Θεμελιωδης Θεωρια Αριθμων

Ν.Γ. Τζανάκης

Τμῆμα Μαθηματικῶν & Ἐφαρμοσμένων Μαθηματικῶν
Πανεπιστήμιο Κρήτης

29-4-2019

Περιεχόμενα

Κεφάλαιο 1

Διαιρετότητα

Τὰ λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους ἀριθμούς

Δουλεύομε στὸ σύνολο $\mathbb{Z}$ τῶν ἀκεραίων ἀριθμῶν. Οἱ θετικοὶ ἀκέραιοι χαρακτηρίζονται καὶ ὡς *φυσικοὶ ἀριθμοὶ* καὶ τὸ σύνολό τους συμβολίζεται $\mathbb{N}$. Τὸ σύνολο τῶν μὴ ἀρνητικῶν ἀκεραίων, δηλαδή, τὸ $\mathbb{N} \cup \{0\}$ συμβολίζεται $\mathbb{N}_0$. Τὸ σύνολο τῶν ρητῶν ἀριθμῶν συμβολίζεται μὲ $\mathbb{Q}$. Ἐξ ὁρισμοῦ, ἕνας ρητὸς ἀριθμὸς εἶναι πηλίκο a/b δύο ἀκεραίων ἀριθμῶν a, b μὲ $b \neq 0$.

Τὸ *ἀκέραιο μέρος* ἑνὸς πραγματικοῦ ἀριθμοῦ α συμβολίζεται $[\alpha]$. Ἰσχύει $[\alpha] \leq \alpha < [\alpha] + 1$.

1.1 Βασικὲς προτάσεις

Τὸ ἄθροισμα, ἡ διαφορὰ καὶ τὸ γινόμενο δύο ἀκεραίων εἶναι πάντα ἀκέραιος. Τὸ πηλίκο τους, ὅμως, δὲν εἶναι πάντα ἀκέραιος. Ἂν γιὰ τοὺς ἀκεραίους a, b, μὲ $b \neq 0$ συμβεῖ νὰ εἶναι τὸ πηλίκο τους a/b ἀκέραιος, δηλαδή, ἂν ὑπάρχει $c \in \mathbb{Z}$, τέτοιος ὥστε $a = bc$, τὸ γεγονὸς αὐτὸ συμβολίζεται $b|a$ καὶ ἐκφράζεται μὲ τὶς ἑξῆς *ἰσοδύναμες διατυπώσεις*.

- Ὁ b διαιρεῖ τὸν a.
- Ὁ b εἶναι διαιρέτης τοῦ a.
- Ὁ a διαιρεῖται ἀπὸ τὸν b (ἢ διαιρεῖται διὰ b).
- Ὁ a εἶναι διαιρετός ἀπὸ τὸν b (ἢ διαιρετὸς διὰ b).
- Ὁ a εἶναι πολλαπλάσιο τοῦ b.

Προσοχή! Νὰ μὴ γίνεται σύγχυση μεταξὺ τῶν συμβολισμῶν $b|a$ καὶ b/a. Ὁ πρῶτος δηλώνει μία ἰδιότητα (b διαιρεῖ a), ἐνῶ ὁ δεύτερος ἕνα ρητὸ ἀριθμό (τὸ πηλίκο b/a).

Πρόταση 1.1.1 *Ἰσχύουν τὰ ἑξῆς:*

α΄. $1|a$ *γιὰ κάθε* a.

β΄. $b|0$ *γιὰ κάθε* $b \neq 0$.

γ΄. Ἂν $b, c \neq 0$ *καὶ* $c|b$ *καὶ* $b|a$, *τότε* $c|a$.

δ΄. Ἂν $c|a$ *καὶ* $c|b$, *τότε* $c|(a'a + b'b)$, *γιὰ ὁποιουσδήποτε ἀκεραίους* a', b'.

ε΄. Ἂν $b|a$ *(*$b \neq 0$*) καὶ* $a \neq 0$, *τότε* $|b| \leq |a|$. *Αὐτὸ συνεπάγεται, εἰδικώτερα, ὅτι τὸ πλῆθος τῶν διαιρετῶν τοῦ* a *εἶναι πεπερασμένο.*

στ΄. Ἂν οἱ a, b *εἶναι μὴ μηδενικοί,* $a|b$ *καὶ* $b|a$ *(δηλαδή, οἱ ἀκέραιοι* ἀλληλοδιαιροῦνται*), τότε* $b = \pm a$.

Ἀπόδειξη α΄ καὶ β΄. Προφανεῖς ἰσχυρισμοὶ λόγῳ τῶν σχέσεων $a = 1 \cdot a$ καὶ $0 = b \cdot 0$.
γ΄. Ἐξ ὑποθέσεως, ὑπάρχουν ἀκέραιοι a_1, b_1, τέτοιοι ὥστε $b = b_1 c$ καὶ $a = a_1 b$. Ἄρα, $a = a_1(b_1 c) = (a_1 b_1)c$, ποὺ σημαίνει ὅτι $c|a$.
δ΄. Ἐξ ὑποθέσεως, ὑπάρχουν ἀκέραιοι a_1, b_1, τέτοιοι ὥστε $b = b_1 c$ καὶ $a = a_1 c$. Ἄρα, $a'a + b'b = a'(a_1 c) + b'(b_1 c) = (a'a_1 + b'b_1)c$, ποὺ σημαίνει ὅτι $c|(a'a + b'b)$.
ε΄. Εἶναι $a = bc$ γιὰ κατάλληλο $c \in \mathbb{Z}$, ἄρα $|a| = |b||c|$. Ἂν εἶναι $a \neq 0$, τότε $|c| \neq 0$, ἄρα $|c| \geq 1$, ὁπότε $|a| = |b||c| \geq |b|$.
στ΄. Ἀπὸ τὸ ε΄, συμπεραίνομε ὅτι $|b| \leq |a|$ καὶ $|a| \leq |b|$, ἄρα $|a| = |b|$ ἤ, ἰσοδύναμα, $b = \pm a$. **ὅ.ἔ.δ.**

Θεώρημα 1.1.2 –Εὐκλείδεια διαίρεση. *Γιὰ κάθε ζεῦγος ἀκεραίων* (a, b) *μὲ* $b > 0$ *ὑπάρχει ἕνα μοναδικὸ ζεῦγος ἀκεραίων* (q, r), *τέτοιο ὥστε*

$$a = bq + r \quad \text{καὶ} \quad 0 \leq r < b\,.$$

Στὴ σχέση αὐτὴ ὁ a *χαρακτηρίζεται διαιρετέος καὶ ὁ* b *διαιρέτης. Ὁ* q *ὀνομάζεται* (ἀκέραιο) πηλίκο τῆς διαίρεσης τοῦ a διὰ b *καὶ ὁ* r *ὑπόλοιπο τῆς διαίρεσης.*

Ἀπόδειξη Πρῶτα θὰ δείξομε ὅτι ὑπάρχει ἕνα τέτοιο ζεῦγος (q, r) καὶ μετὰ ὅτι δὲν ὑπάρχει δεύτερο.

Ἔστω $q = [\frac{a}{b}]$. Τότε, ἀπὸ τὴν ἰδιότητα τοῦ ἀκεραίου μέρους, $q \leq \frac{a}{b} < q + 1$, ποὺ συνεπάγεται ὅτι $bq \leq a < bq + b$. Αὐτό, ὅμως, προφανῶς σημαίνει ὅτι $a = bq + r$ μὲ $r \geq 0$ καὶ $r < b$.

Ἂν ὑποθέσομε τώρα ὅτι καὶ τὸ ζεῦγος (q_1, r_1) ἔχει ἀνάλογες ἰδιότητες μὲ τὸ (q, r), τότε $bq_1 + r_1 = a = bq + r$, ἄρα $b(q_1 - q) = r - r_1$. Ἂν ἦταν $r_1 \neq r$, τότε ἡ τελευταία ἰσότητα θὰ συνεπαγόταν ὅτι ὁ b θὰ διαιροῦσε τὸν θετικὸ ἀκέραιο $|r - r_1|$, ἄρα θὰ ἦταν $b \leq |r - r_1|$, σύμφωνα μὲ τὸ ε΄ τῆς πρότασης 1.1.1. Ἀπὸ τὴν ἄλλη μεριά, ὁ $|r - r_1|$ ἐκφράζει τὴν ἀπόσταση μεταξὺ τῶν r καὶ r_1 πάνω στὸν ἄξονα τῶν παραγματικῶν ἀριθμῶν, ἡ ὁποία εἶναι *γνησίως μικρότερη* τοῦ b, ἀφοῦ, ἐξ ὑποθέσεως, $0 \leq r, r_1 < b$. Αὐτὴ ἡ ἀντίφαση μᾶς ἀναγκάζει νὰ συμπεράνομε ὅτι $r_1 = r$, ὁπότε καὶ $q_1 = q$. **ὅ.ἔ.δ.**

Στὴν εἰδικὴ περίπτωση, ποὺ $b = 2$, οἱ πιθανὲς τιμὲς τοῦ r εἶναι 0 ἢ 1. Στὴν πρώτη περίπτωση, $a = 2q$ καὶ ὁ a χαρακτηρίζεται *ἄρτιος*, ἐνῶ στὴ δεύτερη, $a = 2q + 1$ καὶ ὁ a χαρακτηρίζεται *περιττός* .

Προσοχή! Μὴ γίνεται σύγχυση μεταξὺ τοῦ *πηλίκου δύο ἀκεραίων ἀριθμῶν* καὶ τοῦ *ἀκεραίου πηλίκου* τους. Γιὰ παράδειγμα, τὸ πηλίκο τοῦ 21 διὰ 4 εἶναι ὁ ρητὸς ἀριθμὸς 21/4=5.25, ἐνῶ τὸ (ἀκέραιο) πηλίκο τῆς διαίρεσης 21 διὰ 4 εἶναι 5 (καὶ τὸ ὑπόλοιπο 1). Μόνο στην περίπτωση ποὺ τὸ ὑπόλοιπο εἶναι 0 οἱ δύο ἀριθμοὶ ταυτίζονται. Ἔτσι, τὸ πηλίκο τοῦ 12 διὰ 4 εἶναι 12/4=3, ἀλλὰ καὶ τὸ (ἀκέραιο) πηλίκο τῆς διαίρεσης τοῦ 12 διὰ 4 εἶναι 3.

1.2 Μέγιστος κοινὸς διαιρέτης

Σταθεροποιοῦμε δύο μὴ μηδενικοὺς ἀκεραίους a, b. *Κοινὸς διαιρέτης* τῶν a, b εἶναι κάθε ἀκέραιος, ποὺ διαιρεῖ καὶ τὸν a καὶ τὸν b. Ἀπὸ τὴν Πρόταση 1.1.1 βλέπομε ὅτι τὸ σύνολο τῶν κοινῶν διαιρετῶν τῶν a, b εἶναι μὴ κενό, ἐνῶ κάθε κοινὸς διαιρέτης τῶν a, b εἶναι, μικρότερος ἤ, τὸ πολύ, ἴσος μὲ τὸ $\min(|a|, |b|)$. Συνεπῶς, τὸ σύνολο τῶν κοινῶν διαιρετῶν τῶν a, b εἶναι πεπερασμένο, ὁπότε ἔχει ἕνα μέγιστο στοιχεῖο, τὸ ὁποῖο καλεῖται *μέγιστος κοινὸς διαιρέτης τῶν* a, b καὶ συμβολίζεται (a, b), ἤ, ἂν ὑπάρχει φόβος συγχύσεως, ΜΚΔ(a, b).

Ὁρίζομε τώρα τὸ σύνολο

$$\Delta = \{ax + by \mid x, y \in \mathbb{Z}\} .$$

Εἶναι τετριμμένο νὰ διαπιστώσει κανεὶς τὶς ἑξῆς βασικὲς ἰδιότητες τοῦ Δ:

1. Τὸ ἄθροισμα δύο ἀριθμῶν, ποὺ ἀνήκουν στὸ Δ, ἀνήκει, ἐπίσης, στὸ Δ.

2. Τὸ γινόμενο ἑνὸς ἀριθμοῦ τοῦ Δ μὲ ἕναν *ὁποιονδήποτε ἀκέραιο*, πάλι ἀνήκει στὸ Δ[1]

Παρατηροῦμε τώρα τὰ ἑξῆς:

- Εἶναι $|a|, |b| \in \Delta$.

Πράγματι, διότι $|a| = a \cdot 1 + b \cdot 0$ ἂν $a > 0$ καὶ $|a| = a \cdot (-1) + b \cdot 0$ ἂν $a < 0$· ἀνάλογα καὶ γιὰ τὸ b.

Είδαμε ὅτι τὸ Δ περιέχει *θετικοὺς* ἀκεραίους· ἔστω, λοιπόν, d ὁ ἐλάχιστος θετικὸς ἀκέραιος, ποὺ περιέχεται στὸ Δ.

- Τὸ Δ ταυτίζεται μὲ τὸ σύνολο τῶν πολλαπλασίων τοῦ d· συμβολικά, $\Delta = d\mathbb{Z}$.

Πράγματι, ἀφοῦ $d \in \Delta$, ἡ ἰδιότητα 2, παραπάνω, μᾶς λέει ὅτι $dn \in \Delta$ γιὰ κάθε $n \in \mathbb{Z}$. Ἄρα, $\Delta \supseteq d\mathbb{Z}$. Ἀντιστρόφως, τώρα, ἔστω $m \in \Delta$ καὶ ἂς ἐκτελέσομε τὴν εὐκλείδεια διαίρεση τοῦ m διὰ d: Βάσει τοῦ θεωρήματος 1.1.2, ἂς γράψομε $m = dq + r$ μὲ

[1] Οἱ *ἐπαΐοντες* θὰ ἀναγνωρίσουν σὲ αὐτὲς τὶς δύο ἰδιότητες τοῦ Δ ἕνα *ἰδεῶδες* τοῦ $\mathbb{Z}$.

$0 \leq r < d$. Τώρα, ἀπὸ τὴν ἰδιότητα 2 τοῦ Δ καὶ τὸ γεγονὸς ὅτι $d \in \Delta$ συμπεραίνομε ὅτι $d(-q) \in \Delta$. Ὅμως, ἐξ ὑποθέσεως, $m \in \Delta$, ἄρα, ἀπὸ τὴν ἰδιότητα 1 τοῦ Δ, ἕπεται ὅτι $m - qd \in \Delta$, δηλαδή, $r \in \Delta$. Ὁπότε, ἂν ἦταν $r > 0$, θὰ εἴχαμε βρεῖ ἕνα θετικὸ στοιχεῖο τοῦ Δ μικρότερο τοῦ d, κάτι ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν ἐκλογὴ τοῦ d. Συνεπῶς, $r = 0$, ὁπότε $m = dq \in d\mathbb{Z}$ καὶ καταλήγομε στὸ συμπέρασμα ὅτι $\Delta \subseteq d\mathbb{Z}$.

• Ὁ d εἶναι κοινὸς διαιρέτης τῶν a, b. Αὐτὸ συνεπάγεται, εἰδικώτερα, ὅτι κάθε διαιρέτης τοῦ d εἶναι κοινὸς διαιρέτης τῶν a, b, ἀφοῦ ἡ σχέση τῆς διαιρετότητας εἶναι μεταβατικὴ (γ′ τῆς πρότασης 1.1.1).
Πράγματι, ὅπως εἴδαμε παραπάνω, $a \in \Delta$. Ἀλλὰ $\Delta = d\mathbb{Z}$, καθὼς δείξαμε μόλις πρίν, ἄρα $a \in d\mathbb{Z}$, δηλαδή, ὁ a εἶναι πολλαπλάσιο τοῦ d· ἰσοδύναμα, ὁ d εἶναι διαιρέτης τοῦ a. Ἀνάλογα καὶ γιὰ τὸν b.

• Κάθε κοινὸς διαιρέτης c τῶν a, b διαιρεῖ τὸν d.
Πράγματι, ἐξ ὁρισμοῦ τοῦ Δ καὶ ἐπειδὴ $d \in \Delta$, ὑπάρχουν $x_0, y_0 \in \mathbb{Z}$, τέτοιοι ὥστε $d = ax_0 + by_0$. Γράφοντας τώρα $a = a_1c$, $b = b_1c$, βλέπομε ὅτι $d = c(a_1x_0 + b_1y_0)$, ποὺ σημαίνει ὅτι $c|d$.

Τὸ συμπέρασμα αὐτὸ συνεπάγεται, εἰδικώτερα, ὅτι $|c| \leq d$ (ε′ τῆς πρότασης 1.1.1), ἄρα βάσει τῶν προηγουμένων, ὁ d εἶναι καὶ κοινὸς διαιρέτης τῶν a, b καὶ ὁ μεγαλύτερος ἀπὸ ὅλους τοὺς ἄλλους κοινοὺς διαιρέτες τῶν a, b.

Συνοψίζοντας τὰ συμπεράσματά μας, καταλήγομε στὸ ἑξῆς βασικὸ

Θεώρημα 1.2.1 *Ἔστω d ὁ μέγιστος κοινὸς διαιρέτης δύο ἀκεραίων a, b. Τότε:*

α′. Τὸ σύνολο τῶν κοινῶν διαιρετῶν τῶν a, b ταυτίζεται μὲ τὸ σύνολο τῶν διαιρετῶν τοῦ d.

β′. Ὑπάρχουν ἀκέραιοι x_0, y_0, τέτοιοι ὥστε $d = ax_0 + by_0$.

Ὁ μέγιστος κοινὸς διαιρέτης ἑνὸς πεπερασμένου πλήθους ἀκεραίων $a_1, a_2, \ldots, a_n$ συμβολίζεται $(a_1, a_2, \ldots, a_n)$ καὶ ὁρίζεται ὡς ὁ μέγιστος *θετικὸς* ἀκέραιος, ὁ ὁποῖος διαιρεῖ καθέναν ἀπὸ τοὺς $a_1, \ldots, a_n$. Ὁ ὑπολογισμός του μπορεῖ νὰ γίνει ἀναδρομικά, ὡς ἑξῆς:

$$\begin{aligned}
(a_1, a_2, a_3) &= ((a_1, a_2), a_3) \\
(a_1, a_2, a_3, a_4) &= ((a_1, a_2, a_3), a_4) \\
&\vdots \\
(a_1, \ldots, a_{n-1}, a_n) &= ((a_1, \ldots, a_{n-1}), a_n)
\end{aligned}$$

Χρειάζεται, βέβαια, ἀπόδειξη ὅτι αὐτὴ ἡ ἀναδρομικὴ διαδικασία ὁδηγεῖ στὴν εὕρεση τοῦ μεγίστου κοινοῦ διαιρέτη τῶν $a_1, \ldots, a_n$· βλ. ἄσκηση 16. Ἐπίσης, ἡ ἄσκηση 17 λέει ὅτι ὁ μέγιστος κοινὸς διαιρέτης πολλῶν ἀριθμῶν ἔχει ἰδιότητες ἀνάλογες μὲ αὐτὲς τοῦ μεγίστου κοινοῦ διαιρέτη, ποὺ ἀναφέρονται στὸ θεώρημα 1.2.1.

Ὅταν $(a_1, a_2, \ldots, a_n) = 1$, τότε λέμε ὅτι οἱ $a_1, a_2, \ldots, a_n$ εἶναι *πρῶτοι μεταξύ τους* . Ἡ ἰδιότητα αὐτὴ τῶν $a_1, a_2, \ldots, a_n$ εἶναι ἀσθενέστερη ἀπὸ τὴν ἰδιότητα νὰ εἶναι *ἀνὰ ζεύγη πρῶτοι* , ἐκτός, βέβαια, ἂν $n = 2$, ποὺ οἱ ἰδιότητες εἶναι ἰσοδύναμες. Γιὰ παράδειγμα, οἱ ἀριθμοὶ 10,12,15 εἶναι πρῶτοι μεταξύ τους, ἀφοῦ ὁ μόνος κοινὸς (καὶ γιὰ τοὺς τρεῖς) διαιρέτης τους εἶναι ὁ 1. Ὅμως, ἀνὰ ζεύγη, δὲν εἶναι πρῶτοι, ἀφοῦ $(10, 12) = 2$, $(10, 15) = 5$ καὶ $(12, 15) = 3$. Φυσικά, εἶναι φανερὸ ὅτι, ἂν οἱ $a_1, a_2, \ldots, a_n$ εἶναι πρῶτοὶ ἀνὰ ζεύγη, εἶναι καὶ πρῶτοι μεταξύ τους.

Θεώρημα 1.2.2 –Ἰδιότητες τοῦ ΜΚΔ

α′. Ἂν $b|a$ τότε $(a, b) = |b|$.

β′. Ἂν $a = bq + c$ τότε τὸ σύνολο τῶν κοινῶν διαιρετῶν τῶν a, b συμπίπτει μὲ τὸ σύνολο τῶν κοινῶν διαιρετῶν τῶν b, c· εἰδικώτερα, $(a, b) = (b, c)$.

γ′. Γιὰ ὁποιονδήποτε ἀκέραιο c, $(ca, cb) = |c|(a, b)$

δ′. Ἂν ὁ c εἶναι κοινὸς διαιρέτης τῶν a, b, τότε $\left(\dfrac{a}{c}, \dfrac{b}{c}\right) = \dfrac{(a, b)}{|c|}$. Αὐτό, εἰδικώτερα, συνεπάγεται –γιὰ $c = (a, b)$– ὅτι οἱ $a/(a, b)$ καὶ $b/(a, b)$ εἶναι πρῶτοι μεταξύ τους.

ε′. Ἂν $(a, b) = 1$ καὶ c ὁποιοσδήποτε ἀκέραιος, τότε $(ac, b) = (c, b)$.

στ′. Ἂν $(a, b) = 1$ καὶ $b|ac$, τότε $b|c$.

ζ′. Ἂν καθένας ἀπὸ τοὺς $a_1, \ldots, a_n$ εἶναι πρῶτος πρὸς καθέναν ἀπὸ τοὺς $b_1, \ldots, b_m$, τότε $(a_1 \cdots a_n, b_1 \cdots b_m) = 1$.

Ἀπόδειξη α′. Ὁ $|b|$ εἶναι, προφανῶς, ὁ μέγιστος διαιρέτης τοῦ b καί, ἐξ ὑποθέσεως, διαιρεῖ τὸν a, ἄρα εἶναι μέγιστος κοινὸς διαιρέτης τῶν a, b.
β′. Κάθε κοινὸς διαιρέτης τῶν a, b διαιρεῖ τοὺς a καὶ bq, ἄρα διαιρεῖ καὶ τὸν $c = (-1)a + qb$ (βλ. θεώρημα 1.1.1), ὁπότε εἶναι κοινὸς διαιρέτης τῶν b, c. Ἀντίστροφα, κάθε κοινὸς διαιρέτης τῶν b, c διαιρεῖ τὸν $qb + c = a$, ἄρα εἶναι κοινὸς διαιρέτης τῶν a, b.
γ′. Ἔστω $(a, b) = d$. Ἐπειδὴ ὁ $|c|$ διαιρεῖ τὸν c καὶ ὁ d διαιρεῖ τὸν a, ὁ $|c|d$ διαιρεῖ τὸν ca καί, ὁμοίως, διαιρεῖ καὶ τὸν cb. Ὁ $|c|d$ εἶναι, λοιπόν, κοινὸς διαιρέτης τῶν ca, cb, ἄρα (α′ τοῦ θεωρήματος 1.2.1) διαιρεῖ τὸν (ca, cb). Θὰ δείξομε ὅτι, καὶ ἀντίστροφα, ὁ (ca, cb) διαιρεῖ τὸν $|c|d$. Πράγματι, τὸ Θεώρημα 1.2.1 (β′) μᾶς ἐξασφαλίζει τὴν ὕπαρξη ἀκεραίων x_0, y_0, τέτοιων ὥστε $ax_0 + by_0 = d$, ὁπότε $(ca)x_0 + (cb)y_0 = cd$. Τὸ ἀριστερὸ μέλος αὐτῆς τῆς σχέσης διαιρεῖται, προφανῶς, ἀπὸ τὸν (ca, cb), ἄρα ὁ (ca, cb) διαιρεῖ τὸν cd, ὁπότε καὶ τὸν $|c|d$. Τελικά, οἱ θετικοὶ ἀκέραιοι (ca, cb) καὶ $|c|d = |c|(a, b)$ ἀλληλοδιαιροῦνται, ὁπότε εἶναι ἴσοι (βλ. στ′ τοῦ θεωρήματος 1.1.1).
δ′. Ἐφαρμόζοντας τὸ γ′ μὲ $\frac{a}{c}$ στὴ θέση τοῦ a καὶ $\frac{b}{c}$ στὴ θέση τοῦ b, παίρνομε $|c|(\frac{a}{c}, \frac{b}{c}) = (a, b)$, δηλαδή, τὴν ἀποδεικτέα σχέση.[2]
ε′. Ἔχομε $(c, b)|(ac, b)$. Πράγματι, ὁ (c, b) διαιρεῖ τοὺς c, b ἄρα εἶναι κοινὸς διαιρέτης καὶ τῶν ac, b, ὁπότε εἶναι διαιρέτης τοῦ (ac, b), ἀπὸ τὸ Θεώρημα 1.2.1 (α′». Ἀντίστροφα, θὰ δείξομε ὅτι $(ac, b)|(c, b)$. Ἀπὸ τὸ Θεώρημα 1.2.1 (β′) ξέρομε ὅτι ὑπάρχουν ἀκέραιοι x_0, y_0, τέτοιοι ὥστε $ax_0 + by_0 = 1$, ἄρα $(ac)x_0 + b(cy_0) = c$. Βλέπομε ὅτι τὸ ἀριστερὸ μέλος αὐτῆς τῆς σχέσης διαιρεῖται ἀπὸ τὸν (ac, b), ἄρα ὁ (ac, b) διαιρεῖ καὶ τὸν c, ὁπότε εἶναι κοινὸς διαιρέτης τῶν b, c, ἄρα καὶ διαιρέτης

[2] Δεῖτε, ὅμως τὴν ἄσκηση 18.

τοῦ (b, c), λόγῳ τοῦ τοῦ θεωρήματος 1.2.1 (α′). Οἱ θετικοὶ ἀκέραιοι (c, b) καὶ (ac, b) ἀλληλοδιαιροῦνται λοιπόν, ἄρα (στ′ τοῦ θεωρήματος 1.1.1) εἶναι ἴσοι.
στ′. Ἀπὸ τὸ θεώρημα 1.2.1 (β′) ξέρομε ὅτι ὑπάρχουν ἀκέραιοι x_0, y_0, τέτοιοι ὥστε $ax_0 + by_0 = 1$, ἄρα $(ac)x_0 + b(cy_0) = c$. Ὁ b διαιρεῖ τὸ ἀριστερὸ μέλος, ἄρα διαιρεῖ καὶ τὸν c.
ζ′. Θὰ δείξομε πρῶτα ὅτι $(a_1a_2 \cdots a_n, b_1) = 1$, ἐφαρμόζοντας πολλὲς φορὲς διαδοχικὰ τὸ ε′ καί, φυσικά, τὴν ὑπόθεση ὅτι ὁ b_1 εἶναι πρῶτος πρὸς καθέναν ἀπὸ τοὺς $a_1, a_2, \ldots, a_n$. Λοιπόν, ἔχομε διαδοχικά:

$$\begin{aligned}
(a_1, b_1) = 1 &\quad\Rightarrow\quad (a_1a_2, b_1) = (a_2, b_1) = 1\\
(a_1a_2, b_1) = 1 &\quad\Rightarrow\quad (a_1a_2a_3, b_1) = (a_3, b_1) = 1\\
\vdots\quad &\qquad\quad \vdots\\
(a_1a_2 \cdots a_{n-1}, b_1) = 1 &\quad\Rightarrow\quad (a_1a_2 \cdots a_{n-1}a_n, b_1) = (a_n, b_1) = 1
\end{aligned}$$

Θέτομε τώρα $A = a_1a_2 \cdots a_n$. Μόλις δείξαμε ὅτι $(A, b_1) = 1$. Ἐντελῶς ἀνάλογα ἰσχύει ὅτι $(A, b_k) = 1$ γιὰ ὅλα τὰ $k = 1, \ldots, m$. Τώρα, μὲ διαδοχικὴ ἐφαρμογὴ τοῦ ε′, ἔχομε τὶς διαδοχικὲς συνεπαγωγές: $(b_1, A) = 1 \Rightarrow (b_1b_2, A) = (b_2, A) = 1$, $(b_1b_2, A) = 1 \Rightarrow (b_1b_2b_3, A) = (b_3, A) = 1$ κλπ, μέχρις ὅτου καταλήξομε στὴν $(b_1b_2 \cdots b_m, A) = 1$, δηλαδή, στὴν ἀποδεικτέα. **ὅ.ἔ.δ.**

Ὁ πρακτικὸς ὑπολογισμὸς τοῦ μεγίστου κοινοῦ διαιρέτη δύο ἀκεραίων ἐπιτυγχάνεται πάρα πολὺ ἀποτελεσματικὰ μὲ τὸν *εὐκλείδειο ἀλγόριθμο* , ἕναν ἀπὸ τοὺς πιὸ σημαντικοὺς ἀλγορίθμους τῶν Μαθηματικῶν.

Θεώρημα 1.2.3 *Ἔστω $a \geq b > 0$. Θέτομε $r_0 = a$, $r_1 = b$, $s_{-1} = s_0 = 1$. Γιὰ $i = 1, 2, \ldots$ ὁρίζομε ἀναδρομικὰ q_{i+1}, r_{i+1} νὰ εἶναι, ἀντιστοίχως, τὸ πηλίκο καὶ τὸ ὑπόλοιπο τῆς εὐκλείδειας διαίρεσης τοῦ r_{i-1} διὰ τοῦ r_i (βλ. θεώρημα 1.1.2). Τότε:*

α′. $b = r_1 > r_2 > r_3 > \cdots$ καὶ γιὰ κάποιο $i = n \geq 2$ εἶναι $r_{n+1} = 0$. Γι' αὐτὸ τὸ συγκεκριμένο n ἰσχύει $n < 2\frac{\log b}{\log 2} + 2$ καὶ $r_n = (a, b)$.

β′. Γιὰ $i = 1, \ldots, n$ ὁρίζομε ἀναδρομικὰ $s_i = s_{i-2} - s_{i-1}q_{n-i+2}$. Τότε, $(a, b) = as_{n-1} + bs_n$.

Ἀπόδειξη α′. Ἔχομε, ἐξ ὁρισμοῦ, $r_{i-1} = r_iq_{i+1} + r_{i+1}$, ὅπου $0 \leq r_{i+1} < r_i$ (βλ. θεώρημα 1.1.2). Συνεπῶς, γιὰ τοὺς *μὴ ἀρνητικοὺς ἀκεραίους* r_i ἔχομε $r_0 > r_1 > r_2 > \cdots \geq 0$, ἄρα κάποιο r_i, ἀναγκαστικά, θὰ εἶναι μηδέν. Ἔστω, λοιπόν, $r_{n+1} = 0$

$(n \geq 1)$. Τότε ἔχομε τὴν ἑξῆς κατάσταση:

$$\begin{aligned}
a = r_0 &= r_1q_2 + r_2 = bq_2 + r_2\,, \quad 0 < r_2 < r_1 = b\\
b = r_1 &= r_2q_3 + r_3\,, \quad 0 < r_3 < r_2\\
r_2 &= r_3q_4 + r_4\,, \quad 0 < r_4 < r_3\\
\vdots &\quad \vdots\\
r_{i-1} &= r_iq_{i+1} + r_{i+1}\,, \quad 0 < r_{i+1} < r_i\\
\vdots &\quad \vdots\\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}\,, \quad 0 < r_{n-1} < r_{n-2}\\
r_{n-2} &= r_{n-1}q_n + r_n\,, \quad 0 < r_n < r_{n-1}\\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}$$

Ἡ τελευταία ἀπὸ τὶς παραπάνω ἰσότητες μᾶς λέει ὅτι $r_n = (r_{n-1}, r_n)$ (βλ. αʹ τοῦ θεωρήματος 1.2.2). Τώρα ἐφαρμόζομε τὸ βʹ τοῦ θεωρήματος 1.2.2 διαδοχικά, ἀρχίζοντας ἀπὸ τὴν προτελευταία σχέση καὶ ἀνεβαίνοντας πρὸς τὰ πάνω:
$(r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \cdots = (r_4, r_3) = (r_3, r_2) = (r_2, r_1) = (r_1, r_0) = (b, a)$.
Ἐδῶ, τὸ ἀριστερώτερο = ὀφείλεται στὴν προτελευταία σχέση, τὸ ἑπόμενο = στὴν δεύτερη ἀπὸ τὸ τέλος σχέση κλπ. Τὸ ἄνω φράγμα γιὰ τὸν n θὰ τὸ ἀποδείξομε στὸ τέλος.
βʹ. Γιὰ $i = 0, 1, \ldots, n$ ἰσχύει ἡ σχέση $r_n = s_ir_{n-i+1} + s_{i-1}r_{n-i}$ $(*)$, τὴν ὁποία θὰ ἀποδείξομε μὲ ἐπαγωγὴ στὸ i: Γιὰ $i = 0$ τὸ δεξιὸ μέλος γίνεται $s_0r_{n+1} + s_{-1}r_n = 1 \cdot 0 + 1 \cdot r_n = r_n$. Ἄν, τώρα, ἰσχύει ἡ σχέση γιὰ κάποιο $0 \leq i < n$, τότε πρέπει νὰ δείξομε ὅτι ἰσχύει καὶ γιὰ τὸ $i + 1$, δηλαδή, $r_n = s_{i+1}r_{n-i} + s_ir_{n-i-1}$. Αὐτὸ φαίνεται μὲ ἁπλούστατες πράξεις, ἂν στὸ δεξιὸ μέλος κάνομε τὶς ἀντικαταστάσεις $s_{i+1} = s_{i-1} - s_iq_{n-i+1}$ (βλ. πῶς ὁρίσθηκαν οἱ $s_1, s_2, \ldots$) καὶ $r_{n-i-1} = r_{n-i}q_{n-i+1} + r_{n-i+1}$ (στὴ λίστα τῶν εὐκλειδείων διαιρέσεων, παραπάνω, θέτομε στὴ θέση τοῦ i τὸ $n - i$).
Ἀπὸ τὴ σχέση (*), γιὰ $i = n$ παίρνομε $r_n = s_nr_1 + s_{n-1}r_0$, δηλαδή, $(a, b) = s_nb + s_{n-1}a$.

Τέλος, ἀποδεικνύμε τὸ ἄνω φράγμα γιὰ τὸ n: Θὰ ἀποδείξομε πρῶτα ὅτι, γιὰ $i = 1, \ldots, n$ ἰσχύει $r_{i-1} > 2r_{i+1}$. Πράγματι, ἂς θεωρήσομε ἕνα τέτοιον δείκτη i. Ἂν εἶναι $r_i \leq r_{i-1}/2$, τότε, λόγῳ τῆς $r_{i+1} < r_i$, εἶναι καὶ $r_{i+1} < r_{i-1}/2$, δηλαδή, $r_{i-1} > 2r_{i+1}$. Ἄν, πάλι, $r_i > r_{i-1}/2$, τότε, λόγῳ τῆς $r_{i-1} = r_iq_{i+1} + r_{i+1}$, ἔχομε
$r_{i+1} = r_{i-1} - r_iq_{i+1} < r_{i-1} - \dfrac{r_{i-1}}{2}q_{i+1} \leq r_{i-1} - \dfrac{r_{i-1}}{2} = \dfrac{r_{i-1}}{2}$.
Ἔχοντας ἀποδείξει, τώρα, τὴ σχέση $r_{i-1} > 2r_{i+1}$, παίρνομε διαδοχικὰ τὶς ἀνισότητες:
$b = r_1 > 2r_3 > 2^2r_5 > 2^3r_7 > \cdots > 2^{(n-1)/2}r_n$, ἂν ὁ n εἶναι περιττός,
$b = r_1 > r_2 > 2r_4 > 2^2r_6 > 2^3r_8 > \cdots > 2^{(n-2)/2}r_n$, ἂν ὁ n εἶναι ἄρτιος.
Σὲ κάθε περίπτωση, λοιπόν, $b > 2^{(n-2)/2}$, ἀπ' ὅπου, λογαριθμίζοντας, παίρνομε τὴν ἀποδεικτέα ἀνισότητα. **ὅ.ἔ.δ.**

Μία μικρὴ ἰδέα γιὰ τὴ σπουδαιότητα τοῦ φράγματος, ποὺ ἀποδείξαμε, παίρνει κανεὶς ἀπὸ τὴν ἑξῆς συγκεκριμένη περίπτωση: Γιὰ τὸν ὑπολογισμὸ τοῦ μεγίστου κοινοῦ διαιρέτη τῶν a, b, ὅταν ὁ μικρότερος ἀπὸ τοὺς δύο (ὁ b) εἶναι 300ψήφιος ἀκέραιος, ἀπαιτοῦνται λιγότερα ἀπὸ 2000 βήματα n. Ἀλλὰ 2000 εὐκλείδειες διαιρέσεις κοστίζουν ἀμελητέο χρόνο ἀκόμη καὶ σὲ ἕνα προσωπικὸ ὑπολογιστή.

Παράδειγμα. Ὑποδεικνύομε ἕνα τρόπο ὀργάνωσης τῶν ὑπολογισμῶν, ποὺ περιγράφονται στὸ θεώρημα 1.2.3: Ἔστω ὅτι ζητοῦμε τὸν $(7168, 917)$. Οἱ ἀλλεπάλληλες διαιρέσεις τοῦ θεωρήματος 1.2.3 φαίνονται δίπλα.

$$\begin{aligned} 7168 &= 917 \cdot 7 + 749 \\ 917 &= 749 \cdot 1 + 168 \\ 749 &= 168 \cdot 4 + 77 \\ 168 &= 77 \cdot 2 + 14 \\ 77 &= 14 \cdot 5 + 7 \\ 14 &= 7 \cdot 2 + 0 \end{aligned}$$

Τὸ τελευταῖο πηλῖκο (= τελευταῖο μὴ μηδενικὸ ὑπόλοιπο) εἶναι 7, ἄρα $(7168, 917) = 7$.

Αὐτὴ ἡ ὑπολογιστικὴ διαδικασία, κατὰ τὴν ὁποία,σὲ κάθε βῆμα, διαιρετέος εἶναι ὁ διαιρέτης τοῦ προηγουμένου βήματος καὶ διαιρέτης, τὸ ὑπόλοιπο τοῦ προηγουμένου βήματος, περιγράφεται μὲ πιὸ εὐσύνοπτο τρόπο παραπλεύρως.

$$\begin{array}{rrrrrrrr}
 & & & & & 7168 & \multicolumn{1}{|l}{917} & \\ \cline{7-8}
 & & & & 917 & \multicolumn{1}{|r|}{749} & 7 & \\ \cline{6-6}
 & & & 749 & \multicolumn{1}{|r|}{168} & 1 & & \\ \cline{5-5}
 & & 168 & \multicolumn{1}{|r|}{77} & 4 & & & \\ \cline{4-4}
 & 77 & \multicolumn{1}{|r|}{14} & 2 & & & & \\ \cline{3-3}
14 & \multicolumn{1}{|r|}{7} & 5 & & & & & \\ \cline{2-2}
0 & \multicolumn{1}{|l}{2} & & & & & &
\end{array}$$

Παρατηρῆστε ὅτι, τὸ θεώρημα 1.2.3 προβλέπει, γιὰ τὸ συγκεκριμένο παράδειγμα, πλῆθος βημάτων n, ποὺ δὲν ὑπερβαίνουν τὸ φράγμα $2\log 917/\log 2 + 2 = 21.68155\ldots$, δηλαδή, $n \leq 21$. Στὴν πράξη, εἴδαμε ὅτι $n = 6$.

Ἡ διαδικασία ὑπολογισμοῦ τῶν $s_i, (i = -1, \ldots, n)$ γίνεται πολὺ ἁπλά: Μὲ τονισμένα τυπογραφικὰ στοιχεῖα σημειώνονται τὰ ἐξ ἀρχῆς γνωστὰ δεδομένα. Κατόπιν, τὰ κουτιὰ συμπληρώνονται ἀπὸ ἀριστερὰ πρὸς τὰ δεξιά. Στὴ γραμμὴ τοῦ q τὰ κουτιὰ συμπληρώνονται, ἀπὸ τὴν τρίτη στήλη καὶ μετά, μὲ τὰ πηλίκα τοῦ εὐκλειδείου ἀλγορίθμου *ἀπὸ τὸ τελευταῖο πηλίκο πρὸς τὸ πρῶτο* (βλ. παραπάνω), ἐνῶ στὴ γραμμὴ τοῦ s, στὰ δύο ἀριστερώτερα κουτιὰ μπαίνουν τὰ $s_{-1} = s_0 = 1$ καὶ μετά, ἀναδρομικά, τὰ s_i, σύμφωνα μὲ τὸ διπλανὸ σχῆμα ὅπου ἐννοεῖται ὅτι τὰ A, B, C εἶναι ἤδη γνωστὰ καὶ συμπληρώνεται τὸ κουτὶ κάτω ἀπὸ τὸ A,σύμφωνα μὲ τὸ Θεώρημα 1.2.3 (β′). Κουτιὰ μὲ $*$ δὲν παίζουν ρόλο στὸν συγκεκριμένο ὑπολογισμό.

$*$	$*$	A
C	B	$-A \cdot B + C$

Στὸ συγκεκριμένο παράδειγμα ἔχομε:

q			**2**	**5**	**2**	**4**	**1**	**7**
s	**1**	**1**	-1	6	-13	58	-71	555

Φυσικά, καθὼς προβλέπει τὸ 2 τοῦ θεωρήματος 1.2.3, $(-71) \cdot 7168 + 555 \cdot 917 = 7 = (7168, 917)$.

Ἕνας κάπως διαφορετικὸς καὶ πολὺ εὔχρηστος ἀλγόριθμος ὑπολογισμοῦ ἀκεραίων x_0, y_0, τέτοιων ὥστε $ax_0 + by_0 = (a, b)$, περιγράφεται στὴν ἄσκηση 19.

1.3 Ἐλάχιστο κοινὸ πολλαπλάσιο

Σταθεροποιοῦμε δύο μὴ μηδενικοὺς ἀκεραίους a, b. *Κοινὸ πολλαπλάσιο* τῶν a, b εἶναι κάθε ἀκέραιος, ποὺ εἶναι πολλαπλάσιο καὶ τοῦ a καὶ τοῦ b. Τὸ σύνολο τῶν θετικῶν κοινῶν πολλαπλασίων τῶν a, b εἶναι μὴ κενό (π.χ. περιέχει τὸν $|ab|$) ὁπότε ἔχει ἕνα ἐλάχιστο στοιχεῖο, τὸ ὁποῖο καλεῖται *ἐλάχιστο κοινὸ πολλαπλάσιο τῶν* a, b καὶ συμβολίζεται $[a, b]$.

Θεώρημα 1.3.1 *Ἔστω ὅτι a, b εἶναι μὴ μηδενικοί ἀκέραιοι. Τότε:*

α′. Ἕνας ἀκέραιος εἶναι κοινὸ πολλαπλάσιο τῶν a, b ἄν, καὶ μόνο ἄν, εἶναι τῆς μορφῆς $\dfrac{nab}{(a, b)}$ γιὰ κάποιο $n \in \mathbb{Z}$. Εἰδικώτερα, $[a, b] = \dfrac{|ab|}{(a, b)}$. Ἄρα, ἂν $(a, b) = 1$, τότε $[a, b] = |ab|$.

β′. Τὸ σύνολο τῶν κοινῶν πολλαπλασίων τῶν a, b ταυτίζεται μὲ τὸ σύνολο τῶν πολλαπλασίων τοῦ $[a, b]$.

γ′. Ἂν $(a, b) = 1$ καὶ καθένας ἀπὸ τοὺς a, b διαιρεῖ τὸν m, τότε καὶ τὸ γινόμενό τους ab διαιρεῖ τὸν m.
Γενίκευση: Ἂν οἱ $a_1, \ldots, a_n$ εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους καὶ καθένας ἀπὸ αὐτοὺς διαιρεῖ τὸν m, τότε καὶ τὸ γινόμενο $a_1 \cdots a_n$ διαιρεῖ τὸν m.

Ἀπόδειξη α′. Ἔστω m κοινὸ πολλαπλάσιο τῶν a, b. Ἀφοῦ $a|m$, μποροῦμε νὰ γράψομε $m = ak$ μὲ $k \in \mathbb{Z}$. Ἔστω $d = (a, b)$ καὶ ἂς θέσομε $a = da_1, b = db_1$. Ἀπὸ τὸ δ′ τοῦ θεωρήματος 1.2.2 ἔχομε ὅτι $(a_1, b_1) = 1$. Ἡ ὑπόθεση $b|m$ ἰσοδυναμεῖ μὲ τὸ ὅτι $ak/b \in \mathbb{Z}$, ἄρα $a_1k/b_1 \in \mathbb{Z}$, δηλαδή, $b_1|a_1k$. Τώρα, τὸ στ′ τοῦ θεωρήματος 1.2.2 μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι $b_1|k$, ἄρα $k = nb_1$ γιὰ κάποιο $n \in \mathbb{Z}$. Ἄρα, τελικά, $m = ak = ab_1n = a(db_1)n/d = n(ab)/d$. Ἀντίστροφα, κάθε ἀριθμὸς τῆς μορφῆς $n(ab)/d$ εἶναι κοινὸ πολλαπλάσιο τῶν a, b. Πράγματι, ἕναν τέτοιο ἀριθμὸ μποροῦμε νὰ τὸν δοῦμε ὡς $n(b/d)a$. Ἀλλὰ $d|b$, ἄρα ὁ ἀριθμὸς αὐτὸς εἶναι πολλαπλάσιο τοῦ a. Ἀνάλογα, ἂν γράψομε τὸν ἀριθμὸ ὡς $n(a/d)b$, καταλήγομε στὸ συμπέρασμα ὅτι ὁ ἀριθμὸς εἶναι καὶ πολλαπλάσιο τοῦ b.
Τέλος, εἶναι προφανὲς ὅτι, μιὰ καὶ οἱ a, b εἶναι σταθεροί, τὸ μέγεθος τοῦ nab/d ἐξαρτᾶται ἀπὸ τὸν n, ἄρα ἡ ἐλάχιστη θετικὴ τιμὴ τοῦ ἀριθμοῦ αὐτοῦ –τὸ ἐλάχιστο κοινὸ πολλαπλάσιο τῶν a, b– εἶναι $|ab|/d$.
β′. Ἔστω $d = (a, b)$. Ἀπὸ τὸ α′, κάθε κοινὸ πολλαπλάσιο τῶν a, b εἶναι τῆς μορφῆς nab/d, ἐνῶ $ab/d = \pm[a, b]$. Ἄρα, κάθε κοινὸ πολλαπλάσιο τῶν a, b εἶναι πολλαπλάσιο τοῦ $[a, b]$. Ἀλλὰ καὶ ἀντίστροφα, ἔστω $n[a, b]$ πολλαπλάσιο τοῦ $[a, b]$. Τότε $n[a, b] = nab/d = n(b/d)a = n(a/d)b$, ἀπ' ὅπου βλέπομε ὅτι ὁ ἀριθμὸς αὐτὸς εἶναι πολλαπλάσιο καὶ τοῦ a καὶ τοῦ b.
γ′. Βάσει τοῦ (α′), $[a, b] = |ab|$, ἐνῶ, ἀπὸ τὸ (β′), ὁ m εἶναι πολλαπλάσιο τοῦ $[a, b]$, ἄρα, πολλαπλάσιο τοῦ ab.
Ἔστω τώρα ὅτι οἱ $a_1, \ldots, a_n$ εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους καὶ καθένας διαιρεῖ

τὸν m. Ἐφαρμόζοντας αὐτὸ ποὺ ἀποδείξαμε μόλις πρίν, μὲ $a = a_1, b = a_2$, συμπεραίνομε ὅτι ὁ m εἶναι πολλαπλάσιο τοῦ a_1a_2. Ὁ a_3, τώρα, εἶναι πρῶτος πρὸς τὸν a_1a_2, ἀφοῦ εἶναι πρῶτος πρὸς καθένα ἀπ' τοὺς a_1, a_2 (βλ. ζ′ τοῦ θεωρήματος 1.2.2). Ἔτσι, ἔχομε καὶ πάλι δύο ἀριθμούς, τοὺς $a = a_3$ καὶ $b = a_1a_2$, οἱ ὁποῖοι εἶναι πρῶτοι μεταξύ τους καὶ καθένας διαιρεῖ τὸν m, ἄρα καὶ τὸ γινόμενό τους $ab = a_1a_2a_3$ διαιρεῖ τὸν m. Ἐπαναλαμβάνοντας τοὺς ἀνάλογους συλλογισμούς, ὁδηγούμαστε ἐπαγωγικὰ στὸ συμπέρασμα ὅτι ὁ m εἶναι πολλαπλάσιο τοῦ $a_1a_2 \cdots a_n$. **ὅ.ἔ.δ.**

Τὸ ἐλάχιστο κοινὸ πολλαπλάσιο περισσοτέρων τῶν δύο ἀριθμῶν $a_1, \ldots, a_{n-1}, a_n$ ὁρίζεται ὡς ὁ ἐλάχιστος *θετικὸς* ἀκέραιος, ὁ ὁποῖος εἶναι πολλαπλάσιο καθενὸς ἀπὸ τοὺς $a_1, \ldots, a_{n-1}, a_n$ καὶ συμβολίζεται $[a_1, \ldots, a_{n-1}, a_n]$. Ὁ ὑπολογισμός του γίνεται ἀναδρομικά, δηλαδή,

$$\begin{aligned}
[a_1, a_2, a_3] &= [[a_1, a_2], a_3] \\
[a_1, a_2, a_3, a_4] &= [[a_1, a_2, a_3], a_4] \\
&\vdots \\
[a_1, \ldots, a_{n-1}, a_n] &= [[a_1, \ldots, a_{n-1}], a_n]
\end{aligned}$$

Φυσικά, πρέπει νὰ ἀποδείξομε ὅτι αὐτὴ ἡ διαδικασία μᾶς δίνει, ὄντως, τὸ ἐλάχιστο κοινὸ πολλαπλάσιο τῶν $a_1, \ldots, a_{n-1}, a_n$. Γιὰ τὴν ἀπόδειξη βλ. ἄσκηση 26.

1.4 Πρῶτοι ἀριθμοί

Οἱ πρῶτοι ἀριθμοὶ ἀποτελοῦν τοὺς δομικοὺς λίθους, μὲ τοὺς ὁποίους κτίζονται πολλαπλασιαστικὰ οἱ ἀκέραιοι ἀριθμοί. Ἄς παρατηρήσομε, προκαταρκτικά, ὅτι γιὰ κάθε ἀκέραιο n, οἱ $\pm 1, \pm n$ εἶναι διαιρέτες τοῦ n. Αὐτοὶ λέγονται *τετριμμένοι διαιρέτες* τοῦ n.

Ὁρισμός 1.4.1 *Ὁ ἀκέραιος n καλεῖται πρῶτος ἂν εἶναι διάφορος τῶν $0, \pm 1$ καὶ οἱ μόνοι διαιρέτες του εἶναι οἱ τετριμμένοι ± 1 καὶ $\pm n$. Ὁ n καλεῖται σύνθετος ἂν εἶναι διάφορος τῶν $0, \pm 1$ καὶ ἔχει καὶ ἄλλους διαιρέτες ἐκτὸς τῶν τετριμμένων. Οἱ ἀριθμοὶ ± 1 χαρακτηρίζονται ὡς μονάδες τοῦ $\mathbb{Z}$ καὶ εἶναι τὰ μόνα στοιχεῖα τοῦ $\mathbb{Z}$, τὰ ὁποῖα ἔχουν ἀντίστροφο μέσα στὸ $\mathbb{Z}$. Εἶναι προφανὲς ὅτι, ὁ n εἶναι πρῶτος (ἀντιστοίχως, σύνθετος) ἄν, καὶ μόνο ἄν, ὁ $-n$ εἶναι πρῶτος (ἀντιστοίχως, σύνθετος).*

Γιὰ πράδειγμα, οἱ ± 7 καὶ ± 13 εἶναι πρῶτοι ἀριθμοί, ἀφοῦ καθένας ἀπὸ αὐτοὺς ἔχει μόνο τετριμμένους διαιρέτες. Ἀντίθετα, οἱ ± 10 εἶναι σύνθετοι ἀριθμοί, ἀφοῦ, ἐκτὸς ἀπὸ τοὺς τετριμμένους διαιρέτες τους $\pm 1, \pm 10$ ἔχουν καὶ τοὺς διαιρέτες ± 5.

Θεώρημα 1.4.2 *α′. Γιὰ κάθε $m \neq 0, \pm 1$, ὁ ἐλάχιστος μεγαλύτερος τοῦ 1 διαιρέτης τοῦ m εἶναι πρῶτος. Ἄρα, κάθε ἀκέραιος διάφορος τῶν ± 1 ἔχει ἕνα, τουλάχιστον, πρῶτο διαιρέτη.*

β′. Ἂν ὁ p εἶναι πρῶτος καὶ ὁ a εἶναι τυχὼν ἀκέραιος, τότε, ἕνα ἀπὸ τὰ δύο *συμβαίνει:* $p|a$ *ἢ* $(p,a) = 1$. *Ἐνῶ, ἂν ὁ* p *εἶναι σύνθετος, ὑπάρχουν* a *γιὰ τοὺς ὁποίους τίποτε ἀπὸ τὰ δύο δὲν συμβαίνει.*

γʹ. Ἂν ὁ p *εἶναι πρῶτος καὶ* $(a_i, p) = 1$ *γιὰ ὅλα τὰ* $i = 1, \ldots, n$, *τότε ὁ* p *δὲν διαιρεῖ τὸ γινόμενο* $a_1 \cdots a_n$.

Εἰδικὴ περίπτωση τῆς δύναμης: Ἂν $(p,a) = 1$, *τότε ὁ* p *δὲν διαιρεῖ τὸν* a^n.

Ἰσοδύναμη (λόγῳ τοῦ βʹ) διατύπωση: Ἂν ὁ p *εἶναι πρῶτος καὶ δὲν διαιρεῖ κανέναν ἀπὸ τοὺς* $a_1, \ldots, a_n$, *τότε οὔτε τὸ γινόμενό τους διαιρεῖ.*

Στὴν εἰδικὴ περίπτωση τῆς δύναμης: Ἂν ὁ p *δὲν διαιρεῖ τὸν* a, *τότε, οὔτε καὶ τὸν* a^n *διαιρεῖ.*

Ἰσοδύναμη διατύπωση (ἀντιστροφο-αντίθετη διατύπωση τῆς προηγούμενης): Ἂν ὁ p *εἶναι πρῶτος καὶ διαιρεῖ τὸ γινόμενο* $a_1 \cdots a_n$, *τότε ὁ* p *διαιρεῖ τουλάχιστον ἕναν ἀπὸ τοὺς παράγοντες* $a_1, \ldots, a_n$.

Εἰδικὴ περίπτωση τῆς δύναμης: Ἂν $p|a^n$, *τότε* $p|a$.

Ἄν, ὅμως, ὁ p *εἶναι σύνθετος καὶ διαιρεῖ τὸ γινόμενο* $a_1 \cdots a_n$, *τότε δὲν μποροῦμε νὰ συμπεράνομε ὅτι διαιρεῖ ἕνα, τουλάχιστον, ἀπὸ τοὺς* $a_1, \ldots, a_n$.

δʹ. Ὁ ἐλάχιστος θετικὸς πρῶτος διαιρέτης ἑνὸς σύνθετου ἀριθμοῦ m *δὲν ὑπερβαίνει τὸν* $\sqrt{|m|}$.

εʹ. Ἂν P *εἶναι ἕνα* ὁποιοδήποτε *πεπερασμένο σύνολο θετικῶν πρώτων ἀριθμῶν, τότε ὑπάρχει πρῶτος, ὁ ὁποῖος δὲν ἀνήκει στὸ* P. *Ἄρα, τὸ σύνολο τῶν πρώτων ἀριθμῶν εἶναι ἄπειρο.*[3]

Ἀπόδειξη Γιὰ $m \neq 0, \pm 1$ ἂς συμβολίσομε μὲ $\Delta(m)$ τὸ σύνολο τῶν διαιρετῶν τοῦ m, οἱ ὁποῖοι ὑπερβαίνουν τὸ 1. Προφανῶς, τὸ $\Delta(m)$ εἶναι μὴ κενό καὶ πεπερασμένο, μὲ μέγιστο στοιχεῖο του τὸν $|m|$.

αʹ. Ἔστω p τὸ ἐλάχιστο στοιχεῖο τοῦ $\Delta(m)$. Θὰ ἀποδείξομε ὅτι ὁ p εἶναι πρῶτος. Ἂν δὲν ἦταν, θὰ ἦταν σύνθετος (παρατηρῆστε ὅτι $p > 1$), ἄρα, ἐκτὸς ἀπὸ τοὺς τετριμμένους διαιρέτες του θὰ εἶχε καὶ κάποιο *ἄλλο* διαιρέτη $d > 1$. Ὁπότε θὰ εἴχαμε τὴν ἑξῆς κατάσταση: $d|p$ καὶ $p|m$, ἄρα, ἀπὸ τὸ θεώρημα 1.1.1, $d|m$. Ὅμως $1 < d < p$, ἄρα ὁ d εἶναι στοιχεῖο τοῦ $\Delta(m)$, μικρότερο τοῦ p, τὸ ὁποῖο εἴχαμε ὑποθέσει ἐλάχιστο στοιχεῖο τοῦ συνόλου· ἄτοπο.

βʹ. Ἂς ὑποθέσομε ὅτι ὁ p εἶναι πρῶτος καὶ δὲν ἰσχύει $(a,p) = 1$. Θὰ δείξομε, τότε, ὅτι ἰσχύει ἡ σχέση $p|a$. Ἀλλά, πράγματι, ἀπὸ τὴν ὑπόθεση συμπεραίνομε ὅτι $(a,p) = d > 1$, ὁπότε ὁ p διαιρεῖται ἀπὸ τὸν $d > 1$. Ἐξ ὁρισμοῦ τοῦ πρώτου ἀριθμοῦ, αὐτὸ εἶναι δυνατὸν μόνο ἂν $d = \pm p$. Ἀλλὰ τότε, ἀφοῦ $d|a$, συμπεραίνομε ὅτι $p|a$.

Ἄν, τώρα, ὁ p εἶναι σύνθετος, τότε ἂς τὸν ὑποθέσομε, δίχως βλάβη τῆς γενικότητος θετικό, καὶ ἂς τὸν γράψομε $p = ab$, ὅπου $1 < a, b < p$. Τότε, γι' αὐτὸν τὸν συγκεκριμένο ἀκέραιο a, καὶ οἱ δύο σχέσεις $p|a$ καὶ $(p,a) = 1$ εἶναι ψευδεῖς.

γʹ. Ἡ ἀπόδειξη τοῦ ἰσχυρισμοῦ, στὴν πρώτη του διατύπωση, εἶναι ἄμεση συνέπεια τῆς πρότασης ζʹ τοῦ θεωρήματος 1.2.2, τὴν ὁποία ἐφαρμόζομε θέτοντας $m = 1$ καὶ

[3] Πρόκειται γιὰ τὴν πρόταση 20 τοῦ Βιβλίου Θʹ τῶν *Στοιχείων* τοῦ Εὐκλείδου: «Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν».

$b_1 = p$.
Ὅσον ἀφορᾶ τὸ ὅτι ἡ τελευταία διατύπωση δὲν ἰσχύει ὅταν ὁ p εἶναι σύνθετος: Στὴν περίπτωση αὐτή, μποροῦμε νὰ γράψομε (ὑποθέτοντας, χωρὶς βλάβη τῆς γενικότητος, τὸν p θετικό) $p = a_1a_2$, ὅπου $1 < a_1, a_2 < p$. Τότε, βεβαίως, $p|a_1a_2$, ἀλλὰ καμμία ἀπὸ τὶς σχέσεις $p|a_1$ καὶ $p|a_2$ δὲν εἶναι ἀληθής.
δ΄. Ἀπὸ τὸ (α΄) ξέρομε ἤδη ὅτι τὸ ἐλάχιστο στοιχεῖο, ἔστω p, τοῦ $\Delta(m)$ εἶναι πρῶτος ἀριθμός, ἐνῶ ἡ ὑπόθεση ὅτι ὁ m εἶναι σύνθετος συνεπάγεται ὅτι $p < |m|$. Παρατηρῆστε ὅτι ὁ $\frac{|m|}{p}$ εἶναι ἀκέραιος ἀριθμὸς μεγαλύτερος τοῦ 1, ἄρα, ἀπὸ τὸ (α΄) ἔχει ἕνα πρῶτο διαιρέτη q, τὸν ὁποῖο, χωρὶς βλάβη τῆς γενικότητος, μποροῦμε νὰ ὑποθέσομε θετικό. Ἔτσι, ἔχομε $q|\frac{m}{p}$ καὶ $\frac{m}{p}|m$ (διότι τὸ πηλίκο τοῦ m διὰ $\frac{m}{p}$ εἶναι ἀκέραιος), ὁπότε $q|m$. Ἡ ὑπόθεση ὅτι ὁ p εἶναι ὁ ἐλάχιστος πρῶτος, ποὺ διαιρεῖ τὸν m μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι $p \le q$, ἄρα $p \le \frac{|m|}{p}$, σχέση ἰσοδύναμη μὲ τὴν ἀποδεικτέα.
ε΄. Ὁ ἰσχυρισμὸς εἶναι προφανὴς ἂν τὸ P εἶναι κενό. Ἔστω τώρα ὅτι $P = \{p_1, \ldots, p_k\}$. Θεωροῦμε τὸν $m \overset{o\rho\sigma}{=} p_1 \cdots p_k + 1$, ὁ ὁποῖος, προφανῶς εἶναι ἀκέραιος μεγαλύτερος τοῦ 1, ἄρα, ἀπὸ τὸ (α΄) ἔχει ἕνα, τουλάχιστον, πρῶτο διαιρέτη q. Θὰ δείξομε ὅτι $q \notin P$. Πράγματι, γιατὶ διαφορετικά, ὁ q θὰ ἦταν ἴσος μὲ κάποιον $p_i \in \{p_1, \ldots, p_k\}$, ὁπότε $q|(p_1 \cdots p_i \cdots p_k)$. Ὅμως $q|m$, ἄρα (πρόταση 1.1.1) $d|m - (p_1 \cdots p_k) = 1$, ἄτοπο.
ὅ.ἔ.δ.

Τὸ κόσκινο τοῦ Ἐρατοσθένους. Ἐφαρμόζεται γιὰ τὴν κατασκευὴ τῆς λίστας ὅλων τῶν (θετικῶν) πρώτων ἀριθμῶν, ποὺ δὲν ὑπερβαίνουν δοθέντα ἀκέραιο $n > 2$. Συνίσταται στὴν ἑξῆς διαδικασία, ἡ ὁποία διαγράφει τοὺς σύνθετους ἀριθμούς, οἱ ὁποῖοι εἶναι μικρότεροι τοῦ ἀκεραίου $n > 2$, γιὰ νὰ μείνουν οἱ πρῶτοι, οἱ μὴ ὑπερβαίνοντες τὸν n. Ἔστω π. χ. ὅτι $n = 50$. Γράφομε τοὺς ἀκεραίους 2,3,...,50. Διαγράφομε ὅλα τὰ μεγαλύτερα ἀπὸ τὸν 2 πολλαπλάσιά του, δηλαδή, τοὺς 4,6,...,48,50. Ὁ μικρότερος ἀκέραιος, μετὰ τὸν 2, ποὺ δὲν ἔχει διαγραφεῖ εἶναι ὁ 3. Διαγράφομε ὅλα τὰ μεγαλύτερα ἀπὸ αὐτὸν πολλαπλάσιά του, δηλαδή, τοὺς 6,9,...,45,48. Παρατηροῦμε ὅτι ὁ 6 διαγράφεται καὶ ὡς πολλαπλάσιο τοῦ 2 καὶ ὡς πολλαπλάσιο τοῦ 3, ἀλλὰ αὐτὸ δὲν ἔχει καμμία σημασία. Συνεχίζομε: Ὁ ἐλάχιστος, μετὰ τὸν 3, ἀκέραιος, ποὺ δὲν ἔχει διαγραφεῖ, εἶναι ὁ 5. Διαγράφομε ὅλα τὰ μεγαλύτερα ἀπὸ αὐτὸν πολλαπλάσιά του, δηλαδή, τοὺς 10,15...,45,50. Ἔτσι συνεχίζομε, παρατηρώντας ποιὸς εἶναι ὁ ἀμέσως ἑπόμενος μὴ διαγεγραμμένος ἀκέραιος, τοῦ ὁποίου καὶ διαγράφομε ὅλα τὰ γνησίως μεγαλύτερα ἀπὸ αὐτὸν πολλαπλάσιά του. Σταματοῦμε ὅταν δὲν ἔχομε νὰ διαγράψομε ἄλλους ἀκεραίους μέχρι το 50 καὶ τότε, ὅλοι οἱ μὴ διαγεγραμμένοι, καὶ μόνον αὐτοί, εἶναι οἱ πρῶτοι ἀριθμοί, οἱ μὴ ὑπερβαίνοντες τὸ 50. Πότε, ὅμως, ἀρκεῖ νὰ σταματήσομε; Εἶναι ἀνάγκη, νὰ ἐπιχειρήσομε τὴ διαγραφὴ τῶν πολλαπλασίων τοῦ 17, γιὰ παράδειγμα; Ὄχι! Τὸ θεώρημα 1.4.2 (δ΄) μᾶς λέει ὅτι, ἂν κάποιος ἀριθμὸς εἶναι σύνθετος, θὰ πρέπει νὰ ἔχει διαγραφεῖ ὡς πολλαπλάσιο τοῦ 2, ἢ τοῦ 3, ἢ τοῦ 5, ἢ τοῦ 7. Διότι κάθε σύνθετος, ποὺ δὲν ὑπερβαίνει τὸ 50 ἔχει, σύμφωνα μὲ τὴν πρόταση, ἕνα πρῶτο διαιρέτη $\le \sqrt{50} = 7.071\ldots$. Ἔτσι, στὴ συγκεκριμένη περίπτωση $n = 50$, μετὰ ποὺ θὰ διαγράψομε καὶ τὰ πολλαπλάσια τοῦ 7, ἔχομε τὴν ἑξῆς κατάσταση:

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13
~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~
~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37
~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~
~~50~~											

Εἴμαστε βέβαιοι, σύμφωνα μὲ ὅ,τι εἴπαμε παραπάνω, ὅτι ὅλοι οἱ διαγεγραμμένοι ἀριθμοὶ εἶναι σύνθετοι καὶ ὅλοι οἱ ὑπόλοιποι εἶναι πρῶτοι.

Θεώρημα 1.4.3 –Θεμελιῶδες θεώρημα τῆς Ἀριθμητικῆς. *Κάθε ἀκέραιος $n > 1$ ἀναλύεται σὲ γινόμενο θετικῶν πρώτων: $n = p_1 \cdots p_k$. Ἡ ἀνάλυση αὐτὴ εἶναι μοναδική, ὑπὸ τὴν ἑξῆς ἔννοια: Ἂν $n = q_1 \cdots q_\ell$ καὶ οἱ $q_1, \ldots, q_\ell$ εἶναι θετικοὶ πρῶτοι, τότε $k = \ell$ καὶ οἱ $q_1, \ldots, q_\ell$ ἀποτελοῦν, ἁπλῶς, μία μετάθεση τῶν $p_1, \ldots, p_k$.*

Ἀπόδειξη Πρῶτα ἀποδεικνύομε ὅτι ὁ n ἀναλύεται σὲ γινόμενο πρώτων, χωρὶς νὰ μᾶς ἀπασχολεῖ ἡ μοναδικότητα τῆς ἀνάλυσης.

Λόγῳ τοῦ θεωρήματος 1.4.2 (α′), ὁ n ἔχει ἕνα πρῶτο θετικὸ διαιρέτη p_1 καὶ θέτομε $n = p_1 n_1$. Ἂν $n_1 = 1$, τότε $n = p_1$ καὶ ἔχομε ἀνάλυση τοῦ n σὲ ἕνα πρῶτο διαιρέτη. Διαφορετικά, $1 < n_1 < n$ καὶ ὁ n_1 ἔχει ἕνα πρῶτο διαιρέτη p_2, ὁπότε θέτομε $n_1 = p_2 n_2$, ἄρα $n = p_1 p_2 n_2$. Αν $n_2 = 1$, τότε $n = p_1 p_2$ καὶ ἔχομε ἀνάλυση τοῦ n σὲ δύο πρώτους διαιρέτες. Διαφορετικά, $1 < n_2 < n_1 < n$ καὶ ὁ n_2 ἔχει ἕνα πρῶτο διαιρέτη p_3, ὁπότε θέτομε $n_2 = p_3 n_3$, ἄρα $n = p_1 p_2 p_3 n_3$. Ἔτσι προχωροῦμε, καὶ στὸ βῆμα i ἔχομε $n = p_1 p_2 \cdots p_i n_i$, ὅπου $n > n_1 > n_2 > \cdots n_i > 0$. Ἄρα, δὲν μπορεῖ νὰ ἔχομε *ἄπειρη κάθοδο* , ὁπότε σὲ κάποιο βῆμα $i = k$ θὰ καταλήξομε σὲ $n_k = 1$, δηλαδή, $n = p_1 \cdots p_k$.

Τώρα ἀποδεικνύομε τὴ μοναδικότητα τῆς ἀνάλυσης σὲ πρώτους διαιρέτες. Ἔστω $n = q_1 \cdots q_\ell$ καὶ οἱ $q_1, \ldots, q_\ell$ εἶναι θετικοὶ πρῶτοι. Χωρὶς βλάβη τῆς γενικότητας ὑποθέτομε ὅτι $\ell \geq k$. Ἐπίσης δίχως βλάβη τῆς γενικότητας ὑποθέτομε ὅτι $p_1 \leq p_2 \leq \cdots \leq p_k$ καὶ $q_1 \leq q_2 \leq \cdots \leq q_\ell$. Ἔχομε $q_1 | p_1 \cdots p_k$, ἄρα, ἀπὸ τὸ Θεώρημα 1.4.2 (ζ′), ὁ q_1 διαιρεῖ ἕνα, τουλάχιστον, ἀπὸ τοὺς $p_1, \ldots, p_k$. Ἔστω ὅτι $q_1 | p_i$. Ἀλλά, καθὼς ὁ p_i εἶναι πρῶτος, ὁ μόνος διαιρέτης του ποὺ ὑπερβαίνει τὸ 1 εἶναι ὁ ἑαυτός του, ἄρα $q_1 = p_i \geq p_1$. Ἐντελῶς ἀνάλογα, ἀπὸ τὴ σχέση $p_1 \mid q_1 \cdots q_\ell$ συμπεραίνομε ὅτι, γιὰ κάποιον δείκτη j ἔχομε $p_1 = q_j \geq q_1$. Καταλήξαμε ἔτσι στὶς σχέσεις $q_1 \geq p_1$ καὶ $p_1 \geq q_1$, ἄρα $q_1 = p_1$ καὶ συνεπῶς, διαγράφοντας αὐτοὺς τοὺς παράγοντες ἀπὸ τὴν ἰσότητα $p_1 \cdots p_k = q_1 \cdots q_\ell$, παίρνομε τὴν ἰσότητα $p_2 \cdots p_k = q_2 \cdots q_\ell$. Ἐπαναλάμβάνοντας γι’ αὐτὴ τὴν ἰσότητα ἐντελῶς ἀνάλογο μὲ τὸν παραπάνω συλλογισμό, καταλήγομε στὸ ὅτι $q_2 = p_2$ καί, διαδοχικά, $q_3 = p_3, \ldots q_k = p_k$. Ἀλλά τότε, στὸ k-βῆμα, καθὼς θὰ ἔχουν διαγραφεῖ ἀπὸ τὴν ἰσότητα $p_1 \cdots p_k = q_1 \cdots q_\ell$ τὰ $p_1, q_1, p_2, q_2, p_3, q_3, \ldots, p_k, q_k$, θὰ μείνομε μὲ μία ἰσότητα τῆς ὁποίας τὸ ἀριστερὸ μέλος ἰσοῦται μὲ 1, ἄρα τὸ δεξιὸ δὲν μπορεῖ νὰ εἶναι γινόμενο πρώτων q_j, δηλαδή, $\ell = k$. **ὅ.ἔ.δ.**

Γιὰ κάθε ἀκέραιο $n \neq 0, \pm 1$ ὑπάρχει μία βολική, σὲ πολλὲς περιπτώσεις, ἀνάλυσή του, ποὺ λέγεται *κανονικὴ ἀνάλυση* τοῦ n, ἡ ὁποία εἶναι ἡ ἑξῆς: Τὸ θεώρημα 1.4.3 μᾶς ἐξασφαλίζει ὅτι $n = \pm p_1 p_2 \dots p_k$, ὅπου οἱ $p_1, \dots, p_k$ εἶναι θετικοὶ πρῶτοι, ὄχι, κατ' ἀνάγκη, διαφορετικοί. Ὁπότε ὁμαδοποιώντας ἴσους πρώτους, γράφομε $n = \pm q_1^{a_1} \cdots q_m^{a_m}$, ὅπου τώρα: (α′) Οἱ πρῶτοι $q_1, \dots, q_m$ εἶναι διαφορετικοὶ μεταξύ τους. (β′) $m \le k$ καὶ $a_i \ge 1$ γιὰ κάθε $i = 1, \dots, m$.

Παρατηροῦμε ὅτι, ἂν $n = \pm q_1^{a_1} \cdots q_m^{a_m}$ εἶναι ἡ κανονικὴ ἀνάλυση τοῦ n, τότε $q_1^{a_1}$ εἶναι ἡ μέγιστη δύναμη τοῦ q_1, ποὺ διαιρεῖ τὸν n διότι, ἂν $q_1^b | n$, τότε $n = q_1^b c$, γιὰ κάποιον ἀκέραιο c, ὁπότε $\pm q_1^{a_1} q_2^{a_2} \cdots q_m^{a_m} = q_1^b c$. Ἂν, λοιπόν, ἦταν $b > a_1$, τότε, ἁπλοποιώντας τὰ δύο μέλη διὰ $q_1^{a_1}$, θὰ καταλήγαμε σὲ μία σχέση, στὸ ἀριστερὸ μέλος τῆς ὁποίας θὰ ἐμφανιζόταν ὁ πρῶτος q_1 μὲ θετικὸ ἐκθέτη, ἐνῶ στὸ ἀριστερὸ δὲν θὰ ὑπῆρχε ὁ πρῶτος παράγοντας q_1· αὐτὸ ἀντίκειται στὸ θεώρημα 1.4.3, ποὺ μᾶς λέει ὅτι ἡ ἀνάλυση ἑνὸς ἀριθμοῦ σὲ πρώτους παράγοντες εἶναι μοναδική.

Ἔχοντας αὐτὴ τὴν παρατήρηση κατὰ νοῦ, ὁρίζομε, γιὰ κάθε ἀκέραιο n καὶ κάθε πρῶτο p, τὸν *ἐκθέτη* τοῦ p στὸν n, συμβολιζόμενο $v_p(n)$, ὡς ἑξῆς: $v_p(n) = \infty$ ἂν $n = 0$ καὶ $v_p(n) = a\,(\ge 0)$ ἂν p^a εἶναι ἡ μέγιστη δύναμη τοῦ p, ποὺ διαιρεῖ τὸν n. Γιὰ παράδειγμα, $v_2(1200) = 4$, $v_3(1200) = 1$, $v_5(1200) = 2$, $v_7(1200) = 0$.
Εἶναι ἁπλὸ νὰ ἀποδείξει κανεὶς τὶς ἑξῆς ἰδιότητες τοῦ ἐκθέτη:

- $v_p(ab) = v_p(a) + v_p(b)$. Γενίκευση: $v_p(a_1 \cdots a_n) = v_p(a_1) + \cdots + v_p(a_n)$. Εἰδικώτερα: $v_p(a^n) = n \cdot v_p(a)$.
- $v_p(a \pm b) \ge \min(v_p(a), v_p(b))$. Ἂν $v_p(a) \ne v_p(b)$, τότε ἰσχύει τὸ =. Γενίκευση: $v_p(a_1 + \cdots + a_n) \ge \min\{v_p(a_1), \dots, v_p(a_n)\}$. Ἂν γιὰ ἕνα μόνο $i \in \{1, \dots, n\}$ "πιάνεται" τὸ minimum στὸ δεξιὸ μέλος, τότε ἰσχύει το =.

Συνεπῶς, ἂν $n = \pm q_1^{a_1} \cdots q_m^{a_m}$ εἶναι ἡ κανονικὴ ἀνάλυση τοῦ n, τότε

$$n = \pm q_1^{v_{q_1}(n)} q_2^{v_{q_2}(n)} \cdots q_m^{v_{q_m}(n)} .$$

Ἀλλὰ γιὰ κάθε πρῶτο $p \notin \{q_1, q_2, \dots, q_m\}$ ἔχομε $v_p(n) = 0$, ἄρα ἡ παραπάνω σχέση μπορεῖ νὰ γραφτεῖ, πιὸ ὁμοιόμορφα, ὡς ἑξῆς:

$$n = \pm \prod_{p \text{ πρῶτος}} p^{v_p(n)} , \tag{1.1}$$

ὅπου, βέβαια, τὸ γινόμενο στὸ δεξιὸ μέλος ἔχει ἄπειρους παράγοντες, ἀλλὰ δὲν ἔχει ἄπειρη τιμή, ἀφοῦ μόνο πεπερασμένο πλῆθος ἀπὸ αὐτοὺς τοὺς παράγοντες ἔχει τιμὴ μεγαλύτερη τοῦ 1. Τὴν ἀνάλυση (1.1) τοῦ n θὰ λέμε *γενικευμένη κανονικὴ ἀνάλυση* τοῦ n.

Ἡ ἔννοια τοῦ ἐκθέτη ἐπεκτείνεται καὶ στοὺς ρητούς, κατὰ τρόπο φυσιολογικό: Ἂν $\rho \in \mathbb{Q}$, γράφομε τὸν ρ ὡς πηλίκο ἀκεραίων $\rho = a/b$ καὶ ὁρίζομε $v_p(\rho) = v_p(a) - v_p(b)$. Ὁ ὁρισμὸς αὐτὸς εἶναι ἀνεξάρτητος ἀπὸ τὸν τρόπο, ποὺ θὰ γράψομε τὸν ρ ὡς πηλίκο ἀκεραίων· βλ. ἄσκηση 28. Τώρα μποροῦμε νὰ ἐπεκτείνομε τὴ γενικευμένη κανονικὴ ἀνάλυση καὶ στοὺς ρητούς: Ὁρίζεται ἀπὸ τὴν (1.1), ὅπου τὸ n τώρα μπορεῖ νὰ παριστάνει καὶ ρητό.

Ἡ χρήση τῶν ἐκθετῶν καὶ τῆς γενικευμένης κανονικῆς ἀνάλυσης εἶναι, σὲ πολλὲς περιπτώσεις, πολὺ βοηθητική.

Θεώρημα 1.4.4 *α΄. Ἔστω ὅτι a, b εἶναι ἀκέραιοι καὶ $b \neq 0$. Τότε, ὁ b διαιρεῖ τὸν a ἄν, καὶ μόνο ἄν, $v_p(b) \leq v_p(a)$ γιὰ κάθε (θετικὸ) πρῶτο p.*

β΄. Ἄν $a = \pm p_1^{s_1} \cdots p_m^{s_m}$ εἶναι ἡ κανονικὴ ἀνάλυση τοῦ a, τότε, κάθε θετικὸς διαιρέτης τοῦ a εἶναι τῆς μορφῆς $p_1^{t_1} \cdots p_m^{t_m}$, ὅπου $0 \leq t_i \leq s_i$ γιὰ κάθε $i = 1, \ldots, m$. Κατὰ συνέπεια, τὸ πλῆθος τῶν θετικῶν διαιρετῶν τοῦ a εἶναι $(s_1 + 1) \cdots (s_m + 1)$.

Ἀπόδειξη α΄. Ἔστω ὅτι $b|a$. Τότε $a = bc$, ἄρα, γιὰ κάθε πρῶτο p, ἔχομε $v_p(a) = v_p(bc) = v_p(b) + v_p(c) \geq v_p(b)$. Ἀντιστρόφως, ἔστω ὅτι, γιὰ κάθε πρῶτο p εἶναι $v_p(a) \geq v_p(b)$. Ἄν $b = \pm 1$, τότε $b|a$. Διαφορετικά, ἔστω $b = p_1^{r_1} \cdots p_m^{r_m}$ ἡ κανονικὴ ἀνάλυση τοῦ b. Ἀπὸ τὴν ὑπόθεση, $v_{p_i}(a) \geq r_i$ γιὰ κάθε $i = 1, \ldots, m$. Αὐτὸ σημαίνει ὅτι, ἂν κάνομε τὴν κανονικὴ ἀνάλυση τοῦ a, αὐτὴ θὰ ἔχει τὴ μορφὴ

$$a = \pm p_1^{s_1} \cdots p_m^{s_m} c\,, \quad s_i \geq r_i \quad (i = 1, \ldots, m)\,,$$

ὅπου $c = 1$ ἢ γινόμενο δυνάμεων κάποιων πρώτων διαφορετικῶν ἀπὸ τοὺς $p_1, \ldots, p_m$· οὕτως ἢ ἄλλως, ὅμως, ὁ c εἶναι ἀκέραιος. Συνεπῶς, παραβάλλοντας μὲ τὴν κανονικὴ ἀνάλυση τοῦ b (βλ. λίγο παραπάνω), καταλήγομε στὴ σχέση

$$a = \pm b(c p_1^{s_1 - r_1} \cdots p_m^{s_m - r_m})\,.$$

Τὸ ἐντὸς τῆς παρενθέσεως γινόμενο εἶναι ἀκέραιος ἀριθμός, ἄρα $b|a$.

β΄. Ὁ ἰσχυρισμὸς σχετικὰ μὲ τὴ μορφὴ τῶν διαιρετῶν τοῦ a προκύπτει ἀμέσως ἀπὸ τὸ μέρος α΄ τοῦ θεωρήματος. Ὅσον ἀφορᾶ στὸ πλῆθος τῶν θετικῶν διαιρετῶν τοῦ a, παρατηροῦμε τὰ ἑξῆς: Γιὰ τὸν ἐκθέτη t_1 ὑπάρχουν $s_1 + 1$ ἐπιλογές (ἀφοῦ $0 \leq t_1 \leq s_1$), γιὰ τὸν t_2 ὑπάρχουν $s_2 + 1$ ἐπιλογές,. . . , γιὰ τὸν t_m ὑπάρχουν $s_m + 1$ ἐπιλογές, ἄρα γιὰ τὸν $p_1^{t_1} \cdots p_m^{t_m}$ ὑπάρχουν $(s_1 + 1)(s_2 + 1) \cdots (s_m + 1)$ ἐπιλογὲς καὶ ὅλες εἶναι διαφορετικὲς μεταξύ τους, λόγῳ τῆς μοναδικότητας τῆς ἀνάλυσης σὲ πρώτους παράγοντες. **ὅ.ἔ.δ.**

Ἡ μοναδικότητα τῆς ἀνάλυσης ἑνὸς ἀκεραίου σὲ πρώτους παράγοντες (θεώρημα 1.4.3) ἔχει σημαντικὲς ἐφαρμογὲς στὴν ἐπίλυση διοφαντικῶν ἐξισώσεων, δηλαδή, ἐξισώσεων στὶς ὁποῖες οἱ ἄγνωστοι εἶναι ἀκέραιοι ἤ, κάποιες φορές, ρητοί. Μία θεμελιώδης βοηθητικὴ πρόταση, χρήσιμη στὴν ἐπίλυση τέτοιων ἐξισώσεων, ἀλλὰ καὶ σὲ πολλὲς ἄλλες περιπτώσεις, εἶναι ἡ ἑξῆς.

Πρόταση 1.4.5 *Ἄν a, b, c εἶναι θετικοὶ ἀκέραιοι, τέτοιοι ὥστε $(a, b) = 1$ καὶ $ab = c^n$, ὅπου $n \geq 2$, τότε ὑπάρχουν ἀκέραιοι c_1, c_2 τέτοιοι ὥστε $a = c_1^n$, $b = c_2^n$ καὶ $c_1 c_2 = c$.*

Ἀπόδειξη Ἔστω πρῶτος p. Ἀπὸ τὶς ἰδιότητες τῆς συνάρτησης v_p στὴ σελίδα 16, ἔχομε

$$v_p(a) + v_p(b) = v_p(ab) = v_p(c^n) = n \cdot v_p(c).$$

Οἱ a, b εἶναι πρῶτοι μεταξύ τους, συνεπῶς, ἀποκλείεται νὰ εἶναι $v_p(a) > 0$ καὶ $v_p(b) > 0$, διότι κάτι τέτοιο ἰσοδυναμεῖ μὲ $p|a$ καὶ $p|b$. Ἄν, $v_p(b) = 0$, τότε $v_p(a) = n \cdot v_p(c)$, ἄρα $n|v_p(a)$. Ἀλλά, ἀφοῦ $v_p(b) = 0$, ἔχομε καὶ $n|v_p(b)$. Ἐντελῶς ἀνάλογα, καὶ στὴν περίπτωση $v_p(a) = 0$, συμπεραίνομε ὅτι ὁ n διαιρεῖ τοὺς $v_p(a)$ καὶ $v_p(b)$.

Αὐτὸ ἰσοδυναμεῖ μὲ τὸ ὅτι καθένας ἀπ’ τοὺς a, b εἶναι n-οστὴ δύναμη ἀκεραίου, σύμφωνα μὲ τὴν ἄσκηση 29. **ὅ.ἔ.δ.**

Κάποιες ἐνδιαφέρουσες ἐφαρμογὲς τῶν ἐκθετῶν καὶ τῆς γενικευμένης κανονικῆς ἀνάλυσης δίδονται π.χ. στὶς ἀσκήσεις 30 καὶ 31.

1.5 Πυθαγόρειες τριάδες

Σ’ αὐτὴ τὴν ἑνότητα θὰ λύσομε τὴ Διοφαντικὴ ἐξίσωση $x^2 + y^2 = z^2$, δηλαδή, θὰ ὑπολογίσομε ὅλες τὶς λύσεις της σὲ μὴ μηδενικοὺς *ἀκεραίους* x, y, z. Κάθε τέτοια λύση (x, y, z) λέγεται *πυθαγόρεια τριάδα*.

Ἔστω τώρα ὅτι (x, y, z) εἶναι μία πυθαγόρεια τριάδα. Θέτομε $(x, y) = d$, $x = dX$, $y = dY$ καὶ ξέρομε ἀπὸ τὸ Θεώρημα 1.2.2 (δ′) ὅτι $(X, Y) = 1$. Ἀπὸ τὴ σχέση $x^2 + y^2 = z^2$ παίρνομε, συνεπῶς, $X^2 + Y^2 = (z/d)^2$. Τὸ ἀριστερὸ μέλος τῆς τελευταίας εἶναι ἀκέραιος ἀριθμός, ἄρα καὶ τὸ δεξιό. Τότε, ὅμως, ἡ ἄσκηση 13 μᾶς λέει ὅτι ὁ z/d εἶναι ἀκέραιος, τὸν ὁποῖο συμβολίζομε Z. Ὁπότε, τελικά,

$$x = dX\,,\ y = dY\,,\ z = dZ\,,\ (X, Y) = 1\,,\quad X^2 + Y^2 = Z^2 \tag{1.2}$$

Τώρα κάνομε μία σειρὰ ἀπὸ μικρὲς παρατηρήσεις. Λεπτομέρειες τῶν ἀποδείξεών τους ἀφήνομε ὡς ἀσκήσεις:

- $(X, Z) = 1$ καὶ $(Y, Z) = 1$.

- Οἱ X, Y δὲν μπορεῖ νὰ εἶναι καὶ οἱ δύο περιττοί. Πράγματι, γιατὶ τότε, ὁ ἀκέραιος $X^2 + Y^2$ θὰ ἦταν τῆς μορφῆς $4k + 2$, δηλαδή, ἄρτιος, ἀλλὰ ὄχι διαιρετὸς διὰ 4, ὁπότε δὲν μπορεῖ νὰ ἰσοῦται μὲ τετράγωνο.
  Χωρὶς βλάβη τῆς γενικότητας, λοιπόν, ὑποθέτομε, στὸ ἑξῆς, τὸν X περιττὸ καὶ τὸν Y ἄρτιο. Προφανῶς, ὁ Z εἶναι περιττός. Ἐπίσης, λόγῳ τοῦ ὅτι στὴν ἐξίσωσή μας ἐμφανίζονται μόνο τὰ τετράγωνα τῶν X, Y, Z, μποροῦμε νὰ ὑποθέσομε τοὺς X, Y, Z θετικοὺς ἀκεραίους.

- Γράφομε τὴν (1.2) ὡς $(Z - Y)(Z + Y) = X^2$. Ἀπὸ τὶς προηγούμενες παρατηρήσεις εἶναι εὔκολο νὰ διαπιστώσει κανεὶς ὅτι οἱ $Z + Y, Z - Y$ εἶναι περιττοὶ καὶ $(Z - Y, Z + Y) = 1$.

- Μὲ ἐφαρμογὴ τῆς πρότασης 1.4.5 στὴ σχέση $(Z-Y)(Z+Y) = X^2$ (παρατηρῆστε ὅτι οἱ $X, Z + Y, Z - Y$ εἶναι θετικοί) συμπεραίνομε ὅτι $Z + Y = a^2$, $Z - Y = b^2$ καὶ $X = ab$, ὅπου οἱ a, b εἶναι περιττοὶ καὶ $(a, b) = 1$.

- Λύνοντας ὡς πρὸς Z, Y βρίσκομε $Z = (a^2 + b^2)/2$ καὶ $Y = (a^2 - b^2)/2$. Γιὰ νὰ ἀποφύγομε τὸν παρονομαστὴ 2, θέτομε $a = A + B$ καὶ $b = A - B$, ὅπου οἱ A, B εἶναι *ἑτερότυποι* , δηλαδή, ὁ ἕνας ἄρτιος καὶ ὁ ἄλλος περιττός (δὲν καθορίζεται ποιὸς ὁ ἄρτιος καὶ ποιὸς ὁ περιττός). Εὔκολα διαπιστώνεται ὅτι $(A, B) = 1$. Ὁπότε, λαμβάνοντας ὑπ' ὄψει καὶ τὴν $X = ab$, καταλήγομε, τελικά, στοὺς τύπους τῶν *πρωταρχικῶν* πυθαγορείων τριάδων (X, Y, Z) (πρωταρχικές, σημαίνει ὅτι οἱ X, Y, Z εἶναι, ἀνὰ δύο πρῶτοι μεταξύ τους):

$$X = A^2 - B^2\,,\ Y = 2AB\,,\ Z = A^2 + B^2\,,$$

A, B ἑτερότυποι, πρῶτοι μεταξύ τους.

- Τώρα, λόγῳ τῶν $x = dX, y = dY, z = dZ$ καταλήγομε στοὺς πιὸ γενικοὺς τύπους τῶν πυθαγορείων τριάδων, δίνοντας στὸν d ὁποιεσδήποτε ἀκέραιες τιμές:
$$x = d(A^2 - B^2)\,,\ Y = 2dAB\,,\ Z = d(A^2 + B^2)\,,$$
A, B ἑτερότυποι, πρῶτοι μεταξύ τους. Ἐννοεῖται ὅτι ὁ ρόλος τῶν X, Y μπορεῖ νὰ ἐναλλαγεῖ, λόγῳ τοῦ συμμετρικοῦ ρόλου αὐτῶν τῶν μεταβλητῶν στὴν ἐξίσωσή μας.

Γιὰ $d = 1, A = 2, B = 1$ παίρνομε τὴν ἁπλούστερη πρωταρχικὴ πυθαγόρεια τριάδα (3,4,5), ἡ ὁποία ἔχει τὴν ἀξιοσημείωτη ἰδιότητα ὅτι ἀποτελεῖται ἀπὸ διαδοχικοὺς ἀκεραίους. Γιὰ $d = 1, A = 5, B = 2$ παίρνομε τὴν πρωταρχικὴ πυθαγόρεια τριάδα (21,20,29).

1.6 Ἀσκήσεις τοῦ κεφαλαίου 1

«Ἀριθμὸς» σημαίνει πάντα «ἀκέραιος ἀριθμός»

1. Ἀποδεῖξτε τοὺς ἑξῆς ἰσχυρισμούς:
ἄρτιος + ἄρτιος = ἄρτιος, ἄρτιος + περιττός = περιττός,
περιττός + περιττός = ἄρτιος.

2. Ὑπολογίστε τοὺς $d = (a, b)$, $m = [a, b]$, καθὼς καὶ x_0, y_0 ποὺ νὰ ἐπαληθεύουν τὴ σχέση $ax_0 + by_0 = d$ σὲ κάθε μία ἀπὸ τὶς ἑξῆς περιπτώσεις: (1) $a = 422, b = 182$. (2) $a = 3701, b = 2311$. (3) $a = 703, b = 399$.

3. Ἂν ὁ d εἶναι κοινὸς διαιρέτης τῶν $ax + by$ καὶ $a'x + b'y$ καὶ $(d, ab' - a'b) = 1$, ἀποδεῖξτε ὅτι ὁ d εἶναι κοινὸς διαιρέτης τῶν x, y.

4. Ἔστω $n \geq 1$ καὶ Δ τὸ σύνολο τῶν θετικῶν διαιρετῶν τοῦ n. Ἀποδεῖξτε ὅτι $\Delta = \left\{\dfrac{n}{d} \;:\; d \in \Delta\right\}$ καὶ μετά, ἀποδεῖξτε τὸ ἑξῆς: Ἂν $\Delta = \{d_1, d_2, \ldots, d_k\}$, τότε
$$\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = \frac{d_1 + d_2 + \cdots + d_k}{n}.$$

5. Ἀποδεῖξτε ὅτι, τὸ τετράγωνο ὁποιουδήποτε περιττοῦ ἀριθμοῦ, διαιρούμενο διὰ 8 δίνει ὑπόλοιπο 1· ἄρα διαιρούμενο καὶ διὰ 4 δίνει ὑπόλοιπο 1.

6. Ἀποδεῖξτε ὅτι, τὸ τετράγωνο ἑνὸς ἀριθμοῦ, ὁ ὁποῖος δὲν εἶναι πολλαπλάσιο τοῦ 3, διαιρούμενο διὰ 3 δίνει ὑπόλοιπο 1.

7. Ἀποδεῖξτε ὅτι, ὁ κύβος ἑνὸς ἀριθμοῦ μὴ διαιρετοῦ διὰ 7, ὅταν διαιρεθεῖ διὰ 7 δίνει ὑπόλοιπο 1 ἢ 6.

8. Ἀποδεῖξτε ὅτι, μεταξὺ δύο διαδοχικῶν ἀριθμῶν, ὁ ἕνας εἶναι ἄρτιος. Ἐπίσης, μεταξὺ τριῶν διαδοχικῶν ἀριθμῶν ὁ ἕνας διαιρεῖται διὰ 3. Δεῖξτε ὅτι, γιὰ κάθε n, ὁ $n(n+1)(2n+1)$ εἶναι πολλαπλάσιο τοῦ 6.

9. (α′) Ἂν ὁ ἕνας ἐκ τῶν a, b εἶναι ἄρτιος καὶ ὁ ἄλλος περιττὸς καὶ $(a, b) = 1$, τότε καὶ $(a+b, a-b) = 1$.
   (β′) Ἂν οἱ a, b εἶναι περιττοί, ἀποδεῖξτε ὅτι οἱ $(a+b)/2$ καὶ $(a-b)/2$ εἶναι, καὶ οἱ δύο, ἀκέραιοι, ὁ ἕνας (ὄχι, κατ' ἀνάγκην ὁ πρῶτος) ἄρτιος καὶ ὁ ἄλλος περιττός. Ἂν, ἐπιπλέον, ὑποθέσομε ὅτι $(a, b) = 1$, ἀποδεῖξτε ὅτι $(\frac{a+b}{2}, \frac{a-b}{2}) = 1$.

10. Ἔστω $\frac{a}{b} = \frac{m}{n}$, ὅπου τὸ κλάσμα στὸ δεξιὸ μέλος εἶναι *ἀνάγωγο*, δηλαδή, $(m, n) = 1$. Ἀποδεῖξτε ὅτι ὑπάρχει $k \in \mathbb{Z}$, τέτοιο ὥστε $a = km$ καὶ $b = kn$. Βασισμένοι σὲ αὐτὸ ἀποδεῖξτε ὅτι, ἂν $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, τότε ὑπάρχουν $k, \ell \in \mathbb{Z}$, τέτοια ὥστε $ka_1 = \ell a_2$ καὶ $kb_1 = \ell b_2$.

11. Ἂν $(a, b) = 1$ καὶ $m, n \geq 1$, ἀποδεῖξτε ὅτι $(a^m, b^n) = 1$.

12. Ἀποδεῖξτε ὅτι $(a, b) = (a+b, [a, b])$. Ἐφαρμογή: Ὑπολογῖστε δύο θετικοὺς ἀκεραίους, τῶν ὁποίων τὸ ἄθροισμα εἶναι 64 980 καὶ τὸ ἐλάχιστο κοινὸ πολλαπλάσιό τους ἰσοῦται μὲ 58 639 842.

13. Ἀποδεῖξτε ὅτι, ἂν $n \geq 2$ καὶ ἡ n-οστὴ δύναμη ἑνὸς ρητοῦ εἶναι ἀκέραιος ἀριθμός, τότε ὁ ρητὸς εἶναι, ἀναγκαστικά, ἀκέραιος.
    Ὑπόδειξη: Γρᾶψτε τὸν ρητὸ μὲ τὴ μορφὴ $\frac{a}{b}$, ὅπου $(a, b) = 1$.
    Ἰσοδύναμη διατύπωση: Ἂν ἡ n-οστὴ ρίζα ἑνὸς ἀκεραίου εἶναι ρητὸς ἀριθμός, τότε ὁ ρητὸς αὐτὸς ἀριθμὸς εἶναι ἀκέραιος. Μ' ἄλλα λόγια, ἡ n-οστὴ ρίζα ἀκεραίου εἶναι ἢ ἄρρητος ἀριθμὸς ἢ ἀκέραιος.

14. (Γενίκευση τῆς προηγούμενης) Ἔστω πολυώνυμο $a_n x^n + \cdots a_1 x + a_0$ μὲ ἀκέραιους συντελεστές, ὅπου $n \geq 2$ καὶ $a_n \neq 0$. Ὑποθέτομε ὅτι τὸ πολυώνυμο αὐτὸ ἔχει κάποια ρητὴ ρίζα, τὴν ὁποία γράφομε ὡς ἀνάγωγο κλάσμα $\frac{k}{\ell}$ $((k, \ell) = 1)$. Ἀποδεῖξτε ὅτι $\ell | a_n$ καὶ $k | a_0$. Παρατηρῆστε ὅτι αὐτό, εἰδικώτερα, συνεπάγεται ὅτι, ἂν $a_n = 1$ καὶ τὸ πολυώνυμο ἔχει ρητὴ ρίζα, αὐτὴ εἶναι, ὑποχρεωτικά, ἀκέραια.
    Ἡ ἄσκηση αὐτὴ δίνει μία μέθοδο εὕρεσης ὅλων τῶν *πιθανῶν* ρητῶν ριζῶν ἑνὸς πολυωνύμου μὲ ἀκέραιους συντελεστές, ἂν ὑπάρχουν τέτοιες.

15. Ἔστω ὅτι οἱ a, b εἶναι θετικοὶ ἀκέραιοι, ὄχι καὶ οἱ δύο ἄρτιοι. Ὁρίζομε $a_1 = a$, $b_1 = b$ καὶ γιὰ $k = 2, 3, \ldots$, ἀναδρομικά,
Ἂν ὁ a_{k-1} εἶναι ἄρτιος: $a_k = a_{k-1}/2$, $b_k = b_{k-1}$.
Ἂν ὁ b_{k-1} εἶναι ἄρτιος: $a_k = a_{k-1}$, $b_k = b_{k-1}/2$.
Ἂν οἱ a_{k-1} καὶ b_{k-1} εἶναι περιττοί: $a_k = \min(a_{k-1}, b_{k-1})$, $b_k = |a_{k-1} - b_{k-1}|/2$.
Ἀποδεῖξτε τὰ ἑξῆς: (α′) Γιὰ κάθε $k = 1, 2, 3, \ldots$, οἱ a_k, b_k εἶναι μὴ ἀρνητικοὶ ἀκέραιοι καὶ ὁ ἕνας, τουλάχιστον, εἶναι περιττός.
(β′) Ἂν γιὰ κάποιο $k \geq 2$ εἶναι $a_{k-1}b_{k-1} \neq 0$, τότε $a_k + b_k < a_{k-1} + b_{k-1}$.
(γ′) Γιὰ κάθε $k \geq 2$, $(a_k, b_k) = (a_{k-1}, b_{k-1})$.
(δ′) Ὑπάρχει $n \geq 2$, τέτοιος ὥστε $a_n b_n = 0$ καὶ ὁ μὴ μηδενικὸς ἐκ τῶν a_n, b_n εἶναι ὁ μέγιστος κοινὸς διαιρέτης τῶν a, b.
Ὑπολογῖστε μὲ τὴν παραπάνω διαδικασία τὸν μέγιστο κοινὸ διαιρέτη τῶν 1001 καὶ 4151.

16. Δίδονται οἱ ἀκέραιοι $a_1, \ldots, a_{n-1}, a_n$, $n \geq 3$ καὶ ὁρίζομε ἀναδρομικά: $d_2 = (a_1, a_2)$, $d_{k+1} = (d_k, a_{k+1})$ γιὰ $2 \leq k \leq n-1$. Δεῖξτε μὲ ἐπαγωγὴ ἐπὶ τοῦ k ὅτι οἱ διαιρέτες τοῦ d_k ταυτίζονται μὲ τοὺς κοινοὺς διαιρέτες τῶν $a_1, \ldots, a_k$, ὁπότε, εἰδικώτερα, $d_k = (a_1, \ldots, a_k)$.

17. Ἔστω $d = (a_1, a_2, \ldots, a_n)$ $(n \geq 2)$. Δεῖξτε ἐπαγωγικὰ τὰ ἑξῆς:
(1) Κάθε κοινὸς διαιρέτης τῶν $a_1, a_2, \ldots, a_n$ διαιρεῖ τὸν d.
(2) Ὑπάρχουν ἀκέραιοι $x_1, x_2, \ldots, x_n$, τέτοιοι ὥστε $d = a_1x_1 + a_2x_2 + \cdots a_nx_n$.

18. Στὴν ἀπόδειξη τοῦ θεωρήματος 1.2.2 (δ′), ποῦ ἔπαιξε ρόλο τὸ ὅτι ὁ c εἶναι κοινὸς διαιρέτης τῶν a, b;

19. Ἡ ἄσκηση αὐτὴ προτείνει ἕναν εὔχρηστο ἀλγόριθμο γιὰ νὰ ὑπολογίζει κανείς, ὅταν τοῦ δοθοῦν οἱ θετικοὶ ἀκέραιοι a, b, ἀκεραίους x_0, y_0, τέτοιους ὥστε $ax_0 + by_0 = (a, b)$. Ἐπίσης, δίνει μία ἐναλλακτικὴ ἀπόδειξη τοῦ γεγονότος ὅτι, τὸ τελευταῖο μὴ μηδενικὸ ὑπόλοιπο τοῦ εὐκλειδείου ἀλγορίθμου γιὰ τοὺς a, b ἰσοῦται μὲ τὸν μέγιστο κοινὸ διαιρέτη τους (βλ. θεώρημα 1.2.3).
Δίδονται οἱ θετικοὶ ἀκέραιοι a, b καὶ θεωροῦμε τοὺς n καὶ $q_2, q_3, \ldots$, $r_2, r_3, \ldots$, ὅπως αὐτοὶ ὁρίζονται στὸ θεώρημα 1.2.3 (βλ. καὶ τὶς διαδοχικὲς σχέσεις στὴν ἀπόδειξη τοῦ πρώτου μέρους αὐτοῦ τοῦ θεωρήματος). Ὁρίζομε:

$$\begin{array}{llll} P_1 = q_2\,, & P_2 = q_2q_3 + 1\,, & P_k = q_{k+1}P_{k-1} + P_{k-2} & \text{γιὰ } k = 3, \ldots, n \\ Q_1 = 1\,, & Q_2 = q_3\,, & Q_k = q_{k+1}Q_{k-1} + Q_{k-2} & \text{γιὰ } k = 3, \ldots, n \end{array}$$

(α′) Ἀποδεῖξτε ὅτι $\begin{vmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{vmatrix} = (-1)^{k-1}$ γιὰ κάθε $k = 2, \ldots, n$. Αὐτό, εἰδικώτερα, συνεπάγεται ὅτι $(P_k, Q_k) = 1$ γιὰ κάθε $k = 1, \ldots, n$.
(β′) Ἀποδεῖξτε ὅτι, γιὰ κάθε $k = 1, \ldots, n-1$ ἰσχύουν οἱ σχέσεις

$$P_k r_{k+2} + P_{k+1} r_{k+1} = a \quad \text{καὶ} \quad Q_k r_{k+2} + Q_{k+1} r_{k+1} = b\,.$$

Εἰδικώτερα, γιὰ $k = n-1$ παίρνομε $a = r_nP_n$ καὶ $b = r_nQ_n$. Ἀπὸ τὸ θεώρημα 1.2.3 ξέρομε ὅτι $r_n = (a, b)$. Ὑποθέστε ὅτι ἀγνοεῖτε αὐτὸ τὸ γεγονὸς καὶ ἀποδεῖξτε, μὲ τὴ βοήθεια τῶν γ′ καὶ δ′ τοῦ θεωρήματος 1.2.2 καὶ τοῦ ἐρωτήματος (α′), ὅτι $r_n = (a, b)$.
(γ′) Μὲ τὴ βοήθεια τῶν (α′) καὶ (β′) ἀποδεῖξτε ὅτι $aQ_{n-1} - bP_{n-1} = (-1)^n(a, b)$.
(δ′) Γιὰ $a = 7168$ καὶ $b = 917$ συμπληρῶστε τὸν παρακάτω πίνακα καὶ ἐπαληθεῦστε, στὸ συγκεκριμένο ἀριθμητικὸ παράδειγμα, τὰ (α′),(β′) καὶ (γ′):

$k =$	1	2	3	4	5	$6 = n$
$q_{k+1} =$						
$P_k =$						
$Q_k =$						
$r_{k+1} =$						

20. Ἀκολουθώντας τὴ μεθοδολογία τοῦ ἀριθμητικοῦ παραδείγματος μετὰ τὸ θεώρημα 1.2.3 ὑπολογῖστε τὸν $d = (654321, 123456)$ καί, κατόπιν, δύο ἀκεραίους x_0, y_0, τέτοιους ὥστε $654321x_0 + 123456y_0 = d$. Κατόπιν, ἀκολουθώντας τὴ μεθοδολογία τῆς ἄσκησης 19, ὑπολογῖστε νέα x_0, y_0 μὲ τὴν ἴδια ἰδιότητα. Τὸ ὅτι βρίσκει κανεὶς διαφορετικὲς λύσεις (x_0, y_0) δὲν εἶναι παράλογο· βλ. ἄσκηση 27

21. Ἔστω $n \geq 2$ καὶ θεωροῦμε ὁποιουσδήποτε n *διαδοχικοὺς* ἀκεραίους. Ἀποδεῖξτε ὅτι, ἂν διαιρέσομε καθέναν ἀπὸ αὐτοὺς διὰ n, τὰ ὑπόλοιπα, ποὺ θὰ πάρομε εἶναι διαφορετικὰ μεταξύ τους. Ἀπὸ αὐτὸ συμπεράνατε ὅτι ὁ ἕνας, ἀκριβῶς, ἀπὸ τοὺς n διαδοχικοὺς ἀκεραίους εἶναι διαιρετὸς διὰ n.

22. (Γραφὴ ἀκεραίου σὲ b-αδικὸ σύστημα ἀριθμήσεως). Ἔστω ἀκέραιος $b > 1$. Γιὰ κάθε θετικὸ ἀκέραιο a ἀκολουθοῦμε τὴν ἑξῆς διαδικασία. Ἐκτελοῦμε τὴν εὐκλείδια διαίρεση τοῦ a διὰ b, ἔστω $a = ba_1 + d_0$, $0 \leq d_0 < b$. Ἀναδρομικά, γιὰ $k = 1, 2, \ldots$ ἐκτελοῦμε τὴν εὐκλείδεια διαίρεση τοῦ a διὰ b, ἔστω $a_k = ba_{k+1} + d_k$, $0 \leq d_k < b$. Ἀποδεῖξτε ὅτι, γιὰ κάθε $k \geq 1$ ἰσχύει $a = \sum_{i=0}^{k-1} d_ib^i + a_kb^k$ καὶ γιὰ κάποια τιμὴ $k = n \geq 1$, $a_n = 0$. Συμπεράνετε ὅτι κάθε θετικὸς ἀκέραιος a μπορεῖ νὰ γραφεῖ μὲ τὴ μορφὴ $d_0 + d_1b + \cdots + d_{n_1}b^{n-1}$, ὅπου $0 \leq d_k < b$ γιὰ κάθε $k = 0, \ldots, n-1$ καὶ $d_{n-1} > 0$. Λέμε τότε ὅτι γράψαμε (ἢ παραστήσαμε) τὸν a στὸ *b-αδικὸ σύστημα* ἢ στὸ *σύστημα ἀρίθμησης μὲ βάση* b. Προφανῶς, γιὰ $b = 10$ ἔχομε τὴ γνωστὴ 10-δικὴ παράσταση τοῦ a.

23. Ἔστω $a = bq + r$ μὲ $a, b, r > 0$ (οἱ q, r μπορεῖ νὰ παριστάνουν πηλίκο καὶ ὑπόλοιπο, ἀντιστοίχως, τῆς διαίρεσης τοῦ a διὰ b, ἀλλὰ αὐτὸ δὲν εἶναι ἀπαραίτητο) καὶ n ὁποιοσδήποτε. Ἀποδεῖξτε ὅτι ὑπάρχει s, τέτοιος ὥστε, $n^a - 1 = (n^b - 1)s + n^r - 1$. [4] Μὲ τὴ βοήθεια αὐτοῦ ἀποδεῖξτε τὰ ἑξῆς:

[4]Χρησιμοποιεῖστε τὴν ταυτότητα $x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$.

1. $(n^a - 1, n^b - 1) = (n^b - 1, n^r - 1)$.
2. $(n^a - 1, n^b - 1) = n^d - 1$, ὅπου $d = (a, b)$.

24. Ὑπολογῖστε ἀκέραιες λύσεις κάθε μιᾶς ἀπὸ τὶς ἐξισώσεις $547x + 632y = 1$, $398x + 600y = 2$ καὶ $922x + 2163y = 7$, χρησιμοποιώντας κατάλληλα τὸ θεώρημα 1.2.3.

25. Ὑπάρχουν ἀκέραιες λύσεις x, y τῆς ἐξίσωσης $1841x + 3647y = 1$; Δικαιολογῆστε τὴν ἀπάντησή σας.

26. Δίδονται οἱ ἀκέραιοι $a_1, \ldots, a_{n-1}, a_n$, $n \geq 3$ καὶ ὁρίζομε ἀναδρομικά: $m_2 = [a_1, a_2]$, $m_{k+1} = [m_k, a_{k+1}]$ γιὰ $2 \leq k \leq n-1$. Δεῖξτε μὲ ἐπαγωγὴ ἐπὶ τοῦ k ὅτι τὰ πολλαπλάσια τοῦ m_k ταυτίζονται μὲ τὰ κοινὰ πολλαπλάσια τῶν $a_1, \ldots, a_k$, ὁπότε, εἰδικώτερα, $m_k = [a_1, \ldots, a_k]$.

27. Θεωροῦμε τὴν ἐξίσωση $ax + by = c$, ὅπου οἱ a, b, c εἶναι γνωστοί, μὴ μηδενικοί, καὶ οἱ ἄγνωστοι x, y εἶναι ἀκέραιοι. Ἐξισώσεις, τῶν ὁποίων οἱ ἄγνωστοι εἶναι ἀκέραιοι, ἢ ρητοί, λέγονται *διοφαντικὲς ἐξισώσεις*, πρὸς τιμὴν τοῦ ἀλεξανδρινοῦ μαθηματικοῦ Διοφάντου, τῶν ἑλληνιστικῶν χρόνων, ὁ ὁποῖος ἐμελέτησε συστηματικὰ τέτοιες ἐξισώσεις (ὄχι μόνο πρώτου βαθμοῦ).
(α$'$) Ἀποδεῖξτε ὅτι, ἂν ὁ (a, b) δὲν διαιρεῖ τὸν c, ἡ ἐξίσωση εἶναι ἀδύνατη.
(β$'$) Ἔστω $d = (a, b)$ καὶ $d|c$. Μὲ τὴ βοήθεια τῆς ἄσκησης 21 καὶ ὑποθέτωντας, χωρὶς βλάβη τῆς γενικότητας, ὅτι $b \geq 2$ (γιατὶ δὲν βλάπτεται ἡ γενικότητα;), ἀποδεῖξτε ὅτι ἡ ἐξίσωση ἔχει μία, τουλάχιστον, ἀκέραια λύση (x_0, y_0). Κατόπιν, δεῖξτε ὅτι, γιὰ κάθε $k \in \mathbb{Z}$, λύση εἶναι, ἐπίσης, ἡ $(x, y) = (x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d})$. Συνεπῶς, ἂν ὑπάρχει μία λύση τῆς διοφαντικῆς ἐξίσωσης, τότε ὑπάρχουν ἄπειρες λύσεις της. Μποροῦμε, ὅμως, νὰ προχωρήσομε περισσότερο: Κάθε λύση τῆς διοφαντικῆς ἐξίσωσης ἔχει τὴν παραπάνω μορφή. Δηλαδή, ἂν (x_1, y_1) εἶναι, ἐπίσης, λύση τῆς διοφαντικῆς ἐξίσωσης, τότε ὑπάρχει $k \in \mathbb{Z}$, τέτοιο ὥστε $x_1 = x_0 + k\frac{b}{d}$ καὶ $y_1 = y_0 - k\frac{a}{d}$.

28. Ἂν $b_1 b_2 \neq 0$ καὶ $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, τότε, γιὰ κάθε πρῶτο p ἰσχύει $v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2)$.

29. Ἀποδεῖξτε ὅτι ὁ $a \in \mathbb{N}$ εἶναι n-οστὴ δύναμη ἀκεραίου ἂν καὶ μόνο ἄν, $n|v_p(a)$ γιὰ κάθε πρῶτο p.

30. Ἀποδεῖξτε τὶς σχέσεις

$$(a, b) = \prod_{p \text{ πρῶτος}} p^{\min(v_p(a), v_p(b))}, \quad [a, b] = \prod_{p \text{ πρῶτος}} p^{\max(v_p(a), v_p(b))}.$$

Μὲ τὴ βοήθεια αὐτῶν παρατηρῆστε ὅτι ἀποδεικνύεται ἀμέσως ἡ σχέση $(a, b)[a, b] = ab$.

31. Ἔστω θετικὸς πρῶτος p καὶ θετικὸς ἀκέραιος $k < p$. Ἀποδεῖξτε ὅτι ὁ διωνυμικὸς συντελεστὴς $\binom{p}{k}$ εἶναι πολλαπλάσιο τοῦ p.
   Ὑπόδειξη: Ἀρκεῖ νὰ ἀποδείξετε ὅτι ὁ ἐκθέτης v_p τοῦ διωνυμικοῦ αὐτοῦ συντελεστὴ εἶναι θετικός. Χρησιμοποιῆστε τὴν ταυτότητα $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ καὶ τὶς βασικὲς ἰδιότητες τοῦ ἐκθέτη v_p.

32. (α′) Λίγο παρακάτω ἀπὸ τὴ σχέση (1.1) λέμε πῶς ἡ ἔννοια τοῦ ἐκθέτη $v_p(a)$ ἐπεκτείνεται καὶ σὲ μὴ μηδενικοὺς *ρητοὺς* a. Ἀποδεῖξτε ὅτι οἱ ἰδιότητες τοῦ ἐκθέτη, οἱ ὁποῖες ἀναφέρονται στὴ σελίδα 16 (δεῖτε τὶς δύο •), ἰσχύουν καὶ γιὰ μὴ μηδενικοὺς *ρητοὺς* $a_1, \ldots, a_n$.
   (β′) Ἀποδεῖξτε ὅτι, γιὰ κάθε ἀκέραιο $n \geq 2$, ὁ ρητὸς ἀριθμός $S_n = \sum_{i=2}^{n} \frac{1}{i}$ *δὲν* εἶναι ἀκέραιος.
   Ὑπόδειξη. Δεῖξτε ὅτι τὸ $\min\{v_2(1/i) : i = 2, \ldots, n\}$ πιάνεται μόνο γιὰ $i = 2^k$, ὅπου 2^k εἶναι ἡ μέγιστη δύναμη τοῦ 2 ποὺ εἶναι $\leq n$.

33. (α′) Ἔστω ὅτι a, b εἶναι θετικοὶ ἀκέραιοι καὶ q τὸ πηλῖκο τῆς Εὐκλείδειας διαίρεσης τοῦ a διὰ b. Δεῖξτε ὅτι $q = \left[\frac{a}{b}\right]$ καὶ αὐτὸς ὁ ἀκέραιος ἰσοῦται μὲ τὸ πλῆθος τῶν θετικῶν πολλαπλασίων τοῦ b, τὰ ὁποῖα εἶναι $\leq a$.
   (β′) Ἔστω ὅτι a, p εἶναι θετικοὶ ἀκέραιοι μὲ p πρῶτο. Γιὰ κάθε $i = 1, 2, \ldots$ συμβολίζομε μὲ M_i τὸ πλῆθος τῶν θετικῶν πολλαπλασίων τοῦ p^i ποὺ εἶναι $\leq a$. Ἀποδεῖξτε ὅτι $v_p(a!) = \sum_{i=1}^{\infty} |M_i|$, ὅπου $|M_i|$ συμβολίζει τὸ πλῆθος τῶν στοιχείων τοῦ M_i. Δεῖξτε, ἐπίσης, ὅτι, γιὰ $i > \log a / \log 2$ εἶναι $|M_i| = 0$ καί, συνεπῶς, τὸ ἄπειρο ἄθροισμα ἔχει νόημα.
   (γ′) Μὲ τὴ βοήθεια τῶν (α′) καὶ (β′) ἀποδεῖξτε ὅτι
   $$v_p(a!) = \sum_{i=1}^{\infty} \left[\frac{a}{p^i}\right] < \frac{a}{p-1}.$$

34. Βρεῖτε, μὲ τὴ βοήθεια τῶν πυθαγορείων τριάδων, τύπους στοὺς ὁποίους θὰ γίνεται χρήση δύο ἀκεραίων παραμέτρων, ἔστω C καὶ D καὶ θὰ δίνουν λύσεις τῆς διοφαντικῆς ἐξίσωσης $X^4 + Y^2 = Z^2$ μὲ X ἄρτιο (μία περίπτωση), καὶ X περιττό (δεύτερη περίπτωση).

35. Μιμηθεῖτε, μὲ μικρὲς τροποποιήσεις, τὴν ἀπόδειξη τοῦ Εὐκλείδη γιὰ τὴν ὕπαρξη ἀπείρων πρώτων (πρόταση ε′ τοῦ θεωρήματος 1.4.1) καὶ ἀποδεῖξτε ὅτι ὑπάρχουν ἄπειροι πρῶτοι τῆς μορφῆς $4k + 3$. Ἀνάλογα, ἀποδεῖξτε ὅτι ὑπάρχουν ἄπειροι πρῶτοι τῆς μορφῆς $6k + 5$.

Κεφάλαιο 2

Ἰσοτιμίες

Στὸ κεφάλαιο αὐτό, οἱ m, n εἶναι πάντοτε ἀκέραιοι μεγαλύτεροι τοῦ 1
Τα λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους

2.1 Ὁρισμοὶ καὶ βασικὲς ἰδιότητες

Πρόταση - Ὁρισμός 2.1.1 *Ἔστω ἀκέραιος $m \geq 2$. Οἱ ἑξῆς συνθῆκες εἶναι ἰσοδύναμες γιὰ τοὺς ἀκεραίους a, b:*

1. $m|(b-a)$.
2. *Ὑπάρχει ἀκέραιος k, τέτοιος ὥστε $b = a + km$.*
3. *Τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ a διὰ m εἶναι ἴσο μὲ τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ b διὰ m.*

Ὅταν μία ἀπὸ τὶς παραπάνω ἰσοδύναμες συνθῆκες ἀληθεύει, τότε γράφομε

$$a \equiv b \pmod m$$

καὶ διαβάζομε αὐτὴ τὴ σχέση a ἰσότιμο *b* μέτρῳ *m ἢ a* ἰσότιμο *b* modulo *m. Ὁ m λέγεται* μέτρο τῆς ἰσοτιμίας *$a \equiv b \pmod m$, οἱ δὲ ἀριθμοὶ a, b χαρακτηρίζονται* ἰσότιμοι μέτρῳ *m.* [1] *Αὐτὴ ἡ σχέση ἰσοτιμίας μέτρῳ m εἶναι σχέση ἰσοδυναμίας στὸ σύνολο τῶν ἀκεραίων ἀριθμῶν.*

[1] Ἐδῶ εἶναι σαφὲς τὸ πλεονέκτημα γλωσσικῆς οἰκονομίας, ποὺ παρέχει ἡ χρήση τῆς δοτικῆς «μέτρῳ», δηλαδή, «ὡς πρὸς μέτρο». Ἡ χρήση τοῦ λατινικοῦ modulo εἶναι μᾶλλον κακόηχη στὰ ἑλληνικά, καὶ ἡ ἀντικατάστασή της ἀπὸ τὴ λέξη *μόδιο(ν)*, ποὺ προτείνεται ἀπὸ κάποιους σύγχρονους ἕλληνες συγγραφεῖς (Ν. Μαρμαρίδης, Δ. Νταῆς) μοιάζει πολὺ ἐξεζητημένη, ἂν καὶ εἶναι ἀκριβὴς ἀπὸ ἄποψη γλωσσικῆς ἀντιστοιχίας πρὸς τὸ modulo.

Ἀπόδειξη (1) $\Rightarrow$ (2): Ἡ ὑπόθεση $m|(b-a)$ σημαίνει ὅτι ὑπάρχει k, τέτοιο ὥστε $b-a=mk$, ἄρα $b=a+mk$.
(2) $\Rightarrow$ (3): Ἔστω ὅτι $b=a+mk$. Ἂν q,r εἶναι, ἀντιστοίχως, τὸ πηλίκο καὶ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ a διὰ m, τότε $a=qm+r$ καὶ $0\le r<m$. Ὁπότε, $b=a+mk=(k+q)m+r$ καὶ ἡ σχέση αὐτή, προφανῶς, λέει ὅτι, τὸ πηλίκο τῆς διαίρεσης τοῦ b διὰ m εἶναι $k+q$ καὶ τὸ ὑπόλοιπο (ποὺ αὐτὸ μᾶς ἐνδιαφέρει) εἶναι r. Δηλαδή, οἱ διαιρέσεις τῶν a διὰ m καὶ b διὰ m ἔχουν τὸ ἴδιο ὑπόλοιπο.
(3) $\Rightarrow$ (1): Ἐξ ὑποθέσεως, οἱ διαιρέσεις τῶν a διὰ m καὶ b διὰ m ἔχουν τὸ ἴδιο ὑπόλοιπο, τὸ ὁποῖο ἂς συμβολίσομε r. Ἔστω ὅτι τὰ ἀντίστοιχα πηλίκα εἶναι q_1,q_2. Τότε $a=mq_1+r$, $b=mq_2+r$, ὁπότε $b-a=m(q_2-q_1)$, ἄρα $m|(b-a)$.

Μένει ν' ἀποδείξομε ὅτι ἡ σχέση ἰσοτιμίας μέτρῳ m εἶναι σχέση ἰσοδυναμίας.
Αὐτοπαθὴς ἰδιότητα: $a\equiv a \pmod m$ σημαίνει $m|(a-a)$, σχέση προφανῶς ἀληθής.
Συμμετρικὴ ἰδιότητα: Ἂν ὑποθέσομε ὅτι $a\equiv b \pmod m$, τότε $m|(b-a)$, ὁπότε καὶ $m|(a-b)$. Ἀλλὰ ἡ τελευταία σχέση σημαίνει $b\equiv a \pmod m$.
Μεταβατικὴ ἰδιότητα: Ἂν ὑποθέσομε ὅτι $a\equiv b \pmod m$ καὶ $b\equiv c \pmod m$, τότε $m|(b-a)$ καὶ $m|(c-b)$, ἄρα ὁ m διαιρεῖ τὸν $(b-a)+(c-b)=c-a$. Αὐτό, ἐξ ὁρισμοῦ, σημαίνει ὅτι $a\equiv c \pmod m$. **ὅ.ἔ.δ.**

Ἂν οἱ a,b δὲν εἶναι ἰσότιμοι μέτρῳ m, τότε λέμε ὅτι εἶναι *ἀνισότιμοι μέτρῳ m*

Θεώρημα 2.1.2 - *Βασικὲς ἰδιότητες τῶν ἰσοτιμιῶν.*

α΄. Ἰσοτιμίες μὲ τὸ ἴδιο μέτρο μποροῦν νὰ προστεθοῦν, νὰ ἀφαιρεθοῦν ἢ νὰ πολλαπλασιασθοῦν κατά μέλη.

β΄. Τὰ δύο μέλη μιᾶς ἰσοτιμίας μποροῦν νὰ ὑψωθοῦν στὴν ἴδια δύναμη.

γ΄. Τὰ δύο μέλη μιᾶς ἰσοτιμίας μποροῦν νὰ πολλαπλασιασθοῦν μὲ τὸν ἴδιο ἀριθμό.

δ΄. Ἂν $f(x_1,\dots,x_n)$ εἶναι μία πολυωνυμικὴ παράσταση μὲ ἀκέραιους συντελεστὲς καὶ $a_i\equiv b_i \pmod m$ γιὰ $i=1,\dots,n$, τότε $f(a_1,\dots,a_n)\equiv f(b_1,\dots,b_n) \pmod m$.

ε΄. Ἂν k εἶναι ὁποιοσδήποτε ἀκέραιος, τότε ἡ ἰσοτιμία $a\equiv b \pmod m$ ἂν καὶ μόνο ἂν ἰσχύει ἡ $ka\equiv kb \pmod{km}$. Ἀντιστρόφως, ἂν d εἶναι κοινὸς διαιρέτης τῶν a,b,m, τότε ἡ ἰσοτιμία $a\equiv b \pmod m$ ἰσχύει ἂν καὶ μόνο ἂν ἰσχύει ἡ ἰσοτιμία $\frac{a}{d}\equiv\frac{b}{d} \pmod{\frac{m}{d}}$.

στ΄. Τὰ δύο μέλη μιᾶς ἰσοτιμίας μποροῦν νὰ διαιρεθοῦν μὲ ἕνα κοινὸ διαιρέτη τῶν δύο μελῶν τῆς ἰσοτιμίας, ἀρκεῖ αὐτὸς ὁ διαιρέτης νὰ εἶναι πρῶτος πρὸς τὸ μέτρο.

ζ΄. Ἂν $a\equiv b \pmod m$ καὶ $d\ge 2$ εἶναι διαιρέτης τοῦ m, τότε $a\equiv b \pmod d$.

η΄ Ἂν $a\equiv b \pmod m$, τότε $(a,m)=(b,m)$.

Ἀπόδειξη Δίνομε συνοπτικὰ τὶς οὕτως ἢ ἄλλως ἁπλὲς ἀποδείξεις τῶν ἰσχυρισμῶν τοῦ θεωρήματος.

α΄. Δίνομε τὴν ἀπόδειξη γιὰ δύο ἰσοτιμίες $a_i\equiv b_i \pmod m$, $(i=1,2)$. Γιὰ περισσότερες χρειάζεται ἁπλῆ ἐπαγωγή. Ἔχομε $b_i=a_i+k_im$ $(i=1,2)$ γιὰ κάποιους $k_i\in\mathbb{Z}$. Προσθαφαιρώντας αὐτὲς τὶς σχέσεις παίρνομε $(b_1\pm b_2)=(a_1\pm a_2)+(k_1\pm k_2)m$, δηλαδή, $a_1\pm a_2\equiv b_1\pm b_2 \pmod m$. Πολλαπλασιάζοντας τὶς ἴδιες σχέσεις παίρνομε $b_1b_2=a_1a_2+(a_1k_2+a_2k_1+k_1k_2m)m$, ἄρα $a_1a_2\equiv b_1b_2 \pmod m$.

β′. Ἔστω $a \equiv b\,(\text{mod } m)$. Γράφομε αὐτὴ τὴν ἰσοτιμία n φορὲς καὶ πολλαπλασιάζομε αὐτὲς τὶς n τὸ πλῆθος ἰσοτιμίες κατὰ μέλη (μποροῦμε λόγῳ τοῦ α′), ὁπότε παίρνομε $a^n \equiv b^n\,(\text{mod } m)$.

γ′. Ἂν $a \equiv b\,(\text{mod } m)$ καὶ k εἶναι τυχὼν ἀκέραιος, θέλομε νὰ δείξομε ὅτι $ka \equiv kb\,(\text{mod } m)$, δηλαδή, ὅτι ὁ m διαιρεῖ τὸν $kb - ka = k(b - a)$. Αὐτό, ὅμως, εἶναι ἀληθές, διότι $m|(b - a)$.

δ′. Ἡ παράσταση $f(x_1, \dots, x_n)$ εἶναι ἄθροισμα πεπερασμένου πλήθους ὅρων τῆς μορφῆς $kx_1^{e_1} \cdots x_n^{e_n}$. Ἐπειδὴ μποροῦμε νὰ προσθέτομε ἰσοτιμίες κατὰ μέλη (λόγῳ τοῦ α′), ἀρκεῖ νὰ δείξομε ὅτι, γιὰ κάθε τέτοιο μονώνυμο, ἰσχύει $ka_1^{e_1} \cdots a_n^{e_n} \equiv kb_1^{e_1} \cdots b_n^{e_n}\,(\text{mod } m)$. Πράγματι, ἐξ ὑποθέσεως, $a_1 \equiv b_1\,(\text{mod } m), \dots, a_n \equiv b_n\,(\text{mod } m)$, ἄρα, μὲ χρήση τῶν προτάσεων α′, β′ καὶ γ′, ἔχομε: $a_1^{e_1} \equiv b_1^{e_1}\,(\text{mod } m), \dots, a_n^{e_n} \equiv b_n^{e_n}\,(\text{mod } m)$. Πολλαπλασιάζοντας κατὰ μέλη, $a_1^{e_1} \cdots a_n^{e_n} \equiv b_1^{e_1} \cdots b_n^{e_n}\,(\text{mod } m)$ καί, μετά, πολλαπλασιάζοντας ἐπὶ k, $ka_1^{e_1} \cdots a_n^{e_n} \equiv kb_1^{e_1} \cdots b_n^{e_n}\,(\text{mod } m)$.

ε′ Ἔστω $a \equiv b\,(\text{mod } m)$ καὶ k ὁποιοσδήποτε. Ἡ ὑπόθεσή μας ἰσοδυναμεῖ μὲ τὸ ὅτι ὁ $\frac{b-a}{m}$ εἶναι ἀκέραιος, ὁπότε $\frac{k(b-a)}{km}$ εἶναι ἀκέραιος, δηλαδή, $km|(kb - ka)$, ποὺ σημαίνει $ka \equiv kb\,(\text{mod } km)$.
Ἔστω τώρα κοινὸς διαιρέτης τῶν a, b, m. Ἡ ἰσοτιμία $a \equiv b\,(\text{mod } m)$ ἰσοδυναμεῖ μὲ τὸ ὅτι ὁ $\frac{b-a}{m}$ εἶναι ἀκέραιος. Αὐτό, εἶναι τὸ ἴδιο μὲ τὸ νὰ ποῦμε ὅτι ὁ $\frac{\frac{b}{d} - \frac{a}{d}}{\frac{m}{d}}$ εἶναι ἀκέραιος, καὶ ὁ ἰσχυρισμὸς αὐτὸς ἰσοδυναμεῖ μὲ τὴ σχέση $\frac{a}{d} \equiv \frac{b}{d}\,(\text{mod } \frac{m}{d})$.

στ′. Ἔστω $a \equiv b\,(\text{mod } m)$ καὶ d κοινὸς διαιρέτης τῶν a, b, ὁ ὁποῖος εἶναι πρῶτος πρὸς τὸν m. Γράφομε $a = da_1, b = db_1$ καὶ ἔχομε νὰ δείξομε ὅτι $a_1 \equiv b_1\,(\text{mod } m)$. Ἀλλὰ ἡ ὑπόθεσή μας συνεπάγεται ὅτι ὁ m διαιρεῖ τὸν $b - a = d(b_1 - a_1)$, ἐνῶ $(m, d) = 1$, ὁπότε, ἀπὸ τὴν πρόταση στ′ τοῦ θεωρήματος 1.2.2 ἕπεται ὅτι $m|(b_1 - a_1)$, δηλαδή, $a_1 \equiv b_1\,(\text{mod } m)$.

ζ′. Ἡ ὑπόθεση λέει ὅτι $m|(b - a)$. Ἀλλὰ $d|m$, ἄρα $d|(b - a)$, ὁπότε $a \equiv b\,(\text{mod } d)$.

η′. Ἀπὸ τὴν ὑπόθεση, $b = a + km$ γιὰ κάποιον ἀκέραιο k, ὁπότε, ἀρκεῖ νὰ ἐφαρμόσομε τὴν πρόταση β′ τοῦ θεωρήματος 1.2.2. **ὅ.ἔ.δ.**

2.2 Συστήματα ὑπολοίπων

Ἀπὸ τὴν πρόταση-ὁρισμὸ 2.1.1 εἶναι σαφὲς ὅτι, γιὰ κάθε a ὑπάρχει ἕνας ἀκριβῶς ἀκέραιος $a_0 \in \{0, 1, \dots, m-1\}$, τέτοιος ὥστε $a \equiv a_0\,(\text{mod } m)$. Στὴν πραγματικότητα, ὁ a_0 εἶναι τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ a διὰ m. Εἴδαμε, ἐπίσης, ὅτι ἡ σχέση ἰσοτιμίας μέτρῳ m εἶναι σχέση ἰσοδυναμίας, ἄρα ἔχει νόημα νὰ μιλᾶμε γιὰ κλάσεις ἰσοδυναμίας, τὶς ὁποῖες λέμε *κλάσεις ἰσοτιμίας μέτρῳ m* ἢ *κλάσεις ἰσοτιμίας modulo m*. Ἡ κλάση ἰσοτιμίας τοῦ a μέτρῳ m συμβολίζεται $a \text{ mod } m$ καὶ εἶναι, φυσικά, ἕνα ἄπειρο σύνολο. Ἄρα, $a \equiv b\,(\text{mod } m) \Leftrightarrow a \text{ mod } m = b \text{ mod } m$. Ἄν, ὅπως παραπάνω, a_0 εἶναι τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ a διὰ m, τότε $a \text{ mod } m = a_0 \text{ mod } m$, ἄρα, οἱ κλάσεις μέτρῳ m εἶναι οἱ $0 \text{ mod } m, 1 \text{ mod } m, \dots, m - 1 \text{ mod } m$.
Παράδειγμα. Ἔστω $m = 12$. Ἡ κλάση τοῦ 45 ἀποτελεῖται ἀπὸ ὅλους (τοὺς

ἄπειρους) ἀκεραίους a, γιὰ τοὺς ὁποίους ἰσχύει $a \equiv 45 \pmod{12}$, ἄρα

$$\begin{aligned} 45 \bmod 12 =& \{\ldots, -51, -39, -27, -15, -3, 9, 21, 33, 45, 57, \ldots\} \\ =& \{45 + 12k \,:\, k \in \mathbb{Z}\}\,. \end{aligned}$$

Ἂς φαντασθοῦμε τώρα ὅτι ἀπὸ κάθε κλάση ἐπιλέγομε ἕνα, ἀκριβῶς, ἀκέραιο. Τότε σχηματίζομε ἕνα σύνολο, ἀποτελούμενο ἀπὸ m τὸ πλῆθος ἀκεραίους $a_1, \ldots, a_m$, ἀνὰ δύο ἀνισότιμους μέτρῳ m. Ἕνα τέτοιο σύνολο λέγεται *πλῆρες σύστημα ὑπολοίπων* μέτρῳ (ἢ modulo) m. Τὸ ἁπλούστερο, καὶ συνηθέστερα χρησιμοποιούμενο πλῆρες σύστημα ὑπολοίπων εἶναι τὸ $\{0, 1, \ldots, m-1\}$, ποὺ λέγεται *ἐλάχιστο μὴ ἀρνητικὸ πλῆρες σύστημα*. Ἕνα ἄλλο πλῆρες σύστημα ὑπολοίπων, ποὺ χρησιμοποιεῖται ἀρκετὰ συχνά, εἶναι τὸ

$$\{-\frac{m}{2} + 1, -\frac{m}{2} + 2, \ldots, 0, 1, \ldots, \frac{m}{2} - 1, \frac{m}{2}\}, \quad \text{ἂν ὁ } m \text{ εἶναι ἄρτιος}$$

καὶ

$$\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\}, \quad \text{ἂν ὁ } m \text{ εἶναι περιττός.}$$

Αὐτὸ λέγεται *ἀπολύτως ἐλάχιστο πλῆρες σύστημα*. Παραδείγματος χάριν, τὸ ἀπολύτως ἐλάχιστο πλῆρες σύστημα γιὰ $m = 12$ εἶναι $\{-5, -4, \ldots, 4, 5, 6\}$ καὶ γιὰ $m = 11$ εἶναι $\{-5, -4, \ldots, 4, 5\}$. Πέραν, ὅμως, αὐτῶν τῶν ξεχωριστῶν συστημάτων, ὑπάρχει μία ἄπειρη ποικιλία πλήρων συστημάτων. Λ. χ., γιὰ $m = 6$, τὸ $\{12, 4, 62, -11, 9, 83\}$ εἶναι πλῆρες σύστημα ὑπολοίπων, διότι

$$12 \equiv 0\,,\; 4 \equiv 4\,,\; 62 \equiv 2\,,\; -11 \equiv 1\,,\; 9 \equiv 3\,,\; 83 \equiv 5 \pmod{6}\,,$$

ὅπου παρατηροῦμε ὅτι τὰ δεξιὰ μέλη καλύπτουν ὅλα τὰ δυνατὰ ὑπόλοιπα 0,1,. . . 6.

Πρόταση 2.2.1 *Ἂν τὸ $\{a_1, a_2, \ldots, a_m\}$ εἶναι πλῆρες σύστημα ὑπολοίπων μέτρῳ m, ὁ b εἶναι ὁποιοσδήποτε ἀκέραιος πρῶτος πρὸς τὸν m καὶ ὁ c ὁποιοσδήποτε ἀκέραιος, τότε τὸ $\{ba_1 + c, ba_2 + c, \ldots, ba_m + c\}$ εἶναι, ἐπίσης, πλῆρες σύστημα ὑπολοίπων μέτρῳ m.*

Ἀπόδειξη Βάσει τῆς ἀσκήσεως 14, ἀρκεῖ νὰ δείξομε ὅτι οἱ ἀριθμοὶ $ba_1 + c, ba_2 + c, \ldots, ba_m + c$ εἶναι ἀνὰ δύο ἀνισότιμοι μέτρῳ m. Φυσικά, θὰ στηριχθοῦμε στὴν ὑπόθεση ὅτι οἱ ἀριθμοὶ $a_1, a_2, \ldots, a_m$ εἶναι ἀνὰ δύο ἀνισότιμοι μέτρῳ m. Πράγματι, ἂν $i \neq j$ καὶ συνέβαινε $ba_i + c \equiv ba_j + c \pmod{m}$, τότε, προσθέτοντας σ' αὐτὴ τὴν ἰσοτιμία τὴν $-c \equiv -c \pmod{m}$ θὰ παίρναμε $ba_i \equiv ba_j \pmod{m}$ καὶ κατόπιν, ἀπὸ τὴν πρόταση στ′ τοῦ θεωρήματος 2.1.2, διαιρώντας διὰ b, ποὺ εἶναι πρῶτος πρὸς τὸν m, θὰ καταλήγαμε στὴ σχέση $a_i \equiv a_j \pmod{m}$, ἡ ὁποία ἀντιφάσκει στὴν ὑπόθεση. **ὅ.ἔ.δ.**

Ἂς θεωρήσομε τώρα κάποιον a πρῶτο πρὸς m καὶ b ὁποιονδήποτε ἀριθμὸ τῆς κλάσης $a \bmod m$. Ἀπὸ τὴν πρόταση η′ τοῦ θεωρήματος 2.1.2 ἕπεται ὅτι

$(b,m) = (a,m) = 1$. Ἄρα, ἂν ἕνας ἀριθμὸς μιᾶς κλάσης μέτρῳ m εἶναι πρῶτος πρὸς m, τότε καὶ κάθε ἄλλος ἀριθμὸς αὐτῆς τῆς κλάσης εἶναι πρῶτος πρὸς m. Καταχρηστικά, λέμε ὅτι αὐτὴ ἡ κλάση εἶναι πρώτη πρὸς m. Ἂς φαντασθοῦμε τώρα ὅτι ἔχομε ἕνα πλῆρες σύστημα ὑπολοίπων μέτρῳ m καὶ ἀπὸ αὐτὸ ἐπιλέγομε ἐκείνους τοὺς ἀριθμοὺς τοῦ συστήματος, οἱ ὁποῖοι εἶναι πρῶτοι πρὸς m. Τὸ σύνολο, ποὺ λαμβάνομε μὲ αὐτὸ τὸν τρόπο λέγεται *περιορισμένο σύστημα* μέτρῳ (ἢ modulo) m. Ἂν, γιὰ παράδειγμα, $m = 10$ καὶ θεωρήσομε τὸ πλῆρες σύστημα $\{15, 11, 22, 33, -11, -12, -23, 6, 14, 100\}$ (ἐλέγξτε ὅτι εἶναι ὄντως πλῆρες σύστημα μέτρῳ 10), τότε τὸ περιορισμένο σύστημα ὑπολοίπων, ποὺ προκύπτει εἶναι $\{11, 33, -11, -23\}$, διότι αὐτοὶ καὶ μόνον οἱ ἀριθμοὶ τοῦ πλήρους συστήματος εἶναι πρῶτοι πρὸς τὸ 10. Παρατηρῆστε ὅτι, γιὰ παράδειγμα, οἱ ἀριθμοὶ 7, 17, -63, ποὺ ἀνήκουν στὴν κλάση $-23 \bmod 10$, εἶναι, ἐπίσης, πρῶτοι πρὸς τὸν 10.
Ἂν $\{a_1, \dots a_m\}$ καὶ $\{b_1, \dots, b_m\}$ εἶναι πλήρη συστήματα ὑπολοίπων, τότε κάθε a_i εἶναι ἰσότιμο μέτρῳ m μὲ ἀκριβῶς ἕνα b_j καί, ὅπως παρατηρήσαμε παραπάνω, εἶναι $(b_j, m) = 1$ ἄν, καὶ μόνο ἄν, $(a_i, m) = 1$. Συνεπῶς, ἕνα περιορισμένο σύστημα ὑπολοίπων, ἀπὸ ὁποιοδήποτε πλῆρες σύστημα κι ἂν προέρχεται, ἔχει τὸ ἴδιο πλῆθος ἀριθμῶν. Ἂν ἐπιλέξομε, λοιπόν, τὸ ἐλάχιστο μὴ ἀρνητικὸ πλῆρες σύστημα ὑπολοίπων, τότε τὸ περιορισμένο σύστημα, ποὺ προκύπτει ἀπὸ αὐτό, ἀποτελεῖται ἀπὸ ἐκείνους τοὺς ἀριθμοὺς $1, \dots, m-1$, οἱ ὁποῖοι εἶναι πρῶτοι πρὸς τὸν m.[2] Τὸ πλῆθος τους συμβολίζεται $\phi(m)$. Ἡ συνάρτηση ϕ, ποὺ σὲ κάθε $m \geq 2$ ἀντιστοιχεῖ τὸ πλῆθος $\phi(m)$ τῶν ἀκεραίων τοῦ συνόλου $\{1, \dots, m-1\}$, οἱ ὁποῖοι εἶναι πρῶτοι πρὸς τὸν m, λέγεται *συνάρτηση ϕ τοῦ Euler*. Σύμφωνα, λοιπόν, μὲ ὅσα εἴπαμε πρίν, κάθε περιορισμένο σύστημα ὑπολοίπων περιέχει $\phi(m)$ τὸ πλῆθος ἀριθμούς. Τὸ θεώρημα 2.2.3 παρέχει τύπο γιὰ τὸν ὑπολογισμὸ τοῦ $\phi(m)$ ὅταν εἶναι γνωστὴ ἡ κανονικὴ ἀνάλυση τοῦ m.

Πρόταση 2.2.2 *Ἂν $a_1, a_2, \dots a_k$ εἶναι περιορισμένο σύστημα ὑπολοίπων μέτρῳ m ($k = \phi(m)$), καὶ ὁ b εἶναι πρῶτος πρὸς m, τότε $ba_1, ba_2, \dots, ba_k$ εἶναι, ἐπίσης, περιορισμένο σύστημα ὑπολοίπων μέτρῳ m.*

Ἀπόδειξη Πρῶτα παρατηροῦμε ὅτι κάθε ἀριθμὸς ba_i εἶναι πρῶτος πρὸς τὸν m. Αὐτὸ προκύπτει ἀπὸ τὶς ὑποθέσεις $(a_i, m) = 1$ καὶ $(b, m) = 1$ καὶ τὴν πρόταση ζʹ τοῦ θεωρήματοις 1.2.2.

Βάσει τῆς ἀσκήσεως 15, μένει ν' ἀποδείξομε ὅτι οἱ ἀριθμοὶ ba_i, $i = 1, \dots, k$ εἶναι ἀνὰ δύο ἀνισότιμοι μέτρῳ m. Αὐτὸ ἰσχύει διότι, ἂν $ba_i \equiv ba_j \pmod m$ μὲ $i \neq j$, τότε, ἀπὸ την πρόταση στʹ τοῦ θεωρήματος 2.1.2 θὰ προέκυπτε $a_i \equiv a_j \pmod m$, ἄτοπο. **ὅ.ἔ.δ.**

Δίνομε τώρα τὶς βασικὲς ἰδιότητες τῆς συνάρτησης ϕ τοῦ Euler.

Θεώρημα 2.2.3 *αʹ. Ἂν $(m, n) = 1$, τότε $\phi(mn) = \phi(m)\phi(n)$.*

[2] Τὸ ἴδιο εἶναι, νὰ ποῦμε ὅτι, ἀποτελεῖται ἀπὸ τοὺς ἀριθμοὺς $1, \dots, m-1, m$, οἱ ὁποῖοι εἶναι πρῶτοι πρὸς τὸν m.

β′. Ἂν $m = p_1^{a_1} \cdots p_k^{a_k}$ εἶναι ἡ κανονικὴ ἀνάλυση τοῦ m, τότε

$$\phi(m) = m(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) = p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1 - 1) \cdots (p_k - 1)\,.$$

Προκειμένου νὰ συμπεριλάβομε στὸ πεδίο ὁρισμοῦ τῆς ϕ καὶ τὸ 1, ὁρίζομε $\phi(1) = 1$.

Ἀπόδειξη α′. Ἔστω M καὶ N περιορισμένα συστήματα ὑπολοίπων μέτρῳ m καὶ n, ἀντιστοίχως. Θεωροῦμε τὸ σύνολο

$$S = \{mx + ny \;:\; x \in N \;\; y \in M\}$$

καὶ θὰ δοῦμε κάποιες ἰδιότητες τοῦ S.
(i) Ἂν $x_1, x_2 \in N$, $y_1, y_2 \in M$ καὶ $x_1 \neq x_2$ εἴτε $y_1 \neq y_2$, τότε $mx_1 + ny_1 \not\equiv mx_2 + ny_2 \pmod{mn}$. Πραγματικά, ἂς ὑποθέσομε, δίχως βλάβη τῆς γενικότητας, ὅτι $x_1 \neq x_2$. Τότε καὶ $x_1 \not\equiv x_2 \pmod{n}$, διότι οἱ x_1, x_2 ἀνήκουν στὸ σύστημα ὑπολοίπων N. Ἂν ἴσχυε $mx_1+ny_1 \equiv mx_2+ny_2 \pmod{mn}$, τότε θὰ ἴσχυε καὶ $mx_1+ny_1 \equiv mx_2+ny_2 \pmod{n}$ (πρόταση ζ′ τοῦ θεωρήματος 2.1.2), ἄρα $mx_1 \equiv mx_2 \pmod{n}$, ἀφοῦ $ny_1 \equiv 0 \equiv ny_2 \pmod{n}$. Ἀλλὰ $(m, n) = 1$, ἄρα, διαιρώντας διὰ m, καταλήγομε στὴν $x_1 \equiv x_2 \pmod{n}$, σὲ ἀντίθεση μὲ ὅ,τι παρατηρήσαμε λίγες γραμμὲς πιὸ πάνω.
(ii) Κάθε ἀριθμὸς τοῦ S εἶναι πρῶτος πρὸς τὸν mn. Πράγματι, ἔστω $mx + ny \in S$. Εἶναι $(y, m) = 1$ καὶ $(n, m) = 1$, ἄρα, βάσει τῶν προτάσεων ε′ καὶ β′ τοῦ θεωρήματος 1.2.2, $(mx+ny, m) = (ny, m) = 1$. Ἀνάλογα, $(mx+ny, n) = 1$, ἄρα καὶ $(mx+ny, mn) = 1$.
(iii) Στὸ S τὰ x διατρέχουν $\phi(n)$ καὶ τὰ y $\phi(m)$ διαφορετικὲς τιμές, ἄρα τὸ πλῆθος τῶν ἀριθμῶν τοῦ S εἶναι $\phi(n)\phi(m)$. Ὅπως εἴδαμε στὸ (i), οἱ ἀριθμοὶ αὐτοὶ εἶναι ἀνισότιμοι μέτρῳ mn, ἐνῶ, λόγῳ τοῦ (ii) εἶναι πρῶτοι πρὸς τὸν mn, ἄρα ἀποτελοῦν ὑποσύνολο ἑνὸς περιορισμένου συστήματος ὑπολοίπων μέτρῳ mn.
(iv) Θὰ δείξομε τώρα ὅτι κάθε ἀριθμὸς πρῶτος πρὸς τὸν mn εἶναι ἰσότιμος μέτρῳ mn μὲ κάποιον ἀπὸ τοὺς ἀριθμοὺς τοῦ S. Αὐτό, σὲ συνδυασμὸ μὲ τὸ (iii) θὰ μᾶς 'πεῖ ὅτι τὸ S εἶναι ἕνα περιορισμένο σύστημα ὑπολοίπων καὶ ὄχι, ἁπλῶς, ἕνα ὑποσύνολο περιορισμένου συστήματος ὑπολοίπων. Ἔστω, λοιπόν, k πρῶτος πρὸς mn καὶ ἂς θεωρήσομε τοὺς ἀριθμοὺς $m\ell - k$, $\ell = 0, 1, \ldots, n-1$. Βάσει τῆς πρότασης 2.2.1, οἱ ἀριθμοὶ αὐτοὶ ἀποτελοῦν πλῆρες σύστημα ὑπολοίπων μέτρῳ n, ἄρα γιὰ κάποιο ℓ_0 ἰσχύει $m\ell_0 - k \equiv 0 \pmod{n}$. Αὐτὴ ἡ τελευταία σχέση μᾶς λέει ὅτι ὑπάρχει z ἔτσι ὥστε $m\ell - nz = k$, ὅπου $\ell = \ell_0$. Μὲ χρήση τῶν προτάσεων ε′ καὶ β′ τοῦ θεωρήματος 1.2.2 βλέπομε ὅτι $(\ell, n) = (m\ell, n) = (m\ell - nz, n) = (k, n) = 1$, ἄρα ὁ ℓ εἶναι ἰσότιμος μέτρῳ n μὲ κάποιο $x_0 \in N$. Ἀνάλογα, $(-z, m) = (-nz, m) = (m\ell - nz, m) = (k, m) = 1$, ἄρα ὁ $-z$ εἶναι ἰσότιμος μέτρῳ m μὲ κάποιο $y_0 \in M$. Ἔτσι ἔχομε $\ell \equiv x_0 \pmod{n}$, ἄρα (πρόταση ε′ τοῦ θεωρήματος 2.1.2) $m\ell \equiv mx_0 \pmod{mn}$ καί, ἐπίσης, $-z \equiv y_0 \pmod{m}$, ἄρα $-nz \equiv ny_0 \pmod{nm}$. Προσθέτοντας κατὰ μέλη, $m\ell - nz \equiv mx_0 + ny_0 \pmod{mn}$, δηλαδή, $k \equiv mx_0 + ny_0 \pmod{mn}$, ὅπου $mx_0 + ny_0 \in S$.

Συνοψίζοντας, καταλήγομε στὸ συμπέρασμα ὅτι, τὸ S μὲ πληθάριθμο $\phi(m)\phi(n)$ εἶναι περιορισμένο σύστημα ὑπολοίπων μέτρῳ mn. Ἀλλὰ ἕνα περιορισμένο σύστημα ὑπολοίπων μέτρῳ mn περιέχει $\phi(mn)$ ἀριθμούς. Ἄρα, $\phi(m)\phi(n) = \phi(mn)$.

β′. Προφανῶς, ἡ πρόταση α′ γενικεύεται καὶ γιὰ περισσότερους ἀπὸ δύο ἀριθμούς, ἀρκεῖ αὐτοὶ νὰ εἶναι *ἀνὰ δύο πρῶτοι μεταξύ τους*. Ὁπότε, ἂν ἔχομε τὴν κανονικὴ ἀνάλυση τοῦ m, ὅπως στὸ β′ τῆς ἐκφώνησης, τότε

$$\phi(m) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) \tag{2.1}$$

καὶ ἀρκει νὰ βροῦμε ἕνα γενικὸ τύπο γιὰ τὸ $\phi(p^a)$ ὅταν p πρῶτος καὶ $a \geq 1$. Αὐτό, ὅμως, εἶναι εὔκολο: Θέλομε νὰ ὑπολογίσομε πόσοι θετικοὶ ἀκέραιοι μικρότεροι τοῦ p^a εἶναι πρῶτοι πρὸς τὸν p^a. Εἶναι εὐκολώτερο νὰ ὑπολογίσομε πόσοι *δὲν* εἶναι, διότι, ἕνας ἀριθμὸς δὲν εἶναι πρῶτος πρὸς τὸν p^a ἄν, καὶ μόνο ἄν, εἶναι πολλαπλάσιο τοῦ p. Τὰ θετικὰ πολλαπλάσια τοῦ p τὰ μικρότερα τοῦ p^a εἶναι οἱ ἀριθμοὶ $p, 2p, 3p, \ldots, (p^{a-1} - 1)p$, ὁπότε, τὸ πλῆθος τους εἶναι $p^{a-1} - 1$. Ἄρα, τὸ πλῆθος τῶν θετικῶν ἀκεραίων, ποὺ εἶναι μικρότεροι τοῦ p^a καὶ πρῶτοι πρὸς τὸν p^a εἶναι $(p^a - 1) - (p^{a-1} - 1) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$. Ἔτσι, $\phi(p^a) = p^a(1 - \frac{1}{p})$ καὶ τώρα ἀπὸ τὴν (2.1), ἔχομε πολὺ εὔκολα τοὺς ἀποδεικτέους τύπους. **ὅ.ἔ.δ.**

Θεώρημα 2.2.4 *α′.* (Euler) *Ἂν $(a, m) = 1$, τότε $a^{\phi(m)} \equiv 1 \pmod{m}$.*
β′. (Fermat) *Ἂν ὁ p εἶναι πρῶτος καὶ $(a, p) = 1$, τότε $a^{p-1} \equiv 1 \pmod{p}$.*
Ἰσοδύναμη διατύπωση: *Ἂν ὁ p εἶναι πρῶτος, τότε $a^p \equiv a \pmod{p}$ γιὰ κάθε a.*
γ′. Ἂν $(a, m) = 1$ καὶ $\nu \equiv \mu \pmod{\phi(m)}$, τότε $a^\nu \equiv a^\mu \pmod{m}$.

Ἀπόδειξη α′. Ἔστω $k = \phi(m)$ καὶ $\{a_1, \ldots, a_k\}$ ἕνα περιορισμένο σύστημα ὑπολοίπων μέτρῳ m. Ἀπὸ τὸ θεώρημα 2.2.2, τὸ $\{aa_1, \ldots, aa_k\}$ εἶναι, ἐπίσης, περιορισμένο σύστημα ὑπολοίπων μέτρῳ m, ἄρα, καθένας ἀπὸ τοὺς ἀριθμοὺς τοῦ δευτέρου συστήματος ὑπολοίπων εἶναι ἰσότιμος μέτρῳ m μὲ ἕναν ἀκριβῶς ἀπὸ τοὺς ἀριθμοὺς τοῦ πρώτου συστήματος, ὁπότε $(aa_1) \cdots (aa_k) \equiv a_1 \cdots a_k \pmod{m}$, δηλαδή, $a^k(a_1 \cdots a_k) \equiv a_1 \cdots a_k \pmod{m}$. Ἀλλὰ $(a_1 \cdots a_k, m) = 1$, διότι καθένας ἀπὸ τοὺς a_i εἶναι πρῶτος πρὸς m (βλ.ζ′ τοῦ θεωρήματος 1.2.2), ἄρα, διαιρώντας καὶ τὰ δύο μέλη διὰ $a_1 \cdots a_k$ (βλ. στ′ τοῦ θεωρήματος 2.1.2), καταλήγομε στὴν ἀποδεικτέα $a^k \equiv 1 \pmod{m}$.
β′. Ἐφαρμόζοντας τὸ α′ μέρος γιὰ $m = p$ καὶ παρατηρώντας ὅτι, προφανῶς, $\phi(p) = p - 1$, καταλήγομε στὴν ἀποδεικτέα σχέση.
γ′. Ὑποθέτομε, δίχως βλάβη τῆς γενικότητας, ὅτι $\nu \geq \mu$. Λόγῳ τῆς $\nu \equiv \mu \pmod{\phi(m)}$, συμπεραίνομε ὅτι ὑπάρχει θετικὸς ἀκέραιος ℓ, τέτοιος ὥστε $\nu = \mu + \ell\phi(m)$. Ἄρα, λόγῳ καὶ τοῦ θεωρήματος τοῦ Euler,

$$a^\nu = a^\mu (a^{(\phi(m)})^\ell \equiv a^\mu \cdot 1^\ell \equiv a^\mu \pmod{m}.$$

ὅ.ἔ.δ.

Μία συνέπεια τοῦ παραπάνω θεωρήματος εἶναι ὅτι, ἂν $m \geq 2$ καὶ $(a, m) = 1$, τότε τὸ σύνολο $E = \{k > 0 : a^k \equiv 1 \pmod{m}\}$ εἶναι μὴ κενό, ἀφοῦ $\phi(m) \in E$. Συνεπῶς, ἔχει νόημα νὰ θεωρήσομε τὸν ἐλάχιστο ἀριθμὸ τοῦ E, ἔστω $r = \min E$. Τὸ r λέγεται *τάξη τοῦ a* mod m καὶ συμβολίζεται $\mathrm{ord}_m(a)$. Λεπτομερέστερη ἀνάπτυξη αὐτῆς τῆς ἔννοιας, καθὼς καὶ πολλὲς ἐφαρμογές της, θὰ δοῦμε στὸ Κεφάλαιο 5. Ἐδῶ θὰ ἀρκεστοῦμε στὴν ἑξῆς πρόταση.

Πρόταση 2.2.5 *Ἔστω* $m > 2$, $(a, m) = 1$ *καὶ* r *ἡ τάξη τοῦ* $a \bmod m$. *Τότε* $r \mid \phi(m)$.

Ἀπόδειξη Ἔστω ἡ εὐκλείδεια διαίρεση τοῦ $\phi(m)$ διὰ r: $\phi(m) = qr + v$, ὅπου $0 \le v < r$. Ἀρκεῖ νὰ δείξομε ὅτι $v = 0$. Ἂς ὑποθέσομε ὅτι $v > 0$. Τότε, $0 < k < v$ καὶ $a^v \equiv 1 \pmod{m}$, διότι

$$1 \equiv a^{\phi(m)} = a^{qr}a^v = (a^r)^q a^v \equiv 1^q a^v = a^v \pmod{m}.$$

Ἔτσι, ὅμως, ἤλθαμε σὲ ἀντίφαση μὲ τὸ γεγονὸς ὅτι r εἶναι ὁ ἐλάχιστος θετικὸς ἐκθέτης k, γιὰ τὸν ὁποῖον $a^k \equiv 1 \pmod{m}$. Συνεπῶς, $v = 0$, ὁπότε $r \mid \phi(m)$. **ὅ.ἔ.δ.**

Παράδειγμα. Νὰ ὑπολογισθεῖ ἡ τάξη τοῦ $5 \bmod 42$.
Λύση. Κατ' ἀρχάς, εἶναι $(5, 42) = 1$, ἄρα ἔχει νόημα ἡ ἀναζήτηση τῆς τάξης τοῦ $5 \bmod 42$. Εἶναι $\phi(42) = \phi(2 \cdot 3 \cdot 7) = 42(1 - 1/2)(1 - 1/3)(1 - 1/7) = 12$, ἄρα ἡ ζητούμενη τάξη εἶναι διαιρέτης τοῦ 12, δηλαδή, ἕνας ἐκ τῶν ἀριθμῶν 1,2,3,4,6,12. Εἶναι 5^1, $5^2 \not\equiv 1 \pmod{42}$, ἐνῶ $5^3 = 125 \equiv -1 \pmod{42}$. Συνεπῶς $5^4 \equiv -5 \not\equiv 1 \pmod{42}$ καὶ $5^6 \equiv (-1)^2 \equiv 1 \pmod{42}$. Συνεπῶς, ὁ ζητούμενος ἐλάχιστος θετικὸς k, γιὰ τὸν ὁποῖον $5^k \equiv 1 \pmod{42}$ εἶναι ὁ 6, δηλαδή, $\mathrm{ord}_{42}(5) = 6$.

Μία ἐξαιρετικὰ χρήσιμη, ἐφαρμογὴ τοῦ θεωρήματος 2.2.4 εἶναι ὁ ὑπολογισμὸς τοῦ ὑπολοίπου μιᾶς διαίρεσης μεγάλων ἀριθμῶν, ὅπως φαίνεται ἀπὸ τὸ παρακάτω παράδειγμα. Ἡ τετριμμένη παρατήρηση εἶναι ὅτι, ἂν $a \equiv r \pmod{m}$, καὶ $0 \le r < m$, τότε, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ a διὰ m εἶναι r. Ἡ παρατήρηση αὐτὴ εἶναι προφανὴς συνδυασμὸς τῆς πρότασης 2.1.1 καὶ τοῦ γεγονότος ὅτι τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ r διὰ m εἶναι r.

Παράδειγμα ὑπολογισμοῦ τοῦ ὑπολοίπου διαιρέσεως. *Νὰ ὑπολογισθεῖ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ* 174379^{32971} *διὰ* 57624.
Ἀρκεῖ νὰ ὑπολογίσομε μὴ ἀρνητικὸ $r < 57624$, τέτοιο ὥστε $174379^{32971} \equiv r \pmod{57624}$. Πρῶτα-πρῶτα, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 174379 διὰ 57624 εἶναι 1507, ἄρα, $174379 \equiv 1507 \pmod{57624}$ καί, συνεπῶς, $174379^{32971} \equiv 1507^{32971} \pmod{57624}$. Πρὶν προχωρήσομε ὑπολογίζομε ὅτι $(1507, 57624) = 1$, ἄρα μποροῦμε νὰ ἐφαρμόσομε τὸ θεώρημα τοῦ Euler μὲ $a = 1507$ καὶ $m = 57624$.
Μὲ τὴ βοήθεια τοῦ θεωρήματος 2.1, ὑπολογίζομε

$$\phi(57624) = \phi(2^3 \cdot 3 \cdot 7^4) = 57264(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = 16464\,,$$

ἐνῶ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 32971 διὰ 16464 εἶναι 43. Ἄρα, $32971 \equiv 43 \pmod{16464}$, ὁπότε, ἀπὸ τὸ γ′ τοῦ θεωρήματος 2.2.4, $1507^{32971} \equiv 1507^{43} \pmod{57264}$. Μέχρι στιγμῆς, λοιπόν, $174379^{32971} \equiv 1507^{43} \pmod{57624}$.
Ὁ ὑπολογισμὸς τοῦ 1507^{43} μέτρῳ 57624 μπορεῖ νὰ γίνει μὲ διάφορους συνδυασμούς. Ἕνας τρόπος, γιὰ παράδειγμα, φαίνεται παρακάτω. Οἱ ὑπολογισμοὶ ἔχουν γίνει μὲ κομπιουτεράκι τσέπης. Σὲ κάθε γραμμή, ἡ πιὸ δεξιὰ ἰσοτιμία mod 57624 ὀφείλεται σὲ ὑπόλοιπο διαιρέσεως, δηλαδή, στὴν πρώτη γραμμή, γιὰ παράδειγμα, εἶναι $2271049 \equiv 23713 \pmod{57624}$ διότι τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 2271049

διὰ 57624 εἶναι 23713. Ἀνάλογα καὶ στὶς ἄλλες γραμμές.

$$
\begin{array}{llllllll}
 & & 1507^2 & = & 2271049 & \equiv & 23713 & \pmod{57624} \\
1507^3 & \equiv & 23713 \cdot 1507 & = & 35735491 & \equiv & 8611 & \pmod{57624} \\
1507^6 & \equiv & 8611^2 & = & 74149321 & \equiv & 44857 & \pmod{57624} \\
1507^9 & \equiv & 44857 \cdot 8611 & = & 386263627 & \equiv & 9955 & \pmod{57624} \\
1507^{18} & \equiv & 9955^2 & = & 99102025 & \equiv & 46369 & \pmod{57624} \\
1507^{21} & \equiv & 46369 \cdot 8611 & = & 399283459 & \equiv & 6763 & \pmod{57624} \\
1507^{42} & \equiv & 6763^2 & = & 45738169 & \equiv & 42337 & \pmod{57624} \\
1507^{43} & \equiv & 42337 \cdot 1507 & = & 63801859 & \equiv & 12091 & \pmod{57624}
\end{array}
$$

Συνεπῶς, τὸ ζητούμενο ὑπόλοιπο εἶναι 12091.

2.3 Ὕψωση σὲ δύναμη

Τὸ παράδειγμα ὑπολογισμοῦ στὸ τέλος τῆς προηγουμένης παραγράφου μπορεῖ νὰ γίνει πιὸ μεθοδικά, ἂν γράψομε τὸν ἐκθέτη 43 ὡς δυαδικὸ ἀριθμό $b_0 + 2b_1 + 2^2 b_2 + 2^3 b_3 \cdots$, ὅπου κάθε b_i εἶναι 0 ἢ 1. Τὰ $b_0, b_1, b_2, \ldots$ εἶναι τὰ δυαδικὰ ψηφία (bits) τοῦ ἀριθμοῦ. Γιὰ παράδειγμα, τὰ δυαδικὰ ψηφία τοῦ 43 ὑπολογίζονται ὡς ἑξῆς: Ἀφοῦ ὁ 43 εἶναι περιττός, ἕπεται ὅτι $b_0 = 1$. Τώρα, $43 = 1 + 2b_1 + 2^2 b_2 + 2^3 b_3 + \cdots$, ἄρα $21 = \frac{43-1}{2} = b_1 + 2b_2 + 2^2 b_3 + \cdots$, ὁπότε, ἀφοῦ ὁ 21 εἶναι περιττός, $b_1 = 1$. Μετά, $10 = \frac{21-1}{2} = b_2 + 2b_3 + \cdots$, ἄρα $b_2 = 0$, ἀφοῦ ὁ 10 εἶναι ἄρτιος. Συνεχίζομε: $5 = \frac{10}{2} = b_3 + 2b_4 + \cdots$, ἄρα $b_3 = 1$. Τελικά, βρίσκομε ὅτι τὰ δυαδικὰ ψηφία τοῦ 43 εἶναι $(b_0, \ldots, b_5) = (1, 1, 0, 1, 0, 1)$ καὶ γράφομε $43 = (101011)$. Πιὸ γενικά, ἂν $b_0, b_1, \ldots, b_k$ εἶναι τὰ δυαδικὰ ψηφία κάποιου θετικοῦ ἀκεραίου N, γράφομε $N = (b_k \ldots b_1 b_0)$. Ὁ συμβολισμὸς αὐτὸς χρησιμοποιεῖται *μόνο σ' αὐτὴ τὴν παράγραφο*.

Τὸ παραπάνω παράδειγμα μᾶς ὑποδεικνύει σαφῶς τὸν παρακάτω ἀλγόριθμο. Κάνομε χρήση τοῦ συμβολισμοῦ $[a]_m$ γιὰ νὰ δηλώσομε τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ a διὰ τοῦ $m > 1$. Ὁπότε, ὁ συμβολισμὸς στὸν ἀλγόριθμο $[a]_2$ σημαίνει 0, ἂν ὁ a εἶναι ἄρτιος καὶ 1, ἂν ὁ a εἶναι περιττός. Ἐπίσης, παρατηρῆστε ὅτι, ἂν ὁ B εἶναι θετικὸς ἀκέραιος, τότε

$$
\left[\frac{B}{2}\right] = \begin{cases} \frac{B}{2} & \text{ἂν } B \text{ ἄρτιος} \\ \frac{B-1}{2} & \text{ἂν } B \text{ περιττός} \end{cases}
$$

Αλγοριθμος Μετατροπης σε Δυαδικο.
Εἰσάγεται θετικὸς ἀκέραιος N.
Ἐξάγονται τὰ δυαδικὰ ψηφία b_I, $I = 0, 1, 2, \ldots$ τοῦ N.
Γίνεται χρήση τῶν βοηθητικῶν μεταβλητῶν I καὶ B.

$I \leftarrow 0 \quad : \quad B \leftarrow N$
ενοσω $B > 0$ επαναλαβε
$b_I = [B]_2 \quad : \quad B \leftarrow \left[\frac{B}{2}\right] \quad : \quad I \leftarrow I + 1$

ΤΕΛΟΣ ΕΠΑΝΑΛΗΨΗΣ

ΤΕΛΟΣ

Ὁ παραπάνω ἀλγόριθμος περιέχεται, μᾶλλον κρυμμένος, στὸν ἀλγόριθμο ὕψωσης σὲ δύναμη, ποὺ θὰ περιγράψομε παρακάτω καὶ τοῦ ὁποίου ἡ ἀναλυτικὴ περιγραφὴ εἶναι ἡ ἑξῆς:

Ἔστω ὅτι θέλομε νὰ ὑπολογίσομε τὸν a^N μέτρῳ m, δηλαδή, μὲ τὸν συμβολισμὸ στὴν ἀρχὴ αὐτῆς τῆς παραγράφου, θέλομε νὰ ὑπολογίσομε τὸν $[a^N]_m$. Ἔστω $N = (b_n \dots b_1 b_0)$· τὰ δυαδικὰ ψηφία b_i ὑπολογίζονται διαδοχικὰ μὲ τὸν *ἀλγόριθμο μετατροπῆς σὲ δυαδικὴ μορφή*. Ἐπίσης, βοηθητικά, ὑπολογίζονται, σὲ κάθε βῆμα k, ἀριθμοὶ D_{k+1} καὶ A_k.

Ἀρχικὸ βῆμα 0: Ὑπολόγισε

$$b_0\,, \quad D_0 = [a^{2^0}]_m = [a]_m\,, \quad A_0 = [a^{b_0}]_m = \begin{cases} [a]_m & \text{ἂν } b_0 = 1 \\ 1 & \text{ἂν } b_0 = 0 \end{cases}$$

Βῆμα k: Ἔχεις ἤδη ὑπολογίσει

$$b_0, \dots, b_k\,, \qquad D_k = [a^{2^k}]_m\,, \quad A_k = [a^{(b_k \dots b_1 b_0)}]_m$$

Ἂν τὸ b_k εἶναι τὸ τελευταῖο δυαδικὸ ψηφίο τοῦ N, τότε $A_k = [a^N]_m$ -ΤΕΛΟΣ. Διαφορετικά,

Βῆμα $k+1$: Ὑπολόγισε

$$b_{k+1}\,,\ D_{k+1} = [a^{2^{k+1}}]_m = [D_k^2]_m\,,\ A_{k+1} = [a^{(b_{k+1} b_k \dots b_1 b_0)}]_m = \begin{cases} [D_{k+1} A_k]_m & \text{ἂν } b_{k+1} = 1 \\ A_k & \text{ἂν } b_{k+1} = 0 \end{cases}$$

Θὰ δοῦμε τώρα πόσοι πολλαπλασιασμοὶ ἀπαιτοῦνται μέχρι νὰ τελειώσει ἡ παραπάνω διαδικασία. Κατ' ἀρχάς, λέγοντας «πολλαπλασιασμός» τῶν a, b, γιὰ παράδειγμα, ἐννοοῦμε «πολλαπλασιασμὸς μέτρῳ m» τῶν a καὶ b, δηλαδή, πρόκειται γιὰ τὸν ὑπολογισμὸ $[\,[a]_m [b]_m\,]_m$. Ἐπειδὴ $0 \le [a]_m, [b]_m < m$, ἀπαιτεῖται ἡ εὕρεση τοῦ ὑπολοίπου τῆς διαίρεσης ἑνὸς μὴ ἀρνητικοῦ ἀκεραίου, μικρότερου τοῦ m^2, διὰ m. Αὐτὸς ὁ ὑπολογισμὸς δὲν κοστίζει πολύ· μπορεῖ νὰ γίνει μὲ στοιχειώδεις πράξεις, ποὺ τὸ πλῆθος τους φράσσεται ἀπὸ μία σταθερὰ ἐπὶ $(\log m)^{1.585}$. Τὸ ζήτημα αὐτὸ εἶναι πέραν τοῦ σκοποῦ αὐτῶν τῶν σημειώσεων. Πάντως, αὐτό, ποὺ πρέπει νὰ κρατήσει κανείς, εἶναι ὅτι τὸ «κόστος» τοῦ πολλαπλασιασμοῦ μέτρῳ m δὲν μᾶς προβληματίζει περισσότερο ἀπὸ τὸ κόστος ἑνὸς συνήθους πολλαπαλσιασμοῦ θετικῶν ἀκεραίων μικρότερων τοῦ m.

Ἐπανερχόμενοι στὸν ἀλγόριθμό μας, παρατηροῦμε ὅτι, στὸ ἀρχικὸ βῆμα δὲν κάνομε πολλαπαλσιασμὸ ἢ ὕψωση σὲ δύναμη, ἐνῶ τὸ πέρασμα ἀπὸ τὸ βῆμα k στὸ βῆμα $k+1$ ἀπαιτεῖ μία ὕψωση στὸ τετράγωνο καί, τὸ πολύ, ἕνα πολλαπλασιασμό, δηλαδή, δύο, τὸ πολύ, πολλαπλασιασμούς. Ἄρα, ἂν $N = (b_n \dots b_1 b_0)$, τότε ἡ παραπάνω διαδικασία ἀπαιτεῖ $2n$, τὸ πολύ, πολλαπλασιασμούς. Ὅμως, $N \ge 2^n$, ἄρα $n \le \frac{\log N}{\log 2}$ καί, συνεπῶς, Γιὰ τὸν ὑπολογισμὸ τοῦ $a^N \pmod{m}$ ἀπαιτοῦνται, τὸ πολύ, $\left[2\frac{\log N}{\log 2}\right]$ πολλαπλασιασμοί.

Ἡ παραπάνω διαδικασία συμπυκνώνεται στὸν παρακάτω κομψὸ ἀλγόριθμο.

Αλγοριθμος Υψωσης σε Δυναμη.
Εἰσάγονται ἀκέραιοι $m > 1$, $a \neq 0$, $N \geq 1$.
Ἐξάγεται $[a^N]_m$, δηλαδή, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ a^N διὰ m.
Γίνεται χρήση τῶν βοηθητικῶν μεταβλητῶν A, B καὶ D.

Ἀρχικὸ βῆμα: $A \leftarrow 1$, $D \leftarrow a$, $B \leftarrow N$.
ΕΝΟΣΩ $B > 0$ ΕΠΑΝΑΛΑΒΕ
ΑΝ B περιττός, $A \leftarrow A \cdot D$ ΤΕΛΟΣ ΑΝ
$D \leftarrow D^2$, $B \leftarrow \lfloor B/2 \rfloor$.
ΤΕΛΟΣ ΕΠΑΝΑΛΗΨΗΣ
Τύπωσε A
ΤΕΛΟΣ

Μὲ τὸν ἀλγόριθμο αὐτόν, ἡ διαδικασία ὑπολογισμοῦ τῆς δύναμης a^{43}, ἡ ὁποία ἔγινε ἀναλυτικὰ στὴν ἀρχὴ αὐτοῦ τοῦ ἐδαφίου, 'κωδικοποιεῖται' στὸν παρακάτω πίνακα:

A	D	B
1	a	43
a	a^2	21
a^3	a^4	10
a^3	a^8	5
a^{11}	a^{16}	2
a^{11}	a^{32}	1
a^{43}	a^{64}	0

2.4 Ἡ κρυπτογραφικὴ μέθοδος RSA

Θὰ δώσομε τὴ βασικὴ ἰδέα τῆς μεθόδου RSA, ποὺ ἐπινοήθηκε κατὰ τὰ τέλη τῆς δεκαετίας τοῦ '70 ἀπὸ τοὺς Rivest, Shamir, Adleman[3]. Διάφορες τεχνικὲς λεπτομέρειες σχετικὲς μὲ τὴν ἐφαρμογὴ τῆς μεθόδου στὴν πράξη δὲν θὰ μᾶς ἀπασχολήσουν ἐδῶ.

Φανταζόμαστε ὅτι ἕνα μήνυμα εἶναι μία πεπερασμένη διαδοχὴ ἀκεραίων ἀριθμῶν. Γιὰ παράδειγμα, ἂς ἀντιστοιχίσομε στὸ Α τὸν ἀριθμὸ 01, στὸ Β τὸ 02,. . . , στὸ Ω τὸ 24 καὶ στὸ «κενὸ» τὸ 25 καὶ ἂς ἑνώνομε ἀνὰ δύο τὰ γράμματα,

[3] Ἐξ οὗ καὶ ἡ ὀνομασία RSA

ὥστε νὰ σχηματίζουν 4ψήφιους ἀκεραίους. Ἔτσι, τὸ μήνυμα[4]

ΠΟΛΕΜΟΣ ΠΑΤΗΡ ΠΑΝΤΩΝ

μετατρέπεται στὸ ἑξῆς διάνυσμα 4ψηφίων ἀκεραίων

$$\mu = (1615, 1105, 1215, 1825, 1601, 1907, 1725, 1601, 1319, 2413)\ ,$$

ὅπου τὸ 1615 προέρχεται ἀπὸ τὸ ΠΟ, τὸ 1105 ἀπὸ τὸ ΛΕ, κ.ὅ.κ. Τὸ 1825 προέρχεται ἀπὸ τὸ Σ τοῦ «πόλεμος» (τὸ Σ ἀντιστοιχεῖ στὸ 18) καὶ τὸ κενὸ (ἀντιστοιχεῖ στὸ 25) μεταξὺ τῶν λέξεων «πόλεμος» καὶ «πατήρ».

Κάθε ἕνας, ποὺ ἐπιθυμεῖ νὰ στέλνει καὶ νὰ λαμβάνει μηνύματα, ἂς ποῦμε ἡ **Α**ΓΝΗ, ἐπιλέγει καὶ δημοσιοποιεῖ τὸ *δημόσιο κλειδί* της (n, e). Ἐδῶ, $n = pq$, ὅπου $p \neq q$ εἶναι πρῶτοι, μεγαλύτεροι ἀπὸ τὸν ἀριθμὸ 2525 (= ἡ μεγαλύτερη δυνατὴ 4ψήφια συνιστώσα ἑνὸς μηνύματος μ) καὶ e εἶναι ἕνας θετικὸς ἀκέραιος πρῶτος πρὸς τὸν $\phi(n) = (p-1)(q-1)$. Οἱ πρῶτοι p, q εἶναι γνωστοὶ μόνο στὴν Α.

Κάποια στιγμή, ὁ **Β**ΙΚΤΩΡ ἀποφασίζει νὰ στείλει στὴν Α ἕνα μήνυμα μ. Βρίσκει σὲ κάποιο «δημόσιο κατάλογο» τὸ κλειδὶ (n, e) τῆς Α, καὶ ἐνεργεῖ ὡς ἑξῆς: Γιὰ κάθε συνιστώσα a τοῦ ἀριθμοποιημένου μηνύματός του μ ὑπολογίζει τὸν ἐλάχιστο θετικὸ ἀριθμὸ τῆς κλάσης $a^e \bmod n$. Μετατρέπει ἔτσι τὸ διάνυσμα μ σ' ἕνα νέο διάνυσμα, μὲ τὸ ἴδιο πλῆθος συνιστωσῶν, ἀλλὰ πολὺ διαφορετικὲς συνιστῶσες ἀπὸ τὶς ἀρχικές.

Γιὰ παράδειγμα, ἔστω ὅτι ὁ Β βρίσκει στὸν δημόσιο κατάλογο ὅτι τὸ κλειδὶ τῆς Α εἶναι $(n, e) = (49144364409017, 1365911)$. Γιὰ κάθε 4ψήφια συνιστώσα a τοῦ μηνύματός του, ὁ Β ὑπολογίζει $a^{1365911} \bmod 49144364409017$. Ἔτσι, τὸ μήνυμα «Πόλεμος πατὴρ πάντων» μετατρέπεται ὡς ἑξῆς. Οἱ ἰσοτιμίες ἐννοοῦνται mod 49144364409017 :

$$\begin{aligned}
1615^{1365911} &\equiv 30709871603611\\
1105^{1365911} &\equiv 41273825308431\\
1215^{1365911} &\equiv 9164816839987\\
1825^{1365911} &\equiv 12180136144268\\
1601^{1365911} &\equiv 14492511666169\\
1907^{1365911} &\equiv 47865660368437\\
1725^{1365911} &\equiv 37381475485785\\
1601^{1365911} &\equiv 41273825308431\\
1319^{1365911} &\equiv 42843960910675\\
2413^{1365911} &\equiv 26456721815013
\end{aligned}$$

Ἔτσι, ὁ Β θὰ στείλει στὴν Α τὸ διάνυσμα μὲ συνιστῶσες τὰ δεξιὰ μέλη τῶν παραπάνω 10 ἰσοτιμιῶν. Ἡ Α κατασκευάζει τὸ «ἀντικλείδι» d τοῦ κλειδιοῦ της

[4] Ὀφειλόμενο στὸν Ἡράκλειτο.

(n, e), ὡς ἑξῆς. Ἐπειδὴ γνωρίζει ὅτι ἡ ἀνάλυση τοῦ n σὲ πρώτους παράγοντες εἶναι $3295321 \cdot 14913377$, μπορεῖ νὰ ὑπολογίσει ὅτι $\phi(n) = (3295321 - 1) \cdot (14913377 - 1) = 49144346200320$. Εἶναι, ἀπὸ ἐπιλογὴ τῆς A, $(e, \phi(n)) = 1$, ὁπότε τὸ β′ τοῦ θεωρήματος 1.2.1, ὑπάρχουν d, y, ἔτσι ὥστε $de + y\phi(n) = 1$, ἄρα $de \equiv 1 \pmod{\phi(n)}$. Μποροῦμε, μάλιστα, νὰ ὑποθέσομε ὅτι $1 \le d < \phi(n)$, ἀντικαθιστώντας τὸν d ἀπὸ τὸ ὑπόλοιπο τῆς διαιρέσεώς του διὰ $\phi(n)$, ἂν χρειασθεῖ. Ὁ πρακτικὸς ὑπολογισμὸς τοῦ d μπορεῖ νὰ γίνει μέσῳ τῆς ἀκολουθίας s_i τοῦ θεωρήματος 1.2.3, κατ' ἀναλογίαν μὲ τὸ παράδειγμα ἐκείνου τοῦ θεωρήματος καὶ τὸ πλῆθος τῶν ἀπαιτουμένων βημάτων εἶναι, τὸ πολύ, τῆς τάξεως τοῦ $\log_2 n$.

Αὐτὸς ὁ ἀριθμὸς d, ποὺ στὸ συγκεκριμένο παράδειγμα ὑπολογίζεται $d = 12848342058791$, εἶναι τὸ ἀντικλείδι τοῦ κλειδιοῦ (n, e) τῆς A. Πράγματι, ἂν γιὰ μία συνιστώσα a τοῦ καθαροῦ (μὴ κρυπτογραφημένου) μηνύματος τοῦ B ἰσχύει $a^e \equiv b \pmod{n}$ (π.χ., γιὰ $a = 1615$ εἶναι $b = 30709871603611$), τότε, κάνοντας χρήση καὶ τοῦ γ′ τῆς πρότασης 2.2.4, ἔχομε $b^d \equiv a^{ed} \equiv a \pmod{n}$, ἄρα, μὲ τὸν ὑπολογισμὸ $b^d \bmod n$ ἡ A βρίσκει τὸν ἀρχικὸ 4ψήφιο ἀριθμὸ a. Ἔτσι, ὑπολογίζει (βλ. τὴν παραπάνω λίστα ἰσοτιμιῶν)

$$30709871603611^d \equiv 1615\,, \quad 41273825308431^d \equiv 1105\,, \ldots$$

καὶ βρίσκει τὸ καθαρὸ μήνυμα $\mu = (1615, 1105, \ldots, 2413)$. Ὕστερα, χωρίζοντάς το σὲ διψήφια τμήματα 16,15,11,05,... καὶ ἀντιστοιχώντας τὰ γράμματα Π,Ο,Λ,Ε,..., διαβάζει τὸ μήνυμα τοῦ B.

Γιατὶ κανεὶς ἄλλος, πλὴν τῆς A, δὲν μπορεῖ νὰ ἀποκρυπτογραφήσει τὸ μήνυμα, οὔτε κἂν ὁ ἴδιος ὁ B, ἂν τὸ ξεχάσει; Διότι, γιὰ νὰ ὑπολογίσει κανεὶς τὸ ἀντικλείδι d, πρέπει νὰ μπορεῖ νὰ ὑπολογίσει τὸ $\phi(n)$ καὶ γιὰ τὸν σκοπὸ αὐτὸ δὲν ξέρομε, μέχρι σήμερα, κανένα ἄλλο τρόπο, παρὰ μόνο μέσῳ τῆς παραγοντοποίησης τοῦ n. Στὴν πράξη, ὁ n εἶναι γινόμενο δύο τυχαίων πρώτων[5], ποὺ καθένας μπορεῖ νὰ ἔχει, ἂς ποῦμε, 150 ψηφία (σὲ δεκαδικὸ σύστημα ἀρίθμησης). Κανεὶς μέχρι σήμερα δὲν μπορεῖ νὰ ἀναλύσει σὲ γινόμενο πρώτων ἕνα τέτοιον ἀριθμὸ n, δίχως νὰ ξοδέψει τρεῖς, ἢ καὶ περισσότερους, αἰῶνες ὑπολογισμοῦ μὲ ἰσχυροὺς ὑπολογιστές!

2.5 Ἀσκήσεις τοῦ κεφαλαίου 2

Στὶς ἑπόμενες ἀσκήσεις, ὅπου γίνεται λόγος γιὰ τὰ ψηφία ἑνὸς ἀριθμοῦ στὸ δεκαδικὸ σύστημα ἀρίθμησης, νὰ ἔχετε ὑπ' ὄψει τὰ ἑξῆς: Ἂν τὰ ψηφία τῶν μονάδων, δεκάδων, κλπ τοῦ ἀριθμοῦ εἶναι $a_0, a_1, \ldots, a_n$, τότε ὁ ἀριθμὸς ἰσοῦται μὲ $a_0 + 10a_1 + \cdots 10^n a_n$.

1. Ἀποδεῖξτε ὅτι, γιὰ x περιττό, $x^2 \equiv 1 \pmod{4}$ καὶ $x^2 \equiv 1 \pmod{8}$. Ἐπίσης, γιὰ y ἄρτιο, $y^2 \equiv 0 \pmod{4}$, ἐνῶ μέτρῳ 8, $y^2 \equiv 0 \pmod{8}$ ἢ $y^2 \equiv 4 \pmod{8}$.

[5] Ἡ ἔννοια «τυχαῖος πρῶτος» δὲν εἶναι καὶ τόσο ἁπλῆ!

2. Μὲ τὴ βοήθεια τῆς ἄσκησης 1 ἀποδεῖξτε ὅτι μία σχέση τῆς μορφῆς $x^2+y^2=z^2$ εἶναι ἀδύνατη ἂν οἱ x, y εἶναι καὶ οἱ δύο περιττοί.

3. Μὲ τὴ βοήθεια τῆς ἄσκησης 1 ἀποδεῖξτε ὅτι μία σχέση τῆς μορφῆς $x^2+3y^2=z^4$ μὲ τοὺς x, y ὄχι καὶ τοὺς δύο ἄρτιους, συνεπάγεται ὅτι ὁ x εἶναι περιττὸς καὶ ὁ y εἶναι διαιρετὸς διὰ 4.

4. Μὲ τὴ βοήθεια τῆς ἄσκησης 1 ἀποδεῖξτε τὸ ἑξῆς: Ἂν ὁ *περιττὸς* πρῶτος ἀριθμὸς p γράφεται ὡς ἄθροισμα δύο (μὴ μηδενικῶν) τετραγώνων (π. χ. $29=5^2+2^2$), τότε $p\equiv 1 \pmod 4$. Ἄρα, κανεὶς πρῶτος τῆς μορφῆς $4k+3$ δὲν μπορεῖ νὰ γραφεῖ ὡς ἄθροισμα δύο τετραγώνων.

5. Ἀποδεῖξτε ὅτι, γιὰ κάθε x, ποὺ δὲν διαιρεῖται διὰ 3, εἶναι $x^2\equiv 1 \pmod 3$. Μὲ τὴ βοήθεια αὐτοῦ ἀποδεῖξτε ὅτι, ἂν γιὰ τὸν πρῶτο p ὑπάρχουν μὴ μηδενικοὶ x, y, τέτοιοι ὥστε $p=x^2+3y^2$, τότε $p\equiv 1 \pmod 6$.

6. Ἀποδεῖξτε ὅτι, γιὰ κάθε x εἶναι $x^3\equiv 0$ ἢ $\pm 1 \pmod 9$. Μὲ τὴ βοήθεια αὐτοῦ, ἀποδεῖξτε ὅτι ἡ διοφαντικὴ ἐξίσωση $x^3+2y^3=5z^3$ εἶναι ἀδύνατη γιὰ μὴ μηδενικοὺς ἀκεραίους x, y, z μὲ $(x, y)=1$.
   Ὑπόδειξη. Ἂν ἰσχύει $x^3+2y^3=5z^3$ μὲ $(x, y)=1$, τότε καὶ $x^3+2y^3\equiv 5z^3 \pmod 9$, ὅπου οἱ x, y δὲν εἶναι καὶ οἱ δύο διαιρετοὶ διὰ 3.

7. Ἀποδεῖξτε ὅτι, γιὰ κάθε n, ὁ $5n^3+7n^5$ εἶναι πολλαπλάσιο τοῦ 12.

8. *Κριτήριο διαιρετότητας διὰ 3 ἢ 9.* Κατ' ἀρχάς, ὁρίζομε τὸν *πυθμένα* ἑνὸς θετικοῦ ἀκεραίου, τὸν ὁποῖο θεωροῦμε γραμμένο στὸ δεκαδικὸ σύστημα, ὡς τὸ ἄθροισμα τῶν ψηφίων του. Γιὰ παράδειγμα, ὁ πυθμὴν τοῦ 54678 εἶναι $5+4+6+7+8=30$.
   Ἀποδεῖξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 3 (ἀντιστοίχως, διὰ 9) εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τὴς διαίρεσης τοῦ πυθμένος τοῦ ἀριθμοῦ διὰ 3 (ἀντιστοίχως, διὰ 9). Γιὰ παράδειγμα, τὸ ὑπόλοιπο τῆς δαίρεσης τοῦ 54678 διὰ 9 εἶναι 3, καθὼς 3 εἶναι καὶ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 30 διὰ 9.
   Ὑπόδειξη. $10\equiv 1 \pmod 3$ καὶ $10\equiv 1 \pmod 9$. Ἄν, λοπόν, $a_0, a_1, \ldots, a_n$ εἶναι τὰ ψηφία τῶν μονάδων, δεκάδων κλπ τοῦ ἀριθμοῦ, ὑπολογῖστε μὲ ποιοὺς ἀριθμοὺς εἶναι ἰσότιμος ὁ ἀριθμός, μέτρῳ 3 καὶ μέτρῳ 9.

9. *Κρίτήριο διαιρετότητας διὰ 4 ἢ 25.* Ἀποδεῖξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 4 (ἀντιστοίχως, διὰ 25) εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τὴς διαίρεσης τοῦ ἀριθμοῦ, ποὺ σχηματίζεται ἀπὸ τὰ δύο τελευταῖα ψηφία τοῦ ἀριθμοῦ (βάση ἀρίθμησης τὸ 10) διὰ 4 (ἀντιστοίχως, διὰ 25).

10. *Κρίτήριο διαιρετότητας διὰ 8 ἢ 125.* Ἀποδεῖξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 8 (ἀντιστοίχως, διὰ 125) εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τὴς διαίρεσης τοῦ ἀριθμοῦ, ποὺ σχηματίζεται ἀπὸ τὰ τρία τελευταῖα ψηφία τοῦ ἀριθμοῦ (βάση ἀρίθμησης τὸ 10) διὰ 8 (ἀντιστοίχως, διὰ 125).

11. *Κριτήριο διαιρετότητας διὰ 11.* Ἀποδεῖξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 11 εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τὴς διαίρεσης τοῦ ἀριθμοῦ, ποὺ προκύπτει ἀπὸ τὸ ἄθροισμα τῶν διψηφίων τμημάτων τοῦ ἀριθμοῦ, λαμβανομένων ἀπὸ τὰ δεξιὰ πρὸς τὰ ἀριστερά. Γιὰ παράδειγμα, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ ἀριθμοῦ 9056781 διὰ 11 εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ $81 + 67 + 05 + 09$ διὰ 11.

12. *Δεύτερο κριτήριο διαιρετότητας διὰ 11.* Ἀποδεῖξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 11 εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τὴς διαίρεσης διὰ 11 τοῦ ἀριθμοῦ $a_0 - a_1 + a_2 - a_3 + \cdots$, ὅπου a_0 τὸ ψηφίο τῶν μονάδων τοῦ ἀριθμοῦ, a_1 τὸ ψηφίο τῶν δεκάδων, a_2 τὸ ψηφίο τῶν ἑκατοντάδων κ.ὄ.κ. Γιὰ παράδειγμα, ὁ 9876781 διαιρούμενος διὰ 11 δίνει ὑπόλοιπο ὅποιο καὶ ὁ ἀριθμὸς $1 - 8 + 7 - 6 + 7 - 8 + 3 = -4$, δηλαδή, 7 ($-4 = 11(-1) + 7$).

13. Ἔστω πρῶτος p.
α′. Ἔστω $a \in \{1, \ldots, p-1\}$. Μὲ τὴ βοήθεια τοῦ β′ τοῦ θεωρήματος 1.2.1 ἀποδεῖξτε ὅτι ὑπάρχει ἕνας, ἀκριβῶς, $a' \in \{1, \ldots, p-1\}$, μὲ τὴν ἰδιότητα $aa' \equiv 1 \pmod p$. Μετά, ἀποδεῖξτε ὅτι, οἱ μόνες περιπτώσεις ποὺ $a' = a$ εἶναι οἱ $a = 1$ καὶ $a = p - 1$.
β′. Ἔστω $p \geq 5$. Θεωρῆστε τὸ γινόμενο $1 \cdot 2 \cdots (p-2)(p-1)$ καί, βασισμένοι στὸ (α′), ζευγαρῶστε κάθε $a \in \{2, \ldots, p-2\}$ μὲ τὸ $a' \in \{2, \ldots, p-2\}$ γιὰ τὸ ὁποῖο ἰσχύει $aa' \equiv 1 \pmod p$. Συμπεράνατε ὅτι $(p-1)! \equiv -1 \pmod p$. Διαπιστῶστε ὅτι ἡ σχέση αὐτή, ποὺ λέγεται *θεώρημα τοῦ Wilson*, ἰσχύει καὶ γιὰ $p = 2, 3$. Ἀποδεῖξτε καὶ τὸ ἀντίστροφο θεώρημα: Ἂν γιὰ κάποιον ἀκέραιο p ἰσχύει $(p-1)! \equiv -1 \pmod p$, τότε ὁ p εἶναι πρῶτος.

14. Ἔστω $m \geq 2$ καὶ $M \subset \mathbb{Z}$, τέτοιο ὥστε, οἱ ἀριθμοὶ τοῦ M εἶναι ἀνισότιμοι μεταξύ τους, καὶ $|M| = m$. Ἀποδεῖξτε ὅτι τὸ M εἶναι πλῆρες σύστημα ὑπολοίπων $\bmod m$.

15. Ἔστω $m \geq 2$ καὶ $M \subset \mathbb{Z}$, ἀποτελούμενο ἀπὸ ἀριθμοὺς πρώτους πρὸς m καὶ ἀνισότιμους μεταξύ τους $\bmod m$. Ἂν, ἐπιπλέον, ὁ πληθάριθμος τοῦ M εἶναι $\phi(m)$, τότε ἀποδεῖξτε ὅτι τὸ M εἶναι περιορισμένο σύστημα ὑπολοίπων $\bmod m$.

16. Ἔστω ὅτι ὁ p εἶναι πρῶτος καὶ $ab' - a'b \not\equiv 0 \pmod p$. Ἀποδεῖξτε ὅτι δὲν ὑπάρχουν ἀκέραιοι x, y, πρῶτοι μεταξύ τους, ποὺ νὰ ἱκανοποιοῦν συγχρόνως καὶ τὶς δύο ἰσοτιμίες $ax + by \equiv 0 \pmod p$ καὶ $a'x + b'y \equiv 0 \pmod p$.
Ὑπόδειξη. Ἀπαλεῖψτε τὸ y ἀπὸ τὶς δύο ἰσοτιμίες καί, μετά, κάντε τὸ ἴδιο καὶ γιὰ τὸ x.

17. Ἀποδεῖξτε ὅτι, ἂν $a|b$, τότε $\phi(a)|\phi(b)$.

18. Ἔστω ὅτι ὁ $n \geq 3$ ἔχει k διαφορετικοὺς πρώτους διαιρέτες. Ἀποδεῖξτε ὅτι, ἂν ὁ n εἶναι ἄρτιος, ἀλλὰ ὄχι πολλαπλάσιο τοῦ 4, τότε $2^{k-1}|\phi(n)$ ἐνῶ, γιὰ ὅλες τὶς ὑπόλοιπες τιμὲς τοῦ n, $2^k|\phi(n)$.

19. Ἀποδεῖξτε ὅτι, οἱ μόνοι θετικοὶ ἀκέραιοι x, γιὰ τοὺς ὁποίους ἰσχύει $\phi(x) = x/2$, εἶναι οἱ $x = 2^a$, $a \geq 1$.

20. Ἀποδεῖξτε ὅτι, γιὰ κάθε θετικὸ περιττὸ ἀκέραιο x ἰσχύει $\phi(x) = \phi(2x)$, ἀλλὰ ἡ σχέση αὐτὴ εἶναι ἀδύνατη γιὰ ἄρτιο x.

21. Βρεῖτε ὅλους τοὺς θετικοὺς ἀκεραίου x, γιὰ τοὺς ὁποίους ἰσχύει $\phi(x) = 12$.

22. Ἔστω $n \geq 1$. Γιὰ κάθε θετικὸ διαιρέτη d τοῦ n ὁρίζομε τὸ σύνολο

$$A(d) = \{k \,:\, 1 \leq k \leq n \quad \text{καὶ} \quad (k,n) = d\}\,.$$

(α′) Ἀποδεῖξτε ὅτι τὸ $A(d)$ περιέχει ἀκριβῶς $\phi(\frac{n}{d})$ ἀριθμούς.
Ὑπόδειξη. Παρατηρῆστε ὅτι $1 \leq k \leq n$ καὶ $(k,n) = d \Leftrightarrow \frac{k}{d}$ ἀκέραιος καὶ $1 \leq \frac{k}{d} \leq \frac{n}{d}$ καὶ $(\frac{k}{d}, \frac{n}{d}) = 1$.
(β′) Ἂν $d_1 \neq d_2$ εἶναι θετικοὶ διαιρέτες τοῦ n, ἀποδεῖξτε ὅτι $A(d_1) \cap A(d_2) = \emptyset$.
(γ′) Συνδυάζοντας τὰ (α′) καὶ (β′) ἀποδεῖξτε ὅτι

$$\sum_{d|n} \phi(\frac{n}{d}) = n\,, \quad \text{ἄρα καὶ} \quad \sum_{d|n} \phi(d) = n\,.$$

Ὑπόδειξη. Γιὰ τὸ «. . . ἄρα καὶ . . . » δεῖτε τὴν ἄσκηση 4 τοῦ κεφαλαίου 1.

23. Ὑπολογῖστε τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ $(12371^{128} + 34)^{172}$ διὰ 111.

24. Ἀποδεῖξτε ὅτι, γιὰ κάθε n, ὁ $n^{37} - n$ εἶναι πολλαπλάσιο τοῦ 383838.
Ὑπόδειξη. Λάβετε ὑπ’ ὄψει ὅτι $383838 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 37$ καὶ ἐφαρμόστε τὸ θεώρημα τοῦ Fermat, κάμποσες φορές, γιὰ κατάλληλους πρώτους.

25. Ἔστω p πρῶτος. Παρατηρῆστε ὅτι, τὸ θεώρημα τοῦ Fermat μπορεῖ νὰ διατυπωθεῖ ὡς ἑξῆς: Γιὰ κάθε a ἰσχύει $a^p \equiv a \pmod{p}$, δίχως νὰ θέσομε τὸν περιορισμὸ ὁ p νὰ μὴ διαιρεῖ τὸν a. Μετά, μὲ τὴ βοήθεια τῆς ἄσκησης 31 τοῦ κεφαλαίου 1, ἀποδεῖξτε ὅτι $(a + b)^p \equiv a^p + b^p \pmod{p}$, γιὰ ὅλους τοὺς a, b. Ἐπίσης, ἀποδεῖξτε ὅτι ἂν γιὰ τὸν περιττὸ πρῶτο p ἰσχύει $a^p + b^p \equiv 0 \pmod{p}$ τότε ἰσχύει καὶ $a^p + b^p \equiv 0 \pmod{p^2}$.

26. Μετατρέψτε τὸν 749 σὲ δυαδικὸ ἀριθμό, ἐφαρμόζοντας τὸν ἀλγόριθμο μετατροπῆς σὲ δυαδικό.

27. Ἐφαρμόζοντας τὸν ἀλγόριθμο ὕψωσης σὲ δύναμη, ὑπολογῖστε τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 13^{370} διὰ 23.

28. Ἔστω ὅτι τὸ δημόσιο κλειδὶ τῆς Α εἶναι (91,25). Ὁ Β θέλει νὰ κρυπτογραφήσει καὶ νὰ στείλει στὴν Α τὸ μήνυμα ΘΑ ΕΛΘΩ ΣΤΙΣ ΟΚΤΩ. Ποιὰ διαδικασία θὰ ἀκολουθήσει γιὰ νὰ κρυπτογραφήσει τὸ μήνυμα καὶ ποιὰ διαδικασία θὰ ἀκολουθήσει ἡ Α, ὅταν λάβει τὸ κρυπτογραφημένο μήνυμα, γιὰ νὰ τὸ ἀποκρυπτογραφήσει; Γιὰ νὰ διευκολυνθεῖτε στὶς πράξεις, μὴ παίρνετε ἀνὰ δύο

τὰ γράμματα, ἀλλὰ ἕνα-ἕνα. Ἔτσι, ἡ «ἀριθμητικὴ μορφὴ» τοῦ μηνύματος, πρὶν τὴν κρυπτογράφησή του, ἀρχίζει ὡς ἑξῆς: (8,1,25,5,11,8,24,. . .).

Κεφάλαιο 3

Ἐπίλυση ἰσοτιμιῶν

Στὸ κεφάλαιο αὐτό, ὁ m εἶναι πάντοτε ἀκέραιος μεγαλύτερος τοῦ 1
Τα λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους

3.1 Γενικά

Ἔστω μὴ μηδενικὸ πολυώνυμο $f(X) \in \mathbb{Z}[X]$ καὶ ἀκέραιος $m > 1$. Ὑποθέτομε ὅτι δὲν εἶναι ὅλοι οἱ συντελεστὲς τοῦ $f(X)$ διαιρετοὶ διὰ m. Τὸ δ′ τοῦ θεωρήματος 2.1.2 συνεπάγεται ὅτι, ἂν $a \equiv b \pmod m$ καὶ $f(a) \equiv 0 \pmod m$, τότε καὶ $f(b) \equiv 0 \pmod m$. Συνεπῶς, ἔχει νόημα νὰ ὁρίσομε ὡς *ἐπίλυση τῆς ἰσοτιμίας* $f(x) \equiv 0 \pmod m$ τὴν εὕρεση ὅλων τῶν κλάσεων $a \bmod m$, τέτοιων ὥστε $f(a) \equiv 0 \pmod m$ καὶ νὰ λέμε ὅτι *ἡ κλάση* $a \bmod m$ (καὶ ὄχι *ὁ ἀριθμὸς* a) εἶναι λύση τῆς ἰσοτιμίας. Εἰδικώτερα, ὅταν λέμε ὅτι «ἡ ἰσοτιμία ἔχει k τὸ πλῆθος λύσεις», ἐννοοῦμε ὅτι ὑπάρχουν k διαφορετικὲς $\bmod m$ κλάσεις, κάθε μία ἀπὸ τὶς ὁποῖες εἶναι λύση τῆς $f(a) \equiv 0 \pmod m$.

Λέμε ὅτι ἡ ἰσοτιμία $f(x) \equiv 0 \pmod m$ εἶναι ἰσοδύναμη μὲ τὴν $g(x) \equiv 0 \pmod m$, ἂν οἱ δύο ἰσοτιμίες ἔχουν τὶς ἴδιες, ἀκριβῶς λύσεις. Προσοχή! Ἡ ἔννοια τῶν ἰσοδυνάμων ἰσοτιμιῶν ἔχει νόημα μόνον ὅταν τὰ μέτρα τῶν δύο ἰσοτιμιῶν εἶναι τὰ ἴδια.

3.2 Ἰσοτιμίες πρώτου βαθμοῦ

Θὰ μελετήσομε πρῶτα τὴν περίπτωση πρωτοβαθμίου πολυωνύμου $f(X)$, ἄρα, οὐσιαστικά, τὴν ἐπίλυση τῆς ἰσοτιμίας $ax \equiv b \pmod m$.

Θεώρημα 3.2.1 *Ἂν $a \neq 0$ καὶ $(a, m) = d$, τότε ἡ ἰσοτιμία $ax \equiv b \pmod m$ ἔχει λύση ἄν, καὶ μόνο ἄν, $d|b$. Στὴν περίπτωση ποὺ ἔχει λύση, τὸ πλῆθος τῶν διαφορετικῶν λύσεων εἶναι, ἀκριβῶς, d· καὶ πιὸ συγκεκριμένα, ἂν ἡ λύση τῆς ἰσοτιμίας $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ εἶναι ἡ $x_0 \bmod \frac{m}{d}$, τότε οἱ d διαφορετικὲς λύσεις τῆς $ax \equiv b$*

(mod m) *εἶναι οἱ*

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \,. \tag{3.1}$$

Ἀπόδειξη Ἂν ἡ $ax \equiv b \pmod{m}$ ἔχει λύση, τότε, γιὰ κάποιο $x_1 \in \mathbb{Z}$ ἔχομε $ax_1 \equiv b \pmod{m}$, ἄρα, ἀπὸ τὸ η′ τοῦ θεωρήματος 2.1.2, $(ax_1, m) = (b, m)$. Ἀλλά, προφανῶς, $d|(ax_1, m)$, ὁπότε $d|b$. Ἀντιστρόφως, ἔστω ὅτι $d|b$. Ἀπὸ τὸ β′ τοῦ θεωρήματος 1.2.1 ξέρομε ὅτι ὑπάρχουν ἀκέραιοι x_0, y_0, τέτοιοι ὥστε $ax_0 + my_0 = d$. Τώρα, παρατηροῦμε ὅτι ὁ $\frac{b}{d}$ εἶναι ἀκέραιος καὶ ἀπὸ τὴν τελευταία ἰσότητα,

$$a(x_0\frac{b}{d}) + m(y_0\frac{b}{d}) = b\,,$$

σχέση, ἡ ὁποία, προφανῶς, συνεπάγεται ὅτι $ax_1 \equiv b \pmod{m}$, ὅπου $x_1 = x_0\frac{b}{d}$· δηλαδή, ἡ ἰσοτιμία $ax \equiv b \pmod{m}$ ἔχει λύση.

Ἔστω τώρα ὅτι ἡ $ax \equiv b \pmod{m}$, ἔχει λύση, ὁπότε, σύμφωνα μὲ τὰ παραπάνω, $d|b$. Θέτοντας ὅπου a, b, m τὰ $\frac{a}{d}, \frac{b}{d}, \frac{m}{d}$, ἀντιστοίχως, καταλήγομε, βάσει τῶν ἀνωτέρω, στὸ συμπέρασμα ὅτι ἡ ἰσοτιμία $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ἔχει μία, τοὐλάχιστον, λύση, ἔστω τὴν $x_0 \bmod \frac{m}{d}$.
Ἰσχυριζόμαστε, κατ' ἀρχάς, ὅτι δὲν μπορεῖ νὰ ἔχει καὶ δεύτερη, διαφορετική, λύση. Πράγματι, ἂν $x_1 \bmod \frac{m}{d}$ εἶναι, ἐπίσης, λύση, τότε

$$\frac{a}{d}x_0 \equiv \frac{b}{d} \equiv \frac{a}{d}x_1 \pmod{\frac{m}{d}}\,.$$

Τὸ στ′ τοῦ θεωρήματος 2.1.2 μᾶς ἐπιτρέπει νὰ διαιρέσομε διὰ $\frac{a}{d}$, διότι $(\frac{a}{d}, \frac{m}{d}) = 1$, ὁπότε καταλήγομε στὴν $x_0 \equiv x_1 \pmod{\frac{m}{d}}$.
Στὴ συνέχεια, ἔστω $x_1 \bmod m$ μία λύση τῆς $ax \equiv b \pmod{m}$. Τότε, βλέπομε πολὺ εὔκολα ὅτι ἡ $x_1 \bmod \frac{m}{d}$ εἶναι λύση τῆς $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, ἄρα, ἀπὸ τὴ μοναδικότητα τῆς λύσης $x_0 \bmod \frac{m}{d}$, ποὺ εἴδαμε παραπάνω, καταλήγομε στὸ συμπέρασμα ὅτι $x_1 \equiv x_0 \pmod{\frac{m}{d}}$. Ἄρα, ὑπάρχει ἀκέραιος ℓ, τέτοιος ὥστε $x_1 = x_0 + \ell\frac{m}{d}$. Ἐκτελώντας τὴν εὐκλείδεια διαίρεση τοῦ ℓ διὰ d ἔχομε $\ell = qd + j$, ὅπου $0 \le j \le d-1$. Συνεπῶς, $x_1 = x_0 + j\frac{m}{d} + qm \equiv x_0 + j\frac{m}{d} \pmod{m}$, ἄρα, ὁ ἡ κλάση $x_1 \bmod m$ συμπίπτει μὲ μία ἀπὸ τὶς κλάσεις (3.1).
Μένει νὰ δείξομε ὅτι οἱ κλάσεις (3.1) εἶναι διαφορετικές. Πράγματι, ἂν δύο ἐξ αὐτῶν συνέπιπταν, θὰ εἴχαμε $x_0 + j_1\frac{m}{d} \equiv x_0 + j_2\frac{m}{d} \pmod{m}$ μὲ $0 \le j_1 < j_2 < d$. Ἀπὸ αὐτὴν θὰ παίρναμε $j_1\frac{m}{d} \equiv j_2\frac{m}{d} \pmod{m}$ καί, διαιρώντας τὰ δύο μέλη καὶ τὸ μέτρο διὰ $\frac{m}{d}$ (βλ. ε′ τοῦ θεωρήματος 2.1.2), θὰ καταλήγαμε στὴν $j_1 \equiv j_2 \pmod{d}$. Ἡ τελευταία, ὅμως, σημαίνει ὅτι $d|(j_2 - j_1)$, προφανῶς ἀδύνατον, ἀφοῦ $0 < j_2 - j_1 < d$.
ὅ.ἔ.δ.

Στὴν πράξη, ἡ ἐπίλυση μιᾶς ἰσοτιμίας $ax \equiv b \pmod{m}$ βασίζεται στὸ θεώρημα 1.2.3. Κατ' ἀρχάς, στὴν ἰσοτιμία $ax \equiv b \pmod{m}$ μποροῦμε πάντα νὰ ὑποθέτομε ὅτι $1 \le a < m$. Ἐφαρμόζομε τὸν εὐκλείδειο ἀλγόριθμο, ὅπως περιγράφεται στὸ θεώρημα αὐτό, μὲ τὸ m τῆς ἰσοτιμίας στὴ θέση τοῦ a τοῦ θεωρήματος καὶ τὸ a τῆς ἰσοτιμίας στὴ θέση τοῦ b τοῦ θεωρήματος. Ἂν τὸ $(n+1)$-οστὸ ὑπόλοιπο στὴ διαδικασία τοῦ εὐκλειδείου ἀλγορίθμου εἶναι 0, τότε, σύμφωνα μὲ τὸ θεώρημα 1.2.3, τὸ τελευταῖο μὴ μηδενικὸ ὑπόλοιπο r_n εἶναι ὁ μέγιστος κοινὸς διαιρέτης d τῶν a, b. Ἂν ὁ d δὲν διαιρεῖ τὸν b, τότε ἡ ἰσοτιμία δὲν ἔχει λύση. Ἂς ὑποθέσομε, λοιπόν, ὅτι $d|b$. Σύμφωνα μὲ τὸ β′ τοῦ θεωρήματος 1.2.3, $ms_{n-1} + as_n = d$, ἄρα

$$\frac{a}{d}\left(\frac{b}{d}s_n\right) \equiv \frac{b}{d} \pmod{\frac{m}{d}},$$

ποὺ σημαίνει ὅτι, μὲ τὸν συμβολισμὸ τοῦ θεωρήματος 3.2.1,

$$x_0 = \frac{b}{d}s_n \tag{3.2}$$

καὶ ἀπὸ αὐτὸ τὸ σημεῖο καὶ πέρα οἱ d διαφορετικὲς λύσεις τῆς ἰσοτιμίας ὑπολογίζονται ἁπλούστατα ἀπὸ τὴν (3.1).

Παράδειγμα. Θὰ λύσομε τὴν ἰσοτιμία $917x \equiv 42 \pmod{7168}$. Στὸ παράδειγμα μετὰ τὸ θεώρημα 1.2.3 ὑπολογίσαμε $(917, 7168) = 7$ καὶ παρατηροῦμε ὅτι $7|42$, ἄρα ἡ ἰσοτιμία μας ἔχει 7 ἀκριβῶς λύσεις, σύμφωνα μὲ τὸ θεώρημα 3.2.1. Σύμφωνα μὲ τὸ ἴδιο θεώρημα καὶ ὅ,τι ἀκολουθεῖ, ἀρκεῖ νὰ ὑπολογίσομε ἀναδρομικὰ τὰ $s_{-1}, s_0, s_1, \ldots$, ποὺ ἀντιστοιχοῦν στὸ ζεῦγος τῶν ἀριθμῶν 7168 καὶ 917. Στὸ προαναφερθὲν παράδειγμα ἔχουν ὑπολογισθεῖ αὐτὰ τὰ s_i. Τὸ τελευταῖο ἐξ αὐτῶν εἶναι τὸ $s_6 = 555$. Ἄρα, σύμφωνα μὲ τὸν συμβολισμὸ τοῦ θεωρήματος 3.2.1 καὶ τὴν (3.2), $x_0 = 6 \cdot 555 = 3330 \equiv 258 \pmod{1024}$ ($1024 = \frac{7168}{7}$), ὁπότε ὅλες οἱ λύσεις τῆς ἰσοτιμίας εἶναι $x \equiv 258 + k\frac{7168}{7}$, $k = 0, 1, \ldots, 6$, δηλαδή,

$$x \equiv 258\,,\ 1282\,,\ 2306\,,\ 3330\,,\ 4354\,,\ 5378\,,\ 6402 \pmod{7168}\,.$$

3.3 Τὸ κινέζικο θεώρημα ὑπολοίπων

Ἀπὸ τὰ ἀρχαῖα χρόνια ἦταν γνωστὰ πάμπολλα προβλήματα ὅπως αὐτὸ ἐδῶ: *Ἕνα στρατιωτικὸ σῶμα ἔχει λιγώτερους ἀπὸ 1000 στρατιῶτες. Ἂν τοποθετηθοῦν κατὰ 15άδες, περισσεύουν 11· ἀ 'ν τοποθετηθοῦν κατὰ 8άδες, περισσεύουν 5 καὶ ἂν τοποθετηθοῦν κατὰ 13άδες, περισσεύουν 12. Ἀπὸ πόσους στρατιῶτες ἀποτελεῖται τὸ σῶμα;* Τέτοιου εἴδους προβλήματα ὁδηγοῦν φυσιολογικὰ στὸ λεγόμενο *κινέζικο θεώρημα ὑπολοίπων*.

Θεώρημα 3.3.1 –Κινέζικο θεώρημα ὑπολοίπων. *Ἔστω ὅτι οἱ $m_1, \ldots, m_k$ εἶναι μεγαλύτεροι τοῦ 1 καὶ ἀνὰ δύο πρῶτοι μεταξύ τους. Τότε, γιὰ ὁποιουσδήποτε ἀκεραίους $a_1, \ldots, a_k$, ὑπάρχει x, τὸ ὁποῖο ἐπαληθεύει συγχρόνως ὅλες τὶς ἰσοτιμίες*

$$x \equiv a_1 \pmod{m_1}\,, \quad x \equiv a_2 \pmod{m_2}\,, \ldots, x \equiv a_k \pmod{m_k} \tag{3.3}$$

καὶ τὸ x αὐτὸ εἶναι μοναδικὸ μέτρῳ $m_1 m_2 \cdots m_k$.

Ἀπόδειξη Θέτομε $M = m_1 m_2 \cdots m_k$ καὶ γιὰ κάθε $i = 1, \ldots, k$, $M_i = M/m_i$. Ἀπὸ τὴν ὑπόθεση ὅτι ὁ m_i εἶναι πρῶτος πρὸς ὅλους τοὺς ὑπόλοιπους m_j καὶ τὸ ζ′ τοῦ θεωρήματος 1.2.2 συμπεραίνομε ὅτι $(m_i, M_i) = 1$. Ἄρα, ἀπὸ τὸ θεώρημα 3.2.1, ὑπάρχει N_i, τέτοιος ὥστε $M_i N_i \equiv 1 \pmod{m_i}$. Ὁρίζομε τώρα

$$x_0 = M_1 N_1 a_1 + M_2 N_2 a_2 + \cdots + M_k N_k a_k$$

καὶ θὰ δείξομε ὅτι, γιὰ κάθε $i = 1, \ldots, k$, $x_0 \equiv a_i \pmod{m_i}$. Πράγματι, ἀπὸ τὸν τρόπο ποὺ ὁρίσθηκαν τὰ $M_1, \ldots, M_k$, βλέπομε ἀμέσως ὅτι, κάθε M_j μὲ $j \neq i$ ἔχει ὡς παράγοντά του τὸν m_i καί, συνεπῶς, εἶναι μηδενικὸς μέτρῳ m_i. Ἄρα, $x_0 \equiv M_i N_i a_i \equiv 1 \cdot a_i \pmod{m_i}$. Ἄρα, γιὰ $x = x_0$ ἐπαληθεύεται τὸ σύστημα τῶν ἰσοτιμιῶν (3.3).

Ἔστω, τώρα, ὅτι $x = x_1$ ἐπίσης ἐπαληθεύει τὶς (3.3). Τότε, γιὰ κάθε $i = 1, \ldots, k$, $x_1 \equiv a_i \equiv x_0 \pmod{m_i}$, ἄρα $m_i | (x_1 - x_0)$ καὶ ἀπὸ τὸ γ′ τοῦ θεωρήματος 1.3.1, $(m_1 m_2 \cdots m_k) | (x_1 - x_0)$, δηλαδή, $x_1 \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$. **ὅ.ἔ.δ.**

Παράδειγμα. Θὰ λύσομε τὸ πρόβλημα, ποὺ ἀναφέραμε στὴν ἀρχὴ αὐτῆς τῆς παραγράφου. Προφανῶς, τὸ πρόβλημα ἰσοδυναμεῖ μὲ τὴν εὕρεση θετικοῦ ἀκεραίου $x < 1000$, τέτοιου ὥστε

$$x \equiv 11 \pmod{15}, \quad x \equiv 5 \pmod{8} \quad x \equiv 12 \pmod{13}.$$

Μὲ τὸν συμβολισμὸ τῆς ἀπόδειξης τοῦ θεωρήματος ἔχομε $M_1 = 8 \cdot 13 = 104$, $M_2 = 15 \cdot 13 = 195$, $M_3 = 15 \cdot 8 = 120$. Ἐπίσης, $104 N_1 \equiv 1 \pmod{15}$, $195 N_2 \equiv 1 \pmod{8}$, $120 N_3 \equiv 1 \pmod{13}$ καὶ οἱ ἰσοτιμίες αὐτὲς ἁπλοποιοῦνται ὡς ἑξῆς: $(-1) N_1 \equiv 1 \pmod{15}$, $3 N_2 \equiv 1 \pmod{8}$, $3 N_3 \equiv 1 \pmod{13}$. Ἡ ἐπίλυση κάθε μιᾶς ἀπὸ αὐτὲς εἶναι ἁπλούστατη, μὲ δοκιμές, ὥστε δὲν χρειάζεται νὰ ἐφαρμόσομε τὸν ἀλγόριθμο τῆς παραγράφου 3.2. Βρίσκομε ἔτσι, $N_1 = -1$, $N_2 = 3$, $N_3 = -4$ καὶ $x_0 = 104 \cdot (-1) \cdot 11 + 195 \cdot 3 \cdot 5 + 120 \cdot (-4) \cdot 12 = -3979$, ἄρα, $x \equiv -3979 \pmod{15 \cdot 8 \cdot 13}$. Συνεπῶς, $x = -3979 + 1560k$ καί, λόγῳ τῆς $0 < x < 1000$, παίρνομε $3979 < 1560k < 4979$, ἀπ' ὅπου $k = 3$ καὶ $x = -3979 + 3 \cdot 1560 = 701$.

3.4 Πολυωνυμικὲς ἰσοτιμίες μὲ ἕνα ἄγνωστο

Ἀρχικά, θὰ θεωρήσομε ὅτι τὸ μέτρο τῆς ἰσοτιμίας εἶναι ἕνας θετικὸς πρῶτος p.

Μία προκαταρκτικὴ ἁπλή, ἀλλὰ βασική, παρατήρηση εἶναι ὅτι κάθε πολυωνυμικὴ ἰσοτιμία $f(x) \equiv 0 \pmod{p}$ εἶναι ἰσοδύναμη μὲ μία ἰσοτιμία $g(x) \equiv 0 \pmod{p}$, στὴν ὁποία, ὁ βαθμὸς τοῦ $g(X)$ εἶναι, τὸ πολύ, $p - 1$.[1] Πράγματι, ἐκτελώντας τὴν εὐκλείδεια διαίρεση τοῦ $f(X)$ διὰ τοῦ πολυωνύμου $x^p - x$, καταλήγομε σὲ μία σχέση $f(X) = (X^p - X)h(X) + g(X)$, ὅπου ὁ βαθμὸς τοῦ $g(X)$ δὲν ὑπερβαίνει τὸν $p - 1$. Ξέρομε, ἀπὸ τὸ θεώρημα τοῦ Fermat (β′ τοῦ θεωρήματος 2.2.4), ὅτι, γιὰ κάθε

[1] Ἐδῶ περιλαμβάνεται καὶ ἡ περίπτωση τοῦ μηδενικοῦ πολυωνύμου, τοῦ ὁποίου ὁ βαθμὸς μπορεῖ νὰ ὁρισθεῖ ὡς $-\infty$.

ἀκέραιο a, εἶναι $a^p - a \equiv 0 \pmod p$, ἄρα, $f(a) \equiv 0 \pmod p$ ἄν, καὶ μόνο ἄν, $g(a) \equiv 0 \pmod p$. Αὐτό, προφανῶς, σημαίνει ὅτι οἱ ἰσοτιμίες $f(x) \equiv 0 \pmod p$ καὶ $g(x) \equiv 0 \pmod p$ εἶναι ἰσοδύναμες.

Θεώρημα 3.4.1 *Ἔστω $f(X) \in \mathbb{Z}[X]$, βαθμοῦ $n \geq 1$, τοῦ ὁποίου ὁ συντελεστὴς τοῦ μεγιστοβαθμίου ὅρου δὲν διαιρεῖται διὰ p. Τότε, ἡ ἰσοτιμία $f(x) \equiv 0 \pmod p$ ἔχει, τὸ πολύ, n τὸ πλῆθος διαφορετικὲς λύσεις.* [2]
Ἰσοδύναμη διατύπωση: Ἂν τὸ $f(X) \in \mathbb{Z}[X]$ εἶναι μὴ μηδενικὸ πολυώνυμο καὶ τὸ πλῆθος τῶν λύσεων τῆς ἰσοτιμίας $f(x) \equiv 0 \pmod p$ ὑπερβαίνει τὸν βαθμὸ τοῦ $f(X)$, τότε ὅλοι οἱ συντελεστὲς τοῦ $f(X)$ εἶναι διαιρετοὶ διὰ p.
Ἀπόδειξη Ἔστω $f(X) = a_nX^n + \cdots a_1X + a_0$, ὅπου, ἐξ ὑποθέσεως, $(a_n, p) = 1$ καὶ ἂς ὑποθέσομε ὅτι ἡ ἰσοτιμία $f(x) \equiv 0 \pmod p$ ἔχει $n + 1$ διαφορετικὲς λύσεις $r_1 \bmod p, \ldots, r_{n+1} \bmod p$. Θὰ καταλήξομε σὲ ἄτοπο. Τὸ γεγονὸς ὅτι οἱ λύσεις αὐτὲς εἶναι διαφορετικές, σημαίνει, φυσικά, $r_i \not\equiv r_j \pmod p$ γιὰ $i \neq j$.
Ἰσχυρισμός: Ὑπάρχουν ἀκέραιοι $b_0, b_1, \ldots, b_{n-1}$, τέτοιοι ὥστε, νὰ ἰσχύει

$$\begin{aligned} f(X) = {} & a_n(X - r_1)(X - r_2) \cdots (X - r_{n-2})(X - r_{n-1})(X - r_n) \\ & + b_{n-1}(X - r_1)(X - r_2) \cdots (X - r_{n-1}) \\ & + b_{n-2}(X - r_1)(X - r_2) \cdots (X - r_{n-2}) \\ & \vdots \\ & + b_2(X - r_1)(X - r_2) \\ & + b_1(X - r_1) \\ & + b_0 \end{aligned} \tag{3.4}$$

Πράγματι, κατ᾽ ἀρχάς, στὴν (3.4) ἂς συμβολίσομε τὸ πολυώνυμο τῆς πρώτης γραμμῆς μὲ $g_n(X)$, τῆς δεύτερης μὲ $g_{n-1}(X)$ ... τῆς προτελευταίας μὲ $g_1(X)$. Τὸ πολυώνυμο $g_n(X)$ εἶναι γνωστό, ἀφοῦ τὰ $a_n, r_1, \ldots, r_n$ εἶναι γνωστά· τὰ ὑπόλοιπα, ὅμως, πολυώνυμα $g_{n-1}(X), \ldots, g_1(X)$ ἐξαρτῶνται ἀπὸ τοὺς μέχρι στιγμῆς ἀγνώστους $b_{n-1}, \ldots, b_1$.
Συγκρίνομε τοὺς συντελεστὲς τῶν $X^n, X^{n-1}, \ldots, X, X^0$ στὰ δύο μέλη. Τοῦ X^n εἶναι a_n καὶ στὰ δύο μέλη. Ἀπὸ τὴ σύγκριση τῶν συντελεστῶν τοῦ X^{n-1} παίρνομε

$$a_{n-1} = b_{n-1} + \text{συντελεστὴς τοῦ } X^{n-1} \text{ στὸ } g_n(X)\,,$$

ἄρα μποροῦμε νὰ ὑπολογίσομε τὸ b_{n-1}, τὸ ὁποῖο, πλέον, θεωρεῖται γνωστό, ὁπότε καὶ τὸ $g_{n-1}(X)$ εἶναι γνωστό.
Ἀπὸ τὴ σύγκριση τῶν συντελεστῶν τοῦ X^{n-2} παίρνομε

$$\begin{aligned} a_{n-2} = b_{n-2} & + \text{συντελεστὴς τοῦ } X^{n-2} \text{ στὸ } g_n(X) \\ & + \text{συντελεστὴς τοῦ } X^{n-2} \text{ στὸ } g_{n-1}(X)\,. \end{aligned}$$

[2] Οἱ *ἐπαΐοντες* θὰ ἀναγνωρίσουν ἐδῶ μία εἰδικὴ περίπτωση τοῦ γενικοῦ θεωρήματος τῆς Ἄλγεβρας, ποὺ λέει ὅτι, ἕνα πολυώνυμο βαθμοῦ n μὲ συντελεστὲς ἀπὸ ἕνα σῶμα, ἔχει, τὸ πολύ, n διαφορετικὲς ρίζες στὸ σῶμα αὐτό. Στὴν προκειμένη περίπτωση, σῶμα εἶναι τὸ $\mathbb{Z}_p$ (ἢ $\mathbb{F}_p$, κατ᾽ ἄλλο συμβολισμό).

Ἀπὸ τὴ σχέση αὐτὴ προσδιορίζεται καὶ τὸ b_{n-2}, ἄρα, στὸ ἑξῆς, καὶ τὸ $g_{n-2}(X)$ εἶναι γνωστό.
Μὲ αὐτὴ τὴ διαδικασία προχωρώντας, καταλήγομε στὸν ὑπολογισμὸ ὅλων τῶν b_i. Φυσικά, δὲν μᾶς ἐνδιαφέρει ὁ ἀκριβὴς ὑπολογισμός τους, ἀλλά, ἁπλῶς, ἡ ὕπαρξή τους, ποὺ καθιστᾶ ἀληθῆ τὴ σχέση (3.4). Ἡ ἀντικατάσταση $X \leftarrow r_1$ στὴ σχέση αὐτὴ δίνει $0 \equiv f(r_1) = b_0 \pmod{p}$. Μετά, ἡ ἀντικατάσταση $X \leftarrow r_2$ στὴν (3.4) δίνει $0 \equiv f(r_2) = b_0 + b_1(r_2 - r_1) \equiv 0 + b_1(r_2 - r_1) \pmod{p}$. Ἐπειδή, ὅμως, $(r_2 - r_1, p) = 1$, τὸ στ′ τοῦ θεωρήματος 2.1.2 μᾶς ἐπιτρέπει νὰ συμπεράνομε ὅτι $b_1 \equiv 0 \pmod{p}$. Μὲ τὸν τρόπο αὐτό, οἱ διαδοχικὲς ἀντικαταστάσεις $X \leftarrow r_i$, $i = 3, \dots, n$ μᾶς δίνουν, ἀντιστοίχως, $b_j \equiv 0 (\mathrm{mod}\ p)$ γιὰ $j = 2, \dots, n$. Τέλος, ἡ ἀντικατάσταση $X \leftarrow r_{n+1}$ στὴν (3.4) δίνει, μὲ δεδομένο ὅτι ὅλοι οἱ b_i εἶναι ἰσότιμοι μὲ 0 μέτρῳ p, $0 \equiv f(r_{n+1}) \equiv a_n(r_{n+1} - r_1)(r_{n+1} - r_2)\cdots(r_{n+1} - r_n) \pmod{p}$. Ἐξ ὑποθέσεως, κάθε παράγων $r_{n+1} - r_j$, στὸ δεξιὸ μέλος, εἶναι πρῶτος πρὸς τὸν p, ἄρα, ἀναγκαστικά, συμπεραίνομε ὅτι $a_n \equiv 0 (\mathrm{mod}\ p)$, τὸ ὁποῖο ἀντιφάσκει πρὸς τὴν ὑπόθεσή μας. **ὅ.ἔ.δ.**

Τώρα θὰ ἐξετάσομε τὴν ἐπίλυση τῆς ἰσοτιμίας

$$f(x) \equiv 0 \pmod{p^a}, \tag{3.5}$$

ὅπου, καὶ πάλι, ὁ p εἶναι πρῶτος καὶ ὁ συντελεστὴς τοῦ μεγιστοβαθμίου ὅρου τοῦ $f(X)$ δὲν εἶναι διαιρετὸς διὰ p. Ὁ ἐκθέτης a εἶναι τουλάχιστον 2. Θὰ δείξομε ὅτι, ἀναδρομικά, ἂν ξέρομε νὰ λύσομε τὴν ἰσοτιμία (3.5) γιὰ κάποια τιμὴ τοῦ ἐκθέτη a, τότε μποροῦμε νὰ τὴ λύσομε καὶ γιὰ τὴν ἀμέσως ἑπόμενη τιμή του.

> Ἡ φράση *«μπορῶ νὰ λύσω μία ἰσοτιμία»* πάντοτε σημαίνει *«μπορῶ νὰ ἀποφασίσω ἂν ἔχει ἢ ὄχι λύσεις καί, σὲ περίπτωση ποὺ ἔχει, μπορῶ νὰ τὶς ὑπολογίσω ὅλες»*.

Ὡς συνήθως, συμβολίζομε μὲ $f^{(k)}(X)$ τὴν k-τάξεως παράγωγο τοῦ $f(X)$. [3] Τὶς περισσότερες φορές, ἀντὶ γιὰ $f^{(1)}(X)$ γράφομε $f'(X)$. Θεωροῦμε γνωστὸ τὸ *ἀνάπτυγμα Taylor* γιὰ πολυώνυμα[4]. Γιὰ κάθε x_0, ἰσχύει ἡ ταυτότητα

$$f(X) = f(x_0) + f'(x_0)(X - x_0) + \frac{1}{2!}f^{(2)}(x_0)(X - x_0)^2 + \cdots \frac{1}{k!}f^{(k)}(x_0)(X - x_0)^k + \cdots ,$$

ὅπου τὸ ἄθροισμα στὸ δεξιὸ μέλος εἶναι πεπερασμένο, ἀφοῦ ὅταν τὸ k ὑπερβεῖ τὸν βαθμὸ τοῦ $f(X)$, τότε $f^{(k)}(X)$ εἶναι τὸ μηδενικὸ πολυώνυμο. Ἐπιπλέον, οἱ συντελεστὲς καθενὸς πολυωνύμου $\frac{1}{k!}f^{(k)}(X)$ εἶναι ἀκέραιοι.

[3] Ἡ παράγωγος ἑνὸς πολυωνύμου $f(X) = a_nX^n + \cdots + a_1X + a_0$ μπορεῖ νὰ ὁρισθεῖ *τυπικά*, δίχως χρήση συνεχείας, ὡς $na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots 2a_2X + a_1$, ἡ δεύτερη παράγωγος ὡς ἡ παράγωγος τῆς παραγώγου κ.ὅ.κ.

[4] Ὁ τύπος τοῦ ἀναπτύγματος Taylor γιὰ πολυώνυμα εἶναι ἀνεξάρτητος ἀπὸ τὸ ἀξίωμα συνεχείας καὶ μπορεῖ νὰ ἀποδειχθεῖ ἐπαγωγικά, δίχως χρήση Ἀπειροστικοῦ Λογισμοῦ.

Πρὶν προχωρήσομε, κάνομε τὴν προφανῆ παρατήρηση ὅτι, ἂν $x \equiv x_0 \pmod{p^a}$ εἶναι λύση τῆς (3.5), τότε $x \equiv x_0 \pmod{p^{a-1}}$ εἶναι λύση τῆς

$$f(x) \equiv 0 \pmod{p^{a-1}}\,. \tag{3.6}$$

Ἄρα, κάθε λύση τῆς (3.5) προέρχεται ἀπὸ λύση τῆς (3.6). Συνεπῶς, ὅταν ἀναζητοῦμε τὶς λύσεις τῆς (3.5), πρέπει νὰ ξεκινήσομε ἀπὸ μία-μία τὶς λύσεις τῆς (3.6) καὶ νὰ δοῦμε, γιὰ κάθε μία ἀπὸ αὐτές, ἂν παράγει λύσεις τῆς (3.5) καὶ ἂν ναί, πόσες.

Θεώρημα 3.4.2 *Ἔστω $a \geq 2$ καὶ $x_0 \bmod p^{a-1}$ λύση τῆς $f(x) \equiv 0 \pmod{p^{a-1}}$.*

α΄. Ἂν $f'(x_0) \not\equiv 0 \pmod p$, τότε, ἡ λύση $x_0 \bmod p^{a-1}$ τῆς (3.6) παράγει μία ἀκριβῶς λύση τῆς (3.5).

β΄. Ἂν $f'(x_0) \equiv 0 \pmod p$ καὶ $f(x_0) \equiv 0 \pmod{p^a}$, τότε, ἡ λύση $x_0 \bmod p^{a-1}$ τῆς (3.6) παράγει p ἀκριβῶς λύσεις τῆς (3.5) καί, συγκεκριμένα τὶς $x_0 + kp^{a-1} \bmod p^a$, $k = 0, 1, \ldots, p-1$.

γ΄. Ἂν $f'(x_0) \equiv 0 \pmod p$ καὶ $f(x_0) \not\equiv 0 \pmod{p^a}$, τότε, προφανῶς, ἡ λύση $x_0 \bmod p^{a-1}$ τῆς (3.6) δὲν παράγει λύσεις γιὰ τὴν (3.5).

Ἀπόδειξη Οἱ τυχὸν λύσεις τῆς (3.5), ποὺ παράγονται ἀπὸ τὴ λύση $x_0 \bmod p^{a-1}$ τῆς (3.6), ἔχουν τὴ μορφὴ $x = x_0 + yp^{a-1}$, ὅπου τὸ y εἶναι προσδιοριστέο.

α΄. Ἡ ἀντικατάσταση $X \leftarrow x_0 + yp^{a-1}$ στὸ ἀνάπτυγμα Taylor τοῦ $f(X)$ μᾶς δίνει

$$f(x) \equiv f(x_0) + f'(x_0)yp^{a-1} \pmod{p^a}\,, \tag{3.7}$$

διότι οἱ ὑπόλοιπο ὅροι στὸ δεξιὸ μέλος εἶναι τῆς μορφῆς $\frac{1}{k!}f^{(k)}(x_0)y^k p^{k(a-1)}$, ὅπου ὁ εκθέτης τοῦ p εἶναι $k(a-1) \geq a$ καὶ ὁ συντελεστὴς τοῦ $p^{k(a-1)}$ εἶναι ἀκέραιος. Συνεπῶς, ἡ σχέση $f(x) \equiv 0 \pmod{p^a}$ ἰσοδυναμεῖ μὲ τὴν

$$f'(x_0)y \equiv -\frac{f(x_0)}{p^{a-1}} \pmod p\,,$$

ὅπου, βέβαια, τὸ δεξιὸ μέλος εἶναι ἀκέραιος, λόγῳ τῆς ὑποθέσεως $f(x_0) \equiv 0 \pmod{p^{a-1}}$. Ἡ παραπάνω ὡς πρὸς y ἰσοτιμία ἔχει μία ἀκριβῶς λύση $y_0 \bmod p$, βάσει τοῦ θεωρήματος 3.2.1. Ἄρα, ἡ γενικὴ μορφὴ τοῦ y εἶναι $y = y_0 + zp$, ὁπότε ἡ γενικὴ μορφὴ τοῦ x εἶναι $x = x_0 + (y_0 + zp)p^{a-1} \equiv x_0 + y_0 p^{a-1} \pmod{p^a}$, ἀπ' ὅπου φαίνεται ὅτι εἶναι μοναδικὴ μέτρῳ p^a.

β΄. Ὅπως καὶ στὴν προηγούμενη περίπτωση, καταλήγομε στὴ σχέση (3.7). Λόγῳ τῶν ὑποθέσεων $f(x_0) \equiv 0 \pmod{p^a}$ καὶ $f'(x_0) \equiv 0 \pmod p$, τὸ ἀριστερὸ μέλος εἶναι ἰσότιμο μὲ τὸ 0 μέτρῳ p^a, ὁποιαδήποτε τιμὴ κι ἂν ἔχει τὸ y. Ἂν $y = zp + y_0$, ὅπου y_0 εἶναι τὸ ὑπόλοιπο τῆς εὐκλείδειας διαίρεσης τοῦ y διὰ p, τότε, ἡ γενικὴ μορφὴ τοῦ x εἶναι $x = x_0 + (y_0 + zp)p^{a-1} \equiv x_0 + y_0 p^{a-1} \pmod{p^a}$, ὁπότε, γιὰ κάθε τιμὴ $y_0 = 0, 1, \ldots, p-1$, παίρνομε μία διαφορετικὴ μέτρῳ p^a λύση τῆς (3.5).

γ΄. Ὁ ἰσχυρισμὸς εἶναι τετριμμένος.

ὅ.ἔ.δ.

Παράδειγμα Νὰ λυθεῖ ἡ ἰσοτιμία

$$f(x) = x^5 + 2x^4 + 2x^3 + 6x^2 - 52x - 49 \equiv 0 \pmod{7^3}.$$

Μὲ δοκιμὲς διαπιστώνομε ὅτι ἡ ἰσοτιμία $f(x) \equiv 0 \pmod 7$ ἔχει τέσσερεις ἀκριβῶς λύσεις, τὶς $0 \bmod 7$, $2 \bmod 7$, $3 \bmod 7$ καὶ $5 \bmod 7$.

Ἔστω $x \equiv 2 \pmod 7$. Ὑπολογίζομε ὅτι $f'(2) \equiv 0 \pmod 7$ καὶ $f(2) \equiv 0 \pmod{7^2}$, ἄρα ἡ λύση $2 \bmod 7$ παράγει ἑπτὰ διαφορετικὲς λύσεις τῆς $f(x) \equiv 0 \pmod{7^2}$, οἱ ὁποῖες, σύμφωνα μὲ τὴν ἀπόδειξη τοῦ β′ μέρους τοῦ θεωρήματος, εἶναι οἱ $2 + 7y_0 \bmod 7^2$, ὅπου $y_0 = 0, \dots, 6$, δηλαδή, οἱ

$$x \equiv 2, 9, 16, 23, 30, 37, 44 \pmod{7^2}.$$

Ὑπολογίζομε ὅτι $f(16), f(30) \equiv 0 \pmod{7^3}$, ἐνῶ καμμία ἀπὸ τὶς ὑπόλοιπες τιμὲς δὲν μηδενίζει τὸ $f(X)$ μέτρῳ 7^3. Συνεπῶς, ἀπὸ τὴ λύση $2 \bmod 7$ τῆς $f(x) \equiv 0 \pmod 7$ παράγονται οἱ λύσεις $16 + 7^2 y_0 \bmod 7^3$ καὶ $30 + 7^2 y_0 \bmod 7^3$ τῆς $f(x) \equiv 0 \pmod{7^3}$, ὅπου τὸ y_0 διατρέχει τὶς τιμὲς $0, 1, \dots, 6$. Παίρνομε ἔτσι τὶς ἑξῆς δεκατέσσερεις λύσεις τῆς $f(x) \equiv 0 \pmod{7^3}$, ἐκ τῶν ὁποίων, οἱ πρῶτες ἑπτὰ προέρχονται ἀπὸ τὴν $16 \bmod 7^2$ καὶ οἱ ὑπόλοιπες ἑπτὰ ἀπὸ τὴν $30 \bmod 7^2$:

$$x \equiv 16, 65, 114, 163, 212, 261, 310, 30, 79, 128, 177, 226, 275, 324 \pmod{7^3}$$

Ἔστω $x \equiv 3 \pmod 7$. Τώρα $f'(3) \not\equiv 0 \pmod 7$, ἄρα ἡ λύση $3 \bmod 7$ τῆς $f(x) \equiv 0 \pmod 7$ παράγει ἀκριβῶς μία λύση τῆς $f(x) \equiv 0 \pmod{7^2}$ καὶ ἡ ἀπόδειξη τοῦ α′ μέρους τοῦ θεωρήματος μᾶς ὑποδεικνύει, ἀκριβῶς, πῶς πρέπει νὰ ἐργασθοῦμε. Ἡ σχέση (3.7) γίνεται στὴν περίπτωσή μας, $659y \equiv -44 \pmod 7$, δηλαδή, ἰσοδύναμα, $y \equiv 5 \pmod 7$. Ἕπεται ὅτι, $x \equiv 3 + 5 \cdot 7 \equiv 38 \pmod{7^2}$. Ἡ λύση $38 \bmod 7^2$ παράγει μία, ἀκριβῶς, λύση τῆς $f(x) \equiv 0 \pmod{7^3}$, μὲ ἀνάλογη διαδικασία. Τώρα ἡ σχέση (3.7) γίνεται $10873724y \equiv -1704527 \pmod 7$, δηλαδή, ἰσοδύναμα, $y \equiv 1 \pmod 7$. Ἄρα, $x \equiv 38 + 1 \cdot 7^2 \equiv 87 \pmod{7^3}$ καὶ αὐτὴ εἶναι ἡ μία καὶ μοναδικὴ λύση τῆς $f(x) \equiv 0 \pmod{7^3}$, ποὺ παράγεται ἀπὸ τὴ λύση $3 \bmod 7$ τῆς $f(x) \equiv 0 \pmod 7$.

Οἱ περιπτώσεις $x \equiv 0 \pmod 7$ καὶ $x \equiv 5 \pmod 7$ εἶναι ἀνάλογες μὲ τὴν περίπτωση $x \equiv 3 \pmod 7$. Οἱ λύσεις τῆς $f(x) \equiv 0 \pmod{7^3}$, ποὺ παράγονται, εἶναι ἡ $98 \bmod 7^3$ ἀπὸ τὴν πρώτη καὶ $12 \bmod 7^3$ ἀπὸ τὴ δεύτερη. Οἱ ὑπολογισμοὶ προτείνονται ὡς καλὴ ἐξάσκηση γιὰ τὸν ἀναγνώστη.

Ἡ ἐπίλυση τῆς $f(x) \equiv 0 \pmod m$ στὴ γενικὴ περίπτωση μέτρου $m > 1$ γίνεται ὡς ἑξῆς: Ἂν $m = p_1^{a_1} \cdots p_k^{a_k}$ εἶναι ἡ κανονικὴ ἀνάλυση τοῦ m, τότε λύνομε πρῶτα κάθε μία ἀπὸ τὶς ἰσοτιμίες $f(x) \equiv 0 \pmod{p_i^{a_i}}$, $i = 1, \dots, k$. Ἄν, ἔστω καὶ μία ἀπὸ τὶς ἰσοτιμίες αὐτὲς δὲν ἔχει λύση, τότε, ἡ ἀρχικὴ ἰσοτιμία δὲν ἔχει λύση. Διαφορετικά, ἔστω S_i, $(i = 1, \dots, k)$ τὸ σύνολο τῶν λύσεων τῆς $f(x) \equiv 0 \pmod{p_i^{a_i}}$. Γιὰ κάθε $(x_1, \dots, x_k) \in S_1 \times \cdots \times S_k$ ἐπιλύομε τὸ σύστημα $x \equiv x_i \pmod{p_i^{a_i}}$, $(i = 1, \dots, k)$, τὸ ὁποῖο, βάσει τοῦ «κινέζικου θεωρήματος» 3.3.1, ἔχει ἀκριβῶς μία λύση $x_0 \bmod m$. Φυσικά, ἡ τιμὴ x_0 ἐξαρτᾶται ἀπὸ τὴν k-άδα $(x_1, \ldots, x_k)$. Τὸ πλῆθος τῶν λύσεων τῆς $f(x) \equiv 0 \pmod m$ ἰσοῦται μὲ τὸν πληθάριθμο τοῦ $S_1 \times \cdots \times S_k$, δηλαδή, μὲ $|S_1| \cdots |S_k|$.

Παράδειγμα. Θὰ λύσομε τὴν ἰσοτιμία $f(x) = x^4 + x^3 - 13x^2 + 10x + 55 \equiv 0 \pmod m$, ὅπου $m = 2^4 \cdot 3^3 \cdot 11^3$. Μοναδικὴ λύση τῆς $f(x) \equiv 0 \pmod{2^4}$ εἶναι ἡ $15 \bmod 16$. Ἡ ἰσοτιμία $f(x) \equiv 0 \pmod{3^3}$ ἔχει τρεῖς λύσεις: $x \equiv 1, 10, 19 \pmod{27}$. Ἡ ἰσοτιμία $f(x) \equiv 0 \pmod{11^3}$ ἔχει, ἐπίσης, μία μόνο λύση, τὴν $1265 \bmod 1331$. Συνεπῶς, τὸ πλῆθος τῶν λύσεων τῆς $f(x) \equiv 0 \pmod m$ εἶναι $1 \cdot 3 \cdot 1 = 3$, οἱ ὁποῖες εὑρίσκονται˙ ἀντιστοίχως, ἀπὸ τὶς ἐπιλύσεις τῶν τριῶν συστημάτων

$$\begin{array}{llllll} x \equiv 15 & \pmod{16}, & x \equiv 1 & \pmod{27}, & x \equiv 1265 & \pmod{1331} \\ x \equiv 15 & \pmod{16}, & x \equiv 10 & \pmod{27}, & x \equiv 1265 & \pmod{1331} \\ x \equiv 15 & \pmod{16}, & x \equiv 19 & \pmod{27}, & x \equiv 1265 & \pmod{1331} \end{array}$$

Ἐφαρμόζοντας τὸ «κινέζικο θεώρημα» στὰ παραπάνω τρία συστήματα βρίσκομε, ἀντιστοίχως, τὶς λύσεις $x \equiv 461791,\ 270127,\ 78463 \pmod{2^4 \cdot 3^3 \cdot 11^3}$.

3.5 Ἀσκήσεις τοῦ κεφαλαίου 3

1. Νὰ λυθεῖ χωριστὰ κάθε μία ἀπ' τὶς ἰσοτιμίες $412x \equiv 108 \pmod{34}$ καὶ $33900x \equiv 56935 \pmod{2995}$. Μετά, νὰ ὑπολογισθοῦν ὅλες οἱ ἀνισότιμες μέτρῳ $2995 \cdot 34$ τιμὲς τοῦ x, οἱ ὁποῖες ἐπαληθεύουν συγχρόνως καὶ τὶς δύο ἰσοτιμίες.

2. Θεωροῦμε τοὺς πρώτους ἀριθμοὺς $p_1 = 29$, $p_2 = 71$ καὶ $p_3 = 113$. Σὲ ὅ,τι ἀκολουθεῖ, οἱ δεῖκτες i, j, k παίρνουν τιμὲς ἀπὸ τὸ $\{1, 2, 3\}$ καὶ εἶναι διαφορετικοὶ ἀνὰ δύο.
   Νὰ βρεθεῖ ἀκέραιος a ἀνάμεσα στὸ 200000 καὶ τὸ 300000, μὲ τὴν ἑξῆς ἰδιότητα: Γιὰ κάθε $i = 1, 2, 3$, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ a διὰ p_i ἰσοῦται μὲ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ $p_j p_k$ διὰ p_i.
   Ὑπόδειξη: Ὁ a ἱκανοποιεῖ, συγχρόνως, τρεῖς ἰσοτιμίες, οἱ ὁποῖες πρέπει νὰ ἐπιλυθοῦν μὲ τὸ «κινέζικο θεώρημα».

3. Νὰ λυθεῖ τὸ σύστημα

$$2x + 11y \equiv 5 \pmod{493}, \quad 3x - 7y \equiv 1 \pmod{493}.$$

4. Ἔστω περιττὸς πρῶτος p καὶ $(a, p) = 1$. Ἀποδεῖξτε ὅτι, ἂν $x_0^2 \equiv a \pmod p$, τότε, ἡ ἰσοτιμία $x^2 \equiv a \pmod p$ ἔχει ἀκριβῶς δύο ἀνισότιμες $\bmod p$ λύσεις: Τὶς $\pm x_0 \pmod p$.
   Ὑπόδειξη: Ἐφαρμόστε τὸ Θεώρημα 3.4.1 στὸ πολυώνυμο $X^2 - a$.

5. Ἔστω

$$\begin{aligned} f(X) = & 132X^{17} + 4X^{16} + 15X^{15} + X^{14} + 11X^{13} + 2X^{12} + 5X^{11} + 3X^{10} \\ & + 1001X^9 + X^8 + 1234X^7 + 2X^6 + 1821X^5 + 13X^4 + 111X^3 \\ & + 12X^2 + 17X + 1\,. \end{aligned}$$

   Ἐπιλῦστε τὴν ἰσοτιμία $f(x) \equiv 0 \pmod 7$, ἀφοῦ πρῶτα βρεῖτε ἕνα πολυώνυμο $g(X)$, βαθμοῦ μικρότερου τοῦ 7, τέτοιο ὥστε, ἡ ἰσοτιμία $g(x) \equiv 0 \pmod 7$ νὰ ἔχει τὶς ἴδιες λύσεις μὲ τὴν $f(x) \equiv 0 \pmod 7$.

6. Νὰ ἐπιλυθεῖ ἡ ἰσοτιμία $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 \pmod{625}$.

7. Ἔστω $p > 2$ πρῶτος. Θέτομε $s_1 = \sum_{1\le i\le p-1} i$, $s_2 = \sum_{1\le i<j\le p-1} ij$ καί, γενικότερα, γιὰ $k \le p-1$, s_k εἶναι τὸ ἄθροισμα ὅλων τῶν δυνατῶν γινομένων k διαφορετικῶν ἀριθμῶν τοῦ συνόλου $\{1, 2, \dots, p-1\}$· εἰδικώτερα, $s_{p-1} = (p-1)!$. Ἀποδεῖξτε ὅτι τὸ πολυώνυμο

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

   εἶναι βαθμοῦ $p-2$ καὶ ἡ ἰσοτιμία $f(x) \equiv 0 \pmod p$ ἔχει $p-1$ διαφορετικὲς λύσεις. Ὕστερα, κάνοντας χρήση τῆς ταυτότητας

$$(X-1)(X-2)\cdots(X-p+1) = X^{p-1} - s_1X^{p-1} + \cdots - s_{p-2} + s_{p-1}$$

   καὶ τοῦ θεωρήματος 3.4.1, ἀποδεῖξτε ὅτι

$$s_1 \equiv s_2 \equiv \cdots \equiv s_{p-2} \equiv 0 \pmod p \quad \text{καὶ} \quad (p-1)! \equiv -1 \pmod p\,.$$

   Ἡ τελευταία ἀπὸ τὶς παραπάνω ἰσοτιμίες εἶναι γνωστὴ ὡς *θεώρημα τοῦ Wilson*, μία ἄλλη ἀπόδειξη τοῦ ὁποίου δίνεται στὴν ἄσκηση 13 τοῦ κεφαλαίου 2.

8. Ἔστω p πρῶτος.

   α΄. Ἔστω $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, ὅπου $1 \le n < p$. Ἀποδεῖξτε ὅτι, ἀναγκαία καὶ ἱκανὴ συνθήκη γιὰ νὰ ἔχει ἡ ἰσοτιμία $f(x) \equiv 0 \pmod p$ n διαφορετικὲς λύσεις εἶναι ἡ ἑξῆς: Τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ $X^p - X$ διὰ τοῦ $f(X)$ εἶναι πολυώνυμο μὲ ὅλους τοὺς συντελεστές του διαιρετοὺς διὰ p.
   Ὑπόδειξη: Ἔστω $X^p - X = f(X)g(X) + r(X)$ μὲ $\deg r(X) < n$. Κατ' ἀρχάς, παρατηρῆστε ὅτι τὸ $g(X)$ εἶναι βαθμοῦ $p-n$. Γιὰ νὰ ἀποδείξετε ὅτι ἡ συνθήκη εἶναι ἀναγκαία, παρατηρῆστε ὅτι, ἂν οἱ $x_1, \dots x_n$ εἶναι ἀνισότιμοι μέτρῳ p καὶ $f(x_i) \equiv 0 \pmod p$ γιὰ $i = 1, \dots, n$, τότε καὶ $r(x_i) \equiv 0 \pmod p$ γιὰ $i = 1, \dots, n$. Γιὰ τὸ ἀντίστροφο παρατηρῆστε ὅτι, ἂν ὅλοι οἱ συντελεστὲς τοῦ $r(X)$ εἶναι διαιρετοὶ διὰ p, τότε, $f(k)g(k) \equiv 0 \pmod p$ γιὰ κάθε $k = 0, 1, \dots, p-1$. Ἂν $f(k) \equiv 0 \pmod p$ γιὰ λιγώτερες ἀπὸ n τιμὲς τοῦ k, τότε .... Καὶ μὴ ξεχᾶστε ὅτι τὸ $g(X)$ εἶναι βαθμοῦ $p-n$.

β′. Ἔστω $a \not\equiv 0 \pmod p$ καὶ $n > 1$ διαιρέτης τοῦ $p-1$. Ἀποδεῖξτε ὅτι ἡ ἰσοτιμία $x^n \equiv a \pmod p$ ἔχει λύση ἄν, καὶ μόνο ἄν, $a^{\frac{p-1}{n}} \equiv 1 \pmod p$. Στὴν περίπτωση δέ, ποὺ ἔχει λύση, τὸ πλῆθος τῶν διαφορετικῶν λύσεων εἶναι ἀκριβῶς n.
Ὑπόδειξη: Τὸ ἀναγκαῖο τῆς συνθήκης εἶναι εὔκολο. Γιὰ τὸ ἱκανὸ θὰ κάνετε χρήση τῆς ταυτότητας

$$\begin{aligned} X^p - X =& X(X^{p-1} - 1) = X(X^{p-1} - a^{\frac{p-1}{n}} + a^{\frac{p-1}{n}} - 1) \\ =& X\left((X^n)^{\frac{p-1}{n}} - a^{\frac{p-1}{n}} + a^{\frac{p-1}{n}} - 1\right) = (X^n - a)(\cdots) + (a^{\frac{p-1}{n}} - 1)X\,, \end{aligned}$$

ὅπου $(\cdots)$ εἶναι κάποιο πολυώνυμο, ἡ ἀκριβὴς τιμὴ τοῦ ὁποίου δὲν ἔχει σημασία. Ἡ ταυτότητα αὐτὴ σᾶς δείχνει ποιὸ εἶναι τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ $X^p - X$ διὰ τοῦ $X^n - a$ καὶ τώρα, θὰ κάνετε χρήση τοῦ (α′).

9. Ἡ ἄσκηση αὐτὴ δείχνει πῶς μποροῦμε νὰ ἐπεκτείνομε στὶς ἰσοτιμίες τὸν κλασματικὸ συμβολισμό. Ὁ $m \geq 2$ εἶναι τὸ μέτρο καὶ ὁποτεδήποτε ἐμφανίζονται παρονομαστὲς σὲ ἰσοτιμίες, ἢ ἀκέραιοι μὲ ἀρνητικὸ ἐκθέτη, ἐννοεῖται, δίχως νὰ λέγεται, ὅτι αὐτοὶ εἶναι πρῶτοι πρὸς τὸν m.

   Οἱ συμβολισμοὶ $a^{-1} \bmod m$ καὶ $\frac{1}{a} \bmod m$ σημαίνουν, ἐξ ὁρισμοῦ, τὴ μοναδικὴ κλάση $a' \bmod m$, γιὰ τὴν ὁποία $aa' \equiv 1 \pmod m$. Συνακόλουθοι συμβολισμοὶ εἶναι οἱ $ba^{-1} \bmod m$, $a^{-1}b \bmod m$ καὶ $\frac{b}{a} \bmod m$, ποὺ σημαίνουν, καὶ οἱ τρεῖς, τὴν κλάση $a'b \bmod m$.
   Ἀποδεῖξτε τὶς ἑξῆς ἰδιότητες:

   (α′) $\dfrac{b}{a} \equiv c \pmod m \Leftrightarrow b \equiv ac \pmod m$.

   (β′) $\dfrac{b_1}{a_1} \equiv \dfrac{b_2}{a_2} \pmod m \Leftrightarrow b_1a_2 \equiv b_2a_1 \pmod m$.

   (γ′) $\dfrac{cb}{ca} \equiv \dfrac{b}{a} \pmod m$.

   (δ′) $\dfrac{b_1}{a_1} + \dfrac{b_2}{a_2} \equiv \dfrac{b_1a_2 + b_2a_1}{a_1a_2} \pmod m$ καὶ $\dfrac{b_1}{a_1} \cdot \dfrac{b_2}{a_2} \equiv \dfrac{b_1b_2}{a_1a_2} \pmod m$.

   (ε′) Γιὰ θετικὸ ἀκέραιο n, $(a^{-1})^n \equiv (a^n)^{-1} \pmod m$. Συμβολίζομε μὲ $a^{-n} \bmod m$ τὴν κλάση $(a^{-1})^n \bmod m$.

   (ϛ′) Γιὰ ὁποιουσδήποτε ἀκεραίους k, n -θετικούς, ἀρνητικοὺς ἢ μηδέν- ἰσχύουν οἱ σχέσεις $(a^k)^n \equiv a^{kn} \pmod m$ καὶ $a^k a^n \equiv a^{k+n} \pmod m$.

10. Στὴν ἄσκηση αὐτὴ γίνεται χρήση κλασματικοῦ συμβολισμοῦ σὲ ἰσοτιμίες, ὁπότε πρέπει νὰ δεῖτε πρῶτα τὴν ἄσκηση 9.

    Γιὰ κάθε πρῶτο $p \geq 5$ ἰσχύει $1 + \frac{1}{2} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$.
    Ὑπόδειξη: Σύμφωνα μὲ τὴν ἄσκηση 9 πρέπει καὶ ἀρκεῖ νὰ ἀποδειχθεῖ ὅτι ὁ ἀριθμητὴς τοῦ κλάσματος, ποὺ προκύπτει ὅταν ἀθροίσομε τὸ ἀριστερὸ μέλος, διαιρεῖται

διὰ p^2. Τὸν ἀριθμητὴ αὐτὸν συναντοῦμε στὸ πολυώνυμο $g(X) = (X-1)(X-2)\cdots(X-p+1)$· ποῦ; Ὑπολογῖστε τὴν τιμὴ $g(p)$ καὶ χρησιμοποιεῖστε τὴν ἄσκηση 7.

Κεφάλαιο 4

Τετραγωνικὰ ἰσοϋπόλοιπα

Στὸ κεφάλαιο αὐτό, τὰ p, q συμβολίζουν πάντα περιττοὺς πρώτους.
Τα λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους

4.1 Ὁρισμοὶ καὶ βασικὲς ἰδιότητες

Ἔστω ἀκέραιος $m > 1$ καὶ a πρῶτος πρὸς τὸν m. Ἂν ἡ ἰσοτιμία $x^2 \equiv a \pmod{m}$ ἔχει λύση, τότε ὁ a χαρακτηρίζεται *τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ* m ,διαφορετικά, *τετραγωνικὸ ἀνισοϋπόλοιπο μέτρῳ* m. Ἂν $a \equiv b \pmod{m}$, εἶναι προφανὲς ὅτι ὁ b εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ m ἄν, καὶ μόνο ἄν, ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ m. Συνήθως θὰ παραλείπομε τὸν προσδιορισμὸ «μέτρῳ ...» ὅταν εἶναι σαφὲς τὸ μέτρο, ὡς πρὸς τὸ ὁποῖο ἐργαζόμαστε.

Στὴν εἰδικώτερη περίπτωση, ποὺ $m = p$, περιττὸς πρῶτος, ἂν ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ p καὶ $x_0 \bmod p$ εἶναι μία λύση τῆς ἰσοτιμίας $x^2 \equiv a \pmod{p}$, τότε $-x_0 \bmod p$ εἶναι, ἐπίσης, λύση τῆς ἴδιας ἰσοτιμίας, διαφορετικὴ ἀπὸ τὴν $x_0 \bmod p$. Πράγματι, ἐξ ὑποθέσεως, $(a, p) = 1$, ἄρα $x_0 \not\equiv 0 \pmod{p}$. Ἀκόμη, ἐπειδὴ ὁ p εἶναι περιττός, $2x_0 \not\equiv 0 \pmod{p}$, ἄρα $x_0 \not\equiv -x_0 \pmod{p}$. Ἐξ ἄλλου, τὸ θεώρημα 3.4.1 μᾶς λέει ὅτι ἡ $x^2 \equiv a \pmod{p}$ ἔχει, τὸ πολύ, δύο διαφορετικὲς λύσεις, ἄρα, βάσει καὶ τῶν παραπάνω, ἔχει *ἀκριβῶς δύο* λύσεις.

Θεώρημα 4.1.1 *Ἔστω περιττὸς πρῶτος p.*
α΄. Ἕνα περιορισμένο σύστημα ὑπολοίπων μέτρῳ p περιέχει ἀκριβῶς $\frac{p-1}{2}$ τὸ πλῆθος τετραγωνικὰ ἰσοϋπόλοιπα, τὰ ὁποῖα εἶναι ἰσότιμα μὲ τοὺς ἀριθμοὺς

$$1^2,\ 2^2,\ \ldots,(\frac{p-1}{2})^2\,. \tag{4.1}$$

β΄. Ἔστω $(a, p) = 1$. Ἂν ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ p, τότε

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}\,, \tag{4.2}$$

ἐνῶ, ἂν ὁ a εἶναι τετραγωνικὸ ἀνισοϋπόλοιπο,

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{4.3}$$

Ἀπόδειξη α′. Καθένας ἀπὸ τοὺς ἀριθμοὺς (4.1) εἶναι, προφανῶς, τετραγωνικὸ ἰσοϋπόλοιπο. Ἐπίσης, οἱ ἀριθμοὶ αὐτοὶ εἶναι ἀνισότιμοι μεταξύ τους. Πράγματι, ἂν $1 \le \ell < k \le \frac{p-1}{2}$ καὶ συνέβαινε νὰ ἰσχύει $k^2 \equiv \ell^2 \pmod{p}$, τότε ὁ p θὰ ἔπρεπε νὰ διαιρεῖ ἕναν ἀπὸ τοὺς $k+\ell$ καὶ $k-\ell$, κάτι ἀδύνατον, ἀφοῦ καὶ οἱ δύο αὐτοὶ ἀριθμοὶ εἶναι θετικοὶ καὶ μικρότεροι τοῦ p.

Συνεπῶς, ἂν R εἶναι ἕνα περιορισμένο σύστημα ὑπολοίπων μέτρῳ p, τότε κάθε ἀριθμὸς k στὴν (4.1) εἶναι ἰσότιμος μὲ ἕνα διαφορετικὸ ἀριθμὸ $r_k \in R$ καί, φυσικά, ὁ r_k εἶναι τετραγωνικὸ ἰσοϋπόλοιπο. Ἀντίστροφα, ἔστω $r \in R$ τετραγωνικὸ ἰσοϋπόλοιπο. Τότε ὑπάρχει $k \in \{1, \dots, p-1\}$, τέτοιος ὥστε $k^2 \equiv r \pmod{p}$. Ἂν $1 \le k \le \frac{p-1}{2}$, τότε ὁ r εἶναι ἰσότιμος πρὸς κάποιον ἀπὸ τοὺς ἀριθμοὺς (4.1)· διαφορετικά, παρατηροῦμε ὅτι $1 \le p-k \le \frac{p-1}{2}$ καὶ $r \equiv k^2 \equiv (p-k)^2 \pmod{p}$.
β′. Ἂν ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο, τότε ὑπάρχει x_0, τέτοιος ὥστε $a \equiv x_0^2 \pmod{p}$ καί, βεβαίως, $(x_0, p) = 1$. Ἄρα, ἀπὸ τὸ θεώρημα τοῦ Fermat (β′ τοῦ θεωρήματος 2.2.4),

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod{p}.$$

Πρὶν προχωρήσομε, ἂς παρατηρήσομε ὅτι, γιὰ κάθε a ἀπὸ τὸ σύνολο ἀριθμῶν (4.1), ἰσχύει ἡ σχέση (4.2), ἄρα ἡ ἰσοτιμία

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p} \tag{4.4}$$

ἔχει τουλάχιστον $\frac{p-1}{2}$ τὸ πλῆθος λύσεις. Ἀπὸ τὸ θεώρημα 3.4.1, δὲν μπορεῖ νὰ ἔχει περισσότερες, ἄρα, οἱ κλάσεις τῶν ἀριθμῶν (4.1), καὶ μόνον αὐτές, εἶναι οἱ λύσεις τῆς ἰσοτιμίας (4.4). Αὐτό, ὅμως, συνεπάγεται ὅτι, ἂν κάποιος a εἶναι τετραγωνικὸ ἀνισοϋπόλοιπο, τότε ἡ κλάση $a \bmod p$ δὲν εἶναι λύση τῆς (4.4) Ἀπὸ τὴν ἄλλη, τὸ θεώρημα τοῦ Fermat, λέει ὅτι $a^{p-1} - 1 \equiv 0 \pmod{p}$ καί, παραγοντοποιώντας τὸ ἀριστερὸ μέλος καταλήγομε στὸ συμπέρασμα ὅτι ὁ p διαιρεῖ ἕναν ἀπὸ τοὺς $a^{(p-1)/2} - 1$, $a^{(p-1)/2} + 1$. Τὸ πρῶτο ἐνδεχόμενο συνεπάγεται ὅτι ἡ $a \bmod p$ εἶναι λύση τῆς (4.4), ὁπότε ἀποκλείεται, βάσει τῶν ὅσων μόλις εἴπαμε παραπάνω. Ἔτσι, μένει τὸ δεύτερο ἐνδεχόμενο, ποὺ ἰσοδυναμεῖ, προφανῶς, μὲ τὴ σχέση (4.3). **ὅ.ἔ.δ.**

4.2 Τὸ σύμβολο τοῦ Legendre

Στὴν παράγραφο αὐτὴ τα λατινικὰ γράμματα, ποὺ δὲν εἶναι ὑποδεῖκτες, συμβολίζουν πάντα ἀκεραίους πρώτους πρὸς τὸν p.

Τὸ σύμβολο *Legendre τοῦ a ὡς πρὸς p* ὁρίζεται ὡς ἑξῆς:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ἂν } a \text{ τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ } p \\ -1 & \text{ἂν } a \text{ τετραγωνικὸ ἀνισοϋπόλοιπο μέτρῳ } p. \end{cases}$$

Οἱ πρῶτες στοιχειώδεις ἰδιότητες τοῦ συμβόλου τοῦ Legendre συνοψίζονται στὴν παρακάτω πρόταση.

Πρόταση 4.2.1 *α΄.* $\left(\frac{a^2}{p}\right) = 1$. *Εἰδικώτερα,* $\left(\frac{1}{p}\right) = 1$.

β΄. *Ἂν* $a \equiv b \pmod{p}$, *τότε* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

γ΄. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

δ΄. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Μ' ἄλλα λόγια, τὸ -1 εἶναι τετραγωνικὸ ἰσοϋπόλοιπο ἂν $p \equiv 1 \pmod{4}$ *καὶ τετραγωνικὸ ἀνισοϋπόλοιπο ἂν* $p \equiv 3 \pmod{4}$.

ε΄. $\left(\frac{a_1 a_2 \dots a_k}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_k}{p}\right)$.

Ἀπόδειξη Οἱ ἰσχυρισμοὶ (α΄) καὶ (β΄) εἶναι ἐντελῶς ἄμεσες συνέπειες τῶν ὁρισμῶν.

(γ΄). Προφανὴς συνδυασμὸς τοῦ ὁρισμοῦ τοῦ συμβόλου Legendre καὶ τοῦ β΄ τοῦ θεωρήματος 4.1.1.

(δ΄). Προφανὴς συνέπεια τοῦ (γ΄).

(ε΄). Ἐφαρμόζοντας τὸ (γ΄) ἔχομε

$$\left(\frac{a_1 \cdots a_k}{p}\right) \equiv (a_1 \cdots a_k)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdots a_k^{\frac{p-1}{2}} \equiv \left(\frac{a_1}{p}\right)\cdots\left(\frac{a_k}{p}\right) \pmod{p}.$$

Τὸ ἀριστερώτερο καὶ τὸ δεξιώτερο μέλος τῆς παραπάνω ἰσοτιμίας εἶναι ἴσα μὲ ± 1, ἄρα, ἀπὸ τὴν ἄσκηση 2, εἶναι ἴσα. **ὅ.ἔ.δ.**

Γιὰ νὰ ἁπλουστεύσομε τοὺς συμβολισμούς, θέτομε $p' = \frac{p-1}{2}$. Τὸ σύνολο $R = \{-p', \dots, -1, 1, \dots, p'\}$ εἶναι ἕνα περιορισμένο σύστημα ὑπολοίπων. Ἂν, λοιπόν, $k \in \{1, 2, \dots, p'\}$, τότε $(ak, p) = 1$, ὁπότε ὁ ka εἶναι ἰσότιμος μὲ κάποιον ἀριθμὸ τοῦ R. Ὁ ἀριθμὸς αὐτὸς τοῦ R εἶναι τῆς μορφῆς $\sigma_k r_k$, ὅπου $\sigma_k \in \{-1, 1\}$ καὶ $r_k \in \{1, \dots, p'\}$. Ἄρα, ἔχομε τὶς σχέσεις

$$\begin{aligned} 1 \cdot a &\equiv \sigma_1 r_1 \pmod{p} \\ 2 \cdot a &\equiv \sigma_2 r_2 \pmod{p} \\ &\vdots \\ p' \cdot a &\equiv \sigma_{p'} r_{p'} \pmod{p}. \end{aligned} \tag{4.5}$$

Ἀκόμη, τὰ $r_1, r_2, \ldots, r_{p'}$ εἶναι ὅλα διαφορετικὰ μεταξύ τους. Πράγματι, ἔστω $1 \le k < \ell \le p'$. Εἶναι, βέβαια, $ka \not\equiv \ell a \pmod p$, ἄρα, ἂν ἦταν $r_k = r_\ell$, αὐτὸ θὰ συνεπαγόταν ὅτι, τὸ ἕνα ἀπὸ τὰ σ_k, σ_ℓ θὰ ἦταν 1 καὶ τὸ ἄλλο -1. Αὐτὸ θὰ σήμαινε ὅτι $ka \equiv -\ell a (\mathrm{mod}\ p)$, δηλαδή, $(k+\ell)a \equiv 0 (\mathrm{mod}\ p)$· ἀδύνατον, ἀφοῦ, ἀφ' ἑνός, $(a,p)=1$ καί, ἀφ' ἑτέρου $2 \le k+\ell < p-1$.

Πολλαπλασιάζοντας τώρα τὶς σχέσεις (4.5) παίρνομε

$$(1 \cdot 2 \cdots p')a^{p'} \equiv (r_1 r_2 \cdots r_{p'})\sigma_1\sigma_2\cdots\sigma_{p'} \pmod p\,.$$

Σύμφωνα μὲ τὰ παραπάνω, ὅμως, οἱ ἀριθμοὶ $r_1, r_2, \ldots, r_{p'}$ εἶναι μία μετάθεση τῶν $1, 2, \ldots, p'$, ἄρα, $r_1 r_2 \cdots r_{p'} = 1 \cdot 2 \cdots p'$ καὶ διαιρώντας τὰ δύο μέλη μὲ τὸν ἀριθμὸ αὐτό, ποὺ εἶναι πρῶτος πρὸς τὸν p, καταλήγομε στὴ σχέση

$$a^{p'} \equiv \sigma_1\sigma_2\cdots\sigma_{p'} \pmod p\,.$$

Τὸ γ′ τοῦ θεωρήματος 4.2.1 μᾶς ἐπιτρέπει νὰ ἀντικαταστήσομε τὸ ἀριστερὸ μέλος μὲ τὸ $\left(\frac{a}{p}\right)$, ὁπότε καταλήγομε σὲ μία ἰσοτιμία, στὴν ὁποία, τὰ δύο μέλη εἶναι 1 ἢ -1. Ἄρα, ἡ ἰσοτιμία εἶναι ἰσότητα (ἄσκηση 2) καὶ καταλήγομε στὴ σχέση

$$\left(\frac{a}{p}\right) = \sigma_1\sigma_2\cdots\sigma_{p'}\,, \tag{4.6}$$

ἡ ὁποία θὰ μᾶς φανεῖ πολὺ χρήσιμη, ὅπως θὰ δοῦμε ἀμέσως τώρα.

Κατ' ἀρχάς, ὑπενθυμίζομε ὅτι, γιὰ $\alpha \in \mathbb{R}$, συμβολίζομε μὲ $[\alpha]$ καὶ $\{\alpha\}$ τὸ ἀκέραιο καὶ τὸ κλασματικὸ μέρος, ἀντιστοίχως, τοῦ α, ὁπότε $\alpha = [\alpha] + \{\alpha\}$. Εἶναι σαφὲς ὅτι, γιὰ ὁποιονδήποτε $\alpha \in \mathbb{R}$ καὶ ὁποιονδήποτε $b \in \mathbb{Z}$, ἰσχύει $[b+\alpha] = b + [\alpha]$.

Ἔστω τώρα θετικὸς ἀκέραιος a, πρῶτος πρὸς τὸν p. Ἂν $1 \le k \le p'$, τότε

$$\left[\frac{2ak}{p}\right] = \left[2\left[\frac{ak}{p}\right] + 2\left\{\frac{ak}{p}\right\}\right] = 2\left[\frac{ak}{p}\right] + \left[2\left\{\frac{ak}{p}\right\}\right].$$

Ἂν v_k εἶναι τὸ ὑπόλοιπο τῆς εὐκλείδειας διαίρεσης τοῦ ak διὰ p, τότε, προφανῶς, $\{\frac{ak}{p}\} = \frac{v_k}{p}$ καὶ τὸ τελευταῖο κλάσμα εἶναι ἀριθμὸς τοῦ διαστήματος [0, 0.5), ἢ τοῦ (0.5, 1), ἀνάλογα μὲ τὸ ἂν $v_k \le p'$ ἢ $v_k > p'$, ἀντιστοίχως. Ἂς παρατηρήσομε, ἐπίσης, ὅτι $v_k \le p' \Leftrightarrow \sigma_k = 1$, ἐνῶ $v_k > p' \Leftrightarrow \sigma_k = -1$.

$$\left[2\left\{\frac{ak}{p}\right\}\right] = \begin{cases} 0 & \text{ἂν } \sigma_k = 1 \\ 1 & \text{ἂν } \sigma_k = -1\,. \end{cases}$$

Ἄρα, συνδυάζοντας τὰ παραπάνω,

$$\left[\frac{2ak}{p}\right] = \begin{cases} \text{ἄρτιος} & \text{ἂν } \sigma_k = 1 \\ \text{περιττὸς} & \text{ἂν } \sigma_k = -1\,, \end{cases}$$

ὁπότε

$$\sigma_k = (-1)^{[\frac{2ak}{p}]}\,.$$

Συνδυάζοντας αὐτὴ τὴ σχέση μὲ τὴν (4.6) ὁδηγούμαστε στὸν πολὺ ἐνδιαφέροντα γενικὸ τύπο

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'}[\frac{2ak}{p}]} . \tag{4.7}$$

Μὲ τὴ βοήθεια τοῦ τύπου (4.7) θὰ ἀποδείξομε τὸν περίφημο *νόμο τῆς τετραγωνικῆς ἀντιστροφῆς τοῦ Gauss* καὶ τὸ *συμπλήρωμα* αὐτοῦ τοῦ νόμου, τὸ ὁποῖο καὶ θὰ ἀποδείξομε πρῶτο, ὡς ἁπλούστερο.

Θεώρημα 4.2.2 –Συμπλήρωμα τοῦ νόμου τετραγωνικῆς ἀντιστροφῆς.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} . \tag{4.8}$$

Συνεπῶς, τὸ 2 εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ p γιὰ πρώτους p τῆς μορφῆς $8n \pm 1$ καὶ τετραγωνικὸ ἀνισοϋπόλοιπο γιὰ πρώτους p τῆς μορφῆς $8n \pm 3$.

Ἀπόδειξη Θεωροῦμε ἕναν ὁποιονδήποτε θετικὸ περιττὸ ἀκέραιο a, πρῶτο πρὸς τὸν p. Θὰ κάνομε χρήση τοῦ τύπου (4.7) γιὰ $\frac{a+p}{2}$ στὴ θέση τοῦ a. Ἐπίσης, θὰ κάνομε χρήση τῶν ἰδιοτήτων α′ καὶ β′ τοῦ θεωρήματος 4.2.1. Ἔχομε λοιπόν,

$$\begin{aligned}\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) &= (-1)^{\sum_{k=1}^{p'}[\frac{(a+p)k}{p}]} \\ &= (-1)^{\sum_{k=1}^{p'}[\frac{ak}{p}]+\sum_{k=1}^{p'}k} \\ &= (-1)^{\sum_{k=1}^{p'}[\frac{ak}{p}]+\frac{p^2-1}{8}} .\end{aligned} \tag{4.9}$$

Ἂν στὴν παραπάνω σχέση θέσομε $a = 1$, τὸ πρῶτο ἄθροισμα στὸν ἐκθέτη τοῦ -1 (σχέση 4.9) εἶναι 0, ἀφοῦ $[k/p] = 0$ γιὰ $k = 1, \ldots, p'$, ἄρα παίρνομε τὴν (4.8).

Τέλος, ἐπειδὴ

$$\frac{(8n \pm 1)^2 - 1}{8} = 8n^2 \pm 2m , \quad \text{ἄρτιος}$$

καὶ

$$\frac{(8n \pm 3)^2 - 1}{8} = 8n^2 \pm 6n + 1 , \quad \text{περιττός,}$$

συμπεραίνομε ὅτι τὸ 2 εἶναι τετραγωνικὸ ἰσοϋπόλοιπο τὼν πρώτων τῆς μορφῆς $8n \pm 1$ καὶ τετραγωνικὸ ἀνισοϋπόλοιπο τῶν πρώτων τῆς μορφῆς $8n \pm 3$. **ὅ.ἔ.δ.**

Θεώρημα 4.2.3 –Νόμος τετραγωνικῆς ἀντιστροφῆς τοῦ Gauss.

Ἂν p, q εἶναι διαφορετικοὶ περιττοὶ πρῶτοι, τότε

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) . \tag{4.10}$$

Συνεπῶς,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{ἂν ἕνας, τουλάχιστον, ἀπὸ τοὺς } p, q \text{ εἶναι} \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{ἂν } p \equiv q \equiv 3 \pmod 4 . \end{cases}$$

Ἀπόδειξη Θὰ ἀποδείξομε τὴν (4.10) ὑπὸ τὴν ἑξῆς ἰσοδύναμη μορφή:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{p'q'} , \tag{4.11}$$

ὅπου, κατ' ἀναλογίαν μὲ τὸ p', ὁρίζομε $q' = \frac{q-1}{2}$.

Ἔχομε

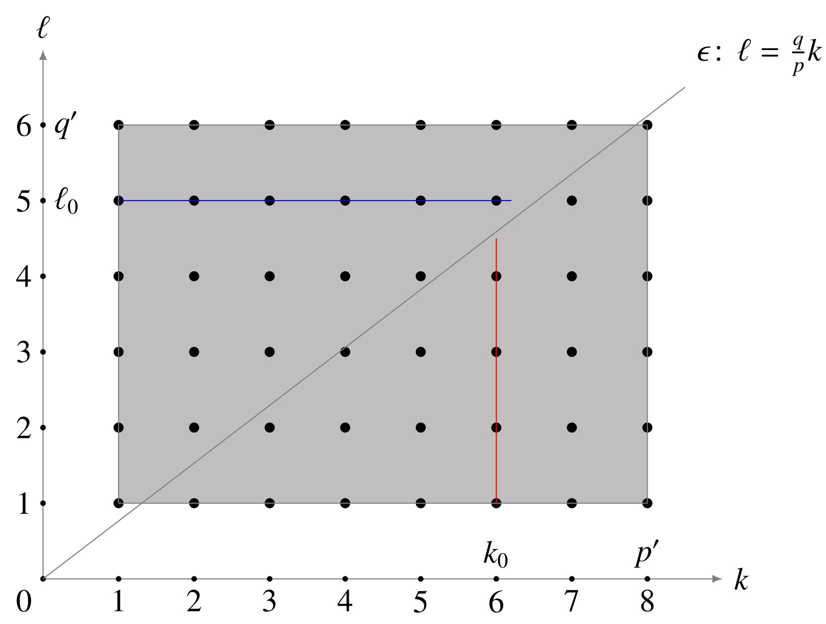
$$\left(\frac{2}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{2q}{p}\right) \overset{(4.9)}{=} (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum_{k=1}^{p'}\left[\frac{qk}{p}\right]} \overset{(4.8)}{=} \left(\frac{2}{p}\right)(-1)^{\sum_{k=1}^{p'}\left[\frac{qk}{p}\right]}$$

ἄρα, $\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{p'}\left[\frac{qk}{p}\right]}$.

Ἐναλλάσοντας τοὺς ρόλους τῶν p, q παίρνομε τὴν ἀνάλογη σχέση $\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'}\left[\frac{p\ell}{q}\right]}$. Συνεπῶς, γιὰ τὴν ἀπόδειξη τῆς σχέσης (4.11) ἀρκεῖ ν' ἀποδειχθεῖ ὅτι

$$\sum_{k=1}^{p'}\left[\frac{q}{p}k\right] + \sum_{\ell=1}^{q'}\left[\frac{p}{q}\ell\right] = p'q' . \tag{4.12}$$

Θὰ δώσομε στὴ σχέση (4.12) "γεωμετρικὴ ἑρμηνεία".



Σχῆμα 4.1: $p = 17$, $q = 13$.

Τὸ σχῆμα 4.1 ἀναφέρεται στὴν περίπτωση $p = 17$, $q = 13$. Κατ' ἀρχάς, σ' ἕνα ὀρθοκανονικὸ σύστημα ἀξόνων $k\,0\,\ell$, ἂς ὁρίσομε ὡς *ἀκέραιο σημεῖο*, ὁποιοδήποτε σημεῖο ἔχει ἀκέραιες καὶ τὶς δύο συντεταγμένες του καὶ ὡς *θετικὸ ἀκέραιο σημεῖο*,

ὁποιοδήποτε ἀκέραιο σημεῖο, τὸ ὁποῖο ἔχει καὶ τὶς δύο συντεταγμένες του θετικές. Θεωροῦμε τώρα τὴν εὐθεία $\epsilon\ :\ \ell = \frac{q}{p}k$.
Μία προκαταρκτικὴ παρατήρηση εἶναι ὅτι, πάνω σὲ αὐτὴ τὴν εὐθεία δὲν ὑπάρχει θετικὸ ἀκέραιο σημεῖο (k, ℓ) μὲ $k \leq p'$ καὶ $\ell \leq q'$· βλ. ἄσκηση 8. Ἔστω ἕνας συγκεκριμένος θετικὸς ἀκέραιος k_0. Ἡ «γεωμετρικὴ ἑρμηνεία» τῆς ποσότητας $[\frac{q}{p}k_0]$ εἶναι τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων, τὰ ὁποῖα βρίσκονται ἐπὶ τῆς εὐθείας $k = k_0$ καὶ «κάτω ἀπὸ τὴν εὐθεία» ϵ. Γιὰ παράδειγμα, στὸ σχῆμα 4.1, γιὰ $k_0 = 6$, βλέπομε ὅτι, τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων $(6, \ell)$ κάτω ἀπ' τὴν εὐθεία ϵ εἶναι $[(q/p)\,6] = [13 \cdot 6/17] = 4$· βλ. καὶ ἄσκηση 9. Ὁμοίως, γιὰ συγκεκριμένο θετικὸ ἀκέραιο ℓ_0, ἡ ποσότητα $[\frac{p}{q}\ell_0]$ δείχνει τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων, τὰ ὁποῖα βρίσκονται ἐπὶ τῆς εὐθείας $\ell = \ell_0$ καὶ «πάνω ἀπὸ τὴν εὐθεία» ϵ. Γιὰ παράδειγμα, στὸ σχῆμα 4.1, γιὰ $\ell_0 = 5$, τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων $(x, 5)$ ἀριστερὰ τῆς ϵ εἶναι $[(p/q)\,5] = [17 \cdot 5/13] = 6$· βλ. καὶ ἄσκηση 10. Ἄρα, τὸ ἄθροισμα στὸ ἀριστερὸ μέλος τῆς σχέσης (4.11) ἑρμηνεύεται ὡς τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων ἐντὸς τοῦ ὀρθογωνίου παραλληλογράμμου, τὸ ὁποῖο ὁρίζεται ἀπὸ τοὺς θετικοὺς ἡμιάξονες καὶ τὶς εὐθεῖες $k = p'$ καὶ $\ell = q'$· στὸ σχῆμα 4.1, αὐτὸ εἶναι τὸ γκρὶ παραλληλόγραμμο· βλ. ἄσκηση 11. Ἕνα τέτοιο σημεῖο, ὅμως, εἶναι τῆς μορφῆς (k, ℓ) μὲ $k \in \{1, \ldots, p'\}$ καὶ $\ell \in \{1, \ldots, q'\}$, ἄρα τὸ πλῆθος τους εἶναι $p'q'$ καὶ αὐτὸ ὁλοκληρώνει τὴν ἀπόδειξη τῆς σχέσης (4.11).

ὅ.ἔ.δ.

Ἀριθμητικὸ παράδειγμα. Ἐξετάζομε ἂν ἡ ἰσοτιμία $x^2 \equiv 1054 \pmod{1811}$ ἔχει λύση, ὅπου ὁ ἀριθμὸς 1811 εἶναι πρῶτος. Στοὺς παρακάτω ὑπολογισμούς, στὰ δεξιὰ κάθε ἰσότητας γράφεται ἡ ἰδιότητα, τῆς ὁποίας ἔγινε χρήση, γιὰ νὰ μεταβοῦμε ἀπὸ τὴν προηγούμενη ἰσότητα σὲ αὐτή. Ὅλοι οἱ ἀριθμοὶ στοὺς «παρονομαστὲς» τῶν συμβόλων Legendre εἶναι πρῶτοι, ἄρα, σὲ κάποια βήματα ἐννοεῖται ὅτι γίνεται παραγοντοποίηση σὲ πρώτους.

$$
\begin{aligned}
\left(\frac{1054}{1811}\right) &= \left(\frac{2}{1811}\right)\cdot\left(\frac{527}{1811}\right) && \text{(Θεώρημα 4.2.1-ε$'$)}\\
&= (-1)\left(\frac{527}{1811}\right) && \text{(Θεώρημα 4.2.2)}\\
&= -\left(\frac{17}{1811}\right)\cdot\left(\frac{31}{1811}\right) && \text{(Θεώρημα 4.2.1-ε$'$)}\\
&= \left(\frac{1811}{17}\right)\cdot\left(\frac{1811}{31}\right) && \text{(Θεώρημα 4.2.3)}\\
&= \left(\frac{9}{17}\right)\cdot\left(\frac{13}{31}\right) && \text{(Θεώρημα 4.2.1-β$'$)}\\
&= (+1)\left(\frac{13}{31}\right) && \text{(Θεώρημα 4.2.1-α$'$)}
\end{aligned}
$$

$$
\begin{aligned}
&=\left(\frac{31}{13}\right) && \text{(Θεώρημα 4.2.3)}\\
&=\left(\frac{5}{13}\right) && \text{(Θεώρημα 4.2.1-β΄)}\\
&=\left(\frac{13}{5}\right) && \text{(Θεώρημα 4.2.3)}\\
&=\left(\frac{-2}{5}\right) && \text{(Θεώρημα 4.2.1-β΄)}\\
&=\left(\frac{-1}{5}\right)\cdot\left(\frac{2}{5}\right) && \text{(Θεώρημα 4.2.1-ε΄)}\\
&=(+1)(-1) = -1 && \text{(Θεωρήματα 4.2.1-δ΄ καὶ 4.2.2)}
\end{aligned}
$$

Συμπεραίνομε, λοιπόν, ὅτι ἡ ἰσοτιμία $x^2 \equiv 1054 \pmod{1811}$ εἶναι ἀδύνατη.

4.3 Τὸ σύμβολο τοῦ Jacobi

Στὴν παράγραφο αὐτὴ τὰ P, Q συμβολίζουν περιττοὺς ἀκεραίους, μὲ $(P, Q) = 1$

Στὸ παράδειγμα, μὲ τὸ ὁποῖο τελειώνομε τὴν προηγούμενη παράγραφο, βλέπομε ὅτι, κάποιες φορὲς χρειάζεται νὰ γίνει παραγοντοποίηση, προκειμένου να μπορέσει νὰ προχωρήσει ἡ διαδικασία ὑπολογισμοῦ, ὅπως, γιὰ παράδειγμα, ὅταν φτάνομε στὸ $\left(\frac{527}{1811}\right)$. Καὶ ἐδῶ μέν, ὁ ἀριθμὸς 527 εἶναι μικρός, ὁπότε ἡ παραγοντοποίησή του δὲν μᾶς δημιουργεῖ ὑπολογιστικὸ πρόβλημα, ἀλλὰ τί γίνεται ὅταν ἕνας ἀριθμὸς μὲ 100, ἂς ποῦμε, δεκαδικὰ ψηφία, ἐμφανίζεται στὸν «ἀριθμητὴ» τοῦ συμβόλου; Τὸ πρόβλημα τῆς παραγοντοποίησης ἑνὸς τέτοιου ἀριθμοῦ εἶναι, ἀπὸ ὑπολογιστικὴ ἄποψη, πολὺ δύσκολο καί, μάλιστα, ἂν ὁ ἀριθμὸς ἔχει, ἀντὶ 100, 300 ψηφία, τότε, πολὺ πιθανὸν νὰ εἶναι καὶ ὑπολογιστικῶς ἀνέφικτο. Ἡ παράκαμψη τῆς παραγοντοποίησης κατὰ τὴ διαδικασία ὑπολογισμοῦ τοῦ συμβόλου Legendre ἐπιτυγχάνεται μὲ τὴ βοήθεια τοῦ συμβόλου Jacobi, τὸ ὁποῖο ἀποτελεῖ γενίκευση τοῦ συμβόλου Legendre.

Ἔστω $P = p_1 \cdots p_n$ ἡ ἀνάλυση τοῦ περιττοῦ ἀκεραίου P σὲ πρώτους παράγοντες. Οἱ $p_1, \ldots, p_n$ δὲν εἶναι, κατ' ἀνάγκη, διαφορετικοί. Γιὰ κάθε a πρῶτο πρὸς τὸν P ὁρίζομε

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_n}\right)$$

καὶ τὸ ἀριστερὸ μέλος καλοῦμε *σύμβολο Jacobi τοῦ a ὡς πρὸς P*. Στὴν περίπτωση ποὺ $P = p_1$, δηλαδή, ὅταν ὁ P εἶναι πρῶτος, τὸ σύμβολο Jacobi τοῦ a ὡς πρὸς P ταυτίζεται μὲ τὸ σύμβολο Legendre τοῦ a ὡς πρὸς P.

Ἡ παρακάτω πρόταση μᾶς λέει ότι ὅλες οἱ ἰδιότητες τοῦ συμβόλου Legendre, πλὴν τῆς γ΄ τοῦ θεωρήματος 4.2.1, ἰσχύουν καὶ γιὰ τὸ σύμβολο τοῦ Jacobi.

Πρόταση 4.3.1 *αʹ.* $\left(\frac{a^2}{P}\right) = 1$. *Εἰδικώτερα,* $\left(\frac{1}{P}\right) = 1$.

βʹ. *Ἂν* $a \equiv b \pmod P$, *τότε* $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.

γʹ. $\left(\frac{a_1 a_2 \dots a_k}{P}\right) = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)\cdots\left(\frac{a_k}{P}\right)$.

δʹ. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

Μ' ἄλλα λόγια, τὸ -1 εἶναι τετραγωνικὸ ἰσοϋπόλοιπο ἂν $P \equiv 1 \pmod 4$ *καὶ τετραγωνικὸ ἀνισοϋπόλοιπο ἂν* $P \equiv 3 \pmod 4$.

εʹ. Ἰσχύει ἡ γενίκευση τοῦ συμπληρώματος τοῦ νόμου τετραγωνικῆς ἀντιστροφῆς:

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}\ .$$

Συνεπῶς, τὸ 2 εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρῳ P *γιὰ* P *τῆς μορφῆς* $8n \pm 1$ *καὶ τετραγωνικὸ ἀνισοϋπόλοιπο γιὰ* P *τῆς μορφῆς* $8n \pm 3$.

στʹ. Ἂν ὁ Q *εἶναι περιττὸς καὶ* $(P, Q) = 1$, *τότε ἰσχύει ἡ γενίκευση τοῦ νόμου τῆς τετραγωνικῆς ἀντιστροφῆς:*

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)\ .$$

Συνεπῶς,

$$\left(\frac{Q}{P}\right) = \begin{cases} \left(\frac{P}{Q}\right) & \text{ἂν ἕνας, τουλάχιστον, ἀπὸ τοὺς } P, Q \text{ εἶναι } \equiv 1 \pmod 4 \\ -\left(\frac{P}{Q}\right) & \text{ἂν } P \equiv Q \equiv 3 \pmod 4\,. \end{cases}\ .$$

Ἀπόδειξη Ἡ ἀπόδειξη τῶν αʹ, βʹ καὶ γʹ ἕπεται ἀμέσως ἀπὸ τὸν ὁρισμὸ τοῦ συμβόλου Jacobi καὶ τῶν ἀντιστοίχων ἰδιοτήτων τοῦ συμβόλου Legendre.

Γιὰ τὴν ἀπόδειξη τῶν ὑπολοίπων ἰδιοτήτων θὰ ὑποθέσομε ὅτι $P = p_1 p_2 \cdots p_n$ καὶ $Q = q_1 \dots q_m$ εἶναι οἱ ἀναλύσεις τῶν P, Q σὲ πρώτους παράγοντες. Λόγῳ τῆς ὑποθέσεως $(P, Q) = 1$, κάθε q_j εἶναι διαφορετικὸς ἀπὸ κάθε p_i.

Κατ' ἀρχάς, κάποιες γενικὲς παρατηρήσεις εἶναι χρήσιμες: Ἂν οἱ $a_1, a_2, \dots, a_n$ εἶναι ἄρτιοι, τότε

$$(1 + a_1)(1 + a_2)\cdots(1 + a_n) \equiv 1 + (a_1 + a_2 + \cdots + a_n) \begin{cases} \bmod 4 & \text{ἂν } 2|a_i\ \forall i \\ \bmod 16 & \text{ἂν } 4|a_i\ \forall i \end{cases} \tag{4.13}$$

διότι

$$(1 + a_1)(1 + a_2)\cdots(1 + a_n) = 1 + \sum_{1\le i\le n} a_i + \sum_{1\le i<j\le n} a_i a_j + \sum_{1\le i<j<k\le n} a_i a_j a_k + \cdots$$

καὶ στὸ δεξιὸ μέλος, ἐκτὸς ἀπὸ τὸ 1 καὶ τὸ πρῶτο ἄθροισμα, ὅλα τὰ ὑπόλοιπα ἀθροίσματα εἶναι πολλαπλάσια τοῦ 4, στὴν πρώτη περίπτωση καὶ πολλαπλάσια τοῦ 16 στὴ δεύτερη.
(δ′) Μὲ τὴ βοήθεια τῆς σχέσης (4.13), τὴν ὁποία ἐφαρμόζομε γιὰ $a_i = p_i - 1$, ἔχομε

$$\begin{aligned} P - 1 &= p_1 p_2 \cdots p_n - 1 = (1 + (p_1 - 1)) \cdot (1 + (p_2 - 1)) \cdots (1 + (p_n - 1)) - 1 \\ &\equiv (1 + (p_1 - 1) + (p_2 - 1) + \cdots + `(p_n - 1)) - 1 \pmod 4 \\ &\equiv (p_1 - 1) + (p_2 - 1) + \cdots + (p_n - 1) \pmod 4 , \end{aligned}$$

ἄρα

$$\frac{P-1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_n - 1}{2} \pmod 2 . \tag{4.14}$$

Κάνοντας χρήση αὐτῆς τῆς σχέσης καὶ τοῦ θεωρήματος 4.2.1-δ′, ἔχομε

$$(-1)^{\frac{P-1}{2}} = (-1)^{\frac{p_1-1}{2}} \cdots (-1)^{\frac{p_n-1}{2}} = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_n}\right) = \left(\frac{-1}{P}\right) .$$

(ε′) Μὲ τὴ βοήθεια τῆς σχέσης (4.13), τὴν ὁποία ἐφαρμόζομε γιὰ $a_i = p_i^2 - 1 \equiv 0 \pmod 4$, ἔχομε

$$\begin{aligned} P^2 - 1 &= (p_1 p_2 \cdots p_n)^2 - 1 = \left(1 + (p_1^2 - 1)\right) \cdot \left(1 + (p_2^2 - 1)\right) \cdots \left(1 + (p_n^2 - 1)\right) - 1 \\ &\equiv \left(1 + (p_1^2 - 1) + (p_2^2 - 1) + \cdots + (p_n^2 - 1)\right) - 1 \pmod{16} \\ &\equiv (p_1^2 - 1) + (p_2^2 - 1) + \cdots + (p_n^2 - 1) \pmod{16} , \end{aligned}$$

ἄρα[1]

$$\frac{P^2-1}{8} \equiv \frac{p_1^2 - 1}{8} + \frac{p_2^2 - 1}{8} + \cdots + \frac{p_n^2 - 1}{8} \pmod 2 .$$

Κάνοντας χρήση αὐτῆς τῆς σχέσης καὶ τοῦ θεωρήματος 4.2.2, ἔχομε

$$(-1)^{\frac{P^2-1}{8}} = (-1)^{\frac{p_1^2-1}{8}} \cdots (-1)^{\frac{p_n^2-1}{8}} = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_n}\right) = \left(\frac{2}{P}\right) .$$

(στ′) Θὰ ἀποδείξομε τὴν ἰσοδύναμη σχέση

$$(-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} = \left(\frac{Q}{P}\right) \cdot \left(\frac{P}{Q}\right) , \tag{4.15}$$

βασισμένοι στὶς σχέσεις

$$(-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} = \left(\frac{q_j}{p_i}\right) \cdot \left(\frac{p_i}{q_j}\right) \quad (i = 1, \ldots, n , \ j = 1, \ldots m) ,$$

[1] Θυμηθῆτε ὅτι, γιὰ κάθε περιττὸ a, $8 | (a^2 - 1)$.

οἱ ὁποῖες εἶναι προφανεῖς συνέπειες τοῦ θεωρήματος 4.2.3. Στὶς παρακάτω σχέσεις, ὁ δείκτης i ἐννοεῖται ὅτι διατρέχει τὸ σύνολο $\{1, \ldots, n\}$ καὶ ὁ δείκτης j τὸ σύνολο $\{1, \ldots, m\}$.

Κάνοντας χρήση τῆς σχέσης (4.14) καὶ τῆς ὅμοίας της γιὰ τὸν Q, ἔχομε

$$\frac{P-1}{2} \cdot \frac{Q-1}{2} \equiv \sum_i \frac{p_i - 1}{2} \sum_j \frac{q_j - 1}{2} \equiv \sum_{i,j} \frac{p_i - 1}{2} \frac{q_j - 1}{2} \pmod 2,$$

ἀπ' ὅπου,

$$\begin{aligned}
(-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} &= \prod_{i,j} (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} = \prod_{i,j} \left(\frac{q_j}{p_i}\right) \cdot \left(\frac{p_i}{q_j}\right) \\
&= \prod_j \prod_i \left(\frac{q_j}{p_i}\right) \cdot \left(\frac{p_i}{q_j}\right) \\
&= \prod_j \left(\frac{q_j}{P}\right) \cdot \left(\frac{P}{q_j}\right) \\
&= \left(\frac{Q}{P}\right) \cdot \left(\frac{P}{Q}\right).
\end{aligned}$$

ὅ.ἔ.δ.

Ἀριθμητικὸ παράδειγμα. Ὑπολογίζομε ξανὰ τὸ $\left(\frac{1054}{1811}\right)$, δίχως να καταφύγομε, σὲ κανένα βῆμα τοῦ ὑπολογισμοῦ, σὲ παραγοντοποίηση, ἐκτὸς ἀπὸ τὴν «ἐξαγωγὴ τοῦ 2». Αὐτὸ τὸ ἐπιτυγχάνομε μὲ χρήση τοῦ συμβόλου Jacobi. Τώρα, πλέον, δὲν μᾶς ἐνδιαφέρει ἂν οἱ «παρονομαστὲς» τῶν συμβόλων εἶναι πρῶτοι ἀριθμοί. Φυσικά, σ' ἕνα παράδειγμα μὲ τόσο μικροὺς ἀριθμούς, αὐτὸ τὸ ὑπολογιστικὸ πλεονέκτημα τοῦ συμβόλου Jacobi –ἡ ἀποφυγὴ τῆς παραγοντοποίησης– δὲν δείχνει τόσο σημαντικό.

Στὸ δεξιώτερο ἄκρο κάθε γραμμῆς σημειώνεται ποιὰ ἀπὸ τὶς ἰδιότητες α′–στ′ τοῦ θεωρήματος 4.3.1 χρησιμοποιήθηκε.

$$\begin{aligned}
\left(\frac{1054}{1811}\right) &= \left(\frac{2}{1811}\right) \cdot \left(\frac{527}{1811}\right) && (\gamma') \\
&= (-1) \left(\frac{527}{1811}\right) && (\varepsilon') \\
&= \left(\frac{1811}{527}\right) && (\sigma\tau')
\end{aligned}$$

$$
\begin{aligned}
&=\left(\frac{230}{527}\right) && (\,\beta')\\
&=\left(\frac{2}{527}\right)\cdot\left(\frac{115}{527}\right) && (\,\gamma')\\
&=(+1)\left(\frac{115}{527}\right) && (\,\varepsilon')\\
&=-\left(\frac{527}{115}\right) && (\,\sigma\tau')\\
&=-\left(\frac{-48}{115}\right) && (\,\beta')\\
&=-\left(\frac{-1}{115}\right)\cdot\left(\frac{16}{115}\right)\cdot\left(\frac{3}{115}\right) && (\,\gamma')\\
&=\left(\frac{3}{115}\right) && (\,\delta'\text{-}\alpha')\\
&=-\left(\frac{115}{3}\right) && (\,\sigma\tau')\\
&=-\left(\frac{1}{3}\right) && (\,\beta')\\
&=-1 && (\,\alpha')
\end{aligned}
$$

Προσοχή! Ἂς ὑποθέσομε ὅτι $\left(\frac{a}{P}\right) = -1$. Αὐτὸ συνεπάγεται ὅτι, γιὰ ἕνα, τουλάχιστον, πρῶτο παράγοντα του P ἰσχύει $\left(\frac{a}{p_i}\right) = -1$, ὁπότε ἡ ἰσοτιμία $x^2 \equiv a \pmod{p_i}$ δὲν ἔχει λύση. Ἀλλὰ τότε, προφανῶς, οὔτε ἡ ἰσοτιμία $x^2 \equiv a \pmod{P}$ ἔχει λύση. Ἂν ὅμως $\left(\frac{a}{P}\right) = 1$ καὶ δὲν εἴμαστε βέβαιοι ὅτι ὁ P εἶναι πρῶτος, τότε δὲν μποροῦμε νὰ συμπεράνομε ὅτι ἡ ἰσοτιμία $x^2 \equiv a \pmod{P}$ ἔχει λύση! Πράγματι, ἂν γιὰ ἄρτιο πλῆθος περιττῶν πρώτων παραγόντων p_i τοῦ P εἶναι $\left(\frac{a}{p_i}\right) = -1$, τότε, ἐνῶ δὲν ἔχει λύση ἡ $x^2 \equiv a \pmod{P}$, εἶναι $\left(\frac{a}{P}\right) = 1$.

4.4 Ἐπίλυση τῆς ἰσοτιμίας $x^2 \equiv a \pmod{m}$

Στὸ κεφάλαιο 3 ἀχοληθήκαμε μὲ τὴν ἐπίλυση τῆς ἰσοτιμίας $f(x) \equiv 0 \pmod{m}$ γιὰ τὸ γενικὸ πολυώνυμο $f(X) \in \mathbb{Z}[X]$. Σ' αὐτὴ τὴν παράγραφο θὰ ἐξειδικεύσομε τὸ πολυώνυμο $f(X)$ στὴν εἰδική, ἀλλὰ πολὺ ἐνδιαφέρουσα περίπτωση $f(X) = X^2 - a$.

Θεώρημα 4.4.1 *Ἔστω περιττὸς πρῶτος p, ἀκέραιος a πρῶτος πρὸς τὸν p καὶ n φυσικὸς ἀριθμός. Ἡ ἰσοτιμία*

$$x^2 \equiv a \pmod{p^n} \tag{4.16}$$

ἔχει λύση, ἂν καὶ μόνο ἂν $\left(\frac{a}{p}\right) = +1$. *Στὴν περίπτωση ποὺ ἔχει λύση, τὸ πλῆθος τῶν ἀνισοτίμων* $\bmod p^n$ *λύσεων εἶναι ἀκριβῶς δύο. Ἂν ἡ μία λύση εἶναι ἡ* $x_n \pmod{p^n}$, *τότε ἡ δεύτερη λύση εἶναι ἡ* $x_n' \equiv -x_n \pmod{p^n}$.

Ἀπόδειξη Ἡ ἀναγκαιότητα τῆς συνθήκης $\left(\frac{a}{p}\right) = +1$ γιὰ τὴν ἐπιλυσιμότητα τῆς (4.16), εἶναι προφανής. Πράγματι, ἂν ἡ (4.16) εἶναι ἐπιλύσιμη, τότε καὶ ἡ $x^2 \equiv a \pmod p$ εἶναι ἐπιλύσιμη, ποὺ σημαίνει ὅτι $\left(\frac{a}{p}\right) = +1$.

Ἀντιστρόφως, ἔστω ὅτι $\left(\frac{a}{p}\right) = +1$. Θὰ ἀποδείξομε τὴν ἐπιλυσιμότητα τῆς (4.16) ἐπαγωγικά. Γιὰ $n = 1$ ἡ ἰσοτιμία ἔχει λύση, ἐπειδή, ἀκριβῶς, $\left(\frac{a}{p}\right) = +1$. Ὑποθέτομε τώρα ὅτι $k \geq 1$ καὶ $x_k \pmod{p^k}$ εἶναι λύση τῆς $x^2 \equiv a \pmod{p^k}$. Θὰ δείξομε ὅτι μποροῦμε νὰ βροῦμε ἀκέραιο x_{k+1}, τέτοιον ὥστε $x_{k+1}^2 \equiv a \pmod{p^{k+1}}$. Πράγματι, γιὰ τὸν σκοπὸν αὐτό, θέτομε $x_{k+1} = x_k + y_k p^k$, ὅπου ὁ y_k εἶναι ἄγνωστος, καὶ ἀπαιτοῦμε νὰ ἱκανοποιεῖται ἡ σχέση $x_{k+1}^2 \equiv a \pmod{p^{k+1}}$. Αὐτὴ ἡ σχέση ἰσοδυναμεῖ μὲ τὴν $x_k^2 + 2x_k y_k p^k + y_k^2 p^{2k} \equiv a \pmod{p^{k+1}}$. Ἐπειδὴ $2k \geq k+1$, ὁ τρίτος προσθετέος στὸ ἀριστερὸ μέλος τῆς τελευταίας ἰσοτιμίας εἶναι $\equiv 0 \pmod{p^{k+1}}$, ἄρα αὐτὴ ἡ ἰσοτιμία εἶναι ἰσοδύναμη μὲ τὴν $x_k^2 + 2x_k y_k p^k \equiv a \pmod{p^{k+1}}$. Ἄρα, ἔχομε νὰ λύσομε τὴν ἰσοτιμία $2x_k y_k p^k \equiv a - x_k^2 \pmod{p^{k+1}}$ ὡς πρὸς y_k. Ἀπὸ τὴν ἐπαγωγικὴ ὑπόθεση, $x_k^2 \equiv a \pmod{p^k}$, ἄρα, τὸ δεξιὸ μέλος τῆς πρὸς ἐπίλυσιν ἰσοτιμίας διαιρεῖται διὰ p^k, ὁπότε[2], ἡ ἰσοτιμία αὐτὴ ἰσοδυναμεῖ μὲ τὴν $(2x_k)y_k \equiv \frac{a-x_k^2}{p^k} \pmod p$. Ὁ συντελεστὴς τοῦ y_k στὸ ἀριστερὸ μέλος εἶναι πρῶτος πρὸς τὸν p, διότι ὁ p εἶναι ἄρτιος καὶ πρῶτος πρὸς τὸν x_k,[3] ἄρα, ἀπὸ τὸ Θεώρημα 3.2.1 , ἡ ἰσοτιμία ἔχει λύση ὡς πρὸς y_k. Αὐτὸ ἀποδεικν;υει ὅτι μποροῦμε νὰ ὑπολογίσομε x_{k+1}, ποὺ νὰ ἱκανοποιεῖ τὴν $x_{k+1}^2 \equiv a \pmod{p^{k+1}}$. Ἔτσι ὁλοκληρώνομε τὴν ἐπαγωγικὴ ἀπόδειξη.

Συνοψίζοντας τὴν κατασκευαστικὴ μέθοδο τῆς ἀπόδειξης, ἔχομε τὰ ἑξῆς: Ξεκινώντας μὲ μία λύση, ἔστω x_1, τῆς $x^2 \equiv a \pmod p$, κατασκευάζομε, διαδοχικά, τοὺς ἀκεραίους $x_2, \ldots, x_k, x_{k+1}, \ldots, x_n$, ἔτσι ὥστε:

$$\begin{aligned}
&x_1^2 \equiv a \pmod p && \\
&x_2^2 \equiv a \pmod{p^2}, && x_2 = x_1 + y_1 p \\
&x_3^2 \equiv a \pmod{p^3}, && x_3 = x_2 + y_2 p^2 = x_1 + y_1 p + y_2 p^2 \\
&\qquad\vdots && \qquad\vdots \\
&x_{k+1}^2 \equiv a \pmod{p^{k+1}}, && x_{k+1} = x_k + y_k p^k = x_1 + y_1 p + y_2 p^2 + \cdots + y_k p^k \\
&\qquad\vdots && \qquad\vdots \\
&x_n^2 \equiv a \pmod{p^n}, && x_n = x_{n-1} + y_{n-1} p^{n-1} = x_1 + y_1 p + y_2 p^2 + \cdots + y_{n-1} p^{n-1}.
\end{aligned}$$

Εἰδικώτερα, ἀπὸ τὴν τελευταία σχέση προκύπτει ὅτι $x_n \equiv x_1 \pmod p$.

Εἶναι προφανὲς ὅτι καὶ ἡ $x \equiv -x_n \pmod{p^n}$ εἶναι λύση τῆς (4.16). Ἂν ἦταν $x_n \equiv -x_n \pmod{p^n}$, τότε θὰ ἦταν καὶ $x_n \equiv -x_n \pmod p$, ἄρα καὶ $x_1 \equiv -x_1 \pmod p$. Ἀλλὰ τότε $2x_1 \equiv 0 \pmod p$, προφανῶς ἀδύνατο, ἀφοῦ $x_1^2 \equiv a \pmod p$ καὶ $(a, p) = 1$.

[2] Βάσει τοῦ Θεωρήματος 2.1.2 (εʹ) μποροῦμε νὰ διαιρέσομε τὰ δύο μέλη τῆς ἰσοτιμίας καὶ τὸ μέτρο, μὲ τὸν ἴδιον ἀριθμό – ἐδῶ τὸν p^k – καὶ νὰ πάρομε ἰσοδύναμη ἰσοτιμία.

[3] Ἀπὸ τὴ σχέση $x_k^2 \equiv a \pmod{p^k}$ καὶ τὴν ὑπόθεση $(a, p) = 1$ συμπεραίνομε ὅτι $(x_k, p) = 1$.

Μένει νὰ δείξομε ὅτι, ἂν $x \equiv x_0 \pmod{p^n}$ εἶναι μιὰ ὁποιαδήποτε λύση τῆς (4.16), τότε $x_0 \equiv x_n \pmod{p^n}$ ἢ $x_0 \equiv -x_n \pmod{p^n}$. Κατ' ἀρχάς, παρατηροῦμε ὅτι $x_0^2 \equiv a \pmod{p}$, ὅπως καὶ $x_n^2 \equiv a \pmod{p}$. Ἄρα, $x_0 \equiv \pm x_n \pmod{p}$ (ἄσκηση 4 τοῦ κεφαλαίου 3). Ἂν ἡ τελευταία ἰσοτιμία ἰσχύει μὲ τὸ πρόσημο $+$, τότε $p|(x_0 - x_n)$, ὁπότε ὁ p δὲν διαιρεῖ τὸν $x_0 + x_n$.[4] Ἂν ἡ ἰσοτιμία ἰσχύει μὲ τὸ πρόσημο $-$, τότε ὁ p διαιρεῖ τὸ $x_0 + x_n$ καὶ δὲν διαιρεῖ τὸ $x_0 - x_n$. Ἄρα, σὲ κάθε περίπτωση, ὁ p διαιρεῖ *ἀκριβῶς ἕναν* ἀπὸ τοὺς $x_0 + x_n, x_0 - x_n$. Ἀλλὰ τώρα, παρατηροῦμε ὅτι $x_0^2 \equiv a \equiv x_n^2 \pmod{p^n}$, ἄρα $(x_0 + x_n)(x_0 - x_n) \equiv 0 \pmod{p^n}$, ποὺ σημαίνει ὅτι $p^n|(x_0 + x_n)(x_0 - x_n)$. Ἂν ὁ p διαιρεῖ τὸν $x_0 - x_n$, τότε δὲν διαιρεῖ τὸν $x_0 + x_n$, ἄρα ἡ σχέση $p^n|(x_0 + x_n)(x_0 - x_n)$ μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι $p^n|(x_0 - x_n)$ καὶ αὐτὸ μᾶς λέει ὅτι $x_0 \equiv x_n \pmod{p^n}$. Ἂν ὁ p διαιρεῖ τὸν $x_0 + x_n$, τότε, ἐντελῶς ἀνάλογα, ὁδηγούμαστε στὸ συμπέρασμα ὅτι $x_0 \equiv -x_n \pmod{p^n}$. **ὅ.ἔ.δ.**

Παράδειγμα. Ἐφαρμόζομε τὴ μέθοδο ποὺ περιγράφεται στὴν ἀπόδειξη τοῦ Θεωρήματος 4.4.1 γιὰ νὰ ἐπιλύσομε τὴν ἰσοτιμία

$$x^2 \equiv 2 \pmod{7^4}.$$

Κατ' ἀρχάς, $\left(\frac{2}{7}\right) = +1$, ἄρα ἡ ἰσοτιμία ἔχει λύση.
Ξεκινοῦμε ἀπὸ μία ὁποιαδήποτε λύση τῆς $x^2 \equiv 2 \pmod{7}$, π.χ. $x_1 \equiv 3 \pmod{7}$. Περιγράφομε συνοπτικὰ τὴν ἐπίλυση ὡς ἑξῆς:

$$\begin{array}{ll}
x_1 = 3 & \\
x_2 = 3 + 7y_1, & (3 + 7y_1)^2 \equiv 2 \pmod{7^2} \\
 & 9 + 6 \cdot 7y_1 \equiv 2 \pmod{7^2} \\
 & 6 \cdot 7y_1 \equiv -7 \pmod{7^2} \\
 & 6y_1 \equiv -1 \pmod{7} \to y_1 = 1 \to x_2 = 3 + 7 \cdot 1 = 10 \\
x_3 = 10 + 7^2 y_2, & (10 + 7^2 y_2)^2 \equiv 2 \pmod{7^3} \\
 & 100 + 20 \cdot 7^2 y_2 \equiv 2 \pmod{7^3} \\
 & 20 \cdot 7^2 y_2 \equiv -98 \pmod{7^3} \\
 & 20y_2 \equiv -2 \pmod{7} \to y_2 = 2 \to x_3 = 10 + 7^2 \cdot 2 = 108 \\
x_4 = 108 + 7^3 y_3, & (108 + 7^3 y_3)^2 \equiv 2 \pmod{7^4} \\
 & 108^2 + 216 \cdot 7^3 y_3 \equiv 2 \pmod{7^4} \\
 & 216 \cdot 7^3 y_3 \equiv -11662 = -34 \cdot 7^3 \pmod{7^4} \\
 & 216y_3 \equiv -34 \pmod{7} \to y_3 = 6 \to x_4 = 108 + 7^3 \cdot 6 = 2166.
\end{array}$$

Ἄρα, μία λύση εἶναι ἡ $x_4 \equiv 2166 \pmod{7^4}$. Σύμφωνα μὲ τὸ Θεώρημα, ἡ δεύτερη λύση εἶναι ἡ $x_4' \equiv -2166 \equiv 235 \pmod{7^4}$.

Τώρα ἐρχόμαστε στὴν ἐπίλυση τῆς ἰσοτιμίας $x^2 \equiv a \pmod{2^n}$.

Θεώρημα 4.4.2 *Ἔστω περιττὸς ἀριθμὸς a καὶ φυσικὸς ἀριθμὸς n. Γιὰ τὴν ἰσοτιμία*

$$x^2 \equiv a \pmod{2^n} \tag{4.17}$$

[4] Ἂν ὁ p διαιροῦσε τὸ $x_0 - x_n$ καὶ τὸ $x_0 + x_n$, τότε θὰ διαιροῦσε καὶ τὸ ἄθροισμά τους $2x_0$, ἄρα καὶ τὸ x_0, ἄτοπο.

ἰσχύουν τὰ ἑξῆς:
Γιὰ $n = 1$, ἡ ἰσοτιμία ἔχει μία ἀκριβῶς λύση.
Γιὰ $n = 2$, ἡ ἰσοτιμία ἔχει λύση ἄν, καὶ μόνο ἄν, $a \equiv 1 \pmod 4$. Ἄν ἱκανοποιεῖται αὐτὴ ἡ ἡ συνθήκη, τότε τὸ πλῆθος τῶν λύσεων τῆς ἰσοτιμίας εἶναι ἀκριβῶς 2.
Γιὰ $n \geq 3$, ἡ ἰσοτιμία ἔχει λύση ἂν καὶ μόνο ἄν, $a \equiv 1 \pmod 8$. Ἄν ἱκανοποιεῖται αὐτὴ ἡ ἡ συνθήκη, τότε τὸ πλῆθος τῶν λύσεων τῆς ἰσοτιμίας εἶναι ἀκριβῶς 4. Ἐπιπλέον, στὴν περίπτωση αὐτή, ἂν $x_n \bmod 2^n$ εἶναι μία λύση, τότε, οἱ τέσσερεις διαφορετικὲς λύσεις εἶναι οἱ

$$x \equiv \pm x_n\,,\ \pm x_n + 2^{n-1} \pmod{2^n}. \tag{4.18}$$

Ἀπόδειξη Οἱ περιπτώσεις $n = 1, 2$ εἶναι τετριμμένες: Ἄν $n = 1$, τότε μοναδικὴ λύση τῆς (4.17) εἶναι ἡ $x \equiv 1 \pmod 2$. Ἄν $n = 2$, τότε, ἐπειδὴ τὸ τετράγωνο κάθε περιττοῦ εἶναι $\equiv 1 \bmod 4$, ἕπεται ὅτι, $a \equiv 1 \pmod 4$. Ἀλλὰ τότε ἡ $x^2 \equiv a \pmod{2^2}$ ἔχει, ἀκριβῶς, τὶς λύσεις $x \equiv 1, 3 \pmod 4$.

Ἔστω, λοιπόν, $n \geq 3$. Ἄν ὑπάρχει ἀκέραιος x, ποὺ νὰ ἱκανοποιεῖ τὴν ἰσοτιμία (4.17), τότε $x^2 \equiv a \pmod 8$. Ἀλλὰ ὁ x εἶναι περιττός, ὁπότε $x^2 \equiv 1 \pmod 8$, ἀπ' ὅπου προκύπτει ἡ ἀναγκαιότητα τῆς συνθήκης $b \equiv 1 \pmod 8$ γιὰ νὰ ἔχει λύση ἡ ἰσοτιμία (4.17).
Ἀντιστρόφως, ἔστω ὅτι $a \equiv 1 \pmod 8$. Θὰ ἀποδείξομε ἐπαγωγικὰ ὅτι ἡ ἰσοτιμία (4.17) ἔχει λύση. Γιὰ $a = 3$, μία λύση εἶναι ἡ $1 \bmod 8$. Ἄς ὑποθέσομε τώρα ὅτι γιὰ $n = k \geq 3$ ὑπάρχει λύση, ἔστω ἡ $x_k \bmod 2^k$. Θέτομε $x_{k+1} = x_k + 2^{k-1}y_{k-1}$ καὶ ἀπαιτοῦμε νὰ ἰσχύει ἡ σχέση $x_{k+1}^2 \equiv a \pmod{2^{k+1}}$. Ἀλλὰ αὐτὴ ἰσοδυναμεῖ μὲ τὴν

$$(x_k^2 - a) + 2^k x_k y_{k-1} + 2^{2k-2} y_{k-1}^2 \equiv 0 \pmod{2^{k+1}}.$$

Εἶναι $2k - 2 \geq k + 1$, ποὺ σημαίνει ὅτι ὁ τρίτος προσθετέος τοῦ ἀριστεροῦ μέλους εἶναι $\equiv 0 \bmod 2^{k+1}$. Ἄρα, ἡ παραπάνω ἰσοτιμία γίνεται $2^k x_k y_{k-1} \equiv a - x_k^2 \pmod{2^{k+1}}$. Ἀπὸ τὴν ἐπαγωγικὴ ὑπόθεση, $x_k^2 \equiv a \pmod{2^k}$, ἄρα ὁ 2^k διαιρεῖ τὸ δεξιὸ μέλος, ὁπότε, διαιρώντας τὰ δύο μέλη τῆς ἰσοτιμίας καὶ τὸ μέτρο διὰ 2^k, ὁδηγούμαστε στὴν ἰσοδύναμη ἰσοτιμία

$$x_k y_{k_1} \equiv \frac{a - x_k^2}{2^k} \pmod 2\,.$$

Ἐπειδὴ ὁ x_k εἶναι περιττός, καταλήγομε, τελικά, στὸ συμπέρασμα ὅτι ἡ παραπάνω ἰσοτιμία εἶναι ἐπιλύσιμη καί, μάλιστα,

$$y_{k-1} = \begin{cases} 0 & \text{ἂν ὁ } (a - x_k^2)/2^k \text{ εἶναι ἄρτιος} \\ 1 & \text{ἂν ὁ } (a - x_k^2)/2^k \text{ εἶναι περιττός.} \end{cases}$$

Μὲ αὐτὸν τὸν τρόπο ὑπολογίζομε x_{k+1} τέτοιον ὥστε $x_{k+1}^2 \equiv a \pmod{2^{k+1}}$.

Συνοψίζοντας τὴν κατασκευαστικὴ μέθοδο τῆς ἀπόδειξης, ἔχομε τὰ ἑξῆς: Ξεκινώντας μὲ x_3, τέτοιον ὥστε $x_3^2 \equiv a \pmod{2^3}$,[5] κατασκευάζομε, διαδοχικά, τοὺς

[5] Σὲ κάθε περίπτωση μποροῦμε νὰ πάρομε $x_3 \in \{1, 3, 5, 7\}$.

ἀκεραίους $x_4, \ldots, x_k, x_{k+1}, \ldots, x_n$, ἔτσι ὥστε:

$$\begin{array}{lll}
x_3^2 \equiv a \pmod{2^3} & & \\
x_4^2 \equiv a \pmod{2^4}, & x_4 = x_3 + y_2 2^2 & \\
x_5^2 \equiv a \pmod{2^5}, & x_5 = x_4 + y_3 2^3 = x_3 + y_2 2^2 + y_3 2^3 & \\
\vdots & \vdots & \\
x_{k+1}^2 \equiv a \pmod{2^{k+1}}, & x_{k+1} = x_k + y_{k-1} 2^{k-1} = x_3 + y_2 2^2 + y_3 2^3 + \cdots + y_{k-1} 2^{k-1} & \\
\vdots & \vdots & \\
x_n^2 \equiv a \pmod{2^n}, & x_n = x_{n-1} + y_{n-2} 2^{n-2} = x_3 + y_2 2^2 + y_3 2^3 + \cdots + y_{n-2} 2^{n-2}. &
\end{array}$$

Παρατηρῆστε ὅτι $y_i \in \{0, 1\}$ καὶ $x_3 \in \{1, 3, 5, 7\} = \{1, 1 + 2, 1 + 2^2, 1 + 2 + 2^2\}$, ὁπότε ἡ λύση x_n εἶναι γραμμένη καὶ στὸ δυαδικὸ σύστημα.
Μένει τώρα νὰ δείξομε ὅτι, ἂν $n \geq 3$ καὶ $x_n \bmod 2^n$ εἶναι μία λύση τῆς ἰσοτιμίας (4.17), τότε οἱ κλάσεις (4.18) εἶναι, ἐπίσης, λύσεις τῆς ἴδιας ἰσοτιμίας καί, μάλιστα, διαφορετικές, ἐπιπλέον δέ, κάθε ἀκέραιος x_0, ποὺ ἐπαληθεύει τὴν ἰσοτιμία, ἀνήκει σὲ μία ἀπὸ αὐτὲς τὶς τέσσερεις κλάσεις. Τὸ ὅτι οἱ κλάσεις αὐτὲς εἶναι λύσεις τῆς ἰσοτιμίας (4.17), μὲ δεδομένο ὅτι ἡ $x_a \bmod 2^n$ εἶναι λύση της, φαίνεται ἀμέσως, ὕστερα ἀπὸ λίγες ἁπλούστατες πράξεις. Ἁπλό, ἐπίσης, εἶναι νὰ δείξει κανεὶς ὅτι οἱ τέσσερεις κλάσεις εἶναι διαφορετικές. Γιὰ παράδειγμα, ἂν ἦταν $x_n \equiv -x_n + 2^{n-1} \pmod{2^n}$, τότε θὰ ἔπρεπε $x_n \equiv 2^{n-2} \pmod{2^{n-1}}$· ἀδύνατον, ἀφοῦ ὁ x_n εἶναι περιττός. Τὸ ἴδιο ἁπλᾶ ἀποκλείεται ἡ ἰσότητα δύο ὁποιωνδήποτε κλάσεων (4.17).
Τέλος, ἂν $x_0^2 \equiv a \pmod{2^n}$ $(n \geq 3)$ καὶ $x_n^2 \equiv a \pmod{2^n}$, τότε $(x_0 + x_n)(x_0 - x_n) \equiv 0 \pmod{2^n}$. Ἀπὸ τὴν ἄσκηση 9 τοῦ κεφαλαίου 1, ἀκριβῶς ἕνας ἀπὸ τοὺς δύο ἀκεραίους ἀριθμοὺς $(x_0 + x_n)/2$, $(x_0 - x_n)/2$ εἶναι περιττός. Ἂν ὁ $(x_0 + x_n)/2$ εἶναι περιττός, τότε ὁ $x_0 + x_n$ διαιρεῖται ἀπὸ τὸ 2, ἀλλὰ ὄχι ἀπὸ τὸ 4, συνεπῶς, ἡ τελευταία ἰσοτιμία μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι ὁ $x_0 - x_n$ διαιρεῖται ἀπὸ τὸ 2^{n-1}. Ἔστω $x_0 - x_n = 2^{n-1} m$. Ἂν ὁ m εἶναι ἄρτιος, ἔστω $m = 2r$, τότε $x_0 - x_n = 2^n r$, ἄρα $x_0 \equiv x_n \pmod{2^n}$. Ἂν ὁ m εἶναι περιττός, ἔστω $m = 2r + 1$, τότε $x_0 - x_n = 2^n r + 2^{n-1}$, ἄρα $x_0 \equiv x_n + 2^{n-1} \pmod{2^n}$. **ὅ.ἔ.δ.**

Παράδειγμα. Ἐφαρμόζομε τὴ μέθοδο ποὺ περιγράφεται στὴν ἀπόδειξη τοῦ Θεωρήματος 4.4.2 γιὰ νὰ ἐπιλύσομε τὴν ἰσοτιμία $x^2 \equiv 41 \pmod{2^8}$.
Κατ᾽ ἀρχάς, $41 \equiv 1 \pmod 8$, ἄρα ἡ ἰσοτιμία ἔχει λύση· μάλιστα, ἀκριβῶς τέσσερις λύσεις.
Ξεκινοῦμε ἀπὸ μία ὁποιαδήποτε λύση τῆς $x^2 \equiv 1 \pmod 8$, π.χ. $x_3 \equiv 1 \pmod 8$.

Περιγράφομε συνοπτικὰ τὴν ἐπίλυση ὡς ἑξῆς:

$$
\begin{array}{ll}
x_3 = 1 & \\
x_4 = 1 + 4y_2, & (1+4y_2)^2 \equiv 41 \pmod{2^4} \\
& 1 + 8y_2 \equiv 41 \pmod{2^4} \\
& 8y_2 \equiv 40 \pmod{2^4} \\
& y_2 \equiv 5 \pmod{2} \to y_2 = 1 \to x_4 = 1 + 4\cdot 1 = 5 = 1 + 2^2 \\
x_5 = 5 + 8y_3, & (5+8y_3)^2 \equiv 41 \pmod{2^5} \\
& 25 + 16y_3 \equiv 41 \pmod{2^5} \\
& 16y_3 \equiv 16 \pmod{32} \\
& y_3 \equiv 1 \pmod{2} \to y_3 = 1 \to x_5 = 5 + 8\cdot 1 = 13 = 1 + 2^2 + 2^3 \\
x_6 = 13 + 16y_4, & (13+16y_4)^2 \equiv 41 \pmod{2^6} \\
& 169 + 32y_4 \equiv 41 \pmod{2^6} \\
& 32y_4 \equiv -128 \pmod{64} \\
& y_4 \equiv -4 \pmod{2} \to y_4 = 0 \to x_6 = 13 + 16\cdot 0 = 13 = 1 + 2^2 + 2^3 \\
x_7 = 13 + 32y_5, & (13+32y_5)^2 \equiv 41 \pmod{2^7} \\
& 169 + 64y_5 \equiv 41 \pmod{2^7} \\
& 64y_5 \equiv -128 \pmod{128} \\
& y_5 \equiv -2 \pmod{2} \to y_5 = 0 \to x_7 = 13 + 32\cdot 0 = 13 = 1 + 2^2 + 2^3 \\
x_8 = 13 + 64y_6, & (13+64y_6)^2 \equiv 41 \pmod{2^8} \\
& 169 + 128y_6 \equiv 41 \pmod{2^8} \\
& 128y_6 \equiv -128 \pmod{256} \\
& y_6 \equiv -1 \pmod{2} \to y_6 = 1 \to x_8 = 13 + 64\cdot 1 = 77 = 1 + 2^2 + 2^3 + 2^6.
\end{array}
$$

Ἄρα, μία λύση εἶναι ἡ $x_8 \equiv 77(\bmod 2^8)$. Σύμφωνα μὲ τὸ Θεώρημα, οἱ ὑπόλοιπες τρεῖς λύσεις εἶναι οἱ $-77 \equiv 179,\ 77 + 2^7 = 205,\ -77 + 2^7 = 51 \pmod{2^8}$.

Ἔστω τώρα $m > 1$ καὶ

$$m = 2^{n_0} p_1^{n_1} \cdots p_k^{n_k} \tag{4.19}$$

εἶναι ἡ κανονικὴ ἀνάλυση τοῦ m σὲ πρώτους παράγοντες, ὅπου

- $p_1, \ldots, p_k$ εἶναι περιττοὶ πρῶτοι.
- $n_0 \geq 0$, $k \geq 0$, ἀλλὰ ἕνας τουλάχιστον ἀπὸ τοὺς δύο εἶναι θετικός.

Θὰ ἀσχοληθοῦμε μὲ τὴν ἐπίλυση τῆς ἰσοτιμίας

$$x^2 \equiv a \pmod{m}, \quad (a, m) = 1. \tag{4.20}$$

Εἶναι σαφὲς ὅτι, ἂν $x \equiv c(\bmod m)$ εἶναι λύση τῆς (4.20), τότε $x \equiv c(\bmod p_i^{n_i})$ εἶναι λύση τῆς $x^2 \equiv a(\bmod p_i^{n_i})$ γιὰ κάθε $i = 1, \ldots, k$, καθὼς καὶ $x \equiv c(\bmod 2^{n_0})$ εἶναι λύση τῆς $x^2 \equiv a(\bmod 2^{n_0})$. Ἄρα, κάθε λύση τῆς (4.20) δίνει λύση σὲ κάθε μία ἀπὸ τὶς ἰσοτιμίες $x^2 \equiv a(\bmod 2^{n_0})$, $x^2 \equiv a(\bmod p_i^{n_i})$ $(i = 1, \ldots, k)$. Ἀντιστρόφως, ἂς πάρομε, γιὰ κάθε μία ἀπὸ τὶς ἰσοτιμίες αὐτές, μία ὁποιαδήποτε λύση της, δηλαδή, ἔστω ὅτι οἱ $x_0, x_1, \ldots, x_k$ εἶναι τέτοιοι ὥστε, $x \equiv x_0 (\text{mod } 2^{n_0})$ εἶναι λύση τῆς $x^2 \equiv a$ $(\text{mod } 2^{n_0})$ καί, γιὰ $i = 1, \ldots, k$, εἶναι $x \equiv x_i (\text{mod } p_i^{n_i})$ λύση τῆς $x^2 \equiv a (\text{mod } p_i^{n_i})$. Τότε, ἀπὸ τὸ Θεώρημα 3.3.1, ὑπάρχει ἀκριβῶς ἕνα c mod m, τέτοιο ὥστε $c \equiv x_0$ $(\text{mod } 2^{n_0})$ καὶ $c \equiv x_i (\text{mod } p_i^{n_i})$ γιὰ $i = 1, \ldots, k$. Συνεπῶς, $c^2 \equiv x_0^2 \equiv a (\text{mod } 2^{n_0})$ καὶ $c^2 \equiv x_i^2 \equiv a (\text{mod } p_i^{n_i})$ γιὰ $i = 1, \ldots, k$. Ἄρα ὁ $c^2 - a$ διαιρεῖται ἀπὸ καθέναν ἀπὸ τοὺς ἀριθμοὺς $2^{n_0}, p_1^{n_1}, \ldots, p_k^{n_k}$. Αὐτοὶ οἱ ἀριθμοὶ εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους, ἄρα, ὁ $c^2 - a$ διαιρεῖται καὶ ἀπὸ τὸ γινόμενό τους, ποὺ εἶναι m· μ' ἄλλα λόγια, $c^2 \equiv a (\text{mod } m)$. Πόσες ἐπιλογὲς εἶναι δυνατὲς γιὰ τὴν $(k + 1)$-άδα $(x_0, x_1, \ldots, x_k)$; Ἂν $n_0 \geq 1$, τότε βάσει τοῦ Θεωρήματος 4.4.2 ἔχομε 1,2, ἢ 4 ἐπιλογές, ἀνάλογα μὲ τὸ ἂν $n_0 = 1, 2$ ἢ ≥ 3, ἀντιστοίχως, ἐνῶ, γιὰ $i = 1, \ldots, k$, βάσει τοῦ Θεωρήματος 4.4.1, ἔχομε δύο ἐπιλογὲς γιὰ τὸ x_i. Μὲ αὐτὲς τὶς παρατηρήσεις, οὐσιαστικά, ἀποδείξαμε τὸ ἑξῆς:

Θεώρημα 4.4.3 *Ἀναγκαία καὶ ἱκανὴ συνθήκη γιὰ νὰ ἔχει λύση ἡ ἰσοτιμία (4.20), ὅταν ἡ κανονικὴ ἀνάλυση τοῦ m δίδεται ἀπὸ τὴ σχέση (4.19), εἶναι νὰ ἱκανοποιοῦνται ὅλες οἱ παρακάτω συνθῆκες:*

$$\left(\frac{a}{p_i}\right) = 1 \quad \textit{γιὰ ὅλα τὰ } i = 1, \ldots, k$$

$$a \equiv 1 \begin{cases} (\text{mod } 4) & \textit{ἂν } n_0 = 2 \\ (\text{mod } 8) & \textit{ἂν } n \geq 3 \end{cases}$$

Στὴν περίπτωση, ποὺ ἔχει λύση ἡ ἰσοτιμία, τὸ πλῆθος τῶν λύσεών της , εἶναι

$$2^k, \textit{ ἂν } n_0 = 0 \textit{ ἢ } 1, \qquad 2^{k+1}, \textit{ ἂν } n = 2, \qquad 2^{k+2}, \textit{ ἂν } n \geq 3.$$

ὅ.ἔ.δ.

Παράδειγμα. Θὰ λύσομε τὴν ἰσοτιμία $x^2 \equiv 13 (\text{mod } 3^4\, 17^2)$. Λύνομε κάθε μία ἰσοτιμία $x^2 \equiv 13 (\text{mod } 3^4)$ καὶ $x^2 \equiv 13 (\text{mod } 17^2)$, ὅπως στὸ παράδειγμα μετὰ τὸ Θεώρημα 4.4.1, καὶ βρίσκομε ὅτι, οἱ λύσεις τῆς πρώτης εἶναι $x \equiv 16, 65 (\text{mod } 3^4)$ καὶ τῆς δεύτερης εἶναι οἱ $x \equiv 59, 230 (\text{mod } 17^2)$. Μὲ τὴ βοήθεια τοῦ Θεωρήματος 3.3.1 λύνομε τὸ σύστημα $x \equiv a (\text{mod } 3^4)$, $x \equiv b (\text{mod } 17^2)$ ὅταν $a \in \{16, 65\}$ καὶ $b \in \{59, 230\}$. Οἱ λύσεις, γιὰ καθένα συνδυασμὸ (a, b) φαίνονται στὸν παρακάτω πίνακα:

(a, b)	$x \pmod{3^4 17^2}$
$(16, 59)$	8440
$(16, 230)$	6010
$(65, 59)$	17399
$(65, 230)$	14969

Ἄρα, ὅλες οἱ λύσεις τῆς $x^2 \equiv 13 (\text{mod } 3^4 17^2)$ εἶναι οἱ $x \equiv 8440,\ 6010,\ 17399,\ 14969$ $(\text{mod } 3^4 17^2)$.

Σημείωση. Στὴν περίπτωση ποὺ $(a, m) > 1$, ἡ ἐπίλυση τῆς $x^2 \equiv a(\text{mod } m)$ ἀνάγεται, μὲ τὴ βοήθεια τῆς ἀσκήσεως 17, σὲ ὅμοιας μορφῆς ἰσοτιμία μὲ νέα a καὶ m, γιὰ τὴν ὁποία, εἴτε δὲν ὑπάρχει λύση, εἴτε ὁ μέγιστος κοινὸς διαιρέτης τῶν νέων a, m εἶναι μικρότερος –ἀκριβέστερα, εἶναι διαιρέτης– τοῦ μεγίστου κοινοῦ διαιρέτη τῶν προηγουμένων a, m. Ἔτσι, βῆμα πρὸς βῆμα, ἂν δὲν καταλήξομε σὲ ἀδύνατη ἰσοτιμία, θὰ φτάσομε, ὕστερα ἀπὸ πεπερασμένο πλῆθος βημάτων, σὲ ἰσοτιμία (4.20), στὴν ὁποία $(a, m) = 1$.

4.5 Ἀσκήσεις τοῦ κεφαλαίου 4

1. Ὑπολογῖστε ὅλα τὰ στοιχεῖα τοῦ κατ' ἀπόλυτη τιμὴ ἐλαχίστου συστήματος ὑπολοίπων μέτρῳ p, τὰ ὁποῖα εἶναι τετραγωνικὰ ἰσοϋπόλοιπα μέτρῳ p, γιὰ $p = 17$ καὶ $p = 19$, ἀντιστοίχως. Γιατὶ στὴ μία περίπτωση τὰ στοιχεῖα αὐτὰ εἶναι ἀνὰ ζεύγη ἀντίθετα καὶ στὴν ἄλλη ὄχι;

2. Ἀποδεῖξτε τὴν ἑξῆς πολὺ ἁπλῆ, πρόταση, τῆς ὁποίας χρήση γίνεται πολὺ συχνά: Ἂν $\epsilon, \eta \in \{-1, 1\}$ καὶ $\epsilon \equiv \eta(\text{mod } p)$, τότε $\epsilon = \eta$.

3. Ἀποδεῖξτε τὴν πρόταση 4.1.1 βασισμένοι στὴν ἄσκηση 8 (β΄) τοῦ κεφαλαίου 3.

4. Ἔστω $N = x^2 + y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξύ τους. Ἀποδεῖξτε ὅτι ὅλοι οἱ περιττοὶ πρῶτοι διαιρέτες τοῦ N εἶναι τῆς μορφῆς $4k + 1$.

5. Ἔστω $N = x^2 - 2y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξύ τους καὶ ὁ x εἶναι περιττός. Ἀποδεῖξτε ὅτι, ἂν ἕνας πρῶτος p διαιρεῖ τὸν N, τότε ὁ p εἶναι ἢ τῆς μορφῆς $8k + 1$ ἢ τῆς μορφῆς $8k + 7$.

6. Ἔστω $N = x^2 + 2y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξύ τους καὶ ὁ x εἶναι περιττός. Ἀποδεῖξτε ὅτι, ἂν ἕνας πρῶτος p διαιρεῖ τὸν N, τότε ὁ p εἶναι ἢ τῆς μορφῆς $8k + 1$ ἢ τῆς μορφῆς $8k + 3$.

7. Ὑπολογῖστε τὴν τιμὴ τοῦ συμβόλου $\left(\frac{7}{13}\right)$. Στὴ συνέχεια, γιὰ $p = 13$ καὶ $a = 7$: Γρᾶψτε τὶς σχέσεις (4.5) (6 ἰσοτιμίες mod 13), καὶ ἐπαληθεῦστε τὶς σχέσεις (4.6) καὶ (4.7).
   Ἐπαναλάβετε τὴν ἄσκηση γιὰ $p = 19$ καὶ $a = 5$.

8. Ἂν οἱ p, q εἶναι διαφορετικοὶ περιττοὶ πρῶτοι, τότε δὲν ὑπάρχουν ἀκέραιοι x, y, μὲ $1 \leq x \leq p'$ καὶ $1 \leq y \leq q'$, τέτοιοι ὥστε $y = qx/p$.

9. Γιὰ $q = 23$, $p = 17$ καὶ γιὰ κάθε $k = 1, 2, \ldots, p' = 8$, χωριστά, ἐπαληθεῦστε τὸν ἰσχυρισμὸ στὴν ἀπόδειξη τοῦ θεωρήματος 4.2.3 ὅτι $[\frac{q}{p}k]$ εἶναι τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων, τὰ ὁποῖα βρίσκονται ἐπὶ τῆς εὐθείας $x = k$ καὶ «κάτω ἀπὸ τὴν εὐθεία» ϵ, τὴν ὁποία θεωρήσαμε στὴ σελίδα 61.

10. Γιὰ $q = 23$, $p = 17$ καὶ γιὰ κάθε $\ell = 1, 2, \ldots, q' = 11$, χωριστά, ἐπαληθεῦστε τὸν ἰσχυρισμὸ στὴν ἀπόδειξη τοῦ θεωρήματος 4.2.3 ὅτι $[\frac{p}{q}\ell]$ δείχνει τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων, τὰ ὁποῖα βρίσκονται ἐπὶ τῆς εὐθείας $y = \ell$ καὶ «ἀριστερὰ τῆς εὐθείας» ϵ, τὴν ὁποία θεωρήσαμε στὴ σελίδα 61.

11. Γιὰ $q = 23$ καὶ $p = 17$ ἐπαληθεῦστε τὸν ἰσχυρισμὸ στὴν ἀπόδειξη τοῦ θεωρήματος 4.2.3 ὅτι τὸ ἄθροισμα στὸ ἀριστερὸ μέλος τῆς σχέσης (4.11) ἰσοῦται μὲ τὸ πλῆθος τῶν θετικῶν ἀκεραίων σημείων ἐντὸς τοῦ ὀρθογωνίου παραλληλογράμμου, τὸ ὁποῖο ὁρίζεται ἀπὸ τοὺς θετικοὺς ἡμιάξονες καὶ τὶς εὐθεῖες $x = p'$ καὶ $y = q'$·

12. Ὁ $p = 104779$ εἶναι πρῶτος. Ὑπολογῖστε τὴν τιμὴ τοῦ συμβόλου $\left(\frac{a}{p}\right)$ γιὰ $a = 194,\ 120400,\ 18660,\ -14530,\ -1821000$ μὲ χρήση τοῦ συμβόλου τοῦ Jacobi.

13. Ἀποδεῖξτε ὅτι, ἂν ὁ p εἶναι πρῶτος > 3, τότε $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Ἀποδεῖξτε μετὰ ὅτι ἕνας πρῶτος p τῆς μορφῆς $3k + 2$ δὲν μπορεῖ νὰ διαιρεῖ ἀριθμὸ τῆς μορφῆς $x^2 + 3y^2$, ὅπου οἱ x, y εἶναι ἀκέραιοι καὶ $(x, 3y) = 1$.

14. Ἔστω $P > 1$ περιττὸς. Ἔστω P_0 ὁ ἀριθμός, ποὺ σχηματίζεται ἀπὸ τὸ γινόμενο ὅλων τῶν διαφορετικῶν πρώτων διαιρετῶν τοῦ P, οἱ ὁποῖοι ἐμφανίζονται μὲ περιττὸ ἐκθέτη στὴν κανονικὴ ἀνάλυση τοῦ P. Ἀποδεῖξτε ὅτι, γιὰ κάθε a πρῶτο πρὸς τὸν P, ἰσχύει $\left(\frac{a}{P}\right) = \left(\frac{a}{P_0}\right)$.

15. Ἔστω $P_0 = p_1 \cdots p_n$, ὅπου $p_1, \ldots, p_n$ εἶναι διαφορετικοὶ περιττοὶ πρῶτοι. Ἀποδεῖξτε, μὲ ἐπαγωγὴ στὸ n, ὅτι ὑπάρχει b, τέτοιος ὥστε $\left(\frac{b}{P_0}\right) = -1$.
Ὑπόδειξη. Γιὰ τὸ ἐπαγωγικὸ βῆμα ἀπὸ τὸ k στὸ $k+1$, κάνετε τὸ ἑξῆς: Ἔστω c, τέτοιος ὥστε $\left(\frac{c}{p_1 \cdots p_k}\right) = -1$ καὶ d, τέτοιος ὥστε $\left(\frac{d}{p_{k+1}}\right) = 1$. Δεῖξτε ὅτι ὑπάρχει b, τέτοιος ὥστε $b \equiv c \pmod{p_1 \cdots p_k}$ καὶ $b \equiv d \pmod{p_{k+1}}$ καὶ γι' αὐτὸν τὸν b, τότε, $\left(\frac{b}{p_1 \cdots p_k p_{k+1}}\right) = -1$.

16. Ἔστω $P > 1$ περιττός. Συνδυᾶστε τὶς δύο προηγούμενες ἀσκήσεις γιὰ νὰ συμπεράνετε πρῶτα ὅτι ὑπάρχει b, πρῶτος πρὸς τὸν P, τέτοιος ὥστε $\left(\frac{b}{P}\right) = -1$ καί, στὴ συνέχεια, ἀποδεῖξτε ὅτι, ἂν R εἶναι ἕνα περιορισμένο σύστημα ὑπολοίπων μέτρῳ P, τότε

$$\sum_{a \in R} \left(\frac{a}{P}\right) = 0\,.$$

Ὑπόδειξη. Τὸ σύνολο $\{ab\ :\ a \in R\}$ εἶναι, ἐπίσης, περιορισμένο σύστημα ὑπολοίπων. Ἀφ' ἑτέρου, τὸ ἄθροισμα τῶν συμβόλων Jacobi, καθὼς ὁ «ἀριθμητὴς» τοῦ συμβόλου διατρέχει ἕνα περιορισμένο σύστημα ὑπολοίπων, δὲν ἀλλάζει ἂν ἀντικαταστήσομε αὐτὸ τὸ σύστημα μὲ ἕνα ἄλλο περιορισμένο σύστημα ὑπολοίπων.

17. Ἔστω ὅτι ἔχομε νὰ λύσομε τὴν ἰσοτιμία $x^2 \equiv a \pmod{m}$ καὶ οἱ a, m ἔχουν ἕνα κοινὸ πρῶτο διαιρέτη p. Ἔστω $a = pa_1$, $m = pm_1$. Ἀποδεῖξτε ὅτι κάθε x,

ποὺ ἱκανοποιεῖ τὴν ἰσοτιμία, πρέπει νὰ διαιρεῖται διὰ p καί, μετά, θέσετε $x = px_1$, ὁπότε ἡ ἰσοτιμία θὰ ἀναχθεῖ στὴν $px_1^2 \equiv a_1 \pmod{m_1}$. Δεῖξτε τὰ ἑξῆς, σχετικὰ μὲ τὴν τελευταία ἰσοτιμία:
(i) Ἂν $(p, m_1) = 1$, τότε ἀναγόμαστε σὲ ἰσοτιμία $x_1^2 \equiv a_1' \pmod{m_1}$, ὅπου ὁ a_1' εἶναι κάποιος ἀκέραιος μὲ $(a_1', m_1) = (b, m)/p$.
(ii) Ἂν $(p, m_1) = p$ καὶ $p|a_1$, τότε ἀναγόμαστε σὲ ἰσοτιμία $x_1^2 \equiv a_2 \pmod{m_2}$, ὅπου $a_2 = b_1/p$, $m_2 = m_1/p$ καὶ $(a_2, m_2) = (a, m)/p^2$.
(iii) Ἂν $(p, m_1) = p$ καὶ ὁ p δὲν διαιρεῖ τὸν a_1, τότε ἡ ἰσοτιμία εἶναι ἀδύνατη.

18. Ἐπιλῦστε κάθε μία ἀπὸ τὶς παρακάτω ἰσοτιμίες:

$$x^2 \equiv 6 \pmod{43^3}, \quad x^2 \equiv -1 \pmod{5^5}, \quad x^2 \equiv 6 \pmod{43^3\,5^2}.$$

Γιὰ τὴν ἐπίλυσή τους, ἐργαστεῖτε, στὴν περίπτωση τῶν δύο πρώτων, ὅπως στὸ παράδειγμα ἀμέσως μετὰ τὸ Θεώρημα 4.4.1, ἐνῶ στὴν περίπτωση τῆς τρίτης, ὅπως στὸ παράδειγμα ἀμέσως μετὰ τὸ Θεώρημα 4.4.3.

19. Ἐπιλῦστε τὴν ἰσοτιμία $x^2 \equiv 17 \pmod{2^{13}}$ ἀκολουθώντας τὸν τρόπο τοῦ παραδείγματος ἀμέσως μετὰ τὸ Θεώρημα 4.4.2.

Κεφάλαιο 5

Γεννήτορες καὶ διακριτοὶ λογάριθμοι

Στὸ κεφάλαιο αὐτό, τὸ p συμβολίζει πάντα περιττὸ πρῶτο.
Τα λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους

5.1 Γεννήτορες

Ἔστω $m > 1$ καὶ $(a, m) = 1$. Τὸ σύνολο $\{k > 0 : a^k \equiv 1 \pmod{m}\}$ εἶναι μὴ κενό, ἀφοῦ, γιὰ παράδειγμα, περιέχει τὸν $\phi(m)$, λόγῳ τοῦ θεωρήματος τοῦ Euler (2.2.4). Τὸ ἐλάχιστο στοιχεῖο αὐτοῦ τοῦ συνόλου λέγεται *τάξη* τοῦ a μέτρῳ m καὶ συμβολίζεται $\mathrm{ord}_m(a)$.

> Ἡ χρήση τοῦ συμβολισμοῦ $\mathrm{ord}_m(a)$ σημαίνει, ἀκόμη κι ἂν αὐτὸ δὲν δηλώνεται, ὅτι $(a, m) = 1$.

Οἱ βασικὲς ἰδιότητες τῆς συνάρτησης ord_m περιλαμβάνονται στὸ παρακάτω θεώρημα.

Θεώρημα 5.1.1 *Ἔστω $m > 1$, $(a, m) = 1$ καὶ $r = \mathrm{ord}_m(a)$. Τότε:*

α΄. Ἡ ἰσοτιμία $a^k \equiv 1 \pmod{m}$ ἰσοδυναμεῖ μὲ τὴν $k \equiv 0 \pmod{r}$. Εἰδικώτερα, $r | \phi(m)$.

β΄. Ἡ ἰσοτιμία $a^k \equiv a^\ell \pmod{m}$ ἰσοδυναμεῖ μὲ τὴν $k \equiv \ell \pmod{r}$.

γ΄. Οἱ ἀριθμοὶ $1, a, \dots, a^{r-1}$ εἶναι ἀνισότιμοι μέτρῳ m καὶ κάθε δύναμη τοῦ a (μὴ ἀρνητικοῦ ἐκθέτη) εἶναι ἰσότιμη μέτρῳ m μὲ κάποιον ἀπὸ αὐτοὺς τοὺς r τὸ πλῆθος ἀριθμούς.

Ἀπόδειξη α΄. Ἡ εὐκλείδεια διαίρεση τοῦ k διὰ r μᾶς δίνει $k = rq + v$, ὅπου $0 \le v < r$. Ἐξ ὑποθέσεως, $a^r \equiv 1 \pmod{m}$, ἄρα $a^k \equiv a^v \pmod{m}$. Ἂν $r | k$, τότε $v = 0$, ἄρα $a^k \equiv 1 \pmod{m}$. Ἀντιστρόφως, ἂν $a^k \equiv 1 \pmod{m}$, τότε $a^v \equiv 1 \pmod{m}$. Συνδυάζοντας αὐτὴ τὴν ἰσοτιμία μὲ τὸν ὁρισμὸ τοῦ r, καταλήγομε στὸ συμπέρασμα

ὅτι ὁ r δὲν μπορεῖ νὰ εἶναι θετικός. Ἄρα, $r = 0$, ὁπότε $r|k$.
β′. Ἔστω $k \geq \ell$, ὁπότε ἡ ἰσοτιμία $a^k \equiv a^\ell \pmod{m}$ ἰσοδυναμεῖ μὲ τὴν $a^{k-\ell} \equiv 1 \pmod{m}$. Ἀπὸ τὸ (α′), ἡ τελευταία ἰσοτιμία ἰσοδυναμεῖ μὲ τὴν $k - \ell \equiv 0 \pmod{m}$.
γ′. Ἂν ἦταν $a^k \equiv a^\ell \pmod{m}$ μὲ $0 \leq k < \ell \leq r-1$, τότε, σύμφωνα μὲ τὸ (β′) θὰ εἴχαμε $r|(\ell - k)$, ποὺ εἶναι ἀδύνατον, ἀφοῦ $1 \leq \ell - k < r$. Τέλος, ἔστω $k \geq 0$. Εἶναι $k \equiv i \pmod{r}$ γιὰ κάποιο $i \in \{0, 1, \dots, r-1\}$ ἄρα, ἀπὸ τὸ β′, $a^k \equiv a^i \pmod{m}$.

ὅ.ἔ.δ.

Ἂν $\mathrm{ord}_m(a) = \phi(m)$, τότε ὁ a χαρακτηρίζεται ὡς *γεννήτορας* μέτρῳ m.

Θεώρημα 5.1.2 *Ὁ πρῶτος πρὸς τὸν m ἀκέραιος a εἶναι γεννήτορας μέτρῳ m ἄν, καὶ μόνο ἄν, οἱ ἀριθμοὶ $a, a^2, \dots, a^{\phi(m)}$ ἀποτελοῦν περιορισμένο σύστημα ὑπολοίπων μέτρῳ m.*

Ἀπόδειξη Ἔστω ὅτι ὁ a εἶναι γεννήτορας μέτρῳ m, ὁπότε $\mathrm{ord}_m(a) = \phi(m)$. Ἀπὸ τὸ γ′ τοῦ θεωρήματος 5.1.1, οἱ ἀριθμοὶ $1 \equiv a^{\phi(m)}, a, a^2, \dots, a^{\phi(m)-1}$ εἶναι ἀνισότιμοι μέτρῳ m καὶ τὸ πλῆθος τους εἶναι $\phi(m)$, συνεπῶς ἀποτελοῦν περιορισμένο σύστημα ὑπολοίπων μέτρῳ m.

Ἀντιστρόφως, ἔστω ὅτι οἱ $\phi(m)$ τὸ πλῆθος ἀριθμοὶ $a, a^2, \dots, a^{\phi(m)}$ ἀποτελοῦν περιορισμένο σύστημα ὑπολοίπων μέτρῳ m· εἰδικώτερα, οἱ $\phi(m)$ τὸ πλῆθος αὐτὲς δυνάμεις εἶναι ἀνισότιμες μέτρῳ m. Ἔστω τώρα ὅτι $\mathrm{ord}_m(a) = r$. Ἀπὸ τὸ α′ τοῦ θεωρήματος 5.1.1 ξέρομε ὅτι $r|\phi(m)$, ἄρα $r \leq \phi(m)$. Ἀλλά, ἀπὸ τὸ γ′ τοῦ ἴδιου θεωρήματος, ὑπάρχουν ἀκριβῶς r τὸ πλῆθος δυνάμεις τοῦ a (μὴ ἀρνητικοῦ ἐκθέτη) ἀνισότιμες μέτρῳ m, ἄρα, ἀπὸ τὴν παρατήρηση λίγες γραμμὲς παραπάνω, $\phi(m) \leq r$, ὁπότε $r = \phi(m)$. **ὅ.ἔ.δ.**

Θεώρημα 5.1.3 *α′. Γιὰ κάθε a πρῶτο πρὸς τὸν m καὶ κάθε θετικὸ ἀκέραιο k ἰσχύει*

$$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), k)} .$$

β′. Ἂν ὁ g εἶναι γεννήτορας μέτρῳ m, τότε ὅλοι οἱ ἀριθμοὶ g^k μὲ $1 \leq k \leq \phi(m)$ καὶ $(k, \phi(m)) = 1$ εἶναι, ἐπίσης, γεννήτορες μέτρῳ m, ἀνισότιμοι μεταξύ τους καὶ κάθε γεννήτορας μέτρῳ m εἶναι ἰσότιμος μὲ ἕναν ἀπὸ αὐτοὺς τοὺς ἀριθμούς. Συνεπῶς, ὑπάρχουν ἀκριβῶς $\phi(\phi(m))$ τὸ πλῆθος ἀνισότιμοι γεννήτορες μέτρῳ m.

Ἀπόδειξη α′. Ἔστω $\mathrm{ord}_m(a) = n$. Γιὰ κάθε θετικὸ ἀκέραιο ℓ, ποὺ ἐπαληθεύει τὴν ἰσοτιμία $(a^k)^\ell \equiv 1 \pmod{m}$, ἰσχύει, βάσει τοῦ α′ τοῦ θεωρήματος 5.1.1, ὅτι $n|k\ell$, δηλαδή, ὁ $k\ell$ εἶναι κοινὸ πολλαπλάσιο τῶν k καὶ n. Συνεπῶς, ἂν $\ell = r$ εἶναι ὁ ἐλάχιστος τέτοιος ἀκέραιος ℓ, τότε ὁ kr εἶναι τὸ *ἐλάχιστο* κοινὸ πολλαπλάσιο τῶν k, n. Μ’ ἄλλα λόγια, ἂν $\mathrm{ord}_m(a^k) = r$, τότε $kr = [k, n] =$ (θεώρημα 1.3.1-α′) $\frac{kn}{(k,n)}$, ἀπ’ ὅπου ἡ ἀποδεικτέα σχέση $r = \frac{n}{(n,k)}$.
β′. Ἕνας ἀκέραιος b εἶναι γεννήτορας μέτρῳ m ἄν, καὶ μόνο ἄν, εἶναι πρῶτος πρὸς τὸν m καὶ ἡ τάξη του μέτρῳ m εἶναι $\phi(m)$. Βάσει τοῦ θεωρήματος 5.1.2, ἡ συνθήκη αὐτὴ ἰσοδυναμεῖ μὲ τὸ ὅτι ὁ b εἶναι ἰσότιμος μέτρῳ m μὲ κάποιον ἀριθμὸ g^k, ὅπου $1 \leq k \leq \phi(m)$ καὶ ἡ τάξη τοῦ g^k μέτρῳ m εἶναι $\phi(m)$. Βάσει τοῦ (α′),

$$\mathrm{ord}_m(g^k) = \frac{\phi(m)}{(\phi(m), k)} ,$$

ἄρα, $\mathrm{ord}_m(g^k) = \phi(m)$ ἄν, καὶ μόνο ἄν, ὁ k εἶναι πρῶτος πρὸς τὸν $\phi(m)$.

Ἀνακεφαλαιώνοντας τὰ παραπάνω ἔχομε ὅτι, ὁ b εἶναι γεννήτορας μέτρῳ m ἄν, καὶ μόνο ἄν, εἶναι ἰσότιμος μέτρῳ m μὲ ἕναν ἀριθμὸ g^k, ὅπου $1 \le k \le \phi(m)$ καὶ $(k, \phi(m)) = 1$. Ἐπιπλέον, ἀπὸ τὸ θεώρημα 5.1.2, ὅλοι οἱ τέτοιοι ἀριθμοὶ g^k –τὸ πλῆθος τους, προφανῶς, εἶναι $\phi(m)$– εἶναι ἀνισότιμοι μέτρῳ m. **ὅ.ἔ.δ.**

Θεώρημα 5.1.4 *Γιὰ τὰ α΄ καὶ β΄, παρακάτω, ὑποθέτομε ὅτι οἱ a, b εἶναι πρῶτοι πρὸς τὸ μέτρο $m > 1$ καὶ $\mathrm{ord}_m(a) = r$, $\mathrm{ord}_m(b) = s$.*

α΄. Ἄν $(r, s) = 1$, τότε, $\mathrm{ord}_m(ab) = rs$.

β΄. Ὑπάρχει c μὲ $\mathrm{ord}_m(c) = [r, s]$ (=ΕΚΠ τῶν r, s).

γ΄. Ὑπάρχει γεννήτορας μέτρῳ p γιὰ κάθε περιττὸ πρῶτο p.

Ἀπόδειξη Θὰ κάνομε συχνὴ χρήση τοῦ θεωρήματος 5.1.1 χωρὶς ἰδιαίτερη μνεία.

α΄. Ἔστω $\mathrm{ord}_m(ab) = t$. Ἔστω, ἐπίσης, b_1 τέτοιος ὥστε $bb_1 \equiv 1 \pmod m$. Ἡ ἄσκηση 1 μᾶς λέει ὅτι $\mathrm{ord}_m(b_1) = s$. Ἀπὸ τὴν $(ab)^t \equiv 1 \pmod m$ παίρνομε ἀμέσως $a^t \equiv b_1^t \pmod m$. Ἔστω $c \equiv a^t \equiv b_1^t \pmod m$. Ἀπὸ τὸ θεώρημα 5.1.3 συμπεραίνομε ὅτι $\mathrm{ord}_m(c) = \mathrm{ord}_m(a^t) = \frac{r}{(r,t)}$, καθὼς ἐπίσης καὶ $\mathrm{ord}_m(c) = \mathrm{ord}_m(b_1^t) = \frac{s}{(s,t)}$. Ἐξισώνοντας, παίρνομε $r(s, t) = s(r, t)$, ἄρα $r|s(s, t)$. Ἐπειδὴ $(r, s) = 1$, ἕπεται ὅτι $r|(r, t)$, ἄρα $r|t$. Ἐντελῶς ἀνάλογα, $s|t$, ὁπότε (γ΄ τοῦ θεωρήματος 1.3.1) $rs|t$. Ἀπὸ τὸ ἄλλο μέρος, ὅμως, $(ab)^{rs} = (a^r)^s(b^s)^r \equiv 1^s \cdot 1^r \equiv 1 \pmod m$, ἄρα $t|rs$, ὁπότε, τελικά, $t = rs$.

β΄. Γιὰ τὴν ἀπόδειξη θὰ κάνομε χρήση τῶν *ἐκθετῶν*, στοὺς ὁποίους ἀναφερθήκαμε ἀμέσως μετὰ τὸ θεώρημα 1.4.3. Γιὰ ἁπλούστευση τοῦ συμβολισμοῦ θὰ γράφομε ord ἀντὶ ord_m. Τὸν τυπικὸ (θετικὸ) πρῶτο ἀριθμὸ θὰ συμβολίζομε μὲ q καὶ τὸ σύμβολο $v_q(x)$ ὑπενθυμίζομε ὅτι σημαίνει τὸν ἐκθέτη τοῦ q στὸν x.

Ἐπίσης, τὸ σύμβολο $\prod$ θὰ σημαίνει $\prod_{q \text{ πρῶτος}}$.

Θέτομε

$$r_0 = \prod q^{\mu(q)} \quad \text{ὅπου} \quad \mu(q) = \begin{cases} v_q(r) & \text{ἂν } v_q(r) \ge v_q(s) \\ 0 & \text{ἂν } v_q(r) < v_q(s) \end{cases}$$

καὶ

$$s_0 = \prod q^{\nu(q)} \quad \text{ὅπου} \quad \nu(q) = \begin{cases} 0 & \text{ἂν } v_q(r) \ge v_q(s) \\ v_q(s) & \text{ἂν } v_q(r) < v_q(s)\,. \end{cases}$$

Εἶναι προφανὲς ὅτι, γιὰ κανένα q δὲν ἔχομε συγχρόνως $\mu(q) > 0$ καὶ $\nu(q) > 0$, ἄρα $(r_0, s_0) = 1$. Ἐπίσης, $\mu(q) + \nu(q) = \max\{v_q(r), v_q(s)\}$, ἄρα, ἀπὸ τὴν ἄσκηση 30 τοῦ κεφαλαίου 1 ἕπεται ὅτι $r_0 s_0 = [r, s]$. Εἶναι ἐπίσης προφανὲς ἀπὸ τὸν ὁρισμὸ τοῦ r_0 ὅτι $r_0|r$, ὁπότε ἂς θέσομε $r = r_0 r_1$ γιὰ κάποιο $r_1 \in \mathbb{N}$. Ἀνάλογα, θέτομε $s = s_0 s_1$, ὅπου $s_1 \in \mathbb{N}$. Ἀπὸ τὸ (α΄) τοῦ θεωρήματος 5.1.3 ἕπεται ὅτι $\mathrm{ord}(a^{r_1}) = \frac{r}{(r,r_1)} = \frac{r}{r_1} = r_0$ καί, ἀνάλογα, $\mathrm{ord}(b^{s_1}) = s_0$. Ἐπειδή, τώρα, $(r_0, s_0) = 1$, τὸ (α΄) μᾶς λέει ὅτι $\mathrm{ord}(a^{r_1} b^{s_1}) = r_0 s_0 = [r, s]$.

γ΄. Ἔστω r ἡ μέγιστη δυνατὴ τάξη μέτρῳ p, δηλαδή, ὑπάρχει ἀκέραιος g μὲ $\mathrm{ord}_p(g) = r$, ἐνῶ $\mathrm{ord}_p(b) \le r$ γιὰ κάθε $b \in \mathbb{Z}$. Προφανῶς $r \le p - 1$. Ἰσχυριζόμαστε τώρα ὅτι ἡ τάξη μέτρῳ p ὁποιουδήποτε ἀκεραίου διαιρεῖ τὸν r. Πράγματι, ἔστω

$\mathrm{ord}_p(b) = s$ καὶ ἂς ὑποθέσομε ὅτι ὁ s δὲν διαιρεῖ τὸν r. Τότε, $(r, s) < s$, ἄρα $[r, s] = \frac{rs}{(r,s)} > \frac{rs}{s} = r$. Ἀλλά, βάσει τοῦ (β′), ὑπάρχει ἀκέραιος, τοῦ ὁποίου ἡ τάξη μέτρῳ p εἶναι ἴση μὲ $[r, s] > r$, ἄτοπο. Συμπεραίνομε, λοιπόν, ὅτι οἱ τάξεις τῶν $1, 2, \ldots, p-1$ μέτρῳ p εἶναι διαιρέτες τοῦ r. Αὐτό, προφανῶς, συνεπάγεται ὅτι ἡ ἰσοτιμία $x^r - 1 \equiv 0 (\mathrm{mod}\ p)$ ἔχει τουλάχιστον $p-1$ διαφορετικὲς λύσεις, ἄρα (θεώρημα 3.4.1) $p - 1 \leq r$. Ὅπως παρατηρήσαμε στὴν ἀρχή, ἰσχύει καὶ ἡ ἀντίστροφη ἀνισότητα, ἄρα $p-1 = r = \mathrm{ord}_p(g)$, ὁπότε ὁ g εἶναι γεννήτορας μέτρῳ p. **ὅ.ἔ.δ.**

Θεώρημα 5.1.5 *α′. Ἂν ὁ g εἶναι γεννήτορας μέτρῳ p, τότε ὑπάρχουν k, ℓ τέτοιοι ὥστε $(g + pk)^{p-1} = 1 + p\ell$ καὶ $\ell \not\equiv 0 \pmod p$. Γιὰ ἕνα τέτοιο k, ὁ $g + pk$ εἶναι γεννήτορας μέτρῳ p^n γιὰ κάθε $n > 1$.*

β′ Ἂν ὁ g εἶναι γεννήτορας μέτρῳ p καὶ $g^{p-1} \not\equiv 1 \pmod{p^2}$, τότε ὁ g εἶναι γεννήτορας μέτρῳ p^n γιὰ κάθε $n > 1$. [1]

γ′ Ἂν $n \geq 1$ καὶ ὁ g εἶναι γεννήτορας μέτρῳ p^n, τότε γεννήτορας μέτρῳ $2p^n$ εἶναι ἐκεῖνος ἀπὸ τοὺς g καὶ $g + p^n$, ὁ ὁποῖος εἶναι περιττός.

Ἀπόδειξη α′. Λόγῳ τοῦ θεωρήματος τοῦ Fermat ἔχομε $g^{p-1} = 1 + pc$, γιὰ κάποιον ἀκέραιο c. Ἄρα, γιὰ κάθε ἀκέραιο x ἔχομε

$$\begin{aligned}(g + px)^{p-1} &= g^{p-1} + (p-1)g^{p-2}(px) + \sum_{i=2}^{p-1} \binom{p-1}{i} g^{p-1-i}(px)^i \\ &= 1 + pc + (p-1)g^{p-2}px + p^2 b_1\end{aligned}$$

ὅπου ὁ b_1 εἶναι κάποιος ἀκέραιος, τοῦ ὁποίου ἡ τιμὴ δὲν μᾶς ἐνδιαφέρει. Ἄρα, $(g+px)^{p-1} = 1+p(c+(p-1)g^{p-2}x+pb_1)$ καὶ ἂν $k \bmod p$ εἶναι ἡ λύση τῆς ἰσοτιμίας $(p-1)g^{p-2}x \equiv 1 - c (\mathrm{mod}\ p)$, τότε $c + (p-1)g^{p-2}k = 1 + pb_2$ γιὰ κάποιο $b_2 \in \mathbb{Z}$, ἄρα $(g + pk)^{p-1} = 1 + p(1 + pb_2 + pb_1)$ καὶ παίρνομε $\ell = 1 + pb_2 + pb_1$.

Θὰ ἀποδείξομε τώρα ὅτι, γιὰ τὸ παραπάνω k καὶ κάθε $\nu \geq 1$ ἰσχύει μία σχέση τῆς μορφῆς

$$(g + pk)^{p^\nu(p-1)} = 1 + p^{\nu+1}\ell_{\nu+1}\,, \quad \text{ὅπου } p \nmid \ell_{\nu+1}\,. \tag{5.1}$$

Γιὰ $\nu = 1$:

$$(g + pk)^{p(p-1)} = (1 + p\ell)^p = 1 + p^2\ell + \sum_{i=2}^{p} \binom{p}{i} (p\ell)^i$$

καὶ κάθε προσθετέος στὸ τελευταῖο ἄθροισμα $\sum$ εἶναι πολλαπλάσιο τοῦ p^3, διότι κάθε διωνυμικὸς συντελεστὴς στὸ ἄθροισμα αὐτὸ εἶναι πολλαπλάσιο τοῦ p (ἄσκηση 31 τοῦ κεφαλαίου 1). Ἄρα, τὸ δεξιὸ μέλος τῆς παραπάνω σχέσης εἶναι τῆς μορφῆς $1 + p^2\ell_2$, ὅπου $\ell_2 = \ell + \{\textit{ὅροι διαιρετοὶ διὰ } p\} \not\equiv 0 \pmod p$.
Γιὰ $\nu = 2$:

$$(g + pk)^{p^2(p-1)} = (1 + p^2\ell_2)^p = 1 + p^3\ell_2 + \sum_{i=2}^{p} \binom{p}{i} (p^2\ell_2)^i$$

[1] Στὴν πράξη, ἡ περίπτωση αὐτὴ δὲν εἶναι καὶ τόσο εἰδική, ἀφοῦ ὁ μόνος πρῶτος $p \leq 104729$, ποὺ δὲν ἱκανοποιεῖ αὐτὴ τὴ συνθήκη, εἶναι ὁ 40487.

καὶ κάθε προσθετέος στὸ τελευταῖο ἄθροισμα $\sum$ εἶναι πολλαπλάσιο τοῦ p^4. Ἄρα, τὸ δεξιὸ μέλος τῆς παραπάνω σχέσης εἶναι τῆς μορφῆς $1 + p^3\ell_3$, ὅπου $\ell_3 = \ell_2 + \{\textit{ὅροι διαιρετοὶ διὰ } p\} \not\equiv 0 \pmod{p}$.
Ἡ ἐπαγωγικὴ ἀπόδειξη τῆς σχέσης (5.1) εἶναι τώρα ξεκάθαρη. Μὲ τὴ βοήθεια τῆς σχέσης αὐτῆς μποροῦμε νὰ ἀποδείξομε ὅτι ὁ $g + pk$ εἶναι γεννήτορας μέτρῳ p^μ γιὰ κάθε $\mu \geq 1$. Κατ' ἀρχάς, ἂς κάνομε τὴν ἁπλῆ παρατήρηση ὅτι, ἀφοῦ ὁ g εἶναι γεννήτορας μέτρῳ p, τὸ ἴδιο θὰ ἰσχύει καὶ γιὰ τὸν $g + pk$, ὁπότε ἡ τάξη τοῦ $g + pk$ μέτρῳ p εἶναι $p - 1$. Ἔστω τώρα ὅτι $\mathrm{ord}_{p^\mu}(g + pk) = r$. Ἡ σχέση $(g + pk)^r \equiv 1 \pmod{p^\mu}$ συνεπάγεται τὴν $(g + pk)^r \equiv 1 \pmod{p}$ ἄρα, ἀφοῦ ἡ τάξη τοῦ $g + pk$ μέτρῳ p εἶναι $p - 1$, συμπεραίνομε ὅτι $(p - 1)|r$ καὶ θέτομε $r = (p - 1)s$. Ἀφ' ἑτέρου, τὸ α΄ τοῦ θεωρήματος 5.1.1 μᾶς λέει ὅτι $r|\phi(p^\mu) = p^{\mu-1}(p - 1)$, ἄρα $s = p^\nu$ γιὰ κάποιο $\nu \leq \mu - 1$. Τώρα, ἡ σχέση (5.1) μᾶς λέει ὅτι $(g + pk)^{p^\nu(p-1)} \not\equiv 1 \pmod{p^{\nu+2}}$, ἄρα, ἂν ἦταν $\nu < \mu - 1$, θὰ εἴχαμε $(g + pk)^r = (g + pk)^{p^\nu(p-1)} \not\equiv 1 \pmod{p^\mu}$, ποὺ ἀντιφάσκει μὲ τὸν ὁρισμὸ τοῦ r. Συνεπῶς, $\nu = \mu - 1$ καὶ $r = (p - 1)s = (p - 1)p^\nu = (p - 1)p^{\mu-1} = \phi(p^\mu)$, ποὺ λέει, ἀκριβῶς, ὅτι ὁ $g + pk$ εἶναι γεννήτορας μέτρῳ p^μ.
β΄. Λόγῳ τοῦ θεωρήματος τοῦ Fermat, $g^{p-1} = 1 + \ell p$. Ἐξ ὑποθέσεως, τὸ ℓ δὲν διαιρεῖται ἀπὸ τὸν p, ἄρα ἐφαρμόζεται τὸ (α΄) μὲ $k = 0$.
γ΄. Ἂν ὁ g εἶναι γεννήτορας μέτρῳ p^n, τό ἴδιο ἰσχύει, προφανῶς καὶ γιὰ τὸν $g + p^n$ καὶ ἕνας, ἀκριβῶς, ἀπὸ τοὺς δύο εἶναι περιττός ἀριθμός, τὸν ὁποῖο ἂς συμβολίσομε μὲ g_1. Εἶναι, ἐπίσης, $\phi(2p^n) = \phi(p^n) =$ (ἔστω) e. Ἀφοῦ ἰσχύει ἡ σχέση $g_1^e \equiv 1 \pmod{p^n}$ καὶ ὁ g_1 εἶναι περιττός, θὰ ἰσχύει καὶ ἡ $g_1^e \equiv 1 \pmod{2p^n}$. Ἐπιπλέον, ἂν ὑπῆρχε θετικὸς $k < e$, τέτοιος ὥστε $g_1^k \equiv 1 \pmod{2p^n}$, τότε θὰ ἴσχυε καὶ $g_1^k \equiv 1 \pmod{p^n}$, κάτι ποὺ ἀντιφάσκει μὲ τὸ γεγονὸς ὁ g_1 εἶναι γεννήτορας μέτρῳ p^n. Συνεπῶς, $\mathrm{ord}_{2p^n}(g_1) = e = \phi(2p^n)$, δηλαδή, ὁ g_1 εἶναι, ἐπίσης, γεννήτορας μέτρῳ $2p^n$. **ὅ.ἔ.δ.**

Σχόλιο. Ένα ἐπιπόλαιο κοίταγμα τοῦ θεωρήματος 5.1.5-α΄ δίνει τὴν ἐντύπωση ὅτι, γιὰ νὰ ὑπολογίσει κανεὶς ἕνα γεννήτορα μέτρῳ p^n ἢ $2p^n$, ὅταν ξέρει ἕνα γεννήτορα μέτρῳ p, πρέπει νὰ ὑπολογίσει τὸν τεράστιο ἀριθμὸ g^{p-1}. Λανθασμένη ἐντύπωση! Ἡ ἄσκηση 4 μᾶς λέει ὅτι, ἀρκεῖ νὰ ὑπολογίσει κανείς, ὄχι αὐτὸν, καθ' ἑαυτόν, τὸν ἀριθμὸ g^{p-1}, ἀλλὰ τὴν κλάση του μέτρῳ p^2 καὶ ἕνα τέτοιο ἐγχείρημα, βέβαια, δὲν εἶναι δύσκολο (δὲς παράγραφο 2.3 τοῦ κεφαλαίου 2).

Μέχρι στιγμῆς ἔχομε δείξει ὅτι, γιὰ $m = p^n$, $2p^n$, μὲ p περιττὸ πρῶτο καὶ $n \geq 1$, ὑπάρχουν γεννήτορες μέτρῳ m. Ἐπίσης, εἶναι φανερὸ ὅτι, μέτρῳ 2 καὶ μέτρῳ 4 ὑπάρχουν γεννήτορες, οἱ 1 καὶ 3, ἀντιστοίχως. Τὸ παρακάτω θεώρημα μᾶς λέει ὅτι οὐδένα ἄλλο μέτρο $m > 1$ ἔχει γεννήτορα.

Θεώρημα 5.1.6 *α΄. Γιὰ κάθε $b \geq 3$ καὶ κάθε περιττὸ a ἰσχύει* $a^{2^{b-2}} \equiv 1 \pmod{2^b}$.
β΄. Ἔστω $m = 2^b \prod_{i=1}^{k} p_i^{b_i}$, ὅπου $k \geq 1$ καὶ οἱ p_i εἶναι διαφορετικοὶ περιττοὶ πρῶτοι καὶ τὰ ἑξῆς ὑποτίθενται: Ἂν $k = 1$, τότε $b \geq 2$· ἂν $b = 0$ ἢ 1, τότε $k \geq 2$. Τότε, γιὰ κάθε a πρῶτο πρὸς τὸν m ἰσχύει

$$a^{\phi(m)/2} \equiv 1 \pmod{m}.$$

γ΄. Γιὰ $m = 2, 4, p^n, 2p^n$, ὅπου p περιττὸς πρῶτος καὶ $n \geq 1$, ὑπάρχουν γεννήτορες μέτρῳ m. Γιὰ $m > 1$, ποὺ δὲν εἶναι τῆς παραπάνω μορφῆς, δὲν ὑπάρχουν γεννήτορες μέτρῳ m.

Ἀπόδειξη α΄. Ἡ ἀπόδειξη γίνεται ἐπαγωγικά. Γιὰ $b = 3$ ἡ ἀποδεικτέα γίνεται $a^2 \equiv 1 \pmod 8$, ποὺ ἰσχύει. Ἔστω ὅτι ἰσχύει γιὰ $b = k$, ὁπότε μποροῦμε νὰ γράψομε $a^{2^{k-2}} = 1 + 2^k t$ γιὰ κάποιον ἀκέραιο t. Ὑψώνοντας στὸ τετράγωνο τὰ δύο μέλη παίρνομε $a^{2^{k-1}} = 1 + 2^{k+1}t + 2^{2k}t^2 \equiv 1 \pmod{2^{k+1}}$.
β΄. Βάσει τοῦ α΄ τοῦ θεωρήματος 2.2.3 ἔχομε

$$\phi(m) = \phi(2^b)\prod_{i=1}^{k}\phi(p_i^{b_i})\,.$$

Στὸ γινόμενο $\prod$ ἐμφανίζεται τουλάχιστον ἕνας παράγων $\phi(p_i^{b_i}) = (p_i - 1)p_i^{b_i-1}$, ποὺ εἶναι ἄρτιος ἀριθμός, ἄρα ὁ $\phi(m)/2$ εἶναι ἀκέραιος.

Ἀποδεικνύομε πρῶτα ὅτι ὁ

$$c = \frac{1}{2}\phi(2^b)\prod_{i=2}^{k}\phi(p_i^{b_i})$$

εἶναι ἀκέραιος. Ἄν $b \geq 2$, τότε ὁ ἀριθμὸς $\frac{1}{2}\phi(2^b) = 2^{b-2}$ εἶναι ἀκέραιος. Ἄν $b = 0$ ἢ 1, τότε, ἐξ ὑποθέσεως, $k \geq 2$ ἄρα στὸ γινόμενο $\prod$ ἐμφανίζεται ὁ παράγων $\phi(p_2^{b_2})$, ὁ ὁποῖος εἶναι ἄρτιος, καθὼς εἴδαμε παραπάνω. Καὶ στὶς δύο περιπτώσεις, λοιπόν, ὁ c εἶναι ἀκέραιος.

Ἔστω τώρα g ἕνας γεννήτορας μέτρῳ $p_1^{b_1}$. Ἐπειδὴ $(a, p_1^{b_1}) = 1$, συμπεραίνομε ὅτι ὑπάρχει s, τέτοιος ὥστε $a \equiv g^s \pmod{p_1^{b_1}}$. Τότε

$$a^{\phi(m)/2} \equiv g^{s\phi(m)/2} = (g^{\phi(p_1^{b_1})})^{cs} \equiv 1^{cs} = 1 \pmod{p_1^{b_1}}$$

καί, κατ' ἀναλογίαν, $a^{\phi(m)/2} \equiv 1 \pmod{p_i^{b_i}}$ γιὰ ὅλα τὰ $i = 1, \ldots, k$. Ὕστερα ἀπὸ τὸ συμπέρασμα αὐτό, τὸ μόνο ποὺ μᾶς μένει γιὰ ν' ἀποδείξομε ὅτι $a^{\phi(m)/2} \equiv 1 \pmod m$, εἶναι ὅτι $a^{\phi(m)/2} \equiv 1 \pmod{2^b}$. Γιὰ $b = 0$ δὲν ἔχομε τίποτε νὰ ἀποδείξομε. Ἄν $b \geq 1$, ὁ a εἶναι περιττὸς, ἀφοῦ $(a, m) = 1$. Γιὰ $b = 1$, ἀποδεικτέα σχέση εἶναι ἡ τετριμμένη ἰσοτιμία $a^{\phi(m)/2} \equiv 1 \pmod 2$. Γιὰ $b = 2$, $\phi(m)/2 = \prod_{i=1}^{k}\phi(p_i^{b_i})$ καὶ κάθε παράγων αὐτοῦ τοὺ γινομένου (ὑπάρχει τουλάχιστον ἕνας) εἶναι ἄρτιος. Ἄρα, $\phi(m)/2 = 2e$, $e \in \mathbb{Z}$ καὶ ἀποδεικτέα σχέση εἶναι ἡ $a^{2e} \equiv 1 \pmod 4$, ἡ ὁποία ἰσχύει, ἀφοῦ $a^2 \equiv 1 \pmod 4$. Γιὰ $b \geq 3$ ὁ $\phi(m)/2$ εἶναι πολλαπλάσιο τοῦ 2^{b-2}, καὶ ἡ ἀποδεικτέα σχέση ἕπεται ἀμέσως ἀπὸ τὸ (α΄).
γ΄. Ὁ 1 εἶναι γεννήτορας μέτρῳ 2 καὶ ὁ 3 εἶναι γεννήτορας μέτρῳ 4. Τὸ γ΄ τοῦ θεωρήματος 5.1.4 καὶ τὸ γ΄ τοῦ θεωρήματος 5.1.5 συνεπάγονται τὴν ὕπαρξη γεννήτορα μέτρῳ m ὅταν $m = p^n$ ἢ $2p^n$ μὲ p περιττὸ πρῶτο καὶ $n \geq 1$. Ὅταν ὁ m δὲν ἔχει μία ἀπὸ αὐτὲς τὶς μορφές, τότε, ἢ $m = 2^b$ μὲ $b \geq 3$, ἢ ὁ m εἶναι ὅπως στὸ (β΄). Καὶ στὶς δύο περιπτώσεις ἰσχύει ὅτι, γιὰ κάθε a πρῶτο πρὸς τὸν

m, $a^{\phi(m)/2} \equiv 1 \pmod{m}$ (παρατηρῆστε ὅτι $\phi(2^b)/2 = 2^{b-2}$), ἄρα κάθε ἀκέραιος a πρῶτος πρὸς τὸν m ἔχει τάξη μέτρῳ m, τὸ πολύ, $\phi(m)/2$ καί, συνεπῶς, δὲν μπορεῖ νὰ εἶναι γεννήτορας μέτρῳ m. **ὅ.ἔ.δ.**

Πίνακας 5.1: Ὅλοι οἱ πρῶτοι $p \leq 659$ μὲ τὸν ἀντίστοιχο ἐλάχιστο γεννήτορα $g(p)$.

p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$
2	1	73	5	179	2	283	3	419	2	547	2
3	2	79	3	181	2	293	2	421	2	557	2
5	2	83	2	191	19	307	5	431	7	563	2
7	3	89	3	193	5	311	17	433	5	569	3
11	2	97	5	197	2	313	10	439	15	571	3
13	2	101	2	199	3	317	2	443	2	577	5
17	3	103	5	211	2	331	3	449	3	587	2
19	2	107	2	223	3	337	10	457	13	593	3
23	5	109	6	227	2	347	2	461	2	599	7
29	2	113	3	229	6	349	2	463	3	601	7
31	3	127	3	233	3	353	3	467	2	607	3
37	2	131	2	239	7	359	7	479	13	613	2
41	6	137	3	241	7	367	6	487	3	617	3
43	3	139	2	251	6	373	2	491	2	619	2
47	5	149	2	257	3	379	2	499	7	631	3
53	2	151	6	263	5	383	5	503	5	641	3
59	2	157	5	269	2	389	2	509	2	643	11
61	2	163	2	271	6	397	5	521	3	647	5
67	2	167	5	277	5	401	3	523	2	653	2
71	7	173	2	281	3	409	21	541	2	659	2

5.2 Διακριτοὶ λογάριθμοι

> Σ' αὐτὴ τὴν παράγραφο $m = p^n$ ἢ $2p^n$, μὲ p περιττὸ πρῶτο καὶ $n \geq 1$.

Σύμφωνα μὲ τὸ θεώρημα 5.1.6 ὑπάρχουν γεννήτορες μέτρῳ m καὶ ἔστω g ἕνας ἀπὸ αὐτούς. Ἔστω a πρῶτος πρὸς τὸν m. Ἀπὸ τὸ θεώρημα 5.1.2 συμπεραίνομε ὅτι ὑπάρχει ἕνας μοναδικὸς $k \in \{0, 1, \ldots, \phi(m) - 1\}$, τέτοιος ὥστε $a \equiv g^k \pmod{m}$. Ὁ k αὐτὸς συμβολίζεται $\mathrm{ind}_g(a)$ καὶ λέγεται *διακριτὸς λογάριθμος τοῦ a μέτρῳ m, ὡς πρὸς βάση g*. Συνήθως παραλείπομε τοὺς προσδιορισμοὺς «μέτρῳ m» καὶ «ὡς πρὸς βάση g». Προτιμοῦμε τὸν συμβολισμὸ ind ἀντὶ τοῦ log διότι, ἀφ' ἑνός, ὑπάρχει κάποιος κίνδυνος συγχύσεως μὲ τὸν συνήθη λογάριθμο καί, ἀφ' ἑτέρου, γιατὶ ἡ χρήση τοῦ συμβολισμοῦ ind ἔχει ἀρκετὰ μακρὰ παράδοση στὴ Θεωρία Ἀριθμῶν.

Ἐξ ὁρισμοῦ, λοιπόν,

$$\operatorname{ind}_g(a) = k \Leftrightarrow a \equiv g^k \pmod m \quad \text{καὶ} \quad 0 \le k \le \phi(m) - 1\,. \tag{5.2}$$

Θεώρημα 5.2.1 *Ἔστω g γεννήτορας μέτρῳ m. Παρακάτω, τὰ a, b συμβολίζουν ἀκεραίους πρώτους πρὸς τὸν m. Γιὰ ἁπλούστευση τοῦ συμβολισμοῦ, στὰ (α΄)-(στ΄) καὶ στὶς ἀποδείξεις τους γράφομε* ind *ἀντὶ* ind_g.
α΄. $a \equiv b \pmod m \Leftrightarrow \operatorname{ind}(a) = \operatorname{ind}(b)$.
β΄. Ἡ ἰσοτιμία $a^n \equiv 1 \pmod m$ *ἰσοδυναμεῖ μὲ τὴν* $n \operatorname{ind}(a) \equiv 0 \pmod{\phi(m)}$.
γ΄. $\operatorname{ind}(ab) \equiv \operatorname{ind}(a) + \operatorname{ind}(b) \pmod{\phi(m)}$.
δ΄. $\operatorname{ind}(a^n) \equiv n \operatorname{ind}(a) \pmod{\phi(m)}$.
ε΄. $\operatorname{ind}(1) = 0$ *καὶ* $\operatorname{ind}(g) = 1$.
στ΄. $\operatorname{ind}(-1) = \phi(m)/2$.
ζ΄. Ἂν g_1 *εἶναι γεννήτορας μέτρῳ* m, *τότε*

$$\operatorname{ind}_g(a) \equiv \operatorname{ind}_g(g_1) \cdot \operatorname{ind}_{g_1}(a) \pmod{\phi(m)}\,.$$

Ἀπόδειξη Σ' αὐτὴ τὴν ἀπόδειξη θὰ χρησιμοποιοῦμε, δίχως νὰ κάνομε ἰδιαίτερη μνεία, τὴ σχέση (5.2) καθὼς ἐπίσης καὶ τὴν ἑξῆς ἰσοδυναμία: $g^k \equiv g^\ell \pmod m \Leftrightarrow k \equiv \ell \pmod{\phi(m)}$, ἡ ὁποία προκύπτει ἀμέσως ἀπὸ τὸ β΄ τοῦ θεωρήματος 5.1.1, σὲ συνδυασμὸ μὲ τὸ ὅτι $\operatorname{ord}_m(g) = \phi(m)$.

Προχωροῦμε τώρα στὴν ἀπόδειξη τῶν διαφόρων προτάσεων τοῦ θεωρήματος.
α΄. Ἔστω $\operatorname{ind}(a) = k$ καὶ $\operatorname{ind}(b) = \ell$. Τότε, ἡ ἰσοτιμία $a \equiv b \pmod m$ ἰσοδυναμεῖ μὲ τὴν $g^k \equiv g^\ell \pmod m$, ἄρα μὲ τὴν ἰσοτιμία $k \equiv \ell \pmod{\phi(m)}$· συνεπῶς, $\phi(m) | (k - \ell)$. Ὅμως $0 \le |k - \ell| < \phi(m)$, ἄρα $k = \ell$.
β΄. Ἔστω $\operatorname{ind}(a) = k$. Ἡ ἰσοτιμία $a^n \equiv 1 \pmod m$ ἰσοδυναμεῖ μὲ τὴν $g^{kn} \equiv g^0 \pmod m$, ἄρα καὶ μὲ τὴν $nk \equiv 0 \pmod{\phi(m)}$, ποὺ εἶναι ἡ ἀποδεικτέα.
γ΄. $g^{\operatorname{ind}(a)+\operatorname{ind}(b)} = g^{\operatorname{ind}(a)} g^{\operatorname{ind}(b)} \equiv ab \equiv g^{\operatorname{ind}(ab)} \pmod m$ καὶ ἡ ἀποδεικτέα προκύπτει τώρα μὲ ἐφαρμογὴ τοῦ θεωρήματος 5.1.1-β΄, λαμβάνοντας ὑπ' ὄψιν ὅτι $\operatorname{ord}_m(g) = \phi(m)$.
δ΄. Ἡ πρόταση (γ΄), ποὺ μόλις ἀποδείξαμε, γενικεύεται μὲ προφανῆ ἐπαγωγή, ὡς ἑξῆς: $\operatorname{ind}(a_1 \cdots a_n) \equiv \operatorname{ind}(a_1) + \cdots + \operatorname{ind}(a_n) \pmod{\phi(m)}$. Γιὰ $a_1 = \cdots = a_n = a$ παίρνομε τὴν ἀποδεικτέα.
ε΄. Τετριμμένη συνέπεια τῆς σχέσης (5.2).
στ΄. Θέτομε $m = 2^j p^n$, ὅπου $j \in \{0, 1\}$, ὁπότε, ὅταν $j = 1$, ὁ g εἶναι περιττός, λόγῳ τῆς σχέσεως $g^{\phi(m)} \equiv 1 \pmod{2^j p^n}$. Σὲ κάθε περίπτωση ὁ $\phi(m)$ εἶναι ἄρτιος, ὁπότε ἡ τελευταία ἰσοτιμία γράφεται ἰσοδύναμα ὡς

$$2^j p^n | (g^{\phi(m)/2} - 1)(g^{\phi(m)/2} + 1)\,.$$

Ἀλλά, προφανῶς, ὁ 2^j διαιρεῖ καὶ τοὺς δύο παράγοντες στὰ δεξιά, ἐνῶ ὁ p ἀποκλείεται νὰ διαιρεῖ καὶ τοὺς δύο συγχρόνως. Ἄρα, ὁ $m = 2^j p^n$ διαιρεῖ ἢ τὸν ἕνα ἢ τὸν ἄλλο παράγοντα. Ἂν διαιροῦσε τὸν $g^{\phi(m)/2} - 1$, τότε θὰ ἐρχόμαστε σὲ ἀντίφαση

μὲ τὸ ὅτι ὁ g εἶναι γεννήτορας μέτρῳ m. Ἄρα ὁ m διαιρεῖ τὸν ἄλλο παράγοντα, δηλαδή, $g^{\phi(m)/2} \equiv -1 \,(\mathrm{mod}\ m)$, ποὺ σημαίνει, $\mathrm{ind}(-1) = \phi(m)/2$.
ζʹ. Θέτομε $\mathrm{ind}_g(a) = n$, $\mathrm{ind}_{g_1}(a) = k$, $\mathrm{ind}_g(g_1) = \ell$, ὁπότε ἔχομε

$$g^n \equiv a\,, \quad g_1^k \equiv a\,, \quad g^\ell \equiv g_1 \pmod{m}\,.$$

Συνδυάζοντας τὶς δύο τελευταῖες παίρνομε $g^{k\ell} \equiv a \,(\mathrm{mod}\ m)$, ἡ ὁποία, σὲ συνδυασμὸ μὲ τὴν πρώτη, μᾶς δίνει $g^{k\ell} \equiv g^n \,(\mathrm{mod}\ m)$. Ἡ τελευταία ἰσοδυναμεῖ μὲ τὴν $n \equiv \ell k$ $(\mathrm{mod}\ \phi(m))$, ποὺ εἶναι ἡ ἀποδεικτέα σχέση. **ὅ.ἔ.δ.**

Πίνακας 5.2: Στὴν τομὴ τῆς στήλης τοῦ πρώτου p καὶ τῆς γραμμῆς τοῦ a ἐμφανίζεται ὁ $\mathrm{ind}_g(a)$ ὅταν g εἶναι ὁ ἐλάχιστος γεννήτορας μέτρῳ p.

a \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18	1	1
3		3	1	8	4	1	13	16	5	1	26	15	1	20	17	50
4		2	4	2	2	12	2	4	2	18	2	12	12	36	2	2
5			5	4	9	5	16	1	22	20	23	22	25	1	47	6
6			3	9	5	15	14	18	6	25	27	1	28	38	18	51
7				7	11	11	6	19	12	28	32	39	35	32	14	18
8				3	3	10	3	6	3	12	3	38	39	8	3	3
9				6	8	2	8	10	10	2	16	30	2	40	34	42
10				5	10	3	17	3	23	14	24	8	10	19	48	7
11					7	7	12	9	25	23	30	3	30	7	6	25
12					6	13	15	20	7	19	28	27	13	10	19	52
13						4	5	14	18	11	11	31	32	11	24	45
14						9	7	21	13	22	33	25	20	4	15	19
15						6	11	17	27	21	13	37	26	21	12	56
16						8	4	8	4	6	4	24	24	26	4	4
17							10	7	21	7	7	33	38	16	10	40
18							9	12	11	26	17	16	29	12	35	43
19								15	9	4	35	9	19	45	37	38
20								5	24	8	25	34	37	37	49	8
21								13	17	29	22	14	36	6	31	10
22								11	26	17	31	29	15	25	7	26
23									20	27	15	36	16	5	39	15
24									8	13	29	13	40	28	20	53
25									16	10	10	4	8	2	42	12

συνέχεια στὴν ἐπόμενη σελίδα

Πίνακας 5.2 *(συνέχεια ἀπὸ τὴν προηγούμενη σελίδα)*

$a \backslash p$	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
26									19	5	12	17	17	29	25	46
27									15	3	6	5	3	14	51	34
28									14	16	34	11	5	22	16	20
29										9	21	7	41	35	46	28
30										15	14	23	11	39	13	57
31											9	28	34	3	33	49
32											5	10	9	44	5	5
33											20	18	31	27	23	17
34											8	19	23	34	11	41
35											19	21	18	33	9	24
36											18	2	14	30	36	44
37												32	7	42	30	55
38												35	4	17	38	39
39												6	33	31	41	37
40												20	22	9	50	9
41													6	15	45	14
42													21	24	32	11
43														13	22	33
44														43	8	27
45														41	29	48
46														23	40	16
47															44	23
48															21	54
49															28	36
50															43	13
51															27	32
52															26	47
53																22
54																35
55																31
56																21
57																30
58																29

Ἐφαρμογές. α′. *Διωνυμικὲς ἰσοτιμίες*. Ἔστω ὅτι ἔχομε νὰ λύσομε μία ἰσοτιμία $x^k \equiv a \pmod{m}$, ὅπου $(a, m) = 1$. Βάσει τοῦ δ′ τοῦ θεωρήματος 5.2.1, ἡ ἰσοτιμία αὐτὴ εἶναι ἰσοδύναμη μὲ τὴν $k\,\mathrm{ind}(x) \equiv \mathrm{ind}(a) \pmod{\phi(m)}$. Ἡ τελευταία γραμμικὴ ὡς πρὸς $\mathrm{ind}(x)$ ἰσοτιμία ἔχει λύση ἄν, καὶ μόνο ἄν, $(k, \phi(m))|\mathrm{ind}(a)$ (θεώρημα 3.2.1). Ἂν ἔχει λύση, τότε ἡ ἐπίλυσή της γίνεται ἁπλούστατα, βάσει τῶν ὅσων περιγράψαμε στὴν παράγραφο 3.2 τοῦ κεφαλαίου 3. Ἔχοντας ὑπολογίσει τὴν κλάση $\mathrm{ind}(x) \bmod \phi(m)$, ὑπολογίζομε μὲ ὕψωση σὲ δύναμη (βλ. παράγραφο 2.3 τοῦ κεφαλαίου 2) τὴν κλάση $x \bmod m$.

Γιὰ παράδειγμα, ἂς ἐπιλύσομε τὴν ἰσοτιμία $x^{12} \equiv 37 \pmod{41}$. Ἡ ἰσοτιμία αὐτὴ ἰσοδυναμεῖ μὲ τὴν

$$12\,\mathrm{ind}(x) \equiv \mathrm{ind}(37) \pmod{40}\,. \tag{5.3}$$

Ἀπὸ τὸν πίνακα 5.2 βλέπομε ὅτι $\mathrm{ind}(37) = 32$. Ὁ πίνακας αὐτὸς ἔχει συνταχθεῖ μὲ βάση τοὺς ἐλάχιστους (θετικοὺς) γεννήτορες, τοὺς ὁποίους μᾶς παρέχει ὁ πίνακας 5.1, δηλαδή, στὸ παράδειγμά μας, ὁ γεννήτορας μέτρῳ 41 εἶναι ὁ 6. Ἐπειδὴ $(12, 40) = 4$ καὶ ὁ 4 διαιρεῖ τὸν $32 = \mathrm{ind}(37)$, συμπεραίνομε, βάσει τοῦ θεωρήματος 3.2.1, ὅτι ἡ ἰσοτιμία (5.3) ἔχει 4 λύσεις. Λύνοντας τὴν ἰσοτιμία (5.3) σύμφωνα μὲ ὅσα περιγράφομε στὴν παράγραφο 3.2 τοῦ κεφαλαίου 3, βρίσκομε τὶς ἑξῆς τέσσερεις λύσεις,

$$\mathrm{ind}(x) \equiv 6,\ 16,\ 26,\ 36 \pmod{40}\,,$$

οἱ ὁποῖες μᾶς δίνουν, ἀντιστοίχως,

$$x \equiv 6^6 \equiv 39\,,\ 6^{16} \equiv 18\,,\ 6^{26} \equiv 2\,,\ 6^{36} \equiv 23 \pmod{41}\,.$$

Ὁ παραπάνω τρόπος ἐπίλυσης τῆς διωνυμικῆς ἰσοτιμίας δὲν εἶναι πρακτικός, ἀφ' ἑνός, διότι ἐφαρμόζεται μόνο γιὰ εἰδικῆς μορφῆς μέτρα m καὶ ἀφ' ἑτέρου –αὐτὸ εἶναι τὸ σημαντικὸ μειονέκτημα–, διότι ἀπαιτεῖ τὸν ὑπολογισμὸ διακριτῶν λογαρίθμων, πρόβλημα ἐξαιρετικὰ δύσκολο ἀπὸ ἄποψη ὑπολογιστική. Γενικὰ μιλώντας, ἡ ἐνδεδειγμένη μέθοδος ἐπιλύσεως τῆς διωνυμικῆς ἰσοτιμίας εἶναι αὐτή, ποὺ ἀναπτύσσεται στὴν παράγραφο 3.4 τοῦ κεφαλαίου 3, καὶ ἐφαρμόζεται σὲ κάθε πολυωνυμικὴ ἰσοτιμία. Δώσαμε, ὅμως, ἐδῶ αὐτὴ τὴν ἐφαρμογή, γιὰ νὰ βοηθήσει στὴν ἐμπέδωση τῆς σχετικῆς θεωρίας.

β′. *Ἐκθετικὲς ἰσοτιμίες*. Ἔστω ὅτι οἱ a, b εἶναι πρῶτοι πρὸς τὸν m καὶ θέλομε νὰ λύσομε τὴν ἰσοτιμία $a^x \equiv b \pmod{m}$ μὲ ἄγνωστο τὸν ἐκθέτη x. Οἱ προτάσεις α′ καὶ δ′ τοῦ θεωρήματος 5.2.1 μᾶς ὁδηγοῦν στὸ συμπέρασμα ὅτι αὐτὴ ἡ ἰσοτιμία εἶναι ἰσοδύναμη μὲ τὴν $\mathrm{ind}(a)x \equiv \mathrm{ind}(b) \pmod{\phi(m)}$. Σύμφωνα μὲ τὸ θεώρημα 3.2.1, ἡ τελευταία ἰσοτιμία ἔχει λύσεις ἄν, καὶ μόνο ἄν, $(\mathrm{ind}(a), \phi(m)) | \mathrm{ind}(b)$ καί, στὴν περίπτωση, ποὺ ἡ συνθήκη αὐτὴ ἱκανοποιεῖται, τὸ πλῆθος τῶν διαφορετικῶν μέτρῳ $\phi(m)$ λύσεων εἶναι ἴσο μὲ $(\mathrm{ind}(a), \phi(m))$· βλ. ἄσκηση 9. Σημειῶστε ὅτι, λόγῳ τοῦ θεωρήματος 2.2.4-γ′, λύσεις τῆς ἐκθετικῆς ἰσοτιμίας, ἰσότιμες μέτρῳ $\phi(m)$, δὲν θεωροῦνται διαφορετικές.

Ἂς ἐπιλύσομε, γιὰ παράδειγμα τὴν ἰσοτιμία $12^x \equiv 13 \pmod{23}$. Ἔχομε, σύμφωνα μὲ τὰ παραπάνω, $\mathrm{ind}(12)x \equiv \mathrm{ind}(13) \pmod{22}$ καὶ ἀπὸ τὸν πίνακα 5.2 βρίσκομε $\mathrm{ind}(12) = 20$, $\mathrm{ind}(13) = 14$, ὁπότε ἔχομε νὰ λύσομε τὴν $20x \equiv 14 \pmod{22}$. Σύμφωνα μὲ τὸ θεώρημα 3.2.1, ἡ τελευταία ἰσοτιμία ἔχει δύο λύσεις καί, συγκεκριμένα τὶς $x \equiv 4,\ 15 \pmod{22}$.

Αὐτὴ ἡ μέθοδος ἐπίλυσης τῆς ἐκθετικῆς ἰσοτιμίας ἀπαιτεῖ ὑπολογισμοὺς διακριτῶν λογαρίθμων καὶ αὐτὸ τὴν καθιστᾶ, ἀπὸ ὑπολογιστικὴ ἄποψη, ἐξαιρετικὰ δύσκολη ἕως ἀνεφάρμοστη, γιὰ μεγάλα ἕως πολὺ μεγάλα μέτρα m. Σὲ ἀντίθεση, ὅμως, μὲ τὶς διωνυμικὲς ἰσοτιμίες, στὶς ὁποῖες παρακάμπτομε αὐτὸ τὸ ἐξαιρετικὰ σοβαρὸ μειονέκτημα, γιὰ τὶς ἐκθετικὲς ἰσοτιμίες δὲν ὑπάρχει, μέχρι σήμερα, πλὴν εἰδικῶν περιπτώσεων, «ὑπολογιστικῶς εὔκολη» μέθοδος ἐπίλυσης. Σὲ αὐτό, ἀκριβῶς, τὸ χαρακτηριστικό τῶν ἐκθετικῶν ἐξισώσεων στηρίζεται ἡ ἀσφάλεια τῶν *ψηφιακῶν ὑπογραφῶν* καὶ τῆς ἀνταλλαγῆς *κρυπτογραφικῶν κλειδιῶν*

γ′. *Ἰσοϋπόλοιπα δυνάμεων*. Κατ' ἀναλογίαν μὲ τὰ τετραγωνικὰ ἰσοϋπόλοιπα, μποροῦμε νὰ ὁρίσομε ὅτι ὁ πρῶτος πρὸς τὸν m ἀκέραιος a εἶναι *k-οστὸ ἰσοϋπόλοιπο μέτρῳ m* γιὰ κάποιον ἀκέραιο $k \geq 2$ ἄν, καὶ μόνο ἄν, ἡ ἰσοτιμία $x^k \equiv a \,(\mathrm{mod}\ m)$ ἔχει λύση. Ὁ ὁρισμὸς αὐτὸς ἰσχύει γιὰ ὁποιοδήποτε μέτρο m, ἀλλὰ ἐδῶ, ὅπως, ἄλλωστε, καὶ σὲ ὅλη αὐτὴ τὴν παράγραφο, θὰ ἐξετάσομε τὸ θέμα γιὰ m τῆς μορφῆς p^n ἢ $2p^n$ μὲ p περιττὸ πρῶτο καὶ $n \geq 1$.

Θεώρημα 5.2.2 *Ἔστω $m = p^n$ ἢ $2p^n$, ὅπου ὁ p εἶναι περιττὸς πρῶτος καὶ $n \geq 1$. Ἔστω, ἐπίσης, $k \geq 2$ καὶ a πρῶτος πρὸς τὸν m. Τέλος, θέτομε $d = (k, \phi(m))$. Ὅλοι οἱ διακριτοὶ λογάριθμοι θεωροῦνται ὡς πρὸς κάποιον αὐθαίρετο, ἀλλὰ σταθερό, γεννήτορα g, ὁπότε, γιὰ ἁπλοποίηση τοῦ συμβολισμοῦ, γράφομε* ind *ἀντὶ* ind_g.

α′. Ὁ a εἶναι k-οστὸ ἰσοϋπόλοιπο μέτρῳ m ἄν, καὶ μόνο ἄν, $d|\mathrm{ind}(a)$.

β′. Τὸ πλῆθος τῶν ἀνισοτίμων k-οστῶν ἰσοϋπολοίπων μέτρῳ m εἶναι $\frac{\phi(m)}{d}$.

γ′. Ὁ a εἶναι k-οστὸ ἰσοϋπόλοιπο μέτρῳ m ἄν, καὶ μόνο ἄν,

$$a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}.$$

δ′.

$$\mathrm{ord}_m(a) = \frac{\phi(m)}{(\phi(m), \mathrm{ind}(a))}.$$

Εἰδικώτερα, ὁ a εἶναι γεννήτορας μέτρῳ m ἄν, καὶ μόνο ἄν, $(\phi(m), \mathrm{ind}(a)) = 1$.

Ἀπόδειξη α′. Ἕνας ἁπλὸς συνδυασμὸς τῶν προτάσεων α′ καὶ δ′ τοῦ θεωρήματος 5.2.1 μᾶς δείχνει ὅτι ἡ ἰσοτιμία $x^k \equiv a \,(\mathrm{mod}\ m)$ ἔχει λύση ἄν, καὶ μόνο ἂν ἔχει λύση ἡ ἰσοτιμία $k\,\mathrm{ind}(x) \equiv \mathrm{ind}(a) \pmod{\phi(m)}$. Σύμφωνα μὲ τὸ θεώρημα 3.2.1, ἡ τελευταία ἰσοτιμία ἔχει λύση ἄν, καὶ μόνο ἄν, $d|\mathrm{ind}(a)$.
β′. Σύμφωνα μὲ τὸ (α′), ἀρκεῖ νὰ μετρήσομε γιὰ πόσους ἀκεραίους a ἑνὸς περιορισμένου συστήματος ὑπολοίπων μέτρῳ m ἰσχύει $d|\mathrm{ind}(a)$. Δεδομένου ὅτι ὁ $\mathrm{ind}(a)$ διατρέχει τὸ σύνολο $\{0, 1, \ldots, \phi(m) - 1\}$, αὐτὸ ἰσοδυναμεῖ μὲ τὸ νὰ μετρήσομε πόσοι ἀπὸ τοὺς ἀριθμοὺς $0, 1, \ldots, \phi(m) - 1$ εἶναι πολλαπλάσια τοῦ d. Ἀλλὰ αὐτὸ εἶναι ἁπλό: τὸ πλῆθος τῶν τέτοιων ἀριθμῶν εἶναι $\frac{\phi(m)}{d}$.
γ′. Σύμφωνα μὲ τὸ (α′), ὁ a εἶναι k-οστὸ ἰσοϋπόλοιπο μέτρῳ m ἄν, καὶ μόνο ἄν, $\mathrm{ind}(a) \equiv 0 \pmod{d}$ καὶ ἡ ἰσοτιμία αὐτὴ εἶναι ἰσοδύναμη μὲ τὴν

$$\frac{\phi(m)}{d}\,\mathrm{ind}(a) \equiv 0 \pmod{\phi(m)},$$

δηλαδή, λόγῳ τῶν δ′ καὶ ε′ τοῦ θεωρήματος 5.2.1, μὲ τὴν

$$\mathrm{ind}(a^{\frac{\phi(m)}{d}}) \equiv 0 = \mathrm{ind}(1) \pmod{\phi(m)},$$

ἡ ὁποία εἶναι ἰσοδύναμη μὲ τὴν ἀποδεικτέα, λόγῳ τοῦ θεωρήματος 5.2.1-α΄.
δ΄. Ἔστω $\mathrm{ord}_m(a) = r$. Τότε $a^r \equiv 1 \pmod m$ καὶ ὁ r εἶναι ὁ ἐλάχιστος θετικὸς ἀκέραιος s μὲ τὴν ἰδιότητα $a^s \equiv 1 \pmod m$. Ἡ τελευταία ἰσοτιμία ἰσοδυναμεῖ μὲ τὴν $\mathrm{ind}(a^s) \equiv 0 \pmod{\phi(m)}$ (α΄ τοῦ θεωρήματος 5.2.1), δηλαδή, μὲ τὴν $s\,\mathrm{ind}(a) \equiv 0 \pmod{\phi(m)}$ (δ΄ τοῦ θεωρήματος 5.2.1). Συνεπῶς, ἡ ἰσοτιμία $a^s \equiv 1 \pmod m$ ἰσοδυναμεῖ μὲ τὸ ὅτι ὁ $s\,\mathrm{ind}(a)$ εἶναι κοινὸ πολλαπλάσιο τῶν $\phi(m)$ καὶ $\mathrm{ind}(a)$. Καθὼς ὁ r εἶναι ὁ ἐλάχιστος s, γιὰ τὸν ὁποῖον ἰσχύει ἡ $a^s \equiv 1 \pmod m$, συμπεραίνομε ὅτι $r\,\mathrm{ind}(a)$ εἶναι τὸ ἐλάχιστο κοινὸ πολλαπλάσιο τῶν $\mathrm{ind}(a)$ καὶ $\phi(m)$, ἄρα, μὲ τὴ βοήθεια καὶ τοῦ θεωρήματος 1.3.1-α΄, ἔχομε

$$r\,\mathrm{ind}(a) = [\phi(m), \mathrm{ind}(a)] = \frac{\phi(m)\,\mathrm{ind}(a)}{(\phi(m), \mathrm{ind}(a))}$$

ἀπ' ὅπου ἕπεται ἀμέσως ἡ ἀποδεικτέα. **ὅ.ἔ.δ.**

5.3 Ἀσκήσεις τοῦ κεφαλαίου 5

Στὶς ὑπολογιστικὲς ἀσκήσεις πρέπει νὰ κάνετε χρήση τῶν πινάκων 5.1 καὶ 5.2

1. Ἔστω $m \geq 2$, $(a, m) = 1$. Ἂν $\mathrm{ord}_m(a) = k$ καὶ $a'a \equiv 1 \pmod m$, τότε $\mathrm{ord}_m(a') = k$.

2. Ἔστω $m \geq 2$, $(a, m) = 1$ καὶ q πρῶτος. Ἂν γιὰ κάποιο $k \geq 1$ ἰσχύει $a^{q^k} \equiv 1 \pmod m$ καὶ $a^{q^{k-1}} \not\equiv 1 \pmod m$ ἀποδεῖξτε ὅτι $\mathrm{ord}_m(a) = q^k$.

3. Ἔστω ὅτι ὁ πρῶτος q διαιρεῖ τὸν $a^{2^m} + 1$ γιὰ κάποιο a. Ἀποδεῖξτε ὅτι $q \equiv 1 \pmod{2^{m+1}}$.
   Ὑπόδειξη: Παρατηρῆστε ὅτι $a^{2^m} \equiv -1 \pmod q$ καὶ ἐφαρμόστε τὴν ἄσκηση 2.

4. Ἔστω ὅτι ὁ p εἶναι περιττὸς πρῶτος καὶ ὁ g εἶναι γεννήτορας μέτρῳ p. Ἔστω k μὴ ἀρνητικὸς ἀκέραιος καὶ $(g + kp)^{p-1} \equiv a \pmod{p^2}$. Ἀποδεῖξτε ὅτι ὁ a εἶναι τῆς μορφῆς $1 + bp$ μὲ b ἀκέραιο. Ἐπιπλέον, ἂν ὁ b δὲν διαιρεῖται διὰ p, τότε ὁ $g + kp$ εἶναι γεννήτορας μέτρῳ p^n γιὰ κάθε $n \geq 1$.
   Ὑπόδειξη: Ἔστω $(g + kp)^{p-1} = 1 + p\ell$. Ἀποδεῖξτε ὅτι, ἂν ὁ b δὲν διαιρεῖται διὰ p, τότε οὔτε ὁ ℓ διαιρεῖται διὰ p καὶ ἐφαρμόστε τὸ α΄ τοῦ θεωρήματος 5.1.5.
   Σύμφωνα μὲ αὐτὴ τὴν ἄσκηση, ἂν $g^{p-1} \equiv a \pmod{p^2}$ καὶ ὁ ἀκέραιος $\frac{a-1}{p}$ δὲν διαιρεῖται διὰ p, τότε ὁ g εἶναι γεννήτορας, ἐπίσης, μέτρῳ p^n, γιὰ κάθε $n \geq 1$.

5. Ὑπολογῖστε τὴν $\mathrm{ord}_{43}(4)$, πρῶτα χωρὶς νὰ χρησιμοποιήσετε τὸ θεώρημα 5.2.2 καὶ μετά, χρησιμοποιώντας το.

6. Θεωρῆστε τὸν πρῶτο 191. Στὸν πίνακα 5.1 θὰ βρεῖτε ἕνα συγκεκριμένο γεννήτορα g μέτρῳ p. Ἀποδεῖξτε, χρησιμοποιώντας τὴν ἄσκηση 4, ὅτι ὁ g

εἶναι γεννήτορας μέτρῳ 191^n, καθὼς καὶ γεννήτορας μέτρῳ $2\cdot 191^n$ γιὰ κάθε $n \geq 1$. Γιὰ τὸ μέτρο $2 \cdot 191^n$ θὰ χρειαστεῖτε τὸ Θεώρημα 5.1.5 (γ′).
Ὑπολογιστικὲς ὁδηγίες: Τοὺς ὑπολογισμοὺς τῆς μορφῆς $a^n \pmod m$ ποὺ θ' ἀπαιτηθοῦν, μπορεῖτε νὰ κάνετε στὸν ὑπολογιστὴ μὲ χρήση ὁποιουδήποτε ὑπολογιστικοῦ πακέτου θέλετε, δίχως αὐτὸ νὰ εἶναι ἀπολύτως ἀπαραίτητο.

7. Θεωρῆστε τὸν πρῶτο 337. Στὸν πίνακα 5.1 θὰ βρεῖτε ἕνα συγκεκριμένο γεννήτορα g μέτρῳ p. Ἀποδεῖξτε, χρησιμοποιώντας τὴν ἄσκηση 4, ὅτι ὁ g εἶναι γεννήτορας μέτρῳ 337^n γιὰ κάθε $n \geq 1$. Κάνοντας χρήση τοῦ Θεωρήματος 5.1.5 (γ′) ὑπολογῖστε ἕνα γεννήτορα g μέτρῳ $2\cdot 337^5$. Ὁ g_1 ποὺ θὰ βρεῖτε εἶναι πολὺ μεγάλος. Μπορεῖ νὰ βρεθεῖ κάποιος πιὸ "φιλικός" γεννήτορας μέτρῳ $2 \cdot 337^n$ καί, μάλιστα, γιὰ ὁποιοδήποτε $n \geq 1$; Ναί, ὡς ἑξῆς (συνεχίζεται ἡ ἄσκηση): Ὑπολογῖστε τὸν $g_2 \equiv g^{11} \pmod{337}$ καὶ διαπιστῶστε ὅτι ὁ g_2 εἶναι πολὺ μικρός. (α′) Γιατὶ g_2 εἶναι, ἐπίσης, γεννήτορας μέτρῳ 337; (β′) Γιατὶ ὁ g_2 εἶναι γεννήτορας μέτρῳ 337^n καθὼς καὶ μέτρῳ $2 \cdot 337^n$ γιὰ κάθε $n \geq 1$;
Ὑπολογιστικὲς ὁδηγίες ἴδιες μὲ αὐτὲς τῆς προηγούμενης ἄσκησης.

8. Ὑπολογῖστε τὴν $\mathrm{ord}_m(a)$ στὶς ἑξῆς περιπτώσεις: (α′) $m = 23^3$ καὶ $a = 5^{11}$. (β′) $m = 82$ καὶ a τὸν ἀκέραιο μὲ $\mathrm{ind}(a) = 10$.

9. Ἔστω $m > 1$ καὶ ὑπάρχουν γεννήτορες μέτρῳ m. Ἀποδεῖξτε ὅτι ἡ ἐκθετικὴ ἰσοτιμία $a^x \equiv b \pmod m$ ἔχει λύσεις ἄν, καὶ μόνο ἄν, $(\mathrm{ind}(a), \phi(m))|b$ καί, στὴν περίπτωση ποὺ ἔχει, τὸ πλῆθος τῶν διαφορετικῶν μέτρῳ $\phi(m)$ λύσεων εἶναι $(\mathrm{ind}(a), \phi(m))$ ἐνῶ, μέτρῳ $\mathrm{ord}_m(a)$, ἡ λύση εἶναι μοναδική. Συνεπῶς, στὴν περίπτωση ποὺ ἡ ἰσοτιμία $a^x \equiv b \pmod m$ ἔχει λύσεις, ὑπάρχει ἕνας μοναδικὸς $x \in \{0, 1, \ldots, \mathrm{ord}_m(a) - 1\}$, ποὺ τὴν ἐπαληθεύει.

10. Ποιοὶ ἀπὸ τοὺς ἀριθμοὺς 6, 27 καὶ 37 εἶναι 35ες δυνάμεις μέτρῳ 31^2;

11. Ἀποδεῖξτε ὅτι ἡ ἐκθετικὴ ἰσοτιμία $12^x \equiv 11 \pmod{47}$ εἶναι ἀδύνατη, ἐνῶ ἡ $12^x \equiv 21 \pmod{47}$ ἔχει λύσεις, τὶς ὁποῖες καὶ νὰ ὑπολογίσετε.

12. Ὑπολογῖστε ὅλους τοὺς ἀριθμοὺς τοῦ συνόλου $\{1, 2, \ldots, 70\}$, οἱ ὁποῖοι εἶναι γεννήτορες μέτρῳ 71.

13. Ἔστω περιττὸς πρῶτος p καὶ $n \geq 1$. Ἂν $S_n(p) = \sum_{k=1}^{p-1} k^n$, ἀποδεῖξτε ὅτι

$$S_n(p) \equiv \begin{cases} -1 \pmod p & \text{ἂν } (p-1) \mid n \\ \ \ 0 \pmod p & \text{ἂν } p - 1 \nmid n \end{cases}.$$

Ὑπόδειξη. Ἔστω g γεννήτορας μέτρῳ p. Γιὰ κάθε $k = 1, 2, \ldots, p-1$ ὑπάρχει ν, τέτοιο ὥστε $k \equiv g^\nu \pmod p$.

14. Ἔστω πρῶτος $p > 3$. Ἀποδεῖξτε ὅτι τὸ γινόμενο τῶν ἀριθμῶν ἑνὸς περιορισμένου συστήματος ὑπολοίπων μέτρῳ p, οἱ ὁποῖοι εἶναι γεννήτορες μέτρῳ p,

εἶναι ἰσότιμο μὲ 1 μέτρῳ p.
Ὑπόδειξη. Ἔστω g ἕνας γεννήτορας μέτρῳ p. Γιὰ ποιοὺς ἐκθέτες k εἶναι καὶ g^k γεννήτορας; Ἂν ὁ g^k εἶναι γεννήτορας, τὸ ἴδιο ἰσχύει καὶ γιὰ τὸν g^{p-1-k}. Ἐπίσης, ἀφοῦ $p > 3$, ὁ $g^{(p-1)/2}$ δὲν εἶναι γεννήτορας .

15. Ἔστω p πρῶτος τῆς μορφῆς $2^{2^k} + 1$.
(α′) Ἀποδεῖξτε ὅτι ἕνας ἀριθμὸς πρῶτος πρὸς τὸν p εἶναι γεννήτορας μέτρῳ p ἂν καὶ μόνο ἂν εἶναι τετραγωνικὸ ἀνισοϋπόλοιπο μέτρῳ p.
Ὑπόδειξη. Ἔστω g γεννήτορας μέτρῳ p. Γιὰ ποιοὺς ἐκθέτες k εἶναι καὶ g^k γεννήτορας; Μετά, ἐφαρμόστε τὴν πρόταση β′ τοῦ θεωρήματος 4.1.1.
(β′). Χρησιμοποιεῖστε τὸ (α′) γιὰ νὰ ἀποδείξετε ὅτι ὁ 7 εἶναι γεννήτορας μέτρῳ p.
Ὑπόδειξη. Ἀποδεῖξτε πρῶτα, ἐπαγωγικά, καὶ ἀνεξάρτητα ἀπὸ τὴ συγκεκριμένη ἄσκηση, ὅτι $2^{2^k} \equiv 2$ ἢ $4 \pmod 7$, ἀνάλογα μὲ τὸ ἂν ὁ k εἶναι ἄρτιος ἢ περιττός, ἀντιστοίχως. Σὲ συνδυασμὸ μὲ αὐτό, θὰ χρειασθεῖτε, ἐπίσης, τὸν νόμο τῆς τετραγωνικῆς ἀντιστροφῆς τοῦ Gauss προκειμένου νὰ ἀποδείξετε ὅτι ὁ 7 εἶναι τετραγωνικὸ ἀνισοϋπόλοιπο μέτρῳ p.

16. Ἡ ἄκηση αὐτὴ περιέχει κριτήρια πιστοποίησης πρώτου, ὀφειλόμενα στοὺς Maurice Borisovich Kraitchik, Derrick Henry Lehmer, Édurad Lucas, Henry Cabourn Pocklington, François Proth, John Selfridge.

Ἔστω $n \geq 3$. Ἀποδεῖξτε ὅτι, ἂν ὁ n ἱκανοποιεῖ μία ὁποιαδήποτε ἀπὸ τὶς παρακάτω συνθῆκες (α′)-(ϛ′), τότε ὁ n εἶναι πρῶτος.

(α′) (Lucas 1876) Ὑπάρχει a τέτοιος ὥστε $a^{n-1} \equiv 1 \pmod n$ καὶ $a^k \not\equiv 1 \pmod n$ γιὰ κάθε $k = 1, \ldots, n-2$.
Ὑπόδειξη: Ἂν ὑπῆρχε γνήσιος πρῶτος διαιρέτης p τοῦ n, τότε, γιὰ κάποιο $k \in \{1, \ldots, n-1\}$ θὰ ἦταν $p \equiv a^k \pmod n$, ὁπότε ὁδηγηθεῖτε σὲ ἄτοπο.

(β′) (Lucas 1878) Ὑπάρχει a τέτοιος ὥστε $a^{n-1} \equiv 1 \pmod n$ καὶ $a^k \not\equiv 1 \pmod n$ γιὰ κάθε θετικὸ διαιρέτη k τοῦ $n-1$, μικρότερο τοῦ $n-1$.
Ὑπόδειξη: Ποιὰ εἶναι ἡ τάξη τοῦ a; Μετὰ ἐφαρμόστε τὸ (16α′).

(γ′) (Lucas-Kraitchik-Lehmer 1927) Ὑπάρχει a τέτοιος ὥστε $a^{n-1} \equiv 1 \pmod n$ καὶ $a^{(n-1)/q} \not\equiv 1 \pmod n$ γιὰ κάθε πρῶτο διαιρέτη q τοῦ $n-1$.
Ὑπόδειξη: Ἔστω $r = \mathrm{ord}_n(a)$. Ἰσχύει $n-1 = rs$. Ἂν $s = 1$, ἐφαρμόστε τὸ (16α′)· ἂν $s > 1$, θεωρῆστε ἕνα πρῶτο διαιρέτη τοῦ s καὶ ἐφαρμόστε τὸ (16β′).

(δ′) (Selfridge 1967) Γιὰ κάθε πρῶτο διαιρέτη q τοῦ $n-1$ ὑπάρχει a_q (δηλαδή, ἀκέραιος ἐξαρτώμενος ἀπὸ τὸν q) τέτοιος ὥστε $a_q^{n-1} \equiv 1 \pmod n$ καὶ $a_q^{(n-1)/q} \not\equiv 1 \pmod n$.
Ὑπόδειξη: Ἔστω ὅτι $q_1, \ldots, q_m$ εἶναι ὅλοι οἱ διαφορετικοὶ πρῶτοι διαιρέτες τοῦ $n-1$ καὶ $a_1, \ldots, a_m$ οἱ ἀκέραιοι $a_{q_1}, \ldots, a_{q_m}$, ποὺ μᾶς ἐξασφαλίζει ἡ ὑπόθεση. Ἔστω $r_i = \mathrm{ord}_n(a_i)$, $(i = 1, \ldots, m)$. Διαπιστῶστε πρῶτα ὅτι ὑπάρχει a μὲ $\mathrm{ord}_n(a) = r$, ὅπου $r = \text{ΕΚΠ}(r_1, \ldots, r_m)$. Ἀποδεῖξτε ὅτι $a^{n-1} \equiv 1 \pmod n$ καὶ $a^{(n-1)/q_i} \not\equiv 1 \pmod n$ γιὰ κάθε $i = 1, \ldots, m$, ὁπότε ἐφαρμόστε τὸ (16γ′).

(ε′) (Proth 1878) Ὁ $n-1$ μπορεῖ νὰ ἀναλυθεῖ ὡς $n-1 = 2^r s$, ὅπου $s < 2^r$ καὶ γιὰ κάθε πρῶτο διαιρέτη p τοῦ n ὑπάρχει a τέτοιος ὥστε $a^{(n-1)/2} \equiv -1 \pmod{p}$.
Ὑπόδειξη: Ἔστω p πρῶτος διαιρέτης τοῦ n. Παρατηρῆστε ὅτι $(a^s)^{2^{r-1}} \equiv -1 \pmod{p}$ καὶ ἐφαρμόστε τὴν ἄσκηση 3 γιὰ νὰ καταλήξετε στὸ συμπέρασμα ὅτι $p \geq 1 + 2^r$. Συνεπῶς, ἂν ὁ n εἶχε δύο πρώτους διαιρέτες (ἴσους ἢ ἄνισους), τότε $n \geq (1+2^r)^2$, ὁπότε ὁδηγηθεῖτε σὲ ἀντίφαση.

(ϛ′) (Pocklington 1914) Ὁ $n-1$ μπορεῖ νὰ ἀναλυθεῖ ὡς $n-1 = km$, ὅπου $1 \leq k < m$ καὶ $(k,m) = 1$ καὶ γιὰ κάθε πρῶτο διαιρέτη q τοῦ m ὑπάρχει a_q τέτοιος ὥστε $a_q^{n-1} \equiv 1 \pmod{n}$ καὶ $(a_q^{(n-1)/q} - 1, n) = 1$.
Ὑπόδειξη: Κατ' ἀρχάς, ἀπὸ τὴν ὑπόθεση γιὰ τοὺς k, m, συμπεράνατε ὅτι $m > \sqrt{n}$. Ὕστερα, παρατηρῆστε ὅτι, ἂν ὁ n εἶναι σύνθετος, τότε ἔχει ἕνα πρῶτο διαιρέτη $p \leq \sqrt{n}$. Ἔστω τώρα q ἕνας ὁποιοσδήποτε πρῶτος διαιρέτης τοῦ $n-1$, $e = v_q(n-1)$ καὶ $c = a_q^{(n-1)/q^e}$. Ἀποδεῖξτε, ἐκμεταλευόμενοι τὶς ὑποθέσεις, ὅτι $c^{q^e} \equiv 1 \pmod{n}$, ἄρα καὶ $c^{q^e} \equiv 1 \pmod{p}$, ἐνῶ $c^{q^{e-1}} \not\equiv 1 \pmod{p}$. Συμπεράνατε τώρα, μὲ τὴ βοήθεια τῆς ἄσκησης 2 ὅτι $q^e | p-1$. Αὐτὸ τὸ συμπέρασμα θὰ σᾶς ἐπιτρέψει νὰ συμπεράνετε, ἂν φαντασθεῖτε τὴν κανονικὴ ἀνάλυση $q_1^{e_1} q_2^{e_2} \cdots$ τοῦ m, ὅτι $m | p-1$, ἄρα $m \leq p-1$. Συνδυᾶστε μὲ τὶς ἀνισότητες $m > \sqrt{n}$ καὶ $p \leq \sqrt{n}$, ποὺ ἀναφέρθηκαν στὴν ἀρχὴ τῆς ὑπόδειξης.

Εὑρετήριο