Συνεπώς δεν ισχύει το τοπικό-γενικό αξίωμα.

Η επόμενη πρόταση αφόρα το σύνολο λύσεων της ισοτιμίας

Πρόταση 5.4.28. *Υποθέτουμε ότι ο p είναι ένας περιττός πρώτος, g μια αρχική ρίζα* $\bmod p$, $n \in \mathbb{Z}$, $n \geq 2$ *και* $d := (n, p-1)$. *Τα n-στα υπόλοιπα* $\bmod p$ *της ισοτιμίας είναι*

$$g^d, g^{2d}, \ldots, g^{\frac{d(p-1)}{d}}$$

Απόδειξη. Άμεση συνέπεια της πρότασης 5.4.25 είναι ότι τα

$$g^d, g^{2d}, \ldots, g^{\frac{d(p-1)}{d}}$$

είναι n-στα υπόλοιπα mod$p$. Θα αποδείξουμε ότι ανά δύο είναι μη-ισόδυναμα mod$p$. Έστω ότι

$$g^{id} \equiv q^{jd} \text{mod} p \text{ για } 1 \leq j < i \leq \frac{p-1}{d}.$$

Αυτό σημαίνει (πρόταση 5.4.5) ότι κατ' ανάγκη

$$id \equiv jd \text{mod}(p-1).$$

Στη συνέχεια θα αποδείξουμε ότι αυτές είναι όλες οι λύσεις της ισοτιμίας. Έστω λοιπόν b ένα n-στο υπόλοιπο mod$p$. Σύμφωνα με την πρόταση 5.4.25

$$b \equiv g^{kd} \text{mod} p$$

για κάποιο $k \in \mathbb{Z}$. Έστω $t := \frac{p-1}{d}$. Γράφουμε το k στη μορφή $k = st + r$, όπου $0 < r \leq t$. Επομένως,

$$\begin{aligned} b &\equiv g^{kd} \equiv g^{(st+r)d} \equiv g^{\left(s\frac{p-1}{d}+r\right)d} \\ &\equiv g^{(p-1)s} g^{rd} \equiv g^{rd} \text{mod} p \end{aligned}$$

Ο b είναι ισότιμος με έναν αριθμό της μορφής g^{rd}. □

Στην απόδειξη των προτάσεων 5.4.26 και 5.4.28 δεν χρησημοποιήθηκε πουθενά ότι το μέτρο ήταν πρώτος αριθμός, παρά μόνο η ύπαρξη αρχικής ρίζας.

Στηριζόμενοι στο θεώρημα 5.4.23, σε συνδυασμό με τις προτάσεις 5.4.26 και 5.4.28 έχουμε

Θεώρημα 5.4.29. *Υποθέτουμε ότι $m = 2, 4, p^\ell$ ή $2p^\ell$, $a \in \mathbb{Z}$ και $(a, m) = 1$.*
Η ισοτιμία

$$x^n \equiv a \text{mod} m$$

έχει λύση ακριβώς τότε όταν

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \text{mod} m,$$

όπου $d = (n, \varphi(m))$. Αν η ισοτιμία έχει λύση, τότε το πλήθος των λύσεων είναι d και τα n-στα υπόλοιπα mod$m$ *είναι ακριβώς οι δυνάμεις*

$$g^d, g^{2d}, \ldots, g^{d\frac{\varphi(m)}{d}},$$

όπου g μια αρχική ρίζα mod$m$.

Στη συνέχεια θα θεωρήσουμε έναν φυσικό αριθμό m, $m \geq 2$. Υποθέτουμε ότι η ανάλυση του m σε γινόμενο πρώτων αριθμών είναι η

$$m = 2^\ell p_1^{\ell_1} p_2^{\ell_2} \cdots p_s^{\ell_s},$$

p_i $i = 1, 2, \ldots s$ είναι περιττοί πρώτοι, $\ell, \ell_i > 0$. Σύμφωνα με το θεώρημα το Κινέζου, η ισοτιμία

$$x^n \equiv a \text{mod} m$$

είναι επιλύσιμη ακριβώς τότε όταν το σύστημα

$$\begin{aligned} x^n &\equiv a \bmod 2^\ell \\ x^n &\equiv a \bmod p_1^{\ell_1} \\ \dots & \quad \dots \\ x^n &\equiv a \bmod p_s^{\ell_s} \end{aligned}$$

έχει λύση.

Επειδή για τις περιττές δυνάμεις πρώτων ισχύει το θεώρημα 5.4.29 έχουμε ένα κριτήριο ελέγχου της επιλυσιμότητας των ισοτιμιών $\bmod p_i^{\ell_i}$.

Όπως έχουμε δει όμως (πρόταση 5.4.19, δεν υπάρχουν αρχικές ρίζες $\bmod 2^\ell$ για $\ell \geq 3$.

Η σημασία της ύπαρξης αρχικών ριζών modulo m εγκείται στο γεγονός ότι αν a μία αρχική ρίζα modulo m και b οποιοσδήποτε ακέραιος με $(b, m) = 1$, υπάρχει ένας μονοσήμαντα ορισμένος modulo $\phi(m)$ ακέραιος k τέτοιος ώστε

$$b = a^k \bmod m$$

Για $m = 2^n$, $n \geq 3$ δεν υπάρχει αρχική ρίζα modulo m.

Θα μας βοηθούσε πολύ αν υπήρχε και εδώ ένα πλήρες σύστημα των πρώτων κλάσεων υπολοίπων $\bmod 2^\ell$ το οποίο να έχει ως αντιπροσώπους δυνάμεις ακέραιων. Θα δούμε αμέσως ότι αυτό ισχύει και ότι ένας τέτοιος αντιπρόσωπος μπορεί να είναι ο $a = 5$.

Πρόταση 5.4.30. *Αν a περιττός ακέραιος, τότε οι ακόλουθες δύο προτάσεις είναι μεταξύ τους ισοδύναμες.*

1. $\mathrm{ord}_{2^\ell}(a) = 2^{\ell-2}$ *για κάθε* $\ell \geq 3$,
2. $a \equiv \pm 3 \bmod 8$

Απόδειξη. (1) $\Rightarrow$ (2) Υποθέτουμε ότι δεν ισχύει η (2) και θα καταλήξουμε σε άτοπο. Επειδή ο a είναι περιττός θα έχουμε $a \equiv \pm 1 \bmod 8$. Άρα $a^2 \equiv 1 \bmod 16$ και επαγωγικά $a^{2^{\ell-3}} \equiv 1 \bmod 2^\ell$ για όλα τα $\ell \geq 4$. Συνεπώς $\mathrm{ord}_{2^\ell} \mid 2^{\ell-3}$, $\mathrm{ord}_{2^\ell}(a) < 2^{\ell-2}$, άτοπο.

(2) $\Rightarrow$ (1) Υποθέτουμε ότι ισχύει $a \equiv \pm 3 \bmod 8$. Θα αποδείξουμε επαγωγικά, ότι για κάθε $k \geq 1$ ισχύει

$$a^{2^k} - 1 = 2^{k+2} \cdot b, \quad (b \text{ περιττός}).$$

Πράγματι για $k = 1$, $8 \| a^2 - 1$, δηλαδή ισχύει.

Υποθέτουμε ότι ισχύει για $k \geq 1$. Γράφουμε

$$a^{2^k} + 1 = \left(2^{k+2} b + 1\right) + 1 = 2^{k+2} b + 2 = 2(1 + 2^{k+1} b).$$

Ο $1 + 2^{k+1} b$ είναι περιττός. Επομένως

$$a^{2^{k+1}} - 1 = \left(a^{2^k} - 1\right)\left(a^{2^k} + 1\right) = 2^{k+2} b \cdot 2\left(1 + 2^{k+1}\right) = 2^{k+3} b',$$

όπου b' περιττός. Σύμφωνα με την απόδειξη της πρότασης 5.2.26 ισχύει

$$a^{2^{\ell-2}} \equiv 1 \bmod 2^\ell$$

για κάθε $\ell \geq 3$. Επομένως $\mathrm{ord}_{2^\ell}(a) = 2^t$ με $t \leq \ell - 2$ και αυτό ισχύει για όλα τα $\ell \geq 3$.

Αυτό σημαίνει ότι $a^{2^t} \equiv 1 \bmod 2^\ell$, δηλαδή ότι $2^\ell \mid a^{2^t} - 1$. Όμως $a^{2^t} - 1 = 2^{t+2} \cdot s$, όπου s περιττός. Επομένως $\ell \leq t + 2$, $\ell - 2 \leq t$. Επειδή $a^{2^{\ell-2}} \equiv 1 \bmod 2^\ell$ έπεται ότι $t = \ell - 2$, $\ell \geq 3$. □

Πρόταση 5.4.31. *Για κάθε ακέραιο $\ell \geq 3$ και $a \equiv \pm 3 \bmod 8$, το σύνολο*

$$\{a, a^2, \ldots, a^{2^{\ell-2}}, -a, -a^2, \ldots, -a^{2^{\ell-2}}\},$$

αποτελεί ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων $\bmod 2^\ell$.

Απόδειξη. Το σύνολο αυτό αποτελείται από $\varphi(2^\ell) = 2^{\ell-1}$ το πλήθος ακέραιων πρώτων προς τον 2^ℓ.

Επομένως αρκεί να αποδείξουμε ότι είναι ανά δύο ανισοϋπόλοιποι $\bmod 2^\ell$. Σύμφωνα με την πρόταση 5.4.30, οι πρώτοι $2^{\ell-2}$ είναι ανά δύο ανισοϋπόλοιποι $\bmod 2^\ell$. Θα αποδείξουμε ότι και οποιοσδήποτε από τους πρώτους $2^{\ell-2}$ είναι ανισοϋπόλοιπος με κάθε έναν από τους δεύτερους. Πράγματι, αν

$$a^i \equiv -a^j \bmod 2^\ell$$

για κάποια $1 \leq i, j \leq 2^{\ell-2}$ και υποθέσουμε ότι $j \leq i$, έχουμε

$$a^{i-j} \equiv -1 \bmod 2^\ell.$$

Επομένως

$$a^{2(i-j)} \equiv 1 \bmod 2^{\ell+1}.$$

Όμως (πρόταση 5.4.30), έχουμε $\mathrm{ord}_{2^{\ell+1}}(a) = 2^{\ell-1}$. Άρα $2^{\ell-1} \mid 2(i-j)$, δηλαδή $2^{\ell-2} \mid (i-j)$. Επειδή $0 \leq i - j < 2^{\ell-2}$ θα πρέπει $i = j$. Τότε όμως θα είχαμε

$$a^i \equiv -a^i \bmod 2^\ell$$

και επειδή $(a^i, 2^\ell) = 1$ έχουμε $1 \equiv -1 \bmod 2^\ell$, το οποίο δεν ισχύει αφού $\ell \geq 3$. □

Πόρισμα 5.4.32. *Όταν δοθεί οποιοσδήποτε ακέραιος ℓ, $\ell \geq 3$ και οποιοσδήποτε ακέραιος a, $a \equiv \pm 3 \bmod 8$, τότε για κάθε περιττό ακέραιο b, υπάρχουν δύο θετικοί ακέραιοι s, t ορισμένοι* $\bmod 2$ *και* $\bmod 2^{\ell-2}$ *αντίστοιχα τέτοιοι ώστε να ισχύει:*

$$b \equiv (-1)^s a^t \bmod 2^\ell$$

Παρατήρηση 5.4.33. Συνήθως επιλέγουμε $a = 5$. Είναι φανερό ότι αν $b \equiv 1 \bmod 4$ τότε $b \equiv 5^t \bmod 2^\ell$, για κάποιο $t \in \{0, 1, \ldots, 2^{\ell-2} - 1\}$, ενώ αν $b \equiv 3 \bmod 4$, τότε $b \equiv -5^t \bmod 2^\ell$, για κάποιο $t \in \{0, 1, \ldots, 2^{\ell-2} - 1\}$.

Είμαστε πλέον σε θέση να μελετήσουμε n-στά υπόλοιπα $\bmod 2^\ell$, $\ell \geq 3$, αφού έχουμε ήδη στα χέρια μας κάτι «ανάλογο» των αρχικών ριζών.

Πρόταση 5.4.34. *Υποθέτουμε ότι ο $\ell \geq 3$ και ο a περιττός. Αν ο n είναι περιττός φυσικός αριθμός τότε η ισοτιμία*

$$x^n \equiv a \bmod 2^\ell$$

έχει πάντοτε λύση η οποία είναι μοναδική. Αν ο n είναι άρτιος φυσικός αριθμός τότε η ισοτιμία

$$x^n \equiv a \bmod 2^\ell$$

είναι επιλύσιμη ακριβώς τότε όταν

$$a \equiv 1 \bmod 2^{k+2}$$

όπου το k ορίζεται από τη σχέση $2^k = (n, 2^\ell)$. Μάλιστα, όταν είναι επιλύσιμη, το πλήθος των λύσεων είναι 2^{k+1}.

Απόδειξη. Σύμφωνα με το πόρισμα 5.4.32 υπάρχουν ακέραιοι s, t τέτοιοι ώστε

$$a \equiv (-1)^s 5^t \mathrm{mod} 2^\ell$$

Αν x λύση της ισοτιμίας $x^n \equiv a \mathrm{mod} 2^\ell$, τότε ο x είναι περιττός. Επομένως, πάλι σύμφωνα με το πόρισμα 5.4.32 ισχύει

$$x \equiv (-1)^u 5^v \mathrm{mod} 2^\ell$$

Η ισοτιμία παίρνει την ακόλουθη μορφή

$$(-1)^{nu} 5^{nv} \equiv (-1)^s 5^t \mathrm{mod} 2^\ell.$$

Παρατηρούμε ότι η τελευταία ισοτιμία είναι ισοδύναμη προς την $nu \equiv s \mathrm{mod} 2$ και $nv \equiv t \mathrm{mod} 2^{\ell-2}$.

Αν ο n είναι περιττός, τότε η ισοτιμία $nu \equiv s \mathrm{mod} 2$ έχει ως προς u, μοναδική mod2 λύση καθώς και η $nv \equiv t \mathrm{mod} 2^{\ell-2}$ έχει επίσης μοναδική $\mathrm{mod} 2^{\ell-2}$ λύση. Επομένως υπάρχει ακριβώς μία λύση της αρχικής ισοτιμίας.

Αν τώρα ο n είναι άρτιος και $s \equiv 0 \mathrm{mod} 2$ η ισοτιμία $nu \equiv s \mathrm{mod} 2$ έχει δύο λύσεις. Αν $s \not\equiv 0 \mathrm{mod} 2$, τότε δεν έχει καμμία. Αν τώρα $t \equiv 0 \mathrm{mod} 2^k$, η ισοτιμία $nv \equiv t \mathrm{mod} 2^{\ell-2}$ έχει ακριβώς 2^k λύσεις, αφού $(n, 2^{\ell-2}) = 2^k | t$. Αλλιώς δεν έχει καμμία λύση.

Επομένως η ισοτιμία, έχει ακριβώς 2^k λύσεις όταν

$$\begin{aligned} a &\equiv 5^t \mathrm{mod} 2^\ell \\ t &\equiv 0 \mathrm{mod} 2^k \end{aligned}$$

και καμία αν δεν ισχύουν οι παραπάνω ισοτιμίες.

Από την πρόταση 5.4.31 προκύπτει το $\mathrm{ord}_{2^{k+2}}(5) = 2^k$. Επομένως $5^t \equiv 1 \mathrm{mod} 2^{k+2}$ αν και μόνο αν $2^k \mid t$. Επειδή $2^{k+2} \mid 2^\ell$ η συνθήκη επιλυσιμότητας είναι $a \equiv 1 \mathrm{mod}^{2^{k+2}}$. □

5.4.2 Δείκτες

Υποθέτουμε ότι για τον φυσικό m, $m \geq 2$, υπάρχει αρχική ρίζα $g \mathrm{mod} m$. Αν $a \in \mathbb{Z}$ με $(a, m) = 1$, τότε υπάρχει μοναδικός ακέραιος ℓ $(0 \leq \ell < \phi(m))$ ώστε

$$a = g^\ell.$$

Ορισμός 5.4.35. Ο εκθέτης ℓ θα λέγεται δείκτης του a ως προς τη βάση $g \mathrm{mod} m$ και θα συμβολίζεται με $I_g(a)$. Όταν αναφερόμαστε ρητά σε συγκεκριμένη αρχική ρίζα g, τότε γράφουμε απλά $I(a)$.

Από τον ορισμό προκύπτει αμέσως

$$a \equiv g^{I_g(a)} \mathrm{mod} m$$

Παράδειγμα. Ας πάρουμε $m = 19$. Από τον παρακάτω πίνακα φαίνεται ότι $g = 2$ είναι αρχική ρίζα mod19.

- Το $I(3) = 13$ αφού $2^{13} \equiv 3 \mathrm{mod} 19$
- $I(4) = 2$ αφού $2^2 \equiv 4 \mathrm{mod} 19$

- $I(5) = 16$ αφού $2^{16} \equiv 5 \mathrm{mod} 19$
- $I(7) = 6$ αφού $2^6 \equiv 7 \mathrm{mod} 19$

Είναι προτιμότερο να φτιάξουμε δύο πίνακες

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$I(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

και

$I(a)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Έτσι τώρα είναι εύκολο να βρούμε τον δείκτη $I(8) = 3, I(14) = 7$ ή αν μας δοθεί ο δείκτης να βρούμε το a. Αν $I(a) = 12$, τότε

$$a = 2^{12} \equiv 11 \mathrm{mod} 19$$

Άμεση συνέπεια του ορισμού είναι ότι

$$I(1) = 0 \;\; I(g) = 1.$$

Επίσης αν $a, b \in \mathbb{Z}$ με $(a, m) = (b, m) = 1$ τότε

$$a \equiv b \mathrm{mod} m \Leftrightarrow g^{I(a)} = g^{I(b)} \mathrm{mod} m$$

και σύμφωνα με την πρόταση 5.4.5 το τελευταίο είναι ισοδύναμο με

$$I(a) \equiv I(b) \mathrm{mod} \phi(m) \Leftrightarrow I(a) = I(b).$$

Η τελευταία ισοδυναμία ισχύει διότι $0 \leq I(a), I(b) \leq \phi(m) - 1$. Βλέπουμε δηλαδή ότι ο δείκτης $I(a)$ είναι αναλλοίωτος της πρώτης κλάσης υπολοίπων $a \mathrm{mod} m$ και όχι του ακέραιου a.

Στη συνέχεια θα αναφερθούμε σε μερικές ιδιότητες του δείκτη. Είναι ανάλογες με αυτές των λογαρίθμων με μόνη διαφορά ότι στους δείκτες η ισότητα έχει αντικατασταθεί από ισοτιμία $\mathrm{mod} \phi(m)$.

Πρόταση 5.4.36. *Αν g μία αρχική ρίζα $\mathrm{mod} m$, $a, b \in \mathbb{Z}$ με $(a, m) = (b, m) = 1$ και $n \in \mathbb{Z}$, $n \geq 1$, τότε*

1. $I(ab) \equiv I(a) + I(b) \mathrm{mod} \phi(m)$ *(κανόνας του γινομένου)*
2. $I(a^n) \equiv nI(a) \mathrm{mod} \phi(m)$ *(κανόνας της δύναμης)*
3. *Αν g' επίσης αρχική ρίζα $\mathrm{mod} m$, τότε (κανόνας αλλαγής βάσης)*

$$I_g(a) \equiv I_g(g') I_{g'}(a) \mathrm{mod} \phi(m)$$

4. $I(-1) = \frac{\phi(m)}{2}$, *για $m > 2$.*

Απόδειξη. Για το πρώτο: $a \equiv g^{I(a)} \mathrm{mod} m$, $b \equiv g^{I(b)} \mathrm{mod} m$ και

$$ab \equiv g^{I(a)+I(b)} \mathrm{mod} m$$

Επίσης $ab \equiv g^{I(ab)} \mathrm{mod} m$.

Επομένως

$$g^{I(ab)} \equiv g^{I(a)+I(b)} \mathrm{mod} m,$$

και η πρόταση 5.4.5 είναι ισοδύναμη με την

$$I(ab) \equiv I(a) + I(b) \mathrm{mod} \phi(m)$$

Σημείωση: Το (1) γενικεύεται επαγωγικά για πεπερασμένο πλήθος προσθετέων.

Το (2) μπορεί να αποδειχτεί με επαγωγή από το (1):

$$I(a^n) = I(a) + \cdots I(a) \equiv nI(a) \mathrm{mod} \phi(m).$$

Για το (3). Από τον ορισμό του δείκτη έπεται ότι

$$a \equiv g^{I_g(a)} \mathrm{mod} m, \quad a \equiv g'^{I_{g'}(a)} \mathrm{mod} m$$

και αφού $g' \equiv g^{I_g(g')} \mathrm{mod} m$ έχουμε

$$I_g(a) \equiv a \equiv g^{I_g(g')I_{g'}(a)} \mathrm{mod} m$$

Η τελευταία ισοτιμία είναι ισοδύναμη (πρόταση 5.4.5) προς την

$$I_g(a) \equiv I_g(g')I_{g'}(a) \mathrm{mod} \phi(m)$$

Για το (4) Για $m > 2$ ο $\phi(m)$ είναι άρτιος. Αν $m = 4$ έχουμε $g = 3$ και $\phi(m) = 2$. Επομένως, $I(-1) = I(3) = 1 = \phi(4)/2$ και ισχύει.

Αν $m = p^\ell$, $p \geq 3$ τότε

$$\left(g^{\frac{\phi(m)}{2}} + 1\right)\left(g^{\frac{\phi(m)}{2}} - 1\right) = g^{\phi(m)} - 1 \equiv 0 \mathrm{mod} m.$$

Επομένως

$$\left(g^{\frac{\phi(m)}{2}} + 1\right)\left(g^{\frac{\phi(m)}{2}} - 1\right) \equiv 0 \mathrm{mod} p$$

Ο p δεν μπορεί να διαιρεί και τους δύο παράγοντες, διότι θα είχαμε $p \mid 2$ και αυτό είναι αδύνατο αφού $p \geq 3$. Επομένως και το $m = p^\ell$ θα διαιρεί ακριβώς έναν από τους δυο. Επειδή g αρχική ρίζα $\mathrm{mod} m$ θα έχουμε

$$g^{\frac{\phi(m)}{2}} + 1 \equiv 0 \mathrm{mod} m \Rightarrow g^{\frac{\phi(m)}{2}} \equiv -1 \mathrm{mod} m$$

και συνεπώς $I(-1) = \phi(m)/2$.

Τέλος αν $m = 2p^\ell$, $p \geq 3$, τότε ισχύει και πάλι η ισοτιμία

$$\left(g^{\frac{\phi(m)}{2}} + 1\right)\left(g^{\frac{\phi(m)}{2}} - 1\right) \equiv 0 \mathrm{mod} m.$$

Αφού ο g είναι περιττός (ισχύει $(g, m) = (a, m) = 1$), έπεται ότι οι $g^{\frac{\phi(m)}{2}} + 1$ και $g^{\frac{\phi(m)}{2}} - 1$ είναι αμφότεροι άρτιοι. Όπως και στην περίπτωση $m - p^\ell$, ο p^ℓ διαιρεί ακριβώς έναν από τους δύο παράγοντες $g^{\frac{\phi(m)}{2}} + 1$ και $g^{\frac{\phi(m)}{2}} - 1$. Ο g είναι αρχική ρίζα $\mathrm{mod} m$. Άρα,

$$g^{\frac{\phi(m)}{2}} + 1 \equiv 0 \mathrm{mod} m \Rightarrow g^{\frac{\phi(m)}{2}} \equiv -1 \mathrm{mod} m$$

Συνεπώς και στην περίπτωση $m = 2p^\ell$ ισχύει $I(-1) = \phi(m)/2$. □

Πόρισμα 5.4.37. 1. $a^n \equiv 1 \bmod m \Leftrightarrow nI(a) \equiv 0 \bmod \phi(m)$

2. $I_g(g')I_{g'}(g) \equiv 1 \bmod \phi(m)$

3. $I(m-a) \equiv I(-a) \equiv \frac{\phi(m)}{2} + I(a) \bmod \phi(m)$

Απόδειξη. Για το πρώτο. Έχουμε

$$a \equiv g^{I(a)} \bmod m$$

επομένως η $a^n \equiv 1 \bmod m$ είναι ισοδύναμη προς την $g^{nI(a)} \equiv g^0 \bmod m$. Σύμφωνα με την πρόταση 5.4.5 η τελευταία είναι ισοδύναμη προς την

$$nI(a) \equiv 0 \bmod \phi(m)$$

Για το (2) παρατηρούμε ότι το (3) της πρότασης 5.4.36 δίνει αμέσως

$$I_g(g')I_{g'}(g) = I_g(g) \equiv 1 \bmod \phi(m).$$

Για το (3) έχουμε $m - a \equiv g^{I(m-a)} \bmod m$ το οποίο μας δίνει ότι $(-1)a \equiv g^{I(m-a)} \bmod m$ δηλαδή

$$g^{\frac{\phi(m)}{2}+I(a)} \equiv g^{I(m-a)} \bmod m$$

από όπου καταλήγουμε ότι

$$I(m-a) \equiv \frac{\phi(m)}{2} + I(a) \bmod \phi(m)$$

□

Τώρα θα επιστρέψουμε για λίγο στο θεώρημα 5.4.29. Υπάρχει ακόμα μία ισοδύναμη έκφραση του πρώτου μέρους του. Συγκεκριμένα ισχύει:

Πρόταση 5.4.38. *Η ισοτιμία*

$$x^n \equiv a \bmod m$$

είναι επιλύσιμη ακριβώς τότε όταν $d \mid I(a)$, όπου $d = (n, \phi(m))$.

Απόδειξη. Από το θεώρημα 5.4.29 η ισοτιμία είναι επιλύσιμη αν και μόνο αν

$$a^{\frac{\phi(m)}{d}} \equiv 1 \bmod m$$

το πόρισμα 5.4.37 μας δίνει ότι

$$\frac{\phi(m)}{d} \cdot I(a) \equiv 0 \bmod \phi(m) \Leftrightarrow \phi(m) \mid \frac{\phi(m)I(a)}{d}$$

και το τελευταίο ισχύει αν και μόνο αν $d \mid I(a)$. □

Τέλος επιστρέφουμε στα τετραγωνικά υπόλοιπα και αποδεικνύουμε:

Πρόταση 5.4.39. *Αν p περιττός πρώτος και $a \in \mathbb{Z}$ με $p \nmid a$, τότε ο a είναι τετραγωνικό υπόλοιπο* $\bmod p$ *ακριβώς τότε όταν $I(a) \equiv 0 \bmod 2$.*

Απόδειξη. Αν ο a είναι τετραγωνικό υπόλοιπο mod$p$ τότε υπάρχει ακέραιος x_0 για τον οποίο ισχύει $x_0^2 \equiv a \mathrm{mod} p$. Επομένως από την πρόταση 5.4.36.2 η παραπάνω ισοτιμία είναι ισοδύναμη προς την

$$2I(x_0) \equiv I(a) \mathrm{mod}(p-1).$$

Επειδή ο $p-1$ είναι άρτιος, κατάνάγκη και ο $I(a)$ θα πρέπει να είναι άρτιος.

Αντιστρόφως υποθέτουμε ότι ο $I(a)$ είναι άρτιος, $I(a) = 2s$, $s \in \mathbb{Z}$. Η ισοτιμία

$$a = g^{I(a)} \mathrm{mod} p$$

γράφεται

$$(g^s)^2 \equiv a \mathrm{mod} p$$

Συνεπώς ο a είναι τετραγωνικό υπόλοιπο mod$p$, αφού η ισοτιμία $x^2 \equiv a \mathrm{mod} p$, έχει λύση $x_0 = g^s$. □

Παρατήρηση 5.4.40. Άμεση συνέπεια της πρότασης 5.4.39 είναι ότι καμμία αρχική ρίζα mod$p$ δεν είναι τετραγωνικό υπόλοιπο mod$p$.

Παρατήρηση 5.4.41. Ανάλογη πρόταση της 5.4.39 για $n \geq 3$ δεν ισχύει. Πράγματι για $p = 5$ και $n = 3$ έχουμε δύο μόνο δείκτες οι οποίοι διαιρούνται με 3 (για αρχική ρίζα mod$p$ πήραμε το $g = 2$), ενώ κάθε ένας από τους $1, 2, 3, 4$ είναι κυβικό υπόλοιπο mod5, αφού

$$1 \equiv 1 \mathrm{mod} 5, 2 \equiv 3^3 \mathrm{mod} 5, 3 \equiv 2^3 \mathrm{mod} 5, 4 \equiv 4^3 \mathrm{mod} 5$$

Εφαρμογές της θεωρίας των δεικτών στην εύρεση λύσεων κάποιων κλάσεων ισοτιμιών.

Γραμμικές Ισοτιμίες

Υποθέτουμε ότι το m έχει αρχική ρίζα και $a, b \in \mathbb{Z}$ με $(a, m) = (b, m) = 1$. Η γραμμική ισοτιμία

$$ax \equiv b \mathrm{mod} m$$

είναι ισοδύναμη με την

$$I(a) + I(x) \equiv I(b) \mathrm{mod} \phi(m)$$

Επομένως

$$I(x) \equiv I(b) - I(a) \mathrm{mod} \phi(m).$$

Παράδειγμα. Να λυθεί η ισοτιμία

$$5x \equiv 12 \mathrm{mod} 19$$

Η ισοτιμία δεικτών είναι η

$$I(x) \equiv I(12) - I(5) \mathrm{mod} 18$$

Υπολογίζουμε ότι $I(12) = 15$, $I(5) = 16$, επομένως $I(x) = -1 \equiv 17 \mathrm{mod} 18$ και συνεπώς $x \equiv 10 \mathrm{mod} 19$.

5.4.3 Διωνυμικές ισοτιμίες

Υποθέτουμε ότι ο m έχει αρχική ρίζα και ότι $a, b \in \mathbb{Z}$ με $(a, m) = (b, m) = 1$. Η ισοτιμία

$$ax^n \equiv b \bmod m$$

είναι ισοδύναμη προς την

$$I(a) + nI(x) \equiv I(b) \bmod \phi(m)$$

Επομένως έχουμε

$$nI(x) \equiv I(b) - I(a) \bmod \phi(m)$$

Η γραμμική ισοτιμία έχει λύση ακριβώς τότε όταν ο $d = (n, \phi(m)) \mid (I(b) - I(a))$. Αν πληρούται η τελευταία συνθήκη, τότε έχουμε ακριβώς d-λύσεις.

5.4.4 Εκθετικές ισοτιμίες

Υποθέτουμε ότι ο m έχει αρχικές ρίζες $a, b \in \mathbb{Z}$ και $(a, m) = (b, m) = 1$. Η ισοτιμία

$$a^x \equiv b \bmod m$$

είναι ισοδύναμη με την ισοτιμία δεικτών

$$xI(a) \equiv I(b) \bmod \phi(m)$$

Επομένως ικανή και αναγκαία συνθήκη για να έχει λύση η εκθετική ισοτιμία είναι $(I(a), \phi(m) \mid I(b)$. Αν η τελευταία συνθήκη ισχύει τότε η εκθετική ισοτιμία έχει ακριβώς $(I(a), \phi(m))$ το πλήθος λύσεις.

5.4.5 Υπολογισμός της τάξης a mod m, όταν (a,m)=1.

Έστω $s := \mathrm{ord}_m(a)$. Έστω $a^s \equiv 1 \bmod m$ και $a^t \not\equiv 1 \bmod m$ για κάθε t, $0 < t < s$. Από την ισοτιμία

$$a^s \equiv 1 \bmod m$$

προκύπτει η ισοδύναμη ισοτιμία δεικτών

$$sI(a) \equiv 0 \bmod \phi(m)$$

Αν $d := (I(a), \phi(m))$, τότε $s \equiv 0 \bmod \frac{\phi(m)}{d}$. Επομένως $s = \frac{\phi(m)}{d}$, αφού ο s είναι ο μικρότερος φυσικός με αυτή την ιδιότητα. Μπορούμε να κάνουμε χρήση του πορίσματος 5.4.37.2 και να αποδείξουμε ότι δεν έχει σημασία ποια αρχική ρίζα $\bmod m$ έχουμε επιλέξει. Είναι φανερό λοιπόν από το πόρισμα ότι

$$(I_g(g'), \phi(m)) = (I_{g'}(g), \phi(m)) = 1.$$

Επομένως

$$(I_g(a), \phi(m)) = (I_g(g')I'_g(a), \phi(m)) = (I_{g'}(a), \phi(m)).$$

Παράδειγμα. Να υπολογιστεί η τάξη του $3 \bmod 25$. Το $g = 2$ είναι αρχική ρίζα $\bmod 5$. Επειδή $2^4 - 1 = 15 = 5 \cdot 3$ με $5 \nmid 3$. Από το θεώρημα 5.4.23 έπεται ότι το 2 είναι και αρχική ρίζα $\bmod 25$. Το $a = 3$, $I_2(3) = 7$, $d = (I_2(3), \phi(25)) = (7, 40) = 1$. Επομένως $s = \mathrm{ord}_{25}(3) = 40$. Αν $a = 7$ $I_2(7) = 5$, $(5, 40) = 8$, συνεπώς $s = 40/8 = 5$.

Παρατήρηση 5.4.42. Παρά την κάποια πρακτική τους χρησιμότητα οι δείκτες έχουν δύο σοβαρά μειονεκτήματα. Το πρώτο είναι ότι «λειτουργεί» μόνο για τα m για τα οποία υπάρχει αρχική ρίζα $\mathrm{mod}m$.

Το δεύτερο είναι ότι είναι εξαιρετικά δύσκολο για μεγάλα m, να βρούμε τον δείκτη του a ως προς την αρχική ρίζα g. Το πρόβλημα αυτό θα το εξετάσουμε στην επόμενη παράγραφο.

Επιστρέφουμε στην πρόταση 4.8.6 η οποία χαρακτηρίζει τους αριθμούς Carmichael και θα αποδείξουμε την κατεύθυνση που αφήσαμε χωρίς απόδειξη. Για τον σκοπό μας αυτό θα ορίσουμε τη συνάρτηση λ που ορίσθηκε για πρώτη φορά από τον Carmichael.

Η συνάρτηση λ ορίζεται για κάθε ακέραιο $a \in \mathbb{Z}$, $a \geq 1$.

$$\begin{aligned} \lambda(1) &= 1, \\ \lambda(p^\ell) &= \varphi(p^\ell), \text{ όταν } p \in \mathbb{P}, p \geq 3, \ell \geq 1 \\ \lambda(2^\ell) &= \begin{cases} \varphi(2^\ell) & \text{όταν } \ell = 1 \text{ ή } 2 \\ \frac{1}{2}\varphi(2^\ell), & \text{όταν } \ell \geq 3 \end{cases} \end{aligned}$$

Επιπλέον αν $m = 2^\ell p_1^{\ell_1} p_2^{\ell_2} \cdots p_s^{\ell_s}$, τότε

$$\lambda(m) = [\lambda(2^\ell), \lambda(p_1^{\ell_1}), \ldots, \lambda(p_s^{\ell_s})].$$

Συχνά λέγεται και universal εκθέτης modulo m. Ο λόγος της ονομασίας οφείλεται στην ακόλουθη ιδιότητα:

Πρόταση 5.4.43. *Αν $m \in \mathbb{Z}$, $m \geq 2$, τότε ο $\lambda(m)$ είναι ο ελάχιστος φυσικός ≥ 1 με την ιδιότητα*

$$a^{\lambda(m)} \equiv 1 \mathrm{mod} m$$

για κάθε ακέραιο a πρώτο προς τον m. Επιπλέον, για κάθε m υπάρχει ακέραιος a του οποίου η τάξη $\mathrm{mod}m$ είναι $\lambda(m)$ και αυτή είναι μεγαλύτερη δυνατή τάξη ενός ακέραιου $\mathrm{mod}m$.

Απόδειξη. Υποθέτουμε ότι $m = 2^\ell p_1^{\ell_1} p_2^{\ell_2} \cdots p_s^{\ell_s}$ $\ell \in \mathbb{N}$ $\ell \geq 1$ είναι η κανονική ανάλυση του m σε γινόμενο πρώτων παραγόντων.

Για κάθε $i = 1, 2, \ldots, s$ η συνάρτηση $\lambda(p_i^{\ell_i})$ είναι εξ ορισμού ίση με $\varphi(p_i^{\ell_i})$. Επομένως σύμφωνα με το θεώρημα του Euler έχουμε

$$a^{\lambda(p_i^{\ell_i})} \equiv 1 \mathrm{mod} p_i^{\ell_i}$$

για κάθε $i = 1, 2, \ldots, s$. Επειδή $\lambda(p_i^{\ell_i}) \mid \lambda(m)$, έπεται ότι

$$a^{\lambda(m)} \equiv 1 \mathrm{mod} p_i^{\ell_i}, \tag{5.4.4}$$

για κάθε $i = 1, 2, \ldots, s$.

Αν τώρα ο m είναι άρτιος, ο a θα είναι περιττός αφού $(a, m) = 1$. Η ισοτιμία $a \equiv 1 \mathrm{mod} 2$ γράφεται

$$a^{\lambda(2)} \equiv 1 \mathrm{mod} 2.$$

Επίσης, αφού a περιττός έχουμε

$$a^2 \equiv 1 \mathrm{mod} 4$$

η οποία γράφεται

$$a^{\lambda(4)} \equiv 1 \mathrm{mod} 4$$

Τέλος, για κάθε $\ell \geq 3$ ισχύει (απόδειξη της 5.4.19)

$$a^{\lambda(2^\ell)} \equiv 1 \bmod 2^\ell$$

Καταλήγουμε ότι

$$a^{\lambda(2^\ell)} \equiv 1 \bmod 2^\ell$$

για κάθε $\ell \geq 1$. Επειδή $\lambda(2^\ell) \mid \lambda(m)$, έπεται ότι

$$a^{\lambda(m)} \equiv 1 \bmod 2^\ell \tag{5.4.5}$$

Από τις (5.4.4), (5.4.5) έπεται ότι

$$a^{\lambda(m)} \equiv 1 \bmod m$$

για κάθε ακέραιο a πρώτο προς τον m.

Θα αποδείξουμε ότι $\lambda(m)$ είναι ο ελάχιστος με αυτή την ιδιότητα. Θα βρούμε ακέραιο a του οποίου κάθε δύναμη μικρότερη του $\lambda(m)$ είναι $\not\equiv 1 \bmod m$. Αυτό βέβαια σημαίνει και ότι αρκεί να δείξουμε

$$\mathrm{ord}_m(a) = \lambda(m)$$

και έτσι η απόδειξη θα έχει τελειώσει.

Έστω g_i αρχική ρίζα $\bmod p_i^{\ell_i}$, $i = 1, 2, \ldots, s$. Θεωρούμε το σύστημα

$$\begin{aligned} x &\equiv 3 \bmod 2^\ell \\ x &\equiv g_1 \bmod p_1^{\ell_1} \\ \ldots &\quad \ldots \\ x &\equiv g_s \bmod p_s^{\ell_s} \end{aligned}$$

Το παραπάνω σύστημα σύμφωνα με το θεώρημα υπολοίπων του Κινέζου έχει μοναδική λύση $\bmod m$. Αν $a \in \mathbb{Z}$, λύση του συστήματος θα αποδείξουμε ότι $\mathrm{ord}_m(a) = \lambda(m)$.

Αν $n \in \mathbb{N}$, $n \geq 1$ τέτοιος ώστε

$$a^n \equiv 1 \bmod m$$

θα έχουμε και

$$a^n \equiv 1 \bmod p_i^{\ell_i}$$

για $i = 1, 2, \ldots, s$ καθώς και

$$a^n \equiv 1 \bmod 2^\ell$$

Όμως ο a είναι λύση του συστήματος. Επομένως $a \equiv g_i \bmod p_i^{\ell_i}$, για $i = 1, 2, \ldots, s$. Από αυτό έπεται ότι

$$\mathrm{ord}_{p_i^{\ell_i}}(a) = \mathrm{ord}_{p_i^{\ell_i}}(g_i) = \varphi(p_i^{\ell_i}) = \lambda(p_i^{\ell_i}),$$

για κάθε $i = 1, 2, \ldots, s$. Συνεπώς

$$\lambda(p_i^{\ell_i}) \mid n \tag{5.4.6}$$

για κάθε $i = 1, 2, \ldots, s$. Επίσης, επειδή $a \equiv 3 \bmod 2^\ell$ έχουμε

$$\mathrm{ord}_{2^\ell}(a) = \mathrm{ord}_{2^\ell}(3) = 2^{\ell-2} = \varphi(2^\ell)/2 = \lambda(2^\ell).$$

Για $\ell = 1$, $a \equiv 3 \equiv 1 \bmod 2$ συνεπώς $\mathrm{ord}_2(a) = \mathrm{ord}_2(5) = 1 = \varphi(2) = \lambda(2)$ και για $\ell = 2$ $a^2 \equiv 3^2 \equiv 1 \bmod 4$ συνεπώς $\mathrm{ord}_4(a) = \mathrm{ord}_4(3) = 2 = \varphi(4) = \lambda(4)$.

Επομένως και

$$\lambda(2^{\ell}) \mid n. \tag{5.4.7}$$

Από τις σχέσεις (5.4.6) και (5.4.7) συνεπάγεται ότι

$$\lambda(m) = [\lambda(2^{\ell}), \lambda(p_1^{\ell_1}), \ldots, \lambda(p_s^{\ell_s})] \mid n \tag{5.4.8}$$

Αν τώρα $n := \mathrm{ord}_m(a)$ θα είχαμε και

$$n \mid \lambda(m). \tag{5.4.9}$$

Από τις (5.4.8) και (5.4.9) έχουμε ότι $\lambda(m) = \mathrm{ord}_m(a)$. □

Είμαστε πλέον σε θέση να αποδείξουμε το αντίστροφο της πρότασης 4.8.6.

Πρόταση 5.4.44. *Αν ο φυσικός αριθμός m, $m > 2$ είναι αριθμός Carmichael τότε ο $m = p_1 p_2 \cdots p_s$, με διακεκριμένους μεταξύ τους ανά δύο πρώτους αριθμούς και $(p_j - 1) \mid (m-1)$ για κάθε $j = 1, 2, \ldots, s$.*

Απόδειξη. Λόγω του ορισμού του αριθμού Carmichael έχουμε ότι

$$b^{m-1} \equiv 1 \mathrm{mod} m,$$

για κάθε ακέραιο b με $(b, m) = 1$. Από την πρόταση 5.4.43 έχουμε ότι, υπάρχει $a \in \mathbb{Z}$ τέτοιος ώστε $\mathrm{ord}_m(a) \equiv \lambda(m)$. Και για τον ακέραιο αυτόν ισχύει

$$a^{m-1} \equiv 1 \mathrm{mod} m.$$

Η πρόταση 5.4.3 μας δίνει $\lambda(m) \mid (m-1)$. Αν ο m ήταν άρτιος, ο $m-1$ θα ήταν περιττός. Αφού $m > 2$ ο $\lambda(m)$, από τον ορισμό του, είναι άρτιος. Αυτό όμως είναι αδύνατο. Επομένως ο m αναλύεται σε γινόμενο περιττών πρώτων. Θα αποδείξουμε ότι αναλύεται σε γινόμενο περιττών πρώτων διακεκριμένων μεταξύ τους.

Πράγματι, αν υποθέσουμε ότι υπάρχει περιττός πρώτος p, $p^{\ell} \mid m$, $\ell \geq 2$, τότε

$$\lambda(p^{\ell}) = \phi(p^{\ell}) = p^{\ell}(p-1) \mid (m-1).$$

Αυτό σημαίνει ότι $p \mid (m-1)$, αφού $\ell \geq 2$. Όμως έχουμε και $p \mid m$. Άρα $p \mid 1$, άτοπο.

Συνεπώς $m = p_1 p_2 \ldots p_s$, $p_i \neq 2$ για κάθε $i = 1, 2, \ldots, s$ και $p_i \neq p_j$ για κάθε $i \neq j$. Τελικά έχουμε

$$\lambda(p_i) = \phi(p_i) = p_i - 1 \mid \lambda(m) \mid (m-1).$$

□

Πρόταση 5.4.45. *Κάθε αριθμός Carmichael m διαιρείται από τουλάχιστον τρεις διακεκριμένους πρώτους.*

Απόδειξη. Εξ ορισμού ο m είναι σύνθετος. Αν ήταν $m = pq$, $p, q \in \mathbb{P}\backslash\{2\}$, $p \neq q$ και χωρίς βλάβη της γενικότητας υποθέσουμε ότι $p > q$ τότε

$$(p-1) \mid (m-1) = pq - 1 = (p-1)q + (q-1),$$

δηλαδή ο $(p-1) \mid (q-1)$, άτοπο αφού $p > q$. □

5.4.6 Παρατηρήσεις- Ιστορικά Σχόλια

1 Την ύπαρξη αρχικής ρίζας mod$p$, για κάθε περιττό πρώτο p (πρόταση 5.4.13 διατύπωσε για πρώτη φορά ο J.H. Lambert στα 1769. Ο Euler έδωσε στα 1773 μια απόδειξη η οποία όμως δεν ήταν πλήρης. Ήταν ο πρώτος ο οποίος χρησιμοποίησε τον όρο «αρχική ρίζα mod$p$».

Ο Gauss είναι ο πρώτος ο οποίος δίνει πλήρη απόδειξη στα *Disquisitiones Arithmeticae*, άρθρο 55. Μάλιστα γράφει

Da der Beweis dieses Satzes keineswegs so auf der Hand liegt, als es auf den ersten Anblick scheinen könnte, so wollen wir wegen der Bedeutung des Satzes noch einen andern von dem vorigen etwas verschiedenen Beweis anfügen, zumal die Verschiedenheit der Methoden gewöhnlich sehr viel zur Erläuterung etwas schwerer verständlicher Dinge beiträgt.

(Η απόδειξη του θεωρήματος αυτού δεν είναι καθόλου προαφανής, όπως θα μπορούσε να φανεί με την πρώτη ματιά. Γιάυτό, λόγω της σημασίας του θεωρήματος προτιθέμεθα να προσθέσουμε και μία διαφορετική από την προηγούμενη, απόδειξη μιας που η διαφορετικότητα των μεθόδων συμβάλλει συνήθως αρκετά στην επεξήγηση δύσκολα κατανοητών εννοιών.)

Στο τέλος της πρότασης 55 καταλήγει:

Der letztere Beweis scheint etwas weitläufiger als der erste, dieser aber dafür weniger direct zu sein als jener.

(Η τελευταία απόδειξη φαίνεται κάπως πιο εκτεταμένη από την πρώτη, η πρώτη όμως λιγότερο άμεση από την τελευταία).

Το άρθρο 57 έχει τον λατινικό τίτλο

Radics primitivae bases, indices «Αρχικές ρίζες, βάσεις, δείκτες».

Στην πρόταση 52, ορίζει την τάξη ενός στοιχείου

Irgent eine Zahl a welche zum Exponenten d gehört, d.h. deren $d$te Potenz den Einheit congruent ist, während alle niedrigeren Potenzen derselben nicht congruent sind

((Η τάξη στοιχείου) είναι κάποιος ακέραιος a τέτοιος ώστε να αναφέρεται στην d-στη δύναμη με την έννοια ότι η d-στή δύναμη αυτού να είναι ισότιμη προς το 1mod$n$ ενώ για όλες τις μικρότερες δυνάμεις του a να μην ισχύει η ισοτιμία).

και στην πρόταση 57 συνεχίζει

Die zum Exponenten $p-1$ gehörigen Zahlen werder wir mit Euler primitive Wurtzeln nennen

(Τους αριθμούς των οποίων η τάξη είναι $p-1$ θα τους ονομάζουμε, σύμφωνα και με τον Euler πρωταρχικές ρίζες).

Στη συνέχεια αναφέρεται στην ιδιότητα των αρχικών ριζών που αποδείξαμε στην πρόταση 5.4.9 και συνεχίζει

Deise ausgezeichnete Eigenschaft ist von dem grössten Nutzen und kann die arithmetischen auf die Congruenzen bezüglichen Operationen sehr erheblich erleichtern, etwa in derselben Weise, wie die Einführung der Logarithmen die Operationen der gemeinen Arithmetik

(Αυτή η εξαιρετική ιδιότητα είναι μεγάλης χρησιμότητας και μπορεί να διευκολύνει τα μάλα τις αριθμητικές πράξεις των ισοτιμιών κατά τον ίδιο τρόπο που το έχει κάνει η εισαγωγή των λογαρίθμων στις πράξεις κοινής αριθμητικής).

Στις προτάσεις 53,54 και 55 δίνει ουσιαστικά την απόδειξη της πρότασης 5.4.16.

Στην πρόταση 73 αναφέρει ότι δεν υπάρχει κάποια μέθοδος εύρεσης αρχικών ριζών mod$p$

Die Methoden, die primitiven Wurzeln zu finden, beruhen zum grossen Teil auf Vesuchen

Και ο Euler πίστευε το ίδιο.

Euler gesteht, daß es äusserst schwierig zu sein scheine, solche Zahlen zu finden und daß ihr eigentliches Wesen zu den tiefsten Geheimnissen der Zahlen zu rechnen sei.

(Και ο Euler συμφωνεί στο ότι φαίνεται ότι είναι εξαιρετικά δύσκολο να υπολογιστούν τέτοιοι αριθμοί και ότι η πραγματική τους ουσία λογίζεται στα βαθύτερα μυστικά των αριθμών).

συνεχίζει στην ίδια πρότασή του ο Gauss ο οποίος αναφέρεται σε εργασία του Euler του 1783, στην οποία δίνει ένα πίνακα όλων των αρχικών ριζών για κάθε πρώτο $p \leq 41$.

Ο Gauss συνεχίζει και στις επόμενες προτάσεις να ασχολείται με αρχικές ρίζες mod$m$. Ενδεικτικά αναφέρουμε ότι η πρόταση 5.4.19περιέχεται στην πρόταση 90. Στην πρόταση 92 καταλήγει στην πλήρη απόδειξη του θεωρήματος 5.4.23. Μερικοί το αποκαλούν και θεώρημα του Gauss [4].

5.4.7 Εφαρμογές

Μια γενίκευση του Θεωρήματος του Wilson

Πρόταση 5.4.46. *Αν S_m είναι ένα ανηγμένο πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων* mod$m$, $m \in \mathbb{N}$, $m > 2$, *τότε*

$$\prod_{a \in S_m} a \equiv \pm 1 \mathrm{mod} m$$

και μάλιστα είναι σε όλες τις περιπτώσεις $+1$mod$m$ *εκτός από αυτές με μέτρο* $m = 4, p^\ell, 2p^\ell$, *όπου* $p \in \mathbb{P} - \{2\}$ *και* $\ell \geq 1$, *στις οποίες είναι* -1mod$m$.

Απόδειξη. Η ιδέα της απόδειξης αποτελεί συνδυασμό της ιδέας απόδειξης του κλασικού θεωρήματος του Wilson με το αποτέλεσμα της πρότασης 5.3.4. Όταν δοθεί κάποιο $a \in S_m$, τότε υπάρχει πάντοτε (αφού $(a, m) = 1$) ακριβώς ένα $b \in S_m$ τέτοιο ώστε

$$ab \equiv 1 \mathrm{mod} m$$

Επομένως χωρίζουμε το σύνολο S_m σε ζευγάρια και ξεχωρίζουμε δύο περιπτώσεις. Αν $a \neq b$, τότε μπορούμε να μην τους λάβουμε υπόψη αφού το γινόμενό τους είναι 1mod$m$. Συνεπώς θα πρέπει να μελετήσουμε ζευγάρια (a, b) για τα οποία $b = a$, δηλαδή τις λύσεις της ισοτιμίας

$$x^2 \equiv 1 \mathrm{mod} m$$

Αν τώρα a μια λύση της ισοτιμίας αυτής, τότε και ο $-a$ είναι επίσης λύση. Συνεπώς

$$a^2 \equiv -1 \mathrm{mod} m$$

Επειδή $m > 2$,

$$a \not\equiv -a \mathrm{mod} m$$

δηλαδή οι λύσεις είναι διαφορετικές mod$m$.

Από τα παραπάνω συνάγουμε ότι το αποτέλεσμα είναι $+1$mod$m$ όταν υπάρχει άρτιο πλήθος ζευγαριών λύσεων $(a, -a)$ της ισοτιμίας, δηλαδή όταν το πλήθος των λύσεων διαιρείται με 4.

Από την πρόταση 5.3.4 προκύπτει ότι το πλήθος των λύσεων δεν διαιρείται με 4 παρά μόνο όταν $m = 4, p^\ell, 2p^\ell$, $p \in \mathbb{P} - \{2\}$ και $\ell \geq 1$. □

Παρατηρήσεις

1. Για $m = p \in \mathbb{P} - \{2\}$, προκύπτει η ισοτιμία $(p-1)! \equiv -1$mod$p$, δηλαδή το θεώρημα του Wilson.

2. Σύμφωνα με την πρόταση 5.3.4 (για $m = 4, p^\ell, 2p^\ell$, όπου p περιττός πρώτος) για τις περιπτώσεις όπου
$$\prod_{a \in S_m} a \equiv -1 \mathrm{mod} m$$
το πλήθος των λύσεων της ισοτιμίας $x^2 \equiv 1 \mathrm{mod} m$ είναι 2 και οι λύσεις είναι οι προφανείς
$$x \equiv \pm 1 \mathrm{mod} m$$

3. Για $m = 2$ η πρόταση 5.4.46 δεν θα είχε νόημα αφού $+1 \equiv -1 \mathrm{mod} 2$

4. Η πρόταση 5.4.46 αποτελεί το περιεχόμενο του άρθρου (πρότασης) 78 του *Disquisitiones Arithmeticae* του Gauss.

   "Man kann aber den Wilson'shen Satz allgemeiner so aussprechen"

5.4.8 Αρχικές ρίζες

Μερικές φορές μπορούμε να διαπιστώσουμε ότι κάποιοι ακέραιοι είναι αρχικές ρίζες ως προς διάφορα μέτρα:

Πρόταση 5.4.47. *1. Αν οι ακέραιοι p και $q = 2p + 1$ είναι και οι δύο περιττοί πρώτοι, τότε ο $(-1)^{\frac{p-1}{2}} 2$ είναι αρχική ρίζα* mod$q$.

2. Αν p και $q = 4p + 1$ είναι περιττοί πρώτοι, τότε ο 2 είναι αρχική ρίζα mod$q$.

3. Αν p περιττός πρώτος, τότε οι ακόλουθες προτάσεις είναι μεταξύ τους ισοδύναμες:

- *Κάθε μη-τετραγωνικό υπόλοιπο* mod$p$ *είναι αρχική ρίζα* mod$p$.
- *Ο p είναι της μορφής $p = 2^\ell + 1$, $\ell \geq 1$.*

Απόδειξη. 1. Ξεχωρίζουμε δύο περιπτώσεις:

Αν $p \equiv 1 \mathrm{mod} 4$, επειδή $\phi(q) = q - 1 = 2p$ η $\mathrm{ord}_q(2) \mid 2p$. Από το θεώρημα του Euler έχουμε
$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 2^p \mathrm{mod} q$$

Το $q \equiv 3 \mathrm{mod} 5$, δηλαδή $\left(\frac{2}{q}\right) = -1$. Επομένως η $\mathrm{ord}_q 2 \neq p$. Είναι και διάφορη του 1 και 2 (εδώ $2^1 \equiv 1 \mathrm{mod} q$ συνεπώς $q \mid 1$, άτοπο ενώ αν $2^2 \equiv 1 \mathrm{mod} q$ θα είχαμε $q \mid 3$ αλλά $q \geq 2 \cdot 3 + 1 = 7$, πάλι άτοπο). Επομένως $\mathrm{ord}_q 2 = 2p$, το 2 είναι αρχική ρίζα mod$q$.

Αν $p \equiv 3 \mathrm{mod} 4$, τότε και πάλι από το θεώρημα του Euler προκύπτει ότι
$$\left(\frac{-2}{q}\right) \equiv (-2)^{\frac{q-1}{2}} \equiv (-2)^p \mathrm{mod} q.$$

Επειδή $q \equiv 7 \mathrm{mod} 8$, $\left(\frac{-1}{q}\right) = -1$ και $\left(\frac{2}{q}\right) = 1$. Συνεπώς $(-2)^p \equiv -1 \mathrm{mod} q$, δηλαδή $\mathrm{ord}_q(-2) \neq p$. Η τάξη δεν είναι ούτε 1 ούτε 2. ($-2 \equiv 1 \mathrm{mod} q$ συνεπώς $q \mid 3$, άτοπο, αν $(-2)^2 \equiv 1 \mathrm{mod} q$ και πάλι $q \mid 3$, άτοπο.) Συνεπώς $\mathrm{ord}_q(-2) = 2p$, δηλαδή το (-2) είναι αρχική ρίζα mod$q$.

2. $\varphi(q) = q-1 = 4p$ Άρα $\mathrm{ord}_q(2) \in \{1, 2^4, p, 2p, 4p\}$. Αν $2 \equiv 1 \bmod q$ τότε $q \mid 1$, άτοπο.

   Αν $2^2 \equiv 1 \bmod q$ τότε $q \mid 3$, άτοπο.

   Αν $2^4 \equiv 1 \bmod q$ τότε $q \mid 15$ και άρα $q = 3, 4$, άτοπο.

   Ισχύει $\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 2^{2p} \bmod q$.

   Το $q \equiv 5 \bmod 8$ άρα $\left(\frac{2}{7}\right) = -1$. Συνεπώς $\mathrm{ord}_q(2) \neq 2p$ και επομένως $\mathrm{ord}_q(2) \neq p$. Τελικά $\mathrm{ord}_q(2) = 4p = q-1$, δηλαδή το 2 είναι αρχική ρίζα $\bmod q$.

3. Υπάρχουν ακριβώς $\frac{p-1}{2}$ μη-τετραγωνικό υπόλοιπο $\bmod p$ και $\varphi(p-1)$ αρχικές ρίζες $\bmod p$.

   Επομένως για να είναι κάθε μη-τετραγωνικό υπόλοιπο $\bmod p$ αρχική ρίζα $\bmod p$ πρέπει να ισχύει $\varphi(p-1) = \frac{p-1}{2}$. Αλλά ισχύει $\varphi(n) = \frac{n}{2}$ ακριβώς τότε όταν $n = 2^\ell$, $\ell \in \mathbb{N}$, $\ell \geq 1$. (άσκηση) Από αυτό συμπεραίνουμε ότι κάθε μη τετραγωνικό υπόλοιπο $\bmod p$ είναι και αρχική ρίζα $\bmod p$, ακριβώς όταν $p = 2^\ell + 1$, $\ell \in \mathbb{N}$, $\ell \geq 1$.

□

5.4.9 Τέστ ελέγχου πρώτων αριθμών

Θα διατυπώσουμε και θα αποδείξουμε διάφορα test ελέγχου πρώτων αριθμών , ακριβή και πιθανοθεωρητικά.

Πρόταση 5.4.48. *Αν p περιττός πρώτος, $h < p$, $n = hp+1$ ή $n = hp^2+1$ και $2^h \not\equiv 1 \bmod n$, ενώ $2^{n-1} \equiv 1 \bmod n$, τότε ο n είναι πρώτος.*

Απόδειξη. Γράφουμε $n = hp^b + 1$, όπου $b = 1$ ή 2. Έστω $s := \mathrm{ord}_n(2)$. Λόγω των προτάσεων 5.4.3 και 5.4.5, $s \nmid h$, ενώ $s \mid n-1 = hp^b$. Επομένως $p \mid s$.

Επίσης, αφού $s = \mathrm{ord}_n(2)$, έπεται ότι $s \mid \varphi(n)$ οπότε και $p \mid \varphi(n)$.

Αν

$$n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}, \quad \varphi(n) = p_1^{\ell_1-1} p_2^{\ell_2-1} \cdots p_k^{\ell_k-1} (p_1-1) \cdots (p_k-1).$$

Αφού $p \mid s \mid (n-1)$, συνεπάγεται ότι $p \nmid n$. Αυτό σημαίνει ότι $p \neq p_i$, $(i = 1, 2, \ldots, k)$. Επομένως $p \mid (p_i - 1)$ για κάποιο $i \in \{1, 2, \ldots, k\}$ δηλαδή ο n έχει έναν πρώτο παράγοντα $q := p_i$ τέτοιο ώστε $q \equiv 1 \bmod p$. Γράφουμε το $n = qm$. Επειδή, $q \equiv 1 \bmod p$ και $n \equiv 1 \bmod p$, θα έχουμε $m \equiv 1 \bmod p$.

Αν $m > 1$ τότε $n = (a_1 p + 1)(a_2 p + 1)$, όπου $1 \leq a_1 \leq a_2$. Επομένως $hp^{b-1} = a_1 a_2 p + a_1 + a_2$. Τώρα, αν $b = 1$, έχουμε $h = a_1 a_2 p + a_1 + a_2$. Συνεπώς $p \leq a_1 a_2 p < h < p$, άτοπο. Στην περίπτωση αυτή θα πρέπει $m = 1$, δηλαδή ο n είναι πρώτος.

Αν πάλι $b = 2$, τότε $hp = a_1 a_2 p + a_1 + a_2$ από την οποία έπεται ότι $p \mid (a_1 + a_2)$. Επομένως $a_1 + a_2 \geq p$, $2a_2 \geq a_1 + a_2 \geq p$, συνεπώς $a_2 \geq \frac{p}{2}$. Όμως $a_1 a_2 < h < p$. Συνεπώς ($a_1 a_2 \leq h-1$ και $h - 1 \leq p-2$) έχουμε ότι

$$a_1 a_2 \leq p-2 \Rightarrow a_1 \leq \frac{p-2}{a_2} \leq \frac{2(p-2)}{p} < 2.$$

Επομένως $a_1 = 1$ άρα $1 + a_2 \geq p$ και συνεπώς $a_2 \geq p-1$ άρα $a_1 a_2 \geq p-1$. Καταλήξαμε σε άτοπο, άρα $m = 1$ και ο n είναι πρώτος αριθμός. □

Παίρνοντας αφορμή από την πρόταση 5.4.47.1 φυσικό είναι να αναρωτηθούμε πότε ο $q = 2p+1$ είναι πρώτος όταν ο p περιττός πρώτος. Με τη βοήθεια της πρότασης 5.4.48 θα αποδείξουμε την

Πρόταση 5.4.49. *Αν $\ell > 1$ και $p = 4\ell + 3$ τότε ο $q = 2p + 1$ είναι πρώτος ακριβώς τότε όταν*

$$2^p \equiv 1 \bmod q.$$

Απόδειξη. Υποθέτουμε ότι ο $q := 2p+1$ είναι πρώτος. Είναι φανερό ότι $q \equiv 2(4\ell+3)+1 \equiv 7 \bmod 8$. Επομένως ο 2 είναι τετραγωνικό υπόλοιπο mod$q$. Από το κριτήριο του Euler έπεται ότι

$$2^{\frac{q-1}{2}} = 2^p \equiv \left(\frac{2}{q}\right) \equiv 1 \bmod q.$$

Αντίστροφα, αν $2^p \equiv 1 \bmod q$ και θέσουμε στην πρόταση 5.4.48 $h = 2$ και $n = 2p + 1$, έχουμε $h < p$ και $2^h = 4 \not\equiv 1 \bmod n$. Επίσης

$$2^{n-1} = 2^{2p} \equiv 1 \bmod q$$

Επομένως από την πρόταση 5.4.48, ο $n = 2p + 1$ είναι πρώτος. □

Παρατήρηση 5.4.50. Άμεση συνέπεια της πρότασης 5.4.49 είναι ότι αν p και $q = 2p+1$ περιττοί πρώτοι και $p \equiv 3 \bmod 4$, τότε ο p-στος αριθμός Mersenne $M_p = 2^p - 1$, είναι σύνθετος αφού $q \mid M_p$, αρκεί $p > 3$ αφού

$$M_p = 2^p - 1 > 2p + 1 = q.$$

Παράδειγμα

$$23 \mid M_{11}, 47 \mid M_{23}, 167 \mid M_{83}, 263 \mid M_{131}$$

$$359 \mid M_{179}, 383 \mid M_{191}, 479 | M_{239}, 503 \mid M_{251}$$

$$719 \mid M_{359}, 839 \mid M_{419}, 863 \mid M_{431}, 887 \mid M_{447}$$

$$983 \mid M_{491}, 1319 \mid M_{659}, 1367 \mid M_{683}, 1439 \mid M_{719}$$

$$1487 \mid M_{743}, 1823 \mid M_{911}, 2039 \mid M_{1019}$$

Πρώτοι αριθμοί p για τους οποίους και ο $2p + 1$ είναι πρώτος θα λέγονται *πρώτοι αριθμοί της Sophie Germain*.

Στη συνέχεια θα διατυπώσουμε και θα αποδείξουμε δύο ακόμα προτάσεις σχετικές με τους διαιρέτες των αριθμών Mersenne.

Πρόταση 5.4.51. *Αν p περιττός πρώτος, τότε κάθε διαιρέτης του αριθμού Mersenne $M_p = 2^p - 1$, είναι της μορφής $2\ell p + 1$, $\ell \geq 1$.*

Απόδειξη. Αν q πρώτος διαιρέτης του M_p θα έχουμε την ισοτιμία

$$2^p \equiv 1 \bmod q.$$

Ο q είναι κατ' ανάγκη περιττός. Επομένως $(2, q) = 1$. Έστω $s := \mathrm{ord}_q(2)$. Από την πρόταση 5.4.3, έπεται ότι $s \mid p$ (Το $s > 1$, διότι αν $s = 1$ θα είχαμε $2 \equiv 1 \bmod q$, άτοπο). Επομένως $s = p$. Λόγω του μικρού θεωρήματος του Fermat έχουμε

$$2^{q-1} \equiv 1 \bmod q.$$

Και πάλι λόγω της πρότασης 5.4.3, έχουμε $s \mid (q - 1)$, δηλαδή $p \mid (q - 1)$. Αυτό σημαίνει ότι υπάρχει $t \in \mathbb{Z}$ για το οποίο $q = pt + 1$. Ο t θα πρέπει να είναι άρτιος, διότι αν ο t ήταν περιττός, ο q_p θα ήταν άρτιος διαιρέτης του περιττού $M_p = 2^p - 1$, άτοπο. Αν γράψουμε $t = 2\ell$, $\ell \geq 1$, έχουμε ότι

$$q = 2\ell p + 1.$$

Τέλος, παρατηρούμε ότι κάθε διαιρέτης του M_p είναι επίσης της ίδιας μορφής. □

Παρατήρηση 5.4.52. Αρκετά ασθενής συνέπεια της τελευταίας πρότασης είναι ότι κάθε διαιρέτης n του αριθμού Mersenne M_p, όπου p περιττός πρώτος p, επαληθεύει την ισοτιμία $n \equiv 1 \bmod p$.

Θα αποδείξουμε κάτι περισσότερο

Πρόταση 5.4.53. *Αν p περιττός πρώτος, τότε για κάθε διαιρέτη n του αριθμού Mersenne M_p ισχύει $n \equiv \pm 1 \bmod 8$.*

Απόδειξη. Είναι φανερό ότι αρκεί να αποδείξουμε την πρόταση για $n = q$, πρώτο αριθμό. Ο q διαιρεί τον M_p, άρα από την πρόταση 5.4.51

$$q = 2\ell p + 1, \quad \ell \geq 1 \quad (2^p \equiv 1 \bmod p)$$

Επομένως από το κριτήριο του Euler

$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 2^{\ell p} \equiv (2^p)^\ell \equiv 1 \bmod q$$

από το οποίο έπεται ότι $q \equiv \pm 1 \bmod 8$, σύμφωνα με γνωστή ιδιότητα του συμβόλου του Legendre. □

Γνωρίζουμε ήδη ότι οι μεγαλύτεροι γνωστοί πρώτοι αριθμοί είναι οι αριθμοί του Mersenne. Πώς όμως τους υπολογίζουμε; Σίγουρα χρειάζεται πολύ δουλειά ο ηλεκτρονικός υπολογιστής.

Πρόταση 5.4.54 (Τέστ των Lucas-Lehmer)**.** *Θεωρούμε την αναδρομική ακολουθία*

$$S_0 = 4, S_{n+1} = S_n^2 - 2, n \geq 0.$$

Ο αριθμός Mersenne $M_n = 2^n - 1$ είναι πρώτος ακριβώς όταν $M_n \mid S_{n-2}$.

Η απόδειξη της πρότασης 5.4.54 θα γίνει στο δεύτερο μέρος του βιβλίου.

Επιστρέφουμε σε γενικά κριτήρια ελέγχου πρώτων αριθμών. Πρώτα από όλα ένα ανάλογο της πρότασης 5.4.48.

Πρόταση 5.4.55. *Έστω $m \geq 2$, $h < 2^m$ και $n := h2^m + 1$, ένα τετραγωνικό ανισοϋπόλοιπο $\bmod p$, όπου p περιττός πρώτος αριθμός. Ο n είναι πρώτος ακριβώς τότε όταν*

$$p^{\frac{n-1}{2}} \equiv -1 \bmod p$$

Απόδειξη. Υποθέτουμε ότι n είναι πρώτος. Επειδή $m \geq 2$, έπεται ότι $n \equiv 1 \bmod 4$. Ο n είναι μη τετραγωνικό υπόλοιπο $\bmod p$, συνεπώς $\left(\frac{n}{p}\right) = -1$. Ο τετραγωνικός νόμος αντιστροφής δίνει $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right) = -1$. Σύμφωνα με το κριτήριο του Euler

$$p^{\frac{n-1}{2}} \equiv \left(\frac{p}{n}\right) \equiv -1 \bmod n.$$

Υποθέτουμε ότι ισχύει η ισοτιμία και θα αποδείξουμε ότι ο n είναι πρώτος αριθμός. Έστω q κάποιος πρώτος παράγοντας του n και $s := \mathrm{ord}_q(p)$. Από την ισοτιμία

$$p^{\frac{n-1}{2}} \equiv -1 \bmod p,$$

έπεται ότι $p^{n-1} \equiv 1 \bmod p$, ενώ από το θεώρημα του Fermat $p^{q-1} \equiv 1 \bmod q$. Επομένως το $s \nmid \frac{n-1}{2}$, $s \mid (n-1)$ και $s \mid (q-1)$, δηλαδή $s \nmid h2^{m-1}$, $s \mid h2^m$ και $s \mid (q-1)$.

Όπως και στην πρόταση 5.4.48 έχουμε $2^m \mid s \mid (q-1)$. Υπάρχει ακέραιος t, $q = t2^m + 1$ και $q \equiv 1 \bmod 2^m$. Αλλά και $n \equiv 1 \bmod 2^m$. Άρα $\frac{n}{q} \equiv 1 \bmod 2^m$. Ο n γράφεται στη μορφή

$$n = (a_1 2^m + 1)(a_2 2^m + 1) \text{ όπου } a_1 \geq 1, a_2 \geq 0.$$

Όμως

$$2^m a_1 a_2 < 2^m a_1 a_2 + a_1 + a_2 = h < 2^m.$$

Για να ισχύει η τελευταία ανισότητα θα πρέπει $a_2 = 0$, δηλαδή $\frac{n}{q} = 1$, δηλαδή $n = q$ και αποδείξαμε ότι ο n είναι πρώτος. □

Πόρισμα 5.4.56 (Το κριτήριο του Pepin)**.** *Ο n-οστος αριθμός Fermat $F_n = 2^{2^n} + 1$ είναι πρώτος ακριβώς τότε όταν*

$$3^{\frac{F_n - 1}{2}} \equiv -1 \bmod 3 \tag{5.4.10}$$

Απόδειξη. Επαγωγικά αποδεικνύεται ότι $F_n \equiv 2 \bmod 3$, για κάθε $n \geq 1$. Επομένως $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$ δηλαδή ο F_n είναι μη-τετραγωνικό υπόλοιπο mod3.

Σύμφωνα με την πρόταση 5.4.55, ο F_n είναι πρώτος ακριβώς τότε όταν ισχύει η (5.4.10). □

Παρατήρηση 5.4.57. Άμεση συνέπεια του πορίσματος είναι ότι όταν ο F_n είναι πρώτος, τότε ο 3 είναι αρχική ρίζα modF_n.

Θα μπορούσε να ρωτήσει κάποιος αν υπάρχει για τους αριθμούς Fermat πρόταση ανάλογη της πρότασης 5.4.51 για τους αριθμούς Mersenne. Η απάντηση στο ερώτημα είναι θετική και ισχύει η ακόλουθη:

Πρόταση 5.4.58. *Κάθε πρώτος διαιρέτης του αριθμού Fermat*

$$F_n = 2^{2^n} + 1, \quad n > 1$$

είναι της μορφής $2^{n+2}\ell + 1$ με $\ell \geq 1$.

Απόδειξη. Αν p πρώτος διαιρέτης του F_n έχουμε

$$2^{2^n} \equiv -1 \bmod p$$

από την οποία έπεται

$$2^{2^{n+1}} \equiv 1 \bmod p.$$

Έστω $s := \text{ord}_p(2)$. Επομένως $s \mid 2^{n+1}$. Θα αποδείξουμε ότι $s = 2^{n+1}$. Αν υποθέσουμε ότι $s = 2^k$ για $1 \leq k \leq n$, επειδή $2^s \equiv 1 \bmod p$ θα είχαμε και

$$2^{2^n} \equiv 1 \bmod p.$$

Επομένως θα είχαμε $1 \equiv -1 \bmod p$, δηλαδή $p = 2$, άτοπο.

Σύμφωνα με το θεώρημα του Fermat

$$2^{p-1} \equiv 1 \bmod p.$$

Επομένως $s \mid \phi(s) = p-1$, $2^{n+1} \mid (p-1)$. Αυτό σημαίνει ότι για $n \geq 2$, $p \equiv 1 \bmod 8$ δηλαδή $\left(\frac{2}{p}\right) = 1$.

Σύμφωνα με το κριτήριο του Euler $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv 1 \bmod p$. Επομένως $s \mid \frac{p-1}{2}$, δηλαδή $2^{n+1} \mid \frac{p-1}{2}$. Οπότε $p = \ell 2^{n+2} + 1$, για $\ell \geq 1$. □

Η σωστή αντιστροφή του Θεωρήματος του Fermat είναι το ακόλουθο θεώρημα του Lucas (1891).

Πρόταση 5.4.59. *Αν υπάρχει κάποιος ακέραιος a για τον οποίο ισχύουν*

1. $a^{n-1} \equiv 1 \bmod n$ *και*
2. $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$, *για κάθε πρώτο p διαρέτη του $n-1$,*

τότε ο n είναι πρώτος.

Απόδειξη. Λόγω της 1. και της πρότασης 5.4.3 έχουμε ότι $s := \mathrm{ord}_n(a) \mid (n-1)$. Θα αποδείξουμε ότι $s = n-1$. Υποθέτουμε ότι $s \neq n-1$. Επομένως, υπάρχει $\ell \in \mathbb{Z}$, $\ell > 1$ τέτοιος ώστε $n-1 = s \cdot \ell$. Αν p είναι ένας πρώτος παράγοντας του ℓ, τότε

$$a^{\frac{n-1}{p}} = a^{\frac{s\ell}{p}} = (a^s)^{\frac{\ell}{p}} \equiv 1 \bmod n,$$

άτοπο, λόγω της 2. Επομένως $s = n-1$. Όμως, επειδή $s \leq \varphi(n) \leq n-1 = s$, έπεται ότι $\varphi(n) = n-1$, και συνεπώς ο n είναι πρώτος. Πράγματι, αν ο n δεν είναι πρώτος και d κάποιος γνήσιος διαιρέτης αυτού ($1 < d < n$), τότε το $\varphi(n)$ θα ήταν κατ' ανάγκη $\varphi(n) \leq n-2$, άτοπο. □

Αν τώρα p περιττός πρώτος και a ακέραιος πρώτος προς τον p τότε ισχύει

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Επομένως, αν $n \in \mathbb{N}$, $n > 1$ και $b \in \mathbb{Z}$ με $(b, n) = 1$, τέτοιος ώστε

$$\left(\frac{b}{n}\right) \not\equiv b^{\frac{p-1}{2}} \bmod p$$

συμπεραίνουμε με βεβαιότητα ότι ο n είναι σύνθετος.

Φυσικό και επιθυμητό είναι να ίσχυε και το αντίστροφο του κριτηρίου του Euler. Σε αυτή την περίπτωση θα είχαμε ένα ακριβές κριτήριο ελέγχου πρώτων αριθμών. Δυστυχώς όμως δεν είναι αληθινό. Για $b = 10$ και $n = 91$ έχουμε

$$\left(\frac{10}{91}\right) = -1 \equiv 10^{\frac{91-1}{2}} \bmod 91$$

Ορισμός 5.4.60. Αν n περιττός σύνθετος φυσικός αριθμός και b θετικός ακέραιος με $(b, n) = 1$ για τον οποίο ισχύει

$$\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \bmod n$$

τότε ο n θα λέγεται Euler ψευδο-πρώτος ως προς τη βάση b.

Παράδειγμα. $n = 1105$, $b = 2$,

$$b^{\frac{n-1}{2}} \equiv 2^{552} \equiv 1105$$

και $\left(\frac{2}{1105}\right) = 1$, αφού $1105 \equiv 1 \bmod 8$.

Παράδειγμα. Έστω $n = 341$ και $b = 2$ υπολογίζουμε το $2^{170} \equiv 1 \bmod 341$. Το $341 \equiv -3 \bmod 8$, συνεπώς $\left(\frac{2}{341}\right) = -1$. Επομένως το $341 \not\equiv \left(\frac{2}{341}\right) \bmod 341$. Άρα ο 341 είναι σύνθετος.

Πρόταση 5.4.61. *Αν ο n είναι Euler ψευδοπρώτος ως προς τη βάση b, τότε ο n είναι και ψευδοπρώτος ως προς τη βάση b.*

Απόδειξη. Εξ υποθέσεως ισχύει η ισοτιμία

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \mathrm{mod} n$$

επομένως το

$$b^{n-1} \equiv \left(\frac{b}{n}\right) \equiv 1 \mathrm{mod} n$$

□

Οι παρακάτω προτάσεις αποδεικνύονται στο [20, 454-460].

Παρατήρηση 5.4.62. Το αντίστροφο δεν ισχύει. Ο 341 είναι ψευδοπρώτος ως προς τη βάση 2, ενώ δεν είναι Euler ψευδοπρώτος ως προς αυτή τη βάση.

Στη συνέχεια θα δείξουμε ότι κάθε ισχυρός ψευδο-πρώτος είναι Euler ψευδο-πρώτος.

Πρόταση 5.4.63. *Αν ο φυσικός αριθμός n είναι ισχυρός ψευδο-πρώτος ως προς τη βάση b τότε είναι και Euler ψευδο-πρώτος ως προς αυτή τη βάση.*

Και πάλι δεν ισχύει το αντίστροφο. Δεν είναι όλοι οι Euler ψευδοπρώτοι ως προς κάποια βάση και ισχυροί ψευδοπρώτοι. Όμως ισχύει:

Πρόταση 5.4.64. *Αν $n \equiv 3 \mathrm{mod} 4$ και ο n είναι Euler ψευδοπρώτος ως προς κάποια βάση b τότε ο n είναι ισχυρός ψευδοπρώτος ως προς τη βάση αυτή.*

Πρόταση 5.4.65. *Αν n είναι Euler ψευδοπρώτος ως προς τη βάση b και $\left(\frac{b}{n}\right) = -1$, τότε το n είναι ισχυρός ψευδοπρώτος ως προς αυτή τη βάση.*

Πρόταση 5.4.66. *Αν n περιττός, σύνθετος φυσικός αριθμός, τότε το πλήθος των ακέραιων b, $1 \leq b < n$ με $(b, n) = 1$ για τους οποίους ο n είναι Euler ψευδοπρώτος ως προς βάση b, είναι $\leq \frac{\varphi}{2}$.*

Πιθανοθεωρητικό κριτήριο ελέγχου πρώτων αριθμών.

Δίνεται ένας θετικός ακέραιος n. Επιλέγουμε τυχαίο t-ακέραιους $b_1, b_2, \ldots, b_t$ από το σύνολο $\{1, 2, \ldots, n-1\}$ για τους οποίους ισχύει $(b_j, n) = 1$ για $j = 1, \ldots, t$. Ελέγχουμε την ισχύ των ισοτιμιών

$$b_j^{\frac{n-1}{2}} \equiv \left(\frac{b_j}{n}\right) \mathrm{mod} n$$

Αν κάποια ισοτιμία δεν ισχύει, τότε ο n είναι (σίγουρα) σύνθετος.

(Αν ο n είναι πρώτος τότε ισχύουν όλες οι ισοτιμίες).

Αν όμως ο n είναι σύνθετος, τότε η πιθανότητα να ισχύουν όλες οι ισοτιμίες είναι μικρότερη του $\frac{1}{2^t}$. Δηλαδή αν ο n περάσει το τέστ, τότε είναι πολύ πιθανό να είναι πρώτος.

Βέβαια το ερώτημα παρέμεινε. Είναι δυνατή η εύρεση ενός ντετερμινιστικού αλγορίθμου ελέγχου πρώτων αριθμών ο οποίος να αποφασίζει σε σχετικά σύντομο (πολυωνυμικό) χρόνο;

Το πρόβλημα εθεωρείτο ως ένα από τα πλέον δύσκολα. Έτσι ήταν μια ευχάριστη έκπληξη όταν κυκλοφόρησε στο διαδίκτυο (δημοσιεύθηκε στην ιστοσελίδα τους) στις 6 Αυγούστου του 2002 η εργασία των Maninda Agrawal, Neeraj Kayal και Nitin Saxena «Primes is in P».

Δύο μέρες νωρίτερα είχε σταλεί από τους συγγραφείς της σε 15 διάσημους μαθηματικούς ειδικούς της περιοχής. Έτσι, πολύ σύντομα αποκαταστάθηκε η αξιοπιστία του αποτελέσματος και διαλύθηκε η οποιαδήποτε υποψία ύπαρξης λάθους.

Το αποτέλεσμα δεν στηρίχθηκε σε προηγούμενες εργασίες και ο αλγόριθμος τρέχει σε πολυωνυμικό χρόνο.

Η κεντρική ιδέα της απόδειξης είναι ο ακόλουθος χαρακτηρισμός των πρώτων αριθμών:

Ο φυσικός αριθμός n είναι πρώτος ακριβώς τότε όταν

$$(1-x)^n \equiv (1-x^n) \mathrm{mod} n$$

και σε κάποιο σημαντικό θεώρημα της θεωρίας κοσκίνων (Sieve theory). Η εργασία δημοσιεύθηκε στο περιοδικό Annals of Mathematics [21]

Ο ενδιαφερόμενος αναγνώστης παραπέμπεται επίσης στο διαφωτιστικό άρθρο του Folkmar Bornemann "Ein Durchbruch für Jedermann", DMV-Mitteilungen, 4/2002, ή στην αγγλική του μετάφραση PRIMES is in *P* "Breakthrough for Everyman" [15] καθώς και στα βιβλία

- Paulo Ribenboim "Die Welt der Primzahlen, Geheimnisse und Rekorde" [25] σελ. 120-122
- Richard Crandall, Carl Pomerance "Prime Numbers, a computational Perspective" [27] σελ. 200-207
- Martin Dietzfelbinger "Primality Testing in Polynomial Time from Randomized Algorithms to Primes in *P*" [24]

Το τρίτο μάλιστα βιβλίο είναι όλο αφιερωμένο στον AKS-αλγόριθμο όπως συνηθίζεται σήμερα να λέγεται.

Τέλος αξίζει να σημειωθεί ότι μέχρι σήμερα, ο αλγόριθμός δεν είναι τόσο πρακτικός και γρήγορος όπως άλλοι κυρίως πιθανοθεωρητικοί αλγόριθμοι.

Βιβλιογραφία

[1] A. Venkov: *Elementary Number Theory, Translation Eng. Holland*. 1932.

[2] A. Weil: *Number theory, an approach through history, from Hammurapi to Legendere*. Birkhäuser Boston, 1983.

[3] Alexander Aigner: *Zahlentheorie*. Walter De Gruyter, Berlin, 1975.

[4] Bundschuh: *Einführung in die Zahlentheorie*. 2002.

[5] C. F. Gauss: *Untersuchungen über höhere Arithmetik*. Chelsea Publishing Company, Second Edition, New York, 1981.

[6] C. Hooley: *On Artin's Conjecture*. J. Reine Angew Math., 225:209–220, 1967.

[7] C.F. Gauss: *Disquisitiones Arithmeticae*. Yale University Press, 1965.

[8] C.P. Miller, A.E Western: *Tables of Indices and Primitive Roots*. Cambridge University Press Cambridge, 1968.

[9] D. Hilbert: *Mathematical Problems*. Bulletin of the American Mathematical Society, 8, no. 10:437–479, 1902. Earlier publications (in the originalGerman) appeared in Goettinger Nachrichten, 1900, pp. 253-297, and Archiv der Mathematik und Physik, 3dser., vol. 1, (1901), pp. 44-63, 213-237.

[10] D. Hilbert: *Die Hilbertsche Probleme*. Ostwalds Klassiker der exakten Wissenschaften, Akademische Verlagsgesellschaft, 1976.

[11] Don Redmond: *Number Theory, An Introduction*. Marcel Dekker, 1996.

[12] E. Bach: *The complexity of number-theoretic constants*. Inf. Process. Lett., 62:145–152, 1997.

[13] E. Rose: *A course in number theory*. Oxford science publications, Oxford, 1996. 2nd edition.

[14] Ezra Brown: *The First proof of quadratic reciprocity Law*. The American Mathematical Monthly, 88:257–264, 1981.

[15] Folkmar Barnemann: *Primes is in p, Breakthrough for Everyman*. Notices of the AMS, 50 (7):545–553, 2003.

[16] Franz Lemmermeyer: *Reciprocity Laws from Euler to Eisenstein*. Springer Monographs in Mathematics, Springer, Berlin, 2000.

[17] H. Hasse: *Vorlesungen über Zahlentheorie*. Springer-Verlag Berlin, 1964.

[18] Herbert Piper: *Variationen über ein zahlentheoretishen Thema von Carl Friedrich Gauss*. Birkhäuser, Basel und Stuttgart, 1977.

[19] Horst Kn"orrer, Claus Günther Schmidt, Joachim Schwemer, and Peter Soloday: *Mathematische Miniaturen Arithmetik und Geometrie*. Birkhäuser Basel, 1986.

[20] K.H. Rosen: *Elementary Number Theory and Its Applications*. Addison-Wesley Longman, Limited, 2000.

[21] M. Agrawal, N. Kayal, N. Saxena: *Primes is in p*. Annals of Mathematics 160, pages 781–793, 2004.

[22] M. Gesterhaber: *The 152nd proof of the law of quadratic reciprocity*. The American Math. Monthly, 70:397–398, 1963.

[23] M. Niven and H.S. Zuckerman and H.L. Montgomery: *An introduction to the theory of numbers*. J. Wiley, 1991.

[24] Martin Dietzfelbinger: *Primality Testing in Polynomial Time, from Randomized Algorithms to "Primis in P"*. Springer-Verlag, 2004.

[25] Paulo Ribenboim: *Die Welt Der Primzahlen, Geheimnisse Und Rekorde*. Springer, Heidelberg, 2005.

[26] Pieter Moree: *A note on Artin's conjecture*. Simon Stevin, 67:255–257, 1993.

[27] R. Crandall, C.B. Pomerance: *Prime Numbers: A Computational Perspective*. 2005.

[28] R. Gupta, M. Ram Murty: *A remark on Artin's conjecture*. Inventiones Math., 78:127–130, 1984.

[29] R. Heath-Brown, D.: *Artin's conjecture for primitive roots*. Quart. J. Math. Oxford Ser, (2) 37:27–38, 1986.

[30] V. Shoup: *Searching for primitive roots in finite fields*. Math. Comput., 58 no. 197:369–380, 1992.

[31] Winfried Scharlau, Hans Opolka: *From Fermat to Minkowski, Lectures on the Theory of Numbers and Its Historical Development*. UTM, Springer-Verlag New York, 1985.

[32] W.Sierpinski: *Elementary Theory of Numbers*. P.W.N. Warsawa, 1964.

[33] Αντωνιάδης, Γιάννης Α.: *Θεωρία Αριθμών ΙΙ, L-σειρές*. Ηράκλειο, 1999.

[34] Μάγειρα, Παναγιώτου Ν.: *Εισαγωγή εις την Αριθμοθεωρίαν Μέρος 2ο*. 1965.

Μέρος II

Άρρητοι αριθμοί και αριθμητική

Εισαγωγή

Μέχρι τώρα ασχοληθήκαμε κυρίως με την αριθμητική των ρητών αριθμών. Στο δεύτερο μέρος του βιβλίου θα ασχοληθούμε με άρρητους αριθμούς. Ένας μιγαδικός αριθμός α θα λέγεται άρρητος αν δεν είναι ρητός.

Οι αρχαίοι Έλληνες πρώτοι διαπίστωσαν την ύπαρξη άρρητων ποσοτήτων. Αν έχουμε ένα ορθογώνιο και ισοσκελές τρίγωνο με μήκος πλευράς 1, τότε η υποτείνουσά του έχει μήκος $\sqrt{2}$ και ισχύει η

Πρόταση 5.4.67. *Ο $\sqrt{2}$ είναι άρρητος αριθμός.*

Η αλήθεια της πρότασης διαπιστώθηκε από τον Πυθαγόρα και περιέχεται στον Ευκλείδη (βιβλίο x, πρόταση 117). Η απόδειξη δίνεται με απαγωγή σε άτοπο. Αν υποθέσουμε ότι ο $\sqrt{2}$ είναι ρητός, έστω $\sqrt{2} = a/b$, $a, b \in \mathbb{N}$ με $(a, b) = 1$ θα αποδείξουμε ότι ο b είναι συγχρόνως και άρτιος και περιττός. Από τη σχέση $\sqrt{2} = a/b$ έπεται ότι $2b^2 = a^2$ και επομένως ο a είναι άρτιος, $a = 2c$, $c \in \mathbb{N}$. Επειδή $(a, b) = 1$, έπεται ότι ο b είναι περιττός. Όμως, $(2c^2) = 2b^2$, δηλαδή $4c^2 = 2b^2$ άρα $b^2 = 2c^2$ και συνεπώς και ο b είναι άρτιος, άτοπο.

Ανάλογα αποδεικνύεται ότι αν m, n φυσικοί αριθμοί $m > 1$ και $n > 1$ τότε το $\sqrt[n]{m}$ είναι ρητός αν και μόνο αν ο m είναι n-στη δύναμη ακέραιου.

Πράγματι, αν $m = a^n$, τότε ο $\sqrt[n]{m}$ είναι ρητός. Αν πάλι $\sqrt[n]{m}$ είναι ρητός, έστω $\sqrt[n]{m} = a/b$, όπου $a, b \in \mathbb{Z}$. $(a, b) = 1$. Αν $b > 1$, τότε υπάρχει πρώτος p, $p \mid b$, οπότε η σχέση $b^n m = a^n$ μας δίνει $p \mid a$, δηλαδή $(a, b) > p$, άτοπο.

Από τα παραπάνω συμπεραίνουμε ότι για κάθε θετικό ακέραιο m η $\sqrt{m}$ είναι αριθμός άρρητος, ακριβώς τότε όταν ο m δεν είναι τέλειο τετράγωνο ακέραιου.

Όπως είναι γνωστό, η ανακάλυψη της ύπαρξης αρρήτων ποσοτήτων στην αρχαία Ελλάδα, αποτέλεσε ένα αρκετά ισχυρό οοκ για τους μαθηματικούς της εποχής. Στο δεύτερο μέρος του παρόντος θα ασχοληθούμε με την αριθμητική αρρήτων ποσοτήτων δευτέρου βαθμού. Πρόκειται για (αλγεβρικούς) αριθμούς, ρίζες δευτεροβάθμιων εξισώσεων με ρητούς συντελεστές και διακρίνουσα Δ, όχι τέλειο τετράγωνο ρητού. Στο πρώτο Κεφάλαιο ασχολούμαστε με τους αριθμούς Fibonacci και Lucas, μελετούμε βασικές αριθμοθεωρητικές ιδιότητες αυτών καθώς και τη χρήση τους στον έλεγχο πιστοποίησης πρώτων αριθμών.

Στο κεφάλαιο 7 μελετούμε τα πεπερασμένα και άπειρα συνεχή κλάσματα και την έκφραση ρητών και αρρήτων ποσοτήτων σε σχέση με αυτά. Ιδιαίτερη αναφορά γίνεται στα περιοδικά συνεχή

κλάσματα και στο θεώρημα των Euler-Lagrange, ενώ υπολογίζονται και τα συνεχή κλάσματα υπερβατικών ποσοτήτων όπως των e και π.

Το κεφάλαιο 8 είναι αφιερωμένο στην επίλυση της εξίσωσης του Pell η οποία έχει πολλές εφαρμογές στη Θεωρία Αριθμών αλλά είναι και βασικό εργαλείο των κεφαλαίων που ακολουθούν.

Στο κεφάλαιο 9 μελετάται η θεωρία των τετραγωνικών μορφών, η παράσταση ακέραιων αριθμών μέσω (διωνυμικών) τετραγωνικών μορφών, τα αθροίσματα δύο τετραγώνων και γίνεται ταξινόμηση όλων των τετραγωνικών μορφών διακρίνουσας.

Στο κεφάλαιο 10 δίνονται ορισμοί και ιδιότητες των τετραγωνικών σωμάτων αριθμών, και στοιχεία τα οποία φιλοδοξούν να δώσουν μια πρώτη εισαγωγή στην αλγεβρική θεωρία των αριθμών. Δηλαδή αναπτύσσονται έννοιες όπως ακέραιοι αλγεβρικοί, βάση ακεραιότητας, διακρίνουσα τετραγωνικού σώματος αριθμών. Μονάδες της περιοχής των ακέραιων αλγεβρικών αριθμών τετραγωνικού σώματος αριθμών.

6

Αριθμοί Fibonacci

6.1 Αριθμοί Fibonacci

6.1.1 Ορισμός και βασικές ιδιότητες

Ο πρώτος μεγάλος μαθηματικός του δυτικού κόσμου είναι ο Leonardo Pisano (1170-1250), από την Πίζα, ο οποίος είναι γνωστότερος με το παρατσούκλι Fibonacci, το οποίο αποτελεί σύνθεση των λέξεων filius και Bonacci, (γιος της οικογένειας των Bonacci). Είχε επισκεφθεί διάφορες χώρες όπως την Αίγυπτο, Συρία, Βυζάντιο, Σικελία και είχε έρθει σε επαφή με τα μαθηματικά της Ανατολής. Ήταν ο πρώτος που εισήγαγε στη δύση την ινδική αρίθμηση. Στα 1202 δημοσίευσε το βιβλίο *Liber Abaci*, (Βιβλίο των Υπολογισμών). Ένα πρόβλημα του βιβλίου του ασχολείται με τον πολλαπλασιασμό των κουνελιών.

"Quot paria coniculorum in uno anno ex uno pario germinentur."

Πόσα ζευγάρια κουνέλια προκύπτουν στο τέλος ενός έτους από ένα ζευγάρι, αν κάθε ζευγάρι γεννάει κάθε μήνα ένα καινούργιο ζευγάρι αρχίζοντας όμως από τον δεύτερο μήνα της ζωής του; Ουσιαστικά πρόκειται για την (αναδρομική) ακολουθία των επονομαζόμενων αριθμών Fibonacci

$$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}, \text{ για κάθε } n \geq 1.$$

Πρόκειται για μια αρκετά ενδιαφέρουσα ακολουθία με πολλές εφαρμογές η οποία βρίσκεται μέχρι σήμερα στο κέντρο της ερευνητικής δραστηριότητας. Μάλιστα έχει ιδρυθεί η Fibonacci Association η οποία εκδίδει και περιοδικό με τίτλο The Fibonacci Quarterly. Περισσότερα στοιχεία για τους αριθμούς αυτούς μπορούμε να βρούμε στα [6],[11],[3].

Πρόταση 6.1.1. *Για κάθε φυσικό αριθμό $n \geq 1$ ισχύουν:*

1. $F_1 + F_2 + \ldots + F_n = F_{n+2} - 1$
2. $F_1 + F_3 + \ldots + F_{2n-1} = F_{2n}$
3. $F_2 + F_4 + \ldots + F_{2n} = F_{2n+1} - 1$
4. $F_1^2 + F_2^2 + \ldots + F_n^2 = F_n F_{n+1}$
5. $F_{n+m} = F_{n-1}F_m + F_n F_{m+1}$
6. $F_{n+1}^2 = F_n F_{n+2} + (-1)^n$ **(Τύπος του Cassini)**.

Σχήμα 6.1.1: Fibonacci, Το παρόν έργο αποτελεί κοινό κτήμα (public domain), λόγω παρέλευσης 70 ετών από τον θάνατο του δημιουργού.

Απόδειξη. 1. Γράφουμε $F_1 = F_3 - F_2, F_2 = F_4 - F_3, \ldots, F_n = F_{n+2} - F_{n+1}$ και προσθέτουμε κατά μέλη: $F_1 + F_2 + \ldots + F_n = F_{n+2} - F_2 = F_{n+2} - 1$.

2. Γράφουμε $F_3 = F_4 - F_2$, $F_5 = F_6 - F_4, \ldots, F_{2n-1} = F_{2n} - F_{2n-2}$ και προσθέτουμε κατά μέλη. Υπενθυμίζουμε ότι $F_1 = F_2 = 1$.

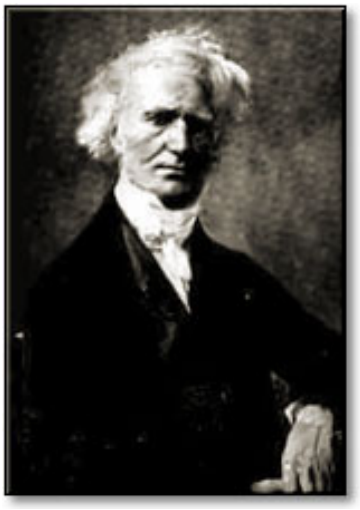
3. Αφαιρούμε την 2. από την 1.(για δείκτη $2n$) κατά μέλη.

4. Ισχύει
$$F_kF_{k+1} - F_{k-1}F_k = F_k(F_{k+1} - F_{k-1}) = F_k^2.$$
Εφαρμόζουμε την ταυτότητα αυτή διαδοχικά για $k = 1, 2, \ldots, n$ και έχουμε: $F_1^2 = F_1F_2$, $F_2^2 = F_2F_3 - F_1F_2$, $\ldots$ $F_n^2 = F_nF_{n+1} - F_{n-1}F_n$. Τις προσθέτουμε κατά μέλη και έχουμε το ζητούμενο.

5. Θα την αποδείξουμε επαγωγικά ως προς m. Για $m = 0$, προφανώς ισχύει. Υποθέτουμε ότι ισχύει για όλα τα m, $m \leq k + 1$. Επομένως ισχύουν $F_{n+k} = F_{n-1}F_k + F_nF_{k+1}$ και $F_{n+k+1} = F_{n-1}F_{k+1} + F_nF_{k+2}$. Προσθέτουμε κατά μέλη και έχουμε $F_{n+k+2} = F_{n-1}F_{k+2} + F_nF_{k+3}$, δηλαδή ισχύει και για $k + 2$ και επομένως για κάθε φυσικό αριθμό m.

6. Θα την αποδείξουμε επαγωγικά ως προς n. Για $n = 0$, προφανώς ισχύει. Υποθέτουμε ότι ισχύει για κάποιο φυσικό k, $F_{k+1}^2 = F_kF_{k+2} + (-1)^k$. Επομένως $F_{k+1}^2 + F_{k+1}F_{k+2} = F_kF_{k+2} + F_{k+1}F_{k+2} + (-1)^k$ Από τη σχέση αυτή προκύπτει $F_{k+1}F_{k+3} = F_{k+2}^2 + (-1)^k$, και συνεπώς $F_{k+2}^2 = F_{k+1}F_{k+3} + (-1)^{k+1}$. Άρα ισχύει για κάθε φυσικό αριθμό n.

□



Σχήμα 6.1.2: Jacques Binet, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Jacques_Binet.jpg`

Αυτονόητο θεωρείται το ερώτημα αν υπάρχει «κλειστός» τύπος για τον n-στό όρο της ακολουθίας F_n. Η απάντηση στο ερώτημα είναι θετική, δόθηκε όμως πολύ αργότερα, στα 1843, από τον Γάλλο μαθηματικό *Binet* μέσω του ομώνυμου *τύπου Binet*.

Πράγματι η εξίσωση

$$x^2 - x - 1 = 0$$

έχει ρίζες $a = \frac{1+\sqrt{5}}{2}$ και $b = \frac{1-\sqrt{5}}{2}$. Επομένως ισχύουν

$$a^2 = a + 1 \text{ και } b^2 = b + 1$$

Για κάθε φυσικό αριθμό $n \geq 1$,έχουμε

$$a^{n+1} = a^n + a^{n-1}, \text{ και } b^{n+1} = b^n + b^{n-1}.$$

Αφαιρούμε τις δύο αυτές ισότητες κατά μέλη και διαιρούμε συγχρόνως με $(a - b)$:

$$\frac{a^{n+1} - b^{n+1}}{a - b} = \frac{a^n - b^n}{a - b} + \frac{a^{n-1} - b^{n-1}}{a - b}.$$

Αν λοιπόν ορίσουμε για κάθε $n \in \mathbb{N}$, $A_n := \frac{a^n - b^n}{a-b}$, τότε για κάθε $n \geq 1$ ισχύει:

$$A_{n+1} = A_n + A_{n-1} \text{ και επιπλέον } A_0 = 0, A_1 = 1.$$

Άρα η ακολουθία A_n ταυτίζεται με αυτήν του Fibonacci, $A_n = F_n$ για κάθε $n \in \mathbb{N}$. Συνεπώς έχουμε τον παρακάτω τύπο που είναι γνωστός ως τύπος Binet:

$$F_n = \frac{a^n - b^n}{a - b} = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right\},$$

Σημείωση: Η απόδειξη που δώσαμε είναι εύκολη αλλά προϋποθέτει τη γνώση του τύπου. Για μιά κάπως διαφορετική απόδειξη δείτε [6], [4, σελ. 62, Satz 34].

Επίσης, οι τύποι του Binet,μπορούν να υπολογιστούν και με χρήση Γραμμικής Άλγεβρας (εφαρμογές της διαγωνιοποίησης), όπως και με τη θεωρία των γεννητριών συναρτήσεων.

Εφαρμογές 6.1.1

Ο άρρητος αριθμός $\varphi = \frac{1+\sqrt{5}}{2}$ ο οποίος ονομάζεται χρυσή αναλογία ικανοποιεί τη σχέση

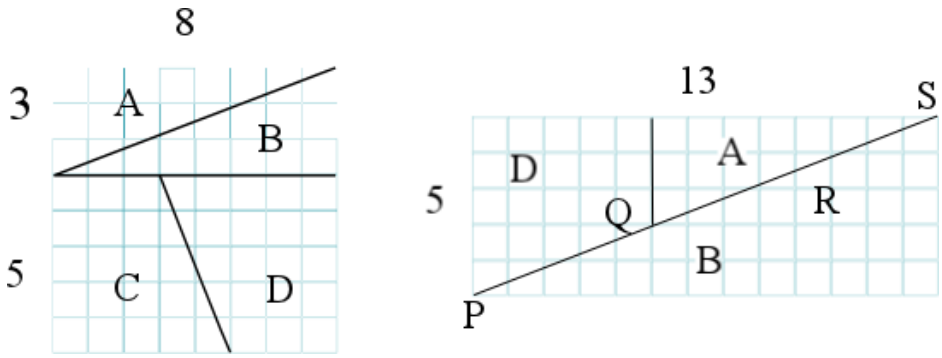
$$1 + \frac{1}{\varphi} = \varphi.$$

Η εμφανίζεται στις αναλογίες του ανθρώπινου σώματος, στην αρχιτεκτονική, στην ζωγραφική, στον φυτικό κόσμο κτλ.

Σχήμα 6.1.3: Άνθος χαμομηλιού (Anthemis tinctoria), στο οποίο έχουνε σχεδιαστεί 21 μπλε και 13 γαλάζια σπιράλ. Οι διατάξεις αυτές εμπλέκουν διαδοχικούς αριθμούς Fibonacci και εμφανίζονται πολύ συχνά στη φύση. Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:FibonacciChamomile.PNG`

.

Μία γεωμετρική οφθαλμαπάτη ή (αλλιώς) ένα γεωμετρικό παράδοξο



Σχήμα 6.1.4: Σχήμα τετραγώνων

Σχήμα 6.1.5: Lucas, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Elucas_1.png`

Το παράδειγμα αυτό το έχουμε πάρει από το [10, σελ. 135]. Μπορούμε να φτιάξουμε ένα τετράγωνο μήκους πλευράς 8 και να το χωρίσουμε σε 64 τετραγωνάκια. Το κόβουμε και το ράβουμε πάλι και «βλέπουμε» ότι σχηματίστηκε ορθογώνιο παραλληλόγραμμο διαστάσεων 13 επί 5, το οποίο όμως έχει εμβαδόν 65 και όχι 64 όπως το αρχικό τετράγωνο, κάτι το οποίο είναι παράδοξο. Πού βρίσκεται το λάθος;
Η απάντηση είναι ότι κάτι που στο σχήμα φαίνεται ευθεία γραμμή είναι οφθαλμαπάτη!. Μέσα στο ορθογώνιο σχηματίζεται ουσιαστικά ένα πολύ μικρό, μακρόστενο παραλληλόγραμμο με μία γωνία $\vartheta = 1^o31'40''$, εμβαδού περίπου ένα.

Το τέχνασμα δούλεψε επειδή το τετράγωνο ενός ακέραιου υπολείπεται του γινομένου δύο ακέραιων κατά ένα. Τέτοιους ακέραιους βρίσκουμε στην ακολουθία του Fibonacci. Από τον τύπο του Cassini, έχουμε

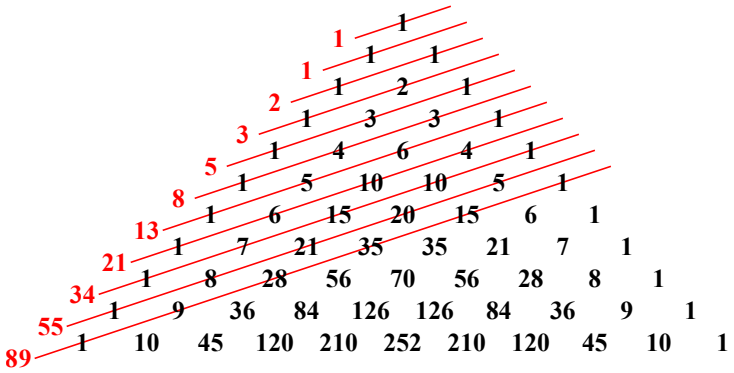
$$F_nF_{n+2} - F_{n+1}^2 = (-1)^{n+1}.$$

Επομένως για $n = 2k - 1$ ισχύει:

$$F_{2k-1}F_{2k+1} - F_{2k}^2 = 1.$$

Στο παράδοξο χρησιμοποιήθηκε ο τύπος για $k = 3$. Θα μπορούσαμε να «αποδείξουμε» κάτι αντίστοιχο για κάθε k. Για παράδειγμα, για $k = 4$, έχουμε τετράγωνο πλευράς 21 και το ορθογώνιο διαστάσεων 34 και 13.

Η επόμενη πρόταση συνδέει τους αριθμούς Fibonacci με τους διωνυμικούς συντελεστές και αποδείχθηκε στα 1876 από τον Γάλλο μαθηματικό Lucas.



Σχήμα 6.1.6: Αριθμοί Fibonacci και το τρίγωνο του Pascal, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons `https://commons.wikimedia.org/wiki/File:PascalTriangleFibanacci.svg`

Πρόταση 6.1.2. *Για κάθε $m \geq 0$ ισχύει*

$$F_{m+1} = \sum_{i=0}^{m} \binom{m-i}{i},$$

όπου $\binom{u}{v} = 0$, όταν $u < v$.

Απόδειξη. Ας ονομάσουμε

$$A_{m+1} := \sum_{i=0}^{m} \binom{m-i}{i}.$$

Για $m = 0$ έχουμε $A_1 = 1$ και για $m = 1$ επίσης $A_2 = \binom{1}{0} + \binom{0}{1} = 1 + 0 = 1$. Τώρα για κάθε $m \geq 0$ ισχύει

$$A_{m+3} = \sum_{i=0}^{m+2} \binom{m+2-i}{i} = \sum_{i=0}^{m+2} \left(\binom{m+1-i}{i} + \binom{m+1-i}{i-1} \right) =$$

$$= \sum_{i=0}^{m+1} \binom{m+1-i}{i} + \sum_{j=0}^{m} \binom{m-j}{j} = A_{m+2} + A_{m+1}.$$

Συνεπώς για κάθε $m \geq 0$ έχουμε $F_{m+1} = A_{m+1}$. □

Είναι σε όλους γνωστό ότι οι διωνυμικοί συντελεστές μπορούν να παρασταθούν από το τρίγωνο του Pascal. Μία γεωμετρική ερμηνεία του θεωρήματος του Lucas είναι ότι το άθροισμα των όρων του τριγώνου Pascal κατά τη βορειοανατολική κατεύθυνση, μας δίνει την ακολουθία των αριθμών Fibonacci.

6.1.2 Αριθμοθεωρητικές ιδιότητες

Στη συνέχεια θα εξετάσουμε μερικές αριθμοθεωρητικές ιδιότητες των αριθμών Fibonacci.

Πρόταση 6.1.3. *Για κάθε $m, n \in \mathbb{N}$ ισχύουν:*

1. *Αν $m|n$, τότε $F_m|F_n$.*
2. *Μ.Κ.Δ.$(F_n, F_{n+1}) = 1$.*
3. *Μ.Κ.Δ.$(F_n, F_m) = F_{\text{Μ.Κ.Δ.}(m,n)}$.*

Απόδειξη. 1. Επειδή $m|n$, έπεται ότι $n = mm_1$ για κάποιο $m_1 \in \mathbb{N}$. Εφαρμόζουμε μαθηματική επαγωγή ως προς m_1. Για $m_1 = 0$, έχουμε $n = 0$, δηλαδή $F_0 = 0$ ο οποίος διαιρείται από κάθε F_m. (Αν $m_1 = 1$ τότε $m = n$ οπότε και $F_m = F_n|F_n$.)

Υποθέτουμε ότι η πρόταση ισχύει για τον m_1, δηλαδή ότι $F_m|F_{mm_1}$. Θα αποδείξουμε ότι ισχύει και για $m_1 + 1$. Πράγματι

$$F_{m(m_1+1)} = F_{mm_1+m} = F_{mm_1-1}F_m + F_{mm_1}F_{m+1}.$$

Συνεπώς $F_m|F_{m(m_1+1)}$.

2. Υποθέτουμε ότι $(F_n, F_{n+1}) = d > 1$. Επομένως $d|F_{n-1} = F_{n+1} - F_n$. Όμοια συμπεραίνουμε ότι $d|F_{n-2}$ και, συνεχίζοντας επαγωγικά, τελικά καταλήγουμε ότι θα πρέπει $d|F_1 = 1$, άτοπο. Άρα $d = 1$.

3. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $m > n$. Εφαρμόζουμε διαδοχικά τον ευκλείδειο αλγόριθμο:

$$m = nq_0 + r_1, \text{ όπου } 0 \le r_1 < n,$$

$$n = r_1q_1 + r_2, \text{ όπου } 0 \le r_2 < r_1,$$

$$r_1 = r_2q_2 + r_3, \text{ όπου } 0 \le r_3 < r_2,$$

$$\dots$$

$$r_{t-2} = r_{t-1}q_{t-1} + r_t, \text{ όπου } 0 \le r_t < r_{t-1}$$

$$r_{t-1} = r_tq_t \text{ και } r_t = (m, n).$$

Επομένως για τους αντίστοιχους αριθμούς Fibonacci έχουμε,

$$(F_m, F_n) = (F_{nq_0+r_1}, F_n) = (F_{nq_0-1}F_{r_1} + F_{nq_0}F_{r_1+1}, F_n) =$$

$$= (F_{nq_0-1}F_{r_1}, F_n) = (F_{r_1}, F_n),$$

διότι, λόγω της 2.,

$$(F_n, F_{nq_0-1})|(F_{nq_0}, F_{nq_0-1}) = 1.$$

Εντελώς όμοια αποδεικνύεται ότι

$$(F_{r_1}, F_n) = (F_{r_2}, F_n),$$

$$(F_{r_2}, F_{r_1}) = (F_{r_3}, F_{r_2}),$$

$$\dots$$

$$(F_{r_{t-1}}, F_{r_{t-2}}) = (F_{r_t}, F_{r_{t-1}}).$$

Λόγω της ιδιότητας 1., επειδή $F_{r_t}|F_{r_{t-1}}$, έπεται ότι $(F_{r_t}, F_{r_{t-1}}) = F_{r_t}$.

Συνεπώς

$$(F_m, F_n) = (F_{r_t}, F_{r_{t-1}}) = F_{r_t} = F_{(m,n)}.$$

□

Παρατηρήσεις

1. Από την Πρόταση 6.1.3 προκύπτει αμέσως ότι για $m, n \in \mathbb{N}$ και $m \geq 3$ ισχύει

$$m|n \iff F_m|F_n.$$

Απόδειξη. Η μία κατεύθυνση έχει ήδη αποδειχθεί στην Πρόταση 6.1.3. Θα αποδείξουμε και την αντίστροφη. Υποθέτουμε ότι $F_m|F_n$. Επομένως $(F_m, F_n) = F_m$. Η 3). της Πρότασης 6.1.3 μας δίνει ότι $(F_m, F_n) = F_{(m,n)}$. Συνεπώς $F_{(m,n)} = F_m$. Επειδή η ακολουθία των αριθμών Fibonacci είναι, για $m \geq 3$, γνήσια αύξουσα, έπεται ότι $m = (m, n)$, δηλαδή $m|n$. □

Επομένως

$$2|F_n \iff 3|n,$$

$$3|F_n \iff 4|n,$$

$$5|F_n \iff 5|n,$$

$$8|F_n \iff 6|n,$$

κ.λ.π.

2. Συχνά επεκτείνουμε την ακολουθία των αριθμών Fibonacci και για αρνητικούς δείκτες κάτι που, όπως θα δούμε, θα μας είναι ιδιαίτερα χρήσιμο στα επόμενα. Εδώ μόνο να παρατηρήσουμε ότι ισχύει $F_{-n} = (-1)^{n-1}F_n$ και ότι η αλήθεια της πρότασης 6.1.3 ισχύει για οποιουσδήποτε ακέραιους m και n .

Πρόταση 6.1.4. *Αν F_{n+1} και F_{n+2} (για $n > 1$) δύο διαδοχικοί όροι της ακολουθίας Fibonacci, τότε ο ευκλείδειος αλγόριθμος χρειάζεται ακριβώς n βήματα για να πιστοποιήσει ότι $(F_{n+1}, F_{n+2}) = 1$.*

Απόδειξη. Απλά αρκεί να παρατηρήσουμε ότι,

$$F_{n+2} = F_{n+1} \cdot 1 + F_n \text{ και } 0 < F_n < F_{n+1},$$

$$F_{n+1} = F_n \cdot 1 + F_{n-1} \text{ και } 0 < F_{n-1} < F_n,$$

$$\dots$$

$$F_4 = F_3 \cdot 1 + F_2 \text{ και } 0 < F_2 < F_3,$$

$$F_3 = F_2 \cdot 2 + 0$$

□

Στη συνέχεια θα εκτιμήσουμε το μέγεθος (πλήθος ψηφίων) του αριθμού F_n στο δεκαδικό σύστημα αρίθμησης. Συγκεκριμένα θα αποδείξουμε την

Πρόταση 6.1.5. *Για κάθε φυσικό αριθμό $m \geq 1$ υπάρχουν τουλάχιστον 4 και το πολύ 5 αριθμοί Fibonacci με πλήθος δεκαδικών ψηφίων ίσο με m.*

Απόδειξη. Η απόδειξη θα γίνει επαγωγικά ως προς m. Για $m = 1$ οι μοναδικοί μονοψήφιοι αριθμοί Fibonacci είναι οι $1, 2, 3, 5$ και 8. Υποθέτουμε ότι η πρόταση ισχύει για κάποιο m. Αν F_n ο μικρότερος αριθμός Fibonacci με πλήθος δεκαδικών ψηφίων μεγαλύτερο του m, τότε:

$$F_n = F_{n-1} + F_{n-2} < 1 \cdot 10^m + 1 \cdot 10^m = 2 \cdot 10^m,$$

$$F_{n+1} = F_n + F_{n-1} < 2 \cdot 10^m + 1 \cdot 10^m = 3 \cdot 10^m,$$

$$F_{n+2} = F_{n+1} + F_n < 3 \cdot 10^m + 2 \cdot 10^m = 5 \cdot 10^m \text{ και}$$

$$F_{n+3} = F_{n+2} + F_{n+1} < 5 \cdot 10^m + 3 \cdot 10^m = 8 \cdot 10^m.$$

Άρα, οι $F_n, F_{n+1}, F_{n+2},$ και F_{n+3} έχουν όλοι τους $(m+1)$- δεκαδικά ψηφία.
Από την άλλη μεριά, λόγω της ανισότητας $10^m \leq F_n = F_{n-1} + F_{n-2} < 2F_{n-1}$, προκύπτει ότι $F_{n-1} > \frac{1}{2} \cdot 10^m$. Επομένως

$$F_{n+1} = F_n + F_{n-1} > 10^m + \frac{1}{2} \cdot 10^m = \frac{3}{2} \cdot 10^m,$$

$$F_{n+2} = F_{n+1} + F_n > \frac{3}{2} \cdot 10^m + 10^m = \frac{5}{2} \cdot 10^m,$$

$$F_{n+3} = F_{n+2} + F_{n+1} > \frac{5}{2} \cdot 10^m + \frac{3}{2} 10^m = \frac{8}{2} \cdot 10^m,$$

$$F_{n+4} = F_{n+3} + F_{n+2} > \frac{8}{2} \cdot 10^m + \frac{5}{2} 10^m = \frac{13}{2} \cdot 10^m, \text{ και}$$

$$F_{n+5} = F_{n+4} + F_{n+3} > \frac{13}{2} \cdot 10^m + \frac{8}{2} 10^m = \frac{21}{2} \cdot 10^m.$$

Η τελευταία ανισότητα μας δίνει $F_{n+5} > 10^{m+1}$. Συνεπώς ο F_{n+5} έχει τουλάχιστον $(m+2)$ δεκαδικά ψηφία, δηλαδή υπάρχουν το πολύ πέντε αριθμοί Fibonacci με πλήθος δεκαδικών ψηφίων $(m+1)$. □

Άμεση συνέπεια της Πρότασης 6.1.5 είναι το ακόλουθο

Πόρισμα 6.1.6. *Αν ο n-στός αριθμός Fibonacci έχει πλήθος δεκαδικών ψηφίων m, τότε $n \leq 5m+1$.*

Απόδειξη. Επαγωγικά ως προς m. Για $m = 1$ έχουμε $F_6 = 8$ και $F_7 = 13$, δηλαδή ισχύει. Υποθέτουμε ότι ισχύει για όλους τους φυσικούς τους μικρότερους ή ίσους του m. Αν τώρα ο F_n έχει $(m+1)$-ψηφία ο F_{n-5}, σύμφωνα με την Πρόταση 6.1.5, θα έχει το πολύ m-ψηφία οπότε, λόγω της υπόθεσης της μαθηματικής επαγωγής, έχουμε $n - 5 \leq 5m + 1$, δηλαδή $n \leq 5(m+1) + 1$. □

Οι αριθμοί Fibonacci είναι χρήσιμοι και στην εκτίμηση των βημάτων του ευκλείδειου αλγόριθμου για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο ακέραιων. Το επόμενο θεώρημα αποδείχθηκε από τον Lame, μαθηματικό του 19ου αιώνα, γνωστού κυρίως από την απόδειξη (στα 1840) της *«Εικασίας Fermat»* για εκθέτη 7.

Θεώρημα 6.1.7. *Αν $a, b \in \mathbb{N}, a > 0, b > 0$ και $\pi(a, b)$ το πλήθος των διαιρέσεων του ευκλείδειου αλγορίθμου για τον υπολογισμό του μέγιστου κοινού διαιρέτη των a, b , τότε ισχύει $\pi(a, b) \leq 5\psi(b)$, όπου $\psi(b)$ το πλήθος των δεκαδικών ψηφίων του b.*

Απόδειξη. Επειδή η ακολουθία αριθμών Fibonacci τείνει στο άπειρο, έπεται ότι υπάρχει κάποιος φυσικός αριθμός n τέτοιος ώστε $F_n \leq b < F_{n+1}$. Θα αποδείξουμε, με μαθηματική επαγωγή ως προς b, ότι $\pi(a,b) \leq n-1$. Αν $b = 1$, τότε $F_2 = 1 \leq b < F_3 = 2$ ισχύει. Αν τώρα $b > 1$ και $a = bq + r$, με $0 \leq r < b$ τότε $\pi(a,b) = \pi(b,r) + 1$. Στη συνέχεια ξεχωρίζουμε δύο περιπτώσεις: Αν $r < F_n$ τότε, λόγω της υπόθεσης της μαθηματικής επαγωγής, ισχύει $\pi(b,r) \leq n-2$, οπότε και $\pi(a,b) \leq n-1$. Αν πάλι $F_n \leq r < b < F_{n+1}$ τότε, από τη σχέση $b = rq_1 + s$, με $0 \leq s < r$ προκύπτει ότι $s < F_{n+1}$. Πράγματι, αν ίσχυε $s \geq F_{n+1}$, θα είχαμε

$$F_{n+1} > b = q_1 r + s \geq r + s \geq F_n + F_{n-1} = F_{n+1},$$

άτοπο. Επομένως, λόγω της υπόθεσης της μαθηματικής επαγωγής, έχουμε $\pi(r,s) \leq n-3$ από την οποία έπεται ότι

$$\pi(a,b) = \pi(r,s) + 2 \leq (n-3) + 2 = n-1.$$

Συνεπώς αποδείξαμε ότι αν $F_n \leq b < F_{n+1}$ και ο F_n έχει m δεκαδικά ψηφία τότε, λόγω του πορίσματος,

$$\pi(a,b) \leq n-1 \leq 5m \leq 5\psi(b).$$

□

Στη συνέχεια θα μελετήσουμε την περιοδικότητα της ακολουθίας των αριθμών Fibonacci ως προς μέτρο κάποιο φυσικό αριθμό m, $m \neq 0$.

Πρόταση 6.1.8. *Η ακολουθία των αριθμών Fibonacci είναι περιοδική $(mod m)$, για κάθε μη-μηδενικό φυσικό αριθμό m. Επίσης υπάρχει τουλάχιστον ένας από τους $F_1, F_2, \ldots, F_{m^2}$ ο οποίος να είναι διαιρετός με m.*

Απόδειξη. Με $\overline{k}$, θα συμβολίζουμε τον ελάχιστο φυσικό αντιπρόσωπο της κλάσης $k(mod m)$ δηλαδή τον ελάχιστο φυσικό για τον οποίο $\overline{k} \equiv k(mod m)$. Σχηματίζουμε τα ζευγάρια

$$\langle \overline{F}_1, \overline{F}_2 \rangle, \langle \overline{F}_2, \overline{F}_3 \rangle, \langle \overline{F}_3, \overline{F}_4 \rangle, \ldots, \langle \overline{F}_n, \overline{F}_{n+1} \rangle, \ldots$$

Το πλήθος των δυνατών, διαφορετικών μεταξύ τους, ζευγαριών είναι m^2. Έστω $\langle \overline{F}_k, \overline{F}_{k+1} \rangle$ το πρώτο ζευγάρι το οποίο εμφανίζεται στην ακολουθία για δεύτερη φορά. Θα αποδείξουμε ότι αυτό είναι το $\langle \overline{1}, \overline{1} \rangle$. Αν ήταν κάποιο άλλο ζευγάρι, έστω το $\langle \overline{F}_k, \overline{F}_{k+1} \rangle$ για κάποιο $k > 1$ τότε θα υπήρχε $l > k$ τέτοιο ώστε

$$\langle \overline{F}_l, \overline{F}_{l+1} \rangle = \langle \overline{F}_k, \overline{F}_{k+1} \rangle.$$

Επειδή $F_{l-1} = F_{l+1} - F_l$ και $F_{k-1} = F_{k+1} - F_k$ έπεται ότι $\overline{F}_{l-1} = \overline{F}_{k-1}$ δηλαδή

$$\langle \overline{F}_{l-1}, \overline{F}_l \rangle = \langle \overline{F}_{k-1}, \overline{F}_k \rangle.$$

το οποίο είναι άτοπο, αφού το $\langle \overline{F}_k, \overline{F}_{k+1} \rangle$ είναι το πρώτο ζευγάρι το οποίο εμφανίζεται για δεύτερη φορά. Επομένως το $\langle \overline{1}, \overline{1} \rangle$ είναι το πρώτο επανεμφανιζόμενο ζευγάρι και συνεπώς η ακολουθία είναι περιοδική.
Από τη σχέση

$$\langle \overline{F}_t, \overline{F}_{t+1} \rangle = \langle \overline{1}, \overline{1} \rangle.$$

έπεται ότι $F_t \equiv 1(mod m)$ και $F_{t+1} \equiv 1(mod m)$. Συνεπώς $F_{t-1} = F_{t+1} - F_t \equiv 0(mod m)$,δηλαδή $m | F_{t-1}$.

□

Ορισμός 6.1.9. Ο δείκτης t του μικρότερου (θετικού) αριθμού Fibonacci F_t για τον οποίο ισχύει $m|F_t$, θα λέγεται *σημεία εισόδου* (entry point) του αριθμού m.

Στη συνέχεια θα περιοριστούμε στην περίπτωση που ο m είναι πρώτος αριθμός.

Πρόταση 6.1.10. *Για κάθε πρώτο $p > 5$ ισχύει $p|F_{p-1}$ ή $p|F_{p+1}$.*

Απόδειξη. Σύμφωνα με τους τύπους του Binet

$$F_n = \frac{a^n - b^n}{a-b} = \frac{1}{\sqrt{5}}\{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n\},$$

Υπολογίζουμε το διωνυμικό ανάπτυγμα των a^n και b^n, όπου $a = \frac{1+\sqrt{5}}{2}$ και $b = \frac{1-\sqrt{5}}{2}$. και αφαιρούμε. Συνεπώς έχουμε,

$$F_n = \frac{1}{2^n\sqrt{5}}\left[1 + \binom{n}{1}\sqrt{5} + \binom{n}{2}\sqrt{5}^2 + \ldots + \binom{n}{n}\sqrt{5}^n\right] +$$

$$-\frac{1}{2^n\sqrt{5}}\left[1 - \binom{n}{1}\sqrt{5} + \binom{n}{2}\sqrt{5}^2 - \ldots + (-1)^n\binom{n}{n}\sqrt{5}^n\right].(*)$$

Εφαρμόζουμε τη σχέση (*) για $n = p$:

$$F_p = \frac{1}{2^{p-1}}\left[\binom{p}{1} + \binom{p}{3}5 + \binom{p}{5}5^2 + \ldots + \binom{p}{p}5^{\frac{p-1}{2}}\right].$$

Επειδή, ως γνωστό, ισχύει $\binom{p}{k} \equiv 0(\mathrm{mod}p)$ για κάθε k, $1 \leq k \leq p-1$ και, σύμφωνα με το μικρό Θεώρημα του Fermat, $2^{p-1} \equiv 1(\mathrm{mod}p)$ έπεται ότι

$$F_p \equiv 2^{p-1}F_p \equiv \binom{p}{p}5^{\frac{p-1}{2}} \equiv 5^{\frac{p-1}{2}}(\mathrm{mod}p).$$

Όμως, σύμφωνα με το θεώρημα του Euler, έχουμε $5^{\frac{p-1}{2}} \equiv (\frac{5}{p}) \equiv \pm 1(\mathrm{mod}p)$, δηλαδή $F_p^2 \equiv 1(mod p)$. Στη συνέχεια από τον τύπο του Cassini προκύπτει ότι

$$F_p^2 = F_{p-1}F_{p+1} + (-1)^{p-1} = F_{p-1}F_{p+1} + 1$$

ο οποίος ως ισοτιμία γράφεται $F_{p-1}F_{p+1} \equiv 0(\mathrm{mod}p)$, δηλαδή $p|F_{p-1}$ είτε $p|F_{p+1}$. Δεν είναι δυνατό ο p να διαιρεί και τους δύο συγχρόνως, διότι τότε θα διαιρούσε και τον $(F_{p-1}, F_{p+1}) = F_{(p-1,p+1)} = F_2 = 1$, άτοπο. □

Παρατήρηση. Βέβαια δεν είναι πάντοτε οι αριθμοί $p-1$ ή $p+1$ και σημεία εισόδου του πρώτου αριθμού p. Για παράδειγμα, ο $13|F_{14} = 377$ αλλά και $13|F_7 = 13$.

Εντελώς φυσικό θεωρείται το ερώτημα. Πότε ισχύει η μία διαιρετότητα και πότε η άλλη ; Είναι δυνατό να χαρακτηρίσουμε τις δύο περιπτώσεις ; Η απάντηση είναι θετική. Εφαρμόζουμε τη σχέση (*) για $n = p+1$ και έχουμε

$$2^p F_{p+1} = \left[\binom{p+1}{1} + \binom{p+1}{3}5 + \binom{p+1}{5}5^2 + \ldots + \binom{p+1}{p}5^{\frac{p-1}{2}}\right].$$

Επειδή, $p|\binom{p+1}{k}$ για κάθε k, $3 \leq k \leq p-1$, έχουμε

$$2^p F_{p+1} \equiv 1 + (\frac{5}{p})(mod p).$$

Από την τελευταία ισοτιμία συμπεραίνουμε ότι,

$$p|F_{p+1} \text{ ακριβώς τότε όταν } (\frac{5}{p}) = -1.$$

Η παραπάνω πρόταση μπορεί επομένως να γραφεί στη μορφή:

Πρόταση 6.1.11. *Αν p πρώτος, τότε ισχύει η ισοτιμία, $F_{p-\varepsilon_p} \equiv 0(\mathrm{mod} p)$, όπου $\varepsilon_p := (\frac{p}{5})$.*

Απόδειξη. Η αλήθεια της πρότασης είναι άμεση συνέπεια της πρότασης 6.1.8, του σχολίου που ακολούθησε και της επαλήθευσης ότι ισχύει και για $p = 2, 3, 5$. (Το σύμβολο $\varepsilon_p = (\frac{p}{5})$ είναι το σύμβολο Kronecker, για p περιττό ταυτίζεται με το σύμβολο του Legendre και για $p = 2$, $\left(\frac{5}{2}\right) = -1$.) □

Το ερώτημα είναι αν ισχύει και το αντίστροφο. Θα είχαμε ένα, ακόμη, κριτήριο πιστοποίησης πρώτων αριθμών. Θα ήταν πολύ ωραίο για να είναι αληθινό. Όμως ο αριθμός 323 δεν είναι πρώτος αλλά επαληθεύει το συμπέρασμα της πρότασης 6.1.11.

Ορισμός 6.1.12. Ένας φυσικός αριθμός n θα λέγεται *ψευδοπρώτος Fibonacci*, όταν επαληθεύει το συμπέρασμα της πρότασης 6.1.11 και είναι *σύνθετος*.

Το θέμα είναι πολύ ενδιαφέρον, αλλά θα επανέλθουμε σε επόμενη παράγραφο στην οποία θα το εξετάσουμε στη γενικότητά του.

Θα κλείσουμε την παράγραφο με μία ακόμη ιδιότητα της ακολουθίας.

Ορισμός 6.1.13. Μία ακολουθία θετικών ακέραιων θα λέγεται *πλήρης* όταν κάθε θετικός ακέραιος m μπορεί να παρασταθεί ως άθροισμα όρων της ακολουθίας και κάθε όρος της ακολουθίας μπορεί να χρησιμοποιηθεί το πολύ μία φορά στην παράσταση του m.

Πρόταση 6.1.14. *Η ακολουθία Fibonacci $F_n, (n \geq 1)$ είναι πλήρης.*

Απόδειξη. Από την Πρόταση 6.1.1,1. έχουμε

$$F_n - 1 = F_1 + F_2 + \ldots + F_{n-2}.$$

Πρώτα απ' όλα παρατηρούμε ότι για $3 \leq n \leq 6$ κάθε ακέραιος $m = 1, 2, 3, \ldots, F_n - 1$ μπορεί να παρασταθεί ως άθροισμα κάποιων εκ των αριθμών Fibonacci. Πράγματι για $n = 3$ έχουμε

$$F_n = F_3 = 2, F_{n-1} = F_2 = 1, F_{n-2} = F_1 = 1,$$

για $n = 4$ έχουμε

$$F_n = F_4 = 3, F_{n-1} = F_3 = 2, F_{n-2} = F_2 = 1,$$

δηλαδή $F_1 = 1, F_1 + F_2 = 2$ κ.λ.π.. Όμοια και για $n = 5$ και $n = 6$.
Υποθέτουμε τώρα ότι κάθε ακέραιος $m = 1, 2, 3, \ldots, F_k - 1, (k \geq 3)$ μπορεί να παρασταθεί ως άθροισμα των αριθμών Fibonacci $F_1, F_2, \ldots, F_{k-2}$. Θα αποδείξουμε ότι κάθε ακέραιος $m =$

$1, 2, 3, \ldots, F_{k+1} - 1$, μπορεί να παρασταθεί ως άθροισμα κάποιων από τους $F_1, F_2, \ldots F_{k-1}, (k \geq 4)$. Αν σε κάθε δοσμένη παράσταση προσθέσουμε το F_{k-1} θα έχουμε

$$1 + F_{k-1}, 2 + F_{k-1}, \ldots, F_k - 1 + F_{k-1} = F_{k+1} - 1.$$

Έτσι πετυχαίνουμε την παράσταση των διαδοχικών θετικών ακέραιων $1, 2, 3, \ldots, F_k - 1$ και $1 + F_{k-1}, 2 + F_{k-1}, 3 + F_{k-1}, \ldots, F_{k+1} - 1$. Δεν υπάρχουν παραλείψεις ανάμεσα στους $F_k - 1$ και $1 + F_{k-1}$ διότι για $k = 3$ έχουμε $F_k - 1 = 1$ και $1 + F_{k-1} = 2$, για $k = 4$ ισχύει $F_k - 1 = 2$ και $1 + F_{k-1} = 3$, ενώ για $k \geq 5$ ισχύει $F_k - 1 \geq 1 + F_{k-1}$,αφού $F_k - F_{k-1} \geq 2$.

□

6.2 Αριθμοί Lucas

Εάν τώρα αλλάξουμε τα αρχικά δεδομένα της ακολουθίας Fibonacci και θέσουμε $L_0 = 2$ και $L_1 = 1$, προκύπτει μία καινούρια αναδρομική ακολουθία η οποία ορίστηκε και μελετήθηκε αρχικά από τον Γάλλο μαθηματικό Francois Edouard Lucas (1842-1891). Μάλιστα πήρε το όνομά του.

Ορισμός 6.3.1. Η αναδρομική ακολουθία ακέραιων $L_0 = 2, L_1 = 1$ και $L_{n+2} = L_{n+1} + L_n$ για κάθε $n \in \mathbb{N}$, λέγεται *ακολουθία Lucas*.

Σημείωση. Υπενθυμίζουμε ότι ο Lucas ήταν ο πρώτος που ονόμασε την ακολουθία που μόλις μελετήσαμε, ακολουθία Fibonacci.

Για την ακολουθία Lucas ισχύουν ανάλογες ιδιότητες αυτής των αριθμών Fibonacci. Επεκτείνουμε την ακολουθία και προς τα αριστερά, για εκθέτες αρνητικούς ακέραιους. Θα αναφέρουμε μερικές ιδιότητες χωρίς απόδειξη. Ισχύουν για κάθε $n \in \mathbb{Z}$. Ο πρώτος είναι γνωστός ως τύπος Binet.

$$L_n = a^n + b^n = \left(\frac{1 + \sqrt{5}}{2}\right)^n + \left(\frac{1 - \sqrt{5}}{2}\right)^n, \tag{6.3.1}$$

$$F_{2n} = F_n L_n, \tag{6.3.2}$$

$$L_n = F_{n-1} + F_{n+1}, \tag{6.3.3}$$

$$L_{-n} = (-1)^n L_n \tag{6.3.4}$$

$$(L_{n+2}, L_{n+1}) = 1, \tag{6.3.5}$$

$$2 \mid L_n \iff 3 \mid n, \tag{6.3.6}$$

$$L_1 + L_2 + \ldots + L_n = L_{n+2} - 3, \tag{6.3.7}$$

$$L_1^2 + L_2^2 + \ldots + L_n^2 = L_n L_{n+1} - 2, \tag{6.3.8}$$

$$L_n^2 = L_{2n} + 2(-1)^n, \tag{6.3.9}$$

$$(F_n, L_n) = \begin{cases} 1, & \text{όταν } 3 \nmid n \\ 2, & \text{όταν } 3 \mid n \end{cases} \tag{6.3.10}$$

Επίσης αποδεικνύεται ότι η ακολουθία Lucas $L_{n-1}, n \geq 0$ είναι πλήρης.

Πρόταση 6.3.2. *Για κάθε ακέραιο n, ισχύει,*

$$L_n^2 - 5F_n^2 = (-1)^n 4. \tag{6.3.11}$$

Απόδειξη. Από τους τύπους του Binet $L_n = a^n + b^n$ και $F_n = \frac{1}{\sqrt{5}}(a^n - b^n)$ έπεται ότι $a^n = \frac{1}{2}(L_n + F_n\sqrt{5})$ και $b^n = \frac{1}{2}(L_n - F_n\sqrt{5})$. Επομένως $\frac{1}{4}(L_n^2 - 5F_n^2) = (ab)^n$ οπότε και $L_n^2 - 5F_n^2 = 4(-1)^n$. □

Σημείωση. Η πρόταση αυτή μπορεί να διατυπωθεί και ως εξής: Τα ζευγάρια

$$(L_n, F_n), n \in \mathbb{Z}$$

είναι λύσεις της διοφαντικής εξίσωσης

$$X^2 - 5Y^2 = 4(-1)^n.$$

Η εξίσωση αυτή λέγεται *εξίσωση του Pell*, είναι πολύ σημαντική και θα μελετηθεί σε ξεχωριστό κεφάλαιο του δεύτερου μέρους.
Αργότερα θα αποδείξουμε ότι ισχύει και το αντίστροφο, δηλαδή ότι αυτές είναι *όλες* οι λύσεις της εξίσωσης αυτής.

Μια εικασία σχετικά με τους αριθμούς Fibonacci ήταν ότι οι μοναδικοί αριθμοί που είναι τέλειο τετράγωνο είναι οι 0, 1, 144. Η εικασία αυτή αποδείχθηκε από τον J.H.E.Cohn [2], [1] στα 1964. Για να την αποδείξουμε χρειαζόμαστε ακόμη μερικές ταυτότητες των αριθμών Fibonacci και Lucas.

$$2F_{m+n} = F_mL_n + F_nL_m, \tag{6.3.12}$$
$$2L_{m+n} = 5F_mF_n + L_mL_n, \tag{6.3.13}$$
$$2 \mid L_m \iff 3 \mid m, \tag{6.3.14}$$
$$3 \mid L_m \iff m \equiv 2(mod4), \tag{6.3.15}$$

Οι επόμενες ισχύουν υπό τις προϋποθέσεις $2 \mid k$ και $3 \nmid k$

$$L_k \equiv 3(\text{mod}4), \tag{6.3.16}$$
$$L_{m+2k} \equiv -L_m(\text{mod}L_k), \tag{6.3.17}$$
$$F_{m+2k} \equiv -F_m(\text{mod}L_k), \tag{6.3.18}$$
$$L_{m+12} \equiv L_m(\text{mod}8). \tag{6.3.19}$$

Απόδειξη. Εδώ θα περιγράψουμε τις ιδέες των αποδείξεων των ιδιοτήτων αυτών. Οι πρώτες δύο αποδεικνύονται με τη βοήθεια των τύπων Binet. Οι επόμενες δύο όπως και οι αντίστοιχες για τους αριθμούς Fibonacci. Επειδή $3 \nmid k$, έπεται ότι $2 \nmid L_k$. Επομένως για $2 \mid k$ η (6.3.9) γράφεται $L_{\frac{k}{2}}^2 = L_k + 2(-1)^{\frac{k}{2}}$, και συνεπώς $L_k \equiv 3(\text{mod}4)$. Από την πρώτη σχέση προκύπτει για $n = 2k$ ότι

$$2F_{m+2k} = F_mL_{2k} + F_{2k}L_m = F_m(L_k^2 + (-1)^{k-1}2) + F_kL_kL_m \equiv -2F_m(\text{mod}L_k).$$

Επειδή $2 \nmid k$, έχουμε

$$F_{m+2k} \equiv -F_m(\text{mod}L_k).$$

Ανάλογα αποδεικνύεται και η (6.3.18). Τέλος, η (6.3.19) είναι απλή γενίκευση του γεγονότος ότι η ακολουθία Lucas είναι περιοδική (mod8) με μήκος περιόδου 12. □

Πρόταση 6.3.3. *1. Αν ο L_n είναι τέλειο τετράγωνο, τότε κατ' ανάγκη $n = 1$ ή $n = 3$.*

2. Αν ο L_n είναι το διπλάσιο τέλειου τετραγώνου, τότε κατ' ανάγκη $n = 0$ ή $n = \pm 6$.

Απόδειξη. 1. Αν ο n είναι άρτιος τότε η (6.3.9) δίνει

$$L_n = y^2 \pm 2 \neq x^2.$$

Αν $n \equiv 1(\text{mod}4)$, τότε $L_1 = 1$, ενώ αν $n \neq 1$, τότε γράφουμε $n = 1 + 2 \cdot 3^r \cdot k$ και από την (6.3.17) επεται ότι

$$L_n \equiv -L_1 \equiv -1(\text{mod}L_k),$$

οπότε για $L_n = x^2$ προκύπτει ότι $x^2 \equiv -1(\text{mod}L_k)$, η οποία, λόγω της (6.3.16), δεν έχει λύση.
Αν τώρα $n \equiv 3(\text{mod}4)$, τότε για $n = 3$ δίνει τη λύση $L_3 = 2^2$ ενώ για $n > 3$ γράφουμε $n = 3 + 2 \cdot 3^r \cdot k$ και έχουμε

$$L_n \equiv -L_3 \equiv -4(\text{mod}L_k),$$

από την οποία προκύπτει, όπως παραπάνω, ότι ο L_n δεν είναι τέλειο τετράγωνο.

2. Αν ο n είναι περιττός και ο L_n άρτιος τότε, λόγω της (6.3.12) , έχουμε $n \equiv \pm 3(\text{mod}12)$. Από την (6.3.16), σε συνδυασμό με την (6.3.4), προκύπτει $L_n \equiv 4(\text{mod}8)$. Άν ήταν $L_n = 2x^2$ θα είχαμε $2x^2 \equiv 4(\text{mod}8)$, δηλαδή $x^2 \equiv 2(\text{mod}4)$, το οποίο είναι άτοπο.
Αν $n \equiv 0 \pmod 4$, τότε για $n = 0$ έχουμε τη λύση $L_0 = 2$, ενώ για $n \neq 0$ γράφουμε $n = 2 \cdot 3^r \cdot k$ και έχουμε

$$2L_n \equiv -2L_0 \equiv -4 \pmod{L_k}.$$

Αν τώρα υποθέσουμε ότι $L_n = 2x^2$ τότε ο $2L_n = (2y)^2$ θα ήταν τέλειο τετράγωνο, το οποίο όμως, λόγω της (1.14), είναι αδύνατο.
Αν $n \equiv 6 \pmod 8$ τότε για $n = 0$, έχουμε τη λύση $L_6 = 2 \cdot 3^2$, ενώ για $n \neq 6$ γράφουμε $n = 6 + 2 \cdot 3^r \cdot k$ (όπου $4 \mid k, 3 \nmid k$) βρίσκουμε

$$2L_n \equiv -2L_6 \equiv -36(mod L_k)$$

από την οποία προκύπτει, όπως παραπάνω, ότι $L_n \neq 2x^2$.
Αν τέλος $n \equiv 2(mod8) \Longrightarrow n \equiv -6(mod8)$, τότε από τη σχέση (3), έπεται ότι έχουμε μία λύση για $n = -6$ και καμμία άλλη για τις υπόλοιπες τιμές του n.

□

Πρόταση 6.3.4. *1. Αν ο F_n είναι τέλειο τετράγωνο τότε, κατ΄ ανάγκη, $n = 0, \pm 1, 2$ ή 12.*

2. Αν $F_n = 2x^2$ τότε , κατ΄ ανάγκη $n = 0, \pm 3$, ή 6.

Απόδειξη. Για το 1. Αν $n \equiv 1 \pmod 4$, τότε για $n = 1$ έχουμε τη λύση $F_1 = 1$ ενώ για $n \neq 1$ γράφουμε $n = 1 + 2 \cdot 3^r k$ και συνεπώς

$$F_n \equiv -F_1 \equiv -1 \pmod 4,$$

δηλαδή $F_n \neq x^2$.
Αν $n \equiv 3(mod4)$ από τη σχέση $F_{-n} = (-1)^{n-1}F_n$ προκύπτει ότι $-n \equiv 1 \pmod 4$ και βρίσκουμε τη λύση $n = -1$.
Αν ο n είναι άρτιος, τότε λόγω της (1.1) $F_n = F_{\frac{n}{2}}L_{\frac{n}{2}}$ και η (1.9) για $F_n = x^2$ και $3|n$ δίνει $F_{\frac{n}{2}} = 2y^2$ και $L_{\frac{n}{2}} = 2z^2$. Από την προηγούμενη πρόταση έπεται ότι $\frac{n}{2} = 0, \pm 6$, δηλαδή ότι $n = 0, \pm 12$. Οι δύο τιμές $n = 0, 12$ δίνουν λύσεις της $F_{\frac{n}{2}} = 2y^2$ ενώ η $n = -12$ όχι. Αν τέλος ο n είναι άρτιος

και 3 δεν διαιρεί το n, τότε η (1.9) δίνει $F_{\frac{n}{2}} = y^2$ και $L_{\frac{n}{2}} = z^2$. Από την προηγούμενη πρόταση και πάλι έχουμε $\frac{n}{2} = 1, 3$, δηλαδή $n = 2, 6$. Η τιμή $n = 2$ δίνει λύση της $F_{\frac{n}{2}} = y^2$, ενώ η $n = 6$ όχι.

Για το 2. Έστω ότι $n \equiv 3(mod 4)$. Αν $n = 3$ τότε έχουμε τη λύση $F_3 = 2$, ενώ για $n \neq 3$ με $n = 3 + 2 \cdot 3^r \cdot k$ με $2 \mid k$ και $3 nok$ έχουμε

$$2F_{2n} \equiv -2F_3 \equiv -4(mod L_k).$$

Έχουμε δει προηγουμένως ότι η $F_n = 2x^2$ δεν έχει λύση. Αν τώρα ο n είναι άρτιος, τότε από τη σχέση (1) $F_n = F_{\frac{n}{2}} L_{\frac{n}{2}}$ και την υπόθεση ότι $F_n = 2x^2$ προκύπτει $F_{\frac{n}{2}} = y^2$ και $L_{\frac{n}{2}} = 2z^2$. (σύμφωνα με το προηγούμενο θεώρημα και το πρώτο μέρος του παρόντος η μοναδική λύση είναι $n = 0$) ή $F_{\frac{n}{2}} = 2y^2$ και $L_{\frac{n}{2}} = z^2$, οπότε και πάλι λόγω της προηγούμενης πρότασης έχουμε $\frac{n}{2} = 1$ ή 3. Για $n = 2$ δεν ισχύει $F_{\frac{n}{2}} = 2y^2$ η οποία ισχύει για $n = 6$. □

Πρόταση 6.3.5. *Οι μοναδικοί αριθμοί Fibonacci της μορφής $F_n = c^2 + 1$ είναι αυτοί με δείκτη $n = \pm 1, 2, \pm 3, \pm 5$.*

Το πρόβλημα του προσδιορισμού των τρίγωνων αριθμών οι οποίοι είναι συγχρόνως και αριθμοί Fibonacci απαντήθηκε. Συγκεκριμένα ισχύει:

Πρόταση 6.3.6. *Οι μοναδικοί αριθμοί Fibonacci οι οποίοι είναι και τρίγωνοι αριθμοί, είναι οι $0, 1, 3, 21, 55$.*

Απόδειξη. Δείτε το άρθρο [5]. □

Στα 1969 ο H.M. Stark διατύπωσε το πρόβλημα: «Να βρεθούν όλοι οι αριθμοί Fibonacci της μορφής $F_n = \frac{1}{2}(X^3 - Y^3)$.» Ισχυρίστηκε μάλιστα ότι η απάντηση σ' αυτό είναι ισοδύναμη με ένα σημαντικό πρόβλημα αλγεβρικής Θεωρίας Αριθμών. Και αυτό το προβλημα είναι ανοιχτό.

6.3.1 Ασκήσεις

1. Αν $2 \mid F_n$, να αποδείξετε ότι $4 \mid (F_{n+1}^2 - F_{n-1}^2)$ και αν $3 \mid F_n$ τότε $9 \mid (F_{n+1}^2 - F_{n-1}^2)$

2. Για κάθε $n \geq 3$ ισχύει

$$F_{n+1}^2 = F_n^2 + 3F_{n-1}^2 + 2(F_1^2 + F_2^2 + \cdots F_{n-2}^2).$$

3. Αν $m \geq 1, n \geq 1$ και $(m, n) = 1$, τότε $F_m F_n \mid F_{mn}$.

4. Για κάθε $n \geq 1$ ισχύει

$$2^{n-1} F_n \equiv n \mathrm{mod} 5.$$

5. Να αποδείξετε ότι

$$F_{2n+2}F_{2n-1} - F_{2n}F_{2n+1} = 1, \text{ για κάθε } n \geq 1.$$

6. Να αποδείξετε ότι

   (α') $F_{n+1}^2 - 4F_nF_{n-1} = F_{n-2}^2$ για κάθε $n \geq 3$

   (β') $F_{n+1}F_{n-1} - F_{n+2}F_{n-2} = 2(-1)^n$, για κάθε $n \geq 3$

   (γ') $F_n^2 - F_{n+2}F_{n-2} = (-1)^n$, για κάθε $n \geq 3$

(δ΄) $F_n^2 - F_{n+3}F_{n-3} = 4(-1)^{n+1}$, για κάθε $n \geq 4$

(ε΄) $F_{2n-1} = F_n^2 + F_{n-1}^2$, για κάθε $n \geq 2$

7. Αν $p \in \mathbb{P}$, $p = 4k+3$ τότε η $a^2 + b^2 \equiv 0 \mathrm{mod} p$ συνεπάγεται ότι $p \mid a$ και $p \mid b$ (Αποδείξτε το ή δεχτείτε το!). Να αποδείξετε ότι αν $p \in \mathbb{P}$, $p \equiv 3 \mathrm{mod} 4$, τότε για κάθε $n \geq 1$ ισχύει $p \nmid F_{2n-1}$.

8. Να αποδείξετε ότι το γινόμενο $F_{2n-1}F_{2n+5}$ γράφεται ως άθροισμα δύο τετραγώνων.

9. Θεωρήστε κατάλληλη υπακολουθία της ακολουθίας Fibonacci και αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $4k+1$.

10. Να αποδείξετε την ταυτότητα

$$(F_nF_{n+3})^2 + (2F_{n+1}F_{n+2})^2 = F_{2n+3}^2.$$

Στη συνέχεια να υπολογίσετε 5 πρωταρχικές πυθαγόρειες τριάδες. Τέλος να αποδείξετε ότι ο αριθμός $F_nF_{n+1}F_{n+2}F_{n+3}$ είναι πάντοτε εμβαδόν ορθογωνίου τριγώνου.

6.4 Ακολουθίες Lucas.

Στην παράγραφο αυτή θα γενικεύσουμε τα προηγούμενα αποτελέσματα. Οι τύποι Binet, τόσο των αριθμών Fibonacci όσο και των αριθμών Lucas, συνδέονται άμεσα με τους αριθμούς $\alpha = \frac{1+\sqrt{5}}{2}$ και $\beta = \frac{1-\sqrt{5}}{2}$, οι οποίοι είναι οι ρίζες του δευτεροβάθμιου πολυωνύμου $x^2 - x - 1$. Θεωρούμε λοιπόν δύο ακέραιους αριθμούς a, b διάφορους του μηδενός. Οι ρίζες του πολυωνύμου $x^2 - ax + b = 0$ είναι $\alpha = \frac{a+\sqrt{D}}{2}$ και $\beta = \frac{a-\sqrt{D}}{2}$, όπου $D = a^2 - 4b$ η διακρίνουσα του πολυωνύμου. Προκειμένου να αποφύγουμε την ιδιάζουσα περίπτωση της διπλής ρίζας, υποθέτουμε ότι η διακρίνουσα $D \neq 0$. Επομένως, $\alpha + \beta = a$, $\alpha - \beta = \sqrt{D}$ και $\alpha\beta = b$. Για κάθε $n \geq 0$ ορίζουμε δύο ακολουθίες, $U_n = U_n(\alpha, \beta)_{n\in\mathbb{N}}$ και $V_n = V_n(\alpha, \beta)_{n\in\mathbb{N}}$ ως εξής:

$$U_n = U_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ και } V_n = V_n(\alpha, \beta) = \alpha^n + \beta^n$$

Οι ακολουθίες $U = (U_n(\alpha, \beta))_{n\in\mathbb{N}}$ και $V = (V_n(\alpha, \beta))_{n\in\mathbb{N}}$ θα λέγονται (πρώτη και δεύτερη αντίστοιχα) *ακολουθίες Lucas* ως προς το ζευγάρι (α, β).

Είναι φανερό ότι, $U_0(\alpha, \beta) = 0$, $V_0(\alpha, \beta) = 2$ και $U_1(\alpha, \beta) = 1$, $V_1(\alpha, \beta) = \alpha + \beta$. Επίσης εύκολα διαπιστώνεται ότι για κάθε $n \geq 2$ ισχύουν:

$$U_n(\alpha, \beta) = aU_{n-1} - bU_{n-2}, V_n(\alpha, \beta) = aV_{n-1} - bV_{n-2}.$$

Οι συνηθισμένοι αριθμοί Fibonacci και Lucas προκύπτουν ως ειδική περίπτωση (πρώτη και δεύτερη αντίστοιχα) της ακολουθίας Lucas ως προς το ζευγάρι $(a, b) = (1, -1)$.
Επεκτείνουμε τους δείκτες και για αρνητικούς ακέραιους έτσι ώστε οι αναδρομικοί τύποι να συνεχίσουν να ισχύουν: $U_{-n} = -\frac{1}{b^n}U_n$ και $V_{-n} = \frac{1}{b^n}V_n$, για κάθε $n \geq 1$.

Ιδιότητες Στη συνέχεια αναφέρουμε, χωρίς αποδείξεις, μερικές ιδιότητες των ακολουθιών

Lucas, οι οποίες αποτελούν γενικεύσεις αντίστοιχων ιδιοτήτων των αριθμών Fibonacci και Lucas.

$$V_n^2 - DU_n^2 = 4b^n, \tag{6.4.1}$$
$$DU_n = V_{n+1} - bV_{n-1}, \tag{6.4.2}$$
$$V_n = U_{n+1} - bU_{n-1}, \tag{6.4.3}$$
$$U_{m+n} = U_mV_n - b^nU_{m-n} \tag{6.4.4}$$
$$V_{m+n} = V_mV_n - b^nV_{m-n}, \tag{6.4.5}$$
$$2U_{m+n} = U_mV_n + U_nV_m, \tag{6.4.6}$$
$$2V_{m+n} = V_mV_n + DU_mU_n, \tag{6.4.7}$$
$$2b^nU_{m-n} = U_mV_n - U_nV_m, \tag{6.4.8}$$
$$U_{2n} = U_nV_n, \tag{6.4.9}$$
$$V_{2n} = V_n^2 - 2b^n, \tag{6.4.10}$$
$$U_{3n} = U_n(V_n^2 - b^n) = U_n(DU_n^2 + 3\beta^n), \tag{6.4.11}$$
$$V_{3n} = V_n(V_n^2 - 3b^n), \tag{6.4.12}$$

Για $U_m \neq 1$, ισχύει $U_m \mid U_n$ ακριβώς τότε όταν $m \mid n$. Για $V_m \neq 1$, ισχύει $V_m \mid V_n$ ακριβώς τότε όταν ($m \mid n$ και $\frac{n}{m}$ είναι *περιττός* ακέραιος). Στις επόμενες τέσσερις ιδιότητες, υποθέτουμε ότι ισχύει $(\alpha, \beta) = 1$.

$$(U_m, U_n) = U_d, \text{ όπου } d = (m, n), \tag{6.4.13}$$
$$(V_m, V_n) = \begin{cases} V_d, & \text{εάν οι } \frac{m}{d} \text{ και } \frac{n}{d} \text{ είναι περιττοί} \\ 1 \text{ ή } 2, & \text{αλλιώς,} \end{cases}, \tag{6.4.14}$$
$$(U_m, V_n) = \begin{cases} V_d, & \text{εάν ο } \frac{m}{d} \text{ είναι άρτιος και ο } \frac{n}{d} \text{ είναι περιττός} \\ 1 \text{ ή } 2, & \text{αλλιώς,} \end{cases}, \tag{6.4.15}$$

όπου $d = (m, n)$.

$$(U_m, V_n) = \begin{cases} V_d, & \text{εάν ο } \frac{m}{d} \text{ είναι άρτιος και ο } \frac{n}{d} \text{ είναι περιττός} \\ 1 \text{ ή } 2, & \text{αλλιώς,} \end{cases},$$

όπου $d = (m, n)$.
Αν $n \geq 1$, τότε $(U_n, b) = 1$ και $(V_n, b) = 1$.

Στη συνέχεια θα διατυπώσουμε μια πρόταση για τις ακολουθίες Lucas, η οποία γενικεύει τις προτάσεις 6.3.3, 6.3.4 για τους αριθμούς των Fibonacci και Lucas.

Πρόταση 6.4.1. *Υποθέτουμε ότι $a \geq 1$, ότι οι αριθμοί a, b είναι περιττοί, $(a, b) = 1$ και $D = a^2 - 4b > 0$.*

- *Αν ο U_n είναι τέλειο τετράγωνο τότε, κατ' ανάγκη, $n = 1, 2, 3, 6,$ ή 12.*
- *Αν ο V_n είναι τέλειο τετράγωνο τότε, κατ' ανάγκη, $n = 1, 3$ ή 5.*
- *Αν ο U_n είναι το διπλάσιο τέλειου τετραγώνου τότε, κατ' ανάγκη $n = 3,$ ή 6.*
- *Αν ο V_n είναι το διπλάσιο τέλειου τετραγώνου τότε, κατ' ανάγκη $n = 3,$ ή 6.*

Τέλος, θα μελετήσουμε τη διαιρετότητα των ακολουθιών Lucas από πρώτους αριθμούς. Το αποτέλεσμα, όπως θα δούμε στην επόμενη παράγραφο, έχει εφαρμογή στην πιστοποίηση πρώτων.

Πρόταση 6.4.2. *Έστω $U = (U_n(\alpha,\beta))_{n\in\mathbb{N}}$ και $V = (V_n(\alpha,\beta))_{n\in\mathbb{N}}$ οι ακολουθίες Lucas ως προς το ζευγάρι (a,b). Αν $p \in \mathbb{P}$, τέτοιος ώστε ο p να μην διαιρεί τον $2\beta D$, τότε ισχύει,*

$$U_{p-\varepsilon_p} \equiv 0(mod p),$$

όπου $\varepsilon_p := (\frac{D}{p})$.

Η πρόταση αυτή αποτελεί γενίκευση της πρότασης 6.1.11. Θα την αποδείξουμε σε μία ειδική περίπτωση. Συγκεκριμένα θα αποδείξουμε ότι

Πρόταση 6.4.3. *Αν p περιττός πρώτος τέτοιος ώστε $(\frac{D}{p}) = -1$, τότε $p \mid U_{p+1}$.*

Απόδειξη. Η απόδειξη είναι όμοια με την πρόταση 6.1.8. Υπολογίζουμε τον διωνυμικό τύπο για τις δυνάμεις

$$\alpha^n = \left(\frac{a+\sqrt{D}}{2}\right)^n = 2^{-n}\sum_{k=0}^{n}\binom{n}{k}a^{n-k}\sqrt{D}^k$$

και

$$\beta^n = \left(\frac{a-\sqrt{D}}{2}\right)^n = 2^{-n}\sum_{k=0}^{n}\binom{n}{k}a^{n-k}(-1)^k\sqrt{D}^k.$$

Από τους τύπους του Binet προκύπτει ότι,

$$U_n = \frac{\alpha^n-\beta^n}{\alpha-\beta} = 2^{-n+1}\sum_{\substack{0\le k\le n\\ k\equiv 1 \bmod 2}}\binom{n}{k}a^{n-k}D^{\frac{k-1}{2}}.$$

Πολλαπλασιάζουμε και τα δύο μέλη με 2^{n-1} και θέτουμε $n = p+1$ οπότε παίρνουμε

$$2^p U_{p+1} = \sum_{\substack{0\le k\le n\\ k\equiv 1 \bmod 2}}\binom{p+1}{k}a^{p+1-k}D^{\frac{k-1}{2}}.$$

Είναι γνωστό ότι $\binom{p+1}{k} \equiv 0 \bmod p$ για κάθε k, $2 \le k \le p-1$. Επομένως, αν το λάβουμε υπόψη και εφαρμόσουμε το (μικρό) Θεώρημα Fermat, έχουμε: $2U_{p+1} \equiv a(1+D^{\frac{p-1}{2}}) \bmod p$. Υπενθυμίζουμε το Θεώρημα του Euler, και την υπόθεση ότι $(\frac{D}{p}) = -1$ από τα οποία προκύπτει ότι $p \mid U_{p+1}$. □

Το πιο γενικό αποτέλεσμα είναι το ακόλουθο: Θεωρούμε τις ακολουθίες Lucas $U = (U_n(\alpha,\beta))_{n\in\mathbb{N}}$ και$V = (V_n(\alpha,\beta))_{n\in\mathbb{N}}$ ως προς το ζευγάρι (a,b) και έστω p ένας περιττός πρώτος αριθμός.

Πρόταση 6.4.4.

1. *Αν ο p δεν διαιρεί το a και διαιρεί το b, τότε ο p δεν διαιρεί το U_n για κάθε $n \ge 1$.*
2. *Αν ο p διαιρεί το a και δεν διαιρεί το b, τότε ο p διαιρεί το U_n ακριβώς τότε όταν ο n είναι άρτιος.*
3. *Αν ο p δεν διαιρεί το ab και διαιρεί το D, τότε ο p διαιρεί το U_n ακριβώς τότε όταν $p \mid n$.*
4. *Αν ο p δεν διαιρεί το abD, τότε ο p διαιρεί το $U_{p-\varepsilon(p)}$.*

Σημείωση. Οι συγγραφείς Crandall, Pomerance [8] και Song Y. Yan [9] θεωρούν ότι για την τελευταία σχέση αρκεί ο περιορισμός ο p να είναι περιττός πρώτος ο οποίος να μη διαιρεί το γινόμενο bD.

5.Εφαρμογές

Της πρότασης 6.4.2 δεν ισχύει το αντίστροφο. Υπάρχουν σύνθετοι φυσικοί αριθμοί n για τους οποίους να ισχύει η ισοτιμία

$$U_{n-\varepsilon_n} \equiv 0 \bmod s \tag{6.5.16}$$

Ορισμός 6.5.5. Ενας *σύνθετος* φυσικός αριθμός n ο οποίος επαληθεύει τη σχέση (6.5.16), θα λέγεται *ψευδοπρώτος Lucas* ως προς το ζευγάρι (a, b).
Οι ψευδοπρώτοι Lucas ως προς το ζευγάρι $(a, b) = (1, -1)$ θα λέγονται *ψευδοπρώτοι Fermat*.

Μερικοί *ψευδοπρώτοι Fermat* είναι οι 323,377,1159,...
Δεν έχει βρεθεί μέχρι σήμερα αριθμός ο οποίος να είναι συγχρόνως ψευδοπρώτος Lucas και αριθμός Carmichael (ή 2-ψευδοπρώτος). Επομένως έχει νόημα η
Εικασία: Αν n φυσικός αριθμός $n > 1$ ο οποίος εχει περάσει με επιτυχία τόσο το test του Lucas όσο και το ισχυρό test των ψευδοπρώτων, τότε ο n είναι πρώτος.
Όποιος αποδείξει την εικασία ή βρει κάποιο αντιπαράδειγμα θα πάρει 620 δολάρια.

Ορισμός 6.5.6. Δίνεται μία ακολουθία Lucas ως προς το ζευγάρι (a, b). Αν n θετικός ακέραιος τέτοιος ώστε $(n, 2bD) = 1$,τότε ο ελάχιστος θετικός ακέραιος $\lambda(n) := \lambda_{(a,b)}(n)$ για τον οποίο ισχύει $U_{\lambda(n)} \equiv 0 \bmod n$, θα λέγεται *σημείο εισόδου* του n στη (δοθείσα) ακολουθία Lucas.

Σύμφωνα με την πρόταση 6.4.2, αν p είναι ένας πρώτος αριθμός με $(p, 2bD) = 1$ τότε $\lambda(p) \mid p - \varepsilon_p$. Στη συνέχεια θα διατυπώσουμε ένα test πιστοποίησης πρώτων:

Το test του Lucas. Υποθέτουμε ότι μας δίνεται κάποια ακολουθία Lucas και ένας θετικός ακέραιος n για τον οποίο ισχύουν, $(n, 2b) = 1$ και $(\frac{D}{n}) = -1$. Αν s είναι ένας διαιρέτης του $n + 1$ και για κάθε πρώτο διαιρέτη q του s ισχύουν

$$U_{n+1} \equiv 0 \bmod n \text{ και } (U_{\frac{n+1}{q}}, n) = 1,$$

τότε για κάθε πρώτο διαιρέτη p του n ισχύει

$$p \equiv \left(\frac{D}{p}\right) \bmod s.$$

Ιδιαίτερα, αν $s > \sqrt{n} + 1$, τότε ο n είναι πρώτος.

Απόδειξη. Υπενθυμίζουμε την ιδιότητα $n \mid U_k \Longleftrightarrow \lambda(n) \mid k$. Από την υπόθεση ότι $U_{n+1} \equiv 0 (mod n)$ έπεται $\lambda(n) \mid n+1$. Επομένως για κάθε πρώτο p διαιρέτη του n έχουμε $\lambda(p) \mid n+1$. Από τη δεύτερη υπόθεση ότι $(U_{\frac{n+1}{q}}, n) = 1$ για κάθε πρώτο διαιρέτη q του s, και επειδή $p \mid n$, έπεται ότι, για κάθε πρώτο διαιρέτη q του s ο p δεν διαιρεί τον $\frac{U_{n+1}}{q}$. Άρα $\lambda(p)$ διαιρεί τον $\frac{n+1}{q}$. Έστω ότι $q^f \| s \mid n + 1$. Από την τελευταία ιδιότητα προκύπτει ότι $q^f \mid \lambda(p)$. Αυτό ισχύει για κάθε q πρώτο διαιρέτη του s, συνεπώς και για το γινόμενό τους, δηλαδή $s \mid \lambda(p)$.
Λόγω της πρότασης 6.4.2, έχουμε ότι $U_{p-\varepsilon_p(D)} \equiv \bmod p$. Επομένως $\lambda(p) \mid p - \varepsilon_p(D)$. Από τις τελευταίες δύο ιδιότητες προκύπτει ότι

$$s \mid p - \varepsilon_p(D) = p - \left(\frac{D}{p}\right),$$

δηλαδή η ισοτιμία

$$p \equiv \left(\frac{D}{p}\right) \bmod s.$$

Αν τώρα $s > \sqrt{n}+1$ τότε, για κάθε πρώτο διαιρέτη p του n έχουμε

$$p+1 \geq p-\left(\frac{D}{p}\right) \geq s > \sqrt{n}+1,$$

δηλαδή $p > \sqrt{n}$. Αν ο n ήταν σύνθετος τότε θα είχε έναν τουλάχιστον πρώτο παράγοντα $p \leq \sqrt{n}$. Συνεπώς ο n είναι πρώτος. □

Θα κλείσουμε την παράγραφο με ένα πολύ πρακτικό και ντετερμινιστικό test πιστοποίησης πρώτων που αφορά στους αριθμούς Mersenne. Ο Lucas είχε τη βασική ιδέα το 1876 και ο Lehmer απλοποίησε τη μέθοδοτο 1930.

Ορισμός 6.5.7. Η ακολουθία $(S_n)_n \in \mathbb{N}$ η οποία ορίζεται από τον αναδρομικό τύπο $S_1 = 4$ και $S_{n+1} = S_n^2 - 2$ θα λέγεται *ακολουθία των Lucas-Lehmer*.

Πρόταση 6.5.8 (*Test των Lucas-Lehmer για τους πρώτους αριθμούς Mersenne M_n*)**.** *Αν p είναι ένας περιττός πρώτος, τότε ο*

$$M_p := 2^p - 1 \text{ είναι πρώτος ακριβώς τότε όταν ο } M_p \mid S_{p-1}.$$

Απόδειξη. Η ιδέα της απόδειξης είναι να αναγάγουμε το πρόβλημα στη μελέτη μιας ακολουθίας Lucas. Το πλεονέκτημα είναι ότι γνωρίζουμε αρκετές ιδιότητες αυτών των ακολουθιών. Η ακολουθία αυτή θα είναι η $(U_n)_{n\in\mathbb{N}}$, $(V_n)_{n\in\mathbb{N}}$ ως προς το ζευγάρι $(\alpha,\beta) = (2,-2)$. Επομένως, $D = 12$, $a = 1+\sqrt{3}$ και $b = 1-\sqrt{3}$. Ισχύει ότι

$$U_p \equiv \left(\frac{3}{p}\right) \mathrm{mod} p$$

και

$$V_p \equiv 2 \mathrm{mod} p,$$

δείτε [7, σελ. 49]. Υποθέτουμε τώρα ότι για $p \geq 3$ ο αριθμός $M_p = 2^p - 1$ είναι πρώτος. Θα αποδείξουμε ότι ο $S_{p-1} \equiv 0 \mathrm{mod} M_p$. Επειδή ο M_p είναι περιττός, η τελευταία ισοτιμία είναι ισοδύναμη προς την

$$2^{2^{p-2}} S_{p-1} \equiv 0 \mathrm{mod} M_p.$$

Για κάθε $i \geq 1$ ορίζουμε $T_i = 2^{(2^{i-1})} S_i$. Συνεπώς, $T_1 = 2^{2^0} S_1 = 2 \cdot 4 = 8$ και

$$T_{i+1} = 2^{(2^{(i+1)-1})} S_{i+1} = (2^{2^{i-1}})^2 [S_i^2 - 2] = (2^{2^{i-1}} S_i)^2 - 2^{(2^i+1)} = T_i^2 - 2^{(2^i+1)}.$$

Επομένως, αρκεί να αποδείξουμε ότι

$$T_{p-1} = 2^{(2^{p-2})} S_{p-1} \equiv 0 \mathrm{mod} M_p.$$

Αλλά $T_p = T_{p-1}^2 - 4 \cdot 2^{(2^{p-1}+1)}$. Επειδή $M_p = 2^p - 1 \equiv 7 \mathrm{mod} 8)$ έπεται ότι $(\frac{2}{M_p}) = 1$. Από το θεώρημα του Euler προκύπτει ότι

$$2^{2^{p-1}-1} = 2^{\frac{M_p-1}{2}} \equiv \left(\frac{2}{M_p}\right) \equiv 1 \mathrm{mod} M_p.$$

Επομένως αρκεί να αποδείξουμε ότι $T_p \equiv -4 \mathrm{mod} M_p$.

Στη συνέχεια παρατηρούμε ότι για κάθε $i \geq 1$ ισχύει $T_i = V_{2^i}$. Η απόδειξη αυτής της σχέσης θα γίνει επαγωγικά. Πράγματι για $i = 1$ έχουμε $T_1 = 8 = 2^2 + (-2)^2 = V_2$, δηλαδή ισχύει. Υποθέτουμε ότι $T_{k-1} = V_{2^{k-1}}$ και θα αποδείξουμε τη σχέση $T_k = V_{2^k}$. Πράγματι,

$$T_k = T_{k-1}^2 - 2^{(2^{k-1}+1)} = V_{2^{k-1}}^2 - 2^{(2^{k-1}+1)}.$$

Από τη γνωστή ιδιότητα $V_n^2 - 2(-2)^n = V_{2n}$ έπεται ότι $T_k = V_{2^{k-1}}^2 + (-2)^{2^{k-1}+1} = V_{2\cdot 2^{k-1}} = V_{2^k}$. Από τη γνωστή σχέση

$$2V_{m+n} = V_m V_n + DU_m U_n,$$

έπεται ότι

$$2T_p = 2V_{2^p} = 2V_{(2^p-1)+1} = 2V_{M_p+1} = V_{M_p}V_1 + 12U_{M_p}U_1 = 2V_{M_p} + 12U_{M_p}.$$

Για κάθε πρώτο p ισχύουν $M_p \equiv 1 \bmod 3$) και $M_p \equiv 1 \bmod 4$. Επομένως $U_{M_p} \equiv (\frac{3}{M_p}) \equiv -(\frac{3}{M_p}) \equiv -(\frac{1}{3}) \equiv -1 \bmod M_p$ και $V_{M_p} \equiv 2 \bmod M_p$. Συνεπώς,

$$T_p \equiv V_{M_p} + 6U_{M_p} \equiv 2 - 6 \equiv -4 \bmod M_p.$$

Στη συνέχεια θα αποδείξουμε το αντίστροφο. Υποθέτουμε ότι για κάποιο φυσικό αριθμό n ισχύει η ισοτιμία $S_{n-1} \equiv 0 \bmod M_n$, και θα αποδείξουμε ότι ο $M_n = 2^n - 1$ είναι πρώτος. Από την υπόθεση έπεται ότι $M_n \mid S_{n-1}$ και επομένως και $M_n = 2^n - 1 \mid T_{n-1} = 2^{(2^{n-1}-1)}S_{n-1}$. Έστω p ένας πρώτος αριθμός $p \mid 2^n - 1$ και $t := \jmath(M_n)$ ο δείκτης εισόδου του p στην ακολουθία Lucas $(U_n)_{n\in\mathbb{N}}$. Επομένως $p \mid U_t$. Από τη γνωστή ιδιότητα $U_{2n} = U_n V_n$ έπεται ότι $U_{2^n} = U_{2^{n-1}}V_{2^{n-1}} = U_{2^{n-1}}T_{n-1}$. Επειδή $2^{n-1} \mid T_{n-1}$, έχουμε $2^n - 1 \mid U_{2^n}$. Άρα $p \mid U_{2^n}$ και συνεπώς $t \mid 2^n$. Θα αποδείξουμε ότι $t = 2^n$. Αν ίσχυε $t \mid 2^{n-1}$, θα είχαμε $p \mid U_{2^{n-1}}$, οπότε, επειδή ισχύει και $p \mid T_{n-1} = V_{2^{n-1}}$ θα ίσχυε $p \mid V_{2^{n-1}}^2 - 12U_{2^{n-1}}^2 = (-2)^{2^{n-1}} + 2 =$ Δύναμη του 2, άτοπο διότι $p \geq 3$.
Αποδείξαμε λοιπόν ότι $t := \jmath(M_n) = 2^n$. Αλλά, επειδή $t := \jmath(M_n) = 2^n \leq p + 1 \leq 2^n$, έπεται ότι $p = 2^{n-1}$. □

Θα δώσουμε τώρα μια υλοποίηση του κριτηρίου Lucas-Lehmer για τους πρώτους αριθμούς Mersenne στο πρόγραμμα sage.

```
p =11
M = 2^p-1; M
s = 4
for i in range(p-2):
    s = mod(s^2-2,M)
    print (i+1,s)
```

Η εκτέλεση του παραπάνω προγράμματος για $p = 11$ έχει αποτέλεσμα

(1, 14)
(2, 194)
(3, 788)
(4, 701)
(5, 119)
(6, 1877)
(7, 240)
(8, 282)
(9, 1736)

Το οποίο σημαίνει ότι ο $M_{11} = 2^{11} - 1 = 2047$ δεν είναι πρώτος. Πράγματι $2047 = 23 \times 89$. Για $p = 13$ έχουμε

(1, 14)
(2, 194)
(3, 4870)
(4, 3953)
(5, 5970)
(6, 1857)
(7, 36)
(8, 1294)
(9, 3470)
(10, 128)
(11, 0)

Το οποίο σημαίνει ότι ο $M_{13} = 8191$ είναι πρώτος.

Παρατηρήσεις:

- Όλοι οι πρώτοι αριθμοί Mersenne έχουν υπολογιστεί σύμφωνα με το παραπάνω κριτήριο. Πρώτος ο Lucas απέδειξε στα 1876 ότι ο M_{127} είναι πρώτος, ενώ ο M_{67} είναι σύνθετος. Λίγο αργότερα ο Perwuschin, απέδειξε ότι ο M_{61} είναι πρώτος, ενώ ο Lehmer στα 1932 απέδειξε ότι ο M_{257} είναι σύνθετος. Η εικασία του Mersenne ήταν ότι είναι πρώτος.

- Η διαδικασία που εφαρμόζεται είναι η εξής: Επιλέγουμε τυχαία έναν πρώτο αριθμό q και στη συνέχεια ελέγχουμε με βάση το κριτήριο αν ο αντίστοιχος αριθμός Mersenne $M_q = 2^q - 1$ είναι πρώτος. Φυσικά μπορούμε να εργασθούμε πιο συστηματικά και να πάρουμε όλους τους πρώτους τους μικρότερους από κάποια συγκεκριμένη τιμή. Πριν από την εποχή των ηλεκτρονικών υπολογιστών αυτό είχε γίνει μέχρι το ≤ 127. Σήμερα, το αποτέλεσμα αυτό είναι γνωστό, τουλάχιστον για 12830000. Φυσικά αν συμβεί για κάποιο πρώτο q να ισχύει $p := 2q + 1$, τότε, ως γνωστό, ισχύει $p \mid M_q$, δηλαδή ο M_q είναι σύνθετος.

  Το Project "The GIMPS", Great Mersenne Prime Search είναι ένα πρόγραμμα κατανεμημένου υπολογισμού που χρησιμοποιεί την υπολογιστική των υπολογιστών εθελοντών προκειμένου να αναζητήσει πρώτους αριθμούς του Mersenne.

Παραδείγματα:

- Για $q = 7$. υπολογίζουμε την ακολουθία S_i για $i = 1, 2, ..., q - 1 = 6$ και έχουμε: $S_1 = 4$, $S_2 \equiv 14 \mathrm{mod} 127$, $S_3 \equiv 67 \mathrm{mod} 127$, $S_4 \equiv 42 \mathrm{mod} 127$ $S_5 \equiv 11 \mathrm{mod} 127$, $S_6 \equiv 0 \mathrm{mod} 127$. Επομένως ο M_7 είναι πρώτος.

- Για $q = 11$ έχουμε $M_{11} = 2047$. Υπολογίζουμε $S_{10} \equiv 1736 (mod 2047)$ και συμπεραίνουμε ότι ο M_{11} δεν είναι πρώτος.

- Για $q = 13$. Επειδή οι αριθμοί μεγαλώνουν είναι πιο εύκολο να εργαζόμαστε στο δυαδικό σύστημα. Εδώ αποδεικνύεται ότι $S_{12} \equiv 0 \mathrm{mod} M_{13}$) ή ότι ο αριθμός M_{13} είναι πρώτος.

  Σημείωση: Σύμφωνα με το δελτίο τύπου της Γερμανικής Μαθηματικής Εταιρείας της με ημερομηνία 27/9/2008, στα πλαίσια του προγράμματος (GIMPS), έχουν βρεθεί

άλλοι δύο πρώτοι αριθμοί. Ο μεγαλύτερος αριθμός είναι ο $2^{43112609} - 1$ και έχει πλήθος ψηφίων σχεδόν 13 εκατομμύρια και επιβεβαιώθηκε στις 6 Αυγούστου. Δικαιούται να πάρει το βραβείο των 100.000 δολαρίων από την Electronic Frontier Foundation, αφού είναι ο πρώτος που βρέθηκε με πλήθος ψηφίων πάνω από 10 εκατομμύρια. Ο δεύτερος, λίγο μικρότερος από τον πρώτο με περισσότερα από 11 εκατομύρια ψηφία, ανακοινώθηκε στις Σεπτεμβρίου `http://primzahlen.de`.

6.6 Ασκήσεις

1. Να αποδείξετε τις ιδιότητες από (6.3.1) μέχρι (6.3.9)
2. Ομοίως από (6.3.12) μέχρι (6.3.15)
3. Ομοίως για τις (6.3.16) με (6.3.19)
4. Να αποδείξετε ότι για κάθε $n \geq 2$ ισχύει η ισοτιμία
$$L_{2^n} \equiv 7 \mathrm{mod} 10$$
5. Να αποδειχτεί ότι για κάθε $n \geq 1$
$$2^n L_n \equiv 2 \mathrm{mod} 10$$
6. Να αποδείξετε ότι $L_{n+1} + L_{n-1} = 5F_n$ για $n \geq 2$. Συμπεράνετε ότι $5 \nmid L_n$ για $n \geq 1$.
7. Αν $m = n^{13} - n$ και $n > 1$ να αποδείξετε ότι $30290 \mid F_m$. (Υπόδειξη: Να αποδείξετε πρώτα ότι $a^{13} \equiv a \mathrm{mod} 2730$).
8. Για κάθε $n \geq 1$ να αποδείξετε ότι $18 \mid F_{n+11} + F_{n+7} + 8F_{n+5} + F_{n+3} + 2F_n$.

Βιβλιογραφία

[1] E. Cohn, J. H.: *On square Fibonacci numbers*. J. London Math. Soc., 39:537–540, 1964.

[2] E. Cohn, J. H.: *Eight Diophantine equations*. Proc. London Math. Soc., (3):16:153–166, 1966.

[3] E. Hoggatt: *Fibonacci and Lucas numbers*. Houghton Mifflin mathematics enrichment series. Houghton Mifflin, 1969.

[4] Frommer, H. Scheid and A.: *Zahlentheorie*. Spektrum Akademischer Verlag.

[5] Luo Ming: *On triangular Fibonacci Number*. The Fibonacci Quarterly, 27, 1988.

[6] Moss, N. Vorobev and H.: *Fibonacci Numbers*. Popular lectures in mathematics, Pergamon Press, 1961.

[7] Paulo Ribenboim: *The Little Book of Bigger Primes*. Springer, 2004.

[8] R. Crandall, C.B. Pomerance: *Prime Numbers: A Computational Perspective*. 2005.

[9] S. Y. Yan: *Number Theory for Computing*. U.S. Government Printing Office, 2002.

[10] T. Koshy: *Elementary Number Theory with Applications*. Elsevier Science, 2007.

[11] Worobjow, N.: *Die Fibonacci Zahlen*. D.V.W Berlin, 1954.

7

Συνεχή κλάσματα

Μια διαφορετική παράσταση των πραγματικών αριθμών.

7.1 Συνεχή κλάσματα ρητών αριθμών

Ας είναι $a = 543$ και $b = 314$ δύο ακέραιοι αριθμοί. Εφαρμόζουμε τον Ευκλείδιο αλγόριθμο:

$$\begin{array}{l|l} 543 = 314 + 229 & \frac{543}{314} = 1 + \frac{229}{314} \\ 314 = 229 + 85 & \frac{314}{229} = 1 + \frac{85}{229} \\ 229 = 2 \cdot 85 + 59 & \frac{229}{85} = 2 + \frac{59}{85} \\ 85 = 59 + 26 & \frac{85}{59} = 1 + \frac{26}{59} \\ 59 = 2 \cdot 26 + 7 & \frac{59}{26} = 2 + \frac{7}{26} \\ 26 = 3 \cdot 7 + 5 & \frac{26}{7} = 3 + \frac{5}{7} \\ 7 = 5 + 2 & \frac{7}{5} = 1 + \frac{2}{5} \\ 5 = 2 \cdot 2 + 1 & \frac{5}{2} = 2 + \frac{1}{2} \end{array}$$

Επομένως, ο ρητός αριθμός $\frac{543}{314}$ μπορεί να γραφεί ως εξής:

$$\frac{543}{314} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{2}}}}}}}}$$

Η παράσταση αυτή λέγεται συνεχές κλάσμα του $\frac{543}{314}$. Μάλιστα για λόγους συντομίας γράφεται:

$$\frac{543}{314} = [1; 1, 2, 1, 2, 3, 1, 2, 2].$$

Ορισμός 7.1.1. Ένα πεπερασμένο συνεχές κλάσμα είναι ένας πραγματικός αριθμός της μορφής

$$[a_0; a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

όπου οι a_i, $i = 0, 1, 2, \ldots, n$ είναι πραγματικοί αριθμοί με $a_i > 0$, για $i \geq 1$. Οι πραγματικοί αριθμοί $a_1, a_2, \ldots, a_n$ λέγονται μερικά υπόλοιπα του συνεχούς κλάσματος. Το κλάσμα λέγεται απλό όταν οι αριθμοί $a_0, a_1, a_2, \ldots, a_n$ είναι όλοι τους ακέραιοι.

Πρόταση 7.1.2. *Κάθε ρητός αριθμός μπορεί να γραφεί ως ένα πεπερασμένο απλό συνεχές κλάσμα.*

Απόδειξη. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη στους όρους του κλάσματος όπως ακριβώς στο παράδειγμα. □

Παρατήρηση 7.1.3. Είναι φανερό ότι ισχύει

$$[a_0; a_1, a_2, \ldots, a_n] = [a_0; a_1, \ldots, a_{n-1}, a_n - 1, 1].$$

Αυτό σημαίνει ότι η παράσταση ενός ρητού σε συνεχές κλάσμα δεν είναι μονοσήμαντη.

Στο παράδειγμά μας το τελευταίο μερικό υπόλοιπο, το 2, μπορούσε να είχε γραφεί $1 + \frac{1}{1}$ οπότε θα είχαμε και

$$\frac{543}{314} = [1; 1, 2, 1, 2, 3, 1, 2, 1, 1].$$

Αυτό σημαίνει ότι το μήκος ενός απλού συνεχούς κλάσματος μπορεί να ληφθεί κατά βούληση ως άρτιο ή περιττό.

Παρατήρηση 7.1.4.

$$[a_0; a_1, a_2, \ldots, a_n] = [a_0, [a_1; a_2, \ldots, a_n]]$$

Της πρότασης 7.1.2 ισχύει και το αντίστροφο:

Πρόταση 7.1.5. *Κάθε απλό πεπερασμένο συνεχές κλάσμα παριστά έναν ρητό αριθμό*

Απόδειξη. Επαγωγικά ως προς n.

Αν $n = 1$ τότε

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + a_1}{a_1} \in \mathbb{Q},$$

δηλαδή ισχύει.

Έστω ότι ισχύει για $n = k$, δηλαδή ότι

$$[a_0; a_1, a_2, \ldots, a_k] \in \mathbb{Q}.$$

Το

$$[a_0; a_1, a_2, \ldots, a_{k+1}] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_{k+1}]}.$$

Όμως το πεπερασμένο απλό συνεχές κλάσμα

$$[a_1; a_2, \ldots, a_{k+1}] =: \frac{r}{s} \in \mathbb{Q},$$

από την υπόθεση της μαθηματικής επαγωγής. Επομένως

$$[a_0; a_1, a_2, \ldots, a_{k+1}] = a_0 + \frac{1}{r/s} = \frac{a_0 s + r}{r} \in \mathbb{Q}.$$

□

Παράδειγμα. Το πεπερασμένο απλό συνεχές κλάσμα $[1; 2, 3, 4, 5, 6]$ παριστά τον ρητό αριθμό $\frac{1393}{972}$.

Ορισμός 7.1.6. Αν ο ρητός αριθμός x παρίσταται από το πεπερασμένο απλό συνεχές κλάσμα

$$[a_0; a_1, a_2, \ldots, a_n],$$

τότε ο ρητός αριθμός

$$c_k := [a_0; a_1, \ldots, a_k],$$

για $0 \leq k \leq n$ θα λέγεται k-στός συγκλίνων του x.

Παράδειγμα. Το συνεχές κλάσμα του ρητού

$$\frac{F_8}{F_7} = \frac{21}{13} = [1; 1, 1, 1, 1, 1, 1].$$

Οι συγκλίνοντες αυτού είναι οι

$$\begin{aligned}
c_0 &= [1] = 1 \\
c_1 &= [1; 1] = 1 + \frac{1}{1} = 2 \\
c_2 &= [1; 1, 1] = 1 + \frac{1}{1 + \frac{1}{1}} = \frac{3}{2} = 1,5 \\
c_3 &= [1; 1, 1, 1, 1] = \frac{5}{3} \sim 1,66 \\
c_4 &= [1; 1, 1, 1, 1, 1] = \frac{8}{5} = 1,60 \\
c_5 &= [1; 1, 1, 1, 1, 1, 1] = \frac{13}{8} = 1,625 \\
c_6 &= [1; 1, 1, 1, 1, 1, 1, 1] = \frac{21}{13} = 1,6153846154
\end{aligned}$$

Πρόταση 7.1.7. *Αν οι ακέραιοι p_k, q_k, για $0 \le k \le n$, ορισθούν ως*

$$p_0 := a_0, \quad q_0 := 1$$

$$p_1 = a_1 a_0 + 1, \quad q_1 := a_1$$

και

$$p_k = a_k p_{k-1} + p_{k-2} \quad q_k = a_k q_{k-1} + q_{k-2}$$

για κάθε k, $2 \le k \le n$, τότε ισχύει $c_k = \frac{p_k}{q_k}$, για $0 \le k \le n$.

Απόδειξη. Για $k = 0$, $\frac{p_0}{q_0} = \frac{a_0}{1} = [a_0] = c_0$.

Για $k = 1$,

$$\frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0; a_1] = c_1.$$

Υποθέτουμε ότι ισχύει για κάποιον k, $2 \le k < n$,

$$c_k = [a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}.$$

Θα αποδείξουμε ότι ισχύει και για $k+1$. Ίσχύει

$$c_{k+1} = [a_0; a_1, a_2, \ldots, a_k, a_{k+1}] = [a_0; a_1, a_2, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}],$$

οπότε από την υπόθεση της μαθηματικής επαγωγής, προκύπτει

$$c_{k+1} = \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} =$$

$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} =$$

$$= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.$$

□

Παράδειγμα. Το συνεχές κλάσμα του $x = \frac{52}{23}$ είναι $[2; 3, 1, 5]$. Σχηματίζουμε τον πίνακα:

k	0	1	2	3
a_k	2	3	1	5
p_k	2	7	9	52
q_k	1	3	4	23

Από τον ορισμό του συνεχούς κλάσματος

$$[a_0; a_1, a_2, \ldots, a_n]$$

έχουμε ότι $a_i \in \mathbb{R}$, $i = 0, 1, 2, \ldots$, και $a_i > 0$ για $i = 1, 2, \ldots, n$. Επομένως $q_n > 0$ για κάθε $n \ge 1$.

Πόρισμα 7.1.8. *Έστω $a_i \in \mathbb{R}$ για $i = 0, 1, 2, \ldots, n$ και $a_i > 0$ για κάθε $i = 1, 2, \ldots, n$. Αν $k \in \mathbb{N}$, $1 \le k \le n$ και $r_k := [a_k, a_{k+1}, \ldots, a_n]$ τότε ισχύει*

$$[a_0; a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{k-1}, r_k] = \frac{r_k p_{k-1} + p_{k-2}}{r_k q_{k-1} + q_{k-2}}.$$

Πόρισμα 7.1.9. *Υποθέτουμε ότι* $a_i, b_i \in \mathbb{R}$, $i = 0, 1, 2, \ldots, n$ *και ότι* $a_i \geq 1$, $b_i \geq 1$ *για* $i = 0, 1, 2, \ldots, n-1$. *Αν* $a_i, b_i \in \mathbb{Z}$, *για* $i = 0, 1, 2, \ldots, (n-1)$, *και*

$$[a_0; a_1, \ldots, a_n] = [b_0; b_1, \ldots, b_n],$$

τότε $a_i = b_i$, *για κάθε* $i = 0, 1, 2, \ldots, n$.

Απόδειξη. Ας ονομάσουμε

$$r_1 := [a_1, a_2, \ldots, a_n] = a_1 + \frac{1}{[a_2, a_3, \ldots, a_n]}.$$

Το $r_1 \geq 1$. Ομοίως αν

$$s_1 = [b_1, b_2, \ldots, b_n]$$

τότε και $s_1 \geq 1$. Από την υπόθεση έπεται ότι

$$a_0 + \frac{1}{r_1} = b_0 + \frac{1}{s_1}.$$

Αν $r_1 = 1$ τότε $a_0 + \frac{1}{r_1} \in \mathbb{Z}$ συνεπώς $b_0 + \frac{1}{s_1} \in \mathbb{Z}$ άρα $s_1 = 1$ οπότε και $a_0 = b_0$.
Αν $r_1 > 1$ τότε $a_0 + \frac{1}{r_1} \notin \mathbb{Z}$, συνεπώς, $b_0 + \frac{1}{s_1} \notin \mathbb{Z}$. Άρα $s_1 > 1$. Και πάλι $a_0 = b_0$ διότι και οι δύο είναι οι μεγαλύτεροι ακέραιοι $\leq [a_0; a_1, \ldots, a_n]$. Επομένως σε κάθε περίπτωση ισχύει $a_0 = b_0$ και $r_1 = s_1$.

Συνεχίζουμε επαγωγικά ως προς n. Αν $n = 1$ τότε $a_0 = b_0$ και $r_1 = a_1 = s_1 = b_1$. Έστω ότι ισχύει για $(n-1)$.

Από την υπόθεση

$$[a_0; a_1, \ldots, a_n] = [b_0; b_1, \ldots, b_n]$$

έπεται ότι

$$[a_0, [a_1, a_2, \ldots, a_n]] = [b_0, [b_1, b_2, \ldots, b_n]]$$

και επομένως $a_0 = b_0$ και $[a_1, a_2, \ldots, a_n] = [b_1; b_2, \ldots, b_n]$. Από την υπόθεση της μαθηματικής επαγωγής ισχύει ότι $a_i = b_i$ για κάθε $i = 1, 2, \ldots, n$. □

Παρατήρηση 7.1.10. Το πόρισμα 7.1.9 μας δίνει τη μοναδικότητα της παράστασης ενός πραγματικού αριθμού, σε άπειρο απλό συνεχές κλάσμα, όταν πληρούνται οι προϋποθέσεις αυτού. Το πόρισμα θα χρησιμοποιηθεί σε επόμενη παράγραφο. Στα επόμενα εδάφια θα χρησιμοποιουμε τον συμβολίσμό της πρότασης 7.1.7.

7.2 Ιδιότητες των συγκλινόντων

Για λόγους ομοιομορφίας των παραστάσεων θέτουμε $p_{-1} := 1$ και $q_{-1} := 0$.

Πρόταση 7.2.1. *Για κάθε φυσικό αριθμό* $n \geq 0$, *ισχύει*

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n.$$

Απόδειξη. Επαγωγικά ως προς n. Η πρόταση ισχύει για $n = 0$, αφού

$$q_0 p_{-1} - p_0 q_{-1} = 1.$$

Από την πρόταση 7.1.7 προκύπτει ότι

$$q_{n-1}p_n = q_{n-1}(a_n p_{n-1} + p_{n-2}) = a_n p_{n-1}q_{n-1} + q_{n-1}p_{n-2}$$

και

$$p_{n-1}q_n = p_{n-1}(a_n q_{n-1} + q_{n-2}) = a_n p_{n-1}q_{n-1} + p_{n-1}q_{n-2}.$$

Αφαιρούμε κατά μέλη και έχουμε

$$q_n p_{n-1} - p_n q_{n-1} = -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}).$$

Από την υπόθεση της μαθηματικής επαγωγής έπεται ότι

$$q_{n-1}p_{n-2} - p_{n-1}q_{n-2} = (-1)^{n-1}.$$

Επομένως,

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n.$$

□

Πόρισμα 7.2.2. *Για κάθε φυσικό αριθμό $n \geq 0$, ισχύει*

$$\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n-1}}.$$

Στη συνέχεια θα υποθέσουμε ότι το συνεχές κλάσμα $[a_0; a_1, a_2, \ldots, a_n]$ είναι απλό, δηλαδή ότι $a_i \in \mathbb{Z}$, για κάθε $i = 0, 1, 2, \ldots, n$.

Πόρισμα 7.2.3. *1. Για κάθε φυσικό $n \geq 0$, ισχύει $(p_n, q_n) = 1$.*

2. Η ακολουθία $(q_n)_{n\in\mathbb{N}}$ είναι γνησίως αύξουσα.

Απόδειξη.

1. Προφανώς $p_n, q_n \in \mathbb{Z}$, για κάθε $n \in \mathbb{N}$. Το συμπέρασμα είναι άμεση συνέπεια της πρότασης 7.2.1.

2. Άμεση συνέπεια της πρότασης 7.1.7.

□

Πόρισμα 7.2.4. *Αν $\alpha = [a_0; a_1, a_2, \ldots, a_{n+2}]$, τότε*

$$q_{n+1}\alpha - p_{n+1} = \frac{(-1)^{n+1}}{a_{n+2}q_{n+1} + q_n}.$$

Απόδειξη. Από την πρόταση 7.2.1 έπεται ότι

$$q_{n+2}p_{n+1} - p_{n+2}q_{n+1} = (-1)^{n+2}.$$

Επομένως

$$p_{n+2}q_{n+1} - q_{n+2}p_{n+1} = (-1)^{n+1}.$$

Διαιρούμε και τα δύο μέλη με $q_{n+2} > 0$

$$\frac{p_{n+2}}{q_{n+2}}q_{n+1} - p_{n+1} = \frac{(-1)^{n+1}}{q_{n+2}}.$$

Όμως, $\frac{p_{n+2}}{q_{n+2}} = \alpha$ και $q_{n+2} = a_{n+2}q_{n+1} + q_n$. Συνεπώς έχουμε το αποδεικτέο. □

Πόρισμα 7.2.5. *Για κάθε φυσικό αριθμό $n \geq 1$, ισχύει*

$$q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n.$$

Απόδειξη. Επαγωγικά ως προς n. Για $n = 1$,

$$q_1 p_{-1} - p_1 q_{-1} = a_1 \cdot 1 - p_1 \cdot 0 = (-1)^0 a_1,$$

το οποίο ισχύει.

Έστω ότι ισχύει για $n = k$, δηλαδή ότι

$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k.$$

Θα αποδείξουμε ότι ισχύει και για $n = k + 1$, δηλαδή ότι

$$q_{k+1} p_{k-1} - p_{k+1} q_{k-1} = (-1)^k a_{k+1}.$$

Το $p_{k+1} = a_{k+1} p_k + p_{k-1}$ και το $q_{k+1} = a_{k+1} p_k + p_{k-1}$. Επομένως

$$q_{k+1} p_{k-1} - p_{k+1} q_{k-1} = (a_{k+1} q_k + q_{k-1}) p_{k-1} - (a_{k+1} p_k + p_{k-1}) q_{k-1} =$$

$$= a_{k+1}(q_k p_{k-1} - p_k q_{k-1}).$$

Από την πρόταση 7.2.1 έχουμε

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k,$$

δηλαδή το πόρισμα ισχύει και για $k + 1$. □

Πόρισμα 7.2.6. *Για κάθε φυσικό n, $n \geq 2$, ισχύει*

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}$$

Πόρισμα 7.2.7. *Αν οι $a_1, a_2, \ldots,$ είναι θετικοί αριθμοί, τότε η ακολουθία $\left\{\frac{p_{2k}}{q_{2k}}\right\}_{k\in\mathbb{N}}$ είναι γνησίως αύξουσα, ενώ η ακολουθία $\left\{\frac{p_{2k+1}}{q_{2k+1}}\right\}_{k\in\mathbb{N}}$ είναι γνησίως φθίνουσα. Τέλος, από το πόρισμα 7.2.2 προκύπτει ότι $\frac{p_{2k}}{q_{2k}} < \frac{p_{2\ell+1}}{q_{2\ell+1}}$, για κάθε k, ℓ.*

Απόδειξη. Άμεση συνέπεια του πορίσματος 7.2.6. □

Πόρισμα 7.2.8. *Αν $\alpha = [a_0; a_1, a_2, \ldots, a_{n+2}]$ τότε ισχύει*

$$q_n \alpha - p_n = \frac{(-1)^n a_{n+2}}{a_{n+2} q_{n+1} + q_n}.$$

Απόδειξη. Υπολογίζουμε ότι

$$q_n \alpha - p_n = q_n \frac{p_{n+2}}{q_{n+2}} - p_n = \frac{q_n p_{n+2} - p_n q_{n+2}}{q_{n+2}}.$$

Ο αριθμητής είναι (από το πόρισμα 7.2.5)

$$q_n p_{n+2} - p_n q_{n+2} = -(p_n q_{n+2} - q_n p_{n+2}) = -(-1)^{n+1} a_{n+2} = (-1)^n a_{n+2}.$$

Τέλος,

$$q_{n+2} = a_{n+2} q_{n+1} + q_n$$

και συνεπώς το πόρισμα αποδείχθηκε. □

Πρόταση 7.2.9. *Για κάθε φυσικό αριθμό $n \geq 1$, ισχύει*

$$\frac{q_n}{q_{n-1}} = [a_n; a_{n-1}, \ldots, a_1].$$

Απόδειξη. Επαγωγικά ως προς το n.

Για $n = 1$, $q_0 = 1$, $q_1 = a_1$, επομένως $\frac{q_1}{q_0} = a_1 = [a_1]$.

Έστω $n > 1$. Υποθετουμε ότι ισχύει για $(n-1)$, δηλαδή ότι

$$\frac{q_{n-1}}{q_{n-2}} = [a_{n-1}; \ldots, a_1].$$

Το $q_n = a_n q_{n-1} + q_{n-2}$. Επομένως

$$\frac{q_n}{q_{n-1}} = a_n + \frac{q_{n-2}}{q_{n-1}} = a_n + \frac{1}{[a_{n-1}; a_{n-2}, \ldots, a_1]} = [a_n; a_{n-1}, \ldots, a_1].$$

□

7.3 Γραμμικές διοφαντικές εξισώσεις και συνεχή κλάσματα

Υπενθυμίζουμε την

Πρόταση 7.3.1. *Αν $a, b, c \in \mathbb{Z}$, η διοφαντική εξίσωση*

$$ax + by = c \text{ έχει λύση } \Leftrightarrow d := (a, b) \mid c.$$

Αν έχει λύση, τότε έχει άπειρες λύσεις. Ιδιαίτερα αν (x_0, y_0) είναι μια λύση, τότε όλες οι λύσεις δίνονται παραμετρικά από τους τύπους:

$$(x_k = x_0 + \frac{b}{d}t, y_k = y_0 - \frac{a}{d}t) \quad t \in \mathbb{Z}.$$

Με την βοήθεια των συνεχών κλασμάτων μπορούμε εύκολα να βρούμε μία λύση.

Θεωρούμε τη διοφαντική εξίσωση

$$aX + bY = 1,$$

όπου $b > 0$ και $(a, b) = 1$.

Ο $\frac{a}{b} \in \mathbb{Q}$. Έστω $[a_0; a_1, a_2, \ldots, a_n]$ το συνεχές κλάσμα αυτού. Γνωρίζουμε ότι

$$\frac{p_n}{q_n} = \frac{a}{b} \Rightarrow p_n b = a q_n.$$

Το $a \mid p_n b$ και $(a, b) = 1$ συνεπώς $a \mid p_n$. Ομοίως το $b \mid a q_n$ και $(a, b) = 1$ συνεπώς $b \mid q_n$. Σύμφωνα με το πόρισμα 7.2.3 ισχύει και $(p_n, q_n) = 1$, οπότε $p_n \mid a$ και $q_n \mid b$.

Από τα παραπάνω έχουμε $p_n = \pm a$, $q_n = \pm b$. Επειδή $b > 0$ και $q_n > 0$ έπεται ότι $q_n = b$ και συνεπώς και $p_n = a$.

Από τη σχέση $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$, προκύπτει ότι $a q_{n-1} - b p_{n-1} = (-1)^{n-1}$. Επομένως:

- Αν ο n είναι περιττός, τότε μια λύση της $aX + bY = 1$ είναι $(x_0, y_0) = (q_{n-1}, -p_{n-1})$.
- Αν ο n είναι άρτιος, τότε $-a q_{n-1} + b p_{n-1} = 1$ και συνεπώς μια λύση της $aX + bY = 1$ είναι $(x_0, y_0) = (-q_{n-1}, p_{n-1})$.

Θεωρούμε τώρα την $aX + bY = c$. Μια λύση αυτής είναι η (cx_0, cy_0), όπου (x_0, y_0) λύση της $aX + bY = 1$.

Παράδειγμα. Να υπολογιστεί μια λύση της διοφαντικής εξίσωσης

$$63x - 23y = -7.$$

Γράφουμε την εξίσωση $-63x + 23y = 7$, ώστε το $b = 23 > 0$. Το συνεχές κλάσμα του $-63/23$ είναι το $-63/23 = [-3; 3, 1, 5]$. Το $p_2/q_2 = -11/4$. Επομένως $p_2 = -11$ και $q_2 = 4$. Επίσης, $p_3/q_3 = -63/23$, άρα $p_3 = -63$, $q_3 = 23$.

$$p_3q_2 - q_3p_2 = (-1)^{3-1} \Rightarrow (-63) \cdot 4 + 23 \cdot 11 = 1.$$

Μια λύση της $(-63)x + 23 \cdot y = 1$ είναι η $(x_0, y_0) = (4, 11)$. Άρα μια λύση της αρχικής είναι η $(x_1, y_1) = (28, 77)$.

Στο sage μπορούμε να κάνουμε πράξεις με συνεχή κλάσματα ως εξής:

```
sage: a=continued_fraction(31/35)
sage: a
[0; 1, 7, 1, 3]
a.convergents()
[0, 1, 7/8, 8/9, 31/35]
```

Η πρώτη εντολή υπολογίζει το συνεχές κλάσμα του ρητού αριθμού 31/35, ενώ η δεύτερη εντολή υπολογίζει τους συγκλίνοντες.

7.4 Το συνεχές κλάσμα ενός πραγματικού αριθμού

Αν α είναι ένας ρητός αριθμός, τότε έχουμε ήδη δείξει ότι το συνεχές κλάσμα αυτού είναι πεπερασμένο.

Ας υποθέσουμε τώρα ότι ο $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Μπορούμε να γράψουμε $\alpha = a_0 + \frac{1}{\alpha_1}$, όπου $a_0 = [\alpha]$ και $\alpha_1 > 1$. Συνεχίζοντας επαγωγικά έχουμε

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}},$$

όπου $a_n = [\alpha_n]$ και $\alpha_{n+1} > 1$. Ο $\alpha \notin \mathbb{Q}$, άρα η ακολουθία των $a_1, a_2, \ldots$ δεν είναι πεπερασμένη. Επομένως, για κάθε $n \geq 0$, μπορούμε να γράψουμε

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, \alpha_{n+1}]$$

ή και

$$\alpha = [a_0; a_1, a_2, \ldots]$$

Οι συγκλίνοντες p_n, q_n αποτελούν μια ακολουθία ακέραιων, με $(p_n, q_n) = 1$ και $q_n \geq 1$. Το πηλίκο $\frac{p_n}{q_n}$ λέγεται n-στή κύρια σύγκλιση του α και ο α_n n-στο μερικό υπόλοιπο του α.

Λόγω των πορισμάτων (7.2.8), (7.2.9) και του (7.2.5) προκύπτει ότι

$$a_n < \alpha_n < a_n + 1$$

και ότι $a_n \geq 1$ για κάθε $n \geq 1$. Επίσης ισχύει

$$0 < q_1 < q_2 < \cdots < q_n < q_{n+1} < \cdots$$

Πρόταση 7.4.1. *Για τις άρτιες τιμές του n οι n-στές κύριες συγκλίσεις του α αποτελούν γνήσια αύξουσα ακολουθία η οποία συγκλίνει στο α.*

Για τις περιττές τιμές του n, οι n-στές συγκλίσεις αποτελούν μια γνήσια φθίνουσα ακολουθία η οποία συγκλίνει στο α. Επιπλέον ισχύει

$$\frac{1}{2q_{n+1}} < \frac{1}{q_{n+1}+q_n} < |q_n\alpha - p_n| < \frac{1}{q_{n+1}}.$$

Απόδειξη. Έχουμε ήδη αποδείξει ότι η ακολουθία $\left\{\frac{p_{2n}}{q_{2n}}\right\}_{n\in\mathbb{N}}$ είναι γνήσια αύξουσα και ότι η ακολουθία $\left\{\frac{p_{2n+1}}{q_{2n+1}}\right\}_{n\in\mathbb{N}}$ γνήσια φθίνουσα και ότι

$$\frac{p_{2k}}{q_{2k}} \le \frac{p_{2\ell+1}}{q_{2\ell+1}},$$

για όλους τους θετικούς ακέραιους k, ℓ.

Μάλιστα, οι ακολουθίες $\left\{\frac{p_{2n}}{q_{2n}}\right\}_{n\in\mathbb{N}}$ και $\left\{\frac{p_{2n+1}}{q_{2n+1}}\right\}_{n\in\mathbb{N}}$ φράσσονται από πάνω και από κάτω αντίστοιχα από τον πραγματικό αριθμό α. Επομένως συγκλίνουν.

Έστω ότι

$$\lim_{n\to\infty}\frac{p_{2n}}{q_{2n}} = \beta \le \alpha$$

και

$$\lim_{n\to\infty}\frac{p_{2n+1}}{q_{2n+1}} = \gamma \ge \alpha.$$

Θα αποδείξουμε ότι $\beta = \alpha = \gamma$. Ως γνωστό,

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{(2n+1)-1}}{q_{2n+1}q_{2n}} < \frac{1}{q_{2n+1}q_{2n}} < \frac{1}{q_{2n}^2} \to 0.$$

Συνεπώς

$$\beta = \lim_{n\to\infty}\frac{p_{2n+1}}{q_{2n+1}} = \lim_{n\to\infty}\frac{p_{2n}}{q_{2n}} = \gamma.$$

Στη συνέχεια έχουμε

$$|q_n - \alpha p_n| = \frac{1}{\alpha_{n+1}q_n + q_{n-1}}.$$

Το

$$\alpha_{n+1}q_n + q_{n-1} > [\alpha_{n+1}]q_n + q_{n-1} = a_{n+1}q_n + q_{n-1} = q_{n+1}.$$

Συνεπώς

$$|q_n - \alpha p_n| < \frac{1}{q_{n+1}}.$$

Ισχύει

$$\left|\alpha - \frac{p_n}{q_n}\right| > \left|\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n}\right| = \frac{a_{n+2}}{q_{n+2}q_n} = \frac{a_{n+2}}{(a_{n+2}q_{n+1}+q_n)q_n}.$$

Το $a_{n+2} = [\alpha_{n+2}] \ge 1$. Επομένως,

$$|\alpha q_n - p_n| > \frac{1}{q_{n+1} + \frac{1}{a_{n+2}}q_n} > \frac{1}{q_{n+1}+q_n} > \frac{1}{2q_{n+1}},$$

αφού $q_{n+1} > q_n$. □

Παρατήρηση 7.4.2. Προφανώς ισχύει

$$|q_n\alpha - p_n| < \frac{1}{q_n}, \text{ αφού } q_{n+1} > q_n.$$

Πόρισμα 7.4.3. *Για κάθε φυσικό αριθμό n, $n \geq 2$ ισχύουν οι σχέσεις*

$$|q_{n-1}\alpha - p_{n-1}| = a_n|q_n\alpha - p_n| + |q_{n+1}\alpha - p_{n+1}|,$$

$$|q_n\alpha - p_n| < |q_{n-1}\alpha - p_{n-1}|$$

και

$$a_n = \left[\frac{|q_{n-1}\alpha - p_{n-1}|}{|q_n\alpha - p_n|}\right]$$

Απόδειξη. Το

$$q_{n+1}\alpha - p_{n+1} = (a_{n+1}q_n + q_{n-1})\alpha - (a_{n+1}p_n + p_{n-1}) = a_{n+1}(q_n\alpha - p_n) + (q_{n-1}\alpha - p_{n-1}).$$

Επομένως

$$(q_{n-1}\alpha - p_{n-1}) = (q_{n+1}\alpha - p_{n+1}) - a_{n+1}(q_n\alpha - p_n).$$

Από το πόρισμα 7.2.4 προκύπτει ότι τα $(q_{n+1}\alpha - p_{n+1})$ και $a_{n+1}(q_n\alpha - p_n)$ έχουν αντίθετα πρόσημα.

Άρα,

$$|q_{n-1}\alpha - p_{n-1}| = |q_{n+1}\alpha - p_{n+1}| + a_{n+1}|q_n\alpha - p_n|.$$

Από την πρόταση 7.4.1 προκύπτει ότι

$$0 < \left|\frac{q_{n+1}\alpha - p_{n+1}}{q_n\alpha - p_n}\right| < \frac{1/q_{n+2}}{1/(q_{n+1} + q_n)} = \frac{q_{n+1} + q_n}{q_{n+2}} = \frac{q_{n+1} + q_n}{a_{n+2}q_{n+1} + q_n} \leq 1,$$

αφού $a_{n+2} \geq 1$. Συνεπώς

$$a_n = \left[\frac{|q_{n+1}\alpha - p_{n-1}|}{|q_n\alpha - p_n|}\right].$$

□

Παρατήρηση 7.4.4. Το όριο των συγκλινόντων ενός απείρου (απλού) συνεχούς κλάσματος λέγεται *τιμή* αυτού.

Αν για παράδειγμα $\alpha = [1; 1, 1, 1, \ldots]$, τότε

$$\alpha = 1 + \frac{1}{[1; 1, 1, 1, \ldots]} = 1 + \frac{1}{\alpha},$$

οπότε

$$\alpha = \frac{1 + \sqrt{5}}{2}.$$

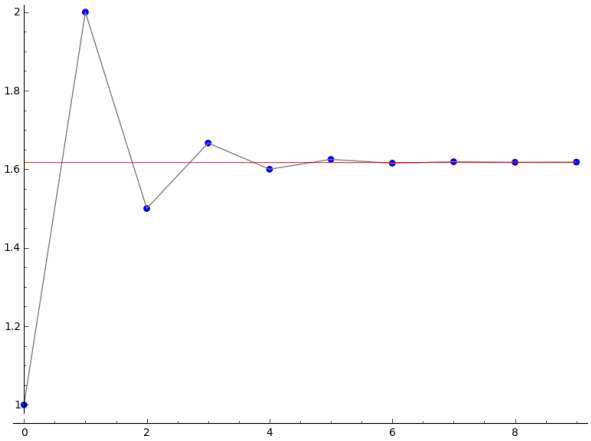
Οι συγκλίνοντες $\frac{p_n}{q_n}$ είναι το πηλίκο των αριθμών Fibonacci $\frac{F_{n+2}}{F_{n+1}}$.

Πράγματι, για $n = 0$, $\frac{p_0}{q_0} = \frac{a_0}{1} = \frac{1}{1} = \frac{F_2}{F_1}$.

Υποθέτουμε ότι ισχύει για k και για $k - 1$, δηλαδή,

$$\frac{p_k}{q_k} = \frac{F_{k+2}}{F_{k+1}} \text{ και } \frac{p_{k-1}}{q_{k-1}} = \frac{F_{k+1}}{F_k}.$$

Σχήμα 7.4.1: Συγκλίνοντες στην χρυσή αναλογία.



Επειδή $(p_k, q_k) = 1$ και $(F_{k+2}, F_{k+1}) = 1$, έπεται ότι $p_k = F_{k+2}$ και $q_k = F_{k+1}$ καθώς και $p_{k-1} = F_{k+1}$ και $q_k = F_k$. Επομένως,

$$\frac{p_{k+1}}{q_{k+1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{F_{k+2} + F_{k+1}}{F_{k+1} + F_k} = \frac{F_{(k+1)+2}}{F_{(k+1)+1}},$$

ισχύει και για $(k+1)$, άρα για κάθε φυσικό αριθμό n. Το όριο

$$\lim_{n\to\infty} \frac{F_{n+2}}{F_{n+1}} = \frac{1+\sqrt{5}}{2},$$

Στο πρόγραμμα sage παρακάτω υπολογίζουμε το συνεχές κλάσμα του αριθμού $\frac{1+\sqrt{5}}{2}$ και στη συνέχεια υπολογίζουμε την ακουλουθία των συγκλινόντων την οποία και ζωγραφίζουμε.

```
c=continued_fraction( (1+sqrt(5))/2)
v = [(i, c.convergent(i)) for i in range(10)]
P = point(v, rgbcolor=(0,0,1), pointsize=40)
L = line(v, rgbcolor=(0.5,0.5,0.5))
L2 = line([(0,c.value()),(10-1,c.value())], \
thickness=0.5, rgbcolor=(0.7,0,0))
(L+L2+P).show(xmin=0,ymin=1)
```

Πρόταση 7.4.5. *Κάθε άπειρο απλό συνεχές κλάσμα συγκλίνει σε έναν άρρητο (πραγματικό) αριθμό.*

Απόδειξη. Η απόδειξη θα γίνει με απαγωγή στο άτοπο.

Έστω $\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots]$, $a_i \in \mathbb{Z}$ και $a_i \geq 1$, για $i \geq 1$. Ο α είναι το όριο της ακολουθίας των συγκλινόντων. Από την πρόταση 7.4.1 προκύπτει ότι

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{n+1}q_n}.$$

Αν ο α ήταν ρητός, $\alpha = \frac{b}{c}$, $b, c \in \mathbb{Z}$, $(b, c) = 1$ τότε θα είχαμε

$$0 < |bq_n - cp_n| < \frac{c}{q_{n+1}q_n}.$$

Επειδή η $\{q_n\}_{n\in\mathbb{N}}$ είναι γνήσια αύξουσα ακολουθία ακέραιων, υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $c < q_{n+1}q_n$, δηλαδή $0 < |bq_n - cp_n| < 1$, άτοπο. □

Παρατήρηση 7.4.6. Από το πόρισμα 7.1.9 προκύπτει και η μοναδικότητα της παράστασης.

Παράδειγμα. Το συνεχές κλάσμα του

$$\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, \ldots] = [1; \overline{1, 2}].$$

Σε επόμενη παράγραφο θα υπολογίσουμε το συνεχές κλάσμα του e. Συγκεκριμένα θα αποδείξουμε ότι

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

δηλαδή ότι $a_0 = 2$ και για κάθε $m \geq 1$, $a_{3m} = a_{3m-2} = 1$ ενώ $a_{3m+1} = 2m$.

Πρόταση 7.4.7 (Dirichlet)**.** *Αν $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, τότε υπάρχουν άπειροι ρητοί αριθμοί p/q τέτοιοι ώστε*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Απόδειξη. Από την παρατήρηση 7.4.2 προκύπτει ότι για όλους τους κύριους συγκλίνοντες $\left\{\frac{p_n}{q_n}\right\}$ ισχύει η σχέση. □

7.5 Η βέλτιστη προσέγγιση

Η θεωρία των συνεχών κλασμάτων αποτελεί μια εξαιρετική μέθοδο προσέγγισης πραγματικών αριθμών με ρητούς. Το γενικό πρόβλημα είναι το περιεχόμενο ενός κλάδου της θεωρίας αριθμών που λέγεται *Διοφαντική προσέγγιση* (Diophantine Approximation).

Η κλασική θεωρία της διοφαντικής προσέγγισης χρησιμοποιεί εκτός της θεωρίας των συνεχών κλασμάτων και αυτές των σειρών Farey καθώς και το αξίωμα του Dirichlet ή αλλιώς το «αξίωμα του περιστερώνα».

Ορισμός 7.5.1. Το κλάσμα $\frac{p}{q}$ $(q > 0)$ λέγεται μία καλή προσέγγιση του $\alpha \in \mathbb{R}$, όταν για κάθε q', $1 \leq q' < q$ και οποιοδήποτε p', ισχύει:

$$|q'\alpha - p'| > |q\alpha - p|.$$

Παρατήρηση 7.5.2. Αν το p/q είναι μια καλή προσέγγιση του α τότε το p/q είναι ανάγωγο.

Απόδειξη. Αν $d := (p, q) > 1$ και $p = dp'$, $q = dq'$ τότε $1 < q' < q$ και

$$|q'\alpha - p'| < |q\alpha - p| = d|q'\alpha - p'|$$

άτοπο, αφού $d > 1$. □

Πρόταση 7.5.3. *Οι καλές προσεγγίσεις του $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ είναι οι συγκλίνουτες $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ του άπειρου απλού συνεχούς κλάσματος αυτού.*

Αυτό σημαίνει ότι, για κάθε $n \geq 1$, αν ισχύει

$$|b\alpha - a| < |q_n\alpha - p_n|,$$

τότε κατάνάγκη $b \geq q_{n+1}$.

Απόδειξη. Στο πρώτο βήμα θα αποδείξουμε ότι μια καλή προσέγγιση του α είναι κατ' ανάγκη μια κύρια σύγκλιση του α.

Έστω λοιπόν ότι $\frac{a}{b}$ ανάγωγο κλάσμα ($a, b \in \mathbb{Z}$) με $b > 0$ το οποίο είναι μια καλή προσέγγιση του α. Θα αποδείξουμε ότι υπάρχει $n \in \mathbb{N}$ τέτοιος ώστε

$$\frac{a}{b} = \frac{p_n}{q_n}.$$

Αν υποθέσουμε ότι $\frac{a}{b} < \frac{p_0}{q_0} = a_0$, τότε

$$|\alpha - a_0| < \left|\alpha - \frac{a}{b}\right| \Rightarrow |q_0\alpha - p_0| < |b\alpha - a|,$$

και επομένως ο $\frac{a}{b}$ δεν είναι καλή προσέγγιση του α.

Έστω τώρα ότι $\frac{a}{b} > \frac{p_1}{q_1}$. Επομένως

$$\left|\frac{a}{b} - \alpha\right| > \left|\frac{a}{b} - \frac{p_1}{q_1}\right| \geq \frac{1}{bq_1} \Rightarrow |b\alpha - a| > \frac{1}{q_1}.$$

Το

$$\frac{p_1}{q_1} = [a_0; a_1] = a_0 + \frac{1}{a_1} \Rightarrow \frac{1}{a_1} = \frac{p_1}{q_1} - a_0 = \frac{p_1}{q_1} - \frac{p_0}{q_0} = \frac{p_1q_0 - p_0q_1}{q_0q_1} = \frac{1}{q_0q_1}.$$

Ο α γράφεται

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}.$$

Άρα

$$|b\alpha - a| > \frac{1}{q_1} \geq \frac{1}{a_1} \geq |\alpha - a_0|,$$

άτοπο. Αν πάλι

$$\frac{p_{n-1}}{q_{n-1}} < \frac{a}{b} < \frac{p_n}{q_n},$$

τότε

$$\frac{1}{bq_{n-1}} \leq \left|\frac{a}{b} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_nq_{n-1}}.$$

Επομένως, $b > q_n$. Επίσης,

$$\frac{1}{bq_{n+1}} \leq \left|\frac{p_{n+1}}{q_{n+1}} - \frac{a}{b}\right| \leq \left|\alpha - \frac{a}{b}\right| \Rightarrow |q_n\alpha - p_n| < \frac{1}{q_{n+1}} \leq |b\alpha - a|,$$

και πάλι άτοπο.

Αποδείξαμε ότι κάθε καλή προσέγγιση του α θα πρέπει να είναι μια κύρια συγκλίνουσα αυτού. Το αντίστροφο θα το αποδείξουμε επαγωγικά.

Για $n = 0$, $\frac{p_0}{q_0} = a_0 \in \mathbb{Z}$ και το $q_0 = 1$, δηλαδή δεν υπάρχει q, $1 \leq q < q_0$. Συνεπώς η πρόταση είναι αληθής για $n = 0$.

Υποθέτουμε ότι είναι αληθής, για κάποιο $n \geq 0$, δηλαδή ότι ο $\frac{p_n}{q_n}$ είναι μια καλή προσέγγιση. Θα αποδείξουμε το ίδιο για τον $\frac{p_{n+1}}{q_{n+1}}$. Έστω q ο ελάχιστος ακέραιος $> q_n$ τέτοιος ώστε, για κάποιο p, να ισχύει

$$|q\alpha - p| < |q_n\alpha - p_n|.$$

Αν τώρα $1 < q' < q$ διακρίνουμε δύο περιπτώσεις.

Αν $q' < q_n$, τότε σύμφωνα με την υπόθεση της μαθηματικής επαγωγής υπάρχει p', τέτοιο ώστε $|q'\alpha - p'| > |q\alpha - p|$. Αν πάλι $q_n \leq q' < q$, τότε $|q'\alpha - p'| \geq |q_n\alpha - p_n| > |q\alpha - p|$.

Αυτό σημαίνει ότι το $\frac{p}{q}$ είναι επίσης μια καλή συγκλίνουσα. Σύμφωνα με το πρώτο μέρος της απόδειξης θα πρέπει το $\frac{p}{q}$ να συμπίπτει με μια κύρια συγκλίνουσα. Εξ ορισμού του q, έπεται ότι $q = q_{n+1}$ και τελικά $\frac{p}{q} = \frac{p_{n+1}}{q_{n+1}}$. □

Πόρισμα 7.5.4. *Αν $\frac{p}{q}$ είναι μια κύρια σύγκλιση του $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ και $m \in \mathbb{Z}$, $1 \leq m < q$, τότε*

$$\frac{1}{2q} < |m\alpha - m'|,$$

για κάποιο $m' \in \mathbb{Z}$.

Απόδειξη. Έστω $q = q_n$. Είναι γνωστό από την πρόταση 7.4.1 ότι

$$\frac{1}{2q_n} < |q_{n-1}\alpha - p_{n-1}|.$$

Από την πρόταση 7.5.3, έχουμε ότι ο $\frac{p_{n-1}}{q_{n-1}}$ είναι μια καλή προσέγγιση του α. Επειδή $1 \leq m < q_n$, έπεται ότι

$$|q_{n-1}\alpha - p_{n-1}| < |m\alpha - m'|,$$

για κάποιο $m' \in \mathbb{Z}$. □

Πόρισμα 7.5.5. *Αν $\frac{a}{b}$ είναι ένα ανάγωγο κλάσμα, $b > 0$ και τέτοιο ώστε*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

τότε το $\frac{a}{b}$ είναι μια κύρια σύγκλιση του α.

Απόδειξη. Σύμφωνα με την πρόταση 7.5.3 αρκεί να αποδείξουμε ότι $\frac{a}{b}$ είναι μια καλή προσέγγιση του α. Έστω $\frac{c}{d}$ κλάσμα, $d > 0$, $\frac{c}{d} \neq \frac{a}{b}$ τέτοιο ώστε

$$|d\alpha - c| \leq |b\alpha - a| < \frac{1}{2b}.$$

Το

$$\frac{1}{bd} \leq \left|\frac{c}{d} - \frac{a}{b}\right| \leq \left|\alpha - \frac{c}{d}\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bd} + \frac{1}{2b^2} = \frac{b+d}{2b^2d}.$$

Άρα,

$$\frac{1}{bd} < \frac{b+d}{2b^2d} \Rightarrow b < d,$$

δηλαδή ο $\frac{a}{b}$ είναι μια καλή προσέγγιση του α. □

Η επόμενη πρόταση μας δίνει ακριβέστερο φράγμα της ρητής προσέγγισης ενός πραγματικού (άρρητου) αριθμού α, φυσικά ως προς το μέγεθος του παρονομαστή του κλάσματος. Συγκεκριμένα ισχύει το:

Πρόταση 7.5.6 (Hurwitz). *Αν $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, υπάρχουν άπειροι ρητοί αριθμοί $\frac{a}{b}$ τέτοιοι ώστε να ισχύει*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2\sqrt{5}}.$$

Απόδειξη. Αυτό που θα αποδείξουμε είναι ότι από τρεις, οποιουσδήποτε συγκλίνοντες του πραγματικού αριθμού α, τουλάχιστον ένας από αυτούς επαληθεύει την ανισότητα. Έστω

$$\ell_n := \frac{q_n}{q_{n-1}}.$$

Αν η προς απόδειξη ανισότητα δεν ισχύει για τους συγκλίνοντες $\frac{p_{n-1}}{q_{n-1}}$ και $\frac{p_n}{q_n}$ θα αποδείξουμε ότι, σε ένα πρώτο βήμα, τότε κατ' ανάγκην

$$\ell_n + \ell_n^{-1} < \sqrt{5}.$$

Αφού για τους συγκλίνοντες $\frac{p_{n-1}}{q_{n-1}}$ και $\frac{p_n}{q_n}$ δεν ισχύει η ανισότητα, έχουμε:

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{q_{n-1}^2\sqrt{5}} + \frac{1}{q_n^2\sqrt{5}}.$$

Ο α, ως γνωστόν βρίσκεται ανάμεσα στις τιμές $\frac{p_{n-1}}{q_{n-1}}$ και $\frac{p_n}{q_n}$. Επομένως

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n-1}q_n}.$$

Συνδυάζοντας τις δύο σχέσεις έχουμε:

$$\frac{1}{q_{n-1}q_n} \geq \frac{1}{q_{n-1}^2\sqrt{5}} + \frac{1}{q_n^2\sqrt{5}},$$

από την οποία προκύπτει

$$\frac{q_n}{q_{n-1}} + \frac{q_{n-1}}{q_n} \leq \sqrt{5}.$$

Το αριστερό μέλος της ανισότητας είναι ένας ρητός αριθμός, ενώ το δεξιό άρρητος. Επομένως

$$\ell_n + \ell_n^{-1} < \sqrt{5}.$$

Στη συνέχεια υποθέτουμε ότι η προς απόδειξη ανισότητα δεν ισχύει για τρεις διαδοχικούς συγκλίνοντες

$$\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$$

και θα καταλήξουμε σε άτοπο.

Σύμφωνα με το πρώτο μέρος της απόδειξης έχουμε

$$\ell_n + \ell_n^{-1} < \sqrt{5} \text{ και } \ell_{n+1} + \ell_{n+1}^{-1} < \sqrt{5}.$$

Επειδή $\ell_n > 1$ για κάθε n, από τις τελευταίες ανισότητες προκύπτει ότι

$$\ell_n^{-1} > \frac{1}{2}(\sqrt{5} - 1) \text{ και } \ell_{n+1} < \frac{1}{2}(\sqrt{5} + 1).$$

Όμως, το

$$\ell_{n+1} = \frac{q_{n+1}}{q_n} = \frac{a_{n+1}q_n + q_{n-1}}{q_n} = a_{n+1} + \ell_n^{-1}.$$

Τελικά,

$$\frac{1}{2}(\sqrt{5} + 1) > \ell_{n+1} = a_{n+1} + \ell_n^{-1} > a_{n+1} + \frac{1}{2}(\sqrt{5} - 1) \geq 1 + \frac{1}{2}(\sqrt{5} - 1) = \frac{1}{2}(\sqrt{5} + 1),$$

άτοπο. □

Πρόταση 7.5.7. *Η σταθερά $\sqrt{5}$ είναι η βέλτιστη δυνατή.*

Απόδειξη. Θα αποδείξουμε ότι υπάρχει κάποιος πραγματικός αριθμός για τον οποίο η $\sqrt{5}$ δεν μπορεί να αντικατασταθεί από οποιαδήποτε μεγαλύτερη τιμή. Πράγματι, έστω $\alpha = \frac{1}{2}(\sqrt{5}+1)$. Το συνεχές κλάσμα του α είναι $[1;1,1,1,1\ldots]$. Για κάθε $n \geq 0$, αποδεικνύεται επαγωγικά ότι αν $\alpha = [1;1,\ldots,1,\alpha_n]$, τότε $\alpha_n = \frac{\sqrt{5}+1}{2}$. Παρατηρήστε ότι

$$\alpha_{n+1} = (\alpha_n - a_n)^{-1} = \left(\frac{\sqrt{5}+1}{2} - 1\right)^{-1} = \frac{1}{2}(\sqrt{5}+1).$$

Το $p_0 = q_0 = q_1 = 1$ και $p_1 = q_2 = 2$. Επίσης

$$p_n = p_{n-1} + p_{n-2} \text{ και } q_n = q_{n-1} + q_{n-2}.$$

Επαγωγικά αποδεικνύεται ότι για κάθε $n \geq 1$ ισχύει $q_n = p_{n-1}$. Επομένως,

$$\lim_{n\to\infty} \frac{q_{n-1}}{q_n} = \lim_{n\to\infty} \frac{q_{n-1}}{p_{n-1}} = \frac{1}{\alpha} = \frac{\sqrt{5}-1}{2}$$

και

$$\lim_{n\to\infty} \left(\alpha_{n+1} + \frac{q_{n-1}}{q_n}\right) = \frac{\sqrt{5}+1}{2} + \frac{\sqrt{5}-1}{2} = \sqrt{5}.$$

Αν τώρα c είναι μια οποιαδήποτε σταθερά, $c > \sqrt{5}$, τότε η ανισότητα

$$\alpha_{n+1} + \frac{q_{n-1}}{q_n} > c,$$

ισχύει για πεπερασμένο (το πολύ) πλήθος τιμών του n. Επομένως, σύμφωνα με το πόρισμα 7.1.9

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = -\frac{-(q_n p_{n-1} - p_{n-1}q_n)}{q_n(\alpha_{n+1}q_n + q_{n-1})} = \frac{(-1)^{n+1}}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

οπότε η

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q^2\left(\alpha_{n+1} + \frac{q_{n-1}}{q_n}\right)} < \frac{1}{cq_n^2}$$

ισχύει για πεπερασμένο πλήθος n.

Συνεπώς υπάρχουν πεπερασμένου πλήθους ρητοί $\frac{a}{b}$ οι οποίοι επαληθεύουν την ανισότητα

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{cb^2}.$$

Αφού $\frac{1}{cb^2} < \frac{1}{2b^2}$ και σύμφωνα με το πόρισμα 7.1.9, το κλάσμα $\frac{a}{b}$ συμπίπτει με κάποιον συγκλίνοντα $\frac{p_n}{q_n}$ του α. □

Παρατήρηση 7.5.8. Σύμφωνα με το θεώρημα του Hurwitz η διοφαντική ανισότητα

$$\left|\alpha - \frac{x}{y}\right| < \frac{c}{y^n}$$

έχει άπειρο πλήθος λύσεων αν ο $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, $n = 2$ και $c = \frac{1}{\sqrt{5}}$. Τι γίνεται όμως αν $n > 2$; Το ερώτημα αυτό θα μας οδηγήσει σε επόμενο κεφάλαιο στη μελέτη των υπερβατικών αριθμών και την αποδειξη του πεπερασμένου των λύσεων κλάσεων διοφαντικών εξισώσεων.

7.6 Ισοδύναμοι αριθμοί

Θεωρούμε το σύνολο των πινάκων

$$M = \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ με } a, b, c, d \in \mathbb{Z}, \det \sigma = \pm 1 \right\}.$$

Το M με πράξη τον πολλαπλασιασμό πινάκων αποτελεί ομάδα. Αν $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ και $\sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$ ορίζουμε

$$\sigma\alpha = \frac{a\alpha + b}{c\alpha + d}.$$

Αν $\sigma = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ και $\tau = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ τότε

$$\begin{aligned} \sigma(\tau(\alpha)) &= \sigma\left(\frac{a_1\alpha + b_1}{c_1\alpha + d_1}\right) \\ &= \frac{a_2 \frac{a_1\alpha+b_1}{c_1\alpha+d_1} + b_2}{c_2 \frac{a_1\alpha+b_1}{c_1\alpha+d_1} + d_2} \\ &= \frac{(a_2a_1 + b_2c_1)\alpha + (a_2b_1 + b_2d_1)}{(c_2a_1 + c_1d_2)\alpha + (c_2b_1 + d_2d_1)} = (\sigma\tau)(\alpha) \end{aligned}$$

και

$$I\alpha = \alpha, \text{ όπου } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ορισμός 7.6.1. Έστω $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ και $\beta \in \mathbb{R}\backslash\mathbb{Q}$. Θα λέμε ότι οι α, β είναι ισοδύναμοι αριθμοί αν και μόνο αν υπάρχει $\sigma \in M$ ώστε $\sigma\alpha = \beta$. Προφανώς η παραπάνω σχέση είναι σχέση ισοδυναμίας.

Παράδειγμα. Έστω $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Ο α γράφεται

$$\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n].$$

Έχουμε ότι

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}.$$

Έστω

$$\sigma_{n-1} := \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}.$$

Ο σ_{n-1} θα καλείται ο $(n-1)$-στος συνεχής μετασχηματισμός του α. Ώστε

$$\alpha = \sigma_{n-1}\alpha_n.$$

Το $\sigma_{n-1} \in M$. Άρα ο α είναι ισοδύναμος προς τον α_n, για $n \geq 1$, και οι α_n είναι ισοδύναμοι μεταξύ τους. Έστω

$$A_n := \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \text{ με } \det A_n = -1.$$

Ισχύει

$$\sigma_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_n p_{n-1} + p_{n-2} & p_{n-1} \\ a_n q_{n-1} + q_{n-2} & q_{n-1} \end{pmatrix} =$$

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \sigma_{n-1} A_n.$$

Δηλαδή

$$\sigma_n = A_0 A_1 \cdots A_n.$$

Θεώρημα 7.6.2. *Έστω* $\alpha, \beta \in \mathbb{R}\backslash\mathbb{Q}$ *και* $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$,

$$\alpha = \sigma\beta = \frac{a\beta + b}{c\beta + d}.$$

Υποθέτουμε ακόμη ότι $\beta > 1$ *και* $c > d > 0$. *Τότε* b/a *και* a/c *είναι δύο διαδοχικές κύριες συγκλίσεις του* α, *έστω οι* $\frac{p_{n-2}}{q_{n-2}}$, $\frac{p_{n-1}}{q_{n-1}}$ *και* $\beta = \alpha_n$.

Απόδειξη. Αφού $\sigma \in M$, έχουμε ότι $\det \sigma = \pm 1$ συνεπώς $ad - bc = \pm 1$. Άρα $(a, c) = 1$. Γράφουμε τον ρητό αριθμό a/c ως συνεχές κλάσμα.

$$\frac{a}{c} = [a_0; a_1, \ldots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}},$$

δηλαδή $a = p_{n-1}$ και $c = q_{n-1}$, αφού a/c ανάγωγο.

Στο συνεχές κλάσμα του $\frac{a}{c}$ μπορούμε να επιλέξουμε έτσι το n (αφού το μήκος ενός συνεχούς κλάσματος μπορεί να μεγαλώσει ή να μικραίνει κατά ένα, ανάλογα με τις επιθυμίες μας) ώστε

$$p_{n-1} q_{n-2} - p_{n-2} q_{n-1} = \varepsilon,$$

όπου $ad - bc = \varepsilon$, $\varepsilon = \pm 1$.

Άρα από τη σχέση $ad - bc = p_{n-1} d - q_{n-1} b = \varepsilon$ έχουμε $p_{n-1}(d - q_{n-2}) = q_{n-1}(b - p_{n-2})$. Αφού, ως γνωστόν, $(p_{n-1}, q_{n-1}) = 1$ έπεται ότι $q_{n-1} \mid (d - q_{n-2})$.

Αλλά $q_{n-2} \leq q_{n-1}$ και εξ υποθέσεως $d < q_{n-1} = c$. Δηλαδή

$$|d - q_{n-2}| < q_{n-1} \Rightarrow d - q_{n-2} = 0 \Rightarrow d = q_{n-2}$$

και ακολούθως $b = p_{n-2}$. Με βάση τα παραπάνω έχουμε

$$\alpha = \frac{a\beta + b}{c\beta + d} = \frac{p_{n-1}\beta + p_{n-1}}{q_{n-1}\beta + q_{n-2}}$$

που σημαίνει ότι το α μπορεί να γραφεί ως εξής:

$$\alpha = [a_0; a_1, \ldots, a_{n-1}, \beta].$$

Αφού από την υπόθεση $\beta > 1$ συνεπώς η παραπάνω έκφραση είναι το συνεχές κλάσμα του α, δηλαδή $\beta = \alpha_n$ και a/c και b/d είναι δύο διαδοχικές κύριες συγκλίσεις του α. □

Θεώρημα 7.6.3 (Serret). *Έστω α, β άρρητοι αριθμοί. Ο α είναι ισοδύναμος με τον β εάν και μόνο αν $\alpha_n = \beta_m$ για κάποιο ζευγάρι ακέραιων $n, m \geq 1$, ή ισοδύναμα για τα συνεχή κλάσματά τους*

$$\alpha = [a_0; a_1, a_2, \ldots], \beta = [b_0; b_1, b_2, \ldots]$$

ισχύει $a_n = b_{n+\ell}$ για κάποιο ℓ και όλα τα αρκούντως μεγάλα n.

Απόδειξη. Έστω ότι υπάρχουν ακέραιοι $k, \ell \geq 1$ τέτοιοι ώστε $\alpha_k = \beta_\ell$ δηλαδή

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k]$$

$$\beta = [b_0, b_1, \ldots, b_{\ell-1}, \beta_\ell],$$

$\alpha_k = \beta_\ell$. Αφού $\alpha \sim \alpha_k$ και $\beta \sim \beta_\ell$ έπεται ότι $\alpha \sim \beta$.

Αντιστρόφα. Έστω $\alpha \sim \beta$, δηλαδή

$$\beta = \sigma\alpha = \frac{a\alpha + b}{c\alpha + d}, \text{ όπου } \sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M.$$

Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $c\alpha + d > 0$, σε διαφορετική περίπτωση παίρνουμε ως $\sigma = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. Λόγω της σχέσης $\alpha = \sigma_{n-1}\alpha_n$, $\sigma_{n-1} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}$ έπεται ότι $\beta = \sigma\sigma_{n-1}\alpha_n$ και

$$\sigma\sigma_{n-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} =$$

$$= \begin{pmatrix} * & * \\ cp_{n-1} + dq_{n-1} & cp_{n-2} + dq_{n-2} \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Επομένως

$$cp_{n-1} + dq_{n-1} = q_{n-1}\left(c\frac{p_{n-1}}{q_{n-1}} + d\right) = c'$$

και

$$cp_{n-2} + dq_{n-2} = q_{n-2}\left(c\frac{p_{n-2}}{q_{n-2}} + d\right) = d'.$$

Παίρνουμε n αρκετά μεγάλο, ώστε $\frac{p_{n-1}}{q_{n-1}}$ και $\frac{p_{n-2}}{q_{n-2}}$ να πλησιάζουν πολύ κοντά στο α.

Αφού $c\alpha + d > 0$ συνεπάγεται, για αρκετά μεγάλο n, ότι $c' > 0$ και $d' > 0$. Εξ υποθέσεως (α_n είναι ο n-στός όρος στο συνεχές κλάσμα του αρρήτου α) έχουμε ότι $\alpha_n > 1$. Τελικά μπορούμε να θεωρήσουμε τον n άρτιο ή περιττό, έτσι ώστε $c' > d'$. Από το θεώρημα 7.6.2 έχουμε $\alpha_n = \beta_m$, για κάποιο m. Από την παραπάνω απόδειξη προκύπτει αμέσως το δεύτερο ισοδύναμο της πρότασης. □

Παράδειγμα. Έστω $\alpha = [a_0; a_1, a_2, \ldots]$. Προφανώς

$$\alpha = \frac{(-1)(-\alpha) + 0}{0(-\alpha) + 1} \Rightarrow \alpha \sim (-\alpha)$$

Πράγματι, εύκολα μπορεί να επαληθευθεί ότι

$$-\alpha = \begin{cases} [(-a_0 - 1); 1, a_1 - 1, a_2, a_3, \ldots] & \text{αν } a_1 > 1 \\ [(-a_0 - 1); a_2 + 1, a_3, a_4, \ldots] & \text{αν } a_1 = 1 \end{cases}.$$

Επίσης

$$\alpha = \frac{0\frac{1}{\alpha}+1}{1\frac{1}{\alpha}+0} \Rightarrow \alpha \sim \frac{1}{\alpha}$$

Πράγματι,

$$\frac{1}{\alpha} = \begin{cases} [0; a_0, a_1, \ldots,] & \text{αν } \alpha > 1 \\ [a_1; a_2, a_3, \ldots,] & \text{αν } 0 < \alpha < 1 \end{cases}$$

Στα 1879 ο A. Markoff δημοσίευσε ένα σημαντικό θεώρημα στην περιοχή των συνεχών κλασμάτων [1], [2].

Έστω $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ και α όχι ισοδύναμος προς τον $\vartheta_1 = \frac{1+\sqrt{5}}{2}$, δηλαδή $\alpha \nsim \vartheta_1$.

Υπάρχουν άπειροι ρητοί $\frac{p}{q}$, τέτοιοι ώστε

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{8}q^2}$$

και η σταθερά $\frac{1}{\sqrt{8}}$ είναι η βέλτιστη δυνατή αν ο α είναι ισοδύναμος προς τον $\vartheta_2 = 1 + \sqrt{2}$. Αν ο $\alpha \nsim \vartheta_1, \vartheta_2$, τότε υπάρχουν άπειροι ρητοί $\frac{p}{q}$ τέτοιοι ώστε

$$\left|\alpha - \frac{p}{q}\right| < \frac{5}{\sqrt{221}q^2}$$

και η σταθερά $\frac{5}{\sqrt{221}}$ είναι η βέλτιση δυνατή αν ο α είναι ισοδύναμος προς τον $\vartheta_3 := \frac{9+\sqrt{221}}{10}$. Συγκεκριμένα ισχύει το ακόλουθο θεώρημα του Markoff (1879):

Θεώρημα 7.6.4. *Υπάρχει μια ακολουθία ακέραιων (λέγεται ακολουθία Markoff)*

$$1, 2, 5, 13, 29, 34, \ldots$$

και μια αντίστοιχη ακολουθία τετραγωνικών αρρήτων ϑ_i οι οποίοι ανήκουν στα τετραγωνικά σώματα

$$\mathbb{Q}(\sqrt{D_i}) = \{a + b\sqrt{D_i} | a, b \in \mathbb{Q}\},$$

όπου $D_i := 9m_i^2 - 4$ και m_i ο i-στός όρος της ακολουθίας Markoff με την ακόλουθη ιδιότητα:

$$Αν\ \alpha \in \mathbb{R}\backslash\mathbb{Q}, \alpha \nsim \vartheta_i,\ για\ m_i < m_j,$$

τότε υπάρχουν άπειροι ρητοί $\frac{p}{q}$ τέτοιοι ώστε να ισχύει

$$\left|\alpha - \frac{p}{q}\right| < \frac{m_j}{\sqrt{D_j}q^2}.$$

Η σταθερά $\frac{m_j}{\sqrt{D_j}}$ είναι η βέλτιστη δυνατή τότε και μόνο τότε όταν $\alpha \sim \vartheta_h$, για κάποιο h τέτοιο ώστε $m_h = m_j$.

Τα ζεύγη (m_i, ϑ_i) αντιστοιχούν αμφιμονοσήματνα στις κλάσεις θετικών τριάδων ακέραιων (p, q, r), κατά προσέγγιση μεταθέσεων, οι οποίες τριάδες επαληθεύουν τη διοφαντική εξίσωση

$$p^2 + q^2 + r^2 = 3pqr.$$

Ένα καλά ορισμένο σύνολο αντιπροσώπων ορίζεται ως εξής: Ξεκινούμε από τις τριάδες

$$(1,1,1),(1,1,2),(2,1,5)$$

και συνεχίζουμε από την τριάδα (p,q,r) στις τριάδες $(r,q,3rq-p)$ και $(p,r,3rp-q)$. Η ακολουθία του Markoff είναι η διατεταγμένη ακολουθία των αριθμών r. Η απόδειξη του θεωρήματος ξεπερνά τους στόχους του παρόντος βιβλίου. Παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο [6].

7.7 Περιοδικά συνεχή κλάσματα

Θεωρούμε τον πραγματικό αριθμό $\alpha = \frac{29+\sqrt{15}}{7}$. Υπολογίζουμε το άπειρο συνεχές κλάσμα αυτού:

$$\alpha = [4;1,2,3,2,3,2,3,\ldots].$$

Παρατηρούμε ότι υπάρχει μια επανάληψη των ψηφίων $2,3$, δηλαδή μια περιοδικότητα αυτών. Επίσης το συνεχές κλάσμα του

$$\alpha = 1+\sqrt{2} = [2;2,2,2,\ldots].$$

Είναι, λοιπόν, αυτονόητο να δοδεί ο ακόλουθος

Ορισμός 7.7.1. Ένα άπειρο απλό συνεχές κλάσμα $[a_0;a_1,a_2,\ldots,]$ λέγεται περιοδικό συνεχές κλάσμα, όταν υπάρχουν θετικοί ακέραιοι n και k τέτοιοι ώστε

$$a_m = a_{m+k} \text{ για κάθε } m \geq n.$$

Χρησιμοποιούμε τον συμβολισμό

$$[a_0;a_1,a_1,\ldots,a_{n-1},\overline{a_n,a_{n+1},\ldots,a_{n+k-1}}].$$

Το συνεχές κλάσμα του $\alpha = \frac{29+\sqrt{15}}{7}$ γράφεται

$$\alpha = [4;1,\overline{2,3}].$$

Θα λέμε ότι το συνεχές κλάσμα του α είναι *καθαρά περιοδικό* όταν υπάρχει κάποιος φυσικός k τέτοιος ώστε $a_{n+k} = a_n$ για όλα τα n, δηλαδή όταν

$$\alpha = [\overline{a_0;a_1,a_2,\ldots,a_{k-1}}].$$

Το συνεχές κλάσμα του $\alpha = 1+\sqrt{2}$ είναι καθαρά περιοδικό και $\alpha = [\overline{2}]$. Τέλος, το k λέγεται πρωταρχική περίοδος, αν είναι ο μικρότερος ακέραιος με αυτή την ιδιότητα.

Στη συνέχεια θα εξετάσουμε πότε το συνεχές κλάσμα ενός αρρήτου πραγματικού αριθμού είναι περιοδικό ή καθαρά περιοδικό.

Ορισμός 7.7.2. Ο πραγματικός αριθμός α λέγεται *άρρητη ποσότητα δευτέρου βαθμού* όταν είναι άρρητος και ρίζα ενός πολυωνύμου δευτέρου βαθμού

$$Ax^2+Bx+C,$$

με ακέραιους συντελεστές $(A,B,C)=1$ και $A>0$.

Το $\alpha = \frac{29+\sqrt{15}}{7}$ είναι ρίζα του πολυωνύμου

$$49x^2 - 406x + 826.$$

Επειδή οι ρίζες του πολυωνύμου $Ax^2 + Bx + C$ δεν είναι ρητοί αριθμοί έπεται ότι η διακρίνουσα του α

$$D(\alpha) = B^2 - 4AC > 0$$

και $D(\alpha)$ όχι τέλειο τετράγωνο. Συνεπώς $D(\alpha) = f^2 d$, όπου $d > 1$ ελεύθερος τετραγώνου και ο α γράφεται στη μορφή $\alpha = a + b\sqrt{d}$, με $a, b \in \mathbb{Q}$. Η δεύτερη ρίζα του πολυωνύμου θα είναι η

$$\alpha' = a - b\sqrt{d}$$

και θα λέγεται συζυγής του α.

Το σύνολο

$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$$

με πράξεις τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών είναι σώμα.

Ορισμός 7.7.3. Αν ο α είναι άρρητη ποσότητα δευτέρου βαθμού, ο α θα λέγεται ανάγωγος (reduced) όταν $\alpha > 1$ και $-1 < \alpha' < 0$.

Παρατήρηση 7.7.4. Αν ο α είναι ανάγωγος, τότε και ο $-\frac{1}{\alpha'}$ είναι επίσης ανάγωγος.

Πρόταση 7.7.5. *Αν D θετικός ακέραιος $D = f^2 d$ και d όχι τέλειο τετράγωνο, υπάρχουν πεπερασμένου πλήθους ανάγωγα στοιχεία στο σώμα $K = \mathbb{Q}(\sqrt{d})$ διακρίνουσας D.*

Απόδειξη. Έστω $\alpha \in K$ ανάγωγος. Ο α είναι λύση της εξίσωσης

$$Ax^2 + Bx + C = 0,$$

και $D(a) = B^2 - 4AC = D$. Επομένως

$$\alpha = \frac{-B + \varepsilon\sqrt{D}}{2A} > 1$$

και

$$-1 < \frac{-B - \varepsilon\sqrt{D}}{2A} < 0,$$

όπου $\varepsilon = \pm 1$. Αν ήταν $\varepsilon = -1$ θα είχαμε $-B - \sqrt{D} > 0$ και $-B + \sqrt{D} < 0$, άτοπο. Επομένως $\varepsilon = 1$, οπότε

$$-B + \sqrt{D} > 2A > B + \sqrt{D}.$$

Έτσι $-2B > 0$ άρα $B < 0$ και $\frac{-B-\sqrt{D}}{2A} < 0$ συνεπώς $0 < -B < \sqrt{D}$. Αυτό σημαίνει ότι για το $|B|$ έχουμε πεπερασμένου πλήθους δυνατότητες, οπότε και για το A ισχύει το ίδιο.

Τέλος, από τη σχέση $D = B^2 - 4AC$ το ίδιο ισχύει για το C. □

Πρόταση 7.7.6. *Αν το α έχει διακρίνουσα $D(\alpha) = D > 0$ και ο β είναι ισοδύναμος προς τον α τότε και ο β έχει την ίδια διακρίνουσα. Επίσης, αν $m \in \mathbb{Z}$ και $\beta = \alpha + m$, τότε και πάλι ισχύει $D(\beta) = D(\alpha) = D$.*

Απόδειξη. Η απόδειξη είναι απλή και αφήνεται ως άσκηση στον αναγνώστη. □

Θεώρημα 7.7.7. *Υποθέτουμε ότι α είναι ένας πραγματικός τετραγωνικός και άρρητος αριθμός. Ισχύουν τα ακόλουθα:*

- *Στο συνεχές κλάσμα του α*
$$\alpha = [a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n]$$
ο α_n έχει την ίδια διακρίνουσα με του α για κάθε $n \geq 1$.
- *Αν ο α είναι ανάγωγος, τότε και ο α_n είναι ανάγωγος για κάθε $n \geq 1$.*
- *Αν ο α δεν είναι ανάγωγος τότε υπάρχει $n_0 \in \mathbb{N}$ τέτοιος ώστε για κάθε $n \geq n_0$ ο α_n να είναι ανάγωγος.*

Απόδειξη. (1) Γνωρίζουμε ήδη ότι $\alpha \sim \alpha_n$ για κάθε $n \geq 1$. Το συμπέρασμα είναι άμεση συνέπεια της πρότασης 7.7.6.

(2) Γνωρίζουμε ότι, για κάθε $n \geq 1$, ισχύει $\alpha_n > 1$. Ο α είναι εξ υποθέσεως ανάγωγος. Επομένως $\alpha > 1$ και $-1 < -\alpha' < 0$. Από $\alpha > 1$ έπεται ότι $a_0 = [\alpha] \geq 1$. Αν $\alpha = a_0 + \frac{1}{\alpha_1}$, προκύπτει ότι $\alpha_1 > 1$ και $-\frac{1}{\alpha_1'} = a_0 - \alpha' = a_0 + (-\alpha') > 1$. Επομένως και ο α_1 είναι ανάγωγος. Επαγωγικά αποδεικνύεται ότι ο α_n είναι ανάγωγος για κάθε $n \geq 1$.

(3) Ο
$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}.$$
Λύνουμε ως προς α_n
$$\alpha_n = \frac{p_{n-2} - \alpha q_{n-2}}{\alpha q_{n-1} - p_{n-1}} = -\frac{\alpha q_{n-2} - p_{n-2}}{\alpha q_{n-2} - p_{n-1}}.$$
Επομένως,
$$\alpha_n' = -\frac{\alpha' q_{n-2} - p_{n-2}}{\alpha' q_{n-2} - p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\alpha' - \frac{p_{n-2}}{q_{n-2}}}{\alpha' - \frac{p_{n-1}}{q_{n-1}}}\right).$$
Για αρκετά μεγάλο n, τα κλάσματα $\frac{p_{n-2}}{q_{n-2}}$ και $\frac{p_{n-1}}{q_{n-1}}$ παριστούν μια πολύ καλή προσέγγιση του α και συνεπώς η παραπάνω παράσταση συγκλίνει στο $\frac{\alpha'-\alpha}{\alpha'-\alpha}$, οπότε έχουμε $\alpha_n' < 0$. Υπενθυμίζουμε ότι $q_n > 0$ για κάθε n.

Στη συνέχεια θα αποδείξουμε ότι $\alpha_n' > -1$.

$$\begin{aligned}
\alpha_n' &= -\frac{q_{n-2}\alpha' - p_{n-2}}{q_{n-1}\alpha' - p_{n-1}} = -\frac{q_{n-1}(q_{n-2}\alpha' - p_{n-2})}{q_{n-1}(q_{n-1}\alpha' - p_{n-1})} = \\
&= -\frac{q_{n-1}q_{n-2}\alpha' - q_{n-1}p_{n-2}}{q_{n-1}(q_{n-1}\alpha' - p_{n-1})} = -\frac{q_{n-1}q_{n-2}\alpha' - p_{n-1}q_{n-2} - (-1)^{n-1}}{q_{n-1}(q_{n-1}\alpha' - p_{n-1})} = \\
&= -\frac{q_{n-2}(q_{n-1}\alpha' - p_{n-1}) - (-1)^{n-1}}{q_{n-1}(q_{n-1}\alpha' - p_{n-1})} = -\frac{q_{n-2}}{q_{n-1}} - \frac{(-1)^{n-1}}{q_{n-1}(q_{n-1}\alpha' - p_{n-1})} = \\
&= \frac{1}{q_{n-1}}\left(-q_{n-2} - \frac{(-1)^{n-1}}{q_{n-1}\alpha' - p_{n-1}}\right) = \\
&= \frac{1}{q_{n-1}\left(-q_{n-1} - \frac{(-1)^{n-1}}{q_{n-1}}\left(\alpha' - \frac{p_{n-1}}{q_{n-2}}\right)\right)} = \frac{1}{q_{n-1}}.
\end{aligned}$$

Επομένως

$$\alpha'_n + 1 = \frac{1}{q_{n-1}}\left(q_{n-1} + q_{n-2} - \frac{(-1)^{n-1}}{q_{n-1}\left(\alpha' - \frac{p_{n-1}}{q_{n-1}}\right)}\right)$$

Για αρκετά μεγάλο n, ο όρος $\frac{1}{q_{n-1}\left(\alpha' - \frac{p_{n-1}}{q_{n-1}}\right)}$ είναι ο μικρός. Επομένως $\alpha'_n + 1 > 0$. □

Πρόταση 7.7.8. *Έστω ότι ο α είναι ανάγωγος και $a \in \mathbb{Z}$ τέτοιος ώστε $\alpha = a + \frac{1}{\alpha_1}$. Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:*

1. *Ο α_1 είναι ανάγωγος.*
2. *Ο $a = [\alpha]$.*

Απόδειξη. $2 \Rightarrow 1$ Αν $a = [\alpha]$ τότε $a < \alpha < a + 1$ συνεπώς $0 < \alpha - a < 1$ και $1 < \frac{1}{\alpha - a} = \alpha_1$. Επίσης, ο $a \geq 1$ και $\alpha' < 0$. Άρα

$$\alpha'_1 = \frac{1}{\alpha' - a} < 0.$$

Από τη σχέση $\alpha' - a < -1$, έπεται ότι

$$-1 < \frac{1}{\alpha' - a} = \alpha'_1,$$

δηλαδή ο α_1 είναι ανάγωγος.

$1 \Rightarrow 2$. Αν ήταν $\alpha < a$ θα είχαμε

$$\frac{1}{\alpha_1} = \alpha - a < 0 \Rightarrow \alpha_1 < 0,$$

άτοπο. Αν πάλι $a + 1 < \alpha$ τότε $\frac{1}{\alpha_1} = \alpha - a > 1$ και τελικά $\alpha_1 > 1$, άτοπο.

Επομένως $a < \alpha < a + 1$, δηλαδή $\alpha = [a]$. □

Παρατήρηση 7.7.9. Στην πρόταση 7.7.8 τα α, α_1 καθορίζονται μονοσήμαντα το ένα από το άλλο.

Το θεώρημα που ακολουθεί είναι το σημαντικότερο του κεφαλαίου. Η μια κατεύθυνση αποδείχθηκε από τον Euler το 1737 και η άλλη από τον Lagrange το 1770, και ονομάζεται

Θεώρημα 7.7.10 (Euler-Lagrange)**.** *Έστω $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Το άπειρο απλό συνεχές κλάσμα του α είναι περιοδικό τότε και μόνο τότε όταν ο α είναι τετραγωνικός, δηλαδή άρρητη ποσότητα δευτέρου βαθμού.*

Υποθέτουμε τώρα ότι ο α είναι τετραγωνικός. Ο α είναι ανάγωγος τότε και μόνο τότε όταν ο α είναι καθαρά περιοδικός.

Απόδειξη. Υποθέτουμε ότι α είναι τετραγωνικός (άρρητη ποσότητα δευτέρου βαθμού). Σύμφωνα με το θεώρημα 7.7.7 υπάρχει $n_0 \in \mathbb{N}$ τέτοιος ώστε, για κάθε $n \geq n_0$, ο α_n είναι ανάγωγος. Από την πρόταση 7.7.5 έπεται ότι υπάρχουν το πολύ πεπερασμένου πλήθους τιμές για το α_n. Επομένως, για κάποιο $n \in \mathbb{N}$ και $k > 1$, ισχύει $\alpha_n = \alpha_{n+k}$, δηλαδή το συνεχές κλάσμα του α είναι περιοδικό.

Ας υποθέσουμε τώρα ότι ο α είναι ανάγωγος και έστω α_m ο πρώτος όρος του συνεχούς κλάσματος του α ο οποίος συμπίπτει με κάποιο επόμενο όρο της ακολουθίας του α_{m+k}, δηλαδή

$$\alpha_m = \alpha_{m+k} \text{ με } m > 0 \text{ και } k \geq 1.$$

Από την πρόταση 7.7.8 και την παρατήρηση 7.7.9, προκύπτει ότι ο α_{m-1} ορίζεται μονοσήμαντα από τον α_m. Επομένως $\alpha_{m-1} = \alpha_{m+k-1}$, άτοπο λόγω του ορισμού του m.

Επομένως $m = 0$ και το συνεχές κλάσμα του α είναι καθαρά περιοδικό. Αντίστροφα, αν το συνεχές κλάσμα του α είναι καθαρά περιοδικό, μπορούμε να γράψουμε

$$\alpha = [\overline{a_0; a_1, \ldots, a_m}] = [a_0; a_1, \ldots, a_m, \alpha].$$

Από τη γνωστή σχέση $\alpha = \sigma_m\alpha$ προκύπτει ότι ο α είναι τετραγωνικός. Συγκεκριμένα, από τη σχέση

$$\alpha = \frac{p_{m-1}\alpha + p_{m-2}}{q_{m-1}\alpha + q_{m-2}},$$

έπεται ότι

$$q_{m-1}\alpha^2 - (p_{m-1} - q_{m-2})\alpha - p_{m-2} = 0.$$

Η διακρίνουσα

$$D(\alpha) = (p_{m-1} - q_{m-2})^2 + 4p_{m-2}q_{m-2} > 0.$$

Επομένως ο α είναι άρρητη ποσότητα δευτέρου βαθμού. Επίσης ισχύει (θεώρημα 7.7.7) ότι $\alpha = \alpha_n$ και για αρκετά μεγάλο n ο α_n είναι ανάγωγος οπότε και ο α.

Αν τώρα το το συνεχές κλάσμα του α είναι απλά περιοδικό, δηλαδή

$$\alpha = [a_0; a_1, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+k}}],$$

τότε ο

$$\alpha_{r+1} = [\overline{a_{r+1}, \ldots, a_{r+k}}]$$

είναι καθαρά περιοδικός δηλαδή και τετραγωνικός. Τώρα ο $\alpha = \sigma_{r+1}\alpha_{r+1}$, δηλαδή $\alpha \sim \alpha_{r+1}$ συνεπώς και ο α τετραγωνικός. □

Πρόταση 7.7.11. *Υποθέτουμε ότι ο $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ είναι τετραγωνικός ανάγωγος. Αν*

$$\alpha = [\overline{a_0; a_1, a_2, \ldots, a_{n-1}}],$$

τότε

$$-\frac{1}{\alpha'} = [\overline{a_{n-1}; a_{n-2}, \ldots, a_1, a_0}]$$

Απόδειξη. Έστω $\beta = [\overline{a_{n-1}; a_{n-2}, \ldots, a_1, a_0}]$ και $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$, $\left\{\frac{p'_n}{q'_n}\right\}_{n\in\mathbb{N}}$, οι συγκλίνοντες των α και β, αντίστοιχα.

Εξ ορισμού της περιοδικότητας έχουμε

$$\alpha = [a_0; a_1, a_2, \ldots, a_{n-1}, \alpha]$$

και

$$\beta = [a_{n-1}; \ldots, a_1, a_0, \beta].$$

Επομένως,

$$\alpha = \frac{\alpha p_{n-1} + p_{n-2}}{\alpha q_{n-1} + q_{n-2}}$$

και

$$\beta = \frac{\beta p'_{n-1} + p'_{n-2}}{\beta q'_{n-1} + q'_{n-2}}.$$

Τα α, β είναι λύσεις των εξισώσεων δευτέρου βαθμού,

$$q_{n-1}X^2 + (q_{n-2} - p_{n-1})X - p_{n-2} = 0$$

και

$$q'_{n-1}X^2 + (q'_{n-2} - p'_{n-1})X - p'_{n-2} = 0,$$

αντίστοιχα. Από τη δεύτερη προκύπτει ότι,

$$p'_{n-2}\left(\frac{-1}{\beta}\right)^2 + (q'_{n-2} - p'_{n-1})\left(\frac{-1}{\beta}\right) - q'_{n-1} = 0.$$

Οι εκφράσεις των α, β μπορούν να γραφούν ως εξής: Υπάρχουν $\kappa, \lambda \in \mathbb{R}$, $\kappa \cdot \lambda \neq 0$, τέτοιοι ώστε

$$\kappa\begin{pmatrix}\alpha\\1\end{pmatrix} = \begin{pmatrix}\alpha p_{n-1} + p_{n-2}\\ \alpha q_{n-1} + q_{n-2}\end{pmatrix} = \begin{pmatrix}p_{n-1} & p_{n-2}\\ q_{n-1} & q_{n-2}\end{pmatrix}\begin{pmatrix}\alpha\\1\end{pmatrix}$$

και

$$\lambda\begin{pmatrix}\beta\\1\end{pmatrix} = \begin{pmatrix}\beta p'_{n-1} + p'_{n-2}\\ \beta q'_{n-1} + q'_{n-2}\end{pmatrix}\begin{pmatrix}p'_{n-1} & p'_{n-2}\\ q'_{n-1} & q'_{n-2}\end{pmatrix}\begin{pmatrix}\beta\\1\end{pmatrix}.$$

Όμως

$$\begin{pmatrix}p_{n-1} & p_{n-2}\\ q_{n-1} & q_{n-2}\end{pmatrix} = \begin{pmatrix}a_0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}a_1 & 1\\1 & 0\end{pmatrix}\cdots\begin{pmatrix}a_{n-1} & 1\\1 & 1\end{pmatrix}$$

και

$$\begin{pmatrix}p'_{n-1} & q'_{n-1}\\ p'_{n-2} & q'_{n-2}\end{pmatrix}\begin{pmatrix}a_{n-1} & 1\\1 & 0\end{pmatrix}\begin{pmatrix}a_{n-2} & 1\\1 & 0\end{pmatrix}\cdots\begin{pmatrix}a_0 & 1\\1 & 0\end{pmatrix}.$$

Επομένως,

$$\begin{pmatrix}p_{n-1} & p_{n-2}\\ q_{n-1} & q_{n-2}\end{pmatrix} = \begin{pmatrix}p'_{n-1} & p'_{n-2}\\ q'_{n-1} & q'_{n-2}\end{pmatrix}^t$$

οπότε,

$$p_{n-1} = p'_{n-1}, p_{n-2} = q'_{n-1}, q_{n-1} = p'_{n-2} \text{ και } q_{n-2} = q'_{n-2}.$$

Αυτό σημαίνει ότι ο α και ο $\frac{-1}{\beta}$ είναι λύσεις της ίδιας τετραγωνικής εξίσωσης. Οι ρίζες αυτής είναι τα α και α'. Ο $\frac{-1}{\beta}$ λοιπόν θα είναι είτε ο α είτε ο α'. Το συνεχές κλάσμα του α είναι καθαρά περιοδικό. Επομένως ο $a_0 = a_n \geq 1$ από το οποίο προκύπτει ότι $\alpha, \beta > 0$ και $-\frac{1}{\beta} < 0$. Τελικά, $\alpha' = -\frac{1}{\beta}$, δηλαδή $\beta = -\frac{1}{\alpha'}$. □

Πρόταση 7.7.12. *Υποθέτουμε ότι $D \in \mathbb{N}$, δεν είναι τέλειο τετράγωνο ακέραιου. Το συνεχές κλάσμα του $\sqrt{D}$ είναι,*

$$\sqrt{D} = [a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

και $a_{n-i} = a_i$ για $i = 1, 2, \ldots, n-1$.

Απόδειξη. Ο $a_0 = [\sqrt{D}]$. Θεωρούμε τον αριθμό $\alpha = a_0 + \sqrt{D}$. Το συνεχές κλάσμα του $\sqrt{D}$ και του α διαφέρουν μόνο ως προς τον πρώτο όρο. Ο πρώτος όρος του $\sqrt{D}$ είναι a_0 ενώ του $\alpha = a_0 + \sqrt{D}$ είναι $[a_0 + \sqrt{D}] = 2a_0$.

Ο α είναι ανάγωγος, αφού $\alpha > 1$, και

$$-1 < \alpha' = a_0 - \sqrt{D} < 0.$$

Επομένως το συνεχές κλάσμα του α είναι καθαρά περιοδικό

$$\alpha = [\overline{2a_0; a_1, a_2, \ldots, a_{n-1}}].$$

Από αυτή την έκφραση προκύπτει αμέσως ότι

$$\gamma := \frac{1}{\alpha - 2a_0} = [\overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

Εφαρμόζουμε την πρόταση 7.7.11:

$$[\overline{2a_0; a_{n-1}, \ldots, a_2, a_1}] = -\frac{1}{\gamma'} = -(\alpha - 2a_0)' =$$

$$= -(\alpha' - 2a_0) = -\alpha' + 2a_0 = -a_0 + \sqrt{D} + 2a_0 = a_0 + \sqrt{D} = \alpha$$

από την οποία προκύπτει ότι $a_i = a_{n-i}$ για κάθε $i = 1, 2, \ldots, n-1$. □

Παράδειγμα. (1) Από τα προηγούμενα προκύπτουν οι:

$$\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}]$$

$$\sqrt{73} = [8; \overline{1, 1, 5, 5, 1, 1, 16}]$$

$$\sqrt{94} = [9; \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}]$$

(2) Να αποδείχθεί ότι το απλό συνεχές κλάσμα της $\sqrt{D}$, όπου D θετικός ακέραιος, έχει περίοδο 1 τότε και μόνο τότε όταν $D = a^2 + 1$ όπου ο a είναι κάποιος θετικός ακέραιος.

Απόδειξη. Πράγματι, αν το συνεχές κλάσμα του $\sqrt{D}$ έχει περίοδο 1, θα έχει τη μορφή $[a_0; \overline{2a_0}]$. Επομένως

$$\sqrt{D} = a_0 + \cfrac{1}{2a_0 + \cfrac{1}{2a_0 + \cfrac{1}{\cdots}}}$$

Αν ονομάσουμε

$$\varphi := 2a_0 + \cfrac{1}{2a_0 + \cfrac{1}{2a_0 + \cdots}},$$

τότε έχουμε

$$\varphi = 2a_0 + \frac{1}{\varphi} \Rightarrow \varphi^2 - 2a_0\varphi + 1 = 0.$$

Οι ρίζες της εξίσωσης αυτής είναι

$$\varphi_{1,2} = \frac{2a_0 \pm \sqrt{4a_0^2 + 4}}{2} = a_0 \pm \sqrt{a_0^2 + 1}.$$

Επειδή ο $\varphi > 0$, έπεται ότι $\varphi = a_0 + \sqrt{a_0^2 + 1}$. Επομένως

$$\frac{1}{\varphi} = \frac{a_0 - \sqrt{a_0^2 + 1}}{a_0^2 - (a_0^2 + 1)} = \sqrt{a_0^2 + 1} - a_0,$$

οπότε

$$\sqrt{D} = a_0 + \frac{1}{\varphi} = a_0 + \sqrt{a_0^2+1} - a_0 = \sqrt{a_0^2+1},$$

και $a_0 = [\sqrt{D}] \geq 1$.

Αντίστροφα, αν $D = a^2 + 1$, τότε

$$\begin{aligned}\sqrt{D} &= a + (\sqrt{a^2+1} - a) = \\ &= a + \frac{1}{\sqrt{a^2+1} - a} = \\ &= a + \frac{1}{2a + (\sqrt{a^2+1} - a)} = a + \frac{1}{2a + \frac{1}{2a + \cdots}}.\end{aligned}$$

Έτσι $\sqrt{2} = [1, \overline{2}]$, $\sqrt{5} = [2, \overline{4}]$, $\sqrt{10} = [3, \overline{6}]$, $\sqrt{50} = [7, \overline{14}]$. □

(3) Αν $a, b, c \in \mathbb{N}$, τότε

$$\alpha = [a, \overline{b, c}] = a + \varphi = a + \frac{1}{b + \frac{1}{c + \varphi}}.$$

Επομένως,

$$\varphi = \frac{1}{b + \frac{1}{c + \varphi}} = \frac{c + \varphi}{bc + b\varphi + 1}$$

συνεπώς

$$b\varphi^2 + bc\varphi - c = 0.$$

Οι ρίζες της δευτεροβάθμιας εξίσωσης είναι

$$\varphi_{1,2} = -\frac{c}{2} \pm \sqrt{\left(\frac{c}{2}\right)^2 + \frac{c}{b}}.$$

Συνεπώς,

$$\alpha = a - \frac{c}{2} + \sqrt{\left(\frac{c}{2}\right)^2 + \frac{c}{b}}.$$

Ειδικότερα αν $c = 2a$, τότε $\alpha = [a, \overline{b, 2a}]$. Αν επιπλέον, $b = 1, 2$ ή a τότε έχουμε

$$\alpha = \sqrt{a^2 + 2a} = [a; \overline{1, 2a}],$$

$$\alpha = \sqrt{a^2 + a} = [a; \overline{2, 2a}],$$

$$\alpha = \sqrt{a^2 + 2} = [a; \overline{a, 2a}],$$

αντίστοιχα.

Έχουμε υπολογίσει γενικούς τύπους για το συνεχές κλάσμα διαφόρων κλάσεων αρρήτων ποσοτήτων δευτέρου βαθμού. Για παράδειγμα αν $\alpha = \sqrt{63}$, τότε $\alpha = [7; 1, 14]$, αν $\alpha = \sqrt{132}$ τότε $\alpha = [11; \overline{2, 22}]$ και αν $\alpha = \sqrt{225}$, τότε $\alpha = [15; \overline{15, 30}]$.

7.8 Συνεχή κλάσματα και παραγοντοποίηση

Υπενθυμίζουμε ότι μπορούμε να παραγοντοποιήσουμε έναν θετικό ακέραιο n με τη μέθοδο του Fermat, αν υπάρχουν θετικοί ακέραιοι x, y τέτοιοι ώστε

$$x^2 - y^2 = n \text{ και } x - y \neq 1.$$

Είναι πιθανό, όμως, να μπορέσουμε να παραγοντοποιήσουμε τον n αν υπάρχουν x, y θετικοί ακέραιοι οι οποίοι ικανοποιούν την ασθενέστερη συνθήκη:

$$x^2 \equiv y^2 \mathrm{mod} m, 0 < y < x < n \text{ και } x + y \neq n. \tag{7.8.1}$$

Πράγματι, αν ισχύει η συνθήκη (7.8.1) τότε το

$$n \mid (x+y)(x-y) = x^2 - y^2,$$

ενώ το n δεν διαιρεί ούτε το $x-y$ ούτε το $x+y$, αφού $x+y \neq n$ και $x+y < 2n$. Άρα $n \nmid (x+y)$, ενώ $y < x$ και $x - y < n$ συνεπάγεται $n \nmid (x-y)$. Επομένως, $(n, (x-y))$ και $(n, x+y)$ είναι διαιρέτες του n διάφοροι του 1 και n. Τους διαιρέτες αυτούς τους βρίσκουμε εύκολα χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο.
Παράδειγμα. Εύκολα διαπιστώνουμε ότι

$$1254^2 \equiv 420^2 \mathrm{mod} 4309.$$

Υπολογίζουμε τους $(1254 - 420, 4309) = 31$ και $(1254 + 420, 4309) = 139$. Επομένως $4309 = 31 \cdot 139$. Αλλά, όταν μας δοθεί ο n, πώς θα ψάξουμε να βρούμε θετικούς ακέραιους x, y τέτοιους ώστε $x^2 \equiv y^2 \mathrm{mod} n$;

Θα εφαρμόσουμε τη μέθοδο των συνεχών κλασμάτων. Για τον σκοπό αυτό χρειαζόμαστε την ακόλουθη:

Πρόταση 7.8.1. *Υποθέτουμε ότι n είναι κάποιος θετικός ακέραιος, όχι τέλειο τετράγωνο. Ορίζουμε*

$$\alpha_k := \frac{P_k + \sqrt{n}}{Q_k},$$

για $k = 0, 1, 2, \ldots$, $a_k = [\alpha_k]$,

$$P_{k+1} = a_k Q_k - P_k$$

και

$$Q_{k+1} = \frac{n - P_{k+1}^2}{Q_k}$$

για $k = 0, 1, 2, \ldots$, όπου $\alpha_0 := \sqrt{n}$.

Αν $\frac{p_k}{q_k}$ είναι ο k-στός συγκλίνων του απλού συνεχούς κλάσματος της $\sqrt{n}$, τότε ισχύει

$$p_k^2 - n q_k^2 = (-1)^{k-1} Q_{k+1}.$$

Απόδειξη. Το

$$\alpha_0 = \sqrt{n} = [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}].$$

Επίσης, από το πόρισμα 7.1.8,

$$\sqrt{n} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

Αντικαθιστούμε το $\alpha_{k+1} = \frac{P_{k+1}+\sqrt{n}}{Q_{k+1}}$ και έχουμε

$$\sqrt{n} = \frac{\frac{P_{k+1}+\sqrt{n}}{Q_{k+1}}p_k + p_{k-1}}{\frac{P_{k+1}+\sqrt{n}}{Q_{k+1}}q_k + q_{k-1}}$$

από την οποία προκύπτει ότι

$$nq_k + (P_{k+1}q_k + Q_{k+1}q_{k-1})\sqrt{n} = P_{k+1}p_k + Q_{k+1}p_{k-1} + p_k\sqrt{n}.$$

Ο n δεν είναι τέλειο τετράγωνο ακέραιου. Επομένως

$$\left\{\begin{array}{l} nq_k = P_{k+1}p_k + Q_{k+1}p_{k-1} \\ P_{k+1}q_k + Q_{k+1}q_{k-1} = p_k \end{array}\right\} \Rightarrow \left\{\begin{array}{l} nq_k^2 = P_{k+1}p_kq_k + Q_{k+1}p_{k-1}q_k \\ p_k^2 = P_{k+1}p_kq_k + Q_{k+1}p_kq_{k-1} \end{array}\right\}$$

από όπου καταλήγουμε στο

$$p_k^2 - nq_k^2 = Q_{k+1}(p_kq_{k-1} - p_{k-1}q_k) = (-1)^{k-1}Q_{k+1}.$$

□

7.8.1 Αλγόριθμος συνεχών κλασμάτων για την παραγοντοποίηση ενός ακέραιου n.

Σύμφωνα με τους παραπάνω συμβολισμούς από την πρόταση 7.8.1 προκύπτει ότι, για κάθε ακέραιο k, $k \geq 0$, ισχύει

$$p_k^2 \equiv (-1)^{k-1}Q_k \bmod n.$$

Υποθέτουμε ότι ο k είναι περιττός και ότι το Q_{k+1} είναι τέλειο τετράγωνο δηλαδή $Q_{k+1} = s^2$, $s \geq 1$. Επομένως η ισοδυναμία γράφεται

$$p_k^2 \equiv s^2 \bmod n.$$

Η ισοδυναμία αυτή μπορεί να μας οδηγήσει στην παραγοντοποίηση του n.

Παρατήρηση 7.8.2. Τα a_k για $k = 0, 1, 2, \ldots$ είναι οι όροι του συνεχούς κλάσματος της $\sqrt{n}$. Πράγματι, για $k = 0$, έχουμε $\alpha_0 = \sqrt{n}$. Άρα $\alpha_0 = \frac{0+\sqrt{n}}{1}$ με $P_0 = 0$, $Q_0 = 1$ και $a_0 = [\alpha_0] = [\sqrt{n}]$.

Υποθέτουμε ότι ισχύει για k, δηλαδή ότι

$$a_k = [\alpha_k] = \left[\frac{P_k + \sqrt{n}}{Q_k}\right] = [x_k].$$

Τότε

$$\alpha_{k+1} = \frac{P_{k+1} + \sqrt{n}}{Q_{k+1}} = \frac{P_{k+1} + \sqrt{n}}{\frac{n-P_{k+1}^2}{Q_k}} =$$

$$= \frac{Q_k}{\sqrt{n} - P_{k+1}} = \frac{Q_k}{\sqrt{n} - a_kQ_k + P_k} = \frac{1}{\frac{\sqrt{n}+P_k}{Q_k} - a_k} = x_{k+1}.$$

Συνεπώς

$$a_{k+1} = [\alpha_{k+1}] = [x_{k+1}].$$

Σημείωση: Εδώ με x_k συμβολίζουμε, κατ' εξαίρεση, τους διαδοχικούς όρους του συνεχούς κλάσματος της $\sqrt{n}$.

Παράδειγμα. (1) Έστω $n = 7729$. Θα προσπαθήσουμε να τον παραγοντοποιήσουμε με τη μέθοδο των συνεχών κλασμάτων. Το συνεχές κλάσμα του

$$\sqrt{n} = \sqrt{7729} = [87; 1, 1, 0, 1, 2, 1, 2, 21, \ldots],$$

$$\alpha_0 = \frac{0 + \sqrt{7729}}{1}, \quad P_0 = 0, Q_0 = 1, a_0 = [\alpha_0] = 87$$

$$P_1 = a_0 Q_0 - P_0 = 87, \quad Q_1 = \frac{7729 - P_1^2}{Q_0} = 7729 - 7569 = 160.$$

Το

$$\alpha_1 = \frac{P_1 + \sqrt{7729}}{160}.$$

Επομένως $a_1 = [\alpha_1] = 1$,

$$P_2 = a_1 Q_1 - P_1 = 1 \cdot 160 - 87 = 73,$$

ενώ το

$$Q_2 = \frac{7729 - P_2^2}{Q_1} = \frac{7729 - 73^2}{160} = \frac{7729 - 5329}{160} = 15.$$

Δυστυχώς το Q_2 δεν είναι τέλειο τετράγωνο.

$$\alpha_2 = \frac{P_2 + \sqrt{7729}}{Q_2} = \frac{73 + \sqrt{7729}}{15}, \quad a_2 = [\alpha_2] = 10.$$

$$P_3 = a_2 Q_2 - P_2 = 10 \cdot 15 - 73 = 77, \quad Q_3 = \frac{7729 - P_3^2}{Q_2} = \frac{7729 - 77^2}{15} = 120.$$

$$\alpha_3 = \frac{P_3 + \sqrt{7729}}{Q_3} = \frac{77 + \sqrt{7729}}{120},$$

άρα $a_3 = [\alpha_3] = 1$.

$$P_4 = a_3 Q_3 - P_3 = 1 \cdot 120 - 77 = 43, \quad Q_4 = \frac{7729 - P_4^2}{Q_3} = \frac{7729 - 43^2}{120} = 49.$$

Εδώ το Q_4 έχει άρτιο δείκτη και είναι τέλειο τετράγωνο. Εξετάζουμε την ισοδυναμία

$$P_3^2 \equiv (-1)^{3-1} Q_4 \mathrm{mod} 7729$$

και υπολογίζουμε το p_3,

$$\begin{aligned} p_0 &= a_0 = 87 \\ p_1 &= a_0 a_1 + 1 = 87 \cdot 1 + 1 = 88 \\ p_2 &= a_2 p_1 + p_0 = 10 \cdot 88 + 87 = 880 + 87 = 967 \\ p_3 &= a_3 p_2 + p_1 = 1 \cdot 967 + 88 = 1055 \end{aligned}$$

Επομένως, έχουμε $1055^2 \equiv 7^2 \mathrm{mod} 7729$. Με τη βοήθεια του Ευκλείδειου αλγορίθμου υπολογίζουμε $(1048, 7729) = 131$. Επομένως $7729 = 59 \cdot 131$.

Παράδειγμα. (2) Εργαζόμαστε όπως παραπάνω και αποδεικνύουμε ότι $1000009 = 293 \cdot 3413$.

Παρατήρηση 7.8.3. Ενδέχεται να μην δουλέψει ο αλγόριθμος. Αν, για παράδειγμα, θεωρήσουμε τον $n = 731$ και υπολογίσουμε τα Q_k για $k = 0, 1, 2$ βρίσκουμε $1, 2, 1$ αντίστοιχα. Επειδή το απλό συνεχές κλάσμα του $\sqrt{n}$ υπολογίζεται

$$\sqrt{n} = [27; \overline{27, 54}]$$

ποτέ δεν θα μπορέσουμε να βρούμε κάποιο Q_k με άρτιο δείκτη το οποίο να είναι τέλειο τετράγωνο. Σε αυτές τις περιπτώσεις θεωρούμε τον αριθμό $\sqrt{mn}$, με κατάλληλα επιλεγμένο m (συνήθως ένα γινόμενο από μερικούς πρώτους αποφεύγοντας να δημιουργηθούν τετράγωνα μέσα στη ρίζα).

Αν καταφέρουμε για κάποιο άρτιο k να πάρουμε $Q_k = s^2$, $s \geq 1$, όπου το Q_k αφορά στο ανάπτυγμα του συνεχούς κλάσματος του $\sqrt{mn}$, τότε ισχύει

$$p_k^2 - mnq_k^2 = (-1)^{k-1} Q_{k+1}.$$

Εδώ τα p_k/q_k είναι οι συγκλίνοντες του απλού συνεχούς κλάσματος της $\sqrt{mn}$. Από την ισοδυναμία τώρα

$$p_k^2 \equiv (-1)^{k-1} Q_{k+1} \mathrm{mod} mn$$

θα μπορούσαμε, ίσως, να παραγοντοποιήσουμε το n, αν για παράδειγμα βρίσκαμε ότι $(p_k - s, mn) > 1$. Έτσι στο προηγούμενο παράδειγμα, αν θεωρήσουμε τον $m = 6$,

$$\sqrt{mn} = \sqrt{6 \cdot 731} = \sqrt{4386}$$

και υπολογίζουμε $Q_2 = 7^2$ και $p_1 = 265$. Επομένως έχουμε

$$265^2 \equiv 7^2 \mathrm{mod} 4386$$

και

$$(265 - 7, 4386) = 6 \cdot 43.$$

Συνεπώς $43 \mid 731$ οπότε $731 = 17 \cdot 43$.

Τέλος επιθυμούμε να προσθέσουμε ότι η μέθοδος αυτή έχει χρησιμοποιηθεί από τους M. A. Morrison και John Brillahart [9] προκειμένου να παραγοντοποιήσουν τον έβδομο αριθμό Fermat, $F_7 = 2^{2^7} + 1$. Για τον σκοπό τους αυτό υπολόγισαν τον $13300000 \cdot Q_k$ από το απλό συνεχές κλάσμα του αριθμού $\sqrt{127F_7}$. Το αποτέλεσμα της εργασίας τους ήταν:

$$F_7 = 2^{2^7} + 1 = 59649589127497217 \cdot 5704689200685129054721.$$

7.9 Το συνεχές κλάσμα του e

Στην παράγραφο αυτή θα μελετήσουμε το συνεχές κλάσμα της βάσης των νεπέριων λογαρίθμων του υπερβατικού αριθμού e. Ο λόγος είναι ότι παρουσιάζει μια ενδιαφέρουσα κανονικότητα.

Θεώρημα 7.9.1. *Το συνεχές κλάσμα του e είναι το*

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots]$$

με $a_0 = 2$ και $a_{3m} = a_{3m-2} = 1$, $a_{3m-1} = 2m$, για κάθε $m \geq 1$.

Απόδειξη. Γνωρίζουμε ότι το ανάπτυγμα Taylor του e^x είναι

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \cdots$$

Επίσης

$$e^{-x} = 1 - \frac{x}{1!} + \frac{x^2}{2!} - \frac{x^3}{3!} + \frac{x^4}{4!} - \frac{x^5}{5!} + \cdots$$

Άρα

$$\begin{aligned} e^x - e^{-x} &= 2x + \frac{2x^3}{3!} + \frac{2x^5}{5!} + \cdots = \\ &= 2x\left(1 + \frac{x^2}{3!} + \frac{x^4}{5!} + \cdots\right) = \\ &= 2x\sum_{n=0}^{\infty} \frac{x^{2n}}{(2n+1)!} \end{aligned}$$

και

$$\begin{aligned} \frac{1}{(2n+1)!} &= \frac{1}{3\cdot 5\cdots(2n+1)\cdot 2\cdot(2\cdot 2)\cdot(2\cdot 3)\cdots(2n)} = \\ &= \frac{1}{3\cdot 5\cdots(2n+1)n!2^n} = \\ &= \frac{1}{\frac{3\cdot 5\cdots(2n+1)}{2^n} n!4^n} = \\ &= \frac{1}{\frac{3}{2}\left(\frac{3}{2}+1\right)\left(\frac{3}{2}+2\right)\left(\frac{3}{2}+3\right)\cdots\left(\frac{3}{2}+n-1\right)n!4^n}. \end{aligned}$$

Άρα

$$e^x - e^{-x} = 2xf\left(\frac{3}{2}, \frac{x^2}{4}\right),$$

όπου

$$\begin{aligned} f(c,x) &= 1 + \frac{x}{c} + \frac{1}{c(c+1)}\cdot\frac{x^2}{2!} + \cdots + \frac{1}{c(c+1)\cdots(c+n-1)}\frac{x^n}{n!} + \cdots = \\ &= 1 + \sum_{n=1}^{\infty} \frac{1}{c(c+1)\cdots(c+n-1)}\frac{x^n}{n!}, \end{aligned}$$

με $c \in \mathbb{R}\backslash\{0,-1,-2,\ldots\}$. Όμοια υπολογίζουμε ότι

$$e^x + e^{-x} = 2f\left(\frac{1}{2}, \frac{x^2}{4}\right),$$

οπότε συνολικά

$$\frac{e^w - e^{-w}}{e^w + e^{-w}} = w\frac{f\left(\frac{3}{2}, \frac{w^2}{4}\right)}{f\left(\frac{1}{2}, \frac{w^2}{4}\right)}. \tag{7.9.1}$$

Τώρα,

$$f(c,x) - f(c+1,x) = 1 + \frac{x}{c} + \frac{1}{c(c+1)}\frac{x^2}{2!} + \cdots + \frac{1}{c(c+1)\cdots(c+n-1)}\frac{x^n}{n!} + \cdots$$

$$-1-\frac{x}{c+1}-\frac{1}{(c+1)(c+2)}\frac{x^2}{2!}-\cdots-\frac{1}{(c+1)\cdots(c+n-1)(c+n)}\frac{x^n}{n!}-\cdots$$
$$=\frac{x}{c(c+1)}+\frac{2}{c(c+1)(c+2)}\frac{x^2}{2!}+\cdots+\frac{n}{c(c+1)\cdots(c+n-1)(c+n)}\frac{x^n}{n!}+\cdots=$$
$$=\frac{x}{c(c+1)}\left(1+\frac{x}{c+2}+\frac{1}{(c+2)(c+3)}\frac{x^2}{2!}+\cdots+\frac{1}{(c+1)\cdots(c+n)}\frac{x^{n-1}}{(n-1)!}+\cdots\right)$$
$$=\frac{x}{c(c+1)}f(c+2,x).$$

Άρα

$$f(c,x)-f(c+1,x)=\frac{x}{c(c+1)}f(c+2,x),$$

οπότε

$$\frac{f(c,x)}{f(c+1,x)}-\frac{f(c+1,x)}{f(c+1,x)}=\frac{x}{c(c+1)}\frac{f(c+2,x)}{f(c+1,x)}.$$

Επομένως

$$\frac{f(c+1,x)}{f(c,x)}=1+\frac{x}{c(c+1)}\frac{f(c+2,x)}{f(c+1,x)}$$

και τελικά

$$\frac{f(c+1,x)}{f(c,x)}=\frac{1}{1+\frac{x}{c(c+1)}\frac{f(c+2,x)}{f(c+1,x)}}.$$

Για $x=z^2$ έχουμε

$$\frac{z}{c}\frac{f(c+1,z^2)}{f(c,z^2)}=\frac{1}{\frac{c}{z}+\frac{z}{c+1}\frac{f(c+2,z^2)}{f(c+1,z^2)}}$$

συνεπώς

$$\frac{z}{c}\frac{f(c+1,z^2)}{f(c,z^2)}=\frac{1}{\frac{c}{z}+\frac{1}{\frac{c+1}{z}\frac{f(c+1,z^2)}{f(c+2,z^2)}}}$$

και επαγωγικά προκύπτει

$$\frac{z}{c}\frac{f(c+1,z^2)}{f(c,z^2)}=\left[0;\frac{c}{z},\frac{c+1}{z},\ldots,\frac{c+n}{z},\alpha_{n+2}\right],$$

όπου

$$\alpha_{n+2}=\frac{c+n+1}{z}\frac{f(c+n+1,z^2)}{f(c+n+2,z^2)}.$$

Πράγματι, για $n=0$, ισχύει από την παραπάνω σχέση. Έστω ότι ισχύει μέχρι το $n-1$, δηλαδή

$$\frac{z}{c}\frac{f(c+1,z^2)}{f(c,z^2)}=[0,\frac{c}{z},\frac{c+1}{z},\ldots,\frac{c+n+1}{z},\alpha_{n+1}].$$

Τότε

$$\frac{1}{\alpha_{n+1}}=\frac{1}{\frac{c+n}{z}\frac{f(c+n,z^2)}{f(c+n+1,z^2)}}=\frac{z}{c+n}\frac{f(c+n+1,z^2)}{f(c+n,z^2)}=$$
$$=\frac{1}{\frac{c+n}{z}+\frac{z}{c+n+1}\cdot\frac{f(c+n+2,z^2)}{f(c+n+1,z^2)}}=$$

$$= \frac{1}{\frac{c+n}{z} + \frac{1}{\frac{c+n+1}{z}\cdot\frac{f(c+n+1,z^2)}{f(c+n+2,z^2)}}}.$$

άρα ισχύει και για το n. Συνεπώς μπορούμε να πάρουμε το συνεχές κλάσμα του αριστερού μέλους της παραπάνω ισότητας αν δώσουμε ειδικές τιμές στο c και z έτσι ώστε ο αριθμός $\frac{c+n}{z}$ να είναι ακέραιος ≥ 1, και ο τελευταίος όρος α_{n+2} να είναι ≥ 1, για κάθε $n \geq 0$. Επιλέγουμε, λοιπόν, $c = \frac{1}{2}$ και $z = \frac{1}{2y}$, όπου y ακέραιος ≥ 1.

Θέτουμε στη σχέση (7.9.1) $w = \frac{1}{y}$ και βρίσκουμε ότι το ανάπτυγμα του $\frac{e^w - e^{-w}}{e^w + e^{-w}}$ σε συνεχές κλάσμα είναι

$$\begin{aligned}
\frac{e^{\frac{1}{y}} - e^{-\frac{1}{y}}}{e^{\frac{1}{y}} + e^{-\frac{1}{y}}} &= \frac{e^w - e^{-w}}{e^w + e^{-w}} = w\frac{f\left(\frac{3}{2}, \frac{w^2}{4}\right)}{f\left(\frac{1}{2}, \frac{w^2}{4}\right)} \\
&= \frac{1}{y}\frac{f\left(\frac{3}{2}, \frac{\frac{1}{y^2}}{4}\right)}{f\left(\frac{1}{2}, \frac{\frac{1}{y^2}}{4}\right)} = \frac{\frac{1}{2y}}{\frac{1}{2}}\frac{f\left(\frac{3}{2}, \left(\frac{1}{2y}\right)^2\right)}{f\left(\frac{1}{2}, \left(\frac{1}{2y}\right)^2\right)} \\
&= \left[0; \frac{\frac{1}{2}}{\frac{1}{2y}}, \frac{\frac{1}{2}+1}{\frac{1}{2y}}, \frac{\frac{1}{2}+2}{\frac{1}{2y}}, \ldots\right] = [0; y, 3y, 5y, \ldots]
\end{aligned}$$

Ειδικά για $y = 2$ έχουμε

$$\frac{e^{\frac{1}{2}} - e^{-\frac{1}{2}}}{e^{\frac{1}{2}} + e^{-\frac{1}{2}}} = [0, 2, 6, 10, \ldots].$$

Συνεπώς

$$\frac{\sqrt{e} - \frac{1}{\sqrt{e}}}{\sqrt{e} + \frac{1}{\sqrt{e}}} = [0; 2, 6, 10, \ldots]$$

και έτσι προκύπτει ότι

$$\frac{e-1}{e+1} = [0; 2, 6, 10, \ldots].$$

Επομένως το συνεχές κλάσμα του αντιστρόφου είναι

$$\frac{\sqrt{e} + \frac{1}{\sqrt{e}}}{\sqrt{e} - \frac{1}{\sqrt{e}}} = [2; 6, 10, \ldots]$$

Αν $\alpha = \frac{e+1}{e-1}$ τότε

$$e\alpha - \alpha = e + 1 \Leftrightarrow e = \frac{\alpha + 1}{\alpha - 1}.$$

Έστω

$$\xi := [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1 \ldots]$$

και έστω $\frac{p_n}{q_n}$ οι κύριες συγκλίσεις του ξ και r_n/s_n οι κύριες συγκλίσεις του α.

Θα αποδείξουμε ότι, για κάθε $n \geq 0$, ισχύουν:

$$p_{3n+1} = r_n + s_n \text{ και } q_{3n+1} = r_n - s_n \tag{7.9.2}$$

Για $n = 0$, προφανώς $r_0 = 2$ και $s_0 = 1$. Ενώ $p_{3\cdot 0+1} = p_1 = a_0a_1 + 1 = 2 \cdot 1 + 1 = 3$ και $q_{3\cdot 0+1} = q_1 = a_1 = 1$ άρα $p_1 = 3 = 2 + 1 = r_0 + s_0$ και $q_1 = 1 = 2 - 1 = r_0 - s_0$.

Έστω ότι οι σχέσεις (7.9.2) είναι αληθείς για όλους τους φυσικούς $\leq n$. Θα δείξουμε ότι είναι αληθείς και για το $n+1$.

Όμως, εξ ορισμού $r_n = a_n r_{n-1} + r_{n-2}$ ή $r_n = 2(2n+1)r_{n-1} + r_{n-2}$ και ανάλογα $s_n = 2(2n+1)s_{n-1} + s_{n-2}$.

Τώρα για τα p_n γράφουμε τους αναδρομικούς τύπους, πολλαπλασιάζουμε με τον αντίστοιχο συντελεστή και προσθέτουμε

p_{3n-3}	$= 1 \cdot p_{3n-4} + p_{3n-5}$	$+1$
p_{3n-2}	$= 1 \cdot p_{3n-3} + p_{3n-4}$	-1
p_{3n-1}	$2n \cdot p_{3n-2} + p_{3n-3}$	$+2$
p_{3n}	$= 1 \cdot p_{3n-1} + p_{3n-2}$	$+1$
p_{3n+1}	$1 \cdot p_{3n} + p_{3n-1}$	$+1$
p_{3n+1}	$= 2(2n+1)p_{3n-2} + p_{3n-5}$	

Επιπλέον

$$\begin{aligned} p_{3(n+1)+1} &= 2(2(n+1)+1)p_{3(n+1)-2} + p_{3(n+1)-5} \\ &= 2(2(n+1)+1)p_{3n+1} + p_{3n-2} \text{ (υπόθεση μαθηματικής επαγωγής)} \\ &= 2(2(n+1)+1)(r_n + s_n) + r_{n-1} + s_{n-1} \\ &= 2(2(n+1)+1)r_n + r_{n-1} + 2(2(n+1)+1)s_n + s_{n-1} = \\ &= r_{n+1} + s_{n+1}. \end{aligned}$$

Ομοίως, για τα q_n, έχουμε

$$q_{3n+1} = 2(2n+1)q_{3n-2} + q_{3n-5}$$

και

$$\begin{aligned} q_{3(n+1)} &= 2(2(n+1)+1)q_{3(n+1)-2} + q_{3(n+1)-5} \\ &= 2(2(n+1)+1)q_{3n+1} + q_{3n-2} \\ &= 2(2(n+1)+1)(r_n - s_n) + r_{n-1} - s_{n-1} \\ &= 2(2(n+1)+1)r_n + r_{n-1} - 2(2(n+1)+1)s_n - s_{n-1} \\ &= r_{n+1} - s_{n+1}. \end{aligned}$$

Άρα οι σχέσεις (7.9.2) ισχύουν, οπότε

$$\xi = \lim_{n\to\infty} \frac{p_{3n+1}}{q_{3n+1}} = \lim_{n\to\infty} \frac{r_n + s_n}{r_n - s_n} = \lim_{n\to\infty} \frac{\frac{r_n}{s_n} + 1}{\frac{r_n}{s_n} - 1} = \frac{\alpha - 1}{\alpha + 1} = e.$$

□

Η απόδειξη που παρουσιάσαμε ακολουθεί αυτή του Lang [10]. Για μια διαφορετική απόδειξη παραπεμπουμε στο [7].

Στη συνέχεια καταγράφουμε μερικούς όρους του αναπτύγματος του π σε απλό συνεχές κλάσμα.

$$\pi = [3; 7, 15, 1, 292, \ldots]$$

Μέχρι σήμερα δεν είναι γνωστή η ύπαρξη οποιασδήποτε κανονικότητας για το απλό συνεχές κλάσμα του π.

Στο πρόγραμμα sage μπορούμε να υπολογίσουμε όσο μεγάλο κομμάτι του συνεχούς κλάσματος του e θέλουμε:

```
continued_fraction_list(e, bits=70)
[2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \
1, 1, 14, 1, 1, 16, 2]
```

7.10 Ιστορικά στοιχεία

Ο αλγόριθμος του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη αποτελεί ουσιαστικά μετατροπή ενός κλάσματος σε συνεχές κλάσμα. Αυτό ήταν ίσως και το πρώτο βήμα (~ 300 π.Χ.) προς την κατεύθυνση της ανάπτυξης της ιδέας των συνεχών κλασμάτων.

Αναφορά στα συνεχή κλάσματα βρίσκει κανείς στα ινδικά Μαθηματικά και ιδιαίτερα στο έργο των Aryabhata (6ος αιώνας μ.Χ.) και Bhaskara (12ος αιώνας μ.Χ.). Και οι δύο χρησιμοποιούν τα συνεχή κλάσματα για την επίλυση γραμμικών εξισώσεων.

Η μοντέρνα θεωρία των συνεχών κλασμάτων αρχίζει με τις εργασίες του Rafaell Bombelli (γεννήθηκε γύρω στα 1530). Ο Bombelli χρησιμοποιήσε τα συνεχή κλάσματα για να προσεγγίσει τετραγωνικές ρίζες, κάτι που έκανε και ο Cataldi (1548-1626) πριν από αυτόν. Ο Bombelli υπολογίζει, στην «Άλγεβρα» που εξέδωσε στα 1572, το συνεχές κλάσμα της $\sqrt{13} = [3; \overline{4, 6}]$. Φαίνεται ότι γνώριζε το ανάπτυγμα του συνεχούς κλάσματος αριθμών της μορφής

$$\sqrt{a^2 + b} = [a; \overline{b, 2a}].$$

Ο Cataldi (1548-1626) υπολογίζει στα 1613 το συνεχές κλάσμα του

$$\sqrt{18} = [4; \overline{2, 8}].$$

Ο όρος «συνεχές κλάσμα» χρησιμοποιείται για πρώτη φορά στα 1653 από τον John Wallis στο έργο του "Arithmetica infinitorum".

Μοναδικό έργο του Christian Huygens στο οποίο «πλησίασε» τη Θεωρία Αριθμών ήταν το "Descriptio Automati Planetarii". Το έργο του αυτό θα πρέπει να το είχε ετοιμάσει μεταξύ των ετών 1680 και 1687, αλλά όσο ζούσε δεν το δημοσίευσε ποτέ. Δημοσιεύτηκε το έτος 1703 μετά τον θάνατό του. Στο έργο του αυτό αναπτύσσει τη θεωρία της βέλτιστης προσέγγισης ενός ρητού από ένα κλάσμα, στηριζόμενος στον αλγόριθμο των συνεχών κλασμάτων.

Η κλασική θεωρία, όπως είναι σήμερα, αναπτύχθηκε από τους μεγάλους μαθηματικούς Euler (1707-1783) και Lagrange (1736-1813). Στα 1737, ο Euler αποδεικνύει ότι ένα άπειρο απλό περιοδικό συνεχές κλάσμα ορίζει πάντοντε έναν τετραγωνικό άρρητο πραγματικό αριθμό. Στα 1770, ο Lagrange αποδεικνύει και το αντίστροφο, ότι όλοι οι τετραγωνικοί άρρητοι αριθμοί έχουν περιοδικό απλό άπειρο συνεχές κλάσμα.

Ουσιαστικά αυτά είναι που γνωρίζουμε μέχρι σήμερα. Δεν είναι γνωστός κανείς χαρακτηρισμός άρρητων ποσοτήτων βαθμού 3 μέσω ιδιοτήτων των συνεχών κλασμάτων. Ούτε καν του $\sqrt[3]{2}$.

Ακόμη κανείς δεν γνωρίζει για κανέναν αλγεβρικό αριθμό $\alpha \in \mathbb{R}$ βαθμού ≥ 3 το συνεχές κλάσμα αυτού.

Η σύνδεση της σχέσης του αλγόριθμου των συνεχών κλασμάτων με τις εξισώσεις του Pell (η θεωρία θα αναπτυχθεί στο επόμενο κεφάλαιο) καταγράφεται για πρώτη φορά από τον Euler το 1759. Η εργασία του αυτή πρωτοδημοσιεύεται το 1767.

Σε όλο το κεφάλαιο έχουμε ασχοληθεί με απλά συνεχή κλάσματα. Είναι βέβαια φυσικό να οριστεί η έννοια του συνεχούς κλάσματος γενικότερα.

Ορισμός 7.10.1. Ένα άπειρο συνεχές κλάσμα είναι μια έκφραση της μορφής

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{\cdots}}}},$$

όπου $a_i, b_j \in \mathbb{R}$.

Έτσι, σύμφωνα με αυτόν τον ορισμό, ο William Brouncker μετέτρεψε τον τότε γνωστό τύπο του Wallis

$$\frac{4}{\pi} = \frac{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \cdots}{2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot 8 \cdots}$$

σε συνεχές κλάσμα

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \cdots}}}}$$

Ο Gauss στο ημερολόγιό του (24 Μαΐου του 1796), μετέτρεψε τη σειρά

$$1 - 2 + 8 - 64 + \cdots$$

σε συνεχές κλάσμα

$$\cfrac{1}{1 + \cfrac{2}{1 + \cfrac{2}{1 + \cfrac{8}{1 + \cfrac{12}{1 + \cfrac{32}{1 + \cfrac{56}{\cdots}}}}}}}$$

Ο Carl Lindemann χρησιμοποίησε τον αλγόριθμο των συνεχών κλασμάτων για να αποδείξει ότι ο π είναι υπερβατικός.

Ο S. Ramanujan (1887-1920) έχει υπολογίσει πλειάδα συνεχών κλασμάτων. Ίσως το πιο εντυπωσιακό είναι το

$$e^{\frac{2\pi}{5}} \left(\frac{\sqrt{5 + \sqrt{5}}}{2} - \frac{1 + \sqrt{5}}{2} \right) = \cfrac{1}{1 + \cfrac{e^{-2\pi}}{1 + \cfrac{e^{-4\pi}}{1 + \cfrac{e^{-6\pi}}{1 + \cdots}}}}$$

Όπως θα διαπιστώσουμε σύντομα τα συνεχή κλάσματα παίζουν έναν σημαντικό ρόλο στα Μαθηματικά γενικά και στη Θεωρία Αριθμών ειδικότερα. Τα ιστορικά στοιχεία έχουν αντληθεί από τα [3], [5], [4], [8].

Βιβλιογραφία

[1] A. Markoff: *Sur les formes quadratiques binaires indefinies*. Math. Annalen, 15:381–409, 1879.

[2] A. Markoff: *Sur les formes quadratiques binaires indefinies*. Math. Annalen, 17:379–399, 1879.

[3] A. Weil: *Number theory, an approach through history, from Hammurapi to Legendere*. Birkhäuser Boston, 1983.

[4] Bundschuh: *Einführung in die Zahlentheorie*. 2002.

[5] Damvid, M, Burton: *Elementary Number Theory*. UBS New Delhi, 1998. second edition.

[6] Enrico Bombieri: *Continued fractions and the Markoff tree*. Expositiones Mathematicae, 25:187–213, 2007.

[7] H. Cohn: *A Short proof of the simple continued fraction of e*. Am. Math. Monthly, 113:57–62, 2006.

[8] Jay R. Goldman: *The Queen of Mathematics:A Historically Motivated Guide to Number Theory*. A. K. Peters Massachussets, 1998.

[9] M. A. Morrison, J. Brillhart: *A method of factoring and the factorization of* $\mathbb{F}_7$. Mathematics of Computation, 29:183–205, 1975.

[10] S. Lang: *Introduction to Diophantine Approximation*. Springer, 1995.

8

Η εξίσωση του Pell

8.1 Εισαγωγή

Στην παράγραφο αυτή θα μελετήσουμε τις λύσεις μιας συγκεκριμένης κλάσεως διοφαντικών εξισώσεων, των εξισώσεων του Pell. Αυτό γίνεται όχι μόνο για ιστορικούς λόγους, αλλά και λόγω της χρησιμότητας τους στα επόμενα.

Ας ξεκινήσουμε με δύο απλά παραδείγματα. Παρατηρούμε ότι $10 - 1 = 3^2$ και $\frac{10}{2} - 1 = 2^2$. Υπάρχουν άλλοι αριθμοί οι οποίοι να έχουν ανάλογη ιδιότητα;

Ο αμέσως επόμενος είναι ο 290. Πράγματι, $290 - 1 = 17^2$ και $\frac{290}{2} - 1 = 12^2$. Μπορούμε να τους βρούμε όλους; Είναι πεπερασμένου πλήθους ή άπειρου;

Αν α είναι κάποιος τέτοιος ακέραιος, τότε θα πρέπει να υπάρχουν ακέραιοι x, y τέτοιοι ώστε

$$\alpha - 1 = x^2 \text{ και } \frac{\alpha}{2} - 1 = y^2.$$

Συνεπώς τα x, y θα πρέπει να αποτελούν λύση της διοφαντικής εξίσωσης

$$X^2 - 2Y^2 = 1.$$

Ας θεωρήσουμε τώρα το ακόλουθο πρόβλημα:

Να υπολογιστούν όλες οι θετικές και ακέραιες λύσεις του συστήματος

$$\begin{aligned} 2uv - xy &= 16 \\ xv - uy &= 12 \end{aligned}$$

Λύνουμε το σύστημα ως προς x και u και έχουμε

$$x = \frac{24v + 16y}{2v^2 - y^2}, \quad u = \frac{16v + 12y}{2v^2 - y^2}.$$

Προφανώς το $2v^2 - y^2$ είναι θετικό, αφού $x > 0$, $u > 0$ και οι αριθμητές είναι επίσης θετικοί. Υπολογίζουμε το

$$2(xv - uy)^2 - (2uv - xy)^2 = (x^2 - 2u^2)(2v^2 - y^2).$$

Επομένως

$$(x^2 - 2u^2)(2v^2 - y^2) = 2 \cdot 12^2 - 16^2 = 32.$$

Συνεπώς το $(2v^2 - y^2) \mid 32$, οπότε έχουμε

$$2v^2 - y^2 = 2^s, \ \ 0 \leq s \leq 5.$$

Αν τώρα s περιττός, $s := 2k + 1$, τότε από την εξίσωση

$$2v^2 - y^2 = 2^{2k+1}$$

εφαρμόζοντας διαδοχικά τη διαίρεση με 2, καταλήγουμε στο συμπέρασμα ότι

$$v = 2^k v_0, y = 2^{k+1} y_0 \text{ και } v_0^2 - 2y_0^2 = 1.$$

Αν ο s είναι άρτιος, $s := 2k$, τότε ανάλογα προκύπτει ότι

$$y_0^2 - 2v_0^2 = -1.$$

8.2 Η εξίσωση του Pell

Ορισμός 8.2.1. Αν $d \in \mathbb{N}\backslash\{0\}$, η διοφαντική εξίσωση

$$X^2 - dY^2 = 1$$

λέγεται εξίσωση του Pell.

Παρατήρηση 8.2.2. Αργότερα θα μελετήσουμε τις κάπως γενικότερες εξισώσεις της μορφής

$$X^2 - dY^2 = N, \text{ όπου } N \in \mathbb{Z}.$$

Συχνά και αυτές εμφανίζονται στη βιβλιογραφία με το ίδιο όνομα. Ούτως ή άλλως ιδιαίτερο ενδιαφέρον θα δούμε ότι παρουσιάζει η εξίσωση

$$X^2 - dY^2 = -1.$$

Παρατήρηση 8.2.3. Αν το $d = t^2$, $t > 0$ τότε η εξίσωση γράφεται

$$(X - tY)(X + tY) = 1$$

η οποία έχει λύσεις

$$(x, y) = (1, 0), (-1, 0). \tag{8.2.1}$$

Στη συνέχεια θα υποθέτουμε ότι ο d είναι ελεύθερος τετραγώνου.

Οι λύσεις (8.2.1) θα λέγονται τετριμμένες λύσεις της εξίσωσης του Pell.

Πρόταση 8.2.4. *Αν η εξίσωση του Pell*

$$X^2 - dY^2 = 1,$$

έχει μη-τετριμμένη λύση, έστω (p, q), τότε ο $\frac{p}{q}$ είναι κάποιος κύριος συγκλίνων του συνεχούς κλάσματος του αριθμού $\sqrt{d}$.

Απόδειξη. Από τη σχέση $p^2 - dq^2 = 1$ προκύπτει ότι $p > q\sqrt{d}$ και

$$(p - \sqrt{d}q)(p + \sqrt{d}q) = 1.$$

Επομένως

$$0 < \frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})} < \frac{1}{q(q\sqrt{d} + q\sqrt{d})} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{1}{2q^2}.$$

Το συμπέρασμα είναι άμεση συνέπεια της πρότασης 7.5.5 της σελίδας 267. □

Παρατήρηση 8.2.5. Δεν είναι όλοι οι συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$, λύσεις της εξίσωσης του Pell

$$X^2 - dY^2 = 1.$$

Για παράδειγμα, ο ρητός $\frac{11}{3}$ είναι ένας συγκλίνων του συνεχούς κλάσματος του $\sqrt{13}$, αλλά δεν είναι λύση της εξίσωσης του Pell $X^2 - 13Y^2 = 1$, αφού $11^2 - 13 \cdot 3^2 = 4$. Ο συγκλίνων $\frac{649}{180}$ είναι λύση της εξίσωσης.

Εντελώς φυσιολογικά προκύπτει το ερώτημα. Για κάποιον συγκλίνοντα $\frac{p_n}{q_n}$ του συνεχούς κλάσματος του αριθμού $\sqrt{d}$, ποιο είναι το μέγεθος του αριθμού $(p_n - dq_n)$;

Πρόταση 8.2.6. *Αν p/q συγκλίνων του συνεχούς κλάσματος του αριθμού $\sqrt{d}$, τότε το (p, q) είναι λύση της εξίσωσης του Pell*

$$X^2 - dY^2 = N,$$

όπου $|N| < 1 + 2\sqrt{d}$.

Απόδειξη. Αφού $\frac{p}{q}$ συγκλίνων του $\sqrt{d}$, έπεται ότι

$$\left|\frac{p}{q} - \sqrt{d}\right| < \frac{1}{q^2}.$$

Επομένως $|p - q\sqrt{d}| < \frac{1}{q}$. Στη συνέχεια υπολογιζουμε

$$|p + q\sqrt{d}| = |(p - q\sqrt{d}) + 2q\sqrt{d}| \leq |p - q\sqrt{d}| + |2q\sqrt{d}| < \frac{1}{q} + 2q\sqrt{d} \leq (1 + 2\sqrt{d})q.$$

Τελικά προκύπτει ότι

$$|p^2 - dq^2| = |p - q\sqrt{d}||p + q\sqrt{d}| \leq \frac{1}{q}(1 + 2\sqrt{d})q = 1 + 2\sqrt{d},$$

δηλαδή ότι $p^2 - dq^2 = N$ με $|N| < 1 + 2\sqrt{d}$. □

Παράδειγμα. Το συνεχές κλάσμα του αριθμού $\sqrt{13}$ είναι το

$$\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}].$$

Υπολογίζουμε τους συγκλίνοντες και την αντίστοιχη τιμή της $X^2 - 13Y^2$.

$$\begin{array}{lll} p_0 = 3, & q_0 = 1, & 3^2 - 13 \cdot 1^2 = -4 \\ p_1 = 4, & q_1 = 1, & 4^2 - 13 \cdot 1 = 3 \\ p_2 = 7 & q_2 = 2, & 7^2 - 13 \cdot 2^2 = -3 \\ p_3 = 11 & q_3 = 3, & 11^2 - 13 \cdot 3^2 = 4 \\ p_4 = 18, & q_4 = 5, & 18^2 - 13 \cdot 5^2 = -1 \\ p_5 = 119, & q_5 = 33, & 119^2 - 13 \cdot 33^2 = 4 \\ p_6 = 137, & q_6 = 38, & 137^2 - 13 \cdot 38^2 = -3 \\ p_7 = 256, & q_7 = 71, & 256^2 - 13 \cdot 71^2 = 3 \\ p_8 = 393, & q_8 = 109, & 393^2 - 13 \cdot 109^2 = -4 \\ p_9 = 649, & q_9 = 180, & 649^2 - 13 \cdot 180^2 = 1. \end{array}$$

Από την πρόταση 7.7.12 προκύπτει ότι το συνεχές κλάσμα της $\sqrt{d}$ είναι όχι μόνο απλά περιοδικό αλλά της μορφής

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}].$$

Για $d < 100$ ο αριθμός $\sqrt{94}$ έχει το μέγιστο μήκος περιόδου που είναι 16. Θα εκμεταλευτούμε την περιοδικότητα του συνεχούς κλάσματος του αριθμού $\sqrt{d}$ για να συμπεράνουμε την ύπαρξη μιας και στη συνέχεια άπειρου πλήθους λύσεων της εξίσωσης του Pell.

Πρόταση 8.2.7. *Αν $\frac{p_k}{q_k}$ οι συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$ και n το μήκος της περιόδου αυτού τότε ισχύει:*

$$p_{kn-1}^2 - dq_{kn-1} = (-1)^{kn},$$

για κάθε $k = 1, 2, 3, \ldots$

Απόδειξη. Για κάθε $k \geq 1$, γράφουμε το συνεχές κλάσμα του αριθμού $\sqrt{d}$ στη μορφή

$$\sqrt{d} = [a_0; a_1, a_2, \ldots, a_{kn-1}, r_{kn}],$$

όπου

$$r_{kn} := [2a_0; \overline{a_1, a_2, \ldots, a_{kn-1}, 2a_0}] = a_0 + \sqrt{d}.$$

Από το πόρισμα 7.1.8 έπεται ότι

$$\sqrt{d} = \frac{r_{kn}p_{kn-1} + p_{kn-2}}{r_{kn}q_{kn-1} + q_{kn-2}}.$$

Αντικαθιστούμε την τιμή του r_{kn} και έχουμε

$$\sqrt{d}(a_0q_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0p_{kn-1} + p_{kn-2} - dq_{kn-1}.$$

Συνεπώς

$$\begin{aligned} a_0q_{kn-1} + q_{kn-2} &= p_{kn-1} \\ a_0p_{kn-1} + p_{kn-2} &= dq_{kn-1} \end{aligned}$$

Πολλαπλασιάζουμε τις δύο σχέσεις με p_{kn-1} και q_{kn-1} αντίστοιχα και προσθέτουμε

$$p_{kn-1}^2 - dq_{kn-1}^2 = p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2}.$$

Άλλα, πρόταση 7.2.1,

$$p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2} = (-1)^{kn-2} = (-1)^{kn},$$

δηλαδή προκείπτει ο ισχυρισμός της πρότασης. □

Θεώρημα 8.2.8. *Αν $\frac{p_k}{q_k}$ οι συγκλίνουτες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$ και n το μήκος της περιόδου αυτού, τότε ισχύουν:*

1. *Αν n άρτιος, τότε όλες οι θετικές λύσεις της εξίσωσης του Pell*

$$X^2 - dY^2 = 1,$$

δίνονται από τις σχέσεις

$$x = p_{kn-1}, y = q_{kn-1}, \quad k = 1, 2, 3, \ldots$$

2. *Αν n περιττός, τότε όλες οι θετικές λύσεις τις εξίσωσης του Pell δίνονται από τις σχέσεις*

$$x = p_{2kn-1}, y = q_{2kn-1}, \quad k = 1, 2, 3, \ldots$$

Απόδειξη. Σύμφωνα με την πρόταση 8.2.4, όλες οι λύσεις της εξίσωσης του Pell είναι κάποιοι από τους συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$. Λόγω της πρότασης 8.2.7 έχουμε:

1. Αν ο n είναι άρτιος, τότε όλες οι θετικές λύσεις της εξίσωσης του Pell δίνονται από τους τύπους:

$$x = p_{kn-1}, y = q_{kn-1}, \quad k = 1, 2, 3, \ldots$$

2. Αν ο n είναι περιττός τότε οι λύσεις είναι οι:

$$x = p_{2kn-1}, y = q_{2kn-1}, \quad k = 1, 2, 3, \ldots,$$

□

Παρατήρηση 8.2.9. Είναι φανερό ότι στη δεύτερη περίπτωση του θεωρήματος οι συγκλίνοντες της μορφής

$$x = p_{(2k+1)n-1} \text{ και } y = q_{(2k+1)n-1}, \quad k = 0, 1, 2, 3, \ldots$$

είναι οι λύσεις της $X^2 - dY^2 = -1$. (Στην πρώτη περίπτωση η $X^2 - dY^2 = -1$ δεν έχει ακέραια λύση).

Παρατήρηση 8.2.10. Στο παράδειγμα με $d = \sqrt{13}$ η περίοδος του συνεχούς κλάσματος είναι $n = 5$. Επομένως όλες οι θετικές λύσεις της εξίσωσης του Pell

$$X^2 - dY^2 = 13$$

είναι

$$x = p_{10k-1}, y = q_{10k-1}, k = 1, 2, 3, \ldots$$

Όπως έχουμε ήδη διαπιστώσει, για $k = 1$ έχουμε τη λύση $x = p_9 = 649$, $y = q_9 = 180$.

Παρατήρηση 8.2.11. Αν $4 \mid d$ ή $p \mid d$ και $p \in \mathbb{P}$, $p \equiv 3 \bmod 4$, τότε η $X^2 - dY^2 = -1$ δεν έχει ακέραια λύση. Πράγματι, αν ήταν (x, y) μια ακέραια λύση αυτής, τότε θα είχαμε $x^2 \equiv -1 \bmod 4$ ή $x^2 \equiv -1 \bmod p$ αντίστοιχα. Οι ισοτιμίες όμως αυτές δεν είναι επιλύσιμες. Αυτό σημαίνει ότι το μήκος της περιόδου του συνεχούς κλάσματος του αριθμού $\sqrt{d}$ είναι κατ' ανάγκην άρτιο.

Ορισμός 8.2.12. Η μικρότερη θετική λύση (x_1, y_1) της εξίσωσης του Pell $X^2 - dY^2 = 1$ θα λέγεται θεμελιώδης λύση αυτής. (Εδώ μικρότερη εννοούμε ότι $x_1 < x$ και $y_1 < y$ για κάθε άλλη λύση (x, y) αυτής.)

Παρατήρηση 8.2.13. Αν ο n είναι άρτιος, η θεμελιώδης λύση είναι $x_1 = p_{n-1}$, $y_1 = q_{n-1}$. Αν ο n είναι περιττός, τότε αυτή είναι $x_1 = p_{2n-1}$, $y_1 = q_{2n-1}$. (Το n είναι το μήκος της περιόδου του συνεχούς κλάσματος της $\sqrt{d}$.)

Πρόταση 8.2.14. *Αν (x_1, y_1) είναι η θεμελιώσης λύση της $X^2 - dY^2 = 1$, τότε κάθε ζευγάρι (x_n, y_n) το οποίο δίνεται από την ισότητα*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}$$

είναι επίσης λύση αυτής.

Απόδειξη. Είναι προφανές ότι, για κάθε $n \in \mathbb{N}$, ισχύει

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n.$$

Επίσης οι x_n, y_n είναι θετικοί ακέραιοι, αφού οι x_1, y_1 είναι θετικοί ακέραιοι. Η (x_1, y_1) είναι μια λύση της $X^2 - dY^2 = 1$. Επομένως,

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) = \\ &= (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n = \\ &= (x_1^2 - dy_1^2)^n = 1^n = 1. \end{aligned}$$

□

Παράδειγμα. Το συνεχές κλάσμα της $\sqrt{2} = [1; \overline{2}]$. Το $n = 1$. Συνεπώς η θεμελιώδης λύση της εξίσωσης του Pell $X^2 - 2Y^2 = 1$ είναι $x_1 = p_3 = 3$, $y_1 = q_3 = 2$. Άρα και η (x_2, y_2) όπου $x_2 + y_2\sqrt{2} = (3 + 2\sqrt{2})^2$ είναι επίσης λύση. Ομοίως και η (x_3, y_3) όπου $x_3 + y_3\sqrt{2} = (3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2}$.

Στην επόμενη πρόταση θα αποδείξουμε ότι οι λύσεις της πρότασης 8.2.14 είναι όλες οι λύσεις της εξίσωσης του Pell

$$X^2 - dY^2 = 1.$$

Πρόταση 8.2.15. *Έστω (x_1, y_1) η θεμελιώδης λύση της εξίσωσης του Pell $X^2 - dY^2 = 1$. Όλες οι λύσεις αυτής δίνονται από τη σχέση*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}.$$

Απόδειξη. Υποθέτουμε ότι υπάρχει μια λύση (u, v) της εξίσωσης του Pell η οποία δεν προκύπτει από την παραπάνω σχέση και θα καταλήξουμε σε άτοπο.

Επειδή τα x_1 και y_1 είναι θετικοί, οι δυνάμεις $(x_1 + y_1\sqrt{d})^n \to \infty$ για $n \to \infty$. Επομένως, υπάρχει ένας φυσικός αριθμός n_0, τέτοιος ώστε

$$(x_1 + y_1\sqrt{d})^{n_0} < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{n_0+1},$$

δηλαδή

$$x_{n_0} + y_{n_0}\sqrt{d} < u + v\sqrt{d} < (x_{n_0} + y_{n_0}\sqrt{d})(x_1 + y_1\sqrt{d}).$$

Προφανώς ισχύουν $x_{n_0} - y_{n_0}\sqrt{d} > 0$ και $x_{n_0}^2 - dy_{n_0}^2 = 1$. Επομένως έχουμε

$$1 < (x_{n_0} - y_{n_0}\sqrt{d})(u + v\sqrt{d}) < x_1 + y_1\sqrt{d}.$$

Όμως,

$$(x_{n_0} - y_{n_0}\sqrt{d})(u + v\sqrt{d}) = (x_{n_0}u - y_{n_0}vd) + (x_{n_0}v - y_{n_0}u)\sqrt{d}.$$

Αν $a := x_{n_0}u - y_{n_0}vd$ και $b := x_{n_0}v - y_{n_0}u$, τότε

$$a^2 - db^2 = (x_{n_0}^2 - dy_{n_0}^2)(u^2 - dv^2) = 1.$$

Αυτό σημαίνει ότι το ζεύγος (a, b) είναι λύση της εξίσωσης του Pell $X^2 - dY^2 = 1$. Όμως $1 < a + b\sqrt{d} < x_1 + y_1\sqrt{d}$. Θα αποδείξουμε ότι οι a, b είναι θετικοί ακέραιοι. Από τις σχέσεις $1 < a + b\sqrt{d}$ και

$$a^2 - b^2 d = (a - b\sqrt{d})(a + b\sqrt{d}) = 1$$

έπεται ότι

$$0 < a - b\sqrt{b} < 1.$$

Επομένως,

$$2a = (a + b\sqrt{d}) + (a - b\sqrt{d}) > 1 + 0 > 0$$

και $2b\sqrt{d} = (a + b\sqrt{d}) - (a - b\sqrt{d}) > 1 - 1 = 0$. Τελικά αποδείξαμε ότι το (a, b) είναι μια θετική ακέραια λύση με $a < x_1$ και $b < y_1$, άτοπο. Αυτό αποδεικνύει την αλήθεια της πρότασης. □

Παρατήρηση 8.2.16. Από το παραπάνω γίνεται φανερό ότι το σημαντικό είναι ο υπολογισμός μιας θεμελιώδους λύσης της εξίσωσης του Pell. Αυτό επιτυγχάνεται, όπως έχουμε ήδη δει, μέσω του υπολογισμού των συγκλινόντων του συνεχούς κλάσματος του αριθμού $\sqrt{d}$. Ισχύει και το εξής:

Αν (x, y) θετική ακέραια λύση της εξίσωσης του Pell $X^2 - dY^2 = 1$ και $x > \frac{y^2}{2} - 1$, τότε η (x, y) είναι θεμελιώδης. Παραδείγματος χάρη, για $d = 2$, η $(3, 2)$ είναι θεμελιώδης.

8.3 Η γενικευμένη εξίσωση του Pell

Ο d είναι, όπως και στην προηγούμενη παράγραφο, θετικός ακέραιος όχι τέλειο τετράγωνο. Είναι προφανές ότι η εξίσωση

$$X^2 - 3Y^2 = -1,$$

δεν έχει ακέραια λύση αφού $\left(\frac{-1}{3}\right) = -1$. Ομοίως η $X^2 - 5Y^2 = 2$ επίσης δεν έχει ακέραια λύση, αφού $\left(\frac{2}{5}\right) = -1$.

Παρατήρηση 8.3.1. Αν η εξίσωση $X^2 - dY^2 = N$ έχει μια ακέραια λύση, έστω (a, b), και (x, y) είναι μια μη-τετριμμένη λύση της εξίσωσης του Pell $X^2 - dY^2 = 1$, τότε έχουμε

$$N = N \cdot 1 = (a^2 - b^2 d)(x^2 - y^2 d) = (xa - dyb)^2 - d(xb - ay)^2.$$

Αυτό σημαίνει ότι (r, s) όπου $r := xa - dyb$ και $s := xb - ay$ είναι επίσης λύση της $X^2 - dY^2 = N$. Επειδή δε η $X^2 - dY^2 = 1$, έχει άπειρες λύσεις και η αρχική έχει επίσης άπειρο πλήθος λύσεων.

Πρόταση 8.3.2. *Η εξίσωση $X^2 - dY^2 = N$ δεν έχει ακέραια λύση ή έχει άπειρες λύσεις.*

Πρόταση 8.3.3. *Αν p_n/q_n οι συγκλίνουτες του συνεχούς κλάσματος της $\sqrt{d}$ και N ακέραιος τέτοιος ώστε $|N| < \sqrt{d}$ τότε κάθε θετική λύση (x, y) της $X^2 - dY^2 = N$ με $(x, y) = 1$ ικανοποιεί τη σχέση $x = p_n$ και $y = q_n$, για κάποιο $n \in \mathbb{N}, n \neq 0$.*

Απόδειξη. Υποθέτουμε ότι $N > 0$. Από τη σχέση

$$(x + y\sqrt{d})(x - y\sqrt{d}) = n$$

έπεται ότι $x - y\sqrt{d} > 0$, δηλαδή $x > y\sqrt{d}$. Επομένως $\frac{x}{y} - \sqrt{d} > 0$. Η υπόθεση ότι $0 < N < d$ μας δίνει

$$\frac{x}{y} - \sqrt{d} = \frac{(x - y\sqrt{d})}{y} = \frac{x^2 - dy^2}{y(x + y\sqrt{d})} < \frac{N}{y(2y\sqrt{d})} < \frac{d}{2y^2\sqrt{d}} = \frac{1}{2y^2}.$$

Επομένως,

$$0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2},$$

οπότε πρόταση 7.5.5 τα x, y πρέπει να είναι συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$.

Στη συνέχεια υποθέτουμε ότι $N < 0$. Διαιρούμε τα μέλη της $x^2 - dy^2 = N$ με $-d$ και έχουμε

$$y^2 - \frac{1}{d}x^2 = \frac{-N}{d}.$$

Εργαζόμαστε ανάλογα με την περίπτωση που το N ήταν θετικό και συμπεραίνουμε ότι τα x, y είναι συγλίνοντες του συνεχούς κλάσματος του αριθμού $\frac{1}{\sqrt{d}}$. Όμως, αν το συνεχές κλάσμα του άρρητου αριθμού α είναι το

$$\alpha = [a_0; a_1, a_2, \ldots],$$

τότε το συνεχές κλάσμα του $\frac{1}{\alpha}$ είναι το

$$\frac{1}{a} = [0; a_0, a_1, a_2, \ldots,].$$

Αυτό σημαίνει ότι ο n-στός συγκλίνων του $1/\alpha$ ταυτίζεται με τον αντίστροφο του $(n-1)$-στού συγκλίνοντα του α.

Τελικά, έχουμε ότι ο $\frac{x}{y} = \frac{1}{y/x}$ είναι συγκλίνων του συνεχούς κλάσματος του αριθμού $\frac{1}{\frac{1}{\sqrt{d}}} = \sqrt{d}$. □

Παρατήρηση 8.3.4. Από την προηγούμενη πρόταση βλέπουμε ότι για σχετικά μικρά N πιθανές λύσεις προσδιορίζονται από τους συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$.

Επίσης έχουμε δει ότι αν (a, b) λύση της $X^2 - Y^2 b = N$ και (x, y) λύση της $X^2 - dY^2 = 13^2 = 1$, τότε η $u + v\sqrt{d} = (a + b\sqrt{d})(x + y\sqrt{d})$ είναι επίσης λύση της $X^2 - dY^2 = N$.

Ορισμός 8.3.5. Λύσεις της εξίσωσης

$$X^2 - dY^2 = N,$$

οι οποίες προκύπτουν από μία λύση αυτής (a, b) με πολλαπλασιασμό με μια λύση της $X^2 - dY^2 = 1$ λέγονται συνεταιρικές ή συσχετιζόμενες μεταξύ τους.

Το σύνολο όλων αυτών των λύσεων δημιουργεί μια άπειρη κλάση λύσεων.

Παρατήρηση 8.3.6. Προφανώς δύο λύσεις $u_1 + v_1\sqrt{d}$ και $u_2 + v_2\sqrt{d}$ της

$$X^2 - dY^2 = N$$

ανήκουν στην ίδια κλάση ακριβώς όταν οι αριθμοί

$$\frac{u_1u_2 - v_1v_2d}{N}, \frac{v_1u_2 - u_1v_2}{N},$$

είναι αμφότεροι ακέραιοι.

Χωρίς απόδειξη αναφέρουμε ότι

Πρόταση 8.3.7. *Αν N θετικός ακέραιος, τότε το σύνολο των κλάσεων των λύσεων της εξίσωσης $X^2 - dY^2 = N$ είναι πεπερασμένο.*

Θα επανέλθουμε σε σχετικά θέματα στο μεθεπόμενο κεφάλαιο στο οποίο θα μελετήσουμε τετραγωνικά αλγεβρικά σώματα αριθμών.

Παρατήρηση 8.3.8. Για μικρά d είναι δυνατόν η θεμελιώδης λύση να είναι αρκετά μεγάλη. Για παράδειγμα η εξίσωση του Pell

$$X^2 - 991Y^2 = 1$$

έχει θεμελιώδη λύση

$$x = 379516400906811930638014896080,$$

$$y = 12055735790331359497442538767$$

Μάλιστα της εξίσωσης

$$X^2 - 1000099Y^2 = 1$$

η θεμελιώδης λύση έχει 1118-ψηφία. Το μήκος της περιόδου είναι 2174.

Παρατήρηση 8.3.9. Ελαφρά μεταβολή του d αλλάζει άρδην τα δεδομένα. Έτσι για παράδειγμα αν $d = 60$, η θεμελιώδης λύση είναι $x = 31, y = 4$. Αν $d = 61$ η θεμελιώδης λύση είναι $x = 1766319049$, $y = 226153980$. Αν $d = 62$ η θεμελιώδης λύση είναι $x = 63$, $y = 8$, ενώ για $d = 1621$ η συντεταγμένη x της θεμελιώδους λύσης έχει 76-ψηφία.

Αφορμή από το συγκεκριμένο παράδειγμα πήραν οι M.J. Jacobson και H.C. Williams [8] οι οποίοι θεώρησαν τη θεμελιώδη λύση (x_0, y_0) της εξίσωσης του Pell $X^2 - (d-1)Y^2 = 1$ και τη θεμελιώδη λύση (x_1, y_1) της $X^2 - dY^2 = 1$, όρισαν

$$\rho(d) := \frac{\log(x_1)}{\log(x_0)}$$

και απέδειξαν ότι ο λόγος μπορεί να γίνει οσοδήποτε μεγάλος.

8.4 Ιστορικά στοιχεία

8.4.1 Το Βοεικό πρόβλημα του Αρχιμήδη

Το 1773 ο Γερμανός ποιητής G.E. Lessing ανακάλυψε ένα βυζαντινό χειρόγραφο του 14ου αιώνα με 4 άγνωστα ποιήματα της Παλατινής Ανθολογίας. Ένα από αυτά είχε τίτλο στον οποίο δήλωνε ότι επρόκειτο για αριθμητικό πρόβλημα το οποίο πρότεινε με επιστολή του ο Αρχιμήδης στον Ερατοσθένη.

«ὅπερ Ἀρχιμήδης ἐν ἐπιγράμμασιν εὑρών τοῖς ἐν Ἀλεξανδρείᾳ περί ταῦτα πραγματευομένοις ζητεῖν ἀπέστειλεν ἐν τῇ προς Ἐρατοσθένη τον Κυρηναῖον ἐπιστολῇ.»

Στο πρόβλημα αυτό ζητείται να υπολογισθεί το πλήθος των βοοειδών του Θεού Ήλιου και αναφέρεται στη βιβλιογραφία ως «Βοεικό πρόβλημα του Αρχιμήδη».

Αναφέρεται στον υπολογισμό των ταύρων και αγελάδων που ζούσαν στο νησί του Θεού Ήλιου. Έχουν 4 χρώματα (λευκό, μαύρο, ξανθό και ποικιλόχρωμο).

Αν W, X, Y, Z είναι το πλήθος των λευκών, μαύρων, ξανθών και ποικιλόχρωμων ταύρων αντίστοιχα και w, x, y, z το χρώμα των αντίστοιχων αγελάδων. Τότε σύμφωνα με το επίγραμμα, οι παραπάνω μεταβλητές θα πρέπει να επαληθεύουν το ακόλουθο σύστημα εξισώσεων.

$$\begin{aligned} W &= \left(\frac{1}{2}+\frac{1}{3}\right)X + Z \\ X &= \left(\frac{1}{4}+\frac{1}{5}\right)Y + Z \\ Y &= \left(\frac{1}{6}+\frac{1}{7}\right)W + Z \\ w &= \left(\frac{1}{3}+\frac{1}{4}\right)(X + x) \\ x &= \left(\frac{1}{4}+\frac{1}{5}\right)(Y + z) \\ y &= \left(\frac{1}{5}+\frac{1}{6}\right)(Z + z) \\ z &= \left(\frac{1}{6}+\frac{1}{7}\right)(W + w) \\ W + X &= \square \\ Y + Z &= \Delta \end{aligned}$$

Σημείωση: Οι τελευταίοι δύο συμβολισμοί σημαίνουν ότι ο αριθμός $W+X$ είναι τέλειο τετράγωνο και ότι ο $Y + Z$ είναι τρίγωνος αριθμός.

Η λύση του συστήματος αυτού ανάγεται στην επίλυση μιας εξίσωσης του Pell, της

$$T^2 - dU^2 = 1,$$

όπου $d = 410286423278424$. Φυσικά θα μπορούσαμε να λύσουμε την εξίσωση αυτή του Pell υπολογίζοντας τους συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{d}$, αλλά το μήκος της περιόδου είναι 203254 [5].

Ο A. Amthor [1] παρατήρησε ότι ο $d = (9314)^2 4729494$ και ανήγαγε την αρχική εξίσωση στη μορφή

$$T^2 - d_0 U^2 = 1,$$

όπου τώρα το $d_0 = 4729494$ και η περίοδος του συνεχούς κλάσματος του αριθμού $\sqrt{d_0}$, είναι μόνο 92. Η θεμελιώδης λύση της τελευταίας εξίσωσης είναι

$$t = 109931986732829734979866232821433543901088049$$

και

$$u = 50549485234315033074477819735540408986340.$$

Βέβαια, εμείς ενδιαφερόμαστε για τη θεμελιώδη λύση της αρχικής. Αν (x_1, y_1) η θεμελιώδης λύση της αρχικής τότε ο A. Amthor απέδειξε ότι

$$x_1 + y_1\sqrt{d} = (t + u\sqrt{d_0})^{2329}.$$

Του ήταν όμως αδύνατο να λύσει το βοεικό πρόβλημα του Αρχιμήδη επειδή η τιμή του y_1 είναι αρκετά μεγάλη, προσεγγιστικά περίπου

$$1,83 \times 10^{103265}.$$

Ο συνολικός αριθμός των ζώων υπολογίστηκε τελικά το 1965 από τους H.C. Williams, R.A. German και C. R. Zarnke προφανώς και με χρήση υπολογιστή [3].

Αργότερα, ο αριθμός δημοσιεύτηκε από τον H.L. Nelson [4] και καταλαμβάνει 12 τυπωμένες σελίδες.

Περισσότερα σχετικά στοιχεία μπορεί να βρει ο ενδιαφερόμενος αναγνώστης στα άρθρα [6], [5].

Εξαιρετικό ενδιαφέρον παρουσιάζει και το ιστορικό - φιλοσοφικό άρθρο του Μιχάλη Λάμπρου [10].

8.4.2 Σύντομη ιστορική αναδρομή

Φαίνεται ότι η πρώτη αναφορά στις εξισώσεις του Pell γίνεται στο έργο του Θέωνα του Σμυρναίου. Ακολούθησαν σχετικές παρατηρήσεις στο θέμα από τον Πρόκλο. Ουσιαστικά χρησιμοποιήθηκαν οι συγκλίνοντες του συνεχούς κλάσματος του αριθμού $\sqrt{2}$ για να τον προσεγγίσουν.

Στο έργο του «Κύκλου Μέτρησις» ο Αρχιμήδης προσεγγίζει, χωρίς επεξήγηση, τον αριθμό $\sqrt{3}$ ως εξής:

$$\frac{265}{153} < \sqrt{3} < \frac{1350}{780}.$$

Ας σημειωθεί ότι οι $\frac{265}{153}$ και $\frac{1350}{780}$ είναι οι 8ος και 11ος συγκλίνοντες του αριθμού $\sqrt{3}$.

Το 628 ο Brahmagupta ήταν ο πρώτος που ανακάλυψε την ταυτότητα:

$$\text{Αν } X_1^2 - dY_1^2 = a \text{ και } X_2^2 - dY_2^2 = b$$

τότε ισχύει

$$(X_1X_2 + dY_1Y_2)^2 - d(X_1Y_2 + Y_1X_2)^2 = ab.$$

Κάνοντας χρήση της παραπάνω ταυτότητας, ανακάλυψε μια ad hoc μέθοδο επίλυσης της εξίσωσης του Pell:

$$X^2 - 92Y^2 = 1.$$

Παρατήρησε ότι $10^2 - 92 = 8$ και συνθέτοντας αυτή τη λύση με τον εαυτό της, όπως στην ταυτότητα παραπάνω, βρήκε ότι

$$192^2 - 92 \cdot 20^2 = 64.$$

Επομένως $24^2 - 92 \cdot \left(\frac{5}{2}\right)^2 = 1$ και συνθέτοντας και πάλι με τον εαυτό της υπολόγισε ότι

$$1151^2 - 92 \cdot 120^2 = 1.$$

Η σημαντικότερη συμβολή των Ινδικών μαθηματικών όσον αφορά στην εξίσωση του Pell είναι η ανακάλυψη της κυκλικής μεθόδου κατά τον 12ο αιώνα [2], [7].

Ακολούθησε ένα μεγάλο χρονικό διάστημα και η Θεωρία Αριθμών ξαναγεννήθηκε για δεύτερη φορά - όπως ο Ιανός κατά τον A. Weil.

Ο P. de Fermat, το 1657 σε επιστολή του προς τον Frenicle, θέτει προς απόδειξη το ακόλουθο πρόβλημα:

«Δίδεται κάποιος (θετικός) ακέραιος d ο οποίος δεν είναι τέλειο τετράγωνο. Υπάρχει άπειρο πλήθος ακέραιων των οποίων αν στο τετράγωνο αυτού πολλαπλασιασμένο με το d προσθέσουμε και μια μονάδα βρίσκουμε τέλειο τετράγωνο ακέραιου.»

Στη συνέχεια απαιτεί την εύρεση ενός γενικού κανόνα επίλυσης του προβλήματος και ερωτά για τις ειδικές περιπτώσεις $d = 109, 149, 433$.

Οι ειδικές αυτές περιπτώσεις έχουν επιλυθεί από τους Brounker και Wallis [2], [9].

Παρά ταύτα, ούτε ο Brouncker, ούτε ο Wallis, ούτε ο Frénicle κατάφεραν να αποδείξουν ότι η εξίσωση του Pell έχει πάντοτε μη-τετριμμένες λύσεις για κάθε θετικό ακέραιο ο οποίος δεν είναι τέλειο τετράγωνο.

Η μέθοδος του Brouncker τροποποίηθηκε και επεκτάθηκε από τον Euler, ο οποίος παρατήρησε ότι μπορεί να χρησιμοποιηθεί η θεωρία των συνεχών κλασμάτων και να μας δώσει έναν αποτελεσματικό αλγόριθμο επίλυσης της εξίσωσης του Pell.

Σημαντική ήταν και η συνεισφορά του Lagrange.

Η εξίσωση φέρει το όνομα του Άγγλου μαθηματικού John Pell (1611-1685), ο οποίος όμως είχε ελάχιστη σχέση με το πρόβλημα. Το λάθος οφείλεται στον Euler. «Ηθικό δίδαγμα»! Μπορεί κανείς να περάσει στην Ιστορία ακόμα και αν δεν έχει κάνει κάτι σχετικό.

Βιβλιογραφία

[1] A. Amthor: *Das Problema bovinum des Archimedes*. Zeitschrift für Math. u. Physik (Hist. Litt. Abtheilung), 25:153–171, 1880.

[2] A. Weil: *Number theory, an approach through history, from Hammurapi to Legendere*. Birkhäuser Boston, 1983.

[3] H. C. Williams, R. A. German, C. R. Zarnke: *Solution of the cattle Problem of Archimedes*. Math. Comp., 19:671–674, 1965.

[4] H. L. Nelson: *A solution to Archimedes cattle problem*. J. Recreational Math., 13:162–176, 1981.

[5] H. W. Lenstra: *Solving the Pell equation*. Notices of the AMS, 49:182–192, 2002.

[6] I. Vardi: *Archimedes' cattle problem*. Amer. Math. Monthly, 105:305–319, 1998.

[7] J. Jacobson, H.C. Williams: *Solving the Pell equation*. Springer New York, 2009.

[8] M. J. Jacobson, H. C. Williams: *The size of the fundamental solutions of consecutive Pell equations*. Experimental Mathematics, 9:631–640, 2000.

[9] S. Mahoney: *The Mathematical career of Pierre de Fermat*. Princeton University Press New York, 1994. 2nd edition.

[10] Λάμπρου, Μιχάλης: *το βοεικό πρόβλημα του Αρχιμήδη*. σελίδες 195–2, 1992. Κείμενα ιστορίας και φιλοσοφίας των Αρχαίων Ελληνικών Μαθηματικών, Επιμ. Δ. Α. Αναπολιτάνος - Β. Καρασμάνης.

9

Τετραγωνικές μορφές

9.1 Εισαγωγή

Στο κεφάλαιο αυτό θα μελετήσουμε τις δυαδικές τετραγωνικές μορφές (binary quadratic forms). Η όλη θεωρία θα συνδυαστεί στο επόμενο κεφάλαιο με αυτή των τετραγωνικών σωμάτων αριθμών.

Ορισμός 9.1.1. Δυαδική τετραγωνική μορφή λέγεται κάθε ομογενές πολυώνυμο δευτέρου βαθμού, δύο μεταβλητών με συντελεστές ακέραιους:

$$f(X, Y) = aX^2 + bXY + cY^2.$$

Θα ασχοληθούμε με δύο βασικά ερωτήματα:
Ερώτημα 1ο Να υπολογιστούν οι ακέραιοι n οι οποίοι παρίστανται μέσω της τετραγωνικής μορφής $f(X, Y)$, δηλαδή οι φυσικοί αριθμοί n, για τους οποίους υπάρχουν ακέραιοι x, y τέτοιοι ώστε

$$f(x, y) = n.$$

Ερώτημα 2ο Αν ο ακέραιος n παρίσταται από την τετραγωνική μορφή $f(X, Y)$, τότε κατά πόσους διαφορετικούς τρόπους μπορεί να παρασταθεί;

Για λόγους ευκολίας θα συμβολίζουμε την τετραγωνική μορφή

$$f(X, Y) = aX^2 + bXY + cY^2 \text{ ως εξής: } f = [a, b, c].$$

Στη συνέχεια θα ασχοληθούμε, κατ' αρχήν, με το πρώτο ερώτημα. Επειδή ασχολούμαστε αποκλειστικά με δυαδικές τετραγωνικές μορφές, στα επόμενα θα παραλείπουμε το επίθετο «δυαδικές».

Ορισμός 9.1.2. Διακρίνουσα της τετραγωνικής μορφής $[a, b, c]$, λέγεται ο ακέραιος αριθμός $D := b^2 - 4ac$.

Παρατήρηση 9.1.3. Συχνά στη βιβλιογραφία η διακρίνουσα ορίζεται και ως $D = 4ac - b^2$.

Παρατήρηση 9.1.4. Προφανώς $D \equiv 0 \bmod 4$ αν b άρτιος και $D \equiv 1 \bmod 4$ αν b περιττός.

Παρατήρηση 9.1.5. Αν η διακρίνουσα D είναι τέλειο τετράγωνο ακέραιου, τότε η τετραγωνική μορφή αναλύεται σε γινόμενο δύο γραμμικών πολυωνύμων με ακέραιους συντελεστές. Αν η διακρίνουσα D δεν είναι τέλειο τετράγωνο, τότε η τετραγωνική μορφή δεν αναλύεται σε γινόμενο γραμμικών πολυωνύμων, όχι μόνο με συντελεστές ακέραιους, αλλά ούτε και με συντελεστές ρητούς.

Πρόταση 9.1.6. *Αν η τετραγωνική μορφή*

$$f(X,Y) = aX^2 + bXY + cY^2,$$

έχει διακρίνουσα $D = b^2 - 4ac \neq 0$ η οποία δεν είναι τέλειο τετράγωνο ακέραιου, τότε $a \neq 0$, $c \neq 0$ και η μοναδική λύση της εξίσωσης $f(X,Y) = 0$ είναι η $(x,y) = (0,0)$.

Απόδειξη. Αν ήταν $a = 0$ είτε $c = 0$ τότε η διακρίνουσα D θα ήταν τέλειο τετράγωνο $D = b^2$.

Έστω (x,y) μια λύση της $f(X,Y) = 0$. Αν $y = 0$ τότε $ax^2 = 0$ και επειδή $a \neq 0$, έπεται ότι $x = 0$. Αν $x = 0$, ομοίως έπεται ότι και $y = 0$.

Αν $x \neq 0$ και $y \neq 0$ τότε γράφουμε

$$4af(x,y) = (2ax + by)^2 - Dy^2.$$

Από τη σχέση αυτή προκύπτει αμέσως ότι ο D είναι τέλειο τετράγωνο αφού $Dy^2 \neq 0$, άτοπο. □

Στη συνέχεια υποθέτουμε ότι $D \neq 0$. Ξεχωρίζουμε δύο περιπτώσεις:

1η Περίπτωση: Αν $D < 0$, τότε κατ' ανάγκη ισχύει $a \cdot c > 0$, δηλαδή $a > 0$ και $c > 0$ ή $a < 0$ και $c < 0$.

Ορισμός 9.1.7. Αν για την τετραγωνική μορφή $[a,b,c]$ ισχύουν

$$D = b^2 - 4ac < 0 \text{ και } a > 0,$$

τότε η τετραγωνική μορφή λέγεται *θετικά ορισμένη*.

Αν ισχύουν $D < 0$ και $a < 0$, τότε λέγεται *αρνητικά ορισμένη*.

Παρατήρηση 9.1.8. Είναι αυτονόητο ότι όταν η $[a,b,c]$ είναι θετικά ορισμένη, τότε μπορεί να παραστήσει μόνο μη-αρνητικούς ακέραιους, ενώ αν είναι αρνητικά ορισμένη τότε μπορεί να παραστήσει ακέραιους ≤ 0.

Παρατήρηση 9.1.9. Είναι φανερό ότι αν η $[a,b,c]$ είναι θετικά ορισμένη τότε η $[-a,-b,-c]$ είναι αρνητικά ορισμένη. Επομένως δεν χάνουμε κάτι αν περιοριστούμε στην περίπτωση $D < 0$, και θετικά ορισμένες τετραγωνικές μορφές.

Παρακάτω θα περιοριστούμε σε τετραγωνικές μορφές με $D < 0$ η οποία δεν είναι τέλειο τετράγωνο.

2η Περίπτωση: Στην περίπτωση που $D > 0$, η τετραγωνική μορφή παριστά και θετικούς αλλά και αρνητικούς ακέραιους και θα λέγεται απροσδιόριστη (indefinite). Δεν θα ασχοληθούμε με την περίπτωση αυτή.

9.2 Ισοδύναμες τετραγωνικές μορφές

Θα ξεκινήσουμε με ένα παράδειγμα:

Παράδειγμα: Ας θεωρήσουμε τις τετραγωνικές μορφές

$$f(X,Y) = 2X^2 + 5XY + 3Y^2$$

και

$$g(X',Y') = 21(X')^2 + 29X'Y' + 10(Y')^2.$$

Παρατηρούμε ότι, για $(x, y) = (1, 1)$, η $f(X, Y)$ παριστά τον αριθμό 10. Επίσης, και η $g(X', Y')$ για $(x', y') = (0, 1)$ παριστά τον αριθμό 10. Επίσης, για $(x', y') = (1, 1)$, η $g(X', Y')$ παριστά τον αριθμό 60 και η $f(X, Y)$, για $(x, y) = (3, 2)$, παριστά επίσης τον αριθμό 60.

Ακριβέστερα και οι δύο τετραγωνικές μορφές παριστούν τους ίδιους ακέραιους αριθμούς. Ο λόγος είναι ότι αν κάποιος ακέραιος n παρίσταται από την $f(X, Y)$ για $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, τότε ο ίδιος ακέραιος παρίσταται από την $g(X', Y')$ για $(x', y') \in \mathbb{Z} \times \mathbb{Z}$ όπου

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x - y \\ -x + 2y \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

και αντίστροφα, αν ο n παρίσταται από την $g(X', Y')$ για τις τιμές (x', y') τότε ο n παρίσταται και από την $f(X, Y)$ για

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x' + y' \\ x' + y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Είναι λοιπόν φυσικό να ορίσουμε:

Ορισμός 9.2.1. Δύο τετραγωνικές μορφές $f(X, Y)$ και $g(X', Y')$ λέγονται *ισοδύναμες* ακριβώς όταν η

$$g(X', Y') = f(aX + bY, cX + dY),$$

και

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z} \text{ με } \det M = 1.$$

Είναι φανερό ότι η σχέση του ορισμού 9.2.1 είναι σχέση ισοδυναμίας (άσκηση). Η σχέση ισοδυναμίας συχνά γράφεται ως εξής:

$$g(X', Y') = f|_M(X, Y) = f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}\right)$$

Το σύνολο των πινάκων

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\}$$

αποτελεί πολλαπλασιαστική ομάδα.

Αν $M, N \in \mathrm{SL}_2(\mathbb{Z})$ και $f(X, Y)$, $g(X', Y')$ είναι τετραγωνικές μορφές, τότε

$$f|_{MN} \begin{pmatrix} X \\ Y \end{pmatrix} = (f|_M)|_N \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Πρόταση 9.2.2. *Αν η $f(X, Y)$ είναι τετραγωνική μορφή και $M \in \mathrm{SL}_2(\mathbb{Z})$, τότε το σύνολο των ακέραιων που παρίσταται από την $f(X, Y)$ συμπίπτει με το σύνολο των ακέραιων που παρίσταται από την $f|_M(X, Y)$.*

Απόδειξη. Αν $f(x, y) = n$, επειδή $M^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, έχουμε

$$M^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z} \times \mathbb{Z},$$

οπότε

$$f|_M \left(M^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right) = f\left(MM^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right) = f \begin{pmatrix} x \\ y \end{pmatrix} = n.$$

Αντίστροφα, αν $f|_M \begin{pmatrix} x \\ y \end{pmatrix} = n$, τότε $f\left(M \begin{pmatrix} x \\ y \end{pmatrix} \right) = n$, δηλαδή η $f(X, Y)$ παριστά τον n. □

Παράδειγμα. Η τετραγωνική μορφή

$$f(X,Y) = 65X^2 + 224XY + 193Y^2,$$

παριστά ακριβώς τους ακέραιους οι οποίοι γράφονται ως άθροισμα δύο τετραγώνων. Πράγματι, αν

$$g(X,Y) = X^2 + Y^2,$$

η

$$f(X,Y) = g|_M \begin{pmatrix} X \\ Y \end{pmatrix}, \text{ όπου } M = \begin{pmatrix} 7 & 12 \\ 4 & 7 \end{pmatrix}.$$

Παρατήρηση 9.2.3. Οι διακρίνουσες των τετραγωνικών μορφών του αρχικού παραδείγματος είναι 1. Επίσης, οι διακρίνουσες των τετραγωνικών μορφών του δευτέρου παραδείγματος είναι -4.

Πρόταση 9.2.4. *Αν $f(X,Y)$, $g(X',Y')$ είναι ισοδύναμες τετραγωνικές μορφές, τότε οι διακρίνουσες των f, g είναι ίσες, $D(f) = D(g)$.*

Απόδειξη. Αν $M \in \mathrm{SL}_2(\mathbb{Z})$, τότε ισχύει

$$D(f|_M) = D(f) \cdot (\det M)^2 = D(f).$$

Αν τώρα $f \sim g$, υπάρχει $M \in \mathrm{SL}_2(\mathbb{Z})$ τέτοιο ώστε $g = f|_M$ και συνεπώς η πρόταση ισχύει. □

Προσοχή! Το αντίστροφο της πρότασης δεν ισχύει. Οι τετραγωνικές μορφές

$$X^2 + 10Y^2 \text{ και } 2X^2 + 5Y^2$$

έχουν και οι δύο διακρίνουσα -40. Δεν είναι όμως ισοδύναμες, αφού η πρώτη παριστά τον ακέραιο 1 και η δεύτερη όχι.

Πρόταση 9.2.5. *Το σύνολο όλων των διακρινουσών τετραγωνικών μορφών είναι όλοι οι ακέραιοι D, με $D \equiv 0$ ή $1 \bmod 4$.*

Απόδειξη. Έχουμε ήδη παρατηρήσει ότι κάθε διακρίνουσα τετραγωνικής μορφής είναι ένας αριθμός της μορφής αυτής.

Αντίστροφα αν D είναι ένας ακέραιος $D \equiv 0$ ή $1 \bmod 4$ και θέσουμε

$$C := \begin{cases} -\frac{D}{4}, & \text{αν } D \equiv 0 \bmod 4 \\ -\frac{D-1}{4} & \text{αν } D \equiv 1 \bmod 4 \end{cases}$$

τότε η τετραγωνική μορφή $[1,0,C]$ στην πρώτη περίπτωση και η $[1,1,C]$ στη δεύτερη περίπτωση έχει διακρίνουσα ίση με D. □

Ορισμός 9.2.6. Η τετραγωνική μορφή

$$X^2 - \frac{D}{4}Y^2, \text{ όταν } D \equiv 0 \bmod 4$$

και

$$X^2 + XY + \frac{1-D}{4}Y^2, \text{ όταν } D \equiv 1 \bmod 4$$

λέγεται θεμελιώδης τετραγωνική μορφή διακρίνουσας D.

Εντελώς φυσιολογικά τίθεται το ερώτημα: Δίνεται καποιος ακέραιος $D \equiv 0, 1 \bmod 4$, D όχι τέλειο τετράγωνο.

Πόσο είναι το πλήθος των κλάσεων ισοδυναμίας τετραγωνικών μορφών διακρίνουσας D;

Πρόταση 9.2.7. *Έστω $D \in \mathbb{Z}$ και D όχι τέλειο τετράγωνο. Υπάρχει το πολύ πεπερασμένο πλήθος κλάσεων τετραγωνικών μορφών δοσμένης διακρίνουσας D.*

Απόδειξη. Θα αποδείξουμε ότι κάθε τετραγωνική μορφή

$$f(X, Y) = aX^2 + bXY + cY^2$$

διακρίνουσας D είναι ισοδύναμη προς μία τετραγωνική μορφή

$$a'X^2 + b'XY + c'Y^2$$

τέτοια ώστε $|b'| \leq |a'| \leq |c'|$.

Αν το αποδείξουμε, αμέσως έχουμε το πεπερασμένο του αριθμού κλάσεων αφού

$$|D| = |(b')^2 - 4a'c'| \geq \left||b'|^2 - 4|a'||c'|\right| \geq 4|a'||c'| - |b'|^2 \geq 4|a'|^2 - |b'|^2,$$

όπου για την αλήθεια της τελευταίας ανισότητας χρησιμοποιήσαμε ότι $|c'| \geq |a'|$. Τώρα, αφού $|b'| \leq |a'|$, έχουμε

$$4|a'|^2 - |b'|^2 \geq 4|a'|^2 - |a'|^2 = 3|a'|^2.$$

Επομένως,

$$|a'| \leq \sqrt{\frac{|D|}{3}}, |b'| \leq |a'|, |c'| = \frac{(b')^2 - D}{4a'}$$

δηλαδή υπάρχουν πεπερασμένου πλήθους κλάσεις τετραγωνικών μορφών.

Αν $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ και $f = [a, b, c]$, τότε $f|_S = [c, -b, a]$. Επίσης αν $m \in \mathbb{Z}$ και $T_m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, τότε $f|_{T_M} = [a, b + 2md, c + mb + m^2a]$. Εφαρμόζουμε τον αλγόριθμο:

Ξεκινούμε από την τετραγωνική μορφή $f = [a, b, c]$.

1. Αν $|a| < |b|$, επιλέγουμε ένα $m \in \mathbb{Z}$ τέτοιοι ώστε $-|a| < b + 2ma \leq |a|$ και εφαρμόζουμε τον T_m στην f,

$$f|_{T_m} = [a, b' = b + 2ma, c'].$$

Επομένως, $|b'| \leq |a|$.

2. Αν $|a| > |c'|$, εφαρμόζουμε την S στην τετραγωνική μορφή $[a, b', c']$ και βρίσκουμε

$$f|_S = [c', -b', a].$$

Τώρα έχουμε $|c'| < |a|$ και επιστρέφουμε στο βήμα 1.

3. Αν $|a| \leq |c'|$, σταματούμε, αφού έχουμε ήδη μια τετραγωνική μορφή $[a, b', c']$ για την οποία ισχύει

$$|b'| \leq |a| \leq |c'|.$$

□

Στη συνέχεια υποθέτουμε ότι η $f = [a, b, c]$ είναι μια θετικά ορισμένη τετραγωνική μορφή διακρίνουσας $D < 0$, (D όχι τέλειο τετράγωνο.) Αυτό σημαίνει, ότι $a > 0$ και $c > 0$.

Ορισμός 9.2.8. Μια θετικά ορισμένη τετραγωνική μορφή $f = [a, b, c]$ θα λέγεται ανηγμένη τετραγωνική μορφμή (reduced), όταν $|b| \leq a \leq c$ και επιπλέον όταν ισχύει μία από τις δύο ανισότητες, δηλαδή όταν $|b| = a$ ή $a = c$, τότε επιλέγουμε $b \geq 0$.

Πρόταση 9.2.9. *Σε κάθε κλάση ισοδυναμίας μιας θετικά ορισμένης τετραγωνικής μορφής διακρίνουσας D ανήκει ακριβώς μια ανηγμένη.*

Απόδειξη. Ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο θεώρημα 47 του [9]. □

Παράδειγμα. Έστω $D = -12$. Έχουμε $|D| \geq 3a^2$, άρα $a = 1$ ή $a = 2$.

Αν $a = 1$, τότε $|b| \leq 1$, άρα $b = 1$ ή $b = 0$. Για $b = 1$, $c \notin \mathbb{Z}$. Αν $b = 0$, τότε $c = 3$.

Άρα μια είναι η $[1, 0, 3]$. Έστω τώρα $a = 2$, οπότε $|b| \leq 2$. Αν $b = 0, \pm 1$, το $c \notin \mathbb{Z}$. Αν $b = 2$, τότε $c = 2$. Επομένως, μια δεύτερη είναι η $[2, 2, 2]$.

Παρατήρηση 9.2.10. Αν δύο τετραγωνικές μορφές παριστούν ακριβώς το ίδιο σύνολο ακέραιων, δεν είναι κατ' ανάγκην ισοδύναμες.

Αντιπαράδειγμα: Οι τετραγωνικές μορφές $[2, 1, 3]$ και $[2, -1, 3]$ παριστούν ακριβώς τους ίδιους ακέραιους αλλά δεν είναι ισοδύναμες.

Ο πίνακας μετασχηματισμού είναι ο $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, του οποίου η ορίζουσα είναι -1.

Ας σημειωθεί ότι οι δύο τετραγωνικές μορφές έχουν την ίδια διακρίνουσα -23.

Παρατήρηση 9.2.11. Έστω $f(X, Y) = aX^2 + bXY + cY^2$ μια τετραγωνική μορφή διακρίνουσας D. (Επειδή πάντοτε υποθέτουμε ότι η D δεν είναι τέλειο τετράγωνο, έπεται ότι $a \neq 0$).

Μπορούμε να θεωρήσουμε το πολυώνυμο

$$P_f(z) = az^2 + bz + c.$$

Οι ρίζες του πολυωνύμου είναι

$$r_1 = \frac{-b + \sqrt{D}}{2a} \text{ και } r_2 = \frac{-b - \sqrt{D}}{2a}.$$

Υποθέτουμε ότι η $f(X, Y)$ είναι θετικά ορισμένη. Επομένως $D < 0$ και η r_2 είναι η μιγαδική συζυγής της r_1.

Το $a > 0$, άρα $\mathrm{Im}(r_1) = \frac{\sqrt{|D|}}{2a} > 0$.

Στη συνέχεια υποθέτουμε ότι η $f(X, Y)$ είναι ανηγμένη. Από τη σχέση $|b| \leq a$ έπεται ότι

$$-\frac{1}{2} \leq \mathrm{Re} r_1 \leq \frac{1}{2}.$$

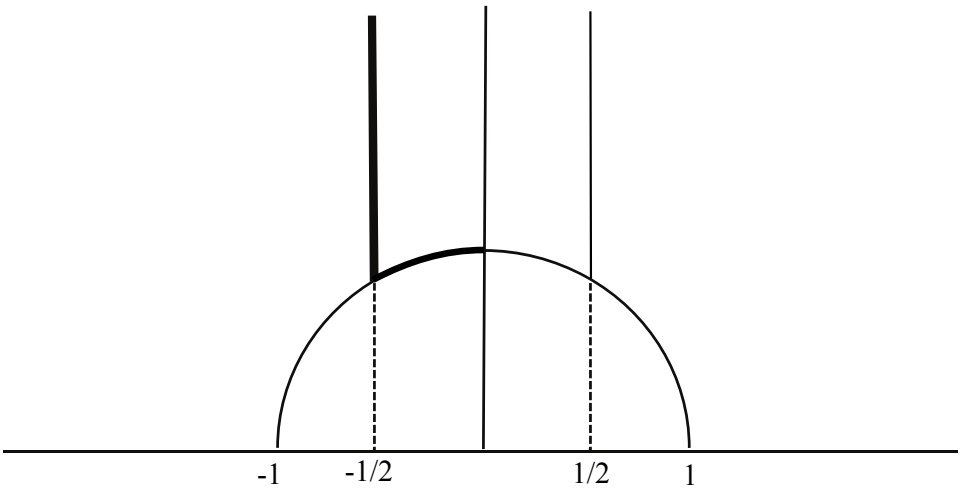
Αν $|b| = a$ παίρνουμε μόνο τη λύση για $b \geq 0$, οπότε $\mathrm{Re} r_1 = -\frac{1}{2}$, δηλαδή

$$-\frac{1}{2} \leq \mathrm{Re} r_1 < \frac{1}{2}.$$

Είναι φανερό ότι

$$|r_1|^2 = r_1 \overline{r_1} = \frac{b^2 - D}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a}.$$

Από τη σχέση $a \leq c$ προκύπτει $\frac{c}{a} \geq 1$, δηλαδή $|r_1| \geq 1$ και αν $c = a$, τότε $b \geq 0$ οπότε $|r_1| = 1$ και $\mathrm{Re} r_1 \leq 0$.



Σχήμα 9.2.1: Θεμελιώδης περιοχή

Επομένως, η τετραγωνική μορφή είναι ανηγμένη ακριβώς τότε όταν η ρίζα r_1 του $P_f(z)$, ($\mathrm{Im} r_1 > 0$) ανήκει στο χωρίο

$$D = \left\{ z \in \mathbb{C} : -\frac{1}{2} \leq \mathrm{Re} z < \frac{1}{2} \text{ και } |z| > 1 \text{ ή } |z| = 1 \text{ και } \mathrm{Re}(z) \leq 0 \right\}.$$

Αν $f(X, Y) = aX^2 + bXY + cY^2$ είναι μια τετραγωνική μορφή διακρίνουσας D και $(a, b, c) =: d$, τότε η $f(X, Y)$ γράφεται ως

$$f(X, Y) = dg(X, Y),$$

όπου

$$g(X, Y) = a'X^2 + b'XY + c'Y^2$$

με $(a', b', c') = 1$ και διακρίνουσα $D' = \frac{D}{d^2}$.

Επομένως μπορούμε να περιοριστούμε σε τετραγωνικές μορφές $f = [a, b, c]$ με $(a, b, c) = 1$, τις οποίες θα ονομάζουμε *πρωταρχικές* (primitive).

Ορισμός 9.2.12. Αν $D \in \mathbb{Z}$ είναι μια διακρίνουσα, τότε ο αριθμός κλάσεων $h(D)$ της D ορίζεται να είναι το πλήθος των κλάσεων ισοδυναμίας πρωταρχικών τετραγωνικών μορφών διακρίνουσας D, όταν $D > 0$ ή το πλήθος των κλάσεων ισοδυναμίας θετικά ορισμένων πρωταρχικών τετραγωνικών μορφών διακρίνουσας D, όταν $D < 0$.

Παρατήρηση 9.2.13. Όταν $D < 0$, τότε σύμφωνα με τα προηγούμενα ο υπολογισμός του αριθμού κλάσεων $h(D)$ είναι εύκολος. Αν για παράδειγμα $D = -23$, εύκολα υπολογίζουμε ότι υπάρχουν ακριβώς τρεις θετικά ορισμένες ανηγμένες τετραγωνικές μορφές, δηλαδή ότι $h(-23) = 3$.

Παρατήρηση 9.2.14. Όταν $D > 0$, υπάρχει αντίστοιχη θεωρία αναγωγής, εξίσου ενδιαφέρουσα, αλλά όχι τόσο «φυσιολογική» όσο αυτή των θετικά ορισμένων τετραγωνικών μορφών και ως εκ τούτου παραλείπεται.

9.3 Παράσταση ακέραιων από τετραγωνικές μορφές και τετραγωνικά υπόλοιπα.

Ορισμός 9.3.1. Θα λέμε ότι ο ακέραιος n παρίσταται γνήσια (properly) από την τετραγωνική μορφή $f = [a, b, c]$, όταν υπάρχουν ακέραιοι x, y ώστε $(x, y) = 1$ και $f(x, y) = n$.

Παρατήρηση 9.3.2. Αν ο n παρίσταται από την $f = [a, b, c]$ και $f(x, y) = n$ για κάποιους ακέραιους x, y με $(x, y) := d$, τότε $(x/d, y/d) = 1$, $d^2 \mid n$ και ο n^2/d παρίσταται γνήσια από την $f = [a, b, c]$.

Επομένως, αν P είναι το σύνολο των ακέραιων οι οποίοι παρίστανται γνήσια από την f, τότε το σύνολο όλων των ακέραιων που παρίστανται από την f είναι το

$$A := \{\ell d^2 \mid \ell \in P \text{ και } d \in \mathbb{Z}\}.$$

Είναι φανερό ότι αν ο ακέραιος n παρίσταται από την f, τότε θα παρίσταται και από κάθε ισοδύναμή της.

Παρατήρηση 9.3.3. Αν $f = [a, b, c] \sim g = [n, k, \ell]$ και $g = f|_M$, με $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ και $\det(M) = 1$, τότε $n = f(a, c)$ και η παράσταση είναι γνήσια αφού $(a, c) = 1$.

Παρατήρηση 9.3.4. Αν ο n παρίσταται γνήσια από την f, έστω $n = f(a, c)$ με $(a, c) = 1$, τότε υπάρχουν ακέραιοι b, d ώστε $ad - bc = 1$. Επομένως, η τετραγωνική μορφή $f|_M$, όπου $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ είναι ισοδύναμη της f και παριστά τον n.

Από τα παραπάνω προκύπτει η επόμενη πρόταση:

Πρόταση 9.3.5. *Το σύνολο των ακέραιων οι οποίοι παρίστανται γνήσια από την f ταυτίζεται με το σύνολο των ακέραιων οι οποίοι εμφανίζονται ως συντελεστές του X^2 για όλες τις τετραγωνικές μορφές που είναι ισοδύναμες προς την f.*

Στη συνέχεια θα δώσουμε ένα κριτήριο του πότε κάποιος φυσικός αριθμός n παρίσταται από μια τετραγωνική μορφή f μέσω τετραγωνικών ισοτιμιών. Συγκεκριμένα ισχύει η

Πρόταση 9.3.6.
1. *Αν ο n παρίσταται γνήσια από την τετραγωνική μορφή $f = [a, b, c]$ διακρίνουσας D, τότε ο D είναι τετραγωνικό υπόλοιπο* $\bmod 4|n|$.
2. *Αν η διακρίνουσα D της τετραγωνικής μορφής $f = [a, b, c]$ είναι τετραγωνικό υπόλοιπο* $\bmod 4|n|$, *τότε ο n παρίσταται από κάποια τετραγωνική μορφή ισοδύναμη της f.*

Απόδειξη. **1.** Σύμφωνα με την πρόταση 9.3.5 αν ο n παρίσταται γνήσια από την τετραγωνική μορφή $f = [a, b, c]$ διακρίνουσας D, τότε υπάρχει μια τετραγωνική μορφή

$$g = [n, k, \ell] \sim f = [a, b, c].$$

Αλλά ισοδύναμες τετραγωνικές μορφές έχουν την ίδια διακρίνουσα σύμφωνα με την πρόταση 9.2.4. Επομένως

$$k^2 - 4n\ell = D,$$

δηλαδή ο D είναι τετραγωνικό υπόλοιπο $\bmod 4|n|$.

2. Από την υπόθεση έπεται ότι υπάρχει κάποιος ακέραιος ℓ τέτοιος ώστε,

$$\ell^2 \equiv D \bmod 4|n|,$$

δηλαδή ότι υπάρχει κάποιος ακέραιος k τέτοιος ώστε,

$$D = \ell^2 - 4|n|k.$$

Αλλά τότε η τετραγωνική μορφή

$$g(X, Y) = nX^2 + \ell XY + kY^2,$$

έχει διακρίνουσα D και παριστά γνήσια τον ακέραιο n αφού $g(1, 0) = n$. □

Πόρισμα 9.3.7. *Αν όλες οι τετραγωνικές μορφές διακρίνουσας D είναι μεταξύ τους ισοδύναμες, τότε η ύπαρξη λύσης της ισοτιμίας*

$$x^2 \equiv D \bmod 4|n|$$

είναι ικανή και αναγκαία συνθήκη ώστε ο n να μπορεί να παρασταθεί από την εν λόγω μορφή.

Παράδειγμα. Άθροισμα δύο τετραγώνων. Θεωρούμε την τετραγωνική μορφή

$$f(X, Y) = X^2 + Y^2$$

η οποία έχει διακρίνουσα $D = -4$.

Πρόταση 9.3.8. *Κάθε πρώτος $p \equiv 1 \bmod 4$ μπορεί να παρασταθεί ως άθροισμα δύο τετραγώνων.*

Απόδειξη. Πράγματι, αν υπάρχει κάποια παράσταση του

$$p = x^2 + y^2, \text{ με } x, y \in \mathbb{Z},$$

αυτή θα είναι κατ' ανάγκη γνήσια αφού αλλιώς θα είχαμε ότι $d^2 \mid p$, όπου $d := (x, y)$, άτοπο.

Είναι γνωστό ότι $h(-4) = 1$, άρα ισχύει η υπόθεση του πορίσματος 9.3.7.

Επειδή $p \equiv 1 \bmod 4$, έπεται ότι η ισοτιμία $X^2 \equiv -1 \bmod p$ είναι επιλύσιμη, συνεπώς και η $Y^2 \equiv -4 \bmod 4p$. □

Στη συνέχεια θα χαρακτηρίσουμε όλους τους θετικούς ακέραιους οι οποίοι μπορούν να παρασταθούν ως άθροισμα δύο τετραγώνων ακέραιων αριθμών.

Πρόταση 9.3.9. *Έστω n θετικός ακέραιος, $n = a^2 \cdot b$ και b ελεύθερος τετραγώνου. Ο n γράφεται ως άθροισμα δύο τετραγώνων, ακριβώς τότε όταν δεν υπάρχει πρώτος $p \equiv 3 \bmod 4$, ο οποίος να διαιρεί τον b.*

Απόδειξη. Υποθέτουμε ότι κάποιος πρώτος αριθμός $p \equiv 3 \bmod 4$, διαιρεί τον n και ότι ο n γράφεται $n = x^2 + y^2$. Επομένως, $x^2 \equiv -y^2 \bmod p$.

Αν $y \not\equiv 0 \bmod p$, τότε $(xy^{-1})^2 \equiv -1 \bmod p$, άτοπο αφού η ισοτιμία $x^2 \equiv -1 \bmod p$ δεν έχει λύση.

Επομένως $p \mid y$ οπότε από την $x^2 \equiv -y^2 \bmod p$ έπεται ότι και $p \mid x$ δηλαδή $p^2 \mid n$ και

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2.$$

Αν τώρα $p \mid \frac{n}{p^2}$ εφαρμόζουμε και πάλι την παραπάνω διαδικασία. Τελικά προκύπτει ότι άρτια δύναμη του p είναι η μεγαλύτερη δύναμη που διαιρεί τον n, δηλαδή $p \nmid b$.

Υποθέτουμε τώρα ότι δεν υπάρχει πρώτος p, $p \equiv 3 \bmod 4$ ο οποίος να διαιρεί τον b.

Από τη γνωστή ταυτότητα

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

προκύπτει ότι αν δύο ακέραιοι μπορούν να παρασταθούν ως άθροισμα δύο τετραγώνων το ίδιο ισχύει και για το γινόμενό τους. Έστω

$$n = 2^r q_1^{2s_1} \cdots q_k^{2s_k} p_1 p_2 \cdots p_m$$

η ανάλυση του n σε γινόμενο πρώτων παραγόντων, όπου $p_i \equiv 1 \bmod 4$ για κάθε $i = 1, 2, \ldots, m$, και $p_i \neq p_j$, για $i \neq j$. Ο $2 = 1^2 + 1^2$, συνεπώς και ο 2^r είναι άθροισμα δυο τετραγώνων. Επίσης

$$q_i^{2s_i} = (q_i^{s_i})^2 + 0 \text{ για κάθε } i = 1, 2, \ldots, k.$$

Τέλος, κάθε p_i είναι άθροισμα δύο τετραγώνων δηλαδή τελικά και ο n είναι άθροισμα δύο τετραγώνων. □

Άσκηση Να αποδειχτεί ότι ο πρώτος αριθμός p μπορεί να παρασταθεί από την τετραγωνική μορφή $X^2 + 2Y^2$ ακριβώς τότε όταν $p \equiv 1$ ή $3 \bmod 8$.

9.4 Το πλήθος των παραστάσεων

Θα μελετήσουμε το πλήθος των παραστάσεων δοθέντος φυσικού αριθμού n από δοθείσα τετραγωνική μορφή $f = [a, b, c]$. Θα περιοριστούμε σε τετραγωνικές μορφές των οποίων η διακρίνουσα είναι *θεμελιώδης*.

Ορισμός 9.4.1. Μία διακρίνουσα λέγεται θεμελιώδης διακρίνουσα όταν

1. Αν $D \equiv 1 \bmod 4$, τότε ο D είναι ελεύθερος τετραγώνου.
2. Αν $D \equiv 0 \bmod 4$, τότε ο αριθμός $\frac{D}{4}$ είναι ελεύθερος τετραγώνου και επιπλέον $\frac{D}{4} \equiv 2$ ή $3 \bmod 4$.

Ορισμός 9.4.2. Χαρακτήρας του Dirichlet $\bmod N$, $N \in \mathbb{N}$, $N \geq 2$, είναι μια συνάρτηση

$$\chi : \mathbb{Z} \to \mathbb{C}$$

για την οποία ισχύουν οι ακόλουθες ιδιότητες

1. $\chi(n) = 0$ αν και μόνο αν $(n, N) > 1$.
2. Η απεικόνιση χ είναι πλήρως πολλαπλασιασική, δηλαδή ισχύει

   $$\chi(mn) = \chi(m)\chi(n)$$

   για όλα τα $m, n \in \mathbb{Z}$.
3. Η τιμή $\chi(n)$ εξαρτάται μόνο από την κλάση $n \bmod N$.

Αν $N_1 \mid N$, $N_1 < N$ και ψ ένας χαρακτήρας Dirichlet modN_1, τότε η σύνθεση

$$\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \longrightarrow \left(\frac{\mathbb{Z}}{N_1\mathbb{Z}}\right)^* \xrightarrow{\psi} \mathbb{C}^*,$$
$$\chi$$

επάγει ένα χαρακτήρα του Dirichlet mod$N$. Στο παραπάνω διάγραμμα η πρώτη απεικόνιση είναι η αναγωγή modN_1.

Χαρακτήρες του Dirichlet οι οποίοι δεν προκύπτουν με αυτό τον τρόπο λέγονται πρωταρχικοί (primitive) χαρακτήρες mod$N$.

Στη συνέχεια, αν D είναι θεμελιώδης διακρίνουσα, ορίζουμε τη συνάρτηση

$$\chi_D : \mathbb{N} \to \mathbb{Z}$$

ως εξής:

1. Αν $p \in \mathbb{P}$, $p \neq 2$, τότε $\chi_D(p) = \left(\frac{D}{p}\right)$,

2. $\chi(2) = \begin{cases} 0 & \text{όταν } D \equiv 0 \bmod 4 \\ 1 & \text{όταν } D \equiv 1 \bmod 8 \\ -1 & \text{όταν } D \equiv 5 \bmod 8 \end{cases}$

3. $\chi_D(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) = \chi_D(p_1^{a_1})\chi_D(p_2^{a_2}) \cdots \chi_D(p_s^{a_s})$.

Αποδεικνύεται ότι η συνάρτηση αυτή είναι περιοδική mod$|D|$ και ότι ορίζει έναν πρωταρχικό χαρακτήρα modulo $|D|$, για τον οποίο επιπλέον ισχύει:

$$\chi_D(-1) = \begin{cases} 1, & \text{όταν } D > 0 \\ -1, & \text{όταν } D < 0 \end{cases}$$

Ένας χαρακτήρας Dirichlet mod$N$ λέγεται πραγματικός, όταν οι μοναδικές τιμές που παίρνει είναι οι $0, 1, -1$. Επιπλέον ισχύει ότι κάθε πραγματικός χαρακτήρας του Dirichlet είναι κάποιος από τους χαρακτήρες χ_D, βλέπε το [5, σελ. 33-40].

Αν τώρα $f(X, Y)$ τετραγωνική μορφή διακρίνουσας D και $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ είναι δυνατόν $f|_M = f$. Σε αυτή την περίπτωση κάθε λύση της $f(x, y) = n$ μας δίνει, μέσω του μετασχηματισμού

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix}$$

μια επιπλέον λύση της $f(X, Y) = n$.

Ορισμός 9.4.3. Τους πίνακες αυτούς θα τους ονομάζουμε αυτομορφισμούς της f.

Είναι προφανές ότι το σύνολο

$$U_f := \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : f|_M = f \right\}$$

αποτελεί υποομάδα της $\mathrm{SL}_2(\mathbb{Z})$.

Αν η $f(X,U)$ είναι πρωταρχική τετραγωνική μορφή διακρίνουσας D, D όχι τέλειο τετράγωνο, τότε αποδεικνύεται [5, σελ. 63] ότι, αν $D>0$, τότε $U_f=\mathbb{Z}\times\mathbb{Z}/2$ και ότι, αν $D<0$, τότε U_f είναι κυκλική ομάδα τάξεως

$$w=\begin{cases}6 & \text{όταν } D=-3\\ 4 & \text{όταν } D=-4\\ 2 & \text{όταν } D<-4\end{cases}.$$

Με $R(n,f)$ συμβολίζουμε το πλήθος των παραστάσεων του n από την τετραγωνική μορφή $f(X,Y)$ οι οποίες δεν είναι ισοδύναμες κάτω από τη δράση της ομάδας U_f. Με $R(n)$ συμβολίζουμε το πλήθος των παραστάσεων του n από τετραγωνικές μορφές διακρίνουσας D.

Ισχύει το ακόλουθο:

Θεώρημα 9.4.4. *Αν D είναι θεμελιώδης διακρίνουσα (D όχι τέλειο τετράγωνο) τότε, για $n\in\mathbb{Z}\backslash\{0\}$ ο αριθμός $R(n)$ των παραστάσεων του n από πρωταρχικές τετραγωνικές μορφές διακρίνουσας D είναι:*

$$R(n)=\sum_{m|n}\chi_D(m).$$

Απόδειξη. Βλέπε το [5, Θεώρημα 3, σελ. 65]. □

Στον παραπάνω τύπο το m διατρέχει όλους τους θετικούς διαιρέτες του n και χ_D είναι ο χαρακτήρας που έχουμε ορίσει.

9.4.1 Ειδική περίπτωση

Έστω $f(X,Y)=X^2+Y^2$. Γνωρίζουμε ότι $D=-4$ και $h(-4)=1$. Επομένως

$$R(n)=R(m,f)=\sum_{m|n}\chi_D(m).$$

Επειδή, για m άρτιο, ισχύει εξ' ορισμού του χ_D ότι $\chi_D(m)=0$, έπεται ότι

$$R(n)=\sum_{\substack{m|n\\ 2\nmid m}}\chi_{-4}(m)=\sum_{\substack{m|n\\ 2\nmid m}}\left(\frac{-4}{m}\right)=$$

$$=\sum_{\substack{m|n\\ 2\nmid m}}\left(\frac{-1}{m}\right)=\sum_{\substack{m|n\\ 2\nmid m}}(-1)^{\frac{m-1}{2}}=$$

$$=\sum_{\substack{m|n\\ m\equiv 1\bmod 4}}1-\sum_{\substack{m|n\\ m\equiv 3\bmod 4}}1=$$

$$=r(1,n)-r(3,n),$$

όπου $r(k,n)$ συμβολίζει το πλήθος των θετικών διαιρετών του φυσικού αριθμού n οι οποίοι είναι ισότιμοι προς τον $k\bmod n$. Επειδή $w(f)=4$, ο συνολικός αριθμός παραστάσεων του φυσικού αριθμού n σε άθροισμα δύο τετραγώνων είναι

$$4\{r(1,n)-r(3,n)\}.$$

Παρατήρηση 9.4.5. Απόδειξη του γενικού τύπου στην ειδική περίπτωση του αθροίσματος δύο τετραγώνων μπορεί να βρει ο αναγνώστης στο [4, σελ 312-318] [7, σελ. 163-176].

Παρατήρηση 9.4.6. Διαφορετική απόδειξη της ειδικής περίπτωσης έδωσε ο G.J. Jacobi, ο οποίος χρησιμοποίησε τη θεωρία των ελλειπτικών συναρτήσεων.

9.5 Ιστορικά στοιχεία

Ο Fermat ήταν ο πρώτος που μελέτησε την παράσταση ακέραιων από τετραγωνικές μορφές. Συγκεκριμένα, σε επιστολή του προς τον Mersenne, τα Χριστούγεννα του 1640, διατυπώνει την πρόταση ότι κάθε πρώτος $p \equiv 1 \mathrm{mod} 4$ παρίσταται ως άθροισμα δύο τετραγώνων θετικών ακέραιων κατά μονοσήμαντο τρόπο.

Μια ιδέα της μεθόδου του (που ονομάζεται «μέθοδος της καθόδου») μας έδωσε αργότερα στα 1659 στην αλληλογραφία του με τον Huygens. Ανάμεσα στα 1742 και 1747 ο Euler έδωσε μια απόδειξη της οποίας η ιδέα ήταν όμοια της ιδέας του Fermat.

Οι περιπτώσεις της παράστασης πρώτων αριθμών από τις τετραγωνικές μορφές $X^2 + 2Y^2$ και $X^2 + 3Y^2$ εμφανίστηκαν αργότερα, το 1659 σε επιστολές του Fermat προς τον Pascal.

Ο Euler στη συνέχεια μελετά και άλλα σχετικά παραδείγματα και διατυπώνει εικασίες όπως ότι για $p \neq 5$ ισχύει

$$p = x^2 + 5y^2 \Leftrightarrow p = 1, 9 \mathrm{mod} 20$$

ή ότι

$$p = x^2 + 27y^2 \Leftrightarrow \left\{ p \equiv 1 \mathrm{mod} 3 \text{ και ότι η ισοτιμία } z^3 \equiv 2 \mathrm{mod} p \text{ έχει λύση} \right\}.$$

Άλλα πρώτος ο Lagrange στο έργο του *Recherches d' arithmetique (1773)* αναπτύσσει τη γενική θεωρία των τετραγωνικών μορφών από την οποία προκύπτουν ως ειδικές περιπτώσεις τα αποτελέσματα του Fermat για την παράσταση πρώτων αριθμών από τις τετραγωνικές μορφές $X^2 + 2Y^2$ και $X^2 + 3Y^2$.

Τέλος, πλήρης θεωρία περιέχεται στο μνημειώδες έργο του Gauss, [2].

Για περισσότερα ιστορικά στοιχεία παραπέμπουμε στα έργα [10], [3], [6], [8], [1].

Βιβλιογραφία

[1] A. Weil: *Number theory, an approach through history, from Hammurapi to Legendere*. Birkhäuser Boston, 1983.

[2] C.F. Gauss: *Disquisitiones Arithmeticae*. Yale University Press, 1965.

[3] David A.Cox: *Primes of the Form* $x^2 + ny^2$. John Wiley and Sons New York, 1989.

[4] Don Redmond: *Number Theory, An Introduction*. Marcel Dekker, 1996.

[5] Don Zagier: *Zetafunktionen Und Quadratische Körper, eine Einführung in die höhere Zahlentheorie*. Springer-Verlag, Berlin, 1981.

[6] Jay R. Goldman: *The Queen of Mathematics:A Historically Motivated Guide to Number Theory*. A. K. Peters Massachussets, 1998.

[7] M. Niven and H.S. Zuckerman and H.L. Montgomery: *An introduction to the theory of numbers*. J. Wiley, 1991.

[8] Sharlau, H. Opolka: *From Fermat to Minkowski, Lectures on the theory, of Numbers and its Historical Development*. Springer, New York, 1985.

[9] J. Hunter: *Αριθμοθεωρία (μετάφραση Ν. Κρητικού)*. Σύλλογος προς διάδοσιν ωφελίμων βιβλίων, Αθήνα, 1980.

[10] Αντωνιάδης, Γιάννης Α.: *Θεωρία Αριθμών κατά τον 17ο και 18ο αιώνα*. Ηράκλειο, 1999.

10

Τετραγωνικά σώματα αριθμών

Στο κεφάλαιο αυτό θα μελετήσουμε την αριθμητική των αρρήτων ποσοτήτων δευτέρου βαθμού σε οργανικά σύνολα, σώματα, καθώς και την αντιστοιχία τους προς τις (διωνυμικές) τετραγωνικές μορφές. Η ύλη του παρόντος κεφαλαίου προοδευτικά θα απαιτεί βασικές γνώσεις από το μάθημα της Άλγεβρας.

Επιθυμούμε να δώσουμε, καταρχήν, μια διαφορετική απόδειξη του Θεωρήματος 9.3.8 το οποίο αποφαίνεται ποιοι φυσικοί αριθμοί παρίστανται ως άθροισμα δύο τετραγώνων.

Αν ο $n \in \mathbb{N}$, γράφεται ως άθροισμα δύο τετραγώνων, δηλαδή υπάρχουν ακέραιοι x, y τέτοιοι ώστε $x^2 + y^2 = n$, τότε έχουμε

$$(x + iy)(x - iy) = n.$$

Επομένως το πρόβλημα ανάγεται στην εύρεση μιγαδικών αριθμών της μορφής $a + ib$ με $a, b \in \mathbb{Z}$, τέτοιους ώστε

$$(a + ib)(a - ib) = n.$$

Θεωρούμε το σύνολο

$$\mathbb{Z}[i] := \{x + iy \text{ με } x, y \in \mathbb{Z}\}.$$

Ορισμός 10.0.1. Το σύνολο $\mathbb{Z}[i]$ θα λέγεται *σύνολο των ακέραιων του Gauss*.

Είναι φανερό ότι το σύνολο αυτό εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού μιγαδικών αριθμών $(\mathbb{Z}[i], +, \cdot)$ αποτελεί ακέραια περιοχή. Επομένως, ακριβέστερα το σύνολο $\mathbb{Z}[i]$ λέγεται *περιοχή του Gauss*.

10.1 Η αριθμητική της περιοχής του Gauss

Αν $\alpha = x + iy$ οποιοσδήποτε μιγαδικός, ο *συζυγής* του θα είναι ο $\alpha' = x - iy$. Ορίζουμε τη *νόρμα (norm)* του α, $N(\alpha) = \alpha \cdot \alpha'$.

Ισχύουν:

(i) Η $N(\alpha)$ είναι μη-αρνητικός πραγματικός αριθμός.

(ii) $N(\alpha) = 0$ τότε και μόνο τότε όταν $\alpha = 0$.

(iii) Ισχύει $N(\alpha\beta) = N(\alpha)N(\beta)$, για κάθε $\alpha, \beta \in \mathbb{Z}[i]$.

(iv) Αν $\alpha \in \mathbb{Z}[i]$ τότε $N(\alpha) \in \mathbb{Z}$.

(v) Αν $\alpha \in \mathbb{Z}[i]$ τότε ο α είναι *μονάδα* του $\mathbb{Z}[i]$, αν και μόνο αν $N(\alpha) = 1$.

(vi) Η ομάδα των μονάδων του $\mathbb{Z}[i]$ είναι $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ (άσκηση).

Θα προσπαθήσουμε τώρα να κατασκευάσουμε μια θεωρία διαιρετότητας και μονοσήμαντης ανάλυσης στην περιοχή του Gauss, εντελώς ανάλογης μ' εκείνη των ακέραιων.

Έστω $\alpha, \beta \in \mathbb{Z}[i]$. Λέμε ότι ο α *διαιρεί* τον β ($\alpha|\beta$), αν και μόνο αν υπάρχει $\gamma \in \mathbb{Z}[i]$ τέτοιος ώστε $\beta = \alpha\gamma$, αλλιώς λέμε ότι ο α δεν διαιρεί τον β ($\alpha \nmid \beta$), π.χ. $2 + i|7 + i$.

Το μέγεθος ενός ακέραιου του Gauss μετριέται μέσω της νόρμας του. Το ανάλογο του αλγόριθμου της διαίρεσης με υπόλοιπο είναι:

Πρόταση 10.1.1. *Έστω $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Υπάρχουν $\gamma, \delta \in \mathbb{Z}[i]$ τέτοιοι ώστε*

$$\alpha = \beta\gamma + \delta, \text{ και } 0 \leq N(\delta) < N(\beta).$$

Απόδειξη: Έχουμε $\alpha = a + bi$, $\beta = c + di$, όπου $a, b, c, d \in \mathbb{Z}$.

$$\frac{\alpha}{\beta} = \frac{a + bi}{c + di}\frac{c - di}{c - di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i = e + fi$$

όπου $e, f \in \mathbb{Q}$

$$e = \frac{ac + bd}{c^2 + d^2},\ f = \frac{bc - ad}{c^2 + d^2}.$$

Υπάρχουν $g, h \in \mathbb{Z}$ τέτοια ώστε $|g - e| \leq \frac{1}{2}$, $|h - f| \leq \frac{1}{2}$. Θέτουμε $\gamma = g + hi$ και βρίσκουμε

$$\frac{\alpha}{\beta} = \gamma + (e - g) + (f - h)i \Longrightarrow \alpha = \beta\gamma + \{(e - g) + (f - h)i\}\beta.$$

Έστω $\delta := \{(e - g) + (f - h)i\}\beta$. Τότε $\alpha = \beta\gamma + \delta$. Επειδή $\gamma \in \mathbb{Z}[i]$, έχουμε $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$. Τώρα:

$$N(\delta) = N((e - g) + (f - h)i)N(\beta) = N(\beta) \cdot \{(e - g)^2 + (f - h)^2\}$$

$$\leq N(\beta\{\frac{1}{4} + \frac{1}{4}\} = \frac{1}{2}N(\beta) < N(\beta)$$

διότι $N(\beta) \neq 0$ καθ' όσον $\beta \neq 0$. □

Ορίζουμε τώρα, εντελώς ανάλογα, τον μέγιστο κοινό διαιρέτη των ακέραιων του Gauss α και β ως εξής: $\gamma = (\alpha, \beta)$ αν και μόνο αν

- $\gamma|\alpha$ και $\gamma|\beta$
- Αν $\delta \in \mathbb{Z}[i]$, και $\delta|\alpha$, $\delta|\beta$ τότε $\delta|\gamma$.

Η διαφορά με τον μέγιστο κοινό διαιρέτη των ακέραιων είναι ότι ζητούμε ο μέγιστος κοινός διαιρέτης στο $\mathbb{Z}$ να είναι θετικός. Αυτό δεν μπορούμε να το κάνουμε στο $\mathbb{Z}[i]$ και αυτό έχει ως συνέπεια ο μέγιστος κοινός διαιρέτης στο $\mathbb{Z}[i]$ να *μην* είναι *μοναδικός*.

Δύο ακέραιοι του Gauss α, β λέγονται *συνεταιρικοί* αν και μόνο εάν υπάρχει $\varepsilon \in E(\mathbb{Z}[i])$ έτσι ώστε $\alpha = \varepsilon\beta$, δηλαδή ο α και ο β είναι συνεταιρικοί συνεπώς αν και μόνο αν ο α είναι κάποιος από τους $\beta, -\beta, i\beta, -i\beta$.

Συμβολισμός: Αν οι α και β είναι συνεταιρικοί συχνά χρησιμοποιούμε τον συμβολισμο $\alpha \cong \beta$.

Πρόταση 10.1.2. *Αν πάλι $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha\beta \neq 0$, τότε οποιοιδήποτε μέγιστοι κοινοί διαιρέτες των α, β είναι μεταξύ τους συνεταιρικοί.*

Απόδειξη: Έστω $\alpha \neq 0$ και γ_1, γ_2 δύο μέγιστοι κοινοί διαιρέτες των α και β. Εξ ορισμού του μέγιστου κοινού διαιρέτη έχουμε

$$\gamma_1|\alpha,\ \gamma_1|\beta,\ \gamma_2|\alpha,\ \gamma_2|\beta$$

καθώς και $\gamma_1|\gamma_2,\ \gamma_2|\gamma_1$. Επειδή $\alpha \neq 0$, έχουμε

$$\gamma_1 \neq 0,\ \gamma_2 = h\gamma_1,\ \gamma_1 = \lambda\gamma_2,\ h, \lambda \in \mathbb{Z}[i].$$

Συνεπώς $\gamma_1 = h\lambda\gamma_1$, δηλαδή $h\lambda = 1 \Rightarrow \lambda = \dfrac{1}{h} \in \mathbb{Z}[i]$. Επομένως $\lambda, h, \in E(\mathbb{Z}[i])$, δηλαδή τα γ_1, γ_2 είναι συνεταιρικά. □

Στη συνέχεια θα αποδείξουμε την ύπαρξη του μέγιστου κοινού διαιρέτη.

Έστω $\alpha, \beta \in \mathbb{Z}[i],\ \alpha, \beta \neq 0$ και

$$S = \{\alpha\lambda + \beta h \mid \lambda, h \in \mathbb{Z}[i]\}.$$

Επειδή $\alpha = \alpha \cdot 1 + \beta \cdot 0$ και $\beta = \alpha \cdot 0 + \beta \cdot 1 \in S$, έπεται ότι το S περιέχει μη-μηδενικούς αριθμούς. Διαλέγουμε $\gamma \in S$ τέτοιο ώστε $N(\gamma)$ να είναι ο ελάχιστος φυσικός (γιατί μπορούμε να βρούμε τον γ;). Ισχυρίζομαι ότι ο γ είναι ένας μέγιστος κοινός διαιρέτης των α και β.

Πράγματι, το γεγονός ότι $\gamma \in S$, συνεπάγεται ότι υπάρχουν $\lambda_0, \upsilon_0 \in \mathbb{Z}[i]$ τέτοιοι ώστε $\gamma = \alpha\lambda_0 + \beta\upsilon_0$.

Αν λοιπόν $\delta|\alpha$ και $\delta|\beta$, έχουμε $\alpha = \delta\vartheta,\ \beta = \gamma\zeta$, οπότε $\gamma = \delta(\vartheta\lambda_0 + \zeta\upsilon_0)$, συνεπώς $\delta|\gamma$.

Θα δείξουμε τώρα ότι κάθε στοιχείο του S (και συνεπώς και τα α, β) είναι πολλαπλάσιο του γ. Καταρχάς παρατηρούμε ότι αν $\varepsilon, \rho \in S$ και $\vartheta \in \mathbb{Z}[i]$ τότε $\varepsilon - \vartheta\rho \in S$.

Πράγματι: Έστω $\varepsilon = \alpha\lambda_1 + \beta\upsilon_1,\ \rho = \alpha\lambda_2 + \beta\upsilon_2$. Τότε

$$\varepsilon - \vartheta\rho = \alpha(\lambda_1 - \vartheta\lambda_2) + \beta(\upsilon_1 - \vartheta\upsilon_2) \in S.$$

Έστω τώρα ω τυχαίο στοιχείο του S. Γράφουμε $\omega = \gamma\zeta + \rho,\ \zeta, \rho \in \mathbb{Z}[i],\ 0 \leq N(\rho) < N(\gamma)$. Επειδή ω και $\gamma \in S$, έπεται ότι$\omega - \gamma\zeta \in S$, δηλαδή $\rho \in S$ οπότε, λόγω της εκλογής του γ, $N(\rho) = 0$ συνεπώς $\rho = 0$. Άρα $\omega = \gamma\zeta$, το οποίο σημαίνει (εξ ορισμού) ότι $\gamma|\omega$.

Άμεση συνέπεια των παραπάνω είναι ότι αν $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha\beta \neq 0$ και γ ένας μέγιστος κοινός διαιρέτης των α και β, υπάρχουν υ και $\lambda \in \mathbb{Z}[i]$ τέτοιοι ώστε

$$\gamma = \alpha\upsilon + \beta\lambda.$$

Στη συνέχεια θα ορίσουμε *πρώτους* αριθμούς στην περιοχή του Gauss. Καταρχήν παρατηρούμε ότι κάθε ακέραιος του Gauss γ διαιρείται από τις μονάδες $\pm 1, \pm i$ και τους συνεταιρικούς του $\pm\gamma, \pm i\gamma$.

- Ένας ακέραιος του Gauss π λέγεται *πρώτος*, αν και μόνο αν δεν είναι μονάδα και οι μόνοι διαιρέτες του είναι οι μονάδες του δακτυλίου $\mathbb{Z}[i]$ και οι συνεταιρικοί του π.
- Έστω π ακέραιος του Gauss τέτοιος ώστε $N(\pi) = p$, όπου p πρώτος αριθμός. Εύκολα φαίνεται ότι ο π είναι *πρώτος*.

Πράγματι, έστω $\delta|\pi$. Τότε $\pi = \delta\gamma$, όπου $\gamma \in \mathbb{Z}[i]$. Συνεπώς

$$N(\pi) = N(\delta)N(\gamma) \Longrightarrow p = N(\delta)N(\gamma) \Longrightarrow N(\gamma) = 1,\ \text{ή } N(\delta) = 1.$$

Επομένως το γ ή το δ είναι μονάδα, δηλαδή $\delta = \pm\pi, \pm i\pi, \pm 1, \pm i$.
Τώρα θα δείξουμε ότι:

Πρόταση 10.1.3. *Αν ο π είναι πρώτος του $\mathbb{Z}[i]$ και α, β είναι ακέραιοι του Gauss τότε*

$$(\pi|\alpha\beta \implies \pi|\alpha \text{ ή } \pi|\beta).$$

Απόδειξη. Πράγματι, έστω ότι $\pi|\alpha\beta$, αλλά $\pi \nmid \beta$. Θα δείξουμε ότι $\pi|\alpha$. Οι μόνοι διαιρέτες του π είναι $\pm 1, \pm i, \pm\pi$ και $\pm i\pi$. Επειδή $\pi \nmid \beta$, έπεται ότι ένας μέγιστος κοινός διαιρέτης (π, β) είναι μια μονάδα του $\mathbb{Z}[i]$, δηλαδή ένας μέγιστος κοινός διαιρέτης $(\pi, \beta) = 1$, οπότε υπάρχουν $\nu, \lambda \in \mathbb{Z}[i]$ τέτοιοι ώστε $1 = \pi\nu + \beta\lambda$, δηλαδή $\alpha = \pi(\nu\alpha) + (\alpha\beta)\lambda$. Επειδή $\pi|\alpha\beta$, έπεται ότι $\pi|\alpha$. □

Ας προσπαθήσουμε τώρα να παραγοντοποιήσουμε ακέραιους του Gauss σε γινόμενο πρώτων. Όπως δεν παραγοντοποιούμε το $0, \pm 1$ στο $\mathbb{Z}$ έτσι δεν παραγοντοποιούμε $0, \pm 1, \pm i$ στον $\mathbb{Z}[i]$. Θα αποδείξουμε ότι

Πρόταση 10.1.4. *Κάθε ακέραιος του Gauss $\gamma \neq 0, \pm 1, \pm i$ αναλύεται σε γινόμενο πρώτων παραγόντων.*

Απόδειξη. Πράγματι, θα το αποδείξουμε επαγωγικά ως προς τη $N(\gamma)$. Προφανώς $N(\gamma) \geq 2$. Αν $N(\gamma) = 2$ τότε (σύμφωνα με την προηγούμενη παρατήρηση) ο γ είναι πρώτος.

Υποθέτουμε τώρα ότι $N(\gamma) > 2$ και ότι κάθε ακέραιος του Gauss που έχει νόρμα μικρότερη της νόρμας του γ, αναλύεται σε γινόμενο πρώτων παραγόντων. Αν ο γ είναι πρώτος, τελειώσαμε. Έστω ότι ο γ δεν είναι πρώτος. Τότε υπάρχουν $\alpha, \beta \in \mathbb{Z}[i]$ όχι μονάδες τέτοιοι ώστε $\gamma = \alpha\beta$. Τότε $1 < N(\alpha),\ N(\beta) < N(\gamma)$ και, λόγω της υπόθεσης της μαθηματικής επαγωγής,

$$\alpha = \pi_1\pi_2\cdots\pi_s, \quad \beta = \nu_1\nu_2\cdots\nu_t,$$

όπου π_i, ν_j πρώτοι του $\mathbb{Z}[i]$. Συνεπώς

$$\gamma = \alpha\beta = \pi_1\pi_2\cdots\pi_s\nu_1\nu_2\cdots\pi_t.$$

□

Στη συνέχεια θα εξετάσουμε αν η ανάλυση αυτή είναι μονοσήμαντη (μοναδική). Βέβαια, αν έχουμε μια ανάλυση, μπορούμε να βάλουμε μονάδες μέσα στο γινόμενο, αλλά αυτήν την ανάλυση δεν θα τη θεωρούμε διαφορετική. Επίσης, δεν ζητούμε η σειρά των πρώτων παραγόντων να είναι η ίδια. Θα αποδείξουμε λοιπόν ότι:

Πρόταση 10.1.5. *Έστω γ ακέραιος του Gauss διαφορετικός των $0, \pm 1, \pm i$. Ο γ γράφεται ως γινόμενο πρώτων. Αν*

$$\gamma = \pi_1\pi_2\cdots\pi_s = \nu_1\nu_2\cdots\nu_t$$

είναι δύο αναλύσεις του γ σε γινόμενο πρώτων, τότε $s = t$ και, αλλάζοντας ίσως τη σειρά των $\nu_1, \nu_2, \cdots, \nu_s$, έχουμε ότι π_1, ν_1 είναι συνεταιρικοί, π_2, ν_2 είναι συνεταιρικοί, $\cdots$, π_s, ν_s είναι συνεταιρικοί.

Απόδειξη. Επαγωγή ως προς την $N(\gamma)$. Έστω $\gamma \neq 0, \pm 1, \pm i$. Τότε $N(\gamma) \geq 2$. Αν $N(\gamma) = 2$ τότε ο γ είναι πρώτος οπότε $\gamma = \pi_1 = \nu_1$, ισχύει. Υποθέτουμε ότι $N(\gamma) > 2$ και ότι η πρόταση είναι αληθής για όλους τους ακέραιους του Gauss με norm μικρότερη της $N(\gamma)$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $s > 1$. Τότε $\pi_1|\pi_1\pi_2\cdots\pi_s \Rightarrow \pi_1|\nu_1\nu_2\cdots\nu_t$, δηλαδή $\pi_1|\nu_j$ για κάποιο j. Ας το ονομάσουμε αυτό ν_1, δηλαδή $\pi_1|\nu_1$. Επειδή ν_1 πρώτος συνεπάγεται ότι $\nu_1 = \pi_1\varepsilon$, ε μονάδα του $\mathbb{Z}[i]$, δηλαδή π_1, ν_1 είναι συνεταιρικά. Η σχέση $\gamma = \pi_1\pi_2\cdots\pi_s = \nu_1\nu_2\cdots\nu_t$ γράφεται

$$\pi_2\pi_3\cdots\pi_s = (\varepsilon\nu_2)\nu_3\cdots\nu_t.$$

Επειδή $N(\pi_1) \geq 2$ και $s > 1$ έπεται

$$1 < N(\pi_2\pi_3\cdots\pi_s) < N(\pi_1\pi_2\cdots\pi_s) = N(\gamma).$$

Λόγω της υπόθεσης της μαθηματικής επαγωγής έχουμε $s-1 = t-1$ και, αλλάζοντας ίσως τη θέση, $(\pi_2, \upsilon_2), \ldots, (\pi_s, \upsilon_s)$ συνεταιρικά. □

Θα δώσουμε τώρα μια καινούργια απόδειξη του προβλήματος, ποιοι φυσικοί μπορούν να γραφούν ως άθροισμα δύο τετραγώνων ακέραιων αριθμών.

Έστω $x^2 + y^2 = n$. Τότε $(x+iy)(x-iy) = n$, οπότε το πρόβλημα γίνεται:

Να βρεθούν όλοι οι ακέραιοι του Gauss με

$$N(x+iy) = x^2 + y^2 = n.$$

Για να λύσουμε αυτό το πρόβλημα θα πρέπει να περιγράψουμε επακριβώς όλους τους πρώτους του $\mathbb{Z}[i]$. Επειδή κάθε συνεταιρικός πρώτου είναι επίσης πρώτος, θα μελετήσουμε τους πρώτους κατά προσέγγιση συνεταιρικών.

Πρόταση 10.1.6. *Έστω π πρώτος του $\mathbb{Z}[i]$. Τότε υπάρχει ακριβώς ένας πρώτος p του $\mathbb{Z}$, τέτοιος ώστε $\pi|p$.*

Απόδειξη. Έχουμε $N(\pi) \in \mathbb{Z}$, συνεπώς $N(\pi) = p_1p_2\cdots p_t$, $p_i \in \mathbb{Z}$, πρώτοι. Επειδή $N(\pi) = \pi\pi'$, έπεται $\pi|p_1p_2\cdots p_t$ δηλαδή $\pi|p_i$ για κάποιο i. Δεν μπορεί να διαιρεί κανέναν άλλο, διότι αν $\pi|p$ και $\pi|q$ με $p \neq q$, τότε $1 = px + qy$ συνεπώς $\pi|px+qy = 1$, επομένως $\pi\upsilon = 1$ άρα $\upsilon = \dfrac{1}{\pi}$ είναι ακέραιος του Gauss, που σημαίνει ότι ο π είναι μονάδα, άτοπο. □

Αρκεί λοιπόν να παραγοντοποιήσουμε όλους τους ακέραιους στον $\mathbb{Z}[i]$. Αν $p = 2$ τότε $2 = -i(1+i)^2$ και ο $1+i$ είναι πρώτος του $\mathbb{Z}[i]$, διότι $N(1+i) = 2$. Δηλαδή όλοι οι πρώτοι του $\mathbb{Z}[i]$, $\pi|2$ είναι συνεταιρικοί του $1+i$.

Έστω τώρα p περιττός πρώτος και έστω $\pi = x+iy|p$, δηλαδή ο p γράφεται $p = \pi\upsilon$, $\upsilon \in \mathbb{Z}[i]$. Επομένως

$$p^2 = N(p) = N(\pi)N(\upsilon) \Longrightarrow N(\pi) = p \quad \text{ή} \quad p^2.$$

Επειδή $x^2 + y^2 \equiv 0, 1, 2 \pmod p$, δεν μπορεί να ισχύει $x^2 + y^2 = p$, όταν $p \equiv 3 \pmod 4$. Σ' αυτή την περίπτωση θα πρέπει να ισχύει $x^2 + y^2 = p^2$, επομένως

$$p^2 = N(p) = N(\pi)N(\upsilon) = p^2N(\upsilon) \Longrightarrow N(\upsilon) = 1,$$

δηλαδή υ μονάδα του $\mathbb{Z}[i]$. Επομένως, αν $p \equiv 3 \pmod 4$ τότε οι π και p είναι συνεταιρικοί.

Έστω τώρα $p \equiv 1 \pmod 4$. Η ισοδυναμία $z^2 \equiv -1 \pmod p$ (1) έχει λύση. Έστω z_0 μια λύση της (1). Τότε

$$p|z_0^2 + 1 \Rightarrow \pi|z_0^2 + 1 \Rightarrow \pi|(z_0 - i)(z_0 + i) \Rightarrow \pi|z_0 - i \text{ ή } \pi|z_0 + i.$$

Σημειώνουμε τώρα ότι $p \nmid (z-i)$ και $p \nmid (z+i)$, διότι $\dfrac{1}{p}z \pm \dfrac{1}{p}i \notin \mathbb{Z}[i]$. Αυτό σημαίνει ότι στην περίπτωση $p \equiv 1 \pmod 4$, οι π και p *δεν* είναι συνεταιρικοί. Επομένως $N(\pi) \neq N(p) = p^2$, δηλαδή $N(\pi) = p$, άρα $\pi\pi' = p$ και συνεπώς ο p διαιρείται από τους π και π'. Για να προσδιορίσουμε πλήρως όλους τους πρώτους του $\mathbb{Z}[i]$, θα πρέπει να δούμε πότε οι π και π' είναι συνεταιρικοί. Έστω λοιπόν $\pi = x+iy$ τέτοιος ώστε $N(\pi) = x^2 + y^2 = p$. Υποθέτουμε ότι οι π και π' είναι συνεταιρικοί, δηλαδή $\pi = \varepsilon\pi'$, $\varepsilon = \pm 1, \pm i$, $\pi' = x - iy$.

Αν $\varepsilon = 1$ τότε $x + iy = x - iy$, δηλαδή $y = 0$ τότε $x^2 = p$, άτοπο. Όμοια αν $\varepsilon = -1$, $x = 0$ και $y^2 = p$, άτοπο.
Αν $\varepsilon = i$ τότε $x + iy = i(x - iy) = y + ix$, δηλαδή $x = y$ και $p = x^2 + x^2 = 2x^2$, άτοπο. Αν $\varepsilon = -i$, τότε $x = -y$, οπότε $2x^2 = p$, άτοπο.

Αποδείξαμε λοιπόν το εξής:

Θεώρημα 10.1.7. *Έστω p πρώτος αριθμός. Η ανάλυση του p στην περιοχή του Gauss είναι:*

- *Αν $p = 2$, τότε $p = -i\pi^2$, όπου π πρώτος του $\mathbb{Z}[i]$ και $N(\pi) = 2$.*
- *Αν $p \equiv 3 \pmod 4$, τότε $p = \pi$ είναι πρώτος και $N(\pi) = p^2$.*
- *Αν $p \equiv 1 \pmod 4$, τότε $p = \pi\pi'$, όπου π και π' πρώτοι μη-συνεταιρικοί και $N(\pi) = N(\pi') = p$.*

Ξαναγυρίζουμε τώρα στο πρόβλημα του καθορισμού των θετικών ακέραιων αριθμών που είναι νόρμα ακέραιων του δακτυλίου του Gauss. Έστω $\alpha \neq 0, \pm 1, \pm i$. Αναλύουμε τον α σε γινόμενο πρώτων στοιχείων του $\mathbb{Z}[i]$. Έστω $\alpha = \pi_1\pi_2\cdots\pi_s$, όπου π_i πρώτοι του $\mathbb{Z}[i]$. Τότε $N(\alpha) = N(\pi_1)N(\pi_2)\cdots N(\pi_s)$. Υποθέτουμε ότι $\pi_i | p_i$, $i = 1, 2, \cdots, s$, p_i πρώτος ακέραιος. Τότε $N(\alpha) = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$, όπου

$$\left\{ \begin{array}{llll} a_i = 2, & \text{αν} & p_i \equiv 3 & (\text{mod } 4) \\ a_i = 1, & \text{αν} & p_i = 2 \text{ ή } & p_i \equiv 1 \pmod 4 \end{array} \right\}$$

Βλέπουμε λοιπόν ότι $N(\alpha) = m^2 q_1 q_2 \cdots q_t$, $m \in \mathbb{Z}$ και $q_1, q_2, \cdots, q_t$ πρώτοι αριθμοί διακεκριμένοι μεταξύ τους και ίσοι με 2 ή ισοδύναμοι με 1 (mod 4).

Ισχύει και το αντίστροφο, ότι δηλαδή κάθε τέτοιος φυσικός αριθμός γράφεται ως άθροισμα δυο τετραγώνων. Δώσαμε επομένως μια άλλη απόδειξη του θεωρήματος 9.3.8 εκμεταλλευόμενοι την αριθμητική της περιοχής του Gauss.

Στη συνέχεια θα εξετάσουμε ένα ακόμα παράδειγμα. Επιθυμούμε να λύσουμε τη διοφαντική εξίσωση

$$Y^3 = X^2 + 1.$$

Υποθέτουμε ότι έχει μια λύση $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ ώστε

$$y^3 = x^2 + 1.$$

Παραγοντοποιούμε το δεξιό μέλος και έχουμε

$$y^3 = (x + i)(x - i), x \pm i \in \mathbb{Z}[i].$$

Η περιοχή $\mathbb{Z}[i]$ είναι ευκλείδεια και συνεπώς και περιοχή κυρίων ιδεωδών καθώς και περιοχή μονοσήμαντης ανάλυσης. Επομένως ορίζεται ο μέγιστος κοινός διαιρέτης δύο στοιχείων αυτής.

Αποδεικνύεται ότι ο μέγιστος κοινός διαιρέτης $(x + i, x - i) \cong 1$. Επομένως, $x + i \cong \xi^3$, για κάποιο στοιχείο $\xi \in \mathbb{Z}[i]$, οπότε $x + i = \varepsilon\xi^3$, όπου ε μία μονάδα του $\mathbb{Z}[i]$. Η ομάδα των μονάδων του $\mathbb{Z}[i]$ είναι η $E(\mathbb{Z}) = \{\pm 1, \pm i\}$. Η απεικόνιση

$$\varphi : \left\{ \begin{array}{ccc} E(\mathbb{Z}[i]) & \longrightarrow & E(\mathbb{Z}[i]) \\ \varepsilon & \longmapsto & \varepsilon^3 \end{array} \right\}$$

είναι ένας αυτομορφισμός της $E(\mathbb{Z}[i])$.

Επομένως μπορούμε να αντικαταστήσουμε τη μονάδα ε με κάποια $u^3, u \in E(\mathbb{Z}[i])$, οπότε προκύπτει

$$x + i = (u\xi)^3 = \eta^3, \text{ όπου } \eta = a + bi, a, b \in \mathbb{Z}.$$

Από τα παραπάνω προκύπτει ότι

$$x + i = (a^3 - 3ab^2) + i(3a^2b - b^3),$$

συνεπώς

$$x = a^3 - 3ab^2 \text{ και } 1 = 3a^2b - b^3 = b(3a^2 - b^2).$$

Από τη δεύτερη ισότητα έχουμε $b = -1$ και $a = 0$. Επομένως η εξίσωση επιδέχεται μοναδική λύση $x = a^3 - 3ab^2 = 0, y = 1$.

Παρατήρηση 10.1.8. Αποφασιστικά στοιχεία για την απόδειξη ήταν:

1. Η ιδιότητα της περιοχής $\mathbb{Z}[i]$ να είναι ευκλείδεια περιοχή και συνεπώς περιοχή μονοσήμαντης ανάλυσης.
2. Η δομή της ομάδας των μονάδων της περιοχής $\mathbb{Z}[i]$.

Ας προσπαθήσουμε τώρα να λύσουμε τη διοφαντική εξίσωση

$$2Y^3 = X^2 + 5.$$

Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση αυτής,

$$2y^3 = x^2 + 5.$$

Παραγοντοποιούμε και πάλι το δεξιό μέλος αυτής.

$$2y^3 = (x + \sqrt{-5})(x - \sqrt{-5}).$$

Σε αυτή την περίπτωση θα πρέπει να εργαστούμε στο σύνολο

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\},$$

το οποίο και πάλι αποτελεί ακέραια περιοχή. Η ομάδα των μονάδων του δακτυλίου $\mathbb{Z}[\sqrt{-5}]$ είναι $E(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$. Το 2 είναι ανάγωγο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$. Πράγματι, αν $2 = a \cdot b$ με $a, b \in \mathbb{Z}[\sqrt{-5}]$ όχι μονάδες, τότε $N(a)N(b) = 4$, οπότε $N(a) = N(b) = \pm 2$. Αυτό όμως είναι αδύνατο αφού αν

$$a = \kappa + \lambda\sqrt{-5},\ \kappa, \lambda \in \mathbb{Z}, N(a) = \kappa^2 + 5\lambda^2 \neq 2.$$

«Επομένως»

$$2 \mid (x + \sqrt{-5}) \text{ είτε } 2 \mid (x - \sqrt{-5})$$

που σημαίνει ότι ο

$$\frac{x + \sqrt{-5}}{2} = \frac{x}{2} + \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

και

$$\frac{x - \sqrt{-5}}{2} = \frac{x}{2} - \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}],$$

το οποίο είναι άτοπο.

Καταλήξαμε στο συμπέρασμα ότι η διοφαντική εξίσωση

$$2Y^3 = X^2 + 5$$

δεν έχει ακέραια λύση.

Και «όμως κινείται» που θα έλεγε και ο Γαλιλαίος! Η εξίσωση έχει τουλάχιστον μια λύση, τη $(x, y) = (\pm 7, 3)$. Πού είναι το λάθος;

Απάντηση: Το 2 είναι *ανάγωγο στοιχείο* του $\mathbb{Z}[\sqrt{-5}]$ αλλά *όχι πρώτο* στοιχείο αυτού. Αυτό σε αντίθεση προς την περιοχή του Gauss.

Γιατί συμβαίνει αυτό;

Απάντηση: Η περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι *περιοχή μονοσήμαντης ανάλυσης*. Αποτελεί εύκολη άσκηση η απόδειξη ότι ο

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

έχει δύο διαφορετικές μεταξύ τους γνήσιες αναλύσεις σε γινόμενα αναγώγων στοιχείων του $\mathbb{Z}[\sqrt{-5}]$.

Υπενθυμίζουμε εδώ την εικασία του Fermat που είδαμε στην παράγραφο 2.3.1 η οποία αποδείχθηκε από τον A. Wiles.

Η διοφαντική εξίσωση

$$X^n + Y^n = Z^n$$

για $n \geq 3$, δεν έχει μη-τετριμμένες ακέραιες λύσεις. Εύκολα διαπιστώνεται ότι αρκεί να αποδειχθεί η εικασία για $n = 4$ και για κάθε περιττό πρώτο αριθμό p. Όπως έχουμε ήδη αναφέρει για $n = 4$ αποδείχθηκε από τον ίδιο τον Fermat.

Για $p = 3$ αποδείχθηκε από τον Euler κατά τα έτη μεταξύ 1753 και 1770, ενώ δημοσιεύθηκε το 1770. Κάποιο μικρό κενό που υπήρχε στην απόδειξη καλύφθηκε από τον Legendre στα 1830.

Την περίπτωση $p = 5$ απέδειξαν κατά τα έτη 1825 και 1828 οι Dirichlet και Legendre, ανεξάρτητα ο ένας από τον άλλο.

Στα 1837 ο E. E. Kummer θεωρεί για κάποιο πρώτο $p > 5$ την πρωταρχική p-ρίζα της μονάδας $\zeta_p = e^{2\pi i/p}$ και παραγοντοποιεί το δεξιό μέλος της εξίσωσης

$$Z^p = X^p + Y^p = \prod_{\nu=0}^{p-1} (X + \zeta_p^\nu Y).$$

Εργάζεται στην ακέραια περιοχή

$$\mathbb{Z}[\zeta_p] := \mathbb{Z} + \zeta_p \mathbb{Z} + \cdots \zeta_p^{p-2} \mathbb{Z}$$

την οποία θεωρεί περιοχή μονοσήμαντης ανάλυσης και «αποδεικνύει»! την εικασία του Fermat. Στα 1843 υποβάλλει την εργασία του στον Dirichlet ο οποίος παρατηρεί ότι για τις περιοχές $\mathbb{Z}[\zeta_p]$ δεν ισχύει για όλους τους πρώτους p η μονοσήμαντη ανάλυση. Ο πιο μικρός πρώτος για τον οποίο δεν ισχύει είναι ο $p = 23$.

Στην προσπάθειά του να διορθώσει το λάθος του ο Kummer εισάγει την έννοια των «ιδεωδών αριθμών» και καταφέρνει να αποδείξει την εικασία του Fermat για τους λεγόμενους ομαλούς (regular) πρώτους. Ας σημειωθεί ότι για $p < 100$ οι μόνοι πρώτοι που δεν είναι ομαλοί είναι οι 37, 59 και 67.

Ακολουθεί η δουλειά του Dedekind (1831-1916), ο οποίος εισάγει δύο έννοιες θεμελιώδους σημασίας για τη Θεωρία των Αριθμών, την Άλγεβρα και τα Μαθηματικά γενικότερα. Αυτές είναι η έννοια του *ιδεώδους* και του *module*.

Στη συνέχεια θα δούμε πώς η αριθμητική των αριθμών θα πρέπει να αντικατασταθεί από την αριθμητική των ιδεωδών.

Στην προσπάθεια λοιπόν επίλυσης της εικασίας του Fermat αναπτύχθηκε η λεγόμενη Αλγεβρική Θεωρία Αριθμών, μια ειδική περίπτωση της οποίας θα εξετάσουμε στα επόμενα.

10.2 Ακέραιοι αλγεβρικοί αριθμοί

Υπενθυμίζουμε ότι ένας μιγαδικός αριθμός α λέγεται αλγεβρικός αριθμός όταν είναι ρίζα ενός πολυωνύμου $f(x) \in \mathbb{Q}[x]$.

Ορισμός 10.2.1. Ο αλγεβρικός αριθμός α λέγεται *ακέραιος αλγεβρικός* τότε και μόνο τότε όταν ο α είναι ρίζα ενός πολυωνύμου

$$f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbb{Z}[x], f(x) \neq 0.$$

Είναι φανερό ότι κάθε ρητός αριθμός α είναι αλγεβρικός, αφού είναι ρίζα του πολυωνύμου $f(x) = x - \alpha \in \mathbb{Q}[x]$.

Παρατήρηση 10.2.2. Ένας ρητός αριθμός α είναι ακέραιος αλγεβρικός τότε και μόνο τότε όταν ο $\alpha \in \mathbb{Z}$. Πράγματι, κάθε ακέραιος αριθμός α είναι ακέραιος αλγεβρικός αφού είναι ρίζα του πολυωνύμου $f(x) = x - \alpha \in \mathbb{Z}[x]$.

Αντίστροφα, έστω $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$ και $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$ και $b > 1$. Υποθέσαμε ότι ο α είναι ακέραιος αλγεβρικός. Επομένως υπάρχει ένα πολυώνυμο

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

το οποίο να έχει τον α ως ρίζα. Δηλαδή

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

Πολλαπλασιάζουμε με b^n και έχουμε

$$a^n + ba_{n-1}a^{n-1} + \cdots b^n a_0 = 0,$$

δηλαδή $b \mid a^n$, άτοπο, αφού $(a, b) = 1$.

Πρόταση 10.2.3. *Το σύνολο*

$$\tilde{\mathbb{Q}} = \{\alpha \in \mathbb{C} \text{ όπου } \alpha \text{ αλγεβρικός αριθμός}\}$$

είναι υπόσωμα του σώματος των μιγαδικών αριθμών.

Απόδειξη. Υποθέτουμε ότι $\alpha, \beta \in \tilde{\mathbb{Q}}$. Από τη σχέση

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

έχουμε: Ο α είναι αλγεβρικός επομένως $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. Ο β είναι αλγεβρικός άρα είναι αλγεβρικός και υπέρ το $\mathbb{Q}(\alpha)$, συνεπώς $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] < \infty$. Επομένως $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] < \infty$, δηλαδή η επέκταση $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ είναι αλγεβρική.

Αυτό σημαίνει ότι τα $\alpha \pm \beta, \alpha\beta$, και για $\beta \neq 0$, α/β είναι αλγεβρικοί αριθμοί. Συνεπώς το $\tilde{\mathbb{Q}}$ είναι σώμα. □

Παρατήρηση 10.2.4. Για μια πιο στοιχειώδη απόδειξη παραπέμπουμε στο βιβλίο [4] του Κ. Λάκκη, *Θεωρία Αριθμών*.

Στη συνέχεια θεωρούμε το σύνολο

$$\mathcal{A} := \{\alpha \in \tilde{\mathbb{Q}} \mid \alpha \text{ ακέραιος αλγεβρικός}\}$$

Θα αποδείξουμε ότι το σύνολο $\mathcal{A}$ αποτελεί ακέραια περιοχή, υποδακτύλιο του $\tilde{\mathbb{Q}}$. Για να το πετύχουμε, χρειαζόμαστε μια βοηθητική:

Πρόταση 10.2.5. *Ο μιγαδικός αριθμός α είναι αλγεβρικός ακέραιος αν και μόνο αν η προσθετική ομάδα η οποία παράγεται από όλες τις δυνάμεις του α,*

$$1, \alpha, \alpha^2, \ldots$$

είναι πεπερασμένα παραγόμενη.

Απόδειξη. Είναι σαφές ότι αν ο α είναι ακέραιος αλγεβρικός ικανοποιεί μια εξίσωση της μορφής

$$f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

με συντελεστές ακέραιους αριθμούς. Ας θεωρήσουμε μια οποιαδήποτε πολυωνυμική έκφραση του α, $F(\alpha)$, όπου $F(x) \in \mathbb{Z}[x]$. Έχουμε

$$F(x) = \pi(x)f(x) + u(x),$$

όπου το $u(x)$ είναι ή μηδενικό πολυώνυμο ή $\deg(u) < n$. Συνεπώς $F(\alpha) = u(\alpha)$, και αρκούν οι δυνάμεις $1, \alpha, \ldots, \alpha^{n-1}$ για να παράξουν τη ζητούμενη ομάδα.

Αντιστρόφως, ας υποθέσουμε ότι τα στοιχεία $z_1, \ldots, z_n$ παράγουν την προσθετική ομάδα $\mathbb{Z}[\alpha]$. Αυτό σημαίνει ότι για κάθε $1 \le i \le n-1$ υπάρχουν $\lambda_{ij} \in \mathbb{Z}$ ώστε

$$\alpha z_i = \sum_{\nu=0}^{n-1} \lambda_{\nu,i} z_i.$$

Με άλλα λόγια το σύστημα

$$\left(\alpha \mathbb{I}_n - \lambda_{i,j}\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

επιδέχεται εκτός της μηδενικής λύσης και την $(z_1, \ldots, z_n)^t$. Άρα $\det(\mathbb{I}_n - (\lambda)_{i,j}) = 0$ η οποία είναι μια ορίζουσα της μορφής

$$x^n + b_1 x^{n-1} + \cdots + b_1 x + b_0 = 0, \qquad b_i \in \mathbb{Z}$$

που ικανοποιείται από το α, άρα ο α είναι ακέραιος αλγεβρικός.

□

Θα αποδείξουμε τώρα ότι ο $\mathcal{A}$ είναι υποδακτύλιος του $\tilde{\mathbb{Q}}$.

Έστω $\alpha, \beta \in \mathcal{A}$. Θα πρέπει να αποδείξουμε ότι $\alpha + \beta$ και $\alpha \cdot \beta$ είναι στοιχεία του $\mathcal{A}$.

Σύμφωνα με την πρόταση 10.2.5, το α ανήκει σε μια πεπερασμένα παραγόμενη προσθετική ομάδα G_α, υποομάδα του $\mathbb{C}$. Ομοίως και το β ανήκει σε μια πεπερασμένα παραγόμενα προσθετική ομάδα G_β.

Επόμενως τα $\alpha + \beta$ και $\alpha\beta$ είναι ακέραιοι γραμμικοί συνδυασμοί των στοιχείων $\alpha^i\beta^j$, τα οποία ανήκουν στην ομάδα $G_\alpha G_\beta$ η οποία είναι φανερό ότι είναι πεπερασμένα παραγόμενη.

Από τα παραπάνω συμπεραίνουμε ότι και όλες οι δυνάμεις των $\alpha+\beta$ και $\alpha\beta$ ανήκουν σε μια πεπερασμένα παραγόμενη προσθετική υποομάδα του $\mathbb{C}$. Από την προηγούμενη πρόταση προκύπτει ότι $\alpha+\beta$ και $\alpha\cdot\beta\in\mathcal{A}$, επομένως $\mathcal{A}$ υποδακτύλιος του $\tilde{\mathbb{Q}}$.

Ουσιαστικά το κύριο αντικείμενο της αλγεβρικής θεωρίας αριθμών είναι η μελέτη της αριθμητικής του σώματος $\tilde{\mathbb{Q}}$. Επειδή, όμως, αυτό είναι αρκετά δύσκολο θα περιορίσουμε τις ... φιλοδοξίες μας!

Ορισμός 10.2.6. Ένα σώμα K υπόσωμα του $\mathbb{C}$ θα λέγεται *αλγεβρικό σώμα αριθμών* ακριβώς τότε όταν η επέκταση $K/\mathbb{Q}$ είναι πεπερασμένη.

Αφού $K/\mathbb{Q}$ είναι πεπερασμένη, έπεται ότι είναι αλγεβρική, δηλαδή το K είναι υπόσωμα του $\tilde{\mathbb{Q}}$.

Σημείωση 10.2.7. Η επέκταση $\tilde{\mathbb{Q}}/\mathbb{Q}$ είναι άπειρη αλγεβρική.

Η επέκταση $K/\mathbb{Q}$ είναι πεπερασμένη και διαχωρίσιμη. Επομένως είναι απλή, δηλαδή υπάρχει ένα $\vartheta\in K$ τέτοιο ώστε $K=\mathbb{Q}(\vartheta)$.

Παρατήρηση 10.2.8. Αν $\alpha\in\tilde{\mathbb{Q}}$, τότε υπάρχει ακέραιος m τέτοιος ώστε $m\alpha\in\mathcal{A}$.

Πράγματι, $\alpha\in\tilde{\mathbb{Q}}$ σημαίνει ότι υπάρχει ένα πολυώνυμο

$$f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0\in\mathbb{Q}[X],$$

τέτοιο ώστε $f(\alpha)=0$. Επιλέγουμε έναν ακέραιο m, τέτοιον ώστε $ma_i\in\mathbb{Z}$, για κάθε $i=0,1,2,\ldots,m-1$. Επομένως έχουμε

$$(m\alpha)^n+ma_{n-1}(m\alpha)^{n-1}+\cdots+m^na_0=0,$$

δηλαδή ότι $m\alpha\in\mathcal{A}$.

Άμεση συνέπεια της παρατήρησης αυτής είναι ότι αν K είναι αλγεβρικό σώμα αριθμών, τότε υπάρχει $\vartheta\in\mathcal{A}$ τέτοιο ώστε $K=\mathbb{Q}(\vartheta)$.

Πράγματι, $K=\mathbb{Q}(h)$ με $h\in\tilde{\mathbb{Q}}$. Έστω $m\in\mathbb{Z}$ ώστε $\vartheta:=mh\in\mathcal{A}$. Είναι φανερό ότι $K=\mathbb{Q}(h)=\mathbb{Q}(\vartheta)$.

Η περιοχή των ακέραιων αλγεβρικών αριθμών του K είναι $R:=K\cap\mathcal{A}\leq K$.

Στη συνέχεια θα περιοριστούμε στα *τετραγωνικά σώματα αριθμών*, δηλαδή αλγεβρικά σώματα αριθμών K με $[K:\mathbb{Q}]=2$.

Αποτελούν, μετά το $\mathbb{Q}$, την απλούστερη περίπτωση αλγεβρικών σωμάτων αριθμών. Έχουν όμως το πλεονέκτημα ότι όλες οι βασικές ιδιότητες των αλγεβρικών σωμάτων αριθμών εμφανίζονται ήδη στα τετραγωνικά σώματα αριθμών και θα διατυπώσουμε τις γενικές προτάσεις χωρίς απόδειξη.

Έστω ϑ αλγεβρικός αριθμός του τετραγωνικού σώματος αριθμών K, τέτοιος ώστε $K=\mathbb{Q}(\vartheta)$. Αφού $[K,\mathbb{Q}]=2$ θα πρέπει ο βαθμός του αναγώγου πολυωνύμου $\mathrm{Irr}(\vartheta,\mathbb{Q})$ να είναι δύο, δηλαδή το ανάγωγο πολυώνυμο του ϑ υπέρ το $\mathbb{Q}$ να έχει τη μορφή

$$\mathrm{Irr}(\vartheta,\mathbb{Q})=X^2-aX-b.$$

Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $a=0$, διότι αλλιώς παίρνουμε τον αριθμό $\vartheta^*=\vartheta-\frac{a}{2}$ ο οποίος είναι ρίζα του πολυωνύμου

$$X^2-b',$$

όπου $b'=\frac{a^2}{4}+b$ και $K=\mathbb{Q}(\vartheta^*)$. Ο ρητός b' δεν είναι τέλειο τετράγωνο στο $\mathbb{Q}$, διότι το X^2-b' είναι ανάγωγο στο $\mathbb{Q}[X]$.

Γράφουμε το $b' = mr^2$, $r \in \mathbb{Q}$ όπου $m \in \mathbb{Z}$ ο οποίος δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Προφανώς $m \neq 1$, διότι αλλιώς θα είχαμε $b' = r^2$. Αν $r \neq 1$ τότε θεωρούμε τον αριθμό

$$\partial'' := \frac{\partial'}{r} \in K$$

ο οποίος είναι ρίζα του πολυωνύμου

$$X^2 - m.$$

Αποδείξαμε το

Θεώρημα 10.2.9. *Κάθε τετραγωνικό σώμα αριθμών K προκύπτει από το $\mathbb{Q}$ με επισύναψη της τετραγωνικής ρίζας ενός ακέραιου αριθμού $m \neq 1$ ελευθέρου τετραγώνου.*

Γνωρίζουμε από την Άλγεβρα ότι

$$K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m}, a, b \in \mathbb{Q}\}.$$

Αν $m > 0$, τότε $K = \mathbb{Q}(\sqrt{m}) \subseteq \mathbb{R}$ και το K λέγεται *πραγματικό τετραγωνικό σώμα αριθμών*. Αν, όμως, $m < 0$, τότε κάθε στοιχείο του K που δεν είναι ρητός είναι μιγαδικός και το σώμα λέγεται *μιγαδικό σώμα αριθμών*.

Το K είναι σώμα αναλύσεως του διαχωρίσιμου πολυωνύμου $X^2 - m$. Συνεπώς η επέκταση $K/\mathbb{Q}$ είναι επέκταση του Galois. Η ομάδα Galois της επέκτασης αυτής είναι η

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\},$$

όπου $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$ για $a, b \in \mathbb{Q}$.

Κάθε στοιχείο $\alpha = a + b\sqrt{m}$ έχει ίχνος

$$S_K(\alpha) = \alpha + \sigma(\alpha) = 2a$$

και νόρμα

$$N_K(\alpha) = \alpha \cdot \sigma(\alpha) = a^2 - mb^2.$$

Προφανώς το ανάγωγο πολυώνυμο του $\alpha = a + b\sqrt{m}$ υπέρ το $\mathbb{Q}$ είναι το

$$(X - \alpha)(X - \sigma(\alpha)) = X^2 - S_K(\alpha)X + N_K(\alpha). \tag{10.2.1}$$

Παρατήρηση: Τα $S_K(\alpha), N_K(\alpha)$ στην περίπτωση του τετραγωνικού σώματος αριθμών θα μπορούσαν να οριστούν και από το ανάγωγο ποολυώνυμο του $a + b\sqrt{m}$, από την εξίσωση (10.2.1).

Ώστε:

Θεώρημα 10.2.10. *Έστω $\alpha \in \mathbb{Q}(\sqrt{m})$. Ο α είναι ακέραιος αλγεβρικός ακριβώς τότε όταν $S_K(\alpha) \in \mathbb{Z}$ και $N_K(\alpha) \in \mathbb{Z}$.*

Γράφουμε $\alpha = a + b\sqrt{m}$ και θέτουμε $2a = \gamma$, $2b = \delta$, οπότε το ίχνος είναι ακέραιος τότε και μόνο τότε ο γ είναι ακέραιος και η νόρμα του α είναι ακέραιος. Η τελευταία συνθήκη γράφεται

$$a^2 - mb^2 = \frac{\gamma^2}{4} - m\frac{\delta^2}{4} = \frac{\gamma^2 - m\delta^2}{4}.$$

Επομένως ο α είναι ακέραιος αλγεβρικός αν και μόνο αν

$$\gamma, \delta \in \mathbb{Z} \text{ και } \gamma^2 \equiv m\delta^2 \mathrm{mod} 4.$$

Αν $m \equiv 2,3 \mathrm{mod} 4$, επειδή για κάθε $x \in \mathbb{Z}$ έχουμε $x^2 \equiv 0,1 \mathrm{mod} 4$ για να έχει η $\gamma^2 \equiv m\delta^2 \mathrm{mod} 4$ λύση θα έπρεπε $\gamma \equiv \delta \equiv 0 \mathrm{mod} 2$, δηλαδή $\alpha, \beta \in \mathbb{Z}$.

Αν $m \equiv 1 \mathrm{mod} 4$, τότε για να έχει η ισοτιμία $\gamma^2 \equiv m\delta^2 \mathrm{mod} 4$ λύση, θα πρέπει

$$\gamma \equiv \delta \mathrm{mod} 2$$

οπότε ο $\frac{\gamma-\delta}{2} \in \mathbb{Z}$ και

$$\alpha = a + b\sqrt{m} = \frac{\gamma}{2} + \frac{\delta}{2}\sqrt{m} = \frac{\gamma-\delta}{2} + \delta\frac{1+\sqrt{m}}{2}.$$

Παράδειγμα. Αν $K = \mathbb{Q}(i)$, τότε η περιοχή των ακέραιων αλγεβρικών αριθμών του K είναι $R_K = \mathbb{Z}[i]$. Αν $K = \mathbb{Q}(\sqrt{-5})$, τότε η περιοχή των ακέραιων αλγεβρικών είναι $R_K = \mathbb{Z}[\sqrt{-5}]$.

10.3 Βάση και διακρίνουσα

Ορισμός 10.3.1. Έστω R ένας δακτύλιος και $(\omega_1, \omega_2, \ldots, \omega_n)$ μια n-άδα στοιχείων αυτού. Η n-άδα αυτή θα λέγεται *βάση ακεραιότητας* του δακτυλίου R όταν κάθε στοιχείο $\alpha \in R$ γράφεται μονοσήμαντα στη μορφή:

$$\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$$

και $a_i \in \mathbb{Z}$ για $i = 1, 2, \ldots, n$.

Φυσικά δεν έχει κάθε δακτύλιος μια βάση ακεραιότητας. Ούτε, αν έχει ο R μια βάση ακεραιότητας είναι μοναδική.

Έστω τώρα $K = \mathbb{Q}(\sqrt{m})$ ένα τετραγωνικό σώμα αριθμών και

$$\omega_m = \begin{cases} \frac{1}{2}(1+\sqrt{m}) & \text{όταν } m \equiv 1 \mathrm{mod} 4 \\ \sqrt{m} & \text{όταν } m \equiv 2,3 \mathrm{mod} 4 \end{cases}$$

Σύμφωνα με τα προηγούμενα της παραγράφου 10.2 προκύπτει αμέσως η αλήθεια της επόμενης πρότασης.

Πρόταση 10.3.2. *Μια βάση ακεραιότητας του R_K είναι το σύνολο $\{1, \omega_m\}$.*

Παρατήρηση 10.3.3. Αντίστοιχη πρόταση ισχύει και στη γενική περίπτωση σωμάτων αριθμών.

Πρόταση 10.3.4. *Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και R_K η περιοχή των ακέραιων αλγεβρικών αριθμών του K. Η R_K έχει μια βάση ακεραιότητας «διάστασης» n.*

Φυσικά δεν είναι τόσο εύκολος ο υπολογισμός της, όπως στα τετραγωνικά σώματα αριθμών.

Στη συνέχεια υποθέτουμε ότι $K = \mathbb{Q}(\sqrt{m})$ είναι ένα τετραγωνικό σώμα αριθμών και $\{1, \omega_m\}$ η βάση ακεραιότητας της πρότασης 10.3.2.

Ορισμός 10.3.5. Διακρίνουσα D_K του τετραγωνικού αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ λέγεται η ορίζουσα

$$D_K = \left(\det\begin{pmatrix} 1 & 1 \\ \omega_m & \bar{\omega}_m \end{pmatrix}\right)^2 = \begin{cases} m & \text{αν } m \equiv 1 \mathrm{mod} 4 \\ 4m & \text{αν } m \equiv 2,3 \mathrm{mod} 4 \end{cases}.$$

Παρατήρηση 10.3.6. Αποδεικνύεται ότι η διακρίνουσα είναι ανεξάρτητη της επιλογής της βάσης του δακτυλίου των ακέραιων αλγεβρικών.

Ο λόγος είναι ότι αν έχουμε δύο βάσεις ακεραιότητας του R_K τότε η μία προκύπτει από την άλλη δια πολλαπλασισμού με έναν ορθμοναδιαίο (unimodular) πίνακα, δηλαδή πίνακα με στοιχεία ακέραιους αριθμούς και ορίζουσα ± 1 (άσκηση).

Παρατήρηση 10.3.7. Είναι φανερό ότι στα τετραγωνικά σώματα αριθμών η διακρίνουσα ορίζεται μονοσήμαντα από το σώμα $K = \mathbb{Q}(\sqrt{m})$.

Παρατήρηση 10.3.8. Η διακρίνουσα ορίζεται σε κάθε αλγεβρικό σώμα αριθμών. Αποδεικνύεται ότι υπάρχουν πεπερασμένου πλήθους αλγεβρικά σώματα αριθμών με διακρίνουσα δοσμένο ακέραιο αριθμό.

10.4 Η ομάδα των μονάδων

Έστω $K = \mathbb{Q}(\sqrt{m})$ τετραγωνικό αλγεβρικό σώμα αριθμών και R_K η περιοχή των ακέραιων αλγεβρικών αριθμών. Θα μελετήσουμε την ομάδα των μονάδων του R_K.

Ως γνωστό το στοιχείο $\varepsilon \in R_K$ είναι μονάδα της περιοχής R_K ακριβώς τότε όταν η norm $N_{K/\mathbb{Q}}(\varepsilon) = \varepsilon\varepsilon' = \pm 1$, όπου ε' είναι το συζυγές του ε.

Ώστε το στοιχείο $\varepsilon = a + b\omega_m$ είναι μονάδα του δακτυλίου R_K ακριβώς τότε όταν

$$a^2 - b^2 m = \pm 1 \text{ για } m \equiv 2, 3 \bmod 4$$

και

$$a^2 + ab + \frac{1-m}{4} b^2 = \pm 1 \text{ για } m \equiv 1 \bmod 4.$$

Ξεχωρίζουμε τώρα δύο περιπτώσεις:

Περίπτωση I $m < 0$ δηλαδή το $K = \mathbb{Q}(\sqrt{m})$ είναι μιγαδικό τετραγωνικό σώμα αριθμών. Έστω πάλι $m \equiv 2$ ή $3 \bmod 4$. Αφού $a^2 - b^2 m > 0$ αρκεί να εξετάσουμε μόνο την περίπτωση

$$a^2 + |m| b^2 = 1.$$

Αν $|m| > 1$, τότε για να ισχύει η ισότητα θα πρέπει $b = 0$, οπότε $a = \pm 1$ και τελικά $\varepsilon = \pm 1$.

Αν $m = -1$ έχουμε

$$a^2 + b^2 = 1,$$

δηλαδή τις τέσσερις λύσεις $a = \pm 1, b = 0$ και $a = 0, b = \pm 1$, δηλαδή $\varepsilon = \pm 1, \pm i$.

Έστω τώρα ότι $m \equiv 1 \bmod 4$. Αφού

$$a^2 + ab + \frac{1-m}{4} b^2 = (a + b/2)^2 + \frac{|m|}{4} b^2 \geq 0$$

αρκεί να θεωρήσουμε την

$$a^2 + ab + \frac{1-m}{4} b^2 = (a + b/2)^2 + \frac{|m|}{4} b^2 = 1.$$

Αν $|m| > 4$ τότε $b = 0$, δηλαδή και πάλι $a = \pm 1$ άρα $\varepsilon = \pm 1$. Αν $|m| \leq 4$ αφού $m \equiv 1 \bmod 4$, η μοναδική προς εξέταση τιμή του m είναι η $m = -3$. Σε αυτή την περίπτωση έχουμε

$$a^2 + ab + \frac{1-m}{4} b^2 = (a + b/2)^2 + \frac{3}{4} b^2 = 1.$$

Για $|b| \geq 2$ δεν υπάρχουν λύσεις. Για $b = 1$ καταλήγουμε στην $a^2 + a + 1 = 1$, η οποία έχει τις λύσεις $a = 0$ ή $a = 1$.

Για $b = 0$ οι λύσεις είναι $a = \pm 1$ και για $b = -1$ έχουμε $a = 0$. Άρα οι μονάδες είναι οι

$$\pm 1, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}.$$

Επομένως έχουμε αποδείξει το

Θεώρημα 10.4.1. *Έστω $K = \mathbb{Q}(\sqrt{m})$ μιγαδικό τετραγωνικό σώμα αριθμών. Η ομάδα των μονάδων της περιοχής R_K είναι η*

$$E(R_K) = \begin{cases} \{\pm 1\} & \text{αν } m < -4 \\ \{\pm 1, \pm i\} & \text{αν } m = -4 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & \text{αν } m = -3 \end{cases}$$

Περίπτωση II Έστω ότι $m > 0$, δηλαδή το K είναι ένα πραγματικό σώμα αριθμών. Η περίπτωση αυτή είναι πολύ πιο δύσκολη από την προηγούμενη.

Στον R_K υπάρχουν άπειρες το πλήθος μονάδες και αυτό είναι συνέπεια του ότι η εξίσωση του Pell

$$X^2 - mY^2 = 1$$

έχει άπειρες λύσεις, και της απλούστατης παρατήρησης ότι κάθε αριθμός του K της μορφής $x + y\sqrt{m}$, $x, y \in \mathbb{Z}$ είναι ακέραιος αλγεβρικός.

Λήμμα 10.4.2. *Έστω $B \in \mathbb{R}$. Υπάρχουν πεπερασμένου πλήθους μονάδες του R_K για τις οποίες ισχύει $1 < \varepsilon < B$.*

Απόδειξη. Έστω ε μια ρίζα του πολυωνύμου

$$X^2 - S_K(\varepsilon)X \pm 1.$$

Τώρα $\varepsilon > 1$ και $N_K(\varepsilon) = \pm 1$, συνεπώς αν ε' είναι η άλλη ρίζα του παραπάνω πολυωνύμου $|\varepsilon'| = \varepsilon^{-1} < 1$, οπότε

$$|S_K(\varepsilon)| = |\varepsilon + \varepsilon'| \leq |\varepsilon| + |\varepsilon'| < B + 1.$$

Δηλαδή ο ε είναι ρίζα ένος πολυωνύμου της μορφής

$$X^2 + \lambda X \pm 1,$$

όπου $\lambda \in \mathbb{Z}$ και $|\lambda| \leq B + 1$. Υπάρχουν πεπερασμένου πλήθους τέτοια πολυώνυμα και κάθε ένα από αυτά έχει δύο ρίζες, άρα καταλήγουμε σε πεπερασμένου πλήθους επιλογές για το ε. □

Έστω $\varepsilon \in E(R_K) \backslash \{\pm 1\}$. Τότε κάποια από τις $\varepsilon, -\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$ θα είναι μεγαλύτερη του 1.

Υποθέτουμε, λοιπόν, ότι $\varepsilon \in E(R_K)$ με $\varepsilon > 1$. Παρατηρούμε ότι ανάμεσα στο 1 και στο ε υπάρχουν πεπερασμένες το πλήθος μονάδες του R_K, θα υπάρχει και μια ελάχιστη, έστω η ε_0, με $1 < \varepsilon_0 \leq \varepsilon$.

Θα αποδείξουμε τώρα ότι

Θεώρημα 10.4.3. *Η ομάδα των μονάδων δίνεται από*

$$E(R_K) = \{\pm \varepsilon_0^n : n \in \mathbb{Z}\}.$$

Απόδειξη. Έστω $\varepsilon \geq 1$ μια μονάδα του R_K. Αφού $\varepsilon_0 > 1$ έπεται ότι $\varepsilon_0^n \to \infty$ για $n \to \infty$. Άρα υπάρχει φυσικός n, ώστε

$$\varepsilon_0^n \leq \varepsilon < \varepsilon_0^{n+1}.$$

Οπότε $1 \leq \varepsilon_0^{-n}\varepsilon < \varepsilon_0$ και αφού ε_0 η ελάχιστη μεγαλύτερη του 1 μονάδα, έχουμε ότι $\varepsilon\varepsilon_0^{-n} = 1$, συνεπώς $\varepsilon = \varepsilon_0^n$.

Αν ε τυχαία μονάδα του R_K, μια από τις $\pm\varepsilon, \pm\varepsilon^{-1}$ θα είναι μεγαλύτερη της μονάδας και τελικά η ε θα είναι της μορφής $\pm\varepsilon_0^n$ με $n \in \mathbb{Z}$. □

Το ερώτημα είναι γιατί τα τετραγωνικά σώματα αριθμών έχουν πεπερασμένο πλήθος μονάδων και τα τετραγωνικά πραγματικά άπειρο πλήθος; Τι γίνεται στη γενική περίπτωση;

Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$, $K = \mathbb{Q}(\vartheta)$. Αν $f(X)$ είναι το ανάγωγο πολυώνυμο του ϑ υπέρ το $\mathbb{Q}$ τότε $\deg f(X) = n$ και

$$f(X) = (X - \vartheta^{(1)})(X - \vartheta^{(2)}) \cdots (X - \vartheta^{(n)}),$$

$\vartheta^{(1)} = \vartheta$. Υποθέτουμε ότι r_1 είναι το πλήθος των πραγματικών ριζών του $f(X)$ και $2r_2$ είναι το πλήθος των μιγαδικών. Οι μιγαδικές ρίζες έχουν άρτιο πλήθος γιατί αν ένα πολυώνυμο με συντελεστές πραγματικούς αριθμούς έχει μια μιγαδική ρίζα τότε έχει και τη συζυγή της. Επομένως $r_1 + 2r_2 = n$.

Θεώρημα 10.4.4 (Θεώρημα μονάδων του Dirichlet)**.** *Υπάρχουν $r := r_1 + r_2 - 1$ μονάδες $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ μονάδες της ομάδας $E(R_K)$ έτσι ώστε κάθε μονάδα του R_K να έχει μονοσήμαντη παράσταση της μορφής*

$$\varepsilon = \zeta\varepsilon_1^{s_1}\varepsilon_2^{s_2} \cdots \varepsilon_r^{s_r},$$

όπου $s_i \in \mathbb{Z}$ για $i \in 1, 2, \ldots, r$ και ζ είναι μια ρίζα της μονάδας.

Εφαρμογή: Αν $K = \mathbb{Q}(\sqrt{m})$ είναι τετραγωνικό μιγαδικό σώμα αριθμών, το $f(X) = X^2 - m$ έχει δύο μιγαδικές ρίζες και συνεπώς $r_1 = 0$ και $r_2 = 1$. Άρα $r = r_1 + r_2 - 1 = 0$.

Αν πάλι $K = \mathbb{Q}(\sqrt{m})$ τετραγωνικό πραγματικό σώμα αριθμών, τότε $r_1 = 2$ και $r_2 = 0$, συνεπώς $r = r_1 + r_2 - 1 = 1$.

Πρόβλημα: Πώς θα βρούμε μια θεμελιώδη μονάδα ενός πραγματικού τετραγωνικού σώματος αριθμών;

Η θεωρία των συνεχών κλασμάτων είναι και πάλι χρήσιμη. Προκειμένου να διατυπώσουμε το θεώρημα, χρειαζόμαστε να «ομογενοποιήσουμε» τη βάση ακεραιότητας του R_K, όπου K τετραγωνικό σώμα αριθμών, έτσι ώστε να μην υπάρχει ανάγκη να ξεχωρίζουμε δύο περιπτώσεις.

Πρόταση 10.4.5. *Έστω K τετραγωνικό σώμα αριθμών διακρίνουσας D. Τότε $K = \mathbb{Q}(\sqrt{D})$ και $R_K = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$*

Απόδειξη. Αν $K = \mathbb{Q}(\sqrt{m})$, τότε $D \in \{m, 4m\}$. Επομένως $K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{D})$. Υπολογίζουμε ότι

$$\frac{D + \sqrt{D}}{2} = \begin{cases} \frac{4m+\sqrt{4m}}{2} = 2m + \sqrt{m}, & \text{αν } m \equiv 2, 3 \bmod 4 \\ \frac{m+\sqrt{m}}{2} = \frac{m-1}{2} + \frac{1+\sqrt{m}}{2}, & \text{αν } m \equiv 1 \bmod 4 \end{cases}$$

το οποίο modulo $\mathbb{Z}$ είναι ισοδύναμο με $\sqrt{m}$ και $\frac{1+\sqrt{m}}{2}$, αντίστοιχα. □

Θεώρημα 10.4.6. *Έστω K πραγματικό τετραγωνικό σώμα αριθμών διακρίνουσας D και $R_K = \mathbb{Z}[\omega]$, με $\omega = \frac{D+\sqrt{D}}{2}$, η περιοχή των ακέραιων αλγεβρικών αριθμών αυτού.*

Έστω ακόμη $\vartheta := \frac{1}{\omega - [\omega]}$. Ο αριθμός ϑ είναι ανάγωγος (reduced) και συνεπώς απλά περιοδικός.

Υποθέτουμε ότι $\vartheta = \overline{[a_0, a_1, \ldots, a_{r-1}]}$ με την ελάχιστη περίοδο.

Ο αριθμός $\varepsilon_0 := q_{r-1}\vartheta + q_{r-2}$ είναι η θεμελιώδης μονάδα του R_K. Τα q_k είναι οι αριθμοί που ορίστηκαν στα συνεχή κλάσματα.

Απόδειξη. Η απόδειξη είναι μακροσκελής και ως εκ τούτου παραλείπεται. Τον ενδιαφερόμενο αναγνώστη παραπέμπουμε στο [2]. □

10.5 Νόμος Ανάλυσης στα τετραγωνικά σώματα αριθμών

10.5.1 Περιοχές μονοσήμαντης ανάλυσης

Έστω τώρα $K = \mathbb{Q}(\sqrt{m})$, και R_K δακτύλιος μονοσήμαντης ανάλυσης. Ας ρίξουμε μια ματιά στα ανάγωγα στοιχεία (πρώτα), χωρίς φυσικά να κάνουμε διάκριση μεταξύ συνεταιρικών, δηλαδή στοιχεία που διαφέρουν κατά μονάδα.

Αν π, λοιπόν, ανάγωγο στοιχείο του K, τότε υπάρχει τουλάχιστο ένας φυσικός αριθμός n, η νόρμα του π, $N(\pi) = \pi\pi'$, ο οποίος διαιρείται με π, δηλαδή υπάρχει (ρητός) πρώτος p ώστε $\pi \mid p$. Προφανώς ο p είναι ο μοναδικός πρώτος που διαιρείται με π.

Ορισμός 10.5.1. Αν $\pi \mid p$ λέμε ότι ο p είναι ρητός πρώτος που ανήκει στο π ή αλλιώς ο π είναι ένας πρώτος διαιρέτης του p στο σώμα K.

Η σχέση $\pi \mid p$ δίνει $N(\pi) \mid p^2$, επομένως $N(\pi) \cong p$ ή p^2.

Αν $N(\pi) \cong p$, τότε $p \cong \pi\pi'$, με π' πρώτο στοιχείο του K. Ξεχωρίζουμε δύο περιπτώσεις. Την $\pi \ncong \pi'$ και $\pi \cong \pi'$.

Αν πάλι $N(\pi) \cong p^2$, τότε $p^2 = \pi\pi'$ και λόγω του μονοσημάντου της ανάλυσης $p \cong \pi \cong \pi'$.

Όταν λοιπόν το p διατρέχει όλους τους ρητούς πρώτους τότε οι πρώτοι π, π' (εξαιρούμε ένα από τους δύο αν $\pi \cong \pi'$) διατρέχουν ένα σύστημα πρώτων του K.

Εντελώς φυσιολογικά τώρα τίθεται το ερώτημα της εύρεσης ενός κανόνα που να μας δίνει ποια από τις τρεις περιπτώσεις

$$\begin{aligned} p &\cong \pi\pi', && \text{με} && N(\pi) = N(\pi') \cong p \\ p &\cong \pi^2, && \text{με} && N(\pi) = N(\pi') \cong p \\ p &\cong \pi, && \text{με} && N(\pi) = N(\pi') = p^2, \end{aligned}$$

ισχύει. Ένας τέτοιος κανόνας λέγεται *νόμος ανάλυσεως* για το $K = \mathbb{Q}(\sqrt{m})$ και η εύρεσή του είναι ένα από τα πιο βασικά και σπουδαία προβλήματα της θεωρίας των τετραγωνικών σωμάτων αριθμών.

Προτού διατυπώσουμε τον νόμο αναλύσεως, παρατηρούμε ότι κάθε ακέραιος αλγεβρικός αριθμός του K γράφεται στη μορφή

$$\alpha = \frac{a + b\sqrt{D}}{2},$$

με $a, b \in \mathbb{Z}$ και

$$a \equiv Db \bmod 2,$$

όπου D είναι η διακρίνουσα του σώματος.

Επιπλέον χρειαζόμαστε μια γενίκευση του συμβόλου του Legendre.

Ορισμός 10.5.2. Αν D είναι διακρίνουσα τετραγωνικού σώματος αριθμών, τότε το σύμβολο του Kronecker $\left(\frac{D}{p}\right)$, για κάθε πρώτο αριθμό p, ορίζεται ως:

- Αν $p \neq 2$ και $p \nmid D$, τότε το $\left(\frac{D}{p}\right)$ ταυτίζεται με το σύμβολο του Legendre.
- Αν $p \mid D$ τότε $\left(\frac{D}{p}\right) = 0$.
- Αν $D \equiv 1 \bmod 4$, τότε $\left(\frac{D}{2}\right) = \left(\frac{2}{D}\right)$ = σύμβολο του Jacobi δηλαδή

$$\left(\frac{D}{2}\right) = \begin{cases} 1 & \text{αν } D \equiv 1 \bmod 8 \\ -1 & \text{αν } D \equiv 5 \bmod 8 \end{cases}$$

Θεώρημα 10.5.3 (Νόμος ανάλυσης στο K)**.** *Έστω $K = \mathbb{Q}(\sqrt{m})$, τετραγωνικό σώμα αριθμών με R_K δακτύλιος μονοσήμαντης ανάλυσης. Οι τρεις περιπτώσεις*

$$p \cong \pi\pi', \qquad p \cong \pi^2, \qquad p \cong \pi$$

αντιστοιχούν στις τιμές του συμβόλου του Kronecker

$$\left(\frac{D}{p}\right) = 1, \qquad \left(\frac{D}{p}\right) = 0, \qquad \left(\frac{D}{p}\right) = -1.$$

Απόδειξη. Αρκεί να δείξουμε ότι

1. $p \cong \pi^2$ αν και μόνο αν $\left(\frac{D}{p}\right) = 0$ και
2. $p \cong \pi\pi'$ αν και μόνο αν $\left(\frac{D}{p}\right) = 1$

Για το 1. Θα αποδείξουμε ότι αν $\left(\frac{D}{p}\right) = 0$, τότε $p \cong \pi^2$. Έστω $p \mid D$. Υποθέτουμε καταρχάς ότι $p \cong \pi$, δηλαδή ότι ο p παραμένει στο K και πάλι πρώτος. Σε όλες τις άλλες περιπτώσεις, εκτός της $p = 2$ και $m \equiv 3 \bmod 4$, έχουμε $p \mid \sqrt{m}$ και καταλήγουμε στο ότι $p^2 \mid m$, άτοπο, αφού ο m είναι ελεύθερος τετραγώνου.

Αν $p = 2$ και $m \equiv 3 \bmod 4$ τότε

$$2 \mid 1 - m = (1 - \sqrt{m})(1 + \sqrt{m}),$$

συνεπώς $2 \mid (1 - \sqrt{m})$ ή $2 \mid (1 + \sqrt{m})$. Άρα $4 \mid (1 - m)$ και $m \equiv 1 \bmod 4$, άτοπο.

Επομένως $p \cong \pi\pi'$ και αρκεί να δείξουμε ότι $\pi \cong \pi'$. Γράφουμε το

$$\pi = \frac{a + b\sqrt{D}}{2}, a, b \in \mathbb{Z}, a \equiv bD \bmod 2$$

και

$$\pi' = \frac{a - b\sqrt{D}}{2}, a, b \in \mathbb{Z}, a \equiv bD \bmod 2,$$

άρα

$$\pi - \pi' = b\sqrt{D}.$$

Τώρα $\pi \mid p \mid D = \sqrt{D}\sqrt{D}$, συνεπώς $\pi \mid \sqrt{D}$ και έχουμε $\pi \mid (\pi - \pi')$, άρα $\pi \mid \pi'$ και καταλήγουμε στο $\pi \cong \pi'$, δηλαδή $p \cong \pi^2$.

Αντιστρόφως έστω ότι $p \cong \pi^2$ άρα $\pi' \cong \pi$, συνεπώς $\pi \mid \pi'$ και $\pi \mid (\pi - \pi')$ οπότε $\pi \mid (\pi - \pi') \mid b\sqrt{D}$ και τελικά $p \mid b^2 D$.

Θα δείξουμε ότι $p \nmid b$. Αν $p \neq 2$ και $p \mid b$ τότε αφού

$$p \cong \frac{a^2 - b^2 D}{4} \Rightarrow p \mid a \Rightarrow p^2 \mid \frac{a^2 - b^2 D}{4} \cong p,$$

άτοπο.

Αν πάλι $p = 2$ και $p \mid b$ τότε η

$$2 \cong \frac{a^2 - Db^2}{4}$$

δίνει για $D \equiv 0 \mathrm{mod} 4$

$$2 \equiv \left(\frac{a}{2}\right)^2 \mathrm{mod} 4$$

το οποίο είναι άτοπο, ενώ για $D \equiv 1 \mathrm{mod} 4$ δίνει

$$2 \cong \left(\frac{a}{2}\right)^2 - \left(\frac{b}{2}\right)^2 \mathrm{mod} 4$$

το οποίο είναι και πάλι άτοπο. Δηλαδή $p \nmid b$ άρα $p \mid D$ το οποίο εξ ορισμού δίνει $\left(\frac{D}{p}\right) = 0$.

Θα αποδείξουμε τώρα το 2.

Έστω $\left(\frac{D}{p}\right) = 1$. Αν $p \neq 2$, τότε η ισοδυναμία

$$x^2 \equiv D \mathrm{mod} p,$$

έχει λύση. Για έναν πρώτο διαιρέτη $\pi \mid p$ στο K, ισχύει

$$(x - \sqrt{D})(x + \sqrt{D}) \equiv 0 \mathrm{mod} \pi$$

και, χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι

$$x - \sqrt{D} \equiv 0 \mathrm{mod} \pi.$$

Η τελευταία όμως ισοδυναμία δεν ισχύει για το p διότι

$$\frac{x - \sqrt{D}}{p} \notin R_K,$$

οπότε $p \ncong \pi$, δηλαδή $p \cong \pi\pi'$. Αν ήταν $\pi \cong \pi'$, τότε λόγω του 1. θα είχαμε $p \mid D$, το οποίο είναι άτοπο.

Αν τώρα $p = 2$, τότε $\left(\frac{D}{p}\right) = 1$ δίνει εξ ορισμού $D \equiv 1 \mathrm{mod} 8$, συνεπώς

$$\left(1 - \frac{1 + \sqrt{D}}{2}\right)\left(1 - \frac{1 - \sqrt{D}}{2}\right) = \frac{1 - D}{4} \equiv 0 \mathrm{mod} 2,$$

οπότε, για κάποιον πρώτο διαιρέτη π του 2 στο K, θα έχουμε

$$1 - \frac{1 + \sqrt{D}}{2} \equiv 0 \mathrm{mod} \pi,$$

ενώ, όπως παραπάνω, $2 \nmid \left(1 - \frac{1+\sqrt{D}}{2}\right)$ στο K , δηλαδή $2 \cong \pi\pi'$ με $\pi \ncong \pi'$.

Αντιστρόφως, έστω $p \cong \pi\pi'$ με $\pi \ncong \pi'$,

$$\pi = \frac{a + b\sqrt{D}}{2} \qquad \pi' = \frac{a - b\sqrt{D}}{2}.$$

Στην απόδειξη του 1. δείξαμε ότι $p \nmid b$.

$$p \cong \frac{a^2 - Db^2}{4} \Rightarrow \frac{a^2 - Db^2}{4} \equiv 0 \mathrm{mod} p \text{ στο } K,$$

οπότε για $p \neq 2$ έχουμε

$$a^2 \equiv Db^2 \mathrm{mod} p \Rightarrow \left(\frac{Db^2}{p}\right) = \left(\frac{D}{p}\right) = 1,$$

αφού $p \nmid b$. Τέλος για $p = 2$

$$a^2 \equiv Db^2 \mathrm{mod} 8 \Rightarrow D \equiv 1 \mathrm{mod} 8 \Rightarrow \left(\frac{D}{2}\right) = 1.$$

□

Παρατήρηση 10.5.4. Αφού λόγω της υποθέσεως ότι ο R_K είναι περιοχή μονοσήμαντης ανάλυσης το κύριο ιδεώδες που παράγεται από τον πρώτο αριθμό π, $(\pi) = \pi R_K$, είναι πρώτο ιδεώδες θα μπορούσαμε να γράψουμε το θεώρημα 10.5.3 και για πρώτα ιδεώδη. Το παραπάνω θεώρημα ισχύει για κάθε δακτύλιο R_Kακόμη και αν δεν είναι περιοχή μονοσήμαντης ανάλυσης.

10.6 Ιδεώδη και αριθμός κλάσεων

Ορισμός 10.6.1. Ένα υποσύνολο A του K λέγεται ιδεώδες του K αν και μόνο αν ισχύουν τα παρακάτω:

1. Για κάθε $a_1, a_2 \in A$ η διαφορά $a_1 - a_2 \in A$
2. Για κάθε $\lambda \in R_K$ και για κάθε $a \in A$ το $\lambda a \in A$
3. $A \neq (0)$
4. Υπάρχει $R_K \ni \delta \neq 0$, ώστε $\delta A \subseteq R_K$.

Αν $A \subseteq R_K$ λέγεται ακέραιο ιδεώδες, αλλιώς λέγεται κλασματικό.

Σημαντική παρατήρηση: Έχουμε ήδη διαπιστώσει ότι ο δακτύλιος των ακέραιων αλγεβρικών αριθμών R_K, ενός αλγεβρικού σώματος αριθμών K δεν είναι, εν γένει, περιοχή μονοσήμαντης ανάλυσης. Ισχύει όμως το

Θεώρημα 10.6.2. *Αν K αλγεβρικό σώμα αριθμών και R_K η περιοχή των ακέραιων αλγεβρικών αριθμών αυτού, τότε κάθε ακέραιο ιδεώδες A του K αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών, δηλαδή*

$$A = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_s^{\alpha_s},$$

με P_i πρώτα ιδεώδη του R_K και $\alpha_i \in \mathbb{N}$ για $i = 1, 2, \ldots, s$.

Αυτό είναι άμεση συνέπεια της ιδιότητας της περιοχής R_K να είναι περιοχή του Dedekind. Η απόδειξη του θεωρήματος αυτού ξεφεύγει από τον σκοπό του παρόντος συγγράμματος.

Μπορούμε λοιπόν να ρωτήσουμε το εξής: Αν $p\mathbb{Z}$ είναι ένα κύριο πρώτο ιδεώδες του $\mathbb{Z}$ και θεωρήσουμε το κύριο ιδεώδες pR_K του δακτυλίου R_K, τότε αυτό είναι κατάνάγκη πρώτο; Ο νόμος ανάλυσης σε τετραγωνικά σώματα αριθμών απαντά ακριβώς αυτό το ερώτημα:

Θεώρημα 10.6.3 (Νόμος ανάλυσης, στα τετραγωνικά σώματα αριθμών, γενική περίπτωση)**.** *Το ιδεώδες pR_K στον δακτύλιο ακέραιων του τετραγωνικού σώματος αριθμών $\mathbb{Q}(\sqrt{m})$ γράφεται ως γινόμενο πρώτων ιδεωδών του R_K ως εξής:*

$$\begin{aligned} pR_K &= Q^2, N(Q) = p && \text{αν} \quad \left(\tfrac{D_K}{p}\right) = 0 \\ pR_K &= Q, N(Q) = p^2 && \text{αν} \quad \left(\tfrac{D_K}{p}\right) = -1 \\ pR_K &= Q_1 Q_2, N(Q_1) = N(Q_2) = p && \text{αν} \quad \left(\tfrac{D_K}{p}\right) = 1 \end{aligned}$$

Απόδειξη. Η απόδειξη απαιτεί αρκετά στοιχεία αλγεβρικής θεωρίας αριθμών. Η ιδέα είναι ότι γενικά ($p \neq 2$) η ανάλυση σε πρώτα ιδεώδη καταλήγει στην ανάλυση σε ανάγωγους παράγοντες του $X^2 - m$ η οποία ελέγχεται από το σύμβολο του Legendre. Η περίπτωση $p = 2$ απαιτεί λίγο περισσότερη προσοχή. Για μια απόδειξη παραπέμπουμε στις σημείωσεις Αλγεβρικής Θεωρίας Αριθμών του πρώτου συγγραφέα [3]. □

10.6.1 Αριθμός Κλάσεων Ιδεωδών

Στο σύνολο όλων των ιδεωδών (κλασματικών και ακέραιων) ορίζουμε ισοδυναμία ιδεωδών:

$$A \sim B \text{ αν και μόνο αν υπάρχει } K \ni \xi \neq 0, A = (\xi) \cdot B$$

και ισοδυναμία ιδεωδών με στενή έννοια:

$$A \sim_\sigma B \text{ αν και μόνο αν υπάρχει } K \ni \xi, N(\xi) > 0, A = (\xi) \cdot B$$

Ορισμός 10.6.4. Ο αριθμός κλάσεων $h(D)$ (αντίστοιχα ο αριθμός κλάσεων με τη στενή έννοια $h_\sigma(D)$) ορίζεται να είναι το πλήθος των κλάσεων σε κάθε μια από τις παραπάνω κλάσεις ισοδυναμίας.

Χωρίς απόδειξη αναφέρουμε το

Θεώρημα 10.6.5. *Για κάθε αλγεβρικό σώμα αριθμών K το σύνολο κλάσεων ιδεωδών του K αποτελεί πεπερασμένη ομάδα.*

Το σύνολο όλων των ιδεωδών (ακέραιων και κλασματικών) I_K ενός αλγεβρικού σώματος αριθμών K αποτελεί αβελιανή ομάδα. Το σύνολο των κύριων ιδεωδών αυτού αποτελεί αβελιανή υποομάδα της I_Kτ την οποία συμβολίζουμε με H_K. Το σύνολο των κλάσεων ισοδυναμίας είναι η ομάδα πηλίκο

$$\mathcal{R}_K = \frac{I_K}{H_K},$$

και λέγεται ομάδα κλάσεων ιδεωδών.

Ανάλογες ιδιότητες ισχύουν και για την ομάδα κλάσεων ιδεωδών με τη στενή έννοια.

Ένα σημαντικότατο πρόβλημα της Αλγεβρικής Θεωρίας Αριθμών είναι, δοθέντος σώματος K, ο προσδιορισμός του αριθμού κλάσεων ιδεωδών αυτού.

Στην περίπτωση που το K είναι μιγαδικό τετραγωνικό σώμα αριθμών, διακρίνουσας D, αυτό είναι εύκολο, αφού οι κλάσεις ιδεωδών του K αντιστοιχούν αμφιμονοσήμαντα στις κλάσεις ισοδυναμίας (θετικά ορισμένων) τετραγωνικών μορφών διακρίνουσας D, σύμφωνα με το ακόλουθο:

Θεώρημα 10.6.6. *Έστω $K = \mathbb{Q}(\sqrt{m})$ μιγαδικό τετραγωνικό σώμα αριθμών διακρίνουσας D. Υπάρχει μια αμφιμονοσήμαντη αντιστοιχία ανάμεσα στις κλάσεις ισοδυναμίας (θετικά ορισμένων) τετραγωνικών μορφών διακρίνουσας D και στις κλάσεις ισοδυναμίας με στενή έννοια ιδεωδών του K.*

Η αντιστοιχία αυτή δίνεται ως εξής: Στο ιδεώδες $A = \mathbb{Z}\alpha + \mathbb{Z}\beta$ με $\frac{\alpha'\beta - \alpha\beta'}{\sqrt{D}} > 0$ αντιστοιχεί η τετραγωνική μορφή

$$f(X, Y) = aX^2 + bXY + cY^2,$$

όπου

$$a = \frac{\alpha\alpha'}{N(A)}, \qquad b = \frac{\alpha\beta' + \alpha'\beta}{N(A)}, \qquad c = \frac{\beta\beta'}{N(A)}.$$

Αντιστρόφως στην τετραγωνική μορφή

$$f(X, Y) = ax^2 + bXY + cY^2,$$

αντιστοιχεί το κλασματικό ιδεώδες

$$\mathbb{Z}\lambda + \mathbb{Z}\frac{b + \sqrt{D}}{2a}\lambda,$$

όπου $\lambda \in K$ και διαλέχτηκε ώστε $N(\lambda)a > 0$.

Απόδειξη. Δείτε στο [1]. □

Παρατήρηση 10.6.7. Αξίζει να σημειωθεί ότι για μιγαδικά τετραγωνικά σώματα αριθμών οι έννοιες ισοδυναμία ιδεωδών και ισοδυναμία ιδεωδών με τη στενή έννοια συμπίπτουν, αφού κάθε στοιχείο του σώματος K έχει θετική νόρμα.

Δεδομένου λοιπόν ότι η τάξη h της αβελιανής ομάδας $\mathcal{R}_K = I_K/H_K$ των κλάσεων ιδεωδών του K είναι πεπερασμένη, έπεται ότι αν A ιδεώδες του R_K τότε το A^h είναι κύριο ιδεώδες.

Πρόταση 10.6.8. *Αν τώρα A^μ κύριο ιδεώδες του K και $(\mu, h_K) = 1$, τότε A είναι κύριο ιδεώδες του K*

Απόδειξη. Γράφουμε $1 = x\mu + yh$, για κατάλληλα $x, y \in \mathbb{Z}$. Στη συνέχεια υπολογίζουμε ότι:

$$A = A^{x\mu + yh} = (A^\mu)^x (A^h)^y \in H_K.$$

□

10.7 Εφαρμογή στις Διοφαντικές Εξισώσεις

Επιστρέφουμε στη διοφαντική εξίσωση:

$$2Y^2 = X^2 + 5, \tag{10.7.1}$$

που λύσαμε με λανθασμένο τρόπο προηγουμένως.

Ισχυριζόμαστε ότι $(x, y) = (\pm 7, 3)$ είναι οι μοναδικές λύσεις της (10.7.1). Καταρχήν χρειαζόμαστε από τον νόμο ανάλυσης στο $K = \mathbb{Q}(\sqrt{-5}), R_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ ότι

$$2R_K = P_2^2 \text{ όπου } P_2 = (2, 1 + \sqrt{-5})$$

$$5R_K = P_3^2 \text{ όπου } P_3 = (\sqrt{-5})$$

και ότι $h_{\mathbb{Q}(\sqrt{-5})} = 2$. Έστω $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση της (10.7.1), δηλαδή

$$2y_0^3 = (x_0 + \sqrt{-5})(x_0 - \sqrt{-5}).$$

Περνάμε στα ιδεώδη

$$(2)(y_0)^2 = ((x_0 + \sqrt{-5}))((x_0 - \sqrt{-5}))$$

Ισχυριζόμαστε ότι ο

$$((x_0 + \sqrt{-5}), (x_0 - \sqrt{-5})) = (x_0 + \sqrt{-5})R + (x_0 - \sqrt{-5})R = P_2.$$

Συνεπώς

$$P_2^2(y_0)^3 = (P_2A)(P_2\bar{A}),$$

όπου

$$(A, \bar{A}) = A + \bar{A} = R_K$$

πρώτα μεταξύ τους και καταλήγουμε στο $(y_0)^3 = A\bar{A}$. Λόγω μονοσήμαντης ανάλυσης στα πρώτα ιδεώδη υπάρχει ακέραιο ιδεώδες A του R_K, με $A = B^3$. Τότε $\bar{A} = \bar{B}^3$,

$$(2)(x_0 + \sqrt{-5}) = P_2^2P_2A = (P_2B)^3,$$

δηλαδή το P_2B είναι κύριο ίσο με λR_K, $\lambda \in \mathbb{Z}[\sqrt{-5}]$. Έτσι

$$(2)(x_0 + \sqrt{-5}) = (\lambda)^3$$

δηλαδή

$$2(x_0 + \sqrt{-5}) = \varepsilon\lambda^3,$$

$$\varepsilon \in E(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}.$$

Η μονάδα μπορεί να ενσωματωθεί στο $\lambda' = a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$. Άρα καταλήγουμε στη σχέση

$$2(x_0 + \sqrt{-5}) = a(a^2 - 15b^2) + b(3a^2 - 5b^2)\sqrt{-5},$$

από όπου έχουμε

$$2x_0 = a(a^2 - 15b^2) \qquad 2 = b(3a^2 - 5b^2) \Rightarrow b \mid 2 \Rightarrow \pm 1, \pm 2.$$

Η λυση $b = -1$ δίνει τον ακέραιο $a = \pm 1$, η οποία οδηγεί στο $x_0 = \pm 7$, $y_0 = 3$. Δηλαδή

$$(x_0, y_0) = (\pm 7, 3)$$

είναι η μοναδική λύση.

Βιβλιογραφία

[1] Don Zagier: *Zetafunktionen Und Quadratische Körper, eine Einführung in die höhere Zahlentheorie*. Springer-Verlag, Berlin, 1981.

[2] Stefan Müller-Stach, Jens Piontkowski: *Elementare und algebraische Zahlentheorie*. Vieweg, 2006.

[3] Αντωνιάδης, Γιάννης Α.: *Αλγεβρική Θεωρία Αριθμών*. Σημειώσεις, Ηράκλειο, 1986.

[4] Λάκκης, Κ.: *Θεωρία Αριθμών*. Εκδόσεις Ζήτη, 1990.

Παράρτημα Α

11.1 Εισαγωγή

Όπως έχει αναφερθεί ήδη προοδευτικά στο δεύτερο μέρος του παρόντος συγγράμματος χρησιμοποιούνται βασικές έννοιες άλγεβρας. Θεωρούμε ότι οι έννοιες αυτές είναι ήδη γνωστές από τη διδασκαλία ενός βασικού εισαγωγικού μαθήματος άλγεβρας. Προκειμένου όμως να στηρίξουμε, κατά κάποιο τρόπο, την αυτοτέλεια του κειμένου θα αναφερθούμε εν συντομία στις έννοιες αυτές καθώς και στις βασικές τους ιδιότητες. Ο αναγνώστης που επιθυμεί να αναζητήσει περισσότερες πληροφορίες μπορεί να ανατρέξει σε γενικά βιβλία Άλγεβρας όπως τα [5], [4], [3], [2], [1].

11.2 Ομάδες

Ορισμός 11.2.1. Ένα μη-κενό σύνολο G εφοδιασμένο με μια διμελή πράξη

$$\circ \left\{ \begin{array}{c} G \times G \to G \\ (x, y) \mapsto x \circ y \end{array} \right\}$$

λέγεται ομάδα όταν επαληθεύει τα ακόλουθα αξιώματα:

G1 Για όλα τα στοιχεία x, y, z του συνόλου G ισχύει (αξίωμα προσεταιριστικότητας):

$$(x \circ y) \circ z = x \circ (y \circ z).$$

G2 Υπάρχει ένα στοιχείο $e \in G$ τέτοιο ώστε για όλα τα στοιχεία $g \in G$ να ισχύει (αξίωμα ύπαρξης μοναδιαίου):

$$e \circ g = g \circ e = g.$$

G3 Αν $g \in G$ τότε υπάρχει ένα στοιχείο $g^* \in G$ τέτοιο ώστε να ισχύει (αξίωμα ύπαρξης αντιστρόφου):

$$g \circ g^* = e = g^* \circ g$$

Παρατήρηση 11.2.2. Εύκολα αποδεικνύεται ότι σε μια ομάδα $(G, \circ)$, το μοναδιαίο στοιχείο είναι μοναδικό καθώς και ότι για κάθε $g \in G$ υπάρχει ακριβώς ένα αντίστροφο αυτού g^*. Στη συνέχεια αντί του συμβολισμού g^* θα χρησιμοποιούμε τον συμβολισμό g^{-1}.

Ορισμός 11.2.3. Η ομάδα $(G, \circ)$ λέγεται αβελιανή ομάδα όταν για όλα τα στοιχεία x, y της G ισχύει

$$x \circ y = y \circ x.$$

Ορισμός 11.2.4. Μια ομάδα $(G, \circ)$ λέγεται *πεπερασμένη ομάδα* όταν το σύνολο G είναι ένα πεπερασμένο σύνολο. Αν το σύνολο G είναι απειροσύνολο, τότε η ομάδα $(G, \circ)$ λέγεται άπειρη ομάδα .

Παραδείγματα ομάδων

1. Το σύνολο των ακέραιων αριθμών $\mathbb{Z}$ με πράξη τη (συνήθη) πρόσθεση αποτελεί *άπειρη αβελιανή ομάδα*. Το ίδιο ισχύει και για τα σύνολα $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

2. Το σύνολο των κλάσεων υπολοίπων modulo n, $n \in \mathbb{N}$, $n > 1$:

   $$\mathbb{Z}_n = \{\bar{a} := a \mathrm{mod} n | a \in \mathbb{Z}\}$$

   με (καλά ορισμένη) πράξη την πρόσθεση κλάσεων

   $$\oplus \left\{ \begin{array}{c} \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \\ (\bar{a}, \bar{b}) \mapsto \bar{a} \oplus \bar{b} \end{array} \right\}$$

   αποτελεί *πεπερασμένη, αβελιανή, ομάδα*.

3. Το σύνολο $M_n(\mathbb{R})$ των τετραγωνικών $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξη την πρόσθεση πινάκων αποτελεί άπειρη *αβελιανή ομάδα*.

4. Έστω $\omega := e^{\frac{2\pi i}{n}}$. Το σύνολο

   $$\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$$

   με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών, αποτελεί πεπερασμένη αβελιανή ομάδα. Η ομάδα αυτή λέγεται ομάδα των n-ριζών της μονάδας.

5. Το σύνολο των πρώτων κλάσεων υπολοίπων mod$n$, $n \in \mathbb{N}$, $n > 1$

   $$\mathbb{Z}_n^* = \{\bar{a} := a \mathrm{mod} n | a \in \mathbb{Z}, (a, n) = 1\}$$

   με πράξη τον (καλά ορισμένο) πολλαπλασιασμό κλάσεων

   $$\odot \left\{ \begin{array}{c} \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^* \\ (\bar{a}, \bar{b}) \mapsto \bar{a} \odot \bar{b} \end{array} \right\}$$

   αποτελεί *πεπερασμένη, αβελιανή ομάδα*.

6. Τα σύνολα $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ των μη-μηδενικών στοιχείων των $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ με πράξη τον συνήθη πολλαπλασιασμό αποτελούν *άπειρη, αβελιανή* ομάδα.

7. Το σύνολο $M_n(\mathbb{R})$ των $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξη τον πολλαπλασισμό πινάκων *δεν* αποτελεί ομάδα, αφού υπάρχουν $n \times n$ πίνακες με στοιχεία πραγματικούς οι οποίοι δεν έχουν αντίστροφο. Αν θεωρήσουμε το υποσύνολο του $M_n(\mathbb{R})$

   $$\mathrm{GL}_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) | \det(A) \neq 0\},$$

   τότε αυτό με πράξη τον πολλαπλασιασμό πινάκων αποτελεί *άπειρη ομάδα*. Η ομάδα αυτή, αν $n > 1$, *δεν* είναι αβελιανή επειδή δεν ισχύει εν γένει $A \cdot B = B \cdot A$.

11.2.1 Υποομάδες και παραδείγματα

Ορισμός 11.2.5. Αν $(G, \circ)$ ομάδα και H ένα μη κενό υποσύνολο της G, τότε το H λέγεται *υποομάδα* της G, όταν το $(H, \circ)$, εφοδιασμένο με την επαγόμενη πράξη από το G, είναι ομάδα.

Συμβολίζουμε το ότι H υποομάδα της G με $H \leq G$.

Ισχύει η ακόλουθη

Πρόταση 11.2.6. *Αν H είναι ένα υποσύνολο της ομάδας $(G, \circ)$, τότε οι ακόλουθες προτάσεις είναι μεταξύ τους ισοδύναμες:*

1. *H $(H, \circ)$ είναι υποομάδα της $(G, \circ)$.*
2. *Το υποσύνολο $H \subseteq G$ πληροί τις ακόλουθες συνθήκες:*
   - *(α΄) Το μοναδιαίο e της G ανήκει στο σύνολο H.*
   - *(β΄) Αν $x, y \in H$, τότε και $x \circ y \in H$.*
   - *(γ΄) Αν $x \in H$, τότε και $x^{-1} \in H$*
3. *Το σύνολο H πληροί τις ακόλουθες συνθήκες:*
   - *(α΄) Το μοναδιαίο e της G ανήκει στο σύνολο H*
   - *(β΄) Αν $a, b \in H$, τότε και $ab^{-1} \in H$.*

Παραδείγματα υποομάδων:

1. Προφανώς $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ καθώς και $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.
2. Το σύνολο
$$\mathrm{SL}_n(\mathbb{R}) := \{A \in \mathrm{GL}_n(\mathbb{R}) | \det(A) = 1\}$$
είναι υποομάδα της $\mathrm{GL}_n(\mathbb{R})$.

11.2.2 Κυκλικές ομάδες

Ορισμός 11.2.7. Μια ομάδα $(G, \circ)$ λέγεται *κυκλική ομάδα* όταν υπάρχει κάποιο στοιχείο αυτής $x \in G$, τέτοιο ώστε όλα τα στοιχεία της G να γράφονται ως δυνάμεις του x.

Κάθε τέτοιο στοιχείο σε μια κυκλική ομάδα λέγεται *γεννήτορας* αυτής.

Σημείωση: Αν $g \in G$ και $n \in \mathbb{Z}$, τότε η δύναμη g^n ορίζεται ως εξής:

$$g^n = \begin{cases} \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ φορές}} & \text{όταν } n \geq 1 \\ e & \text{όταν } n = 0 \\ \underbrace{g^{-1} \circ g^{-n} \circ \cdots \circ g^{-1}}_{-n \text{ φορές}} & \text{όταν } n < 0 \end{cases}$$

Συμβολισμός Αν G είναι κυκλική με γεννήτορα g, τότε γράφουμε $G = \langle g \rangle$.

Παραδείγματα: Οι ομάδες των παραδειγμάτων 4 και 5 είναι κυκλικές.

Ορισμός 11.2.8. Το πλήθος των στοιχείων μιας πεπερασμένης ομάδας, λέγεται *τάξη αυτής*.

Πρόταση 11.2.9. *Αν η ομάδα G είναι πεπερασμένη και κυκλική τάξης n, $G = \langle g \rangle$, τότε οι γεννήτορες αυτής είναι τα στοιχεία της μορφής g^d με $(d, n) = 1$.*

11.2.3 Το θεώρημα του Lagrange

Υποθέτουμε ότι $(G, \circ)$ είναι μια ομάδα και $H \leq G$ είναι μια υποομάδα αυτής. Στο σύνολο $G \times G$ ορίζουμε τη σχέση: $a, b \in G$,

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Η σχέση αυτή είναι μια σχέση ισοδυναμίας. Η κλάση ισοδυναμίας του στοιχείου a είναι το σύνολο $aH := \{ah | h \in H\}$.

Ορισμός 11.2.10. Το πλήθος των κλάσεων ισοδυναμίας της H στην G, λέγεται *δείκτης* της H στην G και συμβολίζεται με $[G : H]$. Η τάξη μιας ομάδας $(G, \circ)$ συμβολίζεται με $|G|$.

Το παρακάτω είναι γνωστό ως θεώρημα του Lagrange .

Θεώρημα 11.2.11 (Lagrange)**.** *Υποθέτουμε ότι η G είναι μια πεπερασμένη ομάδα και $H \leq G$. Ισχύει $|G| = [G : H] \cdot |H|$. Επομένως, η τάξη μιας υποομάδας μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας.*

11.2.4 Ομάδα πηλίκου

Έστω G μια ομάδα και $H \leq G$ μια υποομάδα αυτής. Στο σύνολο των κλάσεων ισοδυναμίας που ορίσαμε παραπάνω, έχουμε τις κλάσεις $\{aH | a \in G\}$. Θα θέλαμε να ορίσουμε ένα πολλαπλασιασμό στο σύνολο κλάσεων ώστε να αποκτήσει δομή ομάδας, την οποία ονομάζουμε ομάδα πηλίκου. Αυτό όμως δεν είναι πάντοτε δυνατό.

Ορισμός 11.2.12. Έστω G μια ομάδα και $H \leq G$. Η H λέγεται *κανονική υποομάδα* της G όταν ισχύει $aH = Ha$ για κάθε $a \in G$, όπου $Ha = \{ha | h \in H\}$.

Αν τώρα G είναι ομάδα και H *κανονική υποομάδα* της G, τότε το σύνολο

$$G/H := \{aH | a \in G\}$$

με πράξη τον (καλά ορισμένο) πολλαπλασιασμό

$$(aH)(bH) = ab(H),$$

αποτελεί ομάδα.

Άμεση συνέπεια του θεωρήματος του Lagrange είναι ότι η τάξη της ομάδας G/H είναι ίση με $|G|/|H|$.

Αν τώρα G είναι αβελιανή, τότε κάθε υποομάδα αυτής H είναι κανονική και συνεπώς πάντοτε ορίζεται η ομάδα πηλίκου G/H.

11.3 Δακτύλιοι

11.3.1 Ορισμοί και παραδείγματα

Ορισμός 11.3.1. Ένα μη-κενό σύνολο R εφοδιασμένο με δύο (διμελής) πράξεις, πρόσθεσης

$$+ \left\{ \begin{array}{c} R \times R \to R \\ (a, b) \mapsto a + b \end{array} \right\}$$

και πολλαπλασίασμου

$$\cdot \left\{ \begin{array}{c} R \times R \to R \\ (a, b) \mapsto a \cdot b \end{array} \right\}$$

λέγεται δακτύλιος, όταν επαληθεύει τα ακόλουθα αξιώματα:

R1 Ο $(R, +)$ αποτελεί αβελιανή ομάδα.

R2 Για όλα τα στοιχεία $x, y, z \in R$ ισχύει (αξίωμα προσεταιριστικότητας)

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

R3 Για όλα τα στοιχεία $x, y, z \in R$ ισχύουν (αξιώματα επιμεριστικότητας)

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z \\ (x + y) \cdot z &= x \cdot z + y \cdot z. \end{aligned}$$

Αν επιπλέον ισχύει το αξίωμα ύπαρξης μοναδιαίου

R4 Υπάρχει ένα στοιχείο $1_R \in R$, $1_R \neq 0$, τέτοιο ώστε για όλα τα στοιχεία $x \in R$ να ισχύει

$$1_R \cdot x = x \cdot 1_R,$$

τότε ο δακτύλιος R λέγεται δακτύλιος με μοναδιαίο.

Αν για τον R ισχύει επιπλέον το αξίωμα της αντιμετάθεσης

R5 Για όλα τα στοιχεία $x, y \in R$ ισχύει:

$$x \cdot y = y \cdot x,$$

τότε ο δακτύλιος R λέγεται αντιμεταθετικός δακτύλιος.

Τέλος αν ισχύουν τα αξιώματα (R4) και (R5) συγχρόνως τότε ο R λέγεται αντιμεταθετικός δακτύλιος με μοναδιαίο.

Παραδείγματα:

1. Το σύνολο των ακέραιων $\mathbb{Z}$ με πράξεις τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο.

2. Για κάθε $m \in \mathbb{N}$, $m > 1$, το σύνολο των κλάσεων υπολοίπων mod$m$, $\mathbb{Z}_m$, με πράξεις τις (καλά ορισμένες) πράξεις πρόσθεσης κλάσεων

$$\oplus \left\{ \begin{array}{l} \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \\ (\bar{a}, \bar{b}) \mapsto \bar{a} \oplus \bar{b} \end{array} \right\}$$

και πολλαπλασιασμού κλάσεων

$$\odot \left\{ \begin{array}{l} \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n^* \\ (\bar{a}, \bar{b}) \mapsto \bar{a} \odot \bar{b} \end{array} \right\}$$

αποτελεί επίσης αντιμεταθετικό δακτύλιο με μοναδιαίο.

3. Το σύνολο των ακέραιων του Gauss

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

με πράξεις τις συνήθεις πράξεις μιγαδικών αποτελεί επίσης αντιμεταθετικό δακτύλιο με μοναδιαίο.

Ορισμός 11.3.2. Έστω R κάποιος αντιμεταθετικός δακτύλιος. Ένα στοιχείο $x \in R$, $x \neq 0$, λέγεται διαιρέτης του μηδενός αν και μόνο αν υπάρχει $y \in R$, $y \neq 0$ με $x \cdot y = 0$.

Ορισμός 11.3.3. Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο λέγεται *ακέραια περιοχή*, όταν δεν έχει διαιρέτες του μηδενός.

Παραδείγματα:

1. Ο δακτύλιος $(\mathbb{Z}, +, \cdot)$ είναι ακέραια περιοχή.
2. Οι δακτύλιοι $(\mathbb{Z}_m, +, \cdot)$ είναι ακέραιες περιοχές αν και μόνο αν ο m είναι πρώτος.
3. Ο δακτύλιος $\mathbb{Z}[i]$ είναι επίσης ακέραια περιοχή.

Ορισμός 11.3.4. Ένα μη κενό υποσύνολο R_1 του αντιμεταθετικού δακτυλίου R λέγεται *υποδακτύλιος* του R όταν είναι δακτύλιος ως προς τις πράξεις πρόσθεσης και πολλαπλασιασμού του R.

Ισχύει:

Πρόταση 11.3.5. *Ένα μη κενό υποσύνολο R_1 του αντιμεταθετικού δακτυλίου R, είναι υποδακτύλιος του R ακριβώς τότε όταν για όλα τα στοιχεία $x, y \in R_1$ ισχύει*

$$x - y \in R_1 \text{ και } x \cdot y \in R_1.$$

11.3.2 Ιδεώδη ενός αντιμεταθετικού δακτυλίου

Ορισμός 11.3.6. Έστω R ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και I ένα μη κενό υποσύνολο του R.

Το I λέγεται ιδεώδες όταν ισχύουν τα αξιώματα:

I1 Το I αποτελεί ομάδα ως προς την πρόσθεση,

I2 Για κάθε $r \in R$ και $x \in I$ ισχύει $rx \in I$.

Ορισμός 11.3.7. Αν $\alpha \in R$, τότε το *κύριο ιδεώδες* του R το οποίο παράγεται από το στοιχείο α, ορίζεται

$$\langle \alpha \rangle := \{r\alpha | r \in R\}.$$

Αν ο R είναι ακέραια περιοχή και όλα τα ιδεώδη του R είναι κύρια, τότε ο R λέγεται *περιοχή κυρίων ιδεωδών*.

Παράδειγμα: Η ακέραια περιοχή των ακέραιων αριθμών $(\mathbb{Z}, +, \cdot)$ όπως και ο δακτύλιος του Gauss είναι περιοχές κυρίων ιδεωδών.

Ορισμός 11.3.8. Αν R ακέραια περιοχή, το στοιχείο $p \in R$ λέγεται *ανάγωγο*, όταν δεν είναι μονάδα του R, δηλαδή δεν είναι πολλαπλασιαστικό αντίστροφο του R, και δεν αναλύεται σε γινόμενο μη τετριμμένων παραγόντων, δηλαδή, αν $p = a \cdot b$, τότε ένα από τα a, b είναι μονάδα του R.

Ορισμός 11.3.9. Μια ακέραια περιοχή R λέγεται *περιοχή μονοσήμαντης ανάλυσης*, όταν κάθε στοιχείο $a \neq 0$ αυτής είναι μονάδα ή ανάγωγο στοιχείο του R ή γινόμενο αναγώγων στοιχείων του R και επιπλέον η παράσταση αυτή είναι (ουσιαστικά) μονοσήμαντη.

Ισχύει η

Πρόταση 11.3.10. *Κάθε περιοχή κυρίων ιδεωδών είναι και περιοχή μονοσήμαντης ανάλυσης.*

Παρατήρηση 11.3.11. Δεν είναι κάθε ακέραια περιοχή, περιοχή μονοσήμαντης ανάλυσης. Για παράδειγμα στην ακέραια περιοχή

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$$

ο αριθμός 6 έχει δύο, διαφορετικές μεταξύ τους, γνήσιες αναλύσεις σε γινόμενο αναγώγων στοιχείων:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

11.4 Σώματα

11.4.1 Ορισμός και παραδείγματα

Ορισμός 11.4.1. Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο στον οποίο κάθε μη-μηδενικό στοιχείο είναι αντιστρέψιμο, λέγεται σώμα.

Παραδείγματα σωμάτων

1. Οι αντιμεταθετικοί δακτύλιο με μοναδιαίο $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ είναι σώματα.

2. Αν p πρώτος αριθμός, τότε ο δακτύλιος $(\mathbb{Z}_p, \oplus, \odot)$ είναι σώμα.

3. Αν $d \in \mathbb{Z}\backslash\{0, 1\}$ ελεύθερος τετραγώνου, τότε ο δακτύλιος

$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\},$$

είναι σώμα.

4. Αν K σώμα και x ανεξάρτητη μεταβλητή, τότε το σύνολο

$$K(x) = \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$

είναι επίσης σώμα και λέγεται το σώμα των ρητών συναρτήσεων υπεράνω του K.

Κάθε σώμα K περιέχει (ισόμορφα) το σώμα των ρητών αριθμών $\mathbb{Q}$ ή ένα σώμα $\mathbb{Z}_p$ για κάποιο πρώτο αριθμό p. Στην πρώτη περίπτωση λέμε ότι το σώμα είναι χαρακτηριστικής μηδέν ενώ στην δεύτερη ότι το σώμα είναι χαρακτηριστικής p.

11.4.2 Επεκτάσεις σωμάτων

Ορισμός 11.4.2. Αν ένα σώμα L περιέχει ως υπόσωμα το σώμα K, τότε λέμε ότι το L είναι *επέκταση* του K και την επέκταση τη συμβολίζουμε με L/K.

Παρατήρηση 11.4.3. Αν L/K επέκταση σωμάτων, τότε το σώμα L μπορεί να θεωρηθεί ως K-διανυσματικός χώρος.

Ορισμός 11.4.4. Βαθμός της επέκτασης σωμάτων L/K λέγεται η διάσταση του L ως K-διανυσματικού χώρου και συμβολίζεται με $[L : K]$.

Η επέκταση λέγεται πεπερασμένη όταν $[L : K] < \infty$, αλλιώς λέγεται άπειρη.

Αν L/K επέκταση σωμάτων και $\alpha \in L$, το α λέγεται *αλγεβρικό* ως προς το σώμα K όταν υπάρχει ένα, μη-μηδενικό, πολυώνυμο $f(x) \in K[x]$, τέτοιο ώστε να έχει το α ως ρίζα του.

Η επέκταση L/K λέγεται *αλγεβρική* όταν κάθε στοιχείο του L είναι αλγεβρικό ως προς το σώμα K.

Ισχύει η

Πρόταση 11.4.5. *Κάθε πεπερασμένη επέκταση L/K είναι κατ' ανάγκη αλγεβρική.*

Παρατήρηση 11.4.6. Το αντίστροφο δεν ισχύει. Υπάρχουν και άπειρες αλγεβρικές επεκτάσεις.

11.4.3 Επισύναψη

Ορισμός 11.4.7. Αν L/K επέκταση σωμάτων και $a_1, a_2, \ldots, a_n \in L$, με $K(a_1, a_2, \ldots, a_n)$ συμβολίζουμε το ελάχιστο υπόσωμα του L το οποίο περιέχει το σώμα K και τα στοιχεία $a_1, a_2, \ldots, a_n$. Το σώμα αυτό λέμε ότι είναι το σώμα που προκύπτει από το K με επισύναψη των $a_1, a_2, \ldots, a_n$.

Παρατήρηση 11.4.8. Αν τα στοιχεία $a_1, a_2, \ldots, a_n$ του L είναι αλγεβρικά στοιχεία ως προς του K τότε το

$$K(a_1, a_2, \ldots, a_n) = \{f(a_1, \ldots, a_n) | f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\}.$$

Παρατήρηση 11.4.9. Αν L/K επέκταση σωμάτων και $\alpha \in L$, αλγεβρικό στοιχείο ως προς το σώμα K, τότε ισχύει $[K(\alpha) : K] = \deg \mathrm{Irr}(\alpha, K)$, όπου $\mathrm{Irr}(\alpha, K)$ συμβολίζει το ανάγωγο (ελάχιστο) πολυώνυμο του α ως προς το K.

11.4.4 Σώμα ανάλυσης

Ορισμός 11.4.10. Αν L/K επέκταση σωμάτων, το L λέγεται σώμα ανάλυσης του πολυωνύμου $f(x) \in K[x]$ ως προς το K, όταν το $f(x)$ αναλύεται πλήρως στον δακτύλιο $L[x]$, δηλαδή ότι

$$f(x) = \alpha(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

και επιπλέον $L = K(\alpha_1, \ldots, \alpha_n)$.

Πρόταση 11.4.11. *Για κάθε πολυώνυμο $f(x)$ με συντελεστές από ένα σώμα K υπάρχει ένα σώμα ανάλυσης αυτου L_f και μάλιστα είναι μοναδικό κατά προσέγγιση ισομορφίας.*

11.4.5 Επεκτάσεις Galois

Ορισμός 11.4.12. Ένα πολυώνυμο $f(x) \in K[x]$ λέγεται *διαωρίσιμο πολυώνυμο* ως προς το K, όταν υπάρχει μια επέκταση L/K τέτοια ώστε κάθε ανάγωγος παράγοντας του $f(x)$ στον δακτύλιο $K[x]$ αναλύεται στον δακτύλιο $L[x]$ σε γινόμενο διαφόρων μεταξύ τους παραγόντων πρώτου βαθμού.

Το στοιχείο $\alpha \in L$ λέγεται διαχωρίσιμο ως προς το K, όταν υπάρχει ένα διαχωρίσιμο ως προς το K πολυώνυμο $f(x) \in K[x]$ του οποίου το α είναι ρίζα.

Η επέκταση L/K λέγεται *διαχωρίσιμη επέκταση* όταν κάθε στοιχείο $\alpha \in L$ είναι διαχωρίσιμο ως προς το K.

Πρόταση 11.4.13. *Κάθε αλγεβρική επέκταση L του σώματος K χαρακτηριστικής μηδέν είναι διαχωρίσιμη ως προς το K.*

Ορισμός 11.4.14. Η επέκταση σωμάτων L/K λέγεται επέκταση Galois , ακριβώς τότε όταν το σώμα L είναι σώμα ανάλυσης ενός διαχωρισίμου ως προς το K πολυωνύμου $f(x) \in K[x]$.

Αν θεωρήσουμε την ομάδα των K-αυτομορφισμών του σώματος L, τότε στην περίπτωση που η επέκταση L/K είναι Galois, υπάρχι μια αμφιμονοσήμαντη αντιστοιχία ανάμεσα στις υποομάδες της ομάδας Galois και στα ενδιάμεσα σώματα της επέκτασης L/K.

Ορισμός 11.4.15. Ένας K-αυτομορφισμός του σώματος L, $K \leq L$ είναι ένας αυτομορφισμός του L ο οποίος αφήνει όλα τα στοιχεία του K σταθερά.

Ορισμός 11.4.16. Μια επέκταση L/K λέγεται *απλή επέκταση* όταν υπάρχει στοιχείο $\vartheta \in L$ τέτοιο ώστε $L = K(\vartheta)$. Αν το ϑ είναι αλγεβρικό ως προς το σώμα K, τότε η L/K λέγεται *απλή αλγεβρική*.

Πρόταση 11.4.17. *Κάθε πεπερασμένη και διαχωρίσιμη επέκταση L/K είναι απλή αλγεβρική.*

Πόρισμα 11.4.18. *Αν η L είναι πεπερασμένη επέκταση ενός σώματος K χαρακτηριστικής μηδέν, τότε η επέκταση L/K είναι απλή αλγεβρική.*

Βιβλιογραφία

[1] Hungerford, T.W.: *Algebra*. Graduate Texts in Mathematics. Springer New York, 2012, ISBN 9781461261018.

[2] Jacobson, N.: *Basic Algebra I: Second Edition*. Dover Books on Mathematics. Dover Publications, 2012, ISBN 9780486135229.

[3] Lang, S.: *Algebra*. Graduate Texts in Mathematics. Springer New York, 2012, ISBN 9781461300410.

[4] Fraleigh B. John: *Εισαγωγή στην Άλγεβρα*. Πανεπιστημιακές Εκδόσεις Κρήτης, 1995, 2011, ΙΣΒΝ 960-7309-71-5.

[5] Βάρσος Δ., Δεριζιώτης Δ., Εμμανουήλ Ι. Μαλιάκας Μ. Ταλέλλη Ο.: *Μια εισαγωγή στην Άλγεβρα*. Εκδόσεις Σοφία 2012, ΙΣΒΝ 978-960-6706-37-0.

Παράρτημα Β, χρήση Sage

Το πρόγραμμα Sage[1] είναι ένα ελεύθερο ανοιχτού κώδικα σύστημα λογισμικού, το οποίο βασίστηκε στον συνδυασμό πολλών υπαρχόντων συστημάτων για υπολογιστικά μαθηματικά και ο σκοπός του είναι να αποτελέσει μια ανοιχτού λογισμικού εναλλακτική λύση για πακέτα όπως το Magma[2], Maple[3], Mathematica [4] και Matlab[5].

Ας δούμε μερικά παραδείγματα:

```
sage: 2 + 2
4
factor(-2015)
-1 * 5 * 13 * 31
```

Μπορούμε να πάρουμε πρώτους αριθμούς

```
prime_range(100)
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,
59, 61, 67, 71, 73, 79, 83, 89, 97]
```

ή να μετρήσουμε το πλήθος των πρώτων που είναι μικρότεροι του 10^6.

```
prime_pi(10^6)
78498
```

Το πρόγραμμα μπορεί επίσης να χειριστεί έννοιες από τον απειροστικό λογισμό, όπως αόριστα και ορισμένα ολοκληρώματα:

```
integrate(1 + x + x^2, x)
1/3*x^3 + 1/2*x^2 + x
numerical_integral(1 + x + x^2, 0, 3)[0]
16.500000000000004
```

[1] http://www.sagemath.org/
[2] http://magma.maths.usyd.edu.au/magma/
[3] http://www.maplesoft.com/
[4] http://www.wolfram.com/mathematica/
[5] http://www.mathworks.com/products/matlab/

Και να κάνει γραφικές παραστάσεις συναρτήσεων και όχι μόνο.

Το πρόγραμμα σαγε αποτελεί μια πλήρη γλώσσα προγραμματισμού με δομή όπως η python[6]. Μπορούμε να εκτελέσουμε βρόγχους (λοοπς) πάνω στα αντικείμενά του. Έτσι μπορούμε να υπολογίσουμε τα τετράγωνα όλων των πρώτων που είναι μικρότεροι του 1000 με τον παρακάτω κώδικα:

```
sum=0
for i in prime_range(1000):
    sum=sum+i^2
    print sum
49345379
```

Ας δούμε πως μπορούμε να χειριστούμε πολυώνυμα με το sage. Θα πρέπει να ορίσουμε πρώτα τον πολυωνυμικό δακτύλιο $\mathbb{Q}[t]$

```
sage: R = PolynomialRing(QQ, 't')
sage: R
Univariate Polynomial Ring in t over Rational Field
```

Οι παραπάνω εντολές δηλώνουν στο σαγε ότι η αλφαριθμητική μεταβλητή (στρινγ) 't' συμβολίζει την μεταβλητή του δακτυλίου στην εμφάνιση στην οθόνη. Αυτό **δεν** ορίζει το σύμβολο t για χρήση στο Σαγε, δηλαδή δεν μπορούμε να το χρησιμοποιήσουμε για να εισαγάγουμε ένα πολυώνυμο όπως το $t^2 + 2t + 1$.

Θα μπορούσαμε εναλλακτικά να δώσουμε

```
sage: S = QQ['t']
sage: S == R
True
```

Στον παραπάνω ορισμό ορίσαμε τον δακτύλιο S και ρωτήσαμε (η έκφραση με τα δύο == έχει την έννοια της ερώτησης) αν οι δακτύλιοι S, R ταυτίζονται, και πήραμε θετική (τρυε) απάντηση. Και αυτός ο τρόπος ορισμού έχει το ίδιο πρόβλημα στη χρήση της μεταβλητής τ.

Ένας πολύ βολικότερος τρόπος είναι να δώσουμε

```
sage: R.<t> = PolynomialRing(QQ)
```

ή

```
sage: R.<t> = QQ['t']
<div>
```

ή

```
sage: R.<t> = QQ[]
```

Οι παραπάνω ορισμοί ορίζουν τη μεταβλητή να είναι η μεταβλητή του πολυωνυμικού δακτυλίου, οπότε μπορούμε εύκολα να ορίσουμε στοιχεία του δακτυλίου:

```
sage: poly = (t+1) * (t+2); poly
t^2 + 3*t + 2
sage: poly in R
True
```

[6] https://www.python.org/

Στο παραπάνω ο τελεστής ìν' έδωσε θετική απάντηση (τρυε), αφού πράγματι το πολυώνυμο είναι στοιχείο του δακτυλίου R.

Σε κάθε περίπτωση θα μπορούσαμε να βρούμε τον γεννήτορα του πολυωνυμικού δακτυλίου ως εξής:

```
sage: R = PolynomialRing(QQ, 't')
sage: t = R.0
sage: t in R
True
```

Οι πραγματικοί και οι μιγαδικοί αριθμοί είναι δομές κινητής υποδιαστολής και οι πράξεις δεν γίνονται με ακριβή τρόπο. Ιδιαίτερα οι μιγαδικοί αριθμοί θεωρούνται ότι παράγονται πάνω από τους πραγματικούς με το σύμβολο i

```
sage: CC
Complex Field with 53 bits of precision
sage: CC.0  # 0th generator of CC
1.00000000000000*I
```

Ας κάνουμε μερικά παραδείγματα στον δακτύλιο $\mathbb{Q}[t]$

```
sage: R, t = QQ['t'].objgen()
sage: f = 2*t^7 + 3*t^2 - 15/19
sage: f^2
4*t^14 + 12*t^9 - 60/19*t^7 + 9*t^4 - 90/19*t^2 + 225/361
sage: cyclo = R.cyclotomic_polynomial(7); cyclo
t^6 + t^5 + t^4 + t^3 + t^2 + t + 1
sage: g = 7 * cyclo * t^5 * (t^5 + 10*t + 2)
sage: g
7*t^16 + 7*t^15 + 7*t^14 + 7*t^13 + 77*t^12 + 91*t^11 +
91*t^10 + 84*t^9+ 84*t^8 + 84*t^7 + 84*t^6 + 14*t^5
sage: F = factor(g); F
(7) * t^5 * (t^5 + 10*t + 2) *
(t^6 + t^5 + t^4 + t^3 + t^2 + t + 1)
sage: F.unit()
7
sage: list(F)
[(t, 5), (t^5 + 10*t + 2, 1), (t^6 + t^5 + t^4 + t^3 + t^2
 + t + 1, 1)]
```

Παρατηρούμε ότι η παραγοντοποίηση καταγράφει και τη μονάδα του δακτυλίου.

Η διαίρεση δύο πολυωνύμων δίνει αποτέλεσμα στον δακτύλιο πηλίκων, τον οποίο το σαγε ορίζει αυτόματα:

```
sage: x = QQ['x'].0
sage: f = x^3 + 1; g = x^2 - 17
sage: h = f/g;  h
(x^3 + 1)/(x^2 - 17)
sage: h.parent()
Fraction Field of Univariate Polynomial Ring in x over
```

```
Rational Field
```

Αν ορίσουμε τη μεταβλητή με διαφορετικό όνομα έχουμε έναν διαφορετικό πολυωνυμικό δακτύλιο για το σαγε

```
sage: R.<x> = PolynomialRing(QQ)
sage: S.<y> = PolynomialRing(QQ)
sage: x == y
False
sage: R == S
False
sage: R(y)
x
sage: R(y^2 - 17)
x^2 - 17
```

Ο δακτύλιος προσδιορίζεται από τη μεταβλητή. Ορίζοντας έναν δακτύλιο με άλλο όνομα αλλά την ίδια μεταβλητή δεν καταλήγουμε σε διαφορετικούς δακτυλίους.

```
sage: R = PolynomialRing(QQ, "x")
sage: T = PolynomialRing(QQ, "x")
sage: R == T
True
sage: R is T
True
sage: R.0 == T.0
True
```

Μπορούμε να ορίσουμε πολυωνυμικούς δακτυλίους πάνω από οποιονδήποτε δακτύλιο βάσης.

```
sage: R.<T> =PolynomialRing(GF(7)); R
Univariate Polynomial Ring in T over Finite Field of size 7
```

Ας δούμε ένα παράδειγμα ενός αθροίσματος όπου κάθε όρος έχει και διαφορετικό όνομα:

```
sage: f = sum(1/var('n%s'%i)^i for i in range(10))
1/n1 + 1/n2^2 + 1/n3^3 + 1/n4^4 + 1/n5^5 + 1/n6^6 +
1/n7^7 + 1/n8^8 + 1/n9^9 + 1
```

Ευρετήριο