Γιάννη Α. Αντωνιάδη
Τμήμα Μαθηματικών,
Πανεπιστήμιο Κρήτης

Θεωρία Αριθμών
κατά τον $17^ο$ και $18^ο$ αιώνα

Έκδοση ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ"
Πανεπιστήμιο Κρήτης
Ηράκλειο, 1999

Στο γυιό μας το νεότερο,

τον Κάρολο.

Περιεχόμενα

Εισαγωγή

Κύριος σκοπός του βιβλίου είναι η μελέτη της ζωής και του αριθμοθεωρητικού έργου των Fermat, Euler, Lagrange και Legendre. Θα μελετήσουμε δηλαδή την ιστορία και τα αποτελέσματα της Θεωρίας Αριθμών που ανακαλύφθηκαν κατά τον 17^o και 18^o αιώνα.

Σε μία περίοδο όπου άλλοι κλάδοι των Μαθηματικών αναπτύσσονται ραγδαία και ο ανταγωνισμός προτεραιότητας είναι πολύ μεγάλος, η Θεωρία Αριθμών εξελίσσεται με βραδείς ρυθμούς και σε ερασιτεχνική βάση.

Στόχος μας δεν είναι να δώσουμε κομψές αποδείξεις, κάτι που συνήθως γίνεται σε κάθε εισαγωγικό μάθημα Θεωρίας Αριθμών, αλλά περισσότερο να δείξουμε τη διαδικασία ανάπτυξης των ιδεών καθώς και τις προσπάθειες που έγιναν μέχρι τη σωστή διατύπωση και απόδειξη των αποτελεσμάτων. Απευθυνόμαστε σε φοιτητές Μαθηματικών και άλλων συναφών προς τα Μαθηματικά Τμημάτων καθώς και σε μαθητές Λυκείου που αγαπούν τα Μαθηματικά και ειδικότερα την Θεωρία Αριθμών. Ελπίζουμε η μελέτη του περιεχομένου του βιβλίου να δώσει σε πολλούς νέους μας το έναυσμα της επέκτασης των γνώσεως τους σε έναν από τους αρχαιότερους και ελκυστικότερους κλάδους των Μαθηματικών.

Το βιβλίο εκδίδεται μέσω του προγράμματος ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ" του Πανεπιστημίου Κρήτης. Θερμές ευχαριστίες χρωστώ στον υπεύθυνο του προγράμματος Αν. Καθηγητή κύριο Γιώργο Τζιρίτα. Τέλος θα ήθελα να ευχαριστήσω τον μαθητή μου Θανάση Βέσση και τον David J. M^{c}Clurkin για την ηλεκτρονική επεξεργασία του κειμένου.

Γιάννης Α. Αντωνιάδης, Καθηγητής

Ηράκλειο, Οκτώβριος 1999

Κεφάλαιο 1

Πρωτοϊστορία

Σύμφωνα με τον Jacobi η θεωρία των ελλειπτικών συναρτήσεων γεννήθηκε ανάμεσα στις 23/12/1751 και 27/1/1752. Την πρώτη ημερομηνία η Ακαδημία των Επιστημών του Βερολίνου παρέδωσε στον Euler το δίτομο έργο του Fagnano, Produzioni Mathematiche το οποίο είχε εκδοθεί ήδη από το 1750. Ο Euler έπρεπε να εξετάσει το έργο και να γράψει και ένα ευχαριστήριο γράμμα στον Fagnano. Την δεύτερη ημερομηνία ο Euler ξεκινώντας από την εργασία του Fagnano για το lemniscate (Λημνίσκο) ανακοίνωσε στην Ακαδημία Επιστημών του Βερολίνου τα αποτελέσματα μιάς σειράς εργασιών του, όπου αποδείκνυε τα θεωρήματα της πρόσθεσης και του πολλαπλασιασμού ελλειπτικών ολοκληρωμάτων.

Αν προσπαθήσει κανείς, όπως για τις ελλειπτικές συναρτήσεις, να βρει πότε γεννήθηκε η Θεωρία των Αριθμών, θα διαπιστώσει ότι, όπως και ο Βάκχος, γεννήθηκε δύο φορές. Η πρώτη γέννηση θα πρέπει να έχει συμβεί μεταξύ 1621 και 1636. Στα 1621 δημοσιεύθηκαν τα Αριθμητικά του Διόφαντου από τον Bachet στο ελληνικό πρωτότυπο, μαζί με λατινική μετάφραση και εκτεταμένα σχόλια. Πότε έπεσε στα χέρια του Fermat αυτό το βιβλίο δεν μας είναι γνωστό. Από την αλληλογραφία του Fermat όμως βγαίνει το συμπέρασμα ότι μέχρι το 1636 όχι μόνο το είχε μελετήσει προσεκτικά αλλά είχε ήδη αναπτύξει και δικές του ιδέες πάνω σε ένα σωρό θέματα που διαπραγματεύονται τα Αριθμητικά του Διόφαντου.

Ο Fermat προσπάθησε να πείσει μερικούς φίλους του, όπως ο Huygens, ο Pascal κ.α., να ασχοληθούν και αυτοί με τον αγαπημένο του κλάδο, αλλά δεν τα κατάφερε. Ο Fermat πέθανε στα 1665. Ο γυιός του Samuel εξέδωσε το βιβλίο του Bachet στα 1670 μαζί με τις παρατηρήσεις που προσέθεσε ο πατέρας του στο περιθώριο και αργότερα (1679) δημοσίευσε και μέρος της αλληλογραφίας του. Μέχρι να φτάσουμε στο σημείο να έχουν οι εκδόσεις αυτές κάποια επίδραση στα Μαθηματικά της εποχής πέρασε μισός αιώνας και στο διάστημα αυτό φαινόταν σαν να είχε πεθάνει η Θεωρία των Αριθμών.

Το πώς ξαναγεννήθηκε η Θεωρία Αριθμών το ξέρουμε τώρα επακριβώς. Στα 1729 ο Euler ήταν μέλος της Ακαδημίας της Αγίας Πετρούπολης. Ο φίλος του Goldbach ήταν στην Μόσχα. Η αλληλογραφία τους διατηρήθηκε προσεκτικά και εκδόθηκε στα 1843. Σε ένα από τα γράμματά του ο Goldbach (ερασιτέχνης μαθηματικός) διατύπωσε την γνωστή σήμερα **εικασία του Goldbach** (θα αναφερθούμε αργότερα σ' αυτήν). Την 1/12/1729 ο Goldbach ρώτησε τον Euler τί γνώμη έχει σχετικά με την εικασία του Fermat ότι όλοι οι ακέραιοι αριθμοί της μορφής

$$2^{2^n}+1, \quad n=0,1,2,\ldots$$

είναι πρώτοι. Στην απάντησή του ο Euler εξέφρασε κάποιες αμφιβολίες αλλά τίποτε το καινούργιο δεν εμφανίστηκε μέχρι την $4^η$ Ιουνίου οπότε ο Euler ανέφερε ότι αυτόν τον καιρό διαβάζει Fermat και ότι είναι πολύ εντυπωσιασμένος από την εικασία του Fermat ότι κάθε ακέραιος μπορεί να γραφεί σαν άθροισμα τεσσάρων τετραγώνων. Από αυτή την ημέρα αρχίζει μία πολύ γόνιμη περίοδος στη Θεωρία των Αριθμών από τον Euler η οποία συνεχίστηκε από τους Lagrange, Legendre για να φθάσει, με τον Gauss, σε πολύ υψηλό επίπεδο ανάπτυξης.

Το ότι ο Fermat επηρεάστηκε από ένα Έλληνα μαθηματικό του $3^{ου}$ μετά Χριστό αιώνα, ήρθε αργότερα στο φως. Οι γνώσεις μας για τα μαθηματικά των αρχαίων αυξάνονταν μέρα με τη μέρα. Οι γνώσεις μας π.χ. για το έργο του Αρχιμήδη αυξήθηκαν πολύ με την ανακάλυψη της περγαμηνής της Κωνσταντινουπόλεως στα 1906. Αρχικά αυτό που είχε επιζήσει από τον Διόφαντο ήταν 6 κεφάλαια (''βιβλία'') παρά το ότι στην εισαγωγή αναφέρονται 13. Στο μεταξύ πρόσφατα ανακαλύφθηκε ένα ακόμα βιβλίο του. Σκοπός μας

βέβαια δεν είναι να γυρίσουμε πίσω στα Μαθηματικά της Ινδίας, της Μεσοποταμίας ή της Κίνας. Δεν μπορούμε όμως να παραλείψουμε να αναφέρουμε το γεγονός ότι ο Ευκλείδης αφιέρωσε τρία κεφάλαια (''βιβλία'') από τα **Στοιχεία** του στη Θεωρία των Αριθμών και συγκεκριμένα τα VII, VIII και IX.

Οι έννοιες του πρώτου αριθμού, του διαιρέτη ενός ακεραίου καθώς και του ελαχίστου κοινού πολλαπλασίου πρέπει να εμφανίστηκαν αρκετά νωρίς. Ο Πλάτων στους Νόμους του μελετάει τον αριθμό 5040 και βρίσκει π.χ. ότι έχει 59 διαιρέτες εκτός του εαυτού του. Φαίνεται ότι στην Ακαδημία του Πλάτωνα κάτι γνώριζαν οι μαθηματικοί για την παραγοντοποίηση των ακεραίων αλλά είναι δύσκολο να διατυπώσουμε ακριβώς το εύρος αυτής της γνώσης.

Από τον Ευκλείδη, τώρα μπορούμε να αναφέρουμε τον ομώνυμο **αλγόριθμό** του (Ευκλ. VII, 1-2) καθώς και την πρόταση ότι **υπάρχουν άπειροι πρώτοι** (Ευκλ. IX, 20):

> **''Οι πρώτοι αριθμοί πλείους εισί παντός του προταθέντος πλήθους πρώτων αριθμών.''**

Το θεμελιώδες θεώρημα της αριθμητικής για μία μεγάλη κλάση αριθμών (Ευκλ. IQ, 14).

Μαγικές και μυστικιστικές ιδιότητες των αριθμών εμφανίζονται σε πολλούς πολιτισμούς. Έτσι ορίζονται οι **τέλειοι** αριθμοί, εκείνοι οι ακέραιοι πού είναι ίσοι με το άθροισμα των γνησίων διαιρετών τους. Το τελευταίο θεώρημα στο κεφάλαιο IX (Ευκλ. IX, 36), ίσως το πιο σπουδαίο από την δουλειά του Ευκλείδη, είναι η

Πρόταση 1.1 *Ο $2^n(2^{n+1}-1)$ είναι τέλειος, όταν ο $2^{n+1}-1$ είναι πρώτος.*

Απόδειξη: Έστω p ο πρώτος $2^{n+1}-1$. Ο $2^n(2^{n+1}-1)$ τότε γράφεται $a = 2^n p$. Οι διαιρέτες του a είναι

$$1,\ 2,\ 2^2,\ \cdots,\ 2^n,\ p,\ 2p,\ \cdots,\ 2^n p$$

και το άθροισμά τους είναι

$$\frac{2^{n+1}-1}{2-1}\cdot(p+1) = 2a,$$

δηλαδή ο a είναι τέλειος. □

Απλές διοφαντικές εξισώσεις πρώτου βαθμού, δηλαδή εξισώσεις της μορφής

$$aX + bY = m, \quad (a, b, m \in \mathbb{Z})$$

των οποίων ζητούνται οι ακέραιες λύσεις x, y, εμφανίζονται στο Διόφαντο, αλλά έχουν προϊστορία. Θα ξαναγυρίσουμε πίσω σ' αυτές όταν αναφερθούμε στη **μέθοδο της καθόδου του Fermat**.

Ένα άλλο πρόβλημα είναι η εύρεση των λεγόμενων **πυθαγορείων τριάδων**, δηλαδή ακεραίων αριθμών x, y, z τέτοιων ώστε

$$x^2 + y^2 = z^2 \tag{1.1}$$

Η πιο ''απλή'' τριάδα είναι $(x, y, z) = (3, 4, 5)$. Ένας πίνακας που περιέχει 15 πυθαγόρειες τριάδες είναι ο παλιός πίνακας της Βαβυλώνας Πλιμπτον 332 που εκδόθηκε από τους O. Neugebauer και A. Sachs, Mathematical Cuneiform Texts, New Haven 1945, pp. 38-41 και χρονολογείται μεταξύ των ετών 1900 και 1600 π.Χ. Δεν είναι γνωστό πως υπολογίστηκαν αυτές οι τριάδες. Η λύση πάντως του προβλήματος ήταν γνωστή στον Ευκλείδη (Ευκλ. X28, Λήμμα 1).

Εύρεση των πυθαγορείων τριάδων

Είναι προφανές ότι αν (x, y, z) είναι λύση της (1.1) και $\lambda \in \mathbb{Z}$ τότε και $(\lambda x, \lambda y, \lambda z)$ είναι λύση. Αρκεί λοιπόν να βρούμε το σύνολο των **πρωταρχικών** (primitive) λύσεων, δηλαδή εκείνων για τις οποίες $(x, y, z) = 1$.

Αν $(x, y, z) = 1$ λύση της (1.1) τότε εύκολα συμπεραίνει κανείς ότι $(x, y) = (y, z) = (x, z) = 1$, οι x και y δεν μπορούν συγχρόνως να είναι άρτιοι (διότι τότε και ο z θα ήταν άρτιος, δηλαδή $(x, y, z) > 1$, άτοπο) ούτε και οι δύο περιττοί διότι τότε θα είχαμε $z^2 \equiv 2 \pmod 4$, άτοπο.

Έστω $x \equiv 0 \pmod 2$ και $y \equiv 1 \pmod 2 \Rightarrow z^2 \equiv 1 \pmod 4 \Rightarrow z$ περιττός. Γράφουμε $x^2 = z^2 - y^2 = (z - y)(z + y)$. Έστω $z + y = 2u,\ z - y = 2v \Rightarrow z = u + v,\ y = u - v$.

$(z+y, z-y) = 2(z,y) = 2 \Rightarrow (u,v) = 2$. Αν u και v συγχρόνως περιττοί τότε z, y άρτιοι, άτοπο. Άρα, ένας από τους u, v είναι άρτιος και ο άλλος περιττός. Τώρα η σχέση $\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2} = uv$ και $(u,v) = 1$ δίνει $u = S^2$, $v = T^2$, $(S,T) = 1$ ένας άρτιος και ο άλλος περιττός.

Ώστε αν (x,y,z) είναι μία πρωταρχική πυθαγόρεια τριάδα τότε $\exists (S,T) \in \mathbb{Z} \times \mathbb{Z}$ με $(S,T) = 1$ ο ένας άρτιος και ο άλλος περιττός έτσι ώστε

$$x = 2ST,\ y = S^2 - T^2,\ z = S^2 + T^2.$$

Αντιστρόφως: Αν $(S,T) \in \mathbb{Z} \times \mathbb{Z}$, ένας άρτιος ο άλλος περιττός, τότε ο x είναι άρτιος y, z είναι περιττοί και μάλιστα $(x,y) = (y,z) = (x,z) = 1$, δηλαδή $(x,y,z) = 1$. Απλή επαλήθευση μας δίνει $x^2 + y^2 = z^2$.

Θεώρημα 1.2 *Όλες οι πυθαγόρειες τριάδες δίνονται από*

$$x = 2\lambda ST,\ y = \lambda(S^2 - T^2),\ z = \lambda(S^2 + T^2)$$

με $\lambda \in \mathbb{Z}$, $(S,T) \in \mathbb{Z} \times \mathbb{Z}$, $(S,T) = 1$ *ένας άρτιος και ο άλλος περιττός.*

Το αποτέλεσμα αυτό περνάει από τον Ευκλείδη στο Διόφαντο και αργότερα, στα 1572, εμφανίζεται στην **Άλγεβρα** του **Bambelli** (το τρίτο βιβλίο της οποίας στηρίζεται στα Αριθμητικά του Διόφαντου) καθώς και στο έργο του **Viéte**.

Αν τώρα, αντί να ζητούμε πυθαγόρειες τριάδες, προσπαθήσουμε να λύσουμε κάποιο γενικότερο πρόβλημα, δηλαδή ποιοί φυσικοί αριθμοί γράφονται σαν άθροισμα δύο τετραγώνων, τότε πολύ χρήσιμη είναι η ταυτότητα

$$(x^2 + y^2)(z^2 + t^2) = (xz \pm yt)^2 + (xt \mp yz)^2. \tag{1.2}$$

Λόγω των δύο δυνατοτήτων που έχουμε ως προς τα πρόσημα στην ταυτότητα (1.2), χρησιμοποιείται συχνά για να κατασκευάσουμε αριθμούς που γράφονται σαν άθροισμα τετραγώνων κατά δύο διαφορετικούς τρόπους. Για $z = t = 1$ έχουμε

$$2(x^2 + y^2) = (x+y)^2 + (x-y)^2 \tag{1.3}$$

η οποία ήταν ήδη γνωστή στον Ευκλείδη (Ευκλ. II, 9-10).
Η (1.2) θα πρέπει να ήταν γνωστή στον Διόφαντο όπως φαίνεται από την παρακάτω παρατήρησή του (δες [11], σελίδα 11):

> ''Είναι στην φύση του αριθμού 65 ότι μπορεί να γραφεί σαν άθροισμα δύο τετραγώνων κατά δύο διαφορετικούς τρόπους, $16 + 49$ και $64 + 1$. Αυτό συμβαίνει διότι ο 65 είναι γινόμενο των 13 και 5 που είναι άθροισμα δύο τετραγώνων.''

Υπάρχει λοιπόν η εικασία ότι η (1.2) ήταν κάποιο από τα χαμένα πορίσματα του Διόφαντου. Απόδειξη πάντως της ταυτότητας (1.2) εμφανίζεται στο Βιβλίο του Fibonacci (Leonardo Pisano) **Liber Quadratorum** που εκδόθηκε το 1225. (Ξαναεκδόθηκε στα 1987 από τον εκδοτικό οίκο Academic Press.) Σε αντίθεση με το πιο δημοφιλές (λαϊκό) έργο του Fibonacci **Liber Abaci** το Liber Quadratorum ήταν ξεχασμένο και δυσεύρετο. Εκδόθηκε, για πρώτη φορά μετά το 1225, από τον **Boncompagni** στα 1856.

Προτού πούμε δύο λέξεις για το βιβλίο του Fibonacci, ας σημειώσουμε εδώ ότι ο Viéte χρησιμοποιούσε την ταυτότητα (1.2) έτσι ώστε από δοσμένα ορθογώνια τρίγωνα να παράγει άλλα και παρατήρησε τη σχέση της ταυτότητας (1.2) με τους τύπους αθροίσματος και διαφοράς των τριγωνομετρικών συναρτήσεων. Ο Viéte ενδιαφερόταν πιο πολύ για την άλγεβρα και την τριγωνομετρία παρά για την Θεωρία Αριθμών.

Εάν

$$x = r\cos a, \;\; y = r\sin a, \;\; z = s\cos b, \;\; t = s\sin b,$$

τότε

$$xz \pm yt = rs\cos(a \mp b), \;\; xt \mp yz = rs\sin(a \mp b)).$$

Ο Fibonacci ταξίδεψε πολύ, ήταν έμπορος, και γνώρισε τους πολιτισμούς των Αράβων, των Ελλήνων και των Λατίνων καθώς και τα μαθηματικά της εποχής του. Κάποτε του ζητήθηκε να βρεί τρία τέλεια τετράγωνα σαν διαδοχικούς όρους αριθμητικής προόδου με λόγο 5, δηλαδή να λύσει στους ρητούς το σύστημα

$$y^2 - x^2 = z^2 - y^2 = 5$$

ή, ισοδύναμα, να λύσει στους ακεραίους το σύστημα

$$Y^2 - X^2 = Z^2 - Y^2 = 5T^2.$$

Αυτό είναι το αντικείμενο το οποίο διαπραγματεύεται στο **Liber Quadratorum**. Προβλήματα που αφορούσαν τέλεια τετράγωνα σε αριθμητικές προόδους είναι αρκετά παλιά λόγω της ταυτότητας (1.3). Το να βρεί κανείς τέτοια τετράγωνα είναι ισοδύναμο με το να βρεί πυθαγόρειες τριάδες.

Πράγματι, αν X^2, Y^2, Z^2 βρίσκονται σε αριθμητική πρόοδο τότε

$$Y^2 = \frac{1}{2}(X^2 + Z^2) = U^2 + V^2,$$

όπου

$$U = \frac{1}{2}(X + Z), \quad V = \frac{1}{2}(Z - X)$$

και η διαφορά (λόγος) $Y^2 - X^2 = Z^2 - Y^2$ έχει τιμή $\frac{1}{2}(Z^2 - X^2) = 2UV$, δηλαδή, τετραπλάσια του εμβαδού του τριγώνου (U, V, Y).

Δεν υπάρχει κανένα στοιχείο που να μας δείχνει ότι ο Leonardo γνώριζε την τελευταία παρατήρηση αλλά σε κάποιο βυζαντινό χειρόγραφο του $11^{ου}$ ή $12^{ου}$ αιώνα υπάρχει το πρόβλημα:

Να βρεθεί πυθαγόρεια τριάδα εμβαδού $5m^2$.

Εικάζεται λοιπόν ότι ο Fibonacci θα το είχε δει κατά την παραμονή του στην Κωνσταντινούπολη. Αυτός που έθεσε το πρόβλημα είχε ήδη αποδείξει ότι μία αριθμητική πρόοδος ήταν η 31^2, 41^2, 49^2. (Ελπίζουμε σ' αυτό το πρόβλημα να μας δοθεί η ευκαιρία να επιστρέψουμε αργότερα και να δούμε τα αποτελέσματα που υπάρχουν μέχρι σήμερα.) Αν τώρα γενικεύσουμε το πρόβλημα και ζητήσουμε να δούμε ποιοί φυσικοί αριθμοί παρίστανται από την τετραγωνική μορφή

$$X^2 \mp NY^2$$

όπου N δοσμένος φυσικός αριθμός, τότε οι ταυτότητες που χρειαζόμαστε είναι

$$(X^2 - NY^2)(Z^2 - NT^2) = (XZ \pm NYT)^2 - (XT \pm YZ)^2 \tag{1.4}$$

$$(X^2 + NY^2)(Z^2 + NT^2) = (XZ \pm NYT)^2 + N(XT \mp YZ)^2 \tag{1.5}$$

Από μοντέρνα αλγεβρική σκοπιά δεν διαφέρουν από τις ταυτότητες (1.2), αλλά αυτό έγινε αντιληπτό για πρώτη φορά τον 18^o αιώνα.

Ο πιο απλός ίσως τρόπος για να τις αποδείξουμε είναι να γράψουμε

$$(X + Y\sqrt{N})(Z \pm T\sqrt{N}) = (XZ \pm NYT) \pm (XT \pm YZ)\sqrt{N}$$

και την ίδια ταυτότητα με το $\sqrt{-N}$ και να πολλαπλασιάσουμε με τις συζυγείς παραστάσεις, δηλαδή το $\sqrt{\pm N}$ το αντικαθιστούμε με το $-\sqrt{\pm N}$. Η απόδειξη αυτή εμφανίζεται για πρώτη φορά στο βιβλίο του Euler, Algebra που εκδόθηκε στα 1770.

Μια και ο Ευκλείδης αφιερώνει ολόκληρο το κεφάλαιο X στις άρρητες ποσότητες δευτέρου βαθμού, μπορεί να φανταστεί κανείς ότι ο Ευκλείδης ή οι "διάδοχοί" του θα πρέπει να είχαν αποδείξει ανάλογα τις ταυτότητες (1.4), (1.5) ή έστω ειδικές περιπτώσεις αυτών. Σίγουρο είναι ότι ο Ευκλείδης γνώριζε την ταυτότητα $(\sqrt{r} + \sqrt{s})(\sqrt{r} - \sqrt{s}) = r - s$ και ότι η

$$\frac{1}{\sqrt{r} + \sqrt{s}} = \frac{\sqrt{r}}{r - s} - \frac{\sqrt{s}}{r - s} \tag{1.6}$$

(Ευκλ. X, 112).

Δυστυχώς το κίνητρο του Ευκλείδη στο X βιβλίο είναι η δημιουργία θεωρίας για την κατασκευή κανονικών πολυγώνων και πολυέδρων και όχι η αλγεβρική θεωρία των τετραγωνικών σωμάτων όπως θα έκαναν οι μοντέρνοι μαθηματικοί. Απομένει λοιπόν να υποθέσουμε ότι ούτε στην αρχαιότητα ούτε αργότερα χρησιμοποιήθηκαν ταυτότητες με τετραγωνική ρίζα για σκοπούς της αριθμητικής. Σίγουρο είναι ότι οι Euler και Lagrange στα τέλη του $18^{ου}$ αιώνα συγχαίρουν ο ένας τον άλλο για την φαεινή ιδέα να χρησιμοποιήσουν μιγαδικές τετραγωνικές ρίζες στην Θεωρία Αριθμών.

Εξισώσεις της μορφής $x^2 - Ny^2 = \pm m$, όπου m, N δοσμένοι φυσικοί αριθμοί, θα πρέπει να είχαν εμφανιστεί στα έργα αρχαίων Ελλήνων πολύ πιθανό σε σύνδεση με το πρόβλημα της καλής ρητής προσέγγισης του άρρητου $\sqrt{N}$. Είναι προφανές ότι αν $x^2 - Ny^2 = \pm m$ και τα x, y είναι μεγάλα σε σύγκριση προς το m τότε ο λόγος $\dfrac{x}{y}$ μας δίνει μία καλή προσέγγιση της $\sqrt{N}$ όπως φαίνεται από την ταυτότητα

$$\frac{x}{y} - \sqrt{N} \;=\; \frac{1}{y} \cdot \frac{x^2 - Ny^2}{x + y\sqrt{N}}$$

η οποία είναι ειδική περίπτωση της (1.6) του (Ευκλ. X, 112).

Έτσι όταν ο Ευτόκιος στα σχόλιά του στον Αρχιμήδη θέλει να επαληθεύσει τις προσεγγίσεις του Αρχιμήδη 256/153 και 1351/780 για τον αριθμό $\sqrt{3}$, γράφει:

$$265^2 - 3 \cdot 153^2 = -2, \quad 1351^2 - 3 \cdot 780^2 = 1.$$

Η ταυτότητα (1.4) τώρα δίνει μία εύκολη μέθοδο κατασκευής μιάς λύσης της

$$X^2 - NY^2 = \pm m$$

αν κάποιος γνωρίζει ήδη μία άλλη λύση της $X^2 - NY^2 = \pm m$ και μία λύση της $\mu^2 - N\nu^2 = \pm 1$ ή (μερικές φορές) της $\mu^2 - N\nu^2 = \pm 2$.

Αν πάρουμε στην (1.4) $N = 3$, $Z = 5$, $T = 3$ βρίσκουμε

$$(5X + 9Y)^2 - 3(3X + 5Y)^2 = -2(X^2 - 3Y^2).$$

Αν τώρα $X^2 - 3Y^2 = -2$ τότε οι X και Y πρέπει να είναι και οι δύο περιττοί, οπότε $5X + 9Y$ και $3X + 5Y$ θα είναι άρτιοι, δηλαδή θα έχουμε

$$\left(\frac{5X + 9Y}{2}\right)^2 - 3\left(\frac{3X + 5Y}{2}\right)^2 = 1.$$

Μία λύση της $X^2 - 3Y^2 = -2$ είναι $X = 5$, $Y = 3$ οπότε

$$\frac{5X + 9Y}{2} = 26, \quad \frac{3X + 5Y}{2} = 15$$

είναι λύση της $X^2 - 3Y^2 = 1$. Από την παραπάνω ταυτότητα προκύπτει ότι

$$(5X + 9Y)^2 - 3(3X + 5Y)^2 = -2$$

και για $X = 26$, $Y = 15$ βρίσκουμε ότι

$$x = 5X + 9Y = 265, \quad \text{και} \quad y = 3Q + 5U = 153$$

είναι λύση της $x^2 - 3y^2 = -2$ οπότε

$$X = \frac{5x + 9y}{2} = 1351, \quad \text{και} \quad Y = \frac{3x + 5y}{2} = 780$$

είναι λύση της $X^2 - 3Y^2 = 1$. Συνεχίζουμε όμοια και βρίσκουμε όσες λύσεις θέλουμε.

Ένα άλλο παράδειγμα, με την ίδια μέθοδο, ίσως παλαιότερο από το προηγούμενο, το οποίο εμφανίζεται τον δεύτερο μ.Χ. αιώνα από τον **Θέωνα τον Σμυρναίο**, είναι η εύρεση διαδοχικών λύσεων της

$$X^2 - 2Y^2 = \pm 1.$$

Ξεκινούμε από την προφανή λύση $x = y = 1$ και κάνουμε διαδοχικά τις αντικαταστάσεις

$$(x, y) \mapsto (x + 2y, x + y)$$

Η μέθοδος δουλεύει εδώ λόγω της ταυτότητας

$$(x + 2y)^2 - 2(x + y)^2 = -(x^2 - 2y^2)$$

η οποία προκύπτει από την (1.4) για $N = 2$, $Z = T = 1$.

Ίχνη των ταυτοτήτων που μελετήσαμε υπάρχουν στον Διόφαντο αλλά και πάλι μένει αναπάντητο αν οι ταυτότητες (1.4) και (1.5) έχουν την αρχή τους στην Ελλάδα (ίσως στα χαμένα βιβλία του Διόφαντου). Σίγουρο είναι πάντως ότι η ταυτότητα (1.4) εμφανίζεται στο έργο του Ινδού μαθηματικού Brahmagupta ($7^{ος}$ μ.Χ. αιώνας) και μάλιστα σε σύνδεση με προβλήματα εύρεσης ακεραίων λύσεων της εξίσωσης $x^2 - Ny^2 = \pm m$.

Ο Γερμανός λογοτέχνης Lessing δημοσίευσε στα 1773 ένα **επίγραμμα** αποτελούμενο από 22 στίχους. Πρόκειται για ένα μαθηματικό πρόβλημα που έστειλε ο Αρχιμήδης στους μαθηματικούς της Αλεξάνδρειας.

Το πρόβλημα οδηγεί στη λύση μιάς **εξίσωσης του Pell**, δηλαδή διοφαντικής εξίσωσης της μορφής

$$x^2 - Ny^2 = 1 \text{ ή } -1.$$

Αυτό σημαίνει ότι ο Αρχιμήδης ενδιαφερόταν για λύσεις τέτοιων εξισώσεων. Πιθανόν μάλιστα να είχε βρει και τρόπο από μία λύση να βρίσκει άλλες κάτι που φυσικά προϋποθέτει τη γνώση της ταυτότητας (1.4).

Εξισώσεις του τύπου $x^2 - Ny^2 = 1$ εμφανίζονται στον Διόφαντο, αλλά αυτός ζητάει **ρητές** λύσεις, παρά το ότι εντελώς συμπωματικά βρίσκει και ακέραιες λύσεις, όπως π.χ.

για

$$N = m^2 + 1, \quad \text{βρίσκει λύσεις} \quad y = 2m,\ x = 2m^2 + 1.$$

Ξαναγυρίζουμε πίσω στον Brahmagupta και στις εξισώσεις της μορφής $x^2 - Ny^2 = m$, όπου N φυσικός και m ακέραιος. Ο Brahmagupta έγραψε την ταυτότητα (1.4) σαν κάποιο ''νόμο σύνθεσης''

$$((x, y; m), (z, t; n)) \Longrightarrow (xz \pm Nyt, xt \pm yz; mn)$$

και δείχνει πως μία λύση της $x^2 - Ny^2 = m$ μαζί με την σύνθεση μιάς λύσης $(p, q, 1)$ της $x^2 - Ny^2 = 1$ δίνει **άπειρες** λύσεις της

$$x^2 - Ny^2 = m.$$

Όμοια, αν κάποιος πάρει μία τριάδα $(x, y; m)$ και την πολλαπλασιάσει με τον εαυτό της θα βρει μία λύση (X, Y, m^2) οπότε $\left(\frac{X}{m}, \frac{Y}{m}, 1\right)$ θα είναι μία **ρητή** λύση της εξίσωσης του Pell

$$x^2 - Ny^2 = 1$$

και αν $\frac{X}{m}$, $\frac{Y}{m}$ ακέραιοι θα είναι $\left(\frac{X}{m}, \frac{Y}{m}; 1\right)$ μία τριάδα.

Γενικότερα από την τριάδα $(X, Y; M)$ παίρνουμε μία $\left(\frac{X}{m}, \frac{Y}{m}; \mu\right)$, όταν $M = \mu m^2$ και $\frac{X}{m}$, $\frac{Y}{m}$ ακέραιοι.

Αυτές οι παρατηρήσεις επέτρεψαν στον Brahmagupta να λύσει αρκετές εξισώσεις του Pell $x^2 - Ny^2 = 1$ (όπως π.χ. για $N = 92,\ N = 83$) και να δώσει κάποιο ''κανόνα'' λύσεως αν είναι γνωστή μία λύση της $x^2 - Ny^2 = m$ όπου $m = -1, \pm 2$ ή ± 4.

Αν $(p, q; m)$ είναι μία λύση της $x^2 - Ny^2 = m$ και $m = -1, \pm 2$ τότε μία λύση της εξίσωσης του Pell είναι

$$\left(p^2 + Nq^2, 2pq; 1\right) \quad \text{ή} \quad \left(\frac{1}{2}(p^2 + Nq^2), pq; 1\right) \quad \text{αντιστοίχως.}$$

Αν τώρα p **άρτιος** και $m = \pm 4$ τότε λύση είναι η $(\frac{1}{4}(p^2 + Nq^2), \frac{1}{2}pq; 1)$.

Αν όμως p **περιττός** τότε θα πρέπει να σχηματίσουμε την σύνθεση της $(p,q;m)$ με τον εαυτό της δύο φορές, δηλαδή

$$(p,q;m)\circ(p,q;m)\circ(p,q;m)=(P,Q,\pm 1)$$

και, αν το αποτέλεσμα είναι $(P,Q,-1)$, να ξανασυνθέσουμε την $(P,Q;-1)$ με τον εαυτό της.

Ο Brahmagupta δίνει τύπους οι οποίοι αποτελούνται από πολυώνυμα ως προς p και q, βαθμού 3 στην πρώτη περίπτωση και βαθμού $6^{ου}$ στη δεύτερη περίπτωση.

Οι παραπάνω παρατηρήσεις του Brahmagupta απέχουν πολύ από το να δώσουν γενική λύση. Μιά μέθοδος εύρεσης της γενικής λύσης εμφανίζεται τον 11^o αιώνα απο τον Jayadera (Ινδία) και σχεδόν πανομοιότυπη από τον Bhāskara ($12^{ος}$ αιώνας). Η μέθοδος αυτή λέγεται μέθοδος της **κυκλικής διαδικασίας (cakravāla)**. Όπως σε πολλές σπουδαίες ανακαλύψεις έτσι και στην περίπτωση της κυκλικής διαδικασίας μπορεί κανείς εκ των υστέρων να παρατηρήσει ότι ήταν φυσιολογική εξέλιξη των ήδη υπαρχόντων αποτελεσμάτων.

Για δοσμένο N, υποθέτουμε ότι έχουμε μία τριάδα $(p,q;m)$, όπου m "σχετικά" μικρός. Θέλουμε τώρα να βρούμε μία άλλη λύση. Κατασκευάζουμε μία τριάδα $(x,y;M)$ με $M=mm'$ και m' μικρό. Παίρνουμε τώρα το γινόμενο

$$(p,q;m)\circ(x,y;M)=(X,Y;m^2m').$$

Αν συμβεί $m|X$ και $m|Y$ τότε έχουμε μία τριάδα $(p',q';m')$, όπου $p'=\dfrac{X}{m},\ q'=\dfrac{Y}{m}$. Συνεχίζουμε ομοίως με την ελπίδα να καταλήξουμε σε μία τριάδα $(u,v;1)$.

Στην cakravāla αυτό επιτεύχθηκε ως εξής. Παίρνουμε $y=1$, οπότε $M=x^2-N$ και ζητούμε κατάλληλη εκλογή. Το γινόμενο των τριάδων τώρα είναι:

$$(p,q;m)\circ(x,1;M)=(X,Y;Mm) \text{ με } X=px+Nq,\ Y=p+qx.$$

Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $(q,m)=1$ διότι αν $(q,m)>1$, έπεται ότι $d=(p,q)>1$ οπότε λόγω της $p^2-Nq^2=m\Rightarrow d^2|m$ και η τριάδα (p,q,m) μπορεί να αντικατασταθεί από την $\left(\dfrac{p}{d},\dfrac{q}{d};\dfrac{m}{d^2}\right)$.

Διαλέγουμε τώρα το $x \pmod m$ έτσι ώστε

$$Y = p + qx \equiv 0 \pmod m.$$

Η λύση των ισοδυναμιών ήταν πολύ πιο νωρίτερα γνωστή. Γράφουμε

$$q^2 M \;=\; q^2x^2 - Nq^2 \;=\; q^2x^2 - p^2 + m \;=\; m \cdot \left(\frac{qx+p}{m} \cdot (qx-p) + 1 \right)$$

και βλέπουμε αμέσως ότι $m|M$ διότι $(q,m) = 1$.

Από τη σχέση τώρα $X^2 = NY^2 + mM \Rightarrow m^2|X^2$, συνεπάγεται ότι $m|X$. Κατ' αυτό τον τρόπο κατασκευάσαμε μία καινούργια τριάδα $(p', q'; m')$, $X = mp'$, $Y = mq'$, $M = mm'$.

Για να φτιάξουμε το m' μικρό διαλέγουμε από την κλάση του $x \pmod m$ σαν αντιπρόσωπο εκείνο το X για το οποίο ισχύει $X < \sqrt{N} < X + |m|$. Υποθέτουμε ότι ο m είναι σχετικά μικρός, δηλαδή ότι $|m| < 2\sqrt{N}$. Αυτό σημαίνει ότι $\sqrt{N} + Q \geq 0$, οπότε

$$0 < M = N - x^2 = (\sqrt{N} - x)(\sqrt{N} + x) < 2|m|\sqrt{N} \implies |m'| < 2\sqrt{N}.$$

Εφαρμόζουμε την ίδια διαδικασία στην τριάδα (p', q', m') και βρίσκουμε μία άλλη τριάδα $(p'', q''; m'')$ με $|m''| < 2\sqrt{N}$ και ούτω καθ' εξής. Επειδή οι ακέραιοι $m, m', m'', \cdots$ είναι φραγμένοι, θα πρέπει να επαναλαμβάνονται και γι' αυτό ίσως ονομάζεται η διαδικασία **κυκλική**. Φυσικά οι Ινδοί γνώριζαν την μέθοδο μόνο πειραματικά. Δεν υπάρχει τίποτα που να δείχνει ότι είχαν αποδείξεις. Ακόμα, για να δουλέψει η μέθοδος, χρειαζόμαστε μία τριάδα $(p, q; m)$ με $|m| < 2\sqrt{N}$ σαν αρχή. Σαν τέτοια τριάδα αυτοί έπαιρναν $(p_0, 1; m_0)$ όπου p_0^2 είναι το πιο κοντινό στο N τέλειο τετράγωνο είτε από πάνω είτε από κάτω του N, οπότε $|m_0| < 2\sqrt{N}$.

Όταν ο Fermat άρχισε την "καριέρα" του σαν αριθμοθεωρητικός λίγα είχε στην διάθεσή του για μελέτη. Εκτός από τα Στοιχεία του Ευκλείδη είχε ακόμη τα Αριθμητικά του Διόφαντου στη έκδοση του Bachet και την παρουσίαση μεγάλου μέρους του έργου του Διόφαντου μέσα στα Zetetica του Viéte.

Τα πιό πολλά από τα προβλήματα του Διόφαντου ανάγονται στην εύρεση κάποιου σημείου με θετικές **ρητές** συντεταγμένες μιάς **αλγεβρικής καμπύλης γένους** 0 ή 1 που δίνεται

από μία ή περισσότερες εξισώσεις. Εδώ παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο βιβλίο: Γιάννη Α. Αντωνιάδη, Αριθμητική Ελλειπτικών Καμπυλών, το Θεώρημα του Mordell, Έκδοση ΕΠΕΑΕΚ ''ΠΡΟΜΗΘΕΑΣ'', Ηράκλειο 1999.

Υπάρχουν όμως και άλλα προβλήματα των αριθμητικών που ασχολούνται με διάφορα θέματα. Σε ένα πρόβλημα ρωτάει ο Διόφαντος πότε ένας αριθμός $A = 2a + 1$ μπορεί να παρασταθεί σαν άθροισμα δύο τετραγώνων ($A = x^2 + y^2$). Σε άλλο έχουμε το αντίστοιχο πρόβλημα για το εάν ένας αριθμός της μορφής $A = 3a + 1$ γράφεται σαν άθροισμα τριών τετραγώνων $A = x^2 + y^2 + z^2$. Η απάντηση του Διόφαντου είναι ότι θα πρέπει $A \neq 8n+7$.

Σε άλλα προβλήματα υποθέτει ότι κάθε δοσμένος φυσικός αριθμός μπορεί να γραφεί σαν άθροισμα τεσσάσων τετραγώνων φυσικών αριθμών. Ίσως αυτό δεν είναι ιδιαίτερη έκπληξη, διότι ισχύει για τα αριθμητικά δεδομένα αυτών των προβλημάτων.

Η απάντηση λοιπόν στο ερώτημα τι ήξερε ο Διόφαντος και οι προγενέστεροί του σχετικά με το πρόβλημα της παράστασης ενός φυσικού αριθμού σαν άθροισμα 2, 3 ή 4 τετραγώνων θα μπορούσε να ήταν ότι είχε **πειραματική** βάση.

Οι πρώτες αποδείξεις σχετικά με το πρόβλημα της παράστασης φυσικού αριθμού μέσω τετραγωνικών μορφών ανήκουν στον Fermat. Αλλά περί αυτού στο επόμενο κεφάλαιο.

Κεφάλαιο 2

Pierre de Fermat (1601-1665)

Γεννήθηκε στην Beaumont de Lomagne, μικρή πόλη της νότιας Γαλλίας, όχι πολύ μακριά από την πόλη Toulouse, στα 1601. Πριν το 1631 πέρασε μερικά από τα χρόνια της ζωής του στο Bordeaux. Στα 1631 διορίστηκε σύμβουλος (councilor) στο ''Κοινοβούλιο'' της Τουλούζης, θέση πού αντιστοιχεί σήμερα με αυτή του ανωτάτου διοικητικού υπαλλήλου. Στη θέση αυτή έμεινε μέχρι τον θάνατό του (12 Ιανουαρίου 1665). Το επάγγελμά του τού άφηνε πολύ χρόνο να ασχοληθεί με τα Μαθηματικά. Πήρε πολύ καλή κλασική παιδεία. Γνώριζε άριστα Λατινικά, Ελληνικά, Ιταλικά και Ισπανικά. Την εποχή αυτή ζωντανή επιστημονική ζωή έχει η Ιταλία (Galileo, Cavalieri, Ricci, Torricelli). Αρκετοί φίλοι του (Carcavi, Mersenne) επισκέφθηκαν την Ιταλία. Αυτός ποτέ δεν έφυγε μακριά από την περιοχή που ζούσε. Δεν έχουμε ακριβή στοιχεία για το πότε άρχισε να ενδιαφέρεται για τα Μαθηματικά, αλλά αυτό θα πρέπει να έγινε στα τέλη της δεκαετίας του 1620 στο Bordeaux. Εκεί έγινε φίλος με τον δικαστή (magistrate), Etienne d' Espagnet. Υποτίθεται ότι αυτός τον ενθάρρυνε στα πρώτα (μαθηματικά) του βήματα. Είχε στην κατοχή του μη δημοσιευμένη εργασία του Viéte και την παρέδωσε στον Fermat. Πιθανόν να κατείχε την πλήρη συλλογή του έργου του Viéte, κάτι που ήταν δύσκολο να βρεθεί στην εποχή αυτή.

Τουλάχιστον μέχρι το 1638 ο Fermat ανταλλάσσει σκέψεις γύρω από τα Μαθηματικά με τον Beaugrand. Γίνεται φίλος με τον Pierre Carcavi ο οποίος από το 1632 μέχρι το 1636

έμεινε στην Τουλούζη. Στα 1636 ο Carcavi πήρε μετάθεση για το Παρίσι και προσχώρησε στον κύκλο των Mersenne, E. Pascal και Roberval. Την περίοδο αυτή αρχίζει και η αλληλογραφία του Fermat με τον Mersenne. Πολλά από τα Μαθηματικά του Fermat περιέχονται στην αλληλογραφία του με τον Mersenne. Όσο ζούσε ήθελε να εκδώσει ένα βιβλίο μαθηματικού περιεχομένου, αλλά τελικά δεν κατάφερε να πραγματοποιήσει το όνειρό του. Ο γιός του, Samuel Fermat εξέδωσε τα Αριθμητικά του Διόφαντου (έκδοση Bachet's του 1621) μαζί με τις παρατηρήσεις που είχε προσθέσει ο Πατέρας του στο περιθώριο του βιβλίου. Στον τόμο αυτό πρόσθεσε ο Ιησουΐτης Jacques de Billy, φίλος του Bachet και δάσκαλος των Μαθηματικών στην Dijon, μία "διατριβή" 36 σελίδων, την **Doctrinae Analyticae Inventum Novum** η οποία στηριζόταν σε αποσπάσματα της αλληλογραφίας του Fermat.

Στα 1679 ακολούθησε η έκδοση του Varia Opera (αποτελείται από γραπτά του Fermat σχετικά με Γεωμετρία, Αλγεβρα, Διαφορικό και Ολοκληρωτικό Λογισμό και γράμματά του προς Mersenne, Roberval, Etienne Pascal, Frenicle, Blaise Pascal, Carcavi, Digby, Gassendi). Πολλά από τα γράμματα του Fermat δεν περιέχονται στην συλλογή για τον προφανή λόγο ότι δεν στάλθηκαν από τους αποδέκτες στον γιό του Fermat, Samuel.

Σήμερα, με την δημοσίευση των άπαντων του Fermat από τους P. Tannery και Ch. Henry (Παρίσι 1891-1912) 4 τόμοι, το Συμπλήρωμα (Supplement) του C. de Waard, 1922 και του J. E. Hofmann, Neues über Fermats Zahlentheoretische Herausforderungen του 1657, Abh. Preuss Akad. d. Wissenschaften 1943-44, είμαστε σχεδόν πεπεισμένοι ότι κατέχουμε το σύνολο του έργου του Fermat.

Το στύλ της δουλειάς του Fermat είναι αργό, τα γράμματά του, τα οποία περιέχουν όλες τις σπουδαίες εργασίες του στην Θεωρία Αριθμών, είναι λακωνικά και ξερά. Ποτέ δεν έδωσε αποδείξεις και μόνο μία φορά υποδεικνύει τη μέθοδο της απόδειξης. Αυτό καθιστά δύσκολο τον καθορισμό των προτάσεων που πράγματι απόδειξε και εκείνων που ήταν **εικασίες** στηριγμένες στον υπολογισμό παραδειγμάτων. Θα δούμε ότι πολλά από τα θεωρήματά του δεν μπορούν να αποδειχθούν εύκολα και ότι πρώτης τάξεως μαθηματικοί όπως ο Euler κοπίασαν αρκετά για να τα αποδείξουν. Από την άλλη μεριά δεν υπάρχει

αμφιβολία ότι ο Fermat γνώριζε τις αποδείξεις των πιό πολλών θεωρημάτων του. Στη συνέχεια θα αναφερθούμε σε μερικά από τα προβλήματα με τα οποία ασχολήθηκε ο Fermat.

F. 1 Ίσως οι δυωνυμικοί συντελεστές να ανήκουν πιο πολύ στην Αλγεβρα παρά στην Θεωρία Αριθμών παρά το ότι ο Fermat περιγράφοντας ένα από το πρώτα του αποτελέσματα σχετικά με δυωνυμικούς συντελεστές σημειώνει ότι:

> **''δύσκολα μπορεί να βρεθεί ποιό όμορφο και πιό γενικό θεώρημα των αριθμών.''**

Οι συνδιασμοί ορίζονται από τον αναδρομικό τύπο

$$\binom{n+m}{m+1} = \binom{n+m-1}{m} + \binom{n+m-1}{m+1} = \sum_{r=1}^{n} \binom{r+m-1}{m}$$

και το θεώρημα του Fermat δεν είναι τίποτε περισσότερο από την ταυτότητα

$$n\binom{n+m-1}{m-1} = m\binom{n+m-1}{m}.$$

Αργότερα, στα 1654, η ταυτότητα αυτή βρήκε εφαρμογή σε αποτελέσματα του Fermat στη Θεωρία Πιθανοτήτων. Στη δεκαετία όμως του 1630 ο Fermat την χρησιμοποιεί για να υπολογίσει αθροίσματα του τύπου

$$S_m(N) = \sum_{n=1}^{N} n^m$$

ή, πιο γενικά, αθροίσματα της μορφής

$$\sum_{n=1}^{N} (an+b)^m.$$

Συνδυάζοντας τη σχέση

$$\binom{N+m}{m+1} = \sum_{n=1}^{N} \binom{n+m-1}{m}$$

με το θεώρημά του, έγραψε

$$\begin{aligned} \binom{n+m-1}{m} &= \frac{1}{m!} n(n+1)\cdots(n+m-1) \\ &= \frac{1}{m!}(n^m + A_1 n^{m-1} + \cdots + A_{m-1}^n) \end{aligned}$$

με (αριθμητικούς) συντελεστές $A_1, A_2, \cdots, A_{m-1}$, οπότε

$$S_m(N) + A_1 S_{m-1}(N) + \cdots + A_{m-1} S_1(N) = \frac{1}{m+1} N(N+1)\cdots(N+m)$$

και επομένως, εφαρμόζοντας επαγωγή ως προς m, μπορούμε να βρούμε τους τύπους των αθροισμάτων $S_m(N)$. Για $m = 2$, ο τύπος ήταν γνωστός στον Αρχιμήδη και για $m = 3$ στον Bachet. Ο **Jacob Bernoulli** έκανε αργότερα την ίδια ανακάλυψη που τον οδήγησε στον ορισμό των σήμερα γνωστών **αριθμών του Bernoulli** και **πολυωνύμων του Bernoulli** των οποίων η σπουδαιότητα για την Θεωρία των Αριθμών εμφανίζεται αργότερα με τη δουλειά του Euler.

F. 2 Στα 1640 ο Frenicle ρώτησε τον Fermat (μέσω Mersenne) αν υπάρχουν τέλειοι αριθμοί ανάμεσα στους 10^{20} και 10^{22}. Φυσικά το ερώτημα αφορούσε άρτιους τέλειους αριθμούς, δηλαδή αριθμούς της μορφής:

$$2^{n-1}(2^n - 1),$$

μία και δεν ήταν γνωστοί περιττοί τέλειοι αριθμοί (όπως και σήμερα!).

Η $10^{20} < 2^{n-1}(2^n - 1) < 10^{22}$ μας δίνει $34 \leq n \leq 37$. Για να είναι ο $2^{n-1}(2^n - 1)$ τέλειος, θα πρέπει ο $2^n - 1$ να είναι πρώτος. Επειδή δε ο $2^n - 1$ δεν είναι πρώτος για n σύνθετο, ο Frenicle ουσιαστικά ρώτησε αν ο $2^{37} - 1$ είναι πρώτος. Ο Fermat βρήκε ότι

$$2^{37} - 1 = 137438953471 = 223 \cdot 616318177$$

και επομένως δεν υπάρχει τέλειος αριθμός εκεί ανάμεσα στα 10^{20} και 10^{22}.

Η μέθοδος που εφάρμοσε για να παραγοντοποιήσει τον αριθμό $2^{37} - 1$ περιγράφεται από τον ίδιο στον Mersenne (Ιούνιος 1640). Βοηθήθηκε από τις παρακάτω προτάσεις:

I. Αν ο n δεν είναι πρώτος, τότε ο $2^n - 1$ είναι σύνθετος.

II. Αν ο n είναι πρώτος, τότε $2n | 2^n - 2$.

III. Αν ο n είναι πρώτος και p πρώτος διαιρέτης του $2^n - 1$, τότε $n | p - 1$.

Η Ι είναι προφανής. Οι ΙΙ και ΙΙΙ είναι τυπικές περιπτώσεις αυτού που σήμερα λέμε **Μικρό Θεώρημα του Fermat**:

> **''Αν p πρώτος αριθμός και $1, a, a^2, \cdots$ τυχούσα γεωμετρική πρόοδος τότε ο p διαιρεί κάποιον αριθμό της μορφής $a^n - 1$ με $n|p-1$. Αν τώρα N είναι οποιοδήποτε πολλαπλάσιο του ελάχιστου φυσικού n για τον οποίο ισχύει η παραπάνω πρόταση τότε $p|a^N - 1$.''**

Η αλήθεια αυτής της πρότασης επαληθεύτηκε κατ' αρχήν **πειραματικά** (π.χ. για $a = 2$). Πειραματικά την επαλήθευσε και ο Leibnitz (ανάμεσα στα 1676-1680), το ίδιο έκανε και ο Euler στα 1731. Δύσκολα θα μπορούσε να αμφιβάλλει κανείς ότι ο Fermat ακολούθησε και αυτός την παραπάνω πειραματική μέθοδο, παρά το ότι στα 1640 ισχυρίζεται ότι έχει μία απόδειξη την οποία θα έστελνε στον **Frenicle** αν δεν φοβόταν ότι θα ήταν αρκετά μακροσκελής.

Υπάρχουν δύο αποδείξεις του μικρού θεωρήματος του Fermat:

Απόδειξη 1η (Euler, 1742)

Για $a = 2$:

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + 1$$

Εύκολα αποδεικνύεται ότι

$$p \mid \binom{p}{\lambda}, \ \forall \lambda = 1, 2, \ldots, p-1.$$

Άρα $2^p \equiv 2 (\mathrm{mod}\, p)$. Τώρα $(a+1)^p \equiv a^p + 1 (\mathrm{mod}\, p)$ και συνεπώς συνεχίζουμε επαγωγικά.

□

Απόδειξη 2η (Euler, 1750)

Το σύνολο των πρώτων κλάσεων υπολοίπων $(\mathrm{mod}\, p)$ αποτελεί πολλαπλασιαστική ομάδα τάξεως $p-1$. Συνεπώς για κάθε $a \in \mathbb{Z}$, $p \nmid a$, έχουμε ότι $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. □

Η δεύτερη απόδειξη είναι καλύτερη, σημειώνει ο Euler, διότι γενικεύεται στην πρόταση:

$$a \in \mathbb{Z},\ m \in \mathbb{N},\ (a,m) = 1 \Longrightarrow a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

(ϕ η γνωστή συνάρτηση του Euler).

Ο Fermat απέδειξε ότι ο $2^{37}-1$ δεν είναι πρώτος ως εξής:
Αν $p|2^{37}-1$ τότε ο 37 διαιρεί τον $p-1$, συνεπώς $p \equiv 1 \pmod{37}$ και επομένως $p \equiv 1 \pmod{74}$. Ο Fermat τώρα δοκίμασε τον $p=149$ και είδε ότι δεν διαιρεί τον $2^{37}-1$. Πήρε τον επόμενο $p=223$ και πέτυχε.

Ασκηση: Αν a^n-1 είναι πρώτος, $n>1$ και $a>1$ τότε $a=2$ και n πρώτος.

Ασκηση: Αν ο αριθμός a^n+1 είναι πρώτος και $a>1$, $n>0$ τότε ο a είναι άρτιος και ο $n=2^r$ για $r \in \mathbb{N}$.

Για $a=2$ και $n=2^r$, $r=0,1,2,3,4$ ο Fermat διαπίστωσε ότι ο $2^{2^r}+1$ είναι πρώτος $3,5,17,257,65537$. Σε ένα γράμμα του στον Frenicle στα 1640 έδωσε και τις τιμές των $2^{2^r}+1$ για $r=5$, που είναι 4294967297 και για $r=6$, που είναι 18446744073709551617 και διατύπωσε την **εικασία** ότι για κάθε φυσικό αριθμό r, ο $2^{2^r}+1$ είναι **πρώτος**.

Είναι λίγο παράξενο το ότι δεν δοκίμασε τη μέθοδο που εφάρμοσε για τον $2^{37}-1$ για να δει ότι ο $2^{32}+1$ **δεν** είναι πρώτος. Το μικρό θεώρημα του Fermat μας δίνει ότι οι πιθανοί διαιρέτες του αριθμού θα είναι της μορφής $p \equiv 1 \pmod{64}$ και συνεπώς θα έπρεπε να δοκιμάσει τους 193, 257, 449, 577, 641 κ.ο.κ, αλλά ήδη θα διαπίστωνε ότι ο 641 διαιρεί τον $2^{32}+1$ συνεπώς ο $2^{32}+1$ δεν είναι πρώτος. Πράγματι,

$$641 = 5 \cdot 2^7 + 1 \Rightarrow 5 \cdot 2^7 = 641 - 1 \Rightarrow 5^4 \cdot 2^{28} = (641-1)^4 = t \cdot 641 + 1,\ t \in \mathbb{Z}.$$

Επίσης

$$641 = 2^4 + 5^4 \Rightarrow 5^4 = 641 - 2^4 \Rightarrow (641-2^4)2^{28} \equiv 1 \pmod{641} \Rightarrow 641|2^{32}+1.$$

Για $r=6$ ισχύει: $274177|2^{64}+1$ (άσκηση).

Στις 29 Σεπτεμβρίου 1999 ο Richard Crandall ανακοίνωσε ότι σε συνεργασία με τους Ernst Meyer και Ιάσονα Παπαδόπουλο απέδειξαν ότι ο αριθμός του Fermat F_{24} είναι σύνθετος. Μέχρι στιγμής όμως κανένας πρώτος παράγοντας δεν είναι γνωστός. Ο αριθμός έχει, στο δεκαδικό σύστημα, περισσότερα από πέντε εκατομμύρια ψηφία. Μετά τον F_4 όλοι οι αριθμοί του Fermat που έχουν ελεγχθεί μέχρι σήμερα είναι σύνθετοι. Πριν

από τον F_{24} αποδείχθηκε το 1993 ότι ο F_{22} είναι σύνθετος. Για μερικούς αριθμούς του Fermat πέραν του δείκτη 24 έχει βρεθεί ότι έχουν κάποιο μικρό πρώτο παράγοντα. Ο ενδιαφερόμενος αναγνώστης μπορεί να βρει σχετικές πληροφορίες στο διαδίκτυο στην διεύθυνση:

`http://vamri.xray.ufl.edu/proths/fermat.html`

Η επόμενη πρόκληση είναι ο F_{31} ο οποίος έχει περισσότερα από 600 εκατομμύρια δεκαδικά ψηφία.

F. 3 Στα χρόνια από το 1636 μέχρι το 1640 ο Fermat ασχολείται κυρίως με διοφαντικές εξισώσεις και το πρόβλημα του αθροίσματος των δύο τετραγώνων.

Η εξίσωση $x^2 + y^2 = 2(x + y)z + z^2$ δεν έχει μη-τετριμμένες ακέραιες λύσεις. Θέτουμε $t = z + x + y$ οπότε η εξίσωση γράφεται $2x^2 + 2xy + 2y^2 = t^2$. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $(x, y, t) = 1$. Έχουμε $2|t$ οπότε x, y δεν μπορούν να είναι συγχρόνως και οι δύο άρτιοι. Αλλά $x^2+xy+y^2 = 2\cdot t'^2$, άτοπο. Δηλαδή δεν έχουμε λύση της ισοδυναμίας $\pmod 2$. Η μέθοδος αυτή είναι η πιο απλή μέθοδος για να αποδείξουμε ότι μία διοφαντική εξίσωση δεν έχει λύση.

Στα 1640 ο Fermat ισχυρίζεται (σε γράμμα του στον Roberval) ότι αν $(a, b) = 1$ **δεν** υπάρχει πρώτος αριθμός της μορφής $4n - 1$ που να διαιρεί τον $a^2 + b^2$. Η απόδειξη του Fermat θα πρέπει να ήταν η ίδια με την απόδειξη που ανακάλυψε ο Euler έναν αιώνα αργότερα, στα 1742.

Υποθέτουμε ότι ο πρώτος $p = 4n - 1$ διαιρεί τον $a^2 + b^2$, όπου $(a, b) = 1$. Προφανώς θα πρέπει $(p, a) = (p, b) = 1$. Έχουμε $a^2 \equiv -b^2 \pmod p$. Θέτουμε $m = 2n - 1$, $p - 1 = 2m$, οπότε βρίσκουμε $a^{2m} \equiv -b^{2m} \pmod p$, κάτι το οποίο όμως είναι άτοπο διότι σύμφωνα με το μικρό θεώρημα του Fermat $a^{2m} \equiv b^{2m} \equiv 1 \pmod p$.

Η περίπτωση $p = 4n + 1$ δυσκόλεψε πιο πολύ τον Fermat, όπως αργότερα και τον Euler. Στην πραγματικότητα όχι μόνο κάθε πρώτος της μορφής $4n + 1$ διαιρεί κάποιο άθροισμα της μορφής a^2+b^2, αλλά και κάθε πρώτος $p = 4n+1$ γράφεται σαν άθροισμα 2 τετραγώνων και μάλιστα κατά τρόπο **μοναδικό**.

Η πρώτη απόδειξη οφείλεται στον Euler, αλλά ο Fermat διατύπωσε αυτήν την πρόταση ήδη στα 1640. Όλες οι γνωστές αποδείξεις αρχίζουν με την απόδειξη του ότι ο -1 είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$ (όταν $p = 4n + 1$). Ο Fermat θα πρέπει να είχε στο μυαλό του μία απόδειξη ανάλογη μ' αυτήν που έδωσε ο Euler.

Απόδειξη: Έστω $p = 4n + 1$. Για οποιουσδήποτε ακεραίους x και y πρώτους προς τον p, θέτουμε $a = x^n$ και $b = y^n$ οπότε $(a^2 - b^2)(a^2 + b^2) = x^{4n} - y^{4n}$.

Σύμφωνα με το θεώρημα του Fermat

$$x^{4n} - y^{4n} = x^{p-1} - y^{p-1} \equiv 0 \,(\mathrm{mod}\, p) \Longrightarrow p|a^2 - b^2 = x^{2n} - y^{2n} \quad \text{ή} \quad p|a^2 + b^2.$$

Αν τώρα ο p δεν διαιρεί κανένα αριθμό της μορφής $a^2 + b^2$ με $(p, a) = (p, b) = 1$ θα διαιρεί όλους τους αριθμούς της μορφής $x^{2n} - y^{2n}$, συνεπώς για $y = 1$ θα είχαμε $x^{2n} \equiv 1 \,(\mathrm{mod}\, p)$ για όλους τους x, $1 \leq x \leq p - 1$. Γνωρίζουμε όμως (από Euler, Lagrange) ότι μία ισοδυναμία βαθμού d δεν μπορεί να έχει πιο πολλές από d λύσεις στο $\mathbb{F}_p$. Στην περίπτωσή μας η ισοδυναμία

$$x^{2n} \equiv 1 \,(\mathrm{mod}\, p)$$

δεν μπορεί να έχει $p - 1 = 4n$ λύσεις. □

Το αποτέλεσμα όμως για το πλήθος των λύσεων μιάς ισοδυναμίας δεν ήταν γνωστό στον Fermat. Εικάζεται ότι ο Fermat το θεώρησε σαν σωστό με βάση αριθμητικά δεδομένα. Φυσικά στη Γεωμετρία του Descartes (1636) υπάρχει η πρόταση ότι η εξίσωση $f(x) = 0$ βαθμού m, δεν έχει περισσότερες από m λύσεις στο σώμα $\mathbb{R}$. Στα 1772 ο Euler διαπίστωσε ότι η απόδειξη μεταφέρεται από το $\mathbb{R}$ στο $\mathbb{F}_p$.

Ας γράψουμε την πρόταση που χρειαστήκαμε στην εξής μορφή:

> **Έστω p πρώτος. Δεν υπάρχει m $< p - 1$ τέτοιο ώστε ο $a^m - 1$ να είναι πολλαπλάσιο του p για όλους τους ακεραίους a για τους οποίους $(a, p) = 1$.**

Στα 1749 ο Euler έδωσε μία διαφορετική απόδειξη αυτής της πρότασης. Χρησιμοποίησε τον τελεστή διαφορών

$$(Df)(x) = f(x + 1) - f(x).$$

Επαγωγικά ως προς m αποδεικνύεται ότι $D^m f(x)$ είναι γραμμικός συνδιασμός των $f(x)$, $f(x+1), \ldots, f(x+m)$ με ακεραίους συντελεστές. Αν λοιπόν για κάποιο $m < p-1$ ο p διαιρεί τον $a^m - 1$ για όλα τα a, $1 \leq a \leq p-1$ θα πρέπει να διαιρεί και το $D^m f(1)$ για $f(x) = x^m - 1$. Αλλά, όπως γνώριζε και ο Ευκλείδης (επαγωγή), $D^m f(1) = m!$ οπότε θα έπρεπε $p|m!$, που είναι άτοπο διότι $m < p-1$. □

Μία άλλη απόδειξη για τον τετραγωνικό χαρακτήρα του -1 δόθηκε από τον Lagrange στα 1771 η οποία δεν εξαρτάται από την προηγούμενη πρόταση, αλλά από το **θεώρημα του Wilson**:

$$(p-1)! \equiv -1 \pmod{p}, \text{ για κάθε πρώτο } p.$$

Για $p = 2m+1$

$$\begin{aligned} (p-1)! &\equiv (1 \cdot 2 \cdots m)(p-1)(p-2)\cdots(p-m) \\ &\equiv m!(-1)^m m! \\ &\equiv (-1)^m (m!)^2 \pmod{p} \end{aligned}$$

οπότε, αν $p = 4n+1$, έχουμε ότι $m = 2n$ δηλαδή $p|(m!)^2 + 1$.

Σε λίγο θα αποδείξουμε ότι κάθε πρώτος p της μορφής $4n+1$ γράφεται μονοσήμαντα σαν άθροισμα δύο τετραγώνων κάνοντας χρήση της αριθμητικής του σώματος $\mathbb{Q}(i)$. Βέβαια οι μιγαδικοί αριθμοί υπήρχαν ήδη στη Αλγεβρα του Bombelli του 1572 αλλά δεν υπάρχει η παραμικρή ένδειξη ότι ο Fermat μελέτησε το βιβλίο του Bombelli. Ακόμη και ένα αιώνα αργότερα ο Euler, παρά το ότι χρησιμοποίησε συχνά τους μιγαδικούς σε προβλήματα ανάλυσης, μόνο προς το τέλος της ζωής του χρησιμοποίησε μιγαδικούς και στην Θεωρία των Αριθμών. Όταν λοιπόν ο Fermat έγραφε, τα Χριστούγεννα του 1640 στον Mersenne, ότι κάθε πρώτος $p \equiv 1 \pmod{4}$ γράφεται μονοσήμαντα σαν άθροισμα 2 τετραγώνων σίγουρα είχε μία διαφορετική απόδειξη στο μυαλό του. Ευτυχώς μας έδωσε μία ιδέα της μεθόδου του αργότερα στα 1659 στην αλληλογραφία του με τον Huygens. Την μέθοδό του την ονομάζει **''μέθοδο της καθόδου''** και ισχυρίζεται ότι αν υπάρχει πρώτος $p \equiv 1 \pmod{4}$, όπου $p \neq a^2 + b^2$ τότε μπορεί να βρει πρώτο $p' < p$, $p' \equiv 1 \pmod{4}$ τέτοιο ώστε $p' \neq a^2 + b^2$ ''και ούτω καθ' εξής μέχρι να φτάσω στο 5'', άτοπο. Ο Huygens σίγουρα

κατάλαβε λίγα από τη μέθοδο. Εμείς όμως είμαστε τυχεροί διότι ο Euler (ανάμεσα στα 1742 και 1747) μας έδωσε μία απόδειξη που η ιδέα της είναι ακριβώς όμοια της ιδέας του Fermat.

Απόδειξη: Έστω p πρώτος της μορφής $p = 4n+1$. Έχουμε ήδη αποδείξει ότι υπάρχουν ακέραιοι a, b, πρώτοι προς τον p, τέτοιοι ώστε $p|a^2+b^2$. Έστω r ο μικρότερος θετικός αντιπρόσωπος της κλάσης $a \pmod p$ (το υπόλοιπο της διαίρεσης του a με τον p). Αν $r \leq 2n$ θέτουμε $a' = r$ αλλιώς ισχύει $0 < p - r \leq 2n$ οπότε θέτουμε $a' = p - r$. Όμοια κατασκευάζουμε το b' από το b και αντικαθιστούμε τα a, b με τα a', b'. Έχουμε $p|a^2+b^2$, $a > 0, b > 0$ και $a, b < \dfrac{p}{2}$ οπότε $a^2 + b^2 < \dfrac{p^2}{2}$. Το ίδιο ισχύει, αν τους αριθμούς a και b τους διαιρέσουμε με (a, b) οπότε, χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι $(a, b) = 1$. Γράφουμε $N = a^2 + b^2$. Αν q πρώτος, $q|N$, $q \neq p$ τότε

$$q < \frac{N}{p} < \frac{p^2/2}{p} = \frac{p}{2}.$$

Όμως $q|N = a^2 + b^2$ συνεπώς $q = 2$ ή $q = 4m + 1$.

Θα δείξουμε τώρα ότι:

> **Αν όλοι οι πρώτοι παράγοντες $\mathbf{q \neq p}$ του N είναι άθροισμα δύο τετραγώνων, το ίδιο ισχύει και για τον p.**

Ο Euler το απέδειξε με τις δύο παρακάτω μεθόδους.

$1^η$ μέθοδος: Λόγω της ταυτότητας

$$(a^2 + b^2)(x^2 + y^2) = (ax \pm by)^2 + (ay \mp bx)^2 \tag{2.1}$$

και επειδή $\forall q|N,\ q \neq p$, ο q γράφεται σαν άθροισμα δυο τετραγώνων, έχουμε $\dfrac{N}{p} = x^2+y^2$, οπότε:

$$p = \frac{a^2 + b^2}{x^2 + y^2} = \left(\frac{ax \pm by}{x^2 + y^2}\right)^2 + \left(\frac{ay \mp bx}{x^2 + y^2}\right)^2.$$

$2^η$ μέθοδος: Αν $N = a^2 + b^2$ και $N' = c^2 + d^2$, έχουμε $NN' = (ac + bd)^2 + (ad - bc)^2$. Η τελευταία παράσταση του NN' σαν άθροισμα δύο τετραγώνων θα λέμε ότι αποτελεί την **σύνθεση** των παραστάσεων του N και N'. Τότε ισχύει:

Για κάθε $N = a^2 + b^2$ και $q = x^2 + y^2$ πρώτος που διαιρεί τον N, ο $\frac{N}{q}$ έχει μία παράσταση της μορφής $u^2 + v^2$ τέτοια ώστε η παράσταση του N είναι η σύνθεση των παραστάσεων των $\frac{N}{q}$ και q.

Απόδειξη της πρότασης: Η ταυτότητα (2.1) δίνει

$$Nq = (ax \pm by)^2 + (ay \mp bx)^2. \tag{2.2}$$

Ο $q|Ny^2 - b^2q = a^2y^2 - b^2x^2 = (ay - bx)(ay + bx)$, συνεπώς ο q διαιρεί έναν από τους δυο αριθμούς $ay - bx$ και $ay + bx$.

Διαλέγουμε κατάλληλα το πρόσημο στην (2.2) και έχουμε ότι ο q διαιρεί το Nq και τον δεξιό όρο του αθροίσματος, άρα διαιρεί και τον αριστερό όρο. Έχουμε λοιπόν

$$ax \pm by = qu,\ ay \mp bx = qv \tag{2.3}$$

Επομένως

$$\frac{N}{q} = \frac{Nq}{q^2} = \left(\frac{ax \pm by}{q}\right)^2 + \left(\frac{ay \mp bx}{q}\right)^2 = u^2 + v^2.$$

Λύνουμε την (2.3) ως προς a και b και βρίσκουμε

$$a = ux + vy,\ b = \pm(uy - vx)$$

δηλαδή η πρόταση. □

Τώρα συνεχίζουμε όπως και πιο μπροστά. Ο p είναι ο πιο μεγάλος διαιρέτης του $N = a^2 + b^2$ με $(a, b) = 1$ και όλοι οι πρώτοι διαιρέτες του N εκτός του p είναι της μορφής $x^2 + y^2$. Εφαρμόζουμε την προηγούμενη πρόταση για κάθε πρώτο q, $q|N$, $q \neq N$ μετά για κάθε πρώτο διαιρέτη του $\dfrac{N}{q}$ διάφορο του p κ.ο.κ. μέχρι που να καταλήξουμε σε μία παράσταση του p σαν άθροισμα δύο τετραγώνων. □

Σαν τελικό συμπέρασμα από τα παραπάνω βγαίνει ότι

ο $n = s^2n'$ είναι άθροισμα δύο τετραγώνων αν και μόνον εαν κάθε πρώτος p που διαιρεί τον n' είναι $p = 2$ ή $p \equiv 1 \pmod 4$.

Ο Fermat ήδη από το 1640 θέτει το ερώτημα και για το πλήθος των παραστάσεων $N = x^2 + y^2$ όπου στο μέτρημα το **πρόσημο** των x, y και η **σειρά** τους δεν παίζουν κανένα ρόλο.

Μια παράσταση θα λέγεται **γνήσια** αν και μόνο αν $(x, y) = 1$.
Αν η παράσταση $N = x^2 + y^2$ δεν είναι γνήσια, τότε $x = dx'$, $y = dy'$, $N = d^2N'$ και x', y' είναι γνήσια παράσταση του N'. Τώρα αν ο $N = x^2 + y^2$ έχει μία γνήσια παράσταση οι περιττοί πρώτοι παράγοντές του θα πρέπει να είναι της μορφής $4n + 1$. Συγχρόνως ο N δεν μπορεί να είναι πολλαπλάσιο του 4, διότι αλλιώς θα έπρεπε $2|(x, y)$. Αν πάλι ήταν $N = 2N'$ με N' περιττό τότε κάθε παράσταση του $N' = x'^2 + y'^2$ δίνει μία παράσταση του $N = x^2 + y^2$ με $x = x' + y'$ και $y = x' - y'$ και αντιστρόφως, αν $N = x^2 + y^2$, τότε x, y περιττοί οπότε θέτουμε $x' = \dfrac{x + y}{2}$, $y' = \dfrac{x - y}{2}$ και $N' = x'^2 + y'^2$. Έχουμε δηλαδή μία αμφιμονοσήμαντη αντιστοιχία ανάμεσα στις παραστάσεις των N και N'.
Αρκεί λοιπόν να μελετήσουμε παραστάσεις περιττών ακεραίων. Η πρώτη παρατήρηση του Fermat είναι ότι αν p πρώτος ίσος με $4n + 1$ τότε έχει **μοναδική** παράσταση της μορφής

$$p = x^2 + y^2.$$

Απόδειξη: Αυτό προκύπτει αμέσως από την προηγούμενη πρόταση. Παίρνουμε $N = q$. Τότε

$$\frac{N}{q} = 1 = u^2 + v^2 \Rightarrow (u, v) = (\pm 1, 0) \text{ ή } (0, \pm 1)$$

οπότε οι τύποι $((a = ux + vy,\ b = \pm(uy - vx))$ ορίζουν την ίδια παράσταση του q μία και η (x, y) είναι, προφανώς, γνήσια. □

Από την προηγούμενη πρόταση προκύπτει ότι κάθε παράσταση ενός ακεραίου N προκύπτει σαν **σύνθεση** παραστάσεων των πρώτων παραγόντων αυτού.

Αργότερα θα αναφερθούμε σε ένα τύπο που μας δίνει το πλήθος των παραστάσεων ενός φυσικού αριθμού N σαν άθροισμα δύο τετραγώνων.

Τη μέθοδο της καθόδου (infinite descent) χρησιμοποίησε ο Fermat για να αποδείξει ότι:

Δεν υπάρχει πυθαγόρειο ορθογώνιο τρίγωνο το οποίο να έχει εμ-

βαδό τέλειο τετράγωνο ή το διπλάσιο τελείου τετραγώνου.

Ο Fermat γράφει: ''Αν το εμβαδό ενός τέτοιου τριγώνου ήταν τέλειο τετράγωνο τότε θα υπήρχε κάποιο μικρότερο με την ίδια ιδιότητα και ούτω καθ' εξής, το οποίο είναι αδύνατο.''
Απόδειξη: Έστω (x, y, z) πυθαγόρεια τριάδα, όπου $(x, y, z) = 1$. Τότε υπάρχουν $(s, t) \in \mathbb{Z} \times \mathbb{Z}$, $(s, t) = 1$, ο ένας άρτιος και ο άλλος περιττός τέτοιοι ώστε

$$x = 2st,\ y = s^2 - t^2,\ z = s^2 + t^2,\ s > t.$$

Το εμβαδό του τριγώνου με πλευρές x, y, z είναι $st(s + t)(s - t)$ όπου κάθε παράγοντας είναι πρώτος προς τους άλλους τρεις. Αν λοιπόν το εμβαδό ήταν τέλειο τετράγωνο θα έπρεπε όλοι οι παράγοντες να ήταν τέλεια τετράγωνα, συνεπώς

$$s = a^2,\ t = b^2,\ s + t = c^2,\ s - t = d^2$$

με c, d περιττούς και $(c, d) = 1$. Οι αριθμοί λοιπόν a, b και $f = cd$ είναι λύση της εξίσωσης

$$a^4 - b^4 = f^2$$

και d^2, a^2, c^2 είναι διαδοχικοί όροι αριθμητικής προόδου με λόγο $b^2 = t$. Άρα

$$2b^2 = c^2 - d^2 \Longrightarrow 2b^2 = (c - d)(c + d).$$

Επειδή δε $(c - d, c + d) = 2(c, d)$ έπεται ότι ένας από τους $c + d, c - d$ είναι της μορφής $2k^2$, οπότε μπορούμε να γράψουμε

$$c = k^2 + 2\lambda^2,\ \pm d = k^2 - 2\lambda^2,\ b = 2k\lambda$$

$$\Longrightarrow a^2 = \frac{1}{2}(c^2 + d^2) = k^4 + 4\lambda^4$$

επομένως η $(k^2, 2\lambda^2, a)$ είναι μία πυθαγόρεια τριάδα εμβαδού $(k\lambda)^2$ της οποίας η υποτείνουσα είναι μικρότερη από την υποτείνουσα z^4 του αρχικού τριγώνου και αυτό συμπληρώνει πλήρως της απόδειξη με τη μέθοδο της καθόδου.

Αν τώρα υποθέσουμε ότι το εμβαδό είναι δύο φορές κάποιο τέλειο τετράγωνο τότε γράφουμε και πάλι

$$(s + t = c^2,\ s - t = d^2) \text{ και}$$

$$(s = a^2,\ t = 2b^2)\ \text{ή}\ (s = 2a^2,\ t = b^2).$$

Επειδή c και d είναι περιττοί και $2s = c^2 + d^2$, ο s πρέπει να είναι περιττός οπότε $(s = a^2,\ t = 2b^2)$. Τότε $4b^2 = c^2 - d^2 = (c-d)(c+d)$ και, λόγω του ότι $(c+d, c-d) = 2$, έχουμε

$$c + d = 2k^2,\ c - d = 2\lambda^2,\ c = k^2 + \lambda^2,\ d = k^2 - \lambda^2$$

οπότε $x^2 = \frac{1}{2}(c^2 + d^2) = k^4 + \lambda^4$.
Το (πυθαγόρειο) τρίγωνο (k^2, λ^2, x) έχει εμβαδό $2(\frac{k\lambda}{2})^2$ και, όπως και παραπάνω, τελειώσαμε. □

Παρατηρήσεις:

- Οι εξισώσεις $x^4 \pm y^4 = z^2$ δεν έχουν μη-τετριμμένες λύσεις.
- Σε μία πυθαγόρεια τριάδα (x, y, z) δεν μπορεί x και y να είναι συγχρόνως τέλεια τετράγωνα διότι τότε το εμβαδό θα ήταν $\dfrac{xy}{2}$, το διπλάσιο ενός τετραγώνου. Τα x και z δεν μπορούν επίσης να είναι συγχρόνως τέλεια τετράγωνα διότι για $x = a^2$, $z = b^2$ θα είχαμε $b^4 - a^4 = y^2$.

Από την τελευταία παρατήρηση βγάζουμε το εξής συμπέρασμα:

> Δεν υπάρχει **τριγωνικός** αριθμός διαφορετικός του 1 ο οποίος να είναι κάποια τετάρτη δύναμη. Τριγωνικοί αριθμοί λέγονται οι αριθμοί της μορφής
>
> $$\frac{1}{2}n(n+1), \quad n = 1, 2, 3, \ldots$$

Αν λοιπόν

$$\frac{1}{2}n(n+1) = x^4 \Longrightarrow n(n+1) = 2x^4 \Longrightarrow \{n, n+1\} = \{s^4, 2t^4\}$$

οπότε θα είχαμε

$$s^4 - 2t^4 = \pm 1.$$

Αν $s > 1$, θεωρούμε το πυθαγόρειο τρίγωνο

$$a = s^2,\ b = \frac{1}{2}(s^4 - 1),\ c = \frac{1}{2}(s^4 + 1).$$

Αν $s^4 - 2t^4 = 1$, τότε a και b τέλεια τετράγωνα.
Αν $s^4 - 2t^4 = -1$, τότε a και c τέλεια τετράγωνα, κάτι που αντιφάσκει στις παραπάνω παρατηρήσεις. Αν τώρα θεωρήσουμε το τρίγωνο

$$a = s^2\lambda^2,\ b = \frac{1}{2}(s^4 - \lambda^4),\ c = \frac{1}{2}(s^4 + \lambda^4)$$

βλέπουμε ότι η εξίσωση $s^4 \pm \lambda^4 = 2\mu^2$ δεν έχει μη-τετριμμένη λύση κάτι που αντιστοιχεί στην απόδειξη που έδωσε ο Euler στα 1738.

Προτού συνεχίσουμε θα δώσουμε μία άλλη απόδειξη της πρότασης του αθροίσματος δύο τετραγώνων. Θα χρειαστούμε όμως πιο μπροστά να μελετήσουμε την περιοχή του Gauss $\mathbb{Z}[i]$.

Οι ακέραιοι του Gauss

Έστω $n \in \mathbb{N}$ και $x, y \in \mathbb{Z}$ τέτοιοι ώστε $x^2 + y^2 = n$. Γράφουμε $(x + iy)(x - iy) = n$.

Το σύνολο $\mathbb{Z}[i] = \{x + iy | x, y \in \mathbb{Z}\}$ θα το λέμε σύνολο των ακεραίων του Gauss, και τους μιγαδικούς αριθμούς της μορφής $x + iy \in \mathbb{Z}[i]$ **ακεραίους του Gauss**. Προφανώς $\mathbb{Z}[i]$ είναι ακέραια περιοχή και θα την λέμε από δω και πέρα **περιοχή του Gauss**.

Αν $\alpha = x + iy$ οποιοσδήποτε μιγαδικός, ο **συζυγής** του θα είναι ο $\alpha' = x - iy$. Ορίζουμε την **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 μία θεωρία διαιρετότητας και μονοσήμαντης ανάλυσης στην περιοχή του Gauss, εντελώς ανάλογης μ' εκείνη των ακεραίων.

Έστω $\alpha, \beta \in \mathbb{Z}[i]$. Θα 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 θα λέμε ότι ο α δεν διαιρεί τον β $(\alpha \nmid \beta)$ π.χ. $2 + i|7 + i$.

Το μέγεθος ενός ακεραίου του Gauss μετριέται μέσω της norm του. Το ανάλογο του αλγόριθμου της διαίρεσης με υπόλοιπο θα είναι:

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 ακεραίων 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 ακεραίων 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 σαν συνέπεια ο μέγιστος κοινός διαιρέτης στο $\mathbb{Z}[i]$ να **μην** είναι **μοναδικός**.

Δύο ακέραιοι του Gauss α, β θα λέγονται **συνεταιρικοί** αν και μόνο εάν υπάρχει $\varepsilon \in E(\mathbb{Z}[i])$ έτσι ώστε $\alpha = \varepsilon\beta$, δηλαδή ο α και β είναι συνεταιρικοί συνεπώς αν και μόνο αν ο α είναι κάποιος από τους $\beta, -\beta, i\beta, -i\beta$.

> **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 $\gamma\cdot$). Ισχυρίζομαι ότι ο γ είναι ένας μέγιστος κοινός διαιρέτης των α και β.

Πράγματι, το γεγονός ότι $\gamma \in S$, συνεπάγεται ότι υπάρχουν $\lambda_0, \nu_0 \in \mathbb{Z}[i]$ τέτοιοι ώστε $\gamma = a\lambda_0 + \beta\nu_0$.

Αν λοιπόν $\delta|\alpha$ και $\delta|\beta$, έχουμε $\alpha = \delta\theta,\ \beta = \gamma\zeta$ οπότε $\gamma = \delta(\theta\lambda_0 + \zeta\nu_0)$, συνεπώς $\delta|\gamma$.

Θα δείξουμε τώρα ότι κάθε στοιχείο του S (και συνεπώς και τα α, β) είναι πολλαπλάσιο του γ.
Κατ' αρχήν παρατηρούμε ότι αν $\varepsilon, \rho \in S$ και $\theta \in \mathbb{Z}[i]$ τότε $\varepsilon - \theta\rho \in S$.

Πράγματι: Έστω $\varepsilon = \alpha\lambda_1 + \beta\nu_1,\ \rho = \alpha\lambda_2 + \beta\nu_2$. Τότε

$$\varepsilon - \theta\rho = \alpha(\lambda_1 - \theta\lambda_2) + \beta(\nu_1 - \theta\nu_2) \in S.$$

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 ν και $\lambda \in \mathbb{Z}[i]$ τέτοιοι ώστε

$$\gamma = \alpha\nu + \beta\lambda.$$

Στην συνέχεια θα ορίσουμε **πρώτους** αριθμούς στην περιοχή του Gauss. Κατ' αρχάς 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 θα 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 γ ή δ είναι μονάδα, δηλαδή $\delta = \pm\pi, \pm i\pi, \pm 1, \pm i$.

Τώρα θα δείξουμε ότι:

Αν π πρώτος του $\mathbb{Z}[i]$ και α, β ακέραιοι του Gauss τότε

$$(\pi|\alpha\beta \implies \pi|a \text{ ή } \pi|\beta).$$

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 μία 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 ακεραίους του Gauss σε γινόμενο πρώτων. Οπως δεν παραγοντοποιούμε το $0, \pm 1$ στο $\mathbb{Z}$ έτσι δεν παραγοντοποιούμε $0, \pm 1, \pm i$ στον $\mathbb{Z}[i]$. Θα αποδείξουμε ότι

Κάθε ακέραιος του Gauss $\gamma \neq 0, \pm 1, \pm i$ αναλύεται σε γινόμενο πρώτων παραγόντων.

Πράγματι, θα το αποδείξουμε επαγωγικά ως προς την $N(\gamma)$. 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 norm μικρότερη της norm 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 μία ανάλυση μπορούμε να βάλουμε μονάδες μέσα στο γινόμενο, αλλά αυτήν την ανάλυση δεν θα την θεωρούμε διαφορετική. Επίσης δεν ζητούμε η σειρά των πρώτων παραγόντων να είναι η ίδια. Θα αποδείξουμε λοιπόν ότι:

Έστω γ ακέραιος του Gauss διαφορετικός των $0, \pm 1, \pm i$.

Ο γ γράφεται σαν γινόμενο πρώτων. Αν

$$\gamma = \pi_1\pi_2\cdots\pi_s = \nu_1\nu_2\cdots\nu_t$$

δύο αναλύσεις του γ σε γινόμενο πρώτων, τότε $s = t$ και, αλλάζοντας ίσως την σειρά των $\nu_1, \nu_2, \cdots, \nu_s$, έχουμε π_1, ν_1 είναι συνεταιρικοί, π_2, ν_2 είναι συνεταιρικοί, $\cdots$, π_s, ν_s είναι συναιτερικοί.

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 ακεραίους 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 την θέση, $(\pi_2,\nu_2),\ldots,(\pi_s,\nu_s)$ συνεταιρικά. □

Θα δώσουμε τώρα μία καινούργια απόδειξη του προβλήματος, ποιοί φυσικοί μπορούν να γραφούν σαν άθροισμα δύο τετραγώνων ακεραίων 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.

> Έστω π πρώτος του $\mathbb{Z}[i]$. Τότε υπάρχει **ακριβώς** ένας πρώτος του $\mathbb{Z}$, p 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 $\pi\nu=1$ άρα $\nu=\dfrac{1}{\pi}$ είναι ακέραιος του Gauss, που σημαίνει ότι ο π είναι μονάδα, άτοπο. □

Αρκεί λοιπόν να παραγοντοποιήσουμε όλους τους ακεραίους στον $\mathbb{Z}[i]$. Αν $p=2$ τότε $2=-i(1+i)^2$ και $1+i$ 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 $p=\pi\nu,\ \nu\in\mathbb{Z}[i]$. Επομένως

$$p^2=N(p)=N(\pi)N(\nu)\Longrightarrow N(\pi)=p\quad\text{ή}\quad p^2.$$

Επειδή $x^2+y^2\equiv 0,1,2\,(\mathrm{mod}\,p)$, δεν μπορεί να ισχύει $x^2+y^2=p$ όταν $p\equiv 3\,(\mathrm{mod}\,4)$. Σ' αυτή την περίπτωση θα πρέπει να ισχύει $x^2+y^2=p^2$, επομένως

$$p^2=N(p)=N(\pi)N(\nu)=p^2N(\nu)\Longrightarrow N(\nu)=1$$

δηλαδή ν μονάδα του $\mathbb{Z}[i]$. Επομένως, αν $p \equiv 3 \pmod 4$ τότε π και p είναι συνεταιρικά.

Έστω τώρα $p \equiv 1 \pmod 4$. Η ισοδυναμία $z^2 \equiv -1 \pmod p$ (1) έχει λύση. Έστω z_0 μία 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 $\frac{1}{p}z \pm \frac{1}{p}i \notin \mathbb{Z}[i]$. 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 π και π' είναι συνεταιρικά, 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 2.1 *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 $p \equiv 3 \,(mod\, 4)$, τότε $p = \pi$ είναι πρώτος και $N(\pi) = p^2$.*
- *Αν $p \equiv 1 \,(mod\, 4)$, 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 ακεραίων αριθμών που είναι norm ακεραίων 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

$$\left\{ \begin{array}{l} a_i = 2, \quad \text{αν} \quad p_i \equiv 3 \pmod 4 \\ a_i = 1, \quad \text{αν} \quad p_i = 2 \quad \text{ή} \quad p_i \equiv 1 \pmod 4 \end{array} \right\}$$

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 $1 \pmod 4$.

Ισχύει και το αντίστροφο, ότι δηλαδή κάθε τέτοιος φυσικός αριθμός γράφεται σαν άθροισμα δυο τετραγώνων. Δώσαμε επομένως μία άλλη απόδειξη της πρότασης της σελίδας 25.

Ξαναγυρίζουμε όμως πίσω στον Fermat.

F. 4 Στα 1654 ο Fermat αναφέρει μερικές από τις ανακαλύψεις του σχετικά με τους "αριθμούς" στον Pascal. Ασχολείται με τις τετραγωνικές μορφές $x^2 + 2y^2$, $x^2 + 3y^2$, αναφέρει ένα "γενικό κανόνα" εύρεσης δύο αριθμών a, b τέτοιων ώστε $p = a^2 + b^2$ (p πρώτος, $p \equiv 1 \pmod 4$) και παρατηρεί ότι

"Κάθε αριθμός της μορφής $3n + 1$ **παρίσταται από την** $x^2 + 3y^2$**"**

καθώς και ότι

"Κάθε αριθμός της μορφής $8n+1, 8n+3$ **παρίσταται από την** x^2+2y^2**."**

Γράφουμε τις ταυτότητες (1.4), (1.5), σελίδα 7 μαζί:

$$(x^2 + Ay^2)(z^2 + At^2) = (xz \pm Ayt)^2 + A(xt \mp yz)^2$$

όπου τώρα $A \in \mathbb{Z}$. Παρατηρούμε ότι η πρόταση της σελίδας 25 μεταφέρεται αυτούσια για την μορφή $x^2 + Ay^2$ και κάθε $A \in \mathbb{Z}$. Οι τύποι (2.3) της σελίδας 25 τώρα δίνουν

$$ax \pm Aby = qu, \; ay \mp bx = qv$$

$$a = ux + Avy, \; b = \pm(uy - vx).$$

Το συμπέρασμα λοιπόν είναι, όπως και πιο μπροστά για $A = 1$, ότι και για $A > 1$ ένας πρώτος q δεν μπορεί να παρασταθεί από την $x^2 + Ay^2$ κατά περισσότερους από **έναν** τρόπους διότι τότε για κάθε $N = q$ θα είχαμε $1 = u^2 + Av^2$ η οποία έχει μοναδική λύση ($u = \pm 1$, $v = 0$). Αν $A < 0$ τότε οδηγούμαστε και πάλι στην εξίσωση του Pell, $x^2 - (-A)y^2 = 1$.

Εντελώς όμοια, όπως πιο μπροστά, αποδεικνύουμε ότι αν ο πρώτος αριθμός $p|N = a^2 + Ab^2$ και αν υποθέτοντας ότι κάθε άλλος πρώτος διαιρέτης του N μπορεί να γραφτεί σαν $x^2 + Ay^2$, τότε το ίδιο ισχύει και για τον p.

Απόδειξη: Θα λέμε ότι ο περιττός πρώτος p είναι ένας **πρώτος διαιρέτης της μορφής** $x^2 + Ay^2$, αν και μόνο αν ο p διαιρεί κάποιον $N = a^2 + Ab^2$ με $(a, p) = (b, p) = 1$. Αυτό συμβαίνει τότε και μόνον τότε όταν ο $-A$ είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$.

Έστω λοιπόν p ένας τέτοιος πρώτος και a, b πρώτοι προς τον p τέτοιοι ώστε $p|a^2 + Ab^2$. Έστω r τό υπόλοιπο της διαίρεσης του a με p. Θέτουμε $a' = r$ ή $p - r$ ανάλογα με το ποιός είναι μικρότερος. Όμοια ορίζουμε το b'. Αντικαθιστούμε τα a, b με τα a', b' και διαιρούμε με το μέγιστο κοινό διαιρέτη τους. Χωρίς περιορισμό της γενικότητας λοιπόν υποθέτουμε ότι a, b είναι πρώτοι μεταξύ τους και μικρότεροι του $\dfrac{p}{2}$. Έστω $N = a^2 + Ab^2$. Αν $A = 2$ τότε $N < \dfrac{3p^2}{4}$ και επομένως όλοι οι πρώτοι διαιρέτες του N, (εκτός του p) είναι μικρότεροι του $\dfrac{3p}{4}$. Υποθέτουμε ότι όλοι αυτοί μπορούν να γραφτούν στην μορφή $x^2 + 2y^2$ (και ο 2 ανήκει σ' αυτή την κατήγορία αν N άρτιος). Εφαρμόζουμε την πρόταση της σελίδας 25 και έχουμε τελειώσει. □

Ασκηση: Κάντε το ίδιο για $A = 3, -2$. Προφανώς κάθε αριθμός της μορφής $x^2 + 3y^2$ που δεν διαιρείται με 3 είναι ισοδύναμος $1 \,(\mathrm{mod}\, 3)$ οπότε η άσκηση δίνει τη μία κατεύθυνση της:

Κάθε **πρώτος διαιρέτης** της $x^2 + 3y^2$ είναι της μορφής $3n + 1$.

Θα αποδείξουμε την άλλη κατεύθυνση της ισοδυναμίας. Γράφουμε $p = 3n+1$ και κάνουμε χρήση της

$$x^{3n} - 1 = (x^n - 1)(x^{2n} + x^n + 1).$$

Για κάθε x, για τον οποίο $(x,p)=1$ ο p διαιρεί το αριστερό μέλος (μικρό θεώρημα του Fermat). Λόγω της πρότασης της σελίδας 22 έπεται ότι υπάρχει κάποιος πρώτος x πρώτος προς τον p, τέτοιος ώστε ο p διαιρεί τον $x^{2n}+x^n+1$. Επομένως ο p διαιρεί τον $4(x^{2n}+x^n+1)=(2x^n+1)^2+3$, δηλαδή είναι ένας πρώτος διαιρέτης της x^2+3y^2. □

Στα 1657 ο Fermat πρότεινε προς λύση το ακόλουθο πρόβλημα:

> **Να βρεθεί κάποιος αριθμός που να είναι τρίτη δύναμη ακεραίου (κύβος) και το άθροισμα των διαιρετών του να είναι τέλειο τετράγωνο.**

Παράδειγμα: Ο 7^3 έχει άθροισμα διαιρετών $1+7+7^2+7^3=20^2$.

Αν λοιπόν έχουμε p^3 όπου p πρώτος αριθμός τότε για να αποτελέσει λύση στο πρόβλημα του Fermat θα πρέπει

$$1+p+p^2+p^3=(p+1)(p^2+1)=x^2,\ x\in\mathbb{Z}.$$

Αφού το 2 δεν αποτελεί λύση έπεται ότι $(p+1,p^2+1)=2$, συνεπώς

$$p+1=2s^2,\ p^2+1=2t^2$$

όπου (s,t) είναι λύση της $(2X^2-1)^2=2Y^2-1$.

Ο Fermat έγραψε στον Huygens στα 1659 ότι η τελευταία εξίσωση δεν έχει άλλες λύσεις εκτός των $(\pm1,\pm1)$ και $(\pm2,\pm5)$. Αυτό αποδείχθηκε από τον Genochi (1883) κάνοντας χρήση του γεγονότος ότι η εξίσωση

$$X^4\pm Y^4=2Z^2$$

δεν έχει μη-τετριμμένες ακέραιες λύσεις (κάτι που γνώριζε ο Euler και ίσως και ο Fermat).

Ο Fermat μελέτησε επίσης την εξίσωση του Pell $X^2-NY^2=1$, τις διοφαντικές εξισώσεις $X^2+2=Y^3$, $X^2+4=Y^3$, το πρόβλημα της εύρεσης των πλευρών ορθογωνίου τριγώνου (Q,U,Z), με Z και $Q+U$ τέλεια τετράγωνα (η πιο μικρή λύση δόθηκε από τον Fermat $Q=4565486027761$, $U=1061652293520$, $Z=4687298610289$).

Περίφημη είναι η **εικασία του Fermat** (ή και μεγάλο "θεώρημα" του Fermat) ότι η εξίσωση:

$$X^n + Y^n = Z^n, \quad n \in \mathbb{N}, n \geq 3$$

δεν έχει μη-τετριμμένη (δηλαδή για $XYZ \neq 0$), ακέραια λύση.

Η εικασία του Fermat αποδείχθηκε τελικά στα 1993 από τον A. Wiles. Η απόδειξη στηρίζεται σε μία ιδέα του G. Frey να συνδέσει το πρόβλημα με άλλο ανοιχτό πρόβλημα της θεωρίας των ελλειπτικών καμπύλων (Εικασία Shimura-Taniyama) και σε σημαντικά ενδιάμεσα αποτελέσματα των G. Frey, J.-P. Serre, K. Ribet και άλλων. Πάρα πολύ σημαντική ήταν και η συνεισφορά του Richard Taylor, μαθητή του A. Wiles, στη σωστή απόδειξη επιμέρους αποτελέσματος το οποίο δεν είχε διατυπωθεί ορθά από τον A. Wiles. Η απόδειξη έχει δημοσιευθεί το 1995 στο περιοδικό Annals of Mathematics. Για την απόδειξη της εικασίας του Fermat απαιτείται η ισχύς μέρους μόνο της εικασίας των Shimura-Taniyama. Η πλήρης εικασία Shimura-Taniyama αποδείχθηκε φέτος, το σωτήριον έτος 1999.

Κεφάλαιο 3

Leonhard Euler (1707-1783)

Ο πατέρας του Leonhard, Paul Euler είχε σπουδάσει Θεολογία στο Πανεπιστήμιο της Βασιλείας (Basel), αλλά κατά τη διάρκεια των σπουδών του παρακολουθούσε και τις παραδόσεις του Jacob Bernoulli. Επιθυμία του ήταν να γίνει και ο γυιός του παπάς όπως και ο ίδιος.

Όταν γεννήθηκε ο L. Euler στα 1707 ο Jacob Bernoulli είχε πεθάνει και τον είχε διαδεχθεί ο Johann Bernoulli, τα παιδιά του οποίου (Nicolas και Daniel) ακολούθησαν την παράδοση της οικογένειας και ασχολήθηκαν και αυτοί με τα Μαθηματικά. Ο Euler έγινε φίλος των Nicolas και Daniel Bernoulli και μαθητής του Johann Bernoulli.

Τρεις μονάρχες έπαιξαν αποφασιστικό ρόλο στην σταδιοδρομία του Euler. Ο Πέτρος ο Μέγας, ο Φρειδερίκος ο Μέγας και η Αικατερίνη η Μεγάλη. Ο Πέτρος ο Μέγας πέθανε στα 1725 ενώ είχε κάνει ήδη σχέδια για τη δημιουργία μιάς Ακαδημίας των Επιστημών, στη νέα του πρωτεύουσα την Πετρούπολη, σχέδια τα οποία εκτελέστηκαν πιστά από τη χήρα του. Το 1725 προσκλήθηκαν οι Nicolas και Daniel Bernoulli στην Πετρούπολη και τον ίδιο χρόνο έφθασε και ο Euler. Ηταν μικρότερος από 20 χρόνων αλλά είχε κερδίσει ένα βραβείο στη Ναυπηγική χωρίς να δεί ποτέ ένα πλοίο να ταξιδεύει. Στα 1733 πήρε τη θέση του Daniel Bernoulli (ο οποίος ξαναγύρισε στη Βασιλεία) στην Ακαδημία των Επιστημών. Η επιστημονική παραγωγή του, παρά τη σχετική του απομόνωση στην Πετρούπολη (λόγω

της αναχώρησης του Daniel Bernoulli) ξεπερνάει κάθε προσδοκία. Διακόπτεται για λίγο λόγω κάποιας σοβαρής ασθένειας η οποία του κοστίζει το του ένα μάτι. Η φήμη του απλώνεται σιγά-σιγά σ΄ όλη την Ευρώπη. Με το θάνατο της Τσαρίνας η Κυβέρνηση αδιαφορεί για την Ακαδημία κι έτσι ο Euler δέχεται την πρόσκληση του Φρειδερίκου του ΙΙ να γίνει μέλος της νεοϊδρυθείσης Ακαδημίας των Επιστημών της Πρωσσίας (Βερολίνο, 1741). Στο Βερολίνο ζεί 24 από τα υπόλοιπα χρόνια της ζωής του. Συγχρόνως κράτησε και την ιδιότητά του σαν μέλους της Ακαδημίας Επιστημών της Πετρούπολης. Το πλήθος των εργασιών του κατά την περίοδο αυτή ξεπερνάει τις 200. Ασχολείται με όλους τους κλάδους των καθαρών και εφαρμοσμένων Μαθηματικών. Οσο περνούσαν τα χρόνια οι σχέσεις του Euler με τον Φρειδερίκο τον ΙΙ όλο και χειροτέρευαν. Ο μονάρχης, θαυμαστής της γαλλικής κουλτούρας, ήθελε να φέρει τον d'Alembert και να τον θέσει επικεφαλής της Ακαδημίας. Από το 1763 ο Euler αρχίζει να σκέπεται να επιστρέψει στην Ρωσία. Στα 1762 ανεβαίνει στον θρόνο της Ρωσίας η Αικατερίνη η Μεγάλη. Από τους πρώτους της στόχους είναι και το να επαναφέρει την Ακαδημία στην παλιά της δόξα. Αυτό είναι σχεδόν ταυτόσημο (συνώνυμο) με την επιστροφή του Euler.

Οι διαπραγματεύσεις κρατούν τρία χρόνια. Στα 1766 ο Euler, παρά την προσπάθεια του Φρειδερίκου να τον κρατήσει (στο μεταξύ κατάλαβε τι χάνει), επιστρέφει στην Πετρούπολη.

Αυτή την περίοδο προσβάλλεται και το άλλο του μάτι από καταρράκτη και έτσι ο Euler χάνει το φώς του. Ο ίδιος, απαντώντας σε ένα γράμμα του Lagrange, στα 1770 γράφει:

> **''Μου διάβασαν όλους τους λογαριασμούς που κάνατε για να λύσετε την εξίσωση** $101 = p^2 - 13q^2$ **και είμαι απόλυτα πεπεισμένος ότι είναι σωστοί. Επειδή όμως δεν μπορώ ούτε να διαβάσω ούτε να γράψω, θα πρέπει να ομολογήσω ότι δεν μπορώ με την φαντασία μου να παρακολουθήσω την λογική όλων των βημάτων της απόδειξης, ούτε να συγκρατήσω όλους τους συμβολισμούς σας στο μυαλό μου. Είναι αλήθεια ότι η ενασχόληση με τέτοια θέματα ήταν για μένα παλαιότερα μία ιδιαίτερη ευχαρίστηση και ότι διέ-**

θεσα πολύ χρόνο ασχολούμενος μ΄ αυτά. Τώρα όμως ασχολούμαι με (θέματα) που μπορώ να κάνω με το μυαλό μου αν και συχνά θα πρέπει να υποχρεωθώ σε κάποιο φίλο για να μου κάνει τους λογαριασμούς που χρειάζομαι.''

Έζησε τα τελαυταία χρόνια της ζωής του τιμώμενος και εκτιμώμενος. Το πλήθος των εργασιών του αυτής της περιόδου ξεπερνάει κατά πολύ τις 100, αριθμός ικανός για να γεμίζει τις σελίδες του περιοδικού της Ακαδημίας για πολλά ακόμη χρόνια μετά το θάνατό του, όπως έλεγε και ο ίδιος. Πέθανε στις 18 Σεπτεμβρίου 1783.

Το έργο του Euler στη Θεωρία Αριθμών καλύπτει μόνο 4 τόμους από τους περισσότερους των 70 που καλύπτουν τα άπαντά του. Και μόνο αυτό θα ήταν αρκετό για να μείνει ο Euler στην Ιστορία της Επιστήμης σαν ένας από τους πιο μεγάλους μαθηματικούς όλων των εποχών. Η Θεωρία Αριθμών αναπτύσσεται ραγδαία τον 18^o αιώνα σε αντίθεση με τον 17^o. Μερικές από τις αποδείξεις του Euler τις έχουμε ήδη αναφέρει στο προηγούμενο Κεφάλαιο.

Το ενδιαφέρον του Euler για την Θεωρία Αριθμών αρχίζει με το ερώτημα του Goldbach (13/10/1729), αν η εικασία του Fermat ότι όλοι οι αριθμοί της μορφής $2^{2^n}+1$ είναι πρώτοι.

Λίγο αργότερα ο Goldbach ισχυρίζεται ότι απέδειξε ότι δεν υπάρχει τρίγωνος αριθμός που να είναι τέλειο τετράγωνο (δες Κεφάλαιο 2). Ο Euler βρίσκει αμέσως το λάθος. Θέτει $x = 2n+1$ και βρίσκει ότι το πρόβλημα είναι ισοδύναμο με την εύρεση λύσης της εξίσωσης του Pell $x^2 - 8y^2 = 1$, η οποία έχει προφανώς ακέραιες λύσεις π.χ. $x = 17$, $y = 6$.

Χρονολογικά τα κυριότερα θέματα με τα οποία ασχολήθηκε είναι τα εξής:

(i) Το (μικρό) θεώρημα του Fermat, η πολλαπλασιαστική ομάδα των ακεραίων $(\mathrm{mod}\, N)$ και στοιχεία της Θεωρίας Ομάδων.

(ii) Άθροισμα τετραγώνων και ''οιχειώδης'' θεωρία των τετραγωνικών μορφών.

(iii) Διοφαντικές εξισώσεις $2^{ου}$ βαθμού.

(iv) Διοφαντικές εξισώσεις $3^{ου}$ και $4^{ου}$ βαθμού.

(v) Ελλειπτικά ολοκληρώματα.

(vi) Συνεχή κλάσματα, εξίσωση του Pell και αναδρομικές ακολουθίες (σειρές).

(vii) Η ζ-συνάρτηση, η τιμή της για τιμή της μεταβλητής άρτιο φυσικό και άλλες συναρτήσεις που σχετίζονται με την ζ.

(viii) Το ''Παρτιτιο νυμερορυμ'' και τυπικές σειρές δυνάμεων.

(ix) Πρώτοι διαιρέτες τετραγωνικών μορφών.

(x) Μεγάλοι πρώτοι αριθμοί.

Με μερικά από τα παραπάνω θα ασχοληθούμε στα επόμενα.

Κάνοντας χρήση του (μικρού) θεωρήματος του Fermat και της παρατήρησης ότι για $p = 4n + 1$ πρώτο η $x^{2n} \equiv 1 \pmod p$ **δεν** επαληθεύεται για κάθε x, $1 \leq x \leq p-1$, ο Euler αποδεικνύει στα 1749 ότι:

> **Αν $p = mn + 1$ είναι πρώτος αριθμός και $p|(a^m - 1)$ τότε ο a είναι n-οστό υπόλοιπο $(\mathbf{mod}\, p)$.**

Πράγματι, αν $a^m \equiv 1 \pmod p$ και γράψουμε την ταυτότητα

$$x^{mn} - a^m \equiv (x^n - a)(x^{(m-1)n} + ax^{(m-2)n} + \cdots + a^{m-1})$$

όπου $mn = p - 1$, το μικρό θεώρημα του Fermat δίνει ότι το αριστερό μέλος είναι πολλαπλάσιο του p για όλα τα x τα πρώτα προς τον p, ενώ η πρόταση του Euler για το πλήθος των λύσεων της ισοδυναμίας μας δίνει ότι ο δεύτερος παράγοντας του δεξιού μέλους δεν μπορεί να έχει αυτή την ιδιότητα. Συνεπώς για κάποιο x (πρώτο προς τον p) θα ισχύει κατ' ανάγκη $x^n \equiv a \pmod p$.

Για $a = -1$ και $n = 2$ η πρόταση αυτή είναι αυτό που έλειπε κατά τις προηγούμενες προσπάθειες για να αποδειχθεί το θεώρημα του Fermat για το άθροισμα των δύο τετραγώνων. Παίρνοντας κουράγιο (δύναμη) από αυτή του την επιτυχία και από την επιτυχία που είχε το βιβλίο του Introductio in Analysin Infinitorum (1748), ο Euler εργάζεται πάνω στην Θεωρία Αριθμών και ετοιμάζει ένα βιβλίο, Εισαγωγή στην Θεωρία Αριθμών. Γράφει 16 ''κεφάλαια'' και σταματάει. Εκδόθηκε στα 1849 κάτω από τον τίτλο **Tractatus de numerorum doctrina**. Μοιάζει αρκετά με το περιεχόμενο των τριών πρώτων κεφαλαίων του βιβλίου του **Gauss**, **Disquisitiones Arithmeticae** (δες [5]).

Εισάγει κατ' αρχήν την ϕ (συνάρτηση του Euler) η οποία μας δίνει το πλήθος των φυσικών αριθμών των μικροτέρων προς το n και πρώτων προς τον n. Στη συνέχεια ακολουθεί μία στοιχειώδης περιγραφή αυτού που ο Gauss αργότερα ονομάζει **ισοδυναμία** ως προς ένα modulus. Η αντίστοιχη λέξη του Euler είναι ''ο διαιρέτης''. Για κάποιο διαιρέτη d, όλοι οι ακέραιοι $r + dx$ θα λέμε ότι ανήκουν στην ίδια ''κλάση'' και θα θεωρούνται ως ''ισοδύναμοι''. Κάθε αντιπρόσωπος της κλάσεως ενός ακεραίου a θα καλείται ''ένα υπόλοιπο'' του a. Η απεικόνιση του a στην κλάση του έχει ιδιότητες τέτοιες που σήμερα ορίζουν τον ομομορφισμό δακτυλίων.

Για κάποιο διαιρέτη d σχηματίζουμε την αριθμητική πρόοδο $a, a+b, a+2b, \cdots$ (σε σύγχρονη γλώσσα, τις πλευρικές ομάδες της υποομάδας που παράγεται από το b στην προσθετική ομάδα $(\mathrm{mod}\, d)$). Έτσι βρίσκει το μέγιστο κοινό διαιρέτη των b και d και λύνει την ισοδυναμία $bx \equiv m\,(\mathrm{mod}\, d)$. Στη συνέχεια ερευνά την πολλαπλασιαστική ομάδα $(\mathrm{mod}\, d)$ και δείχνει ότι αν $(b, d) = 1$ τα υπόλοιπα που παίρνουμε από την $1, b, b^2, \cdots$ σχηματίζουν σύνολο κλειστό προς τον πολλαπλασιασμό και την διαίρεση $(\mathrm{mod}\, d)$, δηλαδή ότι αυτή η ομάδα περιέχεται στην ομάδα των ακεραίων $(\mathrm{mod}\, d)$ πρώτων προς τον d και καταλήγει στην

$$d \mid b^{\phi(d)} - 1,$$

το γνωστό **θεώρημα του Euler**.

Εδώ ξαναθυμίζουμε ότι ο Euler παρατήρησε ότι η απόδειξη του Descartes, ότι μία εξίσωση $f(x) = 0$ βαθμού n έχει το πολύ n ρίζες, μεταφέρεται σε οποιοδήποτε σώμα.

Αν a ρίζα της $f(x) = 0$ διαιρούμε το $f(x)$ με $x - a$ και γράφουμε $f(x) = (x - a)f_1(x)$. Οι ρίζες της $f(x) = 0$ είναι $x = a$ και οι ρίζες της $f_1(x) = 0$. Ο βαθμός $\deg f_1(x) = n-1$ (και κάνοντας χρήση της μαθηματικής επαγωγής), τελειώσαμε.

Ο Euler παρατηρεί ότι αν a είναι μία λύση της ισοδυναμίας $f(x) \equiv 0 \pmod p$, τότε γράφουμε $f(a) = mp$, $m \in \mathbb{Z}$ οπότε το a είναι μία ρίζα της εξίσωσης $f(x) - mp = 0$. Γράφουμε λοιπόν $f(x) - mp = (x - a)f_1(x)$ και συνεχίζουμε επαγωγικά.

Το θεώρημα αυτό χρησιμοποιείται στη συνέχεια για να αποδείξει την ύπαρξη **πρωταρχικών ριζών** $(\mathrm{mod}\, p)$.

Όλη του την ζωή ενδιαφερόταν για την παράσταση των φυσικών αριθμών σαν άθροισμα 2 τεραγώνων ή μέσω τετραγωνικών μορφών της μορφής $X^2 + NY^2$ ή ακόμα γενικότερα της μορφής $\mu X^2 + \nu Y^2$ με $N, \mu, \nu \in \mathbb{Z}$. Με τη γενική περίπτωση $aX^2 + bXY + CY^2$ ασχολήθηκε μόνο τα τελευταία χρόνια της ζωής του και μάλιστα ύστερα από επίδραση του Lagrange ο οποίος ασχολήθηκε εντατικά μ' αυτή. Με την παράσταση φυσικών αριθμών μέσω τετραγωνικών μορφών θα ασχοληθούμε αργότερα.

Εδώ αναφέρουμε μόνο την απλή παρατήρηση του Fermat ότι

- ούτε ο $4mn - m - 1$
- ούτε ο $4mn - m - n - 1$, $m, n \in \mathbb{N}$

μπορούν να είναι τέλειο τετεράγωνο, έστω a^2, διότι αυτό θα είχε σαν συνέπεια

$$m(4n - 1) = 1 + a^2,\ (4m - 1)(4n - 1) = 1 + 4a^2,$$

δηλαδή κάποιος αριθμός της μορφής $4n - 1$ θα διαιρούσε ένα άθροισμα δύο τετραγώνων $x^2 + y^2$ με $(x, y) = 1$ κάτι που είναι αδύνατο και που ήταν ήδη γνωστό στον Fermat.

Στα γράμματά του ο Euler ασχολείται με τη δυνατότητα παράστασης ενός φυσικού αριθμού σαν άθροισμα τριών ή τεσσάρων τετραγώνων. Πραγματική πρόοδο κάνει σ' αυτά τα προβλήματα το 1747 όταν ανακαλύπτει ότι το γινόμενο δύο αριθμών που είναι άθροισμα τεσσάρων τετραγώνων είναι επίσης άθροισμα τεσσάρων τετραγώνων. Ισχύει λοιπόν η ταυτότητα:

Αν

$$m = a^2 + b^2 + c^2 + d^2 \ \text{ και } \ n = p^2 + q^2 + r^2 + s^2$$

τότε

$$mn = A^2 + B^2 + C^2 + D^2,$$

όπου

$$A = ap + bq + cr + ds,\ B = aq - bp - cs + dr,$$
$$C = ar + bs - cp - dq,\ D = as - br + cq - dp.$$

Προφανώς ισχύει και

$$\frac{m}{n} = \left(\frac{A}{n}\right)^2 + \left(\frac{B}{n}\right)^2 + \left(\frac{C}{n}\right)^2 + \left(\frac{D}{n}\right)^2.$$

Τον επόμενο χρόνο έχει ήδη λύσει το πρόβλημα του αθροίσματος δύο τετραγώνων και προσπαθεί να αποδείξει ότι

> **Κάθε φυσικός αριθμός γράφεται σαν άθροισμα τεσσάρων τεραγώνων**

κάνοντας χρήση της μεθόδου που χρησιμοποίησε για το άθροισμα δύο τετεραγώνων και της παραπάνω ταυτότητας που έχει ανακαλύψει. Στην αρχή αποδεικνύει ότι κάθε **πρώτος** p **διαιρεί** κάποιο άθροισμα τεσσάρων τετραγώνων. Αποδεικνύει κάτι παραπάνω, ότι δηλαδή για κάθε πρώτο p η ισοδυναμία

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p}$$

έχει μία **μη τετριμμένη** λύση (δηλ. $(x, y, z) \neq (0, 0, 0)$) και, λίγο αργότερα, γενικεύει, αποδεικνύοντας ότι η ισοδυναμία

$$\lambda x^2 + \mu y^2 + \nu z^2 \equiv 0 \pmod{p}$$

έχει **μη τετριμμένη** λύση.

Η παρατήρηση του Euler είναι ότι η συνάρτηση $x \mapsto \lambda x^2 \pmod p$ παίρνει $\frac{p+1}{2}$ διαφορετικές τιμές (την τιμή 0 και $\frac{p-1}{2}$ μη-ισοδύναμα τετραγωνικά υπόλοιπα $\pmod p$ (δες [2]). Το ίδιο κάνει και η συνάρτηση $x \mapsto -\mu x^2 - \nu$. Αν όλες οι λύσεις ήταν μεταξύ τους διαφορετικές τότε η ισοδυναμία θα είχε περισσότερες από p λύσεις, άτοπο. Άρα υπάρχει μία κοινή λύση, δηλαδή μία μη-τετριμμένη λύση $(x, y, 1)$ της ισοδυναμίας $\lambda x^2 + \mu y^2 + \nu z^2 \equiv 0 \pmod p$.

Στη συνέχει προσπαθεί να δείξει ότι κάθε πρώτος p που διαιρεί ένα άθροισμα $a^2+b^2+c^2+d^2$ με $(a, b, c, d) = 1$ (μερικοί από τους a, b, c, d μπορεί να είναι 0) είναι και ο ίδιος άθροισμα τεσσάρων τετραγώνων. Αυτό που καταφέρνει είναι να αποδείξει ότι είναι άθροισμα τεσσάρων **ρητών** τετραγώνων.

Πράγματι, έστω ότι αυτό δεν ισχύει και έστω p ο ελάχιστος πρώτος που **δεν μπορεί** να γραφτεί σαν άθροισμα τεσσάρων ρητών τετραγώνων. Έστω (a, b, c) μία μη-τετριμμένη λύση της $x^2 + y^2 + z^2 \equiv 0 \pmod p$. Οπως και στο άθροισμα δύο τετραγώνων μπρούμε να υποθέσουμε ότι $0 \le a, b, c < \frac{p}{2}$. Θέτουμε $N = a^2 + b^2 + c^2 = pN'$, οπότε $N < \frac{3}{4}p^2$ και $N' < p$. Όλοι οι πρώτοι παράγοντες του N' είναι μικρότεροι του p. Συνεπώς γράφονται σαν άθροισμα τεσσάρων ρητών τετραγώνων και συνεπώς και ο N', λόγω της γνωστής ταυτότητας, οπότε $p = \frac{N}{N'}$, άθροισμα τεσσάρων ρητών τετραγώνων.

Στα 1772 (περισσότερο από 20 χρόνια αργότερα) πήρε ο Euler την πλήρη απόδειξη που του έστειλε ο **Lagrange**. Ο Euler ξαναπιάνεται με το θέμα και σε μία θαυμάσια εργασία στο **Nova Acta Eruditorium** του 1773, αφού συγχαίρει κατ' αρχήν τον Lagrange για την επιτυχία του και αφού χαρακτηρίζει την απόδειξη του Lagrange **"far-fetched and laborious"** δίνει την δική του κομψή απόδειξη.

Απόδειξη: Έστω p περιττός πρώτος ο οποίος διαιρεί το $\sum_{i=1}^{4} a_i^2$, $(a_1, a_2, a_3, a_4) = 1$ και $0 \le a_i < \frac{p}{2}$. Γράφουμε $\sum_{i=1}^{4} a_i^2 = pm$ και έχουμε $m < p$. Αν $m = 2$ τότε θα πρέπει δύο από τους a_i να είναι άρτιοι και δύο περιττοί, οπότε

$$p = \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2.$$

Έστω τώρα ότι $m > 2$. Για κάθε i γράφουμε

$$a_i = b_i + mc_i,\ |b_i| \leq \frac{m}{2}.$$

$$\sum_{i=1}^{4} b_i^2 \equiv 0 \pmod{m},\ \text{έστω}\ \sum_{i=1}^{4} b_i^2 = mn.$$

Επειδή $(a_1, a_2, a_3, a_4) = 1$, έπεται ότι **δεν** μπορεί να είναι όλα τα $b_i = 0$ ή $\pm\frac{p}{2}$. Επομένως

$$0 < \sum_{i=1}^{4} b_i^2 < m^2 \Longrightarrow 0 < n < m.$$

Εφαρμόζουμε τώρα την ταυτότητα του Euler στα αθροίσματα $\sum_{i=1}^{4} a_i^2, \sum_{i=1}^{4} b_i^2$ και βρίσκουμε

$$m^2 pn = \sum_{i=1}^{4} A_i^2,\ \text{με}\ A_1 = \sum_{i=1}^{4} a_i b_i,\ \text{και}$$

$$A_2 = a_1 b_2 - a_2 b_1 - a_3 b_4 + a_4 b_3 = m(c_1 b_2 - c_2 b_1 - c_3 b_4 + c_4 b_3)$$

(όμοιοι τύποι προς το A_2 για A_3 και A_4). Επειδή $m^2 | A_2^2, A_3^2, A_4^2$ και $m^2 pn$, έπεται ότι $m^2 | A_1^2$, οπότε $A_i = mB_i$ και $pn = \sum_{i=1}^{4} B_i^2$.

Αν $d := (B_1, B_2, B_3, B_4)$, $B_i = da_i'$, τότε $d^2 | pn$. Επειδή $0 < n < m < p$ το d θα πρέπει να είναι πρώτο προς το p και το d^2 θα πρέπει να διαιρεί το n. Θέτουμε $n = d^2 m'$, οπότε $pm' = \sum_{i=1}^{4} a_i'^2$ άθροισμα τεσσάρων τετραγώνων $(a_1', a_2', a_3', a_4') = 1$ και $pm' < pm$. Συνεχίζουμε όμοια μέχρι που $m' = 1$, δηλαδή το p άθροισμα τεσσάρων ακεραίων τετραγώνων. □

Περισσότερο από έναν αιώνα μετά την απόδειξη του Euler, ο Hurwicz έδωσε μία απόδειξη της πρότασης κάνοντας χρήση τετραδικών αριθμών (quaternions). Στην πραγματικότητα πρόκειται για μία μεταφορά της απόδειξης του Euler στη γλώσσα των quaternions.

Για τα αποτελέσματα του Euler στη λύση εξισώσεων του Pell θα αναφερθούμε στο επόμενο Κεφάλαιο.

Με τον Euler γεννήθηκε ο κλάδος της Θεωρίας των Αριθμών που χρησιμοποιεί αναλυτικές μεθόδους και, ως εκ τούτου, ονομάστηκε Αναλυτική Θεωρία Αριθμών.

Κατ' αρχήν είναι γνωστή η γεωμετρική σειρά

$$1 + x + x^2 + \cdots = \frac{1}{1-x}, \quad \text{για}\ |x| < 1. \tag{3.1}$$

Αν αντικαταστήσουμε το x με το $-x$ έχουμε

$$1 - x + x^2 - x^3 + x^4 + \cdots = \frac{1}{1+x}, \quad \text{για } |x| < 1. \tag{3.2}$$

Παίρνοντας το αόριστο ολοκλήρωμα και των δύο μελών της τελευταίας βρίσκουμε

$$log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots, \quad \text{για } |x| < 1. \tag{3.3}$$

Θυμόμαστε τώρα το **θεώρημα ορίου του Abel (Abel's limit theorem, Abelscher Grenzwertsatz)**. Έστω $\sum_{n=0}^{\infty} a(n)X^n$ δυναμοσειρά με ακτίνα σύγκλισης 1 και έστω $f(x) = \sum_{n=0}^{\infty} a(n)X^n$ για $|X| < 1$. Αν η σειρά συγκλίνει και για $X = 1$ (δηλαδή αν η σειρά $\sum_{n=0}^{\infty} a(n)$ συγκλίνει) τότε

$$\lim_{x \to 1^-} f(x) = \sum_{n=0}^{\infty} a(n).$$

Εφαρμόζουμε τώρα το θεώρημα αυτό για την συνάρτηση $f(x) = log(1+x)$ και, αφου $\sum_{0}^{\infty} (-1)^{n-1} \cdot \frac{1}{n}$ συγκλίνει, έχουμε

$$log(2) = 1 - \frac{1}{2} + \frac{1}{3} - \cdots \tag{3.4}$$

Αν γράψουμε πάλι την (3.2) για το x^2 παίρνουμε:

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + \cdots, \quad |x| < 1.$$

Η ολοκλήρωση των δύο μελών μας δίνει

$$\arctan x = x - \frac{x^3}{5} + \frac{x^5}{7} - \cdots, \ |x| < 1 \tag{3.5}$$

και εφαρμόζοντας και πάλι το παραπάνω θεώρημα του Abel προκύπτει ότι

$$\frac{\pi}{4} \ = \ \arctan 1 = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \cdots \ = \ \sum_{n=1}^{\infty} (-1)^n \frac{1}{2n+1}. \tag{3.6}$$

Ας θεωρήσουμε τώρα τις σειρές

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{και} \quad L(s) = \sum_{n=1}^{\infty} \frac{(-1)^n}{(2n+1)^s}, \ \ (s \in \mathbb{R}).$$

Η (3.6) μας δίνει την τιμή $L(1) = \frac{\pi}{4}$.

Η **ζ-συνάρτηση** $\zeta(s)$ προφανώς αποκλίνει για $s = 1$. Αποδεικνύεται εύκολα ότι η $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ συγκλίνει για $s > 1$ και αποκλίνει για $s \leq 1$. Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη.

Γεννιέται λοιπόν το ερώτημα ποιά είναι η τιμή των $\zeta(s)$ και $L(s)$ για $s = 2, 3, 4, \cdots$ Πρόκειται για ένα κλασικό ερώτημα με το οποίο ασχολήθηκαν οι Leibnitz και οι αδερφοί Bernoulli πριν από τον Euler, χωρίς όμως επιτυχία. Ακόμη και η εύρεση κάποιας προσεγγιστικής τιμής για το $\zeta(n)$ ήταν δύσκολη λόγω της αργής σύγκλισης της παραπάνω δυναμοσειράς.

Στα 1728 ο Daniel Bernoulli γράφει στον Goldbach ότι το άθροισμα της σειράς $\zeta(2)$ είναι ''πολύ κοντά στο $\frac{8}{5}$''.

Ο Goldbach χρησιμοποιεί μία πολύ στοιχειώδη μέθοδο και απαντά ότι το $\zeta(2)-1$ βρίσκεται ανάμεσα στις τιμές

$$\frac{16223}{25200} \quad \text{και} \quad \frac{30197}{46800},$$

δηλαδή $0,6437 \leq \zeta(2) - 1 \leq 0,6453$.

Ο Euler γίνεται γνώστης του περιεχομένου της αλληλογραφίας των D. Bernoulli και Goldbach και σύντομα δίνει μία πολύ καλύτερη εκτίμηση

$$\zeta(2) \sim 1,644934$$

κάνοντας ιδιοφυή χρήση του ολοκληρωτικού λογισμού. Αργότερα δίνει πολύ καλύτερη εκτίμηση του $\zeta(2)$ με 20 δεκαδικά ψηφία:

$$\zeta(2) \sim 1,64493406684822643647\cdots$$

Δίνει επίσης τιμές των $\zeta(3)$ με 15 δεκαδικά ψηφία, $\zeta(4)$ με 16 δεκαδικά ψηφία καθώς και την σήμερα ονομαζόμενη ''σταθερά του Euler'' με 16 ψηφία και το π με 15 δεκαδικά ψηφία.

Στα 1735 ο Euler γράφει:

> **"Πολύ δουλειά έχει γίνει για τη σειρά $\zeta(s)$ και φαίνεται ότι είναι δύσκολο να βρει κανείς κάτι καινούργιο. Και εγώ ο ίδιος, παρά τις επανειλλημένες προσπάθειές μου, δεν μπόρεσα να βρώ τίποτε περισσότερο από προσεγγιστικές τιμές για μερικά n. Αυτό μέχρι πρόσφατα, που, εκεί που δεν το περίμενε κανείς, ανακάλυψα ένα πολύ όμορφο τύπο για το $\zeta(2)$."**

Ο τύπος που ανακάλυψε ο Euler ήταν

$$\zeta(2) = \frac{\pi^2}{6}.$$

Λίγο αργότερα ανακάλυψε τύπους της τιμής της $\zeta(s)$ για όλους τους **άρτιους φυσικούς** $2n$.

Αλλά ας πάρουμε τα πράγματα με τη σειρά. Έστω $f(z) = \dfrac{z}{e^z - 1}$, όπου z εδώ **μιγαδικός** αριθμός. Η συνάρτηση είναι **αναλυτική** για $|z| < 2\pi$ και συνεπώς μπορούμε να βρούμε το ανάπτυγμα Taylor αυτής για $z = 0$:

$$f(z) = \sum_{n=0}^{\infty} \frac{B_n}{n} z^n.$$

Ορισμός 3.1 *Τους συντελεστές B_n θα τους λέμε* **αριθμούς του Bernoulli** *(στη μνήμη του Jacob Bernoulli).*

Από

$$1 = \left(\sum_{n=0}^{\infty} \frac{z^n}{(n+1)} \right) \cdot \left(\sum_{n=0}^{\infty} \frac{B_n}{n} z^n \right)$$

και λόγω του γνωστού θεωρήματος που μας λέει ότι μπορούμε να πολλαπλασιάσουμε δύο απολύτως συγκλίνουσες σειρές όπως και τα πολυώνυμα, προκύπτει: $B_0 = 1$ και για κάθε $n \geq 1$

$$c_n = \sum_{k=0}^{n} \frac{B_k}{k!} \cdot \frac{1}{(n-k+1)!} = 0 \implies B_n = -\sum_{k=0}^{n-1} \frac{B_k}{k!} \cdot \frac{n!}{(n-k+1)!} \tag{3.7}$$

Έχουμε λοιπόν έναν **αναδρομικό τύπο** από τον οποίο βγαίνει το συμπέρασμα ότι οι αριθμοί του Bernoulli είναι **ρητοί** αριθμοί.

Ας υπολογίσουμε μερικούς απ΄ αυτούς:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30}$$
$$B_5 = 0,\ B_6 = \frac{1}{42},\ B_7 = 0,\ B_8 = -\frac{1}{30},\ B_9 = 0$$
$$B_{10} = \frac{5}{66},\ B_{11} = 0,\ B_{12} = -\frac{691}{2730},\ \cdots$$

Ο Euler υπολόγισε όλους τους B_k για $k \leq 30$. Οι αριθμοί του Bernoulli χρησιμοποιούνται όχι μόνο σε πάρα πολλά κεφάλαια της Θεωρίας των Αριθμών, αλλά και σε άλλους κλάδους των Μαθηματικών, όπως π.χ. η Αλγεβρική Τοπολογία. Επικρατεί η αίσθηση ότι έχουν να κάνουν με πάρα πολύ βαθιά και σπουδαία προβλήματα.

Αν τώρα πολλαπλασιάσουμε τη σχέση

$$\sum_{k=0}^{n} \frac{1}{k!(n-k+1)} B_k = 0 \ \text{ με } \ (n+1)!$$

βρίσκουμε

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0 \ \text{ για κάθε } \ n \geq 1. \tag{3.8}$$

Αν τώρα για $P(X) = \sum_{k=0}^{n} a_k X^k$ χρησιμοποιήσουμε τον συμβολισμό

$$P(B) := \sum_{k=0}^{n} a_k B_k$$

τότε η (3.8) μπορεί να γραφτεί:

$$(1+B)^{n+1} - B^{n+1} = 0,\ n \geq 1. \tag{3.9}$$

Από τον πίνακα των B_n φαίνεται ότι θα πρέπει να ισχύει:

$$B_n = 0 \ \text{ για κάθε } \textbf{περιττό } \ n > 1. \tag{3.10}$$

Απόδειξη: Έχουμε

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} z^k \ \text{ οπότε } \ \frac{-z}{e^{-z} - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} (-1)^k z^k.$$

Αφαιρώντας κατά μέλη παίρνουμε

$$\frac{z}{e^z-1}-\frac{-z}{e^{-z}-1}=2\sum_{k\equiv 1(2)\ k\geq 1}\frac{B_k}{k!}z^k=-z+2\sum_{k\equiv 1(2)\ k>1}\frac{B_k}{k!}z^k.$$

Επειδή

$$\begin{aligned}\frac{z}{e^z-1}-\frac{-z}{e^{-z}-1}&=\frac{z}{e^z-1}+\frac{ze^z}{1-e^z}=\frac{z}{e^z-1}-\frac{ze^z}{e^z-1}\\&=\frac{z(1-e^z)}{e^z-1}=-z\implies 2\sum_{k\equiv 1(2)\ k>1}\frac{B_k}{k!}z^k=0\\&\implies B_n=0,\ \text{για κάθε περιττό } n,\ n>1.\end{aligned}$$

□

Οι αριθμοί του Bernoulli εμφανίστηκαν για πρώτη φορά στον τύπο:

$$1^k+2^k+\cdots+(n-1)^k=\frac{1}{k+1}((n+B)^{k+1}-B^{k+1}). \tag{3.11}$$

Για $k=1,2,3$ ο τύπος αυτός δίδει αντίστοιχα αθροίσματα

$$\frac{1}{2}(n-1)n,\ \frac{1}{6}n(n-1)(2n-1),\ \frac{1}{4}n^2(n-1)^2.$$

Απόδειξη: Έχουμε

$$\frac{e^{nz}-1}{z}\cdot\frac{z}{e^z-1}=\sum_{r=0}^{n-1}e^{rz}=\sum_{r=0}^{n-1}\sum_{k=0}^{\infty}\frac{r^k}{k!}z^k=\sum_{k=0}^{\infty}(\sum_{r=0}^{n-1}\frac{r^k}{k!})z^k.$$

Από την άλλη μεριά, κάνοντας χρήση του γινομένου σειρών βρίσκουμε:

$$\begin{aligned}\frac{e^{nz}-1}{z}\cdot\frac{z}{e^z-1}&=\left(\sum_{s=0}^{\infty}\frac{n^{s+1}z^s}{(s+1)!}\right)\cdot\left(\sum_{t=0}^{\infty}\frac{B_t}{t!}z^t\right)\\&=\sum_{k=0}^{\infty}\left(\sum_{s=0}^{k}\frac{n^{s+1}B_{k-s}}{(s+1)!(k-s)!}\right)z^k.\end{aligned}$$

Συγκρίνοντας τα αποτελέσματα βρίσκουμε

$$\sum_{r=0}^{n-1}\frac{r^k}{k!}=\sum_{s=0}^{k}\frac{n^{s+1}B_{k-s}}{(s+1)!(k-s)!}.$$

Πολλαπλασιάζουμε με $k!$ και παίρνουμε

$$\begin{aligned}\sum_{r=0}^{n-1} r^k &= \frac{1}{(k+1)}\sum_{s=0}^{k}\frac{(k+1)!}{(s+1)!(k-s)!}n^{s+1}B_{k-s}\\ &= \frac{1}{(k+1)}\sum_{s=0}^{k}\binom{k+1}{s+1}n^{s+1}B_{k-s} = \frac{1}{(k+1)}((n+B)^{k+1}-B^{k+1}).\end{aligned}$$

Ερχόμαστε τώρα στο πιο φημισμένο θεώρημα του Euler.

Θεώρημα 3.2 *Ισχύει*

$$\zeta(2k) = \sum_{n=1}^{\infty}\frac{1}{n^{2k}} = \frac{2^{2k-1}|B_{2k}|}{(2k)!}\pi^{2k}$$

για κάθε $k = 1, 2, 3, \ldots$ *Ιδιαίτερα για* $k = 1, 2, 3$ *έχουμε*

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}, \quad \sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{\pi^4}{90}, \quad \sum_{n=1}^{\infty}\frac{1}{n^6} = \frac{\pi^6}{945}.$$

Απόδειξη: Θα χρησιμοποιήσουμε (χωρίς απόδειξη) ένα αποτέλεσμα της θεωρίας των μιγαδικών συναρτήσεων, για την συνεφαπτομένη

$$\pi\cot\pi z = \frac{1}{z} + \sum_{n=1}^{\infty}\left(\frac{1}{z+n} + \frac{1}{z-n}\right).$$

(Ο ενδιαφερόμενος αναγνώστης μπορεί να δεί το [1], σελίδα 189.) Θέτουμε $z = 2ix$ στην $\dfrac{z}{e^z-1}$ και βρίσκουμε

$$\begin{aligned}\frac{2ix}{e^{2ix}-1} &= \sum_{k=0}^{\infty}\frac{B_k}{k!}(2ix)^k = \sum_{k=0}^{\infty}\frac{2^k i^k B_k}{k!}x^k\\ &= 1 - ix + \sum_{k=1}^{\infty}\frac{2^{2k}(-1)^k B_k}{(2k)!}x^{2k},\end{aligned}$$

διότι $B_k = 0$ για κάθε k περιττό και γνησίως μεγαλύτερο του 1.

Από την άλλη μεριά

$$\begin{aligned}x\cot x &= x\frac{\cos x}{\sin x} = x\cdot\frac{\left(\frac{e^{ix}+e^{-ix}}{2}\right)}{\left(\frac{e^{ix}-e^{-ix}}{2i}\right)}\\ &= ix\cdot\frac{2+e^{2ix}-1}{e^{2ix}-1} = \frac{2ix}{e^{2ix}-1} + ix\end{aligned}$$

και επομένως:

$$x\cot x = 1 + \sum_{k=1}^{\infty} \frac{2^{2k}(-1)^k B_{2k}}{(2k)!} x^{2k}.$$

Για $x = \pi z$, γράφουμε τώρα:

$$\begin{aligned}
x\cot x &= \pi z(\cot \pi z) = 1 + z\sum_{n=1}^{\infty}\left(\frac{1}{z+n} + \frac{1}{z-n}\right) \\
&= 1 + \frac{x}{\pi}\sum_{n=1}^{\infty}\left(\frac{1}{\frac{x}{\pi}+n} + \frac{1}{\frac{x}{\pi}-n}\right) = 1 + x\sum_{n=1}^{\infty}\left(\frac{1}{x+\pi n} + \frac{1}{x-\pi n}\right) \\
&= 1 + 2\sum_{n=1}^{\infty}\frac{x^2}{x^2-\pi^2 n^2} = 1 - 2\sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2}\left(\frac{1}{1-\frac{x^2}{n^2\pi^2}}\right) \\
&= 1 - \sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2}\left(\sum_{k=0}^{\infty}\frac{x^{2k}}{n^{2k}\pi^{2k}}\right) \quad (\text{γεωμετρική πρόοδος}) \\
&= 1 - 2\sum_{k=0}^{\infty}\left(\sum_{n=1}^{\infty}\frac{1}{n^{2k+2}}\right)\frac{x^{2k+2}}{\pi^{2k+2}} \quad (\text{απόλυτη σύγκλιση}) \\
&= 1 - 2\sum_{k=1}^{\infty}\left(\sum_{n=1}^{\infty}\frac{1}{n^{2k}}\right)\frac{x^{2k}}{\pi^{2k}}.
\end{aligned}$$

Συγκρίνοντας τους συντελεστές των δύο παραστάσεων της $x\cot x$, παίρνουμε:

$$\sum_{n=1}^{\infty}\frac{1}{n^{2k}} = \frac{2^{2k-1}\pi^{2k}(-1)^{k+1}B_{2k}}{(2k)!}.$$

□

Πρόσφατα, ο Apery απέδειξε ότι ο $\zeta(3)$ είναι άρρητος (1980). Για την τιμή της ζ συνάρτησης $\zeta(n)$ όπου n περιττός, έχουμε "μαύρα μεσάνυχτα" μέχρι σήμερα.

Ο Euler απέδειξε ότι (για $s > 1$)

$$\zeta(s) = \prod_{p\ \text{πρώτος}} \frac{1}{1-\frac{1}{p^s}}$$

και χρησιμοποίησε αυτή τη σχέση για να αποδείξει ότι υπάρχουν **άπειροι** πρώτοι αριθμοί.

Κάθε παράγοντας του δεύτερου μέλους της παραπάνω ισότητας γράφεται:

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{rs}} + \cdots$$

η οποία προφανώς συγκλίνει απόλυτα για $p = p_1, p_2, p_3, \ldots$ όπου

$$2 = p_1 < 3 = p_2 < p_3 < \cdots$$

η ακολουθία των πρώτων.

Κατ' αρχάς παρατηρούμε ότι

$$\begin{aligned} 1 &\leq \prod_{p>n} \frac{1}{1-\frac{1}{p^s}} = \prod_{p>n} \left(1 + \frac{1}{p^s} + \frac{1}{p^s \cdot (p^s - 1)}\right) \\ &\leq \prod_{p>n} \left(1 + \frac{2}{p^s}\right) \leq e^{2\sum_{p>n} \frac{1}{p^s}} \overset{n\to\infty}{\longrightarrow} 1. \end{aligned}$$

Από την άλλη μεριά ισχύει:

$$\prod_{p\leq n} \frac{1}{1-\frac{1}{p^s}} = \sum_{(a_1,a_2,\cdots,a_k)\in\mathbb{N}^k} \frac{1}{(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})^s} \tag{3.12}$$

όπου $p_1, p_2, \cdots, p_k$ οι πρώτοι αριθμοί οι μικρότεροι ή ίσοι με n. Το θεμελιώδες θεώρημα της αριθμητικής μάς εξασφαλίζει ότι

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} \leq \prod_{p\leq n} \frac{1}{1-\frac{1}{p^s}} \leq \zeta(s) < \infty$$

$$\text{οπότε } \zeta(s) = \prod_{p} \frac{1}{1-\frac{1}{p^s}}.$$

Αν τώρα υπήρχαν μόνο **πεπερασμένου πλήθους** πρώτοι αριθμοί τότε:

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} < \infty.$$

Από την άλλη μεριά όμως

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \left(1 + p^{-1} + p^{-2} + \cdots\right) = \sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

Το άτοπο αυτό μας δίνει άλλη μία απόδειξη ότι υπάρχουν **άπειροι** πρώτοι αριθμοί. □

Μπορεί ακόμη να **αποδείξει** κανείς ότι η σειρά $\displaystyle\sum_{p\in\mathbb{P}} \frac{1}{p}$ **αποκλίνει**.

Μια άμεση συνέπεια αυτού είναι ότι οι πρώτοι αριθμοί είναι πιό **πυκνοί** από τα τέλεια τετράγωνα, διότι $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} < \infty$.

Φυσικά η σειρά $\sum_{p\in\mathbb{P}} \frac{1}{p}$ αποκλίνει πολύ αργά. Το μερικό άθροισμα μετά από 50 εκατομμύρια όρους είναι ακόμη μικρότερο του 4.

Ένα πολύ σπουδαίο πρόβλημα είναι το πρόβλημα της κατανομής των πρώτων αριθμών.

Έστω $x > 0$ και $\pi(x)$ η συνάρτηση που μας δίνει το πλήθος των πρώτων αριθμών που δεν ξεπερνούν τον x. Προφανώς $\pi(x) \to \infty$ καθώς $x \to \infty$ διότι υπάρχουν άπειροι πρώτοι αριθμοί. Η συμπεριφορά της $\pi(x)$ σαν συνάρτηση του x απετέλεσε αντικείμενο μελέτης φημισμένων Μαθηματικών ήδη από τον 19^o αιώνα. Από πίνακες που έφτιαξαν για να δουν την συμπεριφορά της $\pi(x)$ οι Gauss (1792) και Legendre (1798) διατύπωσαν την εικασία ότι η $\pi(x)$ είναι **ασυμπτωτική** προς την $\frac{x}{logx}$ δηλαδή

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

Για πρώτη φορά αποδείχτηκε στα 1896 από τον Hadamard και τον de la Vallée Poussin με χρήση μέσων της μιγαδικής ανάλυσης. Μία στοιχειώδης απόδειξη δόθηκε στα 1949 από τον A. Selberg και, ανεξάρτητα, από τον P. Erdös.

Στην προσπάθειά του να λύσει το πρόβλημα του αθροίσματος των τεσσάρων τετραγώνων ο Euler θεωρεί τη σειρά $f(x) = \sum_{n=0}^{\infty} x^{n^2}$, η οποία προφανώς συγκλίνει για $|x| < 1$ και παίρνει την $f(x)^4 = \sum_{n=0}^{\infty} \tau(n)x^n$. Η $\tau(n)$ μας δείχνει κατά πόσους τρόπους μπορεί να γραφτεί ο n σαν άθροισμα τεσσάρων τετραγώνων. Για να αποδείξουμε λοιπόν ότι κάθε φυσικός αριθμός είναι άθροισμα τεσσάρων τετραγώνων αρκεί να δείξουμε το ισοδύναμο

$$\tau(n) > 0, \quad \forall n \in \mathbb{N}.$$

Αυτό δεν το κατάφερε ο Euler. Το απέδειξε ο C. G. Jacobi ($19^{ος}$ αιώνας) κάνοντας χρήση της θεωρίας των ελλειπτικών συναρτήσεων. Βλέπουμε πάντως πως ένα καθαρά αριθμητικό πρόβλημα μεταφέρεται σε ένα αναλυτικό πρόβλημα.

Η ιδέα όμως του Euler είναι πολύ πιό γενική. Μία **διαμέριση** ενός φυσικού αριθμού είναι μία παράσταση του αριθμού σαν άθροισμα φυσικών αριθμών. Δύο διαμερίσεις θα είναι

ίδιες αν διαφέρουν μόνο στη σειρά των προσθετέων. Μπορούμε λοιπόν να υποθέσουμε ότι σε μία διαμέριση του $n = n_1 + n_2 \cdots + n_k$ ισχύει $n_1 \geq n_2 \geq \cdots \geq n_k$.

Έστω $p(n)$ το πλήθος των διαμερίσεων του n (π.χ. $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$). Η έννοια της διαμέρισης ορίστηκε σε ένα γράμμα του Leibnitz προς τον J. Bernoulli (1663). Είναι πάρα πολύ δύσκολο να υπολογίσουμε το $p(n)$ για τυχαίο n. Η $p(n)$ είναι μία αριθμητική συνάρτηση. Σε κάθε αριθμητική συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ ο Euler ορίζει μία **generating function της** f

$$F(x) := \sum_{n=0}^{\infty} f(n)x^n, \text{ με } f(0) := 1.$$

Αν η $f(n)$ δεν πλησιάζει προς το ∞ καθώς μεγαλώνει το n, η σειρά έχει μία θετική ακτίνα σύγκλισης. Για $f = p$ η ακτίνα σύγκλισης είναι 1. Ο Euler απέδειξε το

Θεώρημα 3.3 *Για* $|x| < 1$, *ισχύει*

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{m=1}^{\infty} \frac{1}{1 - x^m} \quad (p(0) = 1),$$

και μερικά χρόνια αργότερα, το

Θεώρημα 3.4

$$\prod_{m=1}^{\infty}(1 - x^m) = \sum_{k=-\infty}^{+\infty} (-1)^k x^{\frac{3k^2+k}{2}}.$$

Ο Jacobi ήταν και πάλι αυτός που έδωσε την πρώτη "φυσική" απόδειξη του τελευταίου θεωρήματος και αυτό έγινε και πάλι με την χρήση της θεωρίας των ελλειπτικών συναρτήσεων.

Μία παρατήρηση του Euler ήταν ότι οι αριθμοί

$$d = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, \ldots, 1320, 1365, 1848$$

(το πλήθος τους είναι 65) έχουν την εξής ιδιότητα:

Αν $ab = d$ και αν κάποιος αριθμός γράφεται κατά τρόπο μοναδικό σαν $ax^2 + by^2$ με $(ax, by) = 1$ τότε ο αριθμός αυτός θα είναι της μορφής p, $2p$ ή 2^k όπου p πρώτος αριθμός.

Ιδιαίτερα κάθε περιττός αριθμός μεγαλύτερος του 1 που γράφεται μοναδικά κατ΄ αυτό τον τρόπο είναι **πρώτος**. Ο Euler μας δίνει το παράδειγμα $d = 57$. Ο 1000003 γράφεται μοναδικά σαν $19 \cdot 8^2 + 3 \cdot 577^2$, συνεπώς είναι πρώτος. Για $d = 1848$ ο 18518809 έχει μοναδική παράσταση $197^2 + 1848 \cdot 100^2$, δηλαδή είναι πρώτος.

Οι αριθμοί αυτοί d λέγονται **numeri idonei**. Μέχρι σήμερα είναι άγνωστο αν υπάρχουν και άλλοι, εκτός των 65 γνωστών, numeri idonei.

Μία άλλη παρατήρηση του Euler ήταν ότι οι τιμές του πολυωνύμου

$$x^2 + x + 41$$

για $x = 0, 1, 2, \cdots, 39$ είναι **πρώτοι** αριθμοί. Το φαινόμενο θα εξηγηθεί στο επόμενο κεφάλαιο.

Σαν τελευταίο αναφέρουμε την **εικασία του Euler ότι η διοφαντική εξίσωση $x^4 + y^4 + z^4 = w^4$ δεν έχει θετική ακέραια λύση, αποδείχτηκε πρόσφατα λάθος**. Ο Noam Elkies κάνοντας χρήση του computer του Harvard, βρήκε μία λύση το 1987, την:

$$1682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Την ίδια χρονιά ο Roger Frye, κάνοντας και αυτός χρήση ηλεκτρονικού υπολογιστή, βρήκε την πιό **μικρή λύση** της παραπάνω εξίσωσης

$$95800^4 + 217519^4 + 414560^4 = 422560^4.$$

Κεφάλαιο 4

Josef Louis Lagrange (1736-1813), Adrie-Marie Legendre (1752-1833)

Ο Lagrange γεννήθηκε στα 1736 στο Τουρίνο. Ο πατέρας του είχε γαλλική καταγωγή και η μητέρα του ιταλική. Το ενδιαφέρον του περιοριζόταν στην αρχή στην μελέτη των κλασικών γλωσσών, ώσπου έπεσε στα χέρια του μία εργασία του Halley. Σε σύντομο χρονικό διάστημα μελέτησε σε πλάτος και σε βάθος όλη την ανάλυση της εποχής. Στα 19 του χρόνια έγινε καθηγητής της Βασιλικής Σχολής Πυροβολικού του Τουρίνο, όπου και έμεινε περί τα 10 χρόνια. Η παραμονή του στο Τουρίνο διακόπηκε μόνο από ένα ταξίδι που έκανε περί τα τέλη του 1763 στο Παρίσι όπου και γνωρίστηκε με όλους τους Γάλλους Μαθηματικούς της εποχής όπως Clairaut, Lalande, d' Alembert, Condorcet. Ο Clairaut περιγράφει τον Lagrange σε ένα γράμμα του προς τον Daniel Bernoulli, ως εξής:

> **Ένας νεαρός, αξιοπρόσεκτος όχι μόνο για το ταλέντο του αλλά και για την ταπεινοφροσύνη του. Το ταμπεραμέντο του είναι ήρεμο και μελαγχολικό. Δεν γνωρίζει άλλη ευχαρίστηση εκτός της μελέτης.**

Με τον d' Alembert άρχισε αλληλογραφία η οποία κράτησε μέχρι το θάνατο του d' Alembert στα 1783. Με πρόταση του d' Alembert, διαδέχθηκε ο Lagrange τον Euler στην Ακαδημία Επιστημών της Πρωσσίας (Βερολίνο) στα 1766. Στα 1787 εγκατέλειψε

το Βερολίνο για την Ακαδημία των Παρισίων. Εθεωρείτο, μετά τον θάνατο του Euler, ο πιο μεγάλος εν ζωή Μαθηματικός.

Κατά τη διάρκεια της Γαλλικής Επανάστασης έχασε δύο από τους καλύτερους φίλους του, τον Lavoisier και τον Condorcet. Η συνεισφορά του υπήρξε σημαντική στην Ανάλυση και ιδιαίτερα στους κλάδους του λογισμού μεταβολών, διαφορικών εξισώσεων και μηχανικής. Στο Παρίσι δεν ασχολείται με την έρευνα, αλλά διδάσκει στην Ecole Normale και στην Ecole Polytechnique μαθήματα πρωτοποριακά για την εποχή τους όπως:

- Theorie des Fonctions Analytiques (1797)
- Leçons sur le Calcul des Fonctions (1806)

Προς τα τελαυταία χρόνια της ζωής του αναλαμβάνει να ξαναγράψει την

- Mechanique Analytique (1788), αλλά δεν προλαβαίνει να τελειώσει το έργο του.

Πέθανε στις 8 Απριλίου του 1813, τιμήθηκε ιδιαίτερα από τον Ναπολέοντα και τάφηκε στο Πάνθεο.

Σε αντίθεση προς τον ενθουσιασμό του Euler προς τις ανακαλύψεις του, ο Lagrange χαιρόταν πιό πολύ τις ανακαλύψεις των άλλων. Σε ένα γράμμα του στον Laplace, γράφει:

> **Πολύ μεγαλύτερη χαρά μου δίνει η δουλειά των άλλων, σε αντίθεση με την προσωπική μου δουλειά από την οποία ποτέ δεν είμαι ευχαριστημένος.**

Η δουλειά του στην Θεωρία Αριθμών έγινε κατά τα χρόνια της παραμονής του στο Βερολίνο. Πρόκειται για κυρίως 3 εργασίες:

- Solution d' un probleme d' arithmetique (1768), στην αποία ο Lagrange μελετά την εξίσωση $x^2 - dy^2 = 1$.

- Demonstration d' un theoréme d' arithmetique (1770), όπου δίνει την πρώτη απόδειξη ότι κάθε φυσικός γράφεται σαν άθροισμα τεσσάρων τετραγώνων, ακεραίων αριθμών.

- Recherches d' arithmetique (1773), στην οποία ο Lagrange αναπτύσσει την γενική θεωρία των τετραγωνικών μορφών από την οποία σαν ειδικές περιπτώσεις δίνει τα αποτελέσματα του Fermat για την παράσταση πρώτων αριθμών από τις μορφές $x^2 + 2y^2$ και $x^2 + 3y^2$.

Θα ξεκινήσουμε από την τελευταία εργασία του στην οποία αναπτύσσεται συστηματικά μία πλήρης αριθμητική θεωρία η επίδραση της οποίας στην ανάπτυξη της Θεωρίας των Αριθμών και της Άλγεβρας δεν μπορεί να παραγνωριστεί. Εικοσιπέντε χρόνια αργότερα η θεωρία των (binary) τετραγωνικών μορφών πήρε απο τον Gauss (σχεδόν) την τελική της μορφή. Στην ανάπτυξη της θεωρίας θα χρησιμοποιήσουμε την ορολογία του Gauss.

Ο Lagrange λοιπόν παρατήρησε ότι μπορεί κανείς να μελετήσει το πρόβλημα της παράστασης ενός φυσικού αριθμού μέσω μιάς **τετραγωνικής μορφής**

$$q(X, Y) = aX^2 + bXY + cY^2, \ (a, b, c \in \mathbb{Z}).$$

Γενικά: Θα λέμε ότι ο αριθμός m **παρίσταται** από την τετραγωνική μορφή $q(X, Y)$ τότε και μόνον τότε όταν

$$\exists (x, y) \in \mathbb{Z} \times \mathbb{Z} : \ q(x, y) = m.$$

Σχεδόν αντιγράφοντας λέξη προς λέξη τον Lagrange αποδεικνύουμε το

Θεώρημα 4.1 *Έστω ότι ο r είναι ένας διαιρέτης κάποιου αριθμού που παρίσταται από την τετραγωνική μορφή $q(X, Y) = aX^2 + bXY + cY^2$ για $X = x_0$, $Y = y_0$, $(x_0, y_0) = 1$. Τότε και ο r μπορεί να παρασταθεί μέσω μιάς τετραγωνικής μορφής $Q(X, Y) = AX^2 + BXY + CY^2$ για $X = X_0$, $Y = Y_0$, $(X_0, Y_0) = 1$. Ισχύει δε και $B^2 - 4AC = b^2 - 4ac$.*

Απόδειξη: Έστω $rs = ax_0^2 + bx_0y_0 + cy_0^2$ και έστω $t = (s, y_0)$, δηλαδή, $s = tu$, $y_0 = tX_0$ και $(u, X_0) = 1$. Αυτό μας δίνει:

$$rtu = ax_0^2 + bx_0tX_0 + ct^2X_0^2,$$

δηλαδή $t|ax_0^2$. Επειδή $(x_0, y_0) = 1$, έπεται ότι $(t, x_0) = 1$. Αυτό σημαίνει ότι κατ' ανάγκη $t|a$, έστω $a = et$. Αν τώρα διαιρέσουμε και τα δύο μέλη με t βρίσκουμε

$$ru = ex_0^2 + bx_0X_0 + ctX_0^2.$$

Επειδή u και X_0 είναι πρώτοι μεταξύ τους μπορούμε να γράψουμε το x_0 στη μορφή

$$x_0 = uY_0 + wX_0$$

οπότε η τελευταία εξίσωση γίνεται

$$\begin{aligned} ru &= e(uY_0 + wX_0)^2 + b(uY_0 + wX_0)X_0 + ctX_0^2 \\ &= (ew^2 + bw + ct)X_0^2 + (2euw + bu)X_0Y_0 + eu^2Y_0^2. \end{aligned}$$

Επειδή $(u, X_0) = 1$ και $u|(ew^2 + bw + ct)X_0^2$ προκύπτει ότι $u|ew^2 + bw + ct$. Έστω

$$A := \frac{eu^2 + bw + ct}{u},\ B := 2ew + b,\ C := ew.$$

Η τελευταία σχέση γράφεται

$$r = AX_0^2 + BX_0Y_0 + CY_0^2 \ \text{ με } \ (X_0, Y_0) = 1,$$

δηλαδή ο r παρίσταται από την τετραγωνική μορφή $Q(X, Y) = AX^2 + BXY + CY^2$. Εύκολα διαπιστώνει κανείς ότι $4AC - B^2 = 4ac - b^2$. □

Θα λέμε ότι ο m παρίσταται **γνήσια** από την τετραγωνική μορφή $q(X, Y)$, αν υπάρχουν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) = 1$ τέτοιοι ώστε $m = q(x, y)$.

Ο m θα λέγεται **διαιρέτης** της τετραγωνικής μορφής $q(X, Y)$ όταν ο m είναι διαιρέτης κάποιου αριθμού s που παρίσταται **γνήσια** από την $q(X, Y)$. Η έκφραση $4ac - b^2$ θα λέγεται **διακρίνουσα** της τετραγωνικής μορφής $q(X, Y)$.

Το θεώρημα 4.1 μπορεί τώρα να γραφεί ως εξής:

Θεώρημα 4.1′: Αν ο m είναι ένας διαιρέτης της τεραγωνικής μορφής $q(X, Y)$ τότε και ο m παρίσταται γνήσια από μία τετραγωνική μορφή της ίδιας διακρίνουσας.

Στα επόμενα αντί της τετραγωνικής μορφής $aX^2 + bXY + cY^2$ θα θεωρούμε την πιο ειδική τετραγωνική μορφή

$$aX^2 + 2bXY + cY^2.$$

Το θεώρημα 4.1, 4.1′ ισχύει διότι ο B είναι άρτιος αν και μόνο εάν ο b είναι άρτιος μία και $B = 2ew + b$.

Μπορούμε τώρα να γράψουμε την τετραγωνική μορφή σαν γινόμενο πινάκων:

$$aX^2 + 2bXY + cY^2 = (X, Y) \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Παρατηρούμε ότι κάθε τετραγωνική μορφή περιγράφεται πλήρως από τους συντελεστές της a, b, c ή καλύτερα μέσω ενός 2×2 πίνακα των συντελεστών. Με $q(X, Y)$ θα συμβολίζουμε την τετραγωνική μορφή $aX^2 + 2bXY + cY^2$ και με

$$\Delta := \det \begin{pmatrix} a & b \\ c & c \end{pmatrix} = ac - b^2.$$

Στα επόμενα θα υποθέτουμε πάντα ότι $\Delta \neq 0$.

Δύο τετραγωνικές $q(x, y)$ και $Q(X, Y)$ θα λέγονται **ισοδύναμες** αν η μία μπορεί να δώσει την άλλη μέσω ενός αντιστρέψιμου ακέραιου γραμμικού μετασχηματισμού των μεταβλητών, δηλαδή

$$\left\{ \begin{array}{l} X = \alpha x + \beta y \\ Y = \gamma x + \delta y \end{array} \right\} \quad \text{με} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z})$$

όπου $GL_2(\mathbb{Z})$ είνια η ομάδα των αντιστρεψίμων ακεραίων 2×2 πινάκων.

Οι τετραγωνικές μορφές θα λέγονται **γνήσια ισοδύναμες** αν ισχύουν τα παραπάνω για πίνακες

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}), \text{ δηλαδή } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z}) \text{ και } \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1.$$

Υπό μορφή πίνακα, ο μετασχηματισμός γράφεται:

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \text{οπότε}$$

$$(X,Y)\begin{pmatrix} A & B \\ B & C \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix} = (x,y)\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} A & B \\ B & C \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$
$$= (x,y)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

Ώστε δύο πίνακες $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$, $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$ ορίζουν **ισοδύναμες** (**γνήσια ισοδύναμες**) τετραγωνικές μορφές τότε και μόνο τότε όταν

$$\text{Υπάρχει} \quad T \in GL_2(\mathbb{Z}) \ \ (T \in SL_2(\mathbb{Z})) \ \text{τέτοιο ώστε}$$
$$\begin{pmatrix} A & B \\ B & C \end{pmatrix} = T^t \begin{pmatrix} a & b \\ b & c \end{pmatrix} T,$$

όπου T^t ο **ανάστροφος** του T.

Η έννοια της ισοδυναμίας (αντίστοιχα γνήσιας ισοδυναμίας) είναι σχέση ισοδυναμίας. Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. Ισοδύναμες μορφές παριστούν τους ίδιους αριθμούς και έχουν την ίδια διακρίνουσα διότι ισχύει $(\det T)^2 = 1$.

Μία τετραγωνική μορφή $q(x,y) = ax^2 + bxy + cy^2$ θα λέγεται **θετική** (**αρνητική**) αν $q(x,y) \geq 0,\ \forall x,y \in \mathbb{Z}$ ($q(x,y) \leq 0,\ \forall x,y \in \mathbb{Z}$). Αν μία μορφή είναι θετική ή αρνητική θα λέγεται **definite**, αλλιώς θα λέγεται **indefinite**.

Αν γράψουμε

$$q(x,y) = ax^2 + 2bxy + cy^2 = a(x + \frac{b}{a}y)^2 + cy^2 - \frac{b^2}{a}y^2$$

βλέπουμε ότι η $q(x,y)$ είναι θετική αν και μόνο εάν ($\Delta > 0$ και $a > 0$) αντίστοιχα ($q(x,y)$ είναι αρνητική αν και μόνο εάν $\Delta > 0$ και $a < 0$), ενώ $q(x,y)$ είναι indefinite αν και μόνο εάν $\Delta < 0$.

Στα επόμενα θα περιοριστούμε μόνο σε definite τετραγωνικές μορφές. Ο λόγος είναι ότι οι indefinite συμπεριφέρονται εντελώς διαφορετικά από τις definite.

Αν τώρα $q(x,y) = ax^2 + 2bxy + cy^2$ θετική, τετραγωνική μορφή, τότε $\Delta > 0$ και $a > 0$. Αν την πολλαπλασιάσουμε με το -1 βρίσκουμε την τετραγωνική μορφή $q'(x,y) = -ax^2 - 2bxy - cy^2$ με την ίδια διακρίνουσα $\Delta = ac - b^2 > 0$ και $a' = -a < 0$, δηλαδή $q'(x,y)$ είναι αρνητική.

Παρατηρούμε ότι αν $q(x,y)$ είναι θετική τότε και κάθε γνήσια ισοδύναμη προς αυτήν είναι επίσης θετική. Αρκεί λοιπόν να μελετήσουμε τις **κλάσεις ισοδυναμίας θετικών τετραγωνικών μορφών**.

Θα ενδιαφερόμασταν να έχουμε ένα πλήρες σύστημα αντιπροσώπων των κλάσεων, δηλαδή μία μέθοδο με την οποία από κάθε κλάση θα μπορούσαμε να διαλέγουμε ακριβώς μία τετραγωνική μορφή.

Ορίζουμε κατ' αρχήν **ανάγωγες τετραγωνικές μορφές** εκείνες των οποίων τα στοιχεία του πίνακα $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ πληρούν τις σχέσεις $-\frac{a}{2} < b \leq \frac{a}{2}$, $a \leq c$ και, αν $a = c$ τότε $0 \leq b \leq \frac{a}{2}$.

Θεώρημα 4.2 *Κάθε θετική τετραγωνική μορφή $Q(X,Y)$ είναι γνήσια ισοδύναμη προς μία ανάγωγη και σε κάθε κλάση ισοδυναμίας υπάρχει ακριβώς μία ανάγωγη. Τέλος ισχύει ότι*

$$a \leq 2\sqrt{\frac{\Delta}{3}} \qquad (\Delta := ac - b^2).$$

Απόδειξη: Έστω $Q(X,Y)$ τετραγωνική μορφή που δίνεται από τον πίνακα $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$ και έστω ότι ο a είναι ο **ελάχιστος** φυσικός αριθμός, διάφορος του μηδενός, που παρίσταται από την Q. Δηλαδή υπάρχουν $(X_0, Y_0) \in \mathbb{Z} \times \mathbb{Z}$, $a = AX_0^2 + BX_0Y_0 + CY_0^2$. Λόγω της υπόθεσης για τον a θα έχουμε $(X_0, Y_0) = 1$, δηλαδή η παράσταση θα είναι γνήσια. Επομένως υπάρχουν $(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}$ τέτοια ώστε $\alpha X_0 + \beta Y_0 = 1$ και επομένως

$$T = \begin{pmatrix} X_0 & Y_0 \\ -\beta & \alpha \end{pmatrix} \in SL_2(\mathbb{Z}),$$

οπότε βρίσκουμε κάποιον καινούργιο πίνακα που ορίζει γνήσια ισοδύναμη τετραγωνική μορφή, τον

$$T \begin{pmatrix} A & B \\ B & C \end{pmatrix} T^t = \begin{pmatrix} X_0 & Y_0 \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} A & B \\ B & C \end{pmatrix} \begin{pmatrix} X_0 & -\beta \\ Y_0 & \alpha \end{pmatrix} = \begin{pmatrix} a & B' \\ B' & C' \end{pmatrix}$$

με $B', C' \in \mathbb{Z}$. Επαναλαμβάνουμε το ίδιο τώρα με κάποιο πίνακα $\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, $k \in \mathbb{Z}$. Έχουμε

$$\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \begin{pmatrix} a & B' \\ B' & C' \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & B'+ka \\ B'+ak & * \end{pmatrix}.$$

Διαλέγουμε το $k \in \mathbb{Z}$ έτσι ώστε $-\frac{a}{2} < B' + ka \leq \frac{a}{2}$ και θέτουμε $b := B' + ka$, $c = *$, οπότε ο πίνακας $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ είναι, λόγω κατασκευής, γνήσια ισοδύναμος προς τον $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$, πληροί τις $-\frac{a}{2} < b \leq \frac{a}{2}$ και $a \leq c$ (η τελευταία ανισότητα, διότι ο c παρίσταται από την $Q(X,Y)$ για $X = 0, Y = 1$, ενώ ο a είναι ο ελάχιστος μ' αυτή την ιδιότητα). Αν τώρα συμβεί $a = c$ και είναι $b < 0$ τότε χρησομοποιούμε τον πίνακα $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & -b \\ -b & a \end{pmatrix}$$

και ο τελευταίος είναι γνήσια ισοδύναμος προς $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$ με $-\frac{a}{2} < b \leq \frac{a}{2}$, $a \leq c$ και αν $a = c$, τότε $b > 0$.

Αποδείξαμε λοιπόν μέχρι στιγμής ότι **κάθε** θετική τετραγωνική μορφή είναι ισοδύναμη προς μία **ανάγωγη**.

Θα αποδείξουμε τώρα και τη **μοναδικότητα**. Ότι δηλαδή αν δύο θετικές τετραγωνικές μορφές είναι ανάγωγες και γνήσια ισοδύναμες, τότε κατ' ανάγκη οι πίνακες είναι ίσοι.

Κατ' αρχήν αποδεικνύουμε ότι, αν $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ ανάγωγος, τότε ο a είναι ο ελάχιστος φυσικός αριθμός, διαφορετικός του μηδενός, που παρίσταται από την τετραγωνική μορφή $Q(X,Y) = aX^2 + bXY + cY^2$, δηλαδή ο a ορίζεται μονοσήμαντα.

Πράγματι, αν $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ανάγωγος, τότε η τετραγωνική μορφή $Q(X,Y)$ δίνει τιμές $Q(x,y) \geq a$ για $x, y \in \mathbb{Z}$ και αυτό διότι

- Για $0 < |x| \leq |y|$ έπεται ότι $2bxy + cy^2 \geq a$, δηλαδή $Q(x,y) \geq ax^2 \geq a$.
- Για $0 < |y| \leq |x|$ συνεπάγεται $ax^2 + 2bxy \geq 0$, επομένως $Q(x,y) \geq cy^2 \geq a$.
- Για $x = 0$ ή $y = 0$ έπεται ότι $Q(x,y) \geq a$.

Για $x = \pm 1$, $y = 0$ βρίσκουμε τώρα ότι παράγματι ο a είναι ο ελάχιστος φυσικός που παρίσταται από την $Q(X,Y)$.

Αν τώρα ισχύει $a < c$ τότε οι τιμές $x = \pm 1$, $y = 0$ είναι οι μόνες τιμές που μας επιτρέπουν να πάρουμε σαν τιμή της τετραγωνικής μορφής την ελάχιστη τιμή a και αυτό διότι

- Για $|x| > 1$ και $y = 0$ έπεται ότι $Q(x, y) = ax^2 > a$.
- Για $x, y \neq 0$, αν $x \geq y \geq 1$ έχουμε $ax^2+2bxy+cy^2 \geq cy^2 \geq a$, ενώ αν $|y| \geq |x| \geq 1$, ισχύει $ax^2 + 2bxy + cy^2 \geq ax^2 \geq a$.

Έστω τώρα ότι οι τετραγωνικές μορφές που αντιστοιχούν στους πίνακες

$$\begin{pmatrix} a & B \\ B & C \end{pmatrix} \quad \text{και} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

είναι ανάγωγες και γνήσια ισοδύναμες. Υπάρχει λοιπόν ένας πίνακας $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ τέτοιος ώστε

$$\begin{aligned} \begin{pmatrix} a & B \\ B & C \end{pmatrix} &= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= \begin{pmatrix} a\alpha^2+2b\alpha\gamma^2+c\gamma^2 & * \\ * & * \end{pmatrix} \end{aligned}$$

$$\Longrightarrow a = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \Longrightarrow (\gamma = 0,\ \alpha = \pm 1).$$

Επομένως

$$\begin{pmatrix} a & B \\ B & C \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ \beta & \pm 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{pmatrix} = \begin{pmatrix} a & b \pm \beta a \\ * & * \end{pmatrix}.$$

Επειδή δε και οι δύο πίνακες $\begin{pmatrix} a & B \\ B & C \end{pmatrix}$ και $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ είναι ανάγωγοι, έπεται ότι $-\frac{a}{2} < b$, $B \leq \frac{a}{2}$, οπότε θα πρέπει $\beta = 0$, δήλαδή $B = b$.

Από τη σχέση τέλος $AC - B^2 = ac - b^2$ έπεται ότι $c = C$ δηλαδή

$$\begin{pmatrix} A & B \\ B & C \end{pmatrix} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

Θα αποδείξουμε τώρα το ίδιο στην περίπτωση όπου $a = c$, $0 \leq b < \frac{a}{2}$. Εδώ η ελάχιστη τιμή a ''πιάνεται'' όταν $(x = \pm 1,\ y = 0)$ και $(x = 0,\ y = \pm 1)$. Η γνήσια ισοδυναμία μεταξύ των $\begin{pmatrix} a & B \\ B & C \end{pmatrix}$ και $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ εκφράζεται τώρα ως εξής:

$$\begin{aligned} \begin{pmatrix} a & B \\ B & C \end{pmatrix} &= \begin{pmatrix} \pm 1 & 0 \\ \beta & \mp 1 \end{pmatrix} \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{pmatrix} \quad \text{ή} \\ \begin{pmatrix} a & B \\ B & C \end{pmatrix} &= \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & \beta \end{pmatrix} \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & \beta \end{pmatrix}, \end{aligned}$$

οπότε βρίσκουμε $B = \pm a\beta + b$, $B = \pm aB - b$. Οι ανισότητες $0 \le b$, $B \le \frac{a}{2}$ τώρα δίνουν πάλι $\beta = 0$, και συνεπώς

$$\begin{pmatrix} a & B \\ B & C \end{pmatrix} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

Αν τέλος $a = c$ και $b = \frac{a}{2}$ τότε $a = c = 2b$ και ο πίνακας είναι:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} = b \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Αρκεί λοιπόν να θεωρήσουμε τον πίνακα $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Η ελάχιστη τιμή 2 δίνεται τώρα για τις τιμές $(x = \pm 1,\ y = 0)$, $(x = 0,\ y = \pm 1)$, $(x = \pm 1,\ y = \mp 1)$. Και πάλι το συμπέρασμα είναι $B = b$ και $C = c$.

Αποδείξαμε λοιπόν και την μοναδικότητα.
Οι $\Delta = ac - b^2$, $|b| \le \frac{a}{2}$ και $a \le c$ δίνουν

$$4a^2 \le 4ac \ = \ 4(\Delta + b^2) \ = \ 4\Delta + 4b^2 \ \le \ 4\Delta + 4\frac{a^2}{4} \ \le \ 4\Delta + a^2.$$

Επομένως από την $3a^2 \le \Delta$ συνεπάγεται ότι $a \le \sqrt{\frac{\Delta}{3}}$.

Πόρισμα 4.3 *Υπάρχουν* **πεπερασμένου** *πλήθους (γνήσιες) κλάσεις ισοδυναμίας τετραγωνικών μορφών δοσμένης διακρίνουσας* Δ.

Απόδειξη: Σύμφωνα με το θεώρημα, σε κάθε κλάση ισοδυναμίας αντιστοιχεί μία ακριβώς ανάγωγη τετραγωνική μορφή $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Έχουμε ήδη δείξει ότι $a \le 2\sqrt{\frac{\Delta}{3}}$, δηλαδή υπάρχουν πεπερασμένου πλήθους a. Από τη σχέση $-\frac{a}{2} < b \le \frac{a}{2}$ έπεται ότι $|b| \le \frac{a}{2}$ επομένως $|b| \le \sqrt{\frac{\Delta}{3}}$, δηλαδή υπάρχουν πεπερασμένου πλήθους b. Τέλος η σχέση $\Delta = ac - b^2$ μας δίνει πεπερασμένου πλήθους c. □

Παράδειγμα: Έστω $\Delta = ac - b^2 = 9$. Έχουμε $2\sqrt{\frac{\Delta}{3}} = 2\sqrt{3}$ (περίπου $3,4$). Επομένως για το a έχουμε τρεις δυνατότητες $a = 1, 2, 3$. Τώρα $|b| \le \sqrt{\frac{\Delta}{3}}$ επομένως $|b| \le 1,74$ δηλαδή $b = -1, 0, 1$ ενώ θα πρέπει $-\frac{a}{2} < b \le \frac{a}{2}$.
Αν $a = 1$ τότε $-\frac{1}{2} < b \le \frac{1}{2}$, άρα $b = 0$.

Αν $a = 2$ τότε $-1 < b \leq 1$, άρα $b = 0, 1$.
Αν $a = 3$ τότε $-\frac{3}{2} < b \leq \frac{3}{2}$, άρα $b = -1, 0, 1$.

a	b	$\Delta = ac - b^2 \ \Rightarrow \ c = \frac{\Delta + b^2}{a} \in \mathbb{Z}$
1	0	$c = 9$
2	0, 1	$c = 5$ για $b = 1$ (Η $b = 0$ **δεν** δίνει $c \in \mathbb{Z}$)
3	-1, 0, -1	$c = 3$, για $b = 0$

Επομένως οι τετραγωνικές μορφές είναι

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

Δ	Θετικές ανάγωγες τετραγωνικές μορφές
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
2	$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$
3	$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
4	$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
5	$\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$
6	$\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$
7	$\begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 4 \end{pmatrix}$
8	$\begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$
9	$\begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$
10	$\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}$

Στη συνέχεια ο Lagrange ερεύνησε το πρόβλημα ποιοί πρώτοι αριθμοί παρίστανται από την τετραγωνική μορφή x^2+ay^2, $a \in \mathbb{Z}-\{0\}$. Διέκρινε δύο περιπτώσεις ανάλογα με το αν $p=4n-1$ ή $p=4n+1$. Κατ' αρχήν απέδειξε το:

Θεώρημα 4.4 *Έστω $a \in \mathbb{Z}-\{0\}$. Ο πρώτος αριθμός $p=4n-1$ είναι διαιρέτης της μορφής x^2-ay^2 τότε και μόνο τότε όταν ο p* **δεν** *είναι διαιρέτης της μορφής x^2+ay^2.*

Απόδειξη: Έστω ότι $p=4n-1$ είναι ο διαιρέτης της x^2-ay^2. Τότε υπάρχουν $(x_0,y_0) \in \mathbb{Z}\times\mathbb{Z}$, τέτοιοι ώστε $(x_0,y_0)=1$ που ικανοποιούν την ισοδυναμία $x_0^2 \equiv ay_0^2 (\mathrm{mod}\, p)$. Επειδή $(y_0,p)=1$, έπεται ότι ο a είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$. Αν ο p ήταν διαιρέτης και της τεραγωνικής μορφής x^2+ay^2, τότε και ο αριθμός $-a$ θα ήταν τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$. Κατά συνέπεια ο -1 θα ήταν τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$, άτοπο διότι $p=4n-1$. Επομένως αν ο p διαιρεί την x^2-ay^2 τότε δεν θα διαιρεί την x^2+ay^2.

Έστω τώρα ότι ο p δεν διαιρεί την x^2-ay^2. Θα πρέπει να δείξουμε ότι τότε θα διαιρεί την x^2+ay^2, δηλαδή ότι ο $-a$ είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$, υπό την προϋπόθεση ότι ο a δεν είναι. Το κριτήριο του Euler

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p)$$

μας δίνει τώρα ότι αρκεί να αποδείξουμε $p|1+a^{\frac{p-1}{2}}$. Επειδή

$$a^{p-1}-1=\left(a^{\frac{(p-1)}{2}}-1\right)\left(a^{\frac{(p-1)}{2}}+1\right) \equiv 0\,(\mathrm{mod}\, p) \;\; (\text{μικρό θεώρημα Fermat})$$

αρκεί να δείξουμε ότι ο p δεν διαιρεί τον $a^{\frac{p-1}{2}}-1$.
Έστω ότι $p|a^{\frac{(p-1)}{2}}-1$. Θα ισχύει λοιπόν

$$x^{p-1}-1 \equiv x^{p-1}-a^{\frac{(p-1)}{2}} (\mathrm{mod}\, p).$$

Το πολυώνυμο όμως $x^{p-1}-1=(x^2)^{\frac{p-1}{2}}-a^{\frac{p-1}{2}}$ διαιρείται με το x^2-a. Τό $x^{p-1}-1$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο σώμα $\mathbb{F}_p$. Άρα και το x^2-a θα κάνει το ίδιο, δηλαδή η ισοδυναμία $x^2-a \equiv 0\,(\mathrm{mod}\, p)$ έχει λύση. Επομένως υπάρχει $x_0 \in \mathbb{Z}$ τέτοιο ώστε ο p να διαιρεί το x_0^2-a δηλαδή ο p είναι διαιρέτης της x^2-ay^2 (για $x=x_0,\ y=1$), άτοπο. □

Εντελώς ανάλογα, μπορεί κανείς να αποδείξει ότι:

Θεώρημα 4.5 *Κάθε indefinite τετραγωνική μορφή είναι γνήσια ισοδύναμη προς μία της οποίας ο πίνακας* $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ *έχει στοιχεία που πληρούν τις παρακάτω σχέσεις:*

$$|a| \leq |c|, \quad |b| \leq \frac{a}{2}.$$

Σημείωση: Εν γένει η ανάγωγη μορφή μιάς indefinite τετραγωνικής μορφής **δεν** είναι μονοσήμαντα ορισμένη. Επειδή $\Delta = ac - b^2 < 0$ έπεται ότι $ac < 0$ και συνεπώς $|\Delta| \geq 5b^2$, δηλαδή $|b| \leq \sqrt{\frac{|\Delta|}{5}}$.

Όπως και στις θετικές τετραγωνικές μορφές μπορούμε να φτιάξουμε ένα πίνακα:

Δ	Ανάγωγες indefinite τετρ. μορφές (όχι κατ' ανάγκη μη ισοδύναμες)
-2	$\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}$
-3	$\begin{pmatrix} 1 & 0 \\ 0 & -3 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix}$
-5	$\begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 1 \\ 1 & 2 \end{pmatrix}$
-6	$\begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 0 & 3 \end{pmatrix}$

Θα δώσουμε τώρα μερικές **εφαρμογές**:

(i) Κάθε πρώτος της μορφής $p = 8n + 3$ **παρίσταται από την τετραγωνική μορφή** $X^2 + 2Y^2$.

(ii) Κάθε πρώτος της μορφής $p = 12n + 7$ **παρίσταται από την τετραγωνική μορφή** $X^2 + 3Y^2$.

(iii) Κάθε πρώτος της μορφής $p = 24n + 7$ **παρίσταται από την τετραγωνική μορφή** $X^2 + 6Y^2$.

Απόδειξη:

(i) Έστω ότι ο p είναι διαιρέτης της X^2-2Y^2. Σύμφωνα με το Θεώρημα 4.1, υπάρχει τετραγωνική μορφή με ίδια διακρίνουσα που παριστά τον p. Σύμφωνα με τον πίνακα ο p θα παρίσταται από τετραγωνική μορφή X^2-2Y^2 ή $-X^2+2Y^2$. Η X^2-2Y^2 δίνει όμως $\pmod 8$ ± 1 και όχι 3 (το ίδιο και η $-X^2+2Y^2$). Άρα ο p δεν είναι διαιρέτης της X^2-2Y^2 συνεπώς ο p είναι διαιρέτης της X^2+2Y^2. Η διακρίνουσα της τελευταίας είναι 2. Επειδή δε υπάρχει μόνο μία κλάση έπεται ότι ο p παρίσταται από την X^2+2Y^2.

(ii) Έστω ότι ο πρώτος $p=12n+7$ είναι γνήσιος διαιρέτης της X^2-3Y^2. Θα παρίσταται λοπόν από την X^2-3Y^2 ή $-X^2+3Y^2$. Αν θεωρήσουμε τις τετραγωνικές μορφές $\pmod{12}$ τα δυνατά περιττά υπόλοιπα $\pmod{12}$ είναι $\pm 1, \pm 9, \pm 3$ αλλά όχι 7. Επομένως ο p δεν είναι διαιρέτης της X^2-3Y^2 και, σύμφωνα με το τελευταίο θεώρημα, θα είναι κάποιος διαιρέτης της X^2+3Y^2 (Η άλλη ανάγωγη τετραγωνική μορφή διακρίνουσας 3, $2X^2+2XY+2Y^2$ παριστά μόνο άρτιους). Ωστε:

Κάθε πρώτος $p=12n+7$ παρίσταται από την X^2+3Y^2.

(iii) Υποθέτουμε ότι ο $p=24n+7$ είναι ένας διαιρέτης της X^2-6Y^2. Τότε (δες προηγούμενο πίνακα) θα παρίσταται από κάποια των τετραγωνικών μορφών

$$\pm(X^2-6Y^2), \quad \text{ή} \quad \pm(2X^2-3Y^2).$$

Εύκολα βλέπει κανείς ότι αυτές οι τετραγωνικές μορφές δεν δίνουν $7 \pmod{24}$. Επομένως ο p παρίσταται από την X^2+6Y^2 ή $2X^2+3Y^2$. Η δεύτερη δεν δίνει $7 \pmod{24}$ συνεπώς ο p παρίσταται από την X^2+6Y^2. □

Ανάλογα ο Lagrange αποδεικνύει ότι, αν ο p είναι της μορφής $p=4n+1$, τότε ο p είναι διαιρέτης της X^2+aY^2 αν και μόνο αν ο p είναι διαιρέτης της X^2-aY^2 και βγάζει συμπεράσματα όπως:

- Κάθε πρώτος αριθμός της μορφής $p=8n+1$ παρίσταται από την X^2+2Y^2.
- Κάθε πρώτος αριθμός της μορφής $p=12n+1$ παρίσταται από την X^2+3Y^2.

- Κάθε πρώτος αριθμός της μορφής $p = 20n + 1$ παρίσταται από την $X^2 + 5Y^2$.

Έστω τώρα Q θετική τετραγωνική μορφή παριστώμενη από τον πίνακα M. Ένας πίνακας $T \in GL_2(\mathbb{Z})$ θα λέγεται μία **μονάδα** (ή ένας **αυτομορφισμός**) της Q αν και μόνο αν $T^tMT = M$, δηλαδή όταν ο T στέλνει την Q στον εαυτό της.

Μία **μονάδα** (**αυτομορφισμός**) της Q θα λέγεται **γνήσια** αν $\det(T) = 1$. Το σύνολο των γνησίων μονάδων της Q αποτελεί υποομάδα της $SL_2(\mathbb{Z})$, έστω U_Q. Αν δύο τετραγωνικές μορφές Q και Q' που παρίστανται από τους πίνακες M και N είναι γνήσια ισοδύναμες, δηλαδή

$$M = U^tNU, \ \text{με} \ U \in SL_2(\mathbb{Z})$$

τότε η συνάρτηση $T \to UTU^{-1}$ είναι **ισομορφισμός** μεταξύ των ομάδων U_Q και $U_{Q'}$. Η απόδειξη του τελευταίου ισχυρισμού αφήνεται σαν άσκηση στον αναγνώστη.

Χωρίς περιορισμό της γενικότητας τώρα μπορούμε να υποθέσουμε ότι η Q είναι **ανάγωγη**.

Ισχύει το εξής: (χωρίς απόδειξη, δες όμως την απόδειξη του Θεωρήματος 2)

Θεώρημα 4.6 *Οι γνήσιες μονάδες της $Q(X,Y) = a(X^2 + Y^2)$ είναι*

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{και} \quad \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}.$$

Της $Q(X,Y) = a(X^2 + 2XY + Y^2)$ είναι

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & 1 \end{pmatrix} \ \textit{και} \ \begin{pmatrix} \pm 1 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}.$$

Κάθε άλλη ανάγωγη τετραγωνική μορφή έχει μονάδες $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Ένα άλλο πρόβλημα με το οποίο ασχολήθηκε ο Lagrange ήταν η εξίσωση (του Fermat)

$$x^2 - dy^2 = 1.$$

Για να λύσει αυτό το πρόβλημα ο Lagrange κάνει χρήση και επεκτείνει τη θεωρία των συνεχών κλασμάτων. Ας θεωρήσουμε κατ' αρχήν την τετραγωνική μορφή που παρίσταται

από τον πίνακα: $\begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix}$. Τότε ο $\begin{pmatrix} x & u \\ y & v \end{pmatrix} \in GL_2(\mathbb{Z})$ είναι **μονάδα** αν και μόνο αν

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix} \begin{pmatrix} x & u \\ y & v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix}$$

δηλαδή $\begin{pmatrix} x & u \\ y & v \end{pmatrix}$ **μονάδα** τότε και μόνο τότε όταν

$$x^2 - dy^2 = 1,\ xu - dyv = 0,\ u^2 - dv^2 = -d.$$

Για $(x = \pm 1,\ y = 0)$ βρίσκουμε $u = 0$, $v = \pm 1$. Για $x, y \neq 0$ έχουμε

$$u = \frac{dyv}{x}, \quad -d = \frac{d^2y^2v^2}{x^2} - dv^2.$$

Συνεπώς

$$dy^2v^2 - v^2x^2 = -x^2 \quad \Longrightarrow \quad v^2(x^2 - dy^2) = x^2$$
$$\Longrightarrow \quad v^2 = x^2 \quad \Longrightarrow \quad v = \pm x.$$

Επομένως και $u = \pm dy$. Οι μονάδες λοιπόν είναι

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ \begin{pmatrix} x & dy \\ y & x \end{pmatrix},\ \begin{pmatrix} x & -dy \\ y & -x \end{pmatrix}$$

και οι μονάδες με ορίζουσα 1

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

Ο Lagrange ανέπτυξε κατά συστηματικό τρόπο τη θεωρία των συνεχών κλασμάτων.

Έστω $\theta \in \mathbb{R}$. Αν $\theta \notin \mathbb{Z}$ ορίζουμε $\theta := a_0 + \frac{1}{\theta_1}$ με $a_0 := [\theta]$, $\theta_1 > 1$. Συνεχίζουμε όμοια:

$$\theta_1 := a_1 + \frac{1}{\theta_2}, \quad \text{με} \quad a_1 := [\theta_1],\ \theta_2 > 1 \quad \text{αν} \quad \theta_1 \notin \mathbb{Z}.$$

$$\theta_n := a_n + \frac{1}{\theta_{n+1}}, \quad \text{με} \quad a_n := [\theta_n],\ \theta_{n+1} > 1 \quad \text{αν} \quad \theta_n \notin \mathbb{Z}.$$

Μπορούμε λοιπόν να γράψουμε

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\theta_{n+1}}}}}$$

Η ακολουθία $a_1, a_1, a_2, \ldots$ καλείται το **ανάπτυγμα του θ σε συνεχές κλάσμα**.

Εδώ θα ασχοληθούμε εν συντομία με τα αποτελέσματα της θεωρίας. Ο ενδιαφερόμενος μπορεί να βρεί τις αποδείξεις στο [3] ή στο [9].

Σ.Κ. 1 Το ανάπτυγμα σε συνεχές κλάσμα του αριθμού θ είναι **πεπερασμένο** αν και μόνο αν $\theta \in \mathbb{Q}$.

Συνεχή κλάσματα των

$$\begin{aligned}
\pi &: \quad 3, 7, 15, 1, 293, \ldots \\
e &: \quad 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots \\
\sqrt{2} &: \quad 1, 2, 2, 2, \ldots \\
\sqrt{3} &: \quad 1, 1, 2, 1, 2, 1, \ldots \\
\sqrt{5} &: \quad 2, 4, 4, 4, \ldots \\
\sqrt{6} &: \quad 2, 2, 4, 2, 4, 2, \ldots
\end{aligned}$$

Αν $a_0, a_1, \cdots, a_n \in \mathbb{R}$, $a_1, a_2, \cdots, a_n \geq 1$ γράφουμε

$$\langle a_0, a_1, \cdots, a_n \rangle := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

Αν $a_n > 1$ μπρούμε να γράψουμε $a_n = a_n - 1 + \frac{1}{1}$, οπότε

$$\langle a_0, a_1, a_2, \cdots, a_n \rangle = \langle a_0, a_1, \cdots, a_{n-1}, a_n - 1, 1 \rangle \, .$$

Το συνεχές κλάσμα, λοιπόν, ρητού αριθμού είναι μονοσήμαντα ορισμένο, αλλά έχει, κατά βούληση, άρτιο ή περιττό μήκος.

Σ.Κ. 2: Αν $\langle a_0, a_1, \cdots, a_m \rangle = \langle b_0, b_1, \cdots, b_n \rangle$, $a_i, b_j \in \mathbb{Z}$, $a_i \geq 1$, $b_j \geq 1$ και $a_m, b_n > 1$ τότε $m = n$ και $a_i = b_i$ για κάθε $i = 1, 2, 3 \cdots, m$. Αν $\alpha = \langle a_0, a_1, \cdots a_n \rangle$ το συνεχές κλάσμα ρητού αριθμού ($a_n > 1$) τότε ο ρητός αριθμός $\dfrac{P_i}{Q_i} = \langle a_o, a_1, \cdots, a_i \rangle$ θα λέγεται **ι-οστός συγκλίνων** του συνεχούς κλάσματος. Θέτουμε $P_{-2} = Q_{-1} = 0$, $P_{-1} = Q_{-2} = 1$.

Σ.Κ. 3: Ισχύει:

$$\left\{ \begin{array}{c} P_i = a_i P_{i-1} + P_{i-2} \\ Q_i = a_i Q_{i-1} + Q_{i-2} \end{array} \right\} \quad 0 \leq i \leq n.$$

Σ.Κ. 4: Ισχύουν τα ακόλουθα:

(i) $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^{k-1}$, για $1 \leq k \leq n$.

(ii) Για κάθε k τέτοιο ώστε $0 \leq k \leq n$, ισχύει $(P_k, Q_k) = 1$.

(iii) $\dfrac{P_k}{Q_k} - \dfrac{P_{k-1}}{Q_{k-1}} = \dfrac{(-1)^{k-1}}{Q_k Q_{k+1}}$.

(iv) $\dfrac{P_k}{Q_k} - \dfrac{P_{k-2}}{Q_{k-2}} = \dfrac{(-1)^k a_k}{Q_k Q_{k-2}}$.

(v) $Q_i \geq Q_{i-1}$, για κάθε i, $1 \leq i \leq n$ (μάλιστα δε με αυστηρώς θετική ανισότητα για $i > 1$, οπότε προκύπτει ότι $Q_i > i$ για κάθε $i = 1, 2, \ldots, n$).

(vi)

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \cdots < \frac{P_n}{Q_n} < \cdots < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}$$

(vii) Για κάθε i, $1 \leq i \leq n$ ισχύει:

$$|\alpha - \frac{P_i}{Q_i}| < |\alpha - \frac{P_{i-1}}{Q_{i-1}}| \quad \text{και} \quad |\alpha Q_i - P_i| < |\alpha Q_{i-1} - P_{i-1}|.$$

Σημείωση: Όλες οι ιδιότητες της Σ.Κ. 4 ισχύουν και για **άπειρα** συνεχή κλάσματα, αρκεί να εγκαταλείψουμε τα άνω φράγματα για τους δείκτες.

Παίρνουμε την ακολουθία $\left\{ \dfrac{P_{2k}}{Q_{2k}} \right\}_{k \geq 0}$ η οποία είναι αύξουσα και φραγμένη από πάνω και $\left\{ \dfrac{P_{2k+1}}{Q_{2k+1}} \right\}_{k \geq 0}$ η οποία είναι φθίνουσα και φραγμένη από κάτω. Αν

$$\lim_{k \to \infty} \frac{P_{2k}}{Q_{2k}} = S \qquad \text{και} \qquad \lim_{k \to \infty} \frac{P_{2k+1}}{Q_{2k+1}} = T$$

αποδεικνύεται ότι $S = T$, δηλαδή **κάθε άπειρο** συνεχές κλάσμα $\langle a_0, a_1, \cdots, a_n, \ldots \rangle$ παριστά ένα πραγματικό αριθμό (προφανώς λόγω Σ.Κ. 1, άρρητο).

Ισχύει δε και το αντίστροφο, δηλαδή ότι

Σ.Κ. 5: Κάθε άρρητος αριθμός, παρίσταται σαν συνεχές κλάσμα κατά τρόπο **μοναδικό**.

Κάθε συνεχές κλάσμα της μορφής $\langle a_0, a_1, \ldots, a_{n-1}, b_1, b_2, \ldots, b_k, b_1, b_2, \ldots, b_k, \ldots\rangle$ θα λέγεται **περιοδικό** (γράφεται $\langle a_0, a_1, \ldots, a_{n-1}, \overline{b_1, b_2, \ldots, b_k}\rangle$).
Ισχύει:

Σ.Κ. 6: Ο $\theta \in \mathbb{R}$ αναπτύσσεται σε περιοδικό συνεχές κλάσμα αν και μόνο αν $\theta = \alpha + \beta\sqrt{d}$, $\alpha, \beta \in \mathbb{Q}$ και $d \in \mathbb{N}$, d όχι τέλειο τετράγωνο.

Εάν τώρα η περίοδος αρχίζει από την αρχή, δήλαδή $\theta = \langle\overline{a_0, a_1, \ldots, a_{n-1}}\rangle$ τότε το συνεχές κλάσμα λέγεται **καθαρά περιοδικό**. Ισχύει δε

Σ.Κ. 7: Ο $\theta = \alpha + \beta\sqrt{d}$ αναπτύσσεται σε καθαρά περιοδικό κλάσμα τότε και μόνο τότε όταν $\theta > 1$ και $-1 < \theta' < 0$ όπου $\theta' = \alpha - \beta\sqrt{d}$.

Με την βοήθεια τώρα των παραπάνω αποδεικνύεται το

Θεώρημα 4.7 *Όλες οι θετικές λύσεις της $x^2 - dy^2 = \pm 1$ δίνονται από τους συγκλίνοντες του αναπτύγματος του συνεχούς κλάσματος του αριθμού $\sqrt{d}$. Αν n είναι το μήκος της περιόδου του συνεχούς κλάσματος $\sqrt{d}$ και ο n είναι άρτιος τότε η $x^2 - dy^2 = -1$ δεν έχει λύση. Σ΄ αυτή την περίπτωση όλες οι θετικές λύσεις της $x^2 - dy^2 = 1$ δίνονται από $x = P_{nj-1}$, $y = Q_{nj-1}$ για $j = 1, 2, 3, \ldots$. Αν τώρα ο n είναι περιττός, όλες οι θετικές λύσεις της $x^2 - dy^2 = -1$ δίνονται από $x = P_{nj-1}$ και $y = Q_{nj-1}$, $j = 1, 3, 5, \ldots$ και όλες οι θετικές λύσεις της $x^2 - dy^2 = 1$ από $x = P_{nj-1}$, $y = Q_{nj-1}$, για $j = 2, 4, 6, \ldots$*

Ισχύει ακόμη και το

Θεώρημα 4.8 *Έστω (x_1, y_1) η ελάχιστη λύση της $x^2 - dy^2 = 1$. Όλες οι θετικές λύσεις τότε δίνονται από τις σχέσεις*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \qquad n = 1, 2, 3, \ldots$$

Παραδείγματα:

(1) Έστω $d = 2$, δηλαδή έχουμε την εξίσωση $x^2 - 2y^2 = 1$. Ισχύει:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + (\sqrt{2} - 1)} = \left\langle 1, \overline{2} \right\rangle .$$

Ο $n = 1$, περιττός. Επομένως όλες οι λύσεις δίνονται από

$$x = P_{j-1},\ y = Q_{j-1},\ j = 2, 4, 6, \cdots$$

Η πιο μικρή $x = P_1$, $y = Q_1$

	-2	-1	0	1	2
a_i			1	2	2
P_i	0	1	1	3	7
Q_i	1	0	1	2	5

Επομένως $\theta_1 = 3 + \sqrt{2}$ και $x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n$, $n = 1, 2, 3, \ldots$.

(2) Έστω $d = 33$, $\sqrt{33} = [5; \overline{1, 2, 1, 10}]$ και $n = 4$ άρτιος.

	-2	-1	0	1	2	3	4
a_i			5	1	2	1	10
P_i	0	1	5	6	17	23	247
Q_i	1	0	1	1	3	4	43

Οι λύσεις θα είναι:

$$x = P_{4j-1},\ y = Q_{4j-1}.$$

Η μικρότερη $x = P_3 = 23$, $y = Q_3 = 4$. Άρα όλες οι άλλες $x_n + y_n\sqrt{d} = (23 + 4\sqrt{33})^n$, $n \in \mathbb{N}$.

Ο Adrien-Marie Legendre γεννήθηκε στο Παρίσι το 1752. Όπως και ο Λαγρανγε υπήρξε γόνος πλούσιας οικογενείας. Στα 1770 άρχισε τις σπουδές του στα Μαθηματικά και τη Φυσική. Ήταν οικονομικά ανεξάρτητος και έτσι μπορούσε να αφιερώνει τον χρόνο του στην έρευνα. Από το 1775 μέχρι το 1780 ήταν δάσκαλος της Ecole Militaire στο Παρίσι. Μετά το 1783 καταλαμβάνει διάφορες θέσεις στη Γαλλική Ακαδημία, στην αρχή σαν διάδοχος του Laplace σαν "adjoint mecanicien" και αργότερα από το 1785 σαν "associe". Το 1782 κέρδισε ένα βραβείο της Ακαδημίας του Βερολίνου με μία εργασία με θέμα από την περιοχή της Βαλλιστικής. Αυτό υπήρξε και η αιτία που τον πρόσεξε ο Lagrange. Αργότερα δημοσίευσε εργασίες πάνω στην Θεωρία Αριθμών, Ουράνιο Μηχανική και στη Θεωρία των Ελλειπτικών Συναρτήσεων. Κατά τη Γαλλική Επανάσταση έχασε όλη του την περιουσία και υποχρεώθηκε να παραιτηθεί από τη θέση του στην Ακαδημία. Από το 1799 μέχρι το 1815 ήταν εξεταστής της Ecole Polytechnique. Από το 1813 και μέχρι το θάνατό του το 1833 διαδέχθηκε τον Lagrange στο Bureau des Longitudes.

Το έργο του στη Θεωρία των Αριθμών αποτελείται από μία εργασία με τίτλο "Recherches d' Analyse Indéterminées" που έγινε δεκτή στην Γαλλική Ακαδημία το 1785 (δημοσιεύθηκε στα 1788) (Όταν ο Gauss ανακάλυψε την εργασία αυτή στη βιβλιοθήκη του Πανεπιστημίου του Göttingen, έγραψε στον δάσκαλό του Zimmerman τον εξής χαρακτηρισμό για το βιβλίο **"eine vortreffliche Abhandlung"**) και ένα βιβλίο Θεωρίας Αριθμών το οποία εκδόθηκε στα 1798 με τον τίτλο: **Essai sur la theorie des nombres**. Στο βιβλίο περιγράφει τις γνώσεις Θεωρίας Αριθμών της εποχής (μεταξύ άλλων αποτελέσματα των Euler, Lagrange) καθώς και πολλούς πίνακες για να δείξει αποτελέσματα που πίστευε την αλήθεια τους αλλά δεν μπορούσε να αποδείξει. Το έργο ξαναεκδόθηκε με πολλές προσθήκες στα 1808 και, δίτομο, στα 1830 με τίτλο ''Θεωρία Αριθμών''. Θα πρέπει ίσως να παρατηρήσει κανείς ότι το περιεχόμενο του βιβλίου υπερκεράστηκε από το στα 1801 εκδοθέν βιβλίο του Gauss "Disquisitiones Arithmeticae".

Ένα από τα βασικά θεωρήματα που απέδειξε ο Legendre στο τρίτο μέρος των Recherches του είναι το ακόλουθο:

Θεώρημα 4.9 *Έστω ότι a, b, c είναι ακέραιοι όχι και οι τρεις με το ίδιο πρόσημο και*

abc ελεύθερου τετραγώνου. Η εξίσωση $aX^2 + bY^2 + cZ^2 = 0$ *έχει μία ακέραια λύση με* $(x, y, z) \neq (0, 0, 0)$ *τότε και μόνο τότε όταν* $-bc, -ca, -ab$ *είναι τετραγωνικά υπόλοιπα* $(mod\,|a|)$, $(mod\,|b|)$ *και* $(mod\,|c|)$ *αντίστοιχα.*

Μία απόδειξη του θεωρήματος αυτού θα δώσουμε αργότερα.

Στο τέταρτο μέρος της εργασίας του (Recherches) ο Legendre χρησιμοποιεί το θεώρημα αυτό στην προσπάθειά του να αποδείξει τον γνωστό σήμερα σαν **τετραγωνικό νόμο αντιστροφής**. Όπως είναι γνωστό, πρόκειται για μία σχέση ανάμεσα στο λεγόμενο σήμερα **σύμβολο του Legendre** $\left(\frac{p}{q}\right)$ και $\left(\frac{q}{p}\right)$ το οποίο εισήχθη από τον Legendre στα 1798. Στην προσπάθειά του αυτή ο Legendre είχε μόνο μερική επιτυχία. Αυτό που κάνει είναι να ξεχωρίζει 8 περιπτώσεις ανάλογα με τις τιμές των p και $q \pmod 4$ και της τιμής $\left(\frac{p}{q}\right)$. Το ίδιο επιχείρημα χρησιμοποιεί και ο Gauss στην πρώτη του απόδειξη (δες [5], άρθρο 136). Σε κάθε μία από αυτές τις περιπτώσεις ο Legendre εισάγει μία κατάλληλη εξίσωση της μορφής $aX^2 + bY^2 + cZ^2 = 0$ με $a \equiv b \equiv c \equiv 1 \pmod 4$. Η εξίσωση αυτή δεν έχει μη-τετριμμένη λύση διότι η ισοδυναμία $aX^2 + bY^2 + cZ^2 \equiv 0 \pmod 4$ δεν έχει λύση. Σύμφωνα λοιπόν με το προηγούμενο θεώρημα, δεν μπορούν οι αριθμοί $-bc, -ca, -ab$ να είναι και οι τρείς τετραγωνικά υπόλοιπα $\pmod{|a|}$, $\pmod{|b|}$ και $\pmod{|c|}$ αντιστοίχως. Σε κάθε παρίπτωση ο Legendre προσπαθεί να διαλέξει τα a, b, c κατά τέτοιο τρόπο ώστε να έχει το αποτέλεσμα που θέλει.
Παίρνει κατ' αρχήν

$$p \equiv 1 \pmod 4,\ q \equiv -1 \pmod 4,\ \left(\frac{p}{q}\right) = -1$$

και θεωρεί την εξίσωση $X^2 + pY^2 - qZ^2 = 0$. Λόγω της $\left(\frac{-1}{q}\right) = -1$ έπεται $\left(\frac{-p}{q}\right) = 1$. Επειδή $\left(\frac{pq}{1}\right) = 1$ και $\left(\frac{-p}{q}\right) = 1$ έχουμε $\left(\frac{q}{p}\right) = -1$ όπως πράγματι χρειάζεται για να ισχύει ο τετραγωνικός νόμος αντιστροφής.

Το ίδιο μπορούμε να κάνουμε για $q \equiv q' \equiv -1 \pmod 4$ και $\left(\frac{q}{q'}\right) = 1$, κάνοντας χρήση της εξίσωσης

$$X^2 - qY^2 - q'Z^2 = 0.$$

Τώρα παίρνουμε $q \equiv q' \equiv -1 (\mathrm{mod}\, 4)$, $\left(\frac{q}{q'}\right) = -1$ και θεωρούμε την $pX^2 - qY^2 - q'Z^2 = 0$ όπου ο p είναι κάποιος πρώτος που πληροί τις συνθήκες

$$p \equiv 1 \,(\mathrm{mod}\, 4),\ \left(\frac{p}{q}\right) = -1,\ \left(\frac{p}{q'}\right) = -1.$$

Οπότε, όπως και παραπάνω, θα πρέπει $\left(\frac{q'}{q}\right) = 1$, δηλαδή να ισχύει και εδώ ο τετραγωνικός νόμος αντιστροφής.

Το πρόβλημα βέβαια που μένει ανοιχτό είναι αν **υπάρχει** πρώτος με αυτές τις ιδιότητες. Υπάρχει τέτοιος πρώτος αν η αριθμητική πρόοδος

$$\Big\{4qq'x + m | \text{με } x \in \mathbb{Z} \ \text{ και } \ 0 < m < 4qq' \ \text{ τέτοιο ώστε } \ m \equiv 1 \,(\mathrm{mod}\, 4),$$
$$\left(\frac{m}{q}\right) = -1,\ \left(\frac{m}{q'}\right) = -1\Big\}$$

περιέχει έναν πρώτο. Ο Legendre ήταν πεπεισμένος ότι κάθε αριθμητική πρόοδος $\{ax + b | x \in \mathbb{Z}$ με $(a, b) = 1\}$ περιέχει άπειρους το πλήθος πρώτους.

''Ίσως είναι αναγκαίο να αποδειχθεί αυτό προσεκτικά'', έγραφε στα 1785. **''Δεν πρέπει να αμφιβάλλουμε γι΄ αυτό''**, έγραψε στα 1798. Η πρώτη πάντως απόδειξη, ανήκει στον Dirichlet (1837) ο οποίος ανέπτυξε μία πέρα για πέρα πρωτότυπη μέθοδο. Το αποτέλεσμα αυτό θεωρείται μία από τις πιο σπουδαίες συνεισφορές του Dirichlet στα Μαθηματικά.

Ο Legendre θεώρησε το θεώρημα αυτό του Dirichlet σαν ένα είδος αξιώματος και συνέχισε αλλά μετά ήρθαν τα... χειρότερα.

Ας πάρουμε τώρα την περίπτωση που $p \equiv p' \equiv 1 \,(\mathrm{mod}\, 4)$, και ας θεωρήσουμε την $pX^2 + p'Y^2 - qZ^2 = 0$ όπου q είναι πρώτος αριθμός που πληροί τις σχέσεις:

$$q \equiv -1 \,(\mathrm{mod}\, 4),\ \ \left(\frac{q}{p'}\right) = 1,\ \ \left(\frac{p}{q}\right) = -1$$

ή την εξίσωση $X^2 + pY^2 - p'qZ^2 = 0$, όπου q πρώτος $q \equiv -1 \,(\mathrm{mod}\, 4)$, $\left(\frac{p}{q}\right) = -1$. Το πρόβλημα όμως είναι και πάλι αν **υπάρχει** τέτοιος πρώτος.

Κάτι τέτοιο θα μπορούσε να ήταν συνέπεια του θεωρήματος του Dirichlet **και** του τετραγωνικού νόμου αντιστροφής! Κατ' αυτόν τον τρόπο ''βραχυκυκλώθηκε'' η απόδειξη του

Legendre, ενώ είναι αμφίβολο, όπως σημείωσε και ο Gauss στο άρθρο 297, αν μπορούσε να αποδειχθεί αλλιώς. Αυτό όμως το ''βραχυκύκλωμα'' δεν απέτρεψε τον Legendre από το να δηλώνει πικραμένος σε γράμμα του προς τον Jacobi στα 1827 ότι άδικα ο Gauss ισχυρίζεται ότι ανακάλυψε πρώτος τον τετραγωνικό νόμο αντιστροφής.

Όπως είπαμε και πιό μπροστά η εικασία του Fermat είχε λυθεί για $n = 4$ από τον ίδιο τον Fermat και για $n = 3$ από τον Euler. Από τότε το πρόβλημα αποτελούσε πρόκληση για τους αριθμοθεωρητικούς. Στις εκδόσεις του 1798 και του 1808 του βιβλίου του ο Legendre δεν έδωσε τίποτε περισσότερο από τις αποδείξεις των Fermat και Euler για $n = 4$ και 3 αντίστοιχα. Το ενδιαφέρον για το πρόβλημα ξαναζωντάνεψε στο Παρίσι τις επόμενες δεκαετίες, ιδιαίτερα μετά την ανακοίνωση της Γαλλική Ακαδημίας να δώσει ένα βραβείο σε εργασία σχετική με τη Θεωρία Αριθμών. Ο Olbers επέστησε την προσοχή του Gauss σ′ αυτό το γεγονός, και ο Gauss απάντησε ότι δεν τον ενδιαφέρει πολύ το πρόβλημα αλλά η λύση του θα προκύψει κατά τη γνώμη του, μέσω της επέκτασης της θεωρίας της ανώτερης αριθμητικής (einer grossen Erweiterung der höheren Arithmetik).

Στο μεταξύ άρχισε να δουλεύει στο πρόβλημα η Sophie Germain και ανακάλυψε σύντομα ενδιαφέροντα αποτελέσματα.

Στα 1825 οι Dirichlet και Legendre απέδειξαν την εικασία του Fermat για $n = 5$ (κάνοντας χρήση της μεθόδου της καθόδου του Fermat). Ο Dirichlet απέδειξε πρώτος ότι η εξίσωση $x^5 + y^5 + z^5 = 0$ δεν έχει μη-τετριμμένη ακέραια λύση στην περίπτωση που ένας από τους αγνώστους είναι πολλαπλάσιο του 10. Ο Legendre χρησιμοποίησε τις τεχνικές του Dirichlet και έλυσε το πρόβλημα χωρίς περιορισμό. Στο τέλος της ζωής του ευχαριστήθηκε ιδιαιτέρως που είδε τη θεωρία των ελλειπτικών συναρτήσεων να επεκτείνεται τόσο με την συνεισφορά των Abel και Jacobi.

Θα κλείσουμε με τη μελέτη της διοφαντικής εξίσωσης

$$ax^2 + by^2 + cz^2 = 0$$

όπου οι a, b, c δεν διαιρούνται με το τετράγωνο πρώτου αριθμού και $(a, b) = (b, c) = (a, c) = 1$.

Για να έχει η εξίσωση μη-τετριμμένη λύση θα πρέπει να μην είναι όλοι οι a, b, c συγχρόνως θετικοί ή όλοι συγχρόνως αρνητικοί.

Έστω m και n μη μηδενικοί ακέραιοι. Με mRn συμβολίζουμε την πρόταση:

"Ο m είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, n)$"

Επαναλαμβάνουμε το θεώρημα του Legendre:

Θεώρημα 4.10 *Έστω a, b, c ακέραιοι διάφοροι του μηδενός των οποίων το γινόμενο δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Υποθέτουμε ακόμη ότι δεν είναι και οι τρεις ομόδημοι και $(a, b) = (b, c) = (a, c) = 1$. Τότε η εξίσωση $aX^2 + bY^2 + cZ^2 = 0$ έχει μία μη-τετριμμένη ακέραια λύση αν και μόνο αν*

(i) $-abRc$

(ii) $-acRb$

(iii) $-bcRa$.

Κατ' αρχήν αποδεικνύουμε τα παρακάτω δύο λήμματα:

Λήμμα 4.11 *Έστω λ, μ, ν θετικοί πραγματικοί αριθμοί με γινόμενο $\lambda\mu\nu = m$, m ακέραιος. Τότε κάθε ισοδυναμία της μορφής $\alpha x+\beta y+\gamma z \equiv 0 (mod\, m)$ έχει μία μη-τετριμμένη λύση (x, y, z), τέτοια ώστε $|x| \leq \lambda$, $|y| \leq \mu$, $|z| \leq \nu$.*

Απόδειξη: Έστω ότι το x διατρέχει τους $0, 1, 2, \ldots, [\lambda]$, το y τους $0, 1, 2, \ldots, [\mu]$ και το z τους $0, 1, 2, \ldots, [\nu]$. Συνολικά έχουμε $(1 + [\lambda])(1 + [\mu])(1 + [\nu])$ διαφορετικές τριάδες (x, y, z). Αφού $(1 + [\lambda])(1 + [\mu])(1 + [\nu]) > \lambda\mu\nu = m$ έπεται ότι υπάρχουν δύο τριάδες (x_1, y_1, z_1) και (x_2, y_2, z_2) τέτοιες ώστε:

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \pmod{m}$$

$$\Longrightarrow \alpha(x_1 - x_2) + \beta(y_1 - y_2) + \gamma(z_1 - z_2) \equiv 0 \pmod{m}$$

όπου $|x_1 - x_2| \leq [\lambda] \leq \lambda$, $|y_1 - y_2| \leq \mu$, $|z_1 - z_2| \leq \nu$. □

Λήμμα 4.12 *Υποθέτουμε ότι η τετραγωνική μορφή* $aX^2 + bY^2 + cZ^2$ *αναλύεται σε γινόμενο πρωτοβάθμιων παραγόντων μοδ* m *και μοδ* n. *Αν* $(m, n) = 1$ *τότε* $aX^2 + bY^2 + cZ^2$ *αναλύεται σε γινόμενο γραμμικών παραγόντων* $(\mathrm{mod}\, mn)$.

Απόδειξη: Έχουμε

$$\begin{aligned} aX^2 + bY^2 + cZ^2 &\equiv (\alpha_1 X + \beta_1 Y + \gamma_1 Z)(\alpha_2 X + \beta_2 Y + \gamma_2 Z) \pmod m \\ aX^2 + bY^2 + cZ^2 &\equiv (\alpha_3 X + \beta_3 Y + \gamma_3 Z)(\alpha_4 X + \beta_4 Y + \gamma_4 Z) \pmod n \end{aligned}$$

Διαλέγουμε $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ έτσι ώστε:

$$\alpha \equiv \alpha_1,\ \beta \equiv \beta_1,\ \gamma \equiv \gamma_1,\ \alpha' \equiv \alpha_2,\ \beta' \equiv \beta_2,\ \gamma' \equiv \gamma_2 \pmod m$$

$$\alpha \equiv \alpha_3,\ \beta \equiv \beta_3,\ \gamma \equiv \gamma_3,\ \alpha' \equiv \alpha_4,\ \beta' \equiv \beta_4,\ \gamma' \equiv \gamma_4 \pmod n$$

(θεώρημα υπολοίπων του Κινέζου). Τότε η ισοδυναμία

$$aX^2 + bY^2 + cZ^2 \equiv (\alpha X + \beta Y + \gamma Z)(\alpha' X + \beta' Y + \gamma' Z)$$

ισχύει $(\mathrm{mod}\, m)$ και $(\mathrm{mod}\, n)$. Επομένως είναι σωστή και $(\mathrm{mod}\, mn)$. □

Απόδειξη του θεωρήματος:

Έστω $aX^2+bY^2+cZ^2 = 0$, έχει μία λύση $(x_0, y_0, z_0) \neq 0$. Διαιρούμε τους x_0, y_0, z_0 με τον μέγιστο κοινό διαιρέτη (x_0, y_0, z_0) και βρίσκουμε μία λύση (x_1, y_1, z_1) με $(x_1, y_1, z_1) = 1$. Ισχύει $(c, x_1) = 1$. Έστω p πρώτος, $p|c$ και $p|x_1$. Αφού abc δεν διαιρείται με το τετράγωνο πρώτου αριθμού έπεται ότι ο p δεν διαιρεί τον b. Αλλά $p|cx_1$ συνεπώς $p|by_1^2$, επομένως $p|y_1$, δηλαδή $p^2|(ax_1^2 + by_1^2)$ από το οποίο συμπεραίνουμε ότι $p^2|cz_1^2$ δηλαδή $p|z_1^2 \Rightarrow p|z_1$. Επομένως θα είχαμε $p|(x_1, y_1, z_1) = 1$, άτοπο.

Έστω u η λύση της ισοδυναμίας $ux_1 \equiv 1 \pmod c$. Η εξίσωση $ax_1^2 + by_1^2 + cz_1^2 = 0$ δίνει $ax_1^2 + by_1^2 \equiv 0 \pmod c$ επομένως $u^2b^2y_1^2 \equiv -ab \pmod c$ δηλαδή $-abRc$. Όμοια αποδεικνύεται ότι $-bcRa$ και $-acRb$.

Αντιστρόφως, υποθέτουμε ότι ισχύουν οι σχέσεις (i), (ii) και (iii). Προφανώς δεν αλλάζουν αν τα a, b, c τα αντικαταστήσουμε με $-a, -b, -c$ αντίστοιχα. Χωρίς περιορισμό της

γενικότητας λοιπόν υποθέτουμε ότι $a > 0$, $b < 0$, $c < 0$.

Έστω r μία λύση της ισοδυναμίας $r^2 \equiv -ab (\mathrm{mod}\, c)$, και a_1 μία λύση της $aa_1 \equiv 1 (\mathrm{mod}\, c)$. Επομένως

$$\begin{aligned} aX^2 + bY^2 &\equiv aa_1(aX^2 + bY^2) \equiv a_1(a^2X^2 + abY^2) \\ &\equiv a_1(a^2X^2 - r^2Y^2) \equiv a_1(aX - rY)(aX + rY) \\ &\equiv (X - a_1rY)(aX + rY)\, (\mathrm{mod}\, c) \end{aligned}$$

$$\Longrightarrow aX^2 + bY^2 + cZ^2 \equiv (X - a_1rY)(aX + rY)\, (\mathrm{mod}\, c).$$

Αποδείξαμε λοιπόν ότι το $aX^2 + bY^2 + cZ^2$ αναλύεται σε γινόμενο δύο πρωτοβαθμίων παραγόντων $(\mathrm{mod}\, c)$. Όμοια αποδεικνύεται το ίδιο $(\mathrm{mod}\, a)$ και $(\mathrm{mod}\, b)$. Από το Λήμμα 4.2 τώρα παίρνουμε:

$$aX^2 + bY^2 + cZ^2 \equiv (\alpha X + \beta Y + \gamma Z)(\alpha' X + \beta' Y + \gamma' Z)\, (\mathrm{mod}\, abc).$$

Εφαρμόζουμε το Λήμμα 1 στην ισοδυναμία $\alpha X + \beta Y + \gamma Z \equiv 0\, (\mathrm{mod}\, abc)$ με $\lambda := \sqrt{bc}$, $\mu := \sqrt{|ac|}$, $\nu := \sqrt{|ab|}$ και συμπεραίνουμε ότι η ισοδυναμία έχει λύση x_1, y_1, z_1 με

$$|x_1| \leq \sqrt{bc}, \quad |y_1| \leq \sqrt{|ac|}, \quad |z_1| \leq \sqrt{|ab|}$$

Επειδή $(b, c) = 1$, παρατηρούμε ότι $\sqrt{bc} \in \mathbb{Z}$ τότε και μόνο όταν $bc = 1$. Επομένως $|x_1| \leq \sqrt{bc}$ δηλαδή $x_1^2 \leq bc$ (Μάλιστα η ισότητα $x_1^2 = bc$ ισχύει τότε και μόνο τότε όταν $b = c = 1$).

Όμοια $y_1^2 \leq -ac$ ($y_1^2 = -ac$ αν και μόνο αν $a = 1$, $c = -1$).
$z_1^2 \leq -ab$ ($z_1^2 = -ab$ αν και μόνο αν $a = 1, b = -1$).
Άρα, εκτός από την περίπτωση $b = c = -1$, ισχύει $ax_1^2 + by_1^2 + cz_1^2 \leq ax_1^2 < abc$ και

$$ax_1^2 + by_1^2 + cz_1^2 \;\geq\; by_1^2 + cz_1^2 \;>\; b(-ac) + c(-ab) \;=\; -2abc.$$

Αν εξαιρέσουμε λοιπόν την περίπτωση $b = c = -1$ έχουμε

$$-2abc \;<\; ax_1^2 + by_1^2 + cz_1^2 \;<\; abc.$$

Η τριάδα όμως (x_1, y_1, z_1) είναι λύση της ισοδυναμίας

$$ax^2 + by^2 + cz^2 \equiv 0 \,(\mathrm{mod}\, abc) \Longrightarrow ax_1^2 + by_1^2 + cz_1^2 = 0 \;\; \text{ή} \;\; -abc.$$

Στην πρώτη περίπτωση, η (x_1, y_1, z_1) είναι λύση της $ax^2 + by^2 + cz^2 = 0$. Στην δεύτερη περίπτωση μία λύση είναι η

$$x_2 = -by_1 + x_1 z_1, \quad y_2 = ax_1 + y_1 z_1, \quad z_2 = z_1^2 + ab.$$

Έστω τώρα $b = c = -1$. Τότε $-1Ra$. Επομένως αν $R(a)$ συμβολίζει το πλήθος των λύσεων της ισοδυναμίας $X^2 \equiv -1 \,(\mathrm{mod}\, a)$, τότε $R(a) > 0$. Έστω ακόμη $Q(n)$ το πλήθος των λύσεων της εξίσωσης $X^2 + Y^2 = n$, $(X, Y) = 1$. Χωρίς απόδειξη εδώ αναφέρουμε ότι ισχύει $Q(1) = 4$, $Q(n) = 4R(n)$ για $n \geq 1$.

Άρα $Q(a) > 0$. Συνεπώς η εξίσωση $U^2 + Z^2 = a$ έχει κάποια λύση y_1, z_1 με $(y_1, z_1) = 1$. Η $Q = 1$, $U = y_1$, $Z = z_1$ είναι μία μη-τετριμμένη λύση της εξίσωσης $aX^2 + bY^2 + cZ^2 = 0$.

□

Ένα πολύ σπουδαίο πόρισμα του θεωρήματος είναι το λεγόμενο **"Αξίωμα του Hasse"**. Σε γενικές γραμμές το αξίωμα είναι:

> **"Η τοπική (local) επιλυσιμότητα μιάς εξίσωσης συνεπάγεται την γενική (global) επιλυσιμότητα".**

Τοπική επιλυσιμότητα σημαίνει ότι η εξίσωση έχει μία μη-τετριμμένη λύση modulo p^m για όλους τους πρώτους αριθμούς p και όλους τους θετικούς ακεραίους m και μία πραγματική, στο σώμα $\mathbb{R}$, λύση.

Γενική επιλυσιμότητα σημαίνει ότι έχει λύση στους ακεραίους.

Το αξίωμα του Hasse ισχύει για τετραγωνικές μορφές αλλά είναι, εν γένει, λάθος για εξισώσεις βαθμού ανωτέρου του δύο. Παραδείγματος χάριν, θα μπορούσε να αποδείξει κανείς ότι η εξίσωση $X^4 - 17Y^4 = 2Z^4$ έχει μη-τετριμμένη λύση modulo p^m για κάθε πρώτο p και θετικό m και μία πραγματική λύση, αλλά δεν έχει λύση στους ακεραίους ([8]).

Πόρισμα 4.13 *Έστω a, b, c ακέραιοι των οποίων το γινόμενο δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Υποθέτουμε ακόμη ότι δεν είναι όλοι τους ομόσημοι και ότι $(a, b) = (b, c) = (c, a) = 1$. Αν η ισοδυναμία $aX^2 + bY^2 + cZ^2 \equiv 0 \, (mod p^m)$ έχει ακέραια λύση x, y, z για κάθε δύναμη p^m, όπου ο πρώτος p δεν διαιρεί τον μέγιστο κοινό διαιρέτη (x, y, z), τότε η $aX^2 + bY^2 + cZ^2 = 0$ έχει μη-τετριμμένη ακεραία λύση.*

Απόδειξη: Έστω $m = 2$ και $p|a$. Τότε αν (x, y, z) είναι μία λύση, σύμφωνα με τις υποθέσεις του πορίσματος, θα δείξουμε ότι ο p δεν διαιρεί το yz.

Αν $p|y$ τότε $p|cz^2$ και επομένως, αφού $(a, c) = 1$, έχουμε $p|z$. Ωστε $p^2|ax^2$ και αφού ο p δεν διαιρεί το x έπεται ότι $p^2|a$, άτοπο. Συνεπώς $p \nmid y$. Όμοια αποδεικνύεται ότι και $p \nmid z$, δηλαδή $p \nmid yz$.

Επομένως $by^2 + cz^2 \equiv 0 \pmod{p}$. Αφού $(p, z) = 1$, έπεται ότι υπάρχει u τέτοιο ώστε $uz \equiv 1 \pmod{p}$. Πολλαπλασιάζουμε με u^2b και βρίσκουμε

$$u^2b^2y^2 + bcu^2z^2 \equiv 0 \pmod{p} \Longrightarrow (uby)^2 \equiv -bc \pmod{p} \Longrightarrow -bcRp.$$

Είναι γνωστό ότι αν $(m, n) = 1$ τότε aRm και aRn συνεπάγεται ότι $aRmn$. Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. Επειδή τώρα $-bcRp$ ισχύει για κάθε πρώτο διαιρέτη p του a και a ελεύθερος τετραγώνου, έχουμε $-bcRa$. Επομένως έχουμε $-bcRa$. Όμοια βρίσκουμε ότι $-abRa$ και $-acRa$. Το πόρισμα είναι άμεση συνέπεια του θεωρήματος. □

ΤΕΛΟΣ

Βιβλιογραφία

[1] Lars V. Ahlfors, Complex Analysis, McGraw-Hill 1979.

[2] Γιάννη Α. Αντωνιάδη, Στοιχειώδης Θεωρία Αριθμών, Σημειώσεις, Ηράκλειο 1985.

[3] Γιάννη Α. Αντωνιάδη, Ειδικά Θέματα Θεωρίας Αριθμών, Σημειώσεις, Θεσσαλονίκη 1983.

[4] I. G. Bašmakova, Diophant und diophantische Gleichungen, VEB Deutscher Verlag der Wissenschaften, Berlin 1974.

Μικρό αλλά πολύ καλό, βιβλίο. Αποτελεί ιστορική εισαγωγή σε έναν από τους πιο μοντέρνους σήμερα κλάδους της Θεωρίας των Αριθμών, αυτόν της αριθμητικής των αλγεβρικών καμπυλών.

[5] C. F. Gauss, Untersuchungen über höhere Arithmetik, μετάφραση από τα Λατινικά, Chelsea, New York 1981.

Με το βιβλίο αυτό του Gauss άνοιξε μία καινούργια εποχή για την Θεωρία Αριθμών. Για πρώτη φορά η Θεωρία των Τετραγωγικών Μορφών μελετάται συστηματικά. Όχι μόνο συγκεντρώθηκαν αποτελέσματα προηγουμένων ερευνητών αλλά επεκτάθηκαν και συστηματοποιήθηκαν αρκετά. Το βιβλίο έχει μεταφραστεί στα αγγλικά, γαλλικά και γερμανικά.

Ανάλογους σταθμούς έχουμε έναν, σχεδόν, αιώνα αργότερα με το Zahlbericht του D. Hilbert και, κατά την δεκαετία του 20, με το Klassenkörpenbericht του H. Hasse.

[6] Εκδότης Max Miller, Pierre de Fermat, Bemerkungen zur Diophant, Akad. Verlag, Leipzig 1932.

Περιέχει τις σημειώσεις που έγραφε ο Fermat στο περιθώριο του βιβλίου των αριθμητικών του Διοφάντου που είχε στη διάθεσή του. Οι σημείώσεις αυτές δημοσιεύτηκαν για πρώτη φορά από το γυιό του Fermat, Samuel στα 1670. Εδώ πρόκειται για μετάφραση στα Γερμανικά από την λατινο-γαλλική έκδοση του 1891. Ας σημειωθεί ότι υπάρχει και ελληνο-λατινική έκδοση του 1893, του Paul Tannery.

[7] James R. Newman, The World of Mathematics (τόμοι 4), Simon and Schuster, New York 1956.

[8] H. Reichardt, Einige im Kleinen überall Lösbare, in Grössen unlösbare diophantische Gleichungen. J. Reine und Angew. Mathematik, **184** (1942) 12-18.

[9] W. Scharlau, H. Opolka, From Fermat to Minkowski, Lectures on the Theory of Numbers and Its Historical Development, Springer-Verlag, New York 1985.

Το καλογραμμένο αυτό βιβλίο, όπως φαίνεται και από τον τίτλο του, καλύπτει και ολόκληρο σχεδόν τον 19ο αιώνα.

[10] Ε. Σταμάτη, Ευκλείδου Γεωμετρία, Θεωρία Αριθμών, Τόμος ΙΙ, Οργανισμός Εκδόσεως Σχολικών Βιβλίων, Αθήνα 1953.

Περιέχει αρχαίο κείμενο και νεοελληνική μετάφραση, από έναν ακούραστο εργάτη και λάτρη των αρχαιο-ελληνικών μαθηματικών

[11] A. Weil, Number Theory, An Approach through History, From Hammurapi to Legendre, Birkhaüser, Boston 1984.

Πρόκειται για ένα καταπληκτικό βιβλίο. Πραγματικό θησαύρισμα ιστορικών στοιχείων και μαθηματικών εννοιών. Έχει τη σφραγίδα ενός από τους πιο σημαντικούς μαθηματικούς του αιώνα μας.

[12] G. Wertheim, Die Arithmetik und die Schrift über Polygonalzahlen des Diophantus von Alexandria, Teubner, Leipzig 1890.