

ΘΕΜΕΛΙΩΔΗΣ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ν.Γ. Τζανάκης

Τμήμα Μαθηματικῶν - Πανεπιστήμιο Κρήτης

22-5-2012

Περιεχόμενα

1	Διαιρετότητα	3
1.1	Βασικές προτάσεις	3
1.2	Μέγιστος κοινός διαιρέτης	5
1.3	Έλάχιστο κοινό πολλαπλάσιο	11
1.4	Πρώτοι αριθμοί	12
1.5	Πυθαγόρειες τριάδες	17
1.6	Άσκησης του κεφαλαίου 1	19
2	Ίσοτιμίες	25
2.1	Όρισμοί και βασικές ιδιότητες	25
2.2	Συστήματα υπόλοιπων	27
2.3	Ύψωση σε δύναμη	32
2.4	Η κρυπτογραφική μέθοδος RSA	34
2.5	Άσκησης του κεφαλαίου 2	36
3	Έπίλυση ίσοτιμιών	41
3.1	Γενικά	41
3.2	Ίσοτιμίες πρώτου βαθμοῦ	41
3.3	Τὸ κινέζικο θεώρημα ὑπολοίπων	43
3.4	Πολυωνυμικές ίσοτιμίες με ἓνα ἄγνωστο	44
3.5	Άσκησης του κεφαλαίου 3	49
4	Τετραγωνικὰ ἰσοῦπόλοιπα	53
4.1	Όρισμοί και βασικές ιδιότητες	53
4.2	Τὸ σύμβολο του Legendre	54
4.3	Τὸ σύμβολο του Jacobi	59
4.4	Έπίλυση τῆς ἰσοτιμίας $x^2 \equiv b \pmod{m}$	64
4.5	Άσκησης του κεφαλαίου 4	66
5	Γεννήτορες και διακριτοὶ λογάριθμοι	69
5.1	Γεννήτορες	69
5.2	Διακριτοὶ λογάριθμοι	75
5.3	Άσκησης του κεφαλαίου 5	81

Κεφάλαιο 1

Διαιρετότητα

Τὰ λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους ἀριθμούς

Δουλεύουμε στο σύνολο \mathbb{Z} τῶν ἀκεραίων ἀριθμῶν. Οἱ θετικοὶ ἀκέριοι 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 ὀρισμοῦ, ἓνας ρητὸς ἀριθμὸς εἶναι πηλίκο a/b δύο ἀκεραίων ἀριθμῶν a, b μὲ $b \neq 0$.

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

1.1 Βασικὲς προτάσεις

Τὸ ἄθροισμα, ἡ διαφορά καὶ τὸ γινόμενο δύο ἀκεραίων εἶναι πάντα ἀκέραιοι. Τὸ πηλίκο τους, ὅμως, δὲν εἶναι πάντα ἀκέραιοι. Ἄν γιὰ τοὺς ἀκεραίους a, b , μὲ $b \neq 0$ συμβεῖ νὰ εἶναι τὸ πηλίκο τους a/b ἀκέραιοι, δηλαδή, ἂν ὑπάρχει $c \in \mathbb{Z}$, τέτοιος ὥστε $a = bc$, τὸ γεγονός αὐτὸ συμβολίζεται $b|a$ καὶ ἐκφράζεται μὲ τὶς ἐξῆς *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 διαιρετὸς 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 ἓνα ρητὸ ἀριθμὸ (τὸ πηλίκο b/a).

Πρόταση 1.1.1 *Ίσχύουν τὰ ἐξῆς:*

α'. $1|a$ γιὰ κάθε a .

β'. $b|0$ γιὰ κάθε $b \neq 0$.

γ'. Ἐάν $b, c \neq 0$ καὶ $c|b$ καὶ $b|a$, τότε $c|a$.

δ'. Ἐάν $c|a$ καὶ $c|b$, τότε $c|(a'+b')$, γιὰ ὁποιοὺςδήποτε ἀκεραίους a', b' .

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

ζ'. Ἐάν 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, $a' + b' b = a' (a_1 c) + b' (b_1 c) = (a' a_1 + b' b_1) c$, ποὺ σημαίνει ὅτι $c|(a' + b' b)$.

ε'. Εἶναι $a = bc$ γιὰ κατάλληλο $c \in \mathbb{Z}$, ἄρα $|a| = |b||c|$. Ἐάν εἶναι $a \neq 0$, τότε $|c| \neq 0$, ἄρα $|c| \geq 1$, ὁπότε $|a| = |b||c| \geq |b|$.

ζ'. Ἀπὸ τὸ ε', συμπεραίνομε ὅτι $|b| \leq |a|$ καὶ $|a| \leq |b|$, ἄρα $|a| = |b|$ ἢ, ἰσοδύναμα, $b = \pm a$. **Ὡ.ξ.δ.**

Θεώρημα 1.1.2 –Εὐκλείδεια διαίρεση. *Γιὰ κάθε ζευγὸς ἀκεραίων (a, b) μὲ $b > 0$ ὑπάρχει ἓνα μοναδικὸ ζευγὸς 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 ἓνα τέτοιο ζευγὸς (q, r) καὶ μετὰ ὅτι δὲν ὑπάρχει δεύτερο.

Ἐστω $q = \lfloor \frac{a}{b} \rfloor$. Τότε, ἀπὸ τὴν ιδιότητα τοῦ ἀκεραίου μέρους, $q \leq \frac{a}{b} < q+1$, ποὺ συνεπάγεται ὅτι $bq \leq a < bq + b$. Αὐτὸ, ὅμως, προφανῶς σημαίνει ὅτι $a = bq + r$ μὲ $r \geq 0$ καὶ $r < b$.

Ἐάν ὑποθέσομε τώρα ὅτι καὶ τὸ ζευγὸς (q_1, r_1) ἔχει ἀνάλογες ιδιότητες μὲ τὸ (q, r) , τότε $bq_1 + r_1 = a = bq + r$, ἄρα $b(q_1 - q) = r - r_1$. Ἐάν 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, ἢ ὅποια εἶναι γνησίως μικρότερη τοῦ b , ἀφοῦ, ἐξ

υποθέσεως, $0 \leq r, r_1 < b$. Αυτή ή αντίφαση μᾶς αναγκάζει νὰ συμπεράνομε ὅτι $r_1 = r$, ὁπότε καὶ $q_1 = q$. **ὄ.ξ.δ.**

Στὴν εἰδικὴ περίπτωση, πού $b = 2$, οἱ πιθανές τιμές 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 στὴν περίπτωση πού 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 κοινός διαιρέτης

Σταθεροποιῶμε δύο μὴ μηδενικούς ἀκεραίους a, b . Κοινὸς διαιρέτης τῶν a, b εἶναι κάθε ἀκέραιος, πού διαιρεῖ καὶ τὸν a καὶ τὸν b . Ἀπὸ τὸ θεώρημα 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 ἢ, τὸ πολὺ, ἴσος μὲ τὸ $\min(|a|, |b|)$. Συνεπῶς, τὸ σύνολο τῶν κοινῶν διαιρετῶν τῶν a, b εἶναι πεπερασμένο, ὁπότε ἔχει ἓνα μέγιστο στοιχεῖο, τὸ ὁποῖο καλεῖται *μέγιστος κοινός διαιρέτης τῶν a, b* καὶ συμβολίζεται (a, b) , ἢ, ἂν ὑπάρχει φόβος συγχύσεως, $\text{MK}\Delta(a, b)$.

Ὅρίζομε τώρα τὸ σύνολο

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

Εἶναι τετριμμένο νὰ διαπιστώσει κανεὶς τὶς ἐξῆς βασικὲς ιδιότητες τοῦ Δ :

1. Τὸ ἄθροισμα δύο ἀριθμῶν, πού ἀνήκουν στὸ Δ , ἀνήκει, ἐπίσης, στὸ Δ .
2. Τὸ γινόμενο ἑνὸς ἀριθμοῦ τοῦ Δ μὲ ἓναν ὅποιονδήποτε ἀκέραιο, πάλι ἀνήκει στὸ Δ ¹

Παρατηροῦμε τώρα τὰ ἐξῆς:

- 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 .

Εἶδαμε ὅτι τὸ Δ περιέχει θετικούς ἀκεραίους· ἔστω, λοιπόν, d ὁ ἐλάχιστος θετικὸς ἀκέραιος, πού περιέχεται στὸ Δ .

• Τὸ Δ ταυτίζεται μὲ τὸ σύνολο τῶν πολλαπλασίων τοῦ d : συμβολικά, $\Delta = d\mathbb{Z}$. Πράγματι, ἀφοῦ $d \in \Delta$, ἡ ιδιότητα 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 ἄς ἐκτελέσομε τὴν εὐκλείδεια διαίρεση τοῦ m διὰ d : Βάσει τοῦ θεωρήματος 1.1.2, ἄς γράψομε $m = dq + r$ μὲ

¹Οἱ ἐπαίοντες θὰ ἀναγνωρίσουν σὲ αὐτὲς τὶς δύο ιδιότητες τοῦ Δ ἓνα *ιδεῶδες* τοῦ \mathbb{Z} .

$0 \leq r < d$. Τώρα, από την ιδιότητα 2 του Δ και το γεγονός ότι $d \in \Delta$ συμπεραίνουμε ότι $d(-q) \in \Delta$. Όμως, έξ ύποθέσεως, $m \in \Delta$, άρα, από την ιδιότητα 1 του Δ , έπεται ότι $m - qd \in \Delta$, δηλαδή, $r \in \Delta$. Όποτε, αν ήταν $r > 0$, θα είχαμε βρει ένα θετικό στοιχείο του Δ μικρότερο του d , κάτι που έρχεται σε αντίφαση με την έκλογή του d . Συνεπώς, $r = 0$, όποτε $m = dq \in d\mathbb{Z}$ και καταλήγουμε στο συμπέρασμα ότι $\Delta \subseteq d\mathbb{Z}$.

• Ό d είναι κοινός διαιρέτης των a, b . Αυτό συνεπάγεται, ειδικότερα, ότι κάθε διαιρέτης του d είναι κοινός διαιρέτης των a, b , αφού ή σχέση τής διαιρετότητας είναι μεταβατική (γ' τής πρότασης 1.1.1).

Πράγματι, όπως είδαμε παραπάνω, $a \in \Delta$. Άλλα $\Delta = d\mathbb{Z}$, καθώς δείξαμε μόλις πριν, άρα $a \in d\mathbb{Z}$, δηλαδή, ό a είναι πολλαπλάσιο του d : ισοδύναμα, ό d είναι διαιρέτης του a . Άνάλογα και για τον b .

• Κάθε κοινός διαιρέτης c των a, b διαιρεί τον d .

Πράγματι, έξ όρισμού του Δ και έπειδή $d \in \Delta$, υπάρχουν $x_0, y_0 \in \mathbb{Z}$, τέτοιοι ώστε $d = ax_0 + by_0$. Γράφοντας τώρα $a = a_1c$, $b = b_1c$, βλέπομε ότι $d = c(a_1x_0 + b_1y_0)$, που σημαίνει ότι $c|d$.

Τό συμπέρασμα αυτό συνεπάγεται, ειδικότερα, ότι $|c| \leq d$ (έ' τής πρότασης 1.1.1), άρα βάσει των προηγουμένων, ό d είναι και κοινός διαιρέτης των a, b και ό μεγαλύτερος από όλους τους άλλους κοινούς διαιρέτες των a, b .

Συνοψίζοντας τὰ συμπεράσματά μας, καταλήγουμε στο έξής βασικό

Θεώρημα 1.2.1 Έστω d ό μέγιστος κοινός διαιρέτης δύο άκεραίων a, b . Τότε:

α'. Τό σύνολο των κοινών διαιρετών των a, b ταυτίζεται με τό σύνολο των διαιρετών του d .

β'. Υπάρχουν άκεραίοι x_0, y_0 , τέτοιοι ώστε $d = ax_0 + by_0$.

Ό μέγιστος κοινός διαιρέτης ενός πεπερασμένου πλήθους άκεραίων a_1, a_2, \dots, a_n συμβολίζεται (a_1, a_2, \dots, a_n) και όρίζεται ως ό μέγιστος θετικός άκεραίος, ό όποιος διαιρεί καθέναν από τους a_1, \dots, a_n . Ό ύπολογισμός του μπορεί να γίνει αναδρομικά, ως έξής:

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

Χρειάζεται, βέβαια, απόδειξη ότι αυτή ή αναδρομική διαδικασία όδηγει στην εύρεση του μεγίστου κοινού διαιρέτη των a_1, \dots, a_n : βλ. άσκηση 13. Επίσης, ή άσκηση 14 λέει ότι ό μέγιστος κοινός διαιρέτης πολλών αριθμών έχει ιδιότητες ανάλογες με αυτές του μεγίστου κοινού διαιρέτη, που αναφέρονται στο θεώρημα 1.2.1.

Όταν $(a_1, a_2, \dots, a_n) = 1$, τότε λέμε ότι οι a_1, a_2, \dots, a_n είναι *πρώτοι μεταξύ τους*. Η ιδιότητα αυτή των a_1, a_2, \dots, a_n είναι άσθενέστερη από την ιδιότητα να είναι *ανά ζεύγη πρώτοι*, εκτός, βέβαια, αν $n = 2$, που οι ιδιότητες είναι ισοδύναμες. Για

παράδειγμα, οί αριθμοί 10,12,15 είναι πρώτοι μεταξύ τους, αφού ό μόνος κοινός (καί για τούς τρείς) διαιρέτης τους είναι ό 1. Όμως, ανά ζεύγη, δέν είναι πρώτοι, αφού $(10, 12) = 2$, $(10, 15) = 5$ καί $(12, 15) = 3$. Φυσικά, είναι φανερό ότι, αν οί a_1, a_2, \dots, a_n είναι πρώτοι ανά ζεύγη, είναι καί πρώτοι μεταξύ τους.

Θεώρημα 1.2.2 – Ίδιότητες του MKΔ

α'. Αν $b|a$ τότε $(a, b) = |b|$.

β'. Αν $a = bq + c$ τότε τό σύνολο τών κοινών διαιρετών τών a, b συμπίπτει με τό σύνολο τών κοινών διαιρετών τών b, c : ειδικότερα, $(a, b) = (b, c)$.

γ'. Για όποιοδήποτε άκέραιο c , $(ca, cb) = |c|(a, b)$

δ'. Αν ό c είναι κοινός διαιρέτης τών a, b , τότε $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a, b)}{|c|}$. Αυτό, ειδικότερα, συνεπάγεται –για $c = (a, b)$ – ότι οί $a/(a, b)$ καί $b/(a, b)$ είναι πρώτοι μεταξύ τους.

ε'. Αν $(a, b) = 1$ καί c όποιοσδήποτε άκέραιος, τότε $(ac, b) = (c, b)$.

ς'. Αν $(a, b) = 1$ καί $b|ac$, τότε $b|c$.

ζ'. Αν καθένας από τούς a_1, \dots, a_n είναι πρώτος προς καθέναν από τούς b_1, \dots, b_m , τότε $(a_1 \cdots a_n, b_1 \cdots b_m) = 1$.

Άπόδειξη α'. Ό $|b|$ είναι, προφανώς, ό μέγιστος διαιρέτης του b καί, έξ ύποθέσεως, διαιρεί τόν a , άρα είναι μέγιστος κοινός διαιρέτης τών a, b .

β'. Κάθε κοινός διαιρέτης τών a, b διαιρεί τούς a καί bq , άρα διαιρεί καί τόν $c = (-1)a + qb$ (βλ. θεώρημα 1.1.1), όποτε είναι κοινός διαιρέτης τών b, c . Αντίστροφα, κάθε κοινός διαιρέτης τών b, c διαιρεί τόν $qb + c = a$, άρα είναι κοινός διαιρέτης τών a, b .

γ'. Έστω $(a, b) = d$. Έπειδή ό $|c|$ διαιρεί τόν c καί ό d διαιρεί τόν a , ό $|c|d$ διαιρεί τόν ca καί, όμοίως, διαιρεί καί τόν cb . Ό $|c|d$ είναι, λοιπόν, κοινός διαιρέτης τών ca, cb , άρα (α' του θεωρήματος 1.2.1) διαιρεί τόν (ca, cb) . Θα δείξομε ότι, καί αντίστροφα, ό (ca, cb) διαιρεί τόν $|c|d$. Πράγματι, τό β' του θεωρήματος 1.2.1 μάς εξασφαλίζει τήν ύπαρξη άκεραίων x_0, y_0 , τέτοιων ώστε $ax_0 + by_0 = d$, όποτε $(ca)x_0 + (cb)y_0 = cd$. Τό άριστερό μέλος αυτής τής σχέσης διαιρείται, προφανώς, από τόν (ca, cb) , άρα ό (ca, cb) διαιρεί τόν cd , όποτε καί τόν $|c|d$. Τελικά, οί θετικοί άκέραιοι (ca, cb) καί $|c|d = |c|(a, b)$ άλληλοδιαιροϋνται, όποτε είναι ίσοι (βλ. ς' του θεωρήματος 1.1.1).

δ'. Έφαρμόζοντας τό γ' με $\frac{a}{c}$ στη θέση του a καί $\frac{b}{c}$ στη θέση του b , παίρνομε $|c|\left(\frac{a}{c}, \frac{b}{c}\right) = (a, b)$, δηλαδή, τήν άποδεικτέα σχέση.²

ε'. Έχομε $(c, b)|(ac, b)$. Πράγματι, ό (c, b) διαιρεί τούς c, b άρα είναι κοινός διαιρέτης καί τών ac, b , άρα είναι διαιρέτης του (ac, b) (από τό α' του θεωρήματος 1.2.1). Αντίστροφα, θα δείξομε ότι $(ac, b)|(c, b)$. Από τό β' του θεωρήματος 1.2.1 ξέρομε ότι ύπάρχουν άκέραιοι x_0, y_0 , τέτοιοι ώστε $ax_0 + by_0 = 1$, άρα $(ac)x_0 + b(cy_0) = c$. Βλέπομε ότι τό άριστερό μέλος αυτής τής σχέσης διαιρείται από τόν (ac, b) , άρα ό (ac, b) διαιρεί καί τόν c , όποτε είναι κοινός διαιρέτης τών b, c , άρα καί διαιρέτης

²Δείτε, όμως τήν άσκηση 15.

του (b, c) (ἀπὸ τὸ α' τοῦ θεωρήματος 1.2.1). Οἱ θετικοὶ ἀκέραιοι (c, b) καὶ (ac, b) ἀλληλοδιαιροῦνται λοιπὸν, ἄρα (ζ' τοῦ θεωρήματος 1.1.1) εἶναι ἴσοι.

ζ'. Ἀπὸ τὸ β' τοῦ θεωρήματος 1.2.1 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 πολλές φορές διαδοχικὰ τὸ ϵ' καί, φυσικά, τὴν ὑπόθεση ὅτι ὁ b_1 εἶναι πρῶτος πρὸς καθέναν ἀπὸ τοὺς a_1, a_2, \dots, a_n . Λοιπὸν, ἔχομε διαδοχικὰ:

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

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 $k = 1, \dots, m$. 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. **ὦ.ξ.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 Ἐστω $a \geq b > 0$. Θέτομε $r_0 = a$, $r_1 = b$, $s_{-1} = s_0 = 1$. Γιὰ $i = 1, 2, \dots$ ὀρίζομε 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' . $b = r_1 > r_2 > r_3 > \dots$ καὶ γιὰ κάποιον $i = n \geq 2$ εἶναι $r_{n+1} = 0$. Γι' αὐτὸ τὸ συγκεκριμένον n ἰσχύει $n < 2 \frac{\log b}{\log 2} + 2$ καὶ $r_n = (a, b)$.

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

Ἀπόδειξη α' . Ἐχομε, ἐξ ὀρισμοῦ, $r_{i-1} = r_iq_{i+1} + r_{i+1}$, ὅπου $0 \leq r_{i+1} < r_i$ (βλ. θεώρημα 1.1.2). Συνεπῶς, γιὰ τοὺς μὴ ἀρνητικοὺς ἀκεραίους r_i ἔχομε $r_0 > r_1 > r_2 > \dots \geq 0$, ἄρα κάποιον r_i , ἀναγκαστικά, θὰ εἶναι μηδέν. Ἐστω, λοιπὸν, $r_{n+1} = 0$

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

$$\begin{aligned} a = r_0 &= r_1 q_2 + r_2 = b q_2 + r_2, & 0 < r_2 < r_1 = b \\ b = r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ r_2 &= r_3 q_4 + r_4, & 0 < r_4 < r_3 \\ &\vdots & \\ r_{i-1} &= r_i q_{i+1} + r_{i+1}, & 0 < r_{i+1} < r_i \\ &\vdots & \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

Ἡ τελευταία ἀπὸ τὶς παραπάνω ἰσότητες μᾶς λέει ὅτι $r_n = (r_{n-1}, r_n)$ (βλ. ἀ' τοῦ θεωρήματος 1.2.2). Τώρα ἐφαρμόζομε τὸ β' τοῦ θεωρήματος 1.2.2 διαδοχικὰ, ἀρχίζοντας ἀπὸ τὴν προτελευταία σχέση καὶ ἀνεβαίνοντας πρὸς τὰ πάνω:

$$(r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \dots = (r_4, r_3) = (r_3, r_2) = (r_2, r_1) = (r_1, r_0) = (b, a).$$

Ἐδῶ, τὸ ἀριστερότερο = ὀφείλεται στὴν προτελευταία σχέση, τὸ ἐπόμενο = στὴν δεύτερη ἀπὸ τὸ τέλος σχέση κλπ. Τὸ ἄνω φράγμα γιὰ τὸν n θὰ τὸ ἀποδείξομε στὸ τέλος.

β'. Γιὰ $i = 0, 1, \dots, n$ ἰσχύει ἡ σχέση $r_n = s_i r_{n-i+1} + s_{i-1} r_{n-i}$ (*), τὴν ὁποία θὰ ἀποδείξομε μὲ ἐπαγωγή στὸ i : Γιὰ $i = 0$ τὸ δεξιὸ μέλος γίνεται $s_0 r_{n+1} + s_{-1} r_n = 1 \cdot 0 + 1 \cdot r_n = r_n$. Ἄν, τώρα, ἰσχύει ἡ σχέση γιὰ κάποιον $0 \leq i < n$, τότε πρέπει νὰ δείξομε ὅτι ἰσχύει καὶ γιὰ τὸ $i + 1$, δηλαδή, $r_n = s_{i+1} r_{n-i} + s_i r_{n-i-1}$. Αὐτὸ φαίνεται μὲ ἀπλούστατες πράξεις, ἂν στὸ δεξιὸ μέλος κάνομε τὶς ἀντικαταστάσεις $s_{i+1} = s_{i-1} - s_i q_{n-i+1}$ (βλ. πῶς ὀρίσθηκαν οἱ s_1, s_2, \dots) 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 τὴν σχέση (*), γιὰ $i = n$ παίρνομε $r_n = s_n r_1 + s_{n-1} r_0$, δηλαδή, $(a, b) = s_n b + s_{n-1} a$.

Τέλος, ἀποδεικνύμε τὸ ἄνω φράγμα γιὰ τὸ n : Θὰ ἀποδείξομε πρῶτα ὅτι, γιὰ $i = 1, \dots, n$ ἰσχύει $r_{i-1} > 2r_{i+1}$. Πράγματι, ἂς θεωρήσομε ἓνα τέτοιον δείκτη i . Ἄν εἶναι $r_i \leq r_{i-1}/2$, τότε, λόγω 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, λόγω τῆς $r_{i-1} = r_i q_{i+1} + r_{i+1}$, ἔχομε

$$r_{i+1} = r_{i-1} - r_i q_{i+1} < r_{i-1} - \frac{r_{i-1}}{2} q_{i+1} \leq r_{i-1} - \frac{r_{i-1}}{2} = \frac{r_{i-1}}{2}.$$

Ἐχοντας ἀποδείξει, τώρα, τὴν σχέση $r_{i-1} > 2r_{i+1}$, παίρνομε διαδοχικὰ τὶς ἀνισότητες:

$$b = r_1 > 2r_3 > 2^2 r_5 > 2^3 r_7 > \dots > 2^{(n-1)/2} r_n, \text{ ἂν ὁ } n \text{ εἶναι περιττός,}$$

$$b = r_1 > r_2 > 2r_4 > 2^2 r_6 > 2^3 r_8 > \dots > 2^{(n-2)/2} r_n, \text{ ἂν ὁ } n \text{ εἶναι ἄρτιος.}$$

Σὲ κάθε περίπτωση, λοιπόν, $b > 2^{(n-2)/2}$, ἀπ' ὅπου, λογαριθμίζοντας, παίρνομε τὴν ἀποδεικτέα ἀνισότητα. **ὀ.ξ.δ.**

Μία μικρὴ ἰδέα γιὰ τὴν σπουδαιότητα τοῦ φράγματος, πὸ ἀποδείξαμε, παίρνει κανεὶς ἀπὸ τὴν ἐξῆς συγκεκριμένη περίπτωση: Γιὰ τὸν ὑπολογισμό 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 ἓνα προσωπικὸ ὑπολογιστὴ.

Παράδειγμα. Ὑποδεικνύομε ἓνα 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 πηλίκο (= τελευταῖο μὴ μηδενικὸ ὑπόλοιπο) εἶναι 7, ἄρα $(7168, 917) = 7$.

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

$$\begin{array}{r|l} 7168 & 917 \\ \hline 917 & 749 \quad 7 \\ \hline 749 & 168 \quad 4 \\ \hline 168 & 77 \quad 2 \\ \hline 77 & 14 \quad 5 \\ \hline 14 & 7 \quad 2 \\ \hline 0 & 2 \end{array}$$

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

Ἡ διαδικασία ὑπολογισμοῦ τῶν s_i , ($i = -1, \dots, n$) γίνεται πολὺ ἀπλά: Μὲ τονισμένα τυπογραφικὰ στοιχεῖα σημειώνονται τὰ ἕξ ἀρχῆς γνωστὰ δεδομένα. Κατόπιν, τὰ κουτιά συμπληρώνονται ἀπὸ ἀριστερὰ πρὸς τὰ δεξιὰ. Στὴ γραμμὴ τοῦ q τὰ κουτιά συμπληρώνονται, ἀπὸ τὴν τρίτη στήλη καὶ μετὰ, μὲ τὰ πηλίκα τοῦ εὐκλείδειου ἀλγορίθμου ἀπὸ τὸ τελευταῖο πηλίκο πρὸς τὸ πρῶτο (βλ. παραπάνω), ἐνῶ στὴ γραμμὴ τοῦ s , στὰ δύο ἀριστερότερα κουτιά μπαίνουν τὰ $s_{-1} = s_0 = 1$ καὶ μετὰ, 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 β' τοῦ θεωρήματος 1.2.3. Κουτιά 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 εὐχρηστος ἀλγόριθμος ὑπολογισμοῦ ἀκεραίων x_0, y_0 , τέτοιων ὥστε $ax_0 + by_0 = (a, b)$, περιγράφεται στὴν ἄσκηση 16.

1.3 Ἐλάχιστο κοινὸ πολλαπλάσιο

Σταθεροποιῶμε δύο μὴ μηδενικούς ἀκεραίους a, b . Κοινὸ πολλαπλάσιο τῶν a, b εἶναι κάθε ἀκέραιος, πού 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 Ἐστω ὅτι a, b εἶναι μὴ μηδενικοί ἀκέραιοι. Τότε:

α'. Ἐνας ἀκέραιος εἶναι κοινὸ πολλαπλάσιο τῶν a, b ἂν, καὶ μόνο ἂν, εἶναι τῆς μορφῆς $\frac{nab}{(a, b)}$ γιὰ κάποιο $n \in \mathbb{Z}$. Εἰδικότερα, $[a, b] = \frac{|ab|}{(a, b)}$. 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'. Ἄν $(a, b) = 1$ καὶ καθένας ἀπὸ τοὺς a, b διαιρεῖ τὸν m , τότε καὶ τὸ γινόμενὸ τους ab διαιρεῖ τὸν m .

Γενίκευση: Ἄν οἱ a_1, \dots, 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'. Ἐστω m κοινὸ πολλαπλάσιο τῶν a, b . Ἀφοῦ $a|m$, μποροῦμε νὰ γράψουμε $m = ak$ μὲ $k \in \mathbb{Z}$. Ἐστω $d = (a, b)$ καὶ ἂς θέσουμε $a = da_1, b = db_1$. 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 ζ' τοῦ θεωρήματος 1.2.2 μᾶς ὀδηγεῖ 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 γράψουμε τὸν ἀριθμὸ ὡς $n(a/d)b$, καταλήγουμε στὸ συμπέρασμα ὅτι ὁ ἀριθμὸς εἶναι καὶ πολλαπλάσιο τοῦ b .

Τέλος, εἶναι προφανές ὅτι, μὴ 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'. Ἐστω $d = (a, b)$. 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 .

Ἐστω τώρα ὅτι οἱ a_1, \dots, a_n εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους καὶ καθένας διαιρεῖ

τόν m . Ἐφαρμόζοντας αὐτὸ πὸν ἀποδείξαμε μόλις πρὶν, μὲ $a = a_1, b = a_2$, συμπεραίνομε ὅτι ὁ m εἶναι πολλαπλάσιο τοῦ $a_1 a_2$. Ὁ a_3 , τώρα, εἶναι πρῶτος πρὸς τὸν $a_1 a_2$, 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 $b = a_1 a_2$, οἱ ὁποῖοι εἶναι πρῶτοι μεταξὺ τους καὶ καθένας διαιρεῖ τὸν m , ἄρα καὶ τὸ γινόμενό τους $ab = a_1 a_2 a_3$ διαιρεῖ τὸν m . Ἐπαναλαμβάνοντας τοὺς ἀνάλογους συλλογισμούς, ὀδηγοῦμαστε ἐπαγωγικὰ στὸ συμπέρασμα ὅτι ὁ m εἶναι πολλαπλάσιο τοῦ $a_1 a_2 \cdots a_n$. **ὁ.ξ.δ.**

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

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

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

1.4 Πρῶτοι ἀριθμοί

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

Ὁρισμὸς 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) ἂν, καὶ μόνο ἂν, ὁ $-n$ εἶναι πρῶτος (ἀντιστοίχως, σύνθετος).

Γιὰ παράδειγμα, 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 ἓνα, τουλάχιστον, πρῶτο διαιρέτη.*

β'. Ἄν ὁ p εἶναι πρῶτος καὶ ὁ a εἶναι τυχὸν ἀκέραιος, τότε, ἓνα 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.

γ'. Ἄν ὁ p εἶναι πρῶτος καὶ $(a_i, p) = 1$ γιὰ ὅλα τὰ $i = 1, \dots, n$, τότε ὁ p δὲν διαιρεῖ τὸ γινόμενο $a_1 \cdots a_n$.

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

Ἰσοδύναμη (λόγω τοῦ β') διατύπωση: Ἄν ὁ p εἶναι πρῶτος καὶ δὲν διαιρεῖ κανέναν ἀπὸ τοὺς a_1, \dots, a_n , τότε οὔτε τὸ γινόμενό τους διαιρεῖ.

Στὴν εἰδικὴν περίπτωση τῆς δύναμης: Ἄν ὁ p δὲν διαιρεῖ τὸν a , τότε, οὔτε καὶ τὸν a^n διαιρεῖ.

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

Εἰδικὴ περίπτωση τῆς δύναμης: Ἄν $p|a^n$, 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 ἓνα, τουλάχιστον, ἀπὸ τοὺς a_1, \dots, a_n .

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

ε'. Ἄν P εἶναι ἓνα 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 $m \neq 0, \pm 1$ ἄς συμβολίσουμε 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 τοῦ τὸν $|m|$.

α'. Ἐστω p τὸ ἐλάχιστο στοιχεῖο τοῦ $\Delta(m)$. Θὰ ἀποδείξουμε ὅτι ὁ p εἶναι πρῶτος. Ἄν δὲν ἦταν, θὰ ἦταν σύνθετος (παρατηρήστε ὅτι $p > 1$), ἄρα, ἐκτὸς ἀπὸ τοὺς τετριμμένους διαιρέτες τοῦ θ εἶχε καὶ κάποιον ἄλλο διαιρέτη $d > 1$. Ὅποτε θὰ εἶχαμε τὴν ἐξῆς 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 εἶχαμε ὑποθέσει ἐλάχιστο στοιχεῖο τοῦ συνόλου· ἄτοπο.

β'. Ἄς ὑποθέσουμε ὅτι ὁ p εἶναι πρῶτος καὶ δὲν ἰσχύει $(a, p) = 1$. Θὰ δείξουμε, 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 ὀρισμοῦ 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 ἄς τὸν ὑποθέσουμε, δίχως βλάβη τῆς γενικότητος θετικό, καὶ ἄς τὸν γράψουμε $p = ab$, ὅπου $1 < a, b < p$. Τότε, γι' αὐτὸν τὸν συγκεκριμένο ἀκέραιο a , καὶ οἱ δύο σχέσεις $p|a$ καὶ $(p, a) = 1$ εἶναι ψευδεῖς.

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

³Πρόκειται γιὰ τὴν πρόταση 20 τοῦ Βιβλίου Θ' τῶν Στοιχείων τοῦ Εὐκλείδου: «Οἱ πρώτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν».

$b_1 = p$.

Όσον αφορά τὸ ὅτι ἡ τελευταία διατύπωση δὲν ἰσχύει ὅταν ὁ p εἶναι σύνθετος: Στὴν περίπτωση αὐτή, μποροῦμε νὰ γράψουμε (ὑποθέτοντας, χωρὶς βλάβη τῆς γενικότητος, τὸν p θετικό) $p = a_1 a_2$, ὅπου $1 < a_1, a_2 < p$. Τότε, βεβαίως, $p|a_1 a_2$, 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 ἀριθμὸς, ἐνῶ ἡ ὑπόθεση ὅτι ὁ m εἶναι σύνθετος συνεπάγεται ὅτι $p < |m|$. Παρατηρήστε ὅτι ὁ $\frac{|m|}{p}$ εἶναι ἀκέραιος ἀριθμὸς μεγαλύτερος τοῦ 1, ἀρα, ἀπὸ τὸ (α') ἔχει ἓνα πρῶτο διαιρέτη q , τὸν ὁποῖο, χωρὶς βλάβη τῆς γενικότητος, μποροῦμε νὰ ὑποθέσουμε 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, πὺ διαιρεῖ τὸν m μᾶς ὀδηγεῖ στὸ συμπέρασμα ὅτι $p \leq q$, ἀρα $p \leq \frac{|m|}{p}$, σχέση ἰσοδύναμη μὲ τὴν ἀποδεικτέα.

ε'. Ὁ ἰσχυρισμὸς εἶναι προφανῆς ἂν τὸ P εἶναι κενό. Ἔστω τώρα ὅτι $P = \{p_1, \dots, p_k\}$. Θεωροῦμε τὸν $m \stackrel{\text{ορσ}}{=} p_1 \cdots p_k + 1$, ὁ ὁποῖος, προφανῶς εἶναι ἀκέραιος μεγαλύτερος τοῦ 1, ἀρα, ἀπὸ τὸ (α') ἔχει ἓνα, τουλάχιστον, πρῶτο διαιρέτη q . Θὰ δείξομε ὅτι $q \notin P$. Πράγματι, γιατί διαφορετικά, ὁ q θὰ ἦταν ἴσος μὲ κάποιον $p_i \in \{p_1, \dots, p_k\}$, ὁπότε $q|(p_1 \cdots p_i \cdots p_k)$. Ὅμως $q|m$, ἀρα (πρόταση 1.1.1) $d|m - (p_1 \cdots p_k) = 1$, ἄτοπο.

ὁ.ξ.δ.

Τὸ κόσκινο τοῦ Ἐρατοσθένους. Ἐφαρμόζεται γιὰ τὴν κατασκευὴ τῆς λίστας ὄλων τῶν (θετικῶν) πρῶτων ἀριθμῶν, πὺ δὲν ὑπερβαίνουν δοθέντα ἀκέραιο $n > 2$. Συνίσταται στὴν ἐξῆς διαδικασία, ἡ ὁποία διαγράφει τοὺς σύνθετους ἀριθμοὺς, 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, πὺ 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, πὺ 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 ἐπόμενος μὴ διαγεγραμμένος ἀκέραιος, τοῦ ὁποῖου 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 διαγραφή τῶν πολλαπλασίων τοῦ 17, γιὰ παράδειγμα; Ὅχι! Τὸ δ' τοῦ θεωρήματος 1.4.2 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, πὺ δὲν ὑπερβαίνει τὸ 50 ἔχει, σύμφωνα μὲ τὴν πρόταση, ἓνα πρῶτο διαιρέτη $\leq \sqrt{50} = 7.071 \dots$. Ἔτσι, στὴ συγκεκριμένη περίπτωση $n = 50$,

μετά πού θά διαγράψομε καί τὰ πολλαπλάσια τοῦ 7, ἔχομε τήν ἐξῆς 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 μέ ὅ,τι εἶπαμε παραπάνω, ὅτι ὅλοι οἱ διαγεγραμμένοι ἀριθμοί εἶναι σύνθετοι καί ὅλοι οἱ ὑπόλοιποι εἶναι πρώτοι.

Θεώρημα 1.4.3 –Θεμελιῶδες θεώρημα τῆς Ἀριθμητικῆς. *Κάθε ἀκέραιος $n > 1$ ἀναλύεται σέ γινόμενο θετικῶν πρώτων: $n = p_1 \cdots p_k$. Ἡ ἀνάλυση αὐτή εἶναι μοναδική, ὑπό τήν ἐξῆς ἔννοια: Ἐάν $n = q_1 \cdots q_\ell$ καί οἱ q_1, \dots, q_ℓ εἶναι θετικοί πρώτοι, τότε $k = \ell$ καί οἱ q_1, \dots, q_ℓ ἀποτελοῦν, ἀπλῶς, μία μετάθεση τῶν p_1, \dots, p_k .*

Ἀπόδειξη Πρῶτα ἀποδεικνύομε ὅτι ὁ n ἀναλύεται σέ γινόμενο πρώτων, χωρίς νά μᾶς ἀπασχολεῖ ἡ μοναδικότητα τῆς ἀνάλυσης.

Λόγω τοῦ α' τοῦ θεωρήματος 1.4.2 ὁ n ἔχει ἓνα πρῶτο θετικό διαιρέτη p_1 καί θέτομε $n = p_1 n_1$. Ἐάν $n_1 = 1$, τότε $n = p_1$ καί ἔχομε ἀνάλυση τοῦ n σέ ἓνα πρῶτο διαιρέτη. Διαφορετικά, $1 < n_1 < n$ καί ὁ n_1 ἔχει ἓνα πρῶτο διαιρέτη p_2 , ὁπότε θέτομε $n_1 = p_2 n_2$, ἄρα $n = p_1 p_2 n_2$. Ἐάν $n_2 = 1$, τότε $n = p_1 p_2$ καί ἔχομε ἀνάλυση τοῦ n σέ δύο πρώτους διαιρέτες. Διαφορετικά, $1 < n_2 < n_1 < n$ καί ὁ n_2 ἔχει ἓνα πρῶτο διαιρέτη p_3 , ὁπότε θέτομε $n_2 = p_3 n_3$, ἄρα $n = p_1 p_2 p_3 n_3$. Ἐτσι προχωροῦμε, καί στό βῆμα i ἔχομε $n = p_1 p_2 \cdots p_i n_i$, ὅπου $n > n_1 > n_2 > \cdots > n_i > 0$. Ἐπειδή, δὲν μπορεῖ νά ἔχομε ἀπειρη κάθοδο, ὁπότε σέ κάποιο βῆμα $i = k$ θά καταλήξομε σέ $n_k = 1$, δηλαδή, $n = p_1 \cdots p_k$.

Τώρα ἀποδεικνύομε τή μοναδικότητα τῆς ἀνάλυσης σέ πρώτους διαιρέτες. Ἐστω $n = q_1 \cdots q_\ell$ καί οἱ q_1, \dots, q_ℓ εἶναι θετικοί πρώτοι. Χωρίς βλάβη τῆς γενικότητας ὑποθέτομε ὅτι $\ell \geq k$. Ἐχομε $q_1 | p_1 \cdots p_k$, ἄρα, ἀπό τὸ ζ' τοῦ θεωρήματος 1.4.2, ὁ q_1 διαιρεῖ ἓνα, τουλάχιστον, ἀπὸ τοὺς p_1, \dots, p_k , ἔστω, χωρίς βλάβη τῆς γενικότητος, τὸν p_1 . Ἀλλά, καθὼς ὁ p_1 εἶναι πρῶτος, ὁ ὁ μόνος διαιρέτης του, πού ὑπερβαίνει τὸ 1, εἶναι ὁ ἑαυτός του, ἄρα $q_1 = p_1$. Τώρα, διαιρώντας τὴ σχέση $p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_\ell$ διὰ $p_1 = q_1$ καταλήγομε στήν $p_2 \cdots p_k = q_2 \cdots q_\ell$. Συλλογιζόμαστε ἀκριβῶς ὅπως πρὶν: Ὁ q_2 διαιρεῖ τὸ γινόμενο $p_2 \cdots p_k$, ἄρα διαιρεῖ ἓνα, τουλάχιστον, παράγοντα, ὁπότε συμπίπτει μέ ἓναν ἀπὸ τοὺς p_2, \dots, p_k . Χωρίς βλάβη τῆς γενικότητος, ἔστω $q_2 = p_2$ κ. ὅ. κ. Ἐάν ἦταν $\ell > k$, τότε, ὕστερα ἀπὸ k τὸ πλήθος βήματα θά καταλήγαμε σέ σχέση τῆς μορφῆς $1 = q_{k+1} \cdots q_\ell$, ἄτοπο. Ἐπειδή, $\ell = k$ καί $q_1 = p_1, q_2 = p_2, \dots, q_k = p_k$. **Ὡ.ξ.δ.**

Γιὰ κάθε ἀκέραιο $n \neq 0, \pm 1$ ὑπάρχει μία βολική, σέ πολλές περιπτώσεις, ἀνάλυσή του, πού λέγεται *κανονικὴ ἀνάλυση* τοῦ n , ἡ ὁποία εἶναι ἡ ἐξῆς: Τὸ θεώρημα 1.4.3 μᾶς ἐξασφαλίζει ὅτι $n = \pm p_1 p_2 \cdots p_k$, ὅπου οἱ p_1, \dots, p_k εἶναι θετικοί πρώτοι, ὄχι, κατ' ἀνάγκη, διαφορετικοί. Ὅποτε ὁμαδοποιώντας ἴσους πρώτους, γράφομε $n = \pm q_1^{a_1} \cdots q_m^{a_m}$, ὅπου τώρα: (α') Οἱ πρώτοι q_1, \dots, q_m εἶναι διαφορετικοί μεταξὺ τους. (β') $m \leq k$ καί $a_i \geq 1$ γιὰ κάθε $i = 1, \dots, m$.

Παρατηρούμε ότι, αν $n = \pm q_1^{a_1} \cdots q_m^{a_m}$ είναι η κανονική ανάλυση του n , τότε $q_1^{a_1}$ είναι η μέγιστη δύναμη του q_1 , που διαιρεί τον n διότι, αν $q_1^b | n$, τότε $n = q_1^b c$, για κάποιον άκεραίο c , οπότε $\pm q_1^{a_1} q_2^{a_2} \cdots q_m^{a_m} = q_1^b c$. Αν, λοιπόν, ήταν $b > a_1$, τότε, άπλοποιώντας τα δύο μέλη διὰ $q_1^{a_1}$, θα 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, πὺν μᾶς λέει ὅτι ἡ ἀνάλυση ἑνὸς ἀριθμοῦ σὲ πρῶτους παράγοντες εἶναι μοναδική.

Ἔχοντας αὐτὴ τὴν παρατήρηση κατὰ νοῦ, ὀρίζομε, γιὰ κάθε ἀκεραίο n καὶ κάθε πρῶτο p , τὸν ἐκθέτη τοῦ p στὸν n , συμβολιζόμενο $v_p(n)$, ὡς ἐξῆς: $v_p(n) = 0$ ἂν $n = 0$ καὶ $v_p(n) = a$ (≥ 0) ἂν p^a εἶναι ἡ μέγιστη δύναμη τοῦ p , πὺν διαιρεῖ τὸν n . Γιὰ παράδειγμα, $v_2(1200) = 4$, $v_3(1200) = 1$, $v_5(1200) = 2$, $v_7(1200) = 0$. Εἶναι ἀπλὸ νὰ ἀποδείξει κανεὶς τὶς ἐξῆς ιδιότητες τοῦ ἐκθέτη:

- $v_p(ab) = v_p(a) + v_p(b)$.
- $v_p(a \pm b) \geq \min(v_p(a), v_p(b))$. Ἐν $v_p(a) \neq v_p(b)$, τότε ἰσχύει τὸ =.

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 γραφεῖ, πιὸ ὁμοιόμορφα, ὡς ἐξῆς:

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

ὅπου, βέβαια, τὸ γινόμενο στὸ δεξιὸ μέλος ἔχει ἄπειρους παράγοντες, ἀλλὰ δὲν ἔχει ἄπειρη τιμὴ, ἀφοῦ μόνον 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: Ἐν $\rho \in \mathbb{Q}$, γράφομε τὸν ρ ὡς πηλίκον ἀκεραίων $\rho = a/b$ καὶ ὀρίζομε $v_p(\rho) = v_p(a) - v_p(b)$. Ὁ ὀρισμὸς αὐτὸς εἶναι ἀνεξάρτητος ἀπὸ τὸν τρόπο, πὺν θὰ γράφομε τὸν ρ ὡς πηλίκον ἀκεραίων· βλ. ἄσκηση 30. Τώρα μποροῦμε νὰ ἐπεκτεῖνομε τὴν γενικευμένη κανονικὴ ἀνάλυση καὶ στοὺς ρητούς: Ὀρίζεται ἀπὸ τὴν (1.1), ὅπου τὸ n τώρα μπορεῖ νὰ παριστάνει καὶ ρητό.

Ἡ χρῆση τῶν ἐκθετῶν καὶ τῆς γενικευμένης κανονικῆς ἀνάλυσης εἶναι, σὲ πολλὰς περιπτώσεις, πολὺ βοηθητικὴ.

Θεώρημα 1.4.4 *α'. Ἐστω ὅτι a, b εἶναι ἀκεραίοι καὶ $b \neq 0$. Τότε, ὁ b διαιρεῖ τὸν a ἂν, καὶ μόνον ἂν, $v_p(b) \leq v_p(a)$ γιὰ κάθε (θετικὸ) πρῶτο p .*

β'. Ἐν $a = \pm p_1^{s_1} \cdots p_m^{s_m}$ 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 $i = 1, \dots, m$. Κατὰ συνέπεια, τὸ πλῆθος τῶν θετικῶν διαιρετῶν τοῦ a εἶναι $(s_1 + 1) \cdots (s_m + 1)$.

Άπόδειξη *α'*. Έστω ότι $b|a$. Τότε $a = bc$, άρα, για κάθε πρώτο p , έχουμε $v_p(a) = v_p(bc) = v_p(b) + v_p(c) \geq v_p(b)$. Αντιστρόφως, έστω ότι, για κάθε πρώτο p είναι $v_p(a) \geq v_p(b)$. Αν $b = \pm 1$, τότε $b|a$. Διαφορετικά, έστω $b = p_1^{r_1} \cdots p_m^{r_m}$ ή κανονική ανάλυση του b . Από την υπόθεση, $v_{p_i}(a) \geq r_i$ για κάθε $i = 1, \dots, m$. Αυτό σημαίνει ότι, αν κάνουμε την κανονική ανάλυση του a , αυτή θα έχει τη μορφή

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

όπου $c = 1$ ή γινόμενο δυνάμεων κάποιων πρώτων διαφορετικών από τους p_1, \dots, p_m : ούτως ή άλλως, όμως, ό c είναι άκεραιος. Συνεπώς, παραβάλλοντας με την κανονική ανάλυση του b (βλ. λίγο παραπάνω), καταλήγουμε στη σχέση

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

Τò εντός της παρενθέσεως γινόμενο είναι άκεραιος άριθμός, άρα $b|a$.

β'. Ο ίσχυρισμός σχετικά με τη μορφή των διαιρετών του a προκύπτει άμέσως από τò μέρος *α'* του θεωρήματος. Όσον άφορά στο πλήθος των θετικών διαιρετών του a , παρατηρούμε τὰ έξής: Για τόν εκθέτη t_1 υπάρχουν $s_1 + 1$ έπιλογές (άφου $0 \leq t_1 \leq s_1$), για τόν t_2 υπάρχουν $s_2 + 1$ έπιλογές, ..., για τόν t_m υπάρχουν $s_m + 1$ έπιλογές, άρα για τόν $p_1^{t_1} \cdots p_m^{t_m}$ υπάρχουν $(s_1 + 1)(s_2 + 1) \cdots (s_m + 1)$ έπιλογές και όλες είναι διαφορετικές μεταξύ τους, λόγω της μοναδικότητας της ανάλυσης σε πρώτους παράγοντες. **ό.ξ.δ.**

Κάποιες ένδιαφέρουσες εφαρμογές των εκθετών και της γενικευμένης κανονικής ανάλυσης δίδονται π.χ. στις άσκήσεις 31 και 32

1.5 Πυθαγόρειες τριάδες

Η μοναδικότητα της ανάλυσης ενός άκεραίου σε πρώτους παράγοντες (θεώρημα 1.4.3) έχει σημαντικές εφαρμογές στην επίλυση διοφαντικών έξισώσεων. Έδω θα δώσουμε, ως παράδειγμα, την επίλυση της έξίσωσης $x^2 + y^2 = z^2$ σε μη μηδενικούς άκεραίους x, y, z . Κάθε τέτοια λύση (x, y, z) λέγεται *πυθαγόρεια τριάδα*. Μία θεμελιώδης βοηθητική πρόταση, χρήσιμη και σε πολλές άλλες περιπτώσεις, είναι ή έξής.

Πρόταση 1.5.1 Αν a, b, c είναι θετικοί άκεραίοι, τέτοιοι ώστε $(a, b) = 1$ και $ab = c^n$, όπου $n \geq 2$, τότε υπάρχουν άκεραίοι c_1, c_2 τέτοιοι ώστε $a = c_1^n$, $b = c_2^n$ και $c_1 c_2 = c$.

Άπόδειξη Αν $a = 1$ ή $b = 1$, τò άποδεικτέο είναι φανερό. Διαφορετικά, θεωρούμε τις κανονικές αναλύσεις των a και b . Συμβολίζουμε με p_1, \dots, p_k όλους τούς (θετικούς) πρώτους στην κανονική ανάλυση του a και με q_1, \dots, q_ℓ όλους τούς (θετικούς) πρώτους στην κανονική ανάλυση του b . Η υπόθεση $(a, b) = 1$ προφανώς συνεπάγεται ότι, καθένας από τούς p_i είναι διαφορετικός από καθέναν από τούς q_j . Επίσης, λόγω της σχέσεως $ab = c^n$ και της μοναδικότητας της ανάλυσης σε πρώτους παράγοντες, οί πρώτοι στην κανονική ανάλυση του c είναι

οί $p_1, \dots, p_k, q_1, \dots, q_\ell$ και μόνον αυτοί. Άρα, η κανονική ανάλυση του c έχει τη μορφή $c = p_1^{r_1} \cdots p_k^{r_k} q_1^{s_1} \cdots q_\ell^{s_\ell}$, οπότε,

$$ab = c^n = p_1^{nr_1} \cdots p_k^{nr_k} q_1^{ns_1} \cdots q_\ell^{ns_\ell}. \quad (1.2)$$

Άλλά, στην κανονική ανάλυση του a μόνο οι πρώτοι p_i εμφανίζονται και κανένας πρώτος q_j , ενώ για την κανονική ανάλυση του b μόνο οι πρώτοι q_j εμφανίζονται και κανένας πρώτος p_i . Αυτό, αναγκαστικά, συνεπάγεται ότι

$$a = p_1^{nr_1} \cdots p_k^{nr_k} = (p_1^{r_1} \cdots p_k^{r_k})^n = c_1^n \quad \text{και} \quad b = q_1^{ns_1} \cdots q_\ell^{ns_\ell} = (q_1^{s_1} \cdots q_\ell^{s_\ell})^n = c_2^n$$

καί, λόγω της (1.2), $c_1 c_2 = c$. **ὀ.ξ.δ.**

Ἐστω τώρα ὅτι (x, y, z) εἶναι μία πυθαγόρεια τριάδα. Θέτομε $(x, y) = d$, $x = dX$, $y = dY$ και ξέρομε ἀπὸ τὸ δ' τοῦ θεωρήματος 1.2.2 ὅτι $(X, Y) = 1$. Ἀπὸ τὴν σχέση $x^2 + y^2 = z^2$ παίρνομε, συνεπῶς, $X^2 + Y^2 = (z/d)^2$. Τὸ ἀριστερὸ μέλος τῆς τελευταίας εἶναι ἀκέραιος ἀριθμὸς, ἄρα και τὸ δεξιό. Τότε, ὅμως, ἡ ἄσκηση 11 μᾶς λέει ὅτι ὁ z/d εἶναι ἀκέραιος, τὸν ὁποῖο συμβολίζομε Z . Ὅποτε, τελικά,

$$x = dX, \quad y = dY, \quad z = dZ, \quad (X, Y) = 1, \quad X^2 + Y^2 = Z^2 \quad (1.3)$$

Τώρα κάνομε μία σειρά ἀπὸ μικρὲς παρατηρήσεις. Λεπτομέρειες τῶν ἀποδείξεων τους ἀφήνομε ὡς ἀσκήσεις:

- $(X, Z) = 1$ και $(Y, Z) = 1$.
- Οἱ X, Y δὲν μπορεῖ νὰ εἶναι και οἱ δύο περιττοί. Πράγματι, γιατί τότε, ὁ ἀκέραιος $X^2 + Y^2$ θὰ ἦταν τῆς μορφῆς $4k + 2$, δηλαδή, ἄρτιος, ἀλλὰ ὄχι διαιρετὸς διὰ 4, ὅποτε δὲν μπορεῖ νὰ ἰσοῦται μὲ τετράγωνο.
Χωρὶς βλάβη τῆς γενικότητας, λοιπόν, ὑποθέτομε, στὸ ἐξῆς, τὸν X περιττὸ και τὸν Y ἄρτιο. Προφανῶς, ὁ Z εἶναι περιττός. Ἐπίσης, λόγω τοῦ ὅτι στὴν ἐξίσωσή μας εμφανίζονται μόνο τὰ τετράγωνα τῶν X, Y, Z , μποροῦμε νὰ ὑποθέσομε τοὺς X, Y, Z θετικὸς ἀκεραῖους.
- Γράφομε τὴν (1.3) ὡς $(Z - Y)(Z + Y) = X^2$. Ἀπὸ τὶς προηγούμενες παρατηρήσεις εἶναι εὐκόλο νὰ διαπιστώσει κανεὶς ὅτι οἱ $Z + Y, Z - Y$ εἶναι περιττοί και $(Z - Y, Z + Y) = 1$.
- Μὲ ἐφαρμογὴ τῆς πρότασης 1.5.1 στὴν σχέση $(Z - Y)(Z + Y) = X^2$ (παρατηρήστε ὅτι οἱ $X, Z + Y, Z - Y$ εἶναι θετικοί) συμπεραίνομε ὅτι $Z + Y = a^2$, $Z - Y = b^2$ και $X = ab$, ὅπου οἱ a, b εἶναι περιττοί και $(a, b) = 1$.
- Λύνοντας ὡς πρὸς Z, Y βρίσκομε $Z = (a^2 + b^2)/2$ και $Y = (a^2 - b^2)/2$. Γιὰ νὰ ἀποφύγομε τὸν παρονομαστή 2, θέτομε $a = A + B$ και $b = A - B$, ὅπου οἱ A, B εἶναι ἑτερότυποι, δηλαδή, ὁ ἓνας ἄρτιος και ὁ ἄλλος περιττός (δὲν καθορίζεται ποὺς ὁ ἄρτιος και ποὺς ὁ περιττός). Εὐκόλα διαπιστώνεται

ὅτι $(A, B) = 1$. Ὄποτε, 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, λόγω τῶν $x = dX, y = dY, z = dZ$ καταλήγομε στοὺς πιὸ γενικοὺς τύπους τῶν πυθαγορείων τριάδων, δίνοντας στὸν d ὅποιεσδήποτε 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, λόγω τοῦ συμμετρικοῦ ρόλου αὐτῶν τῶν μεταβλητῶν στὴν ἐξίσωσή μας.

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

1.6 Άσκησης τοῦ κεφαλαίου 1

«Ἀριθμὸς» σημαίνει πάντα «ἀκέραιος ἀριθμὸς»

1. Ἄν ὁ d εἶναι κοινὸς διαιρέτης τῶν $ax + by$ καὶ $a'x + b'y$ καὶ $(d, ab' - a'b) = 1$, ἀποδείξτε ὅτι ὁ d εἶναι κοινὸς διαιρέτης τῶν x, y .
2. Ἀποδείξτε τοὺς ἐξῆς ἰσχυρισμοὺς:
ἄρτιος + ἄρτιος = ἄρτιος, ἄρτιος + περιττός = περιττός,
περιττός + περιττός = ἄρτιος.
3. Ἐστω $n \geq 1$. Ἀποδείξτε τὴν ἐξῆς ἰσότητα συνόλων:

$$\{d : 1 \leq d \leq n \text{ καὶ } d|n\} = \left\{ \frac{n}{d} : 1 \leq d \leq n \text{ καὶ } d|n \right\}$$

4. Ἀποδείξτε ὅτι, τὸ τετράγωνο ὁποιοῦδήποτε περιττοῦ ἀριθμοῦ, διαιρούμενο διὰ 8 δίνει ὑπόλοιπο 1· ἄρα διαιρούμενο καὶ διὰ 4 δίνει ὑπόλοιπο 1.
5. Ἀποδείξτε ὅτι, τὸ τετράγωνο ἑνὸς ἀριθμοῦ, ὁ ὁποῖος δὲν εἶναι πολλαπλάσιο τοῦ 3, διαιρούμενο διὰ 3 δίνει ὑπόλοιπο 1.

6. Αποδείξτε ότι, ο κύβος ενός αριθμού μη διαιρετού διὰ 7, όταν διαιρεθεί διὰ 7 δίνει υπόλοιπο 1 ή 6.
7. Αποδείξτε ότι, μεταξύ δύο διαδοχικών αριθμών, ό ένας είναι άρτιος. Επίσης, μεταξύ τριών διαδοχικών αριθμών ό ένας διαιρείται διὰ 3. Δείξτε ότι, για κάθε n , ό $n(n+1)(2n+1)$ είναι πολλαπλάσιο του 6.
8. (α') Άν ό ένας εκ των a, b είναι άρτιος και ό άλλος περιττός και $(a, b) = 1$, τότε και $(a+b, a-b) = 1$.
 (β') Άν οί a, b είναι περιττοί, αποδείξτε ότι οί $(a+b)/2$ και $(a-b)/2$ είναι, και οί δύο, άκέραιοι, ό ένας (όχι, κατ' ανάγκην ό πρώτος) άρτιος και ό άλλος περιττός. Άν, έπιπλέον, υποθέσουμε ότι $(a, b) = 1$, αποδείξτε ότι $(\frac{a+b}{2}, \frac{a-b}{2}) = 1$.
9. Έστω ότι οί a, b είναι θετικοί άκέραιοι, όχι και οί δύο άρτιοι. Ορίζουμε $a_1 = a, b_1 = b$ και για $k = 2, 3, \dots$, αναδρομικά,
 Άν ό a_{k-1} είναι άρτιος: $a_k = a_{k-1}/2, b_k = b_{k-1}$.
 Άν ό b_{k-1} είναι άρτιος: $a_k = a_{k-1}, b_k = b_{k-1}/2$.
 Άν οί a_{k-1} και b_{k-1} είναι περιττοί: $a_k = \min(a_{k-1}, b_{k-1}), b_k = |a_{k-1} - b_{k-1}|/2$.
- Αποδείξτε τὰ έξής: (α') Για κάθε $k = 1, 2, 3, \dots$, οί a_k, b_k είναι μη άρνητικοί άκέραιοι και ό ένας, τουλάχιστον, είναι περιττός.
 (β') Άν για κάποιο $k \geq 2$ είναι $a_{k-1}b_{k-1} \neq 0$, τότε $a_k + b_k < a_{k-1} + b_{k-1}$.
 (γ') Για κάθε $k \geq 2$, $(a_k, b_k) = (a_{k-1}, b_{k-1})$.
 (δ') Υπάρχει $n \geq 2$, τέτοιος ώστε $a_n b_n = 0$ και ό μη μηδενικός εκ των a_n, b_n είναι ό μέγιστος κοινός διαιρέτης των a, b .
- Υπολογίστε με την παραπάνω διαδικασία τον μέγιστο κοινό διαιρέτη των 1001 και 4151.
10. Έστω $\frac{a}{b} = \frac{m}{n}$, όπου τὸ κλάσμα στο δεξιό μέλος είναι ανάγωγο, δηλαδή, $(m, n) = 1$. Αποδείξτε ότι υπάρχει $k \in \mathbb{Z}$, τέτοιο ώστε $a = km$ και $b = kn$. Βασισμένοι σέ αυτό αποδείξτε ότι, αν $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, τότε υπάρχουν $k, \ell \in \mathbb{Z}$, τέτοιο ώστε $ka_1 = \ell a_2$ και $kb_1 = \ell b_2$.
11. Αποδείξτε ότι, αν $n \geq 2$ και ή n -οστή δύναμη ενός ρητού είναι άκέραιος αριθμός, τότε ό ρητός είναι, αναγκαστικά, άκέραιος. Ίσοδύναμη διατύπωση: Άν ή n -οστή ρίζα ενός άκεραίου είναι ρητός αριθμός, τότε ό ρητός αυτός αριθμός είναι άκέραιος. Μ' άλλα λόγια, ή n -οστή ρίζα άκεραίου είναι ή άρρητος αριθμός ή άκέραιος.
12. (Γενίκευση τής προηγούμενης) Έστω πολυώνυμο $a_n x^n + \dots + a_1 x + a_0$ με άκέραιους συντελεστές, όπου $n \geq 2$ και $a_n \neq 0$. Υποθέτομε ότι τὸ πολυώνυμο αυτό έχει κάποια ρητή ρίζα, την όποία γράφομε ως ανάγωγο κλάσμα $\frac{k}{\ell}$ ($(k, \ell) = 1$). Αποδείξτε ότι $\ell | a_n$ και $k | a_0$. Παρατηρήστε ότι αυτό, ειδικότερα, συνεπάγεται ότι, αν $a_n = 1$, τότε, αν τὸ πολυώνυμο έχει ρητή ρίζα, αυτή είναι, υποχρεωτικά, άκέραια.

Ἡ ἄσκηση αὐτὴ δίνει μία μέθοδο ἀνίχνευσης ὄλων τῶν ρητῶν ριζῶν ἑνὸς πολυωνύμου μὲ ἀκέραιους συντελεστές, ἂν ὑπάρχουν τέτοιες.

13. Δίδονται οἱ ἀκέραιοι a_1, \dots, a_{n-1}, a_n , $n \geq 3$ καὶ ὀρίζομε 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 κοινούς διαιρέτες τῶν a_1, \dots, a_k , ὁπότε, εἰδικώτερα, $d_k = (a_1, \dots, a_k)$.
14. Ἐστω $d = (a_1, a_2, \dots, a_n)$ ($n \geq 2$). Δεῖξτε ἐπαγωγικὰ τὰ ἐξῆς:
 (1) Κάθε κοινὸς διαιρέτης τῶν a_1, a_2, \dots, a_n διαιρεῖ τὸν d .
 (2) Ὑπάρχουν ἀκέραιοι x_1, x_2, \dots, x_n , τέτοιοι ὥστε $d = a_1x_1 + a_2x_2 + \dots + a_nx_n$.
15. Στὴν ἀπόδειξη τοῦ δ' τοῦ θεωρήματος 1.2.2, ποῦ ἔπαιξε ρόλο τὸ ὅτι ὁ c εἶναι κοινὸς διαιρέτης τῶν a, b ;
16. Ἡ ἄσκηση αὐτὴ προτείνει ἕναν εὐχρηστο ἀλγόριθμο γιὰ νὰ ὑπολογίσει κανεῖς, 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 εὐκλείδειου 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 $q_2, q_3, \dots, r_2, r_3, \dots$, ὅπως αὐτοὶ ὀρίζονται στὸ θεώρημα 1.2.3 (βλ. καὶ τὶς διαδοχικὲς σχέσεις στὴν ἀπόδειξη τοῦ πρώτου μέρους αὐτοῦ τοῦ θεωρήματος). Ὅρίζομε:

$$P_1 = q_2, \quad P_2 = q_2q_3 + 1, \quad P_k = q_{k+1}P_{k-1} + P_{k-2} \quad \text{γιὰ } k = 3, \dots, n$$

$$Q_1 = 1, \quad Q_2 = q_3, \quad Q_k = q_{k+1}Q_{k-1} + Q_{k-2} \quad \text{γιὰ } k = 3, \dots, n$$

(α') Ἀποδείξτε ὅτι $\begin{vmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{vmatrix} = (-1)^{k-1}$ γιὰ κάθε $k = 2, \dots, n$. Αὐτό, εἰδικώτερα, συνεπάγεται ὅτι $(P_k, Q_k) = 1$ γιὰ κάθε $k = 1, \dots, n$.

(β') Ἀποδείξτε ὅτι, γιὰ κάθε $k = 1, \dots, n-1$ 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 $a = r_n P_n$ καὶ $b = r_n Q_n$. Ἀπὸ τὸ θεώρημα 1.2.3 ξέρομε ὅτι $r_n = (a, b)$. Ὑποθέστε ὅτι ἀγνοεῖτε αὐτὸ τὸ γεγονός καὶ ἀποδείξτε, 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') ἀποδείξτε 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
$q_{k+1} =$						
$P_k =$						
$Q_k =$						
$r_{k+1} =$						

17. Ακολουθώντας τη μεθοδολογία του αριθμητικού παραδείγματος μετά το θεώρημα 1.2.3 υπολογίστε τον $d = (654321, 123456)$ και, κατόπιν, δύο άκεραίους x_0, y_0 , τέτοιους ώστε $654321x_0 + 123456y_0 = d$. Κατόπιν, ακολουθώντας τη μεθοδολογία της άσκησης 16, υπολογίστε νέα x_0, y_0 με την ίδια ιδιότητα. Το ότι βρίσκει κανείς διαφορετικές λύσεις (x_0, y_0) δεν είναι παράλογο· βλ. άσκηση 29
18. Έστω $n \geq 2$ και θεωρούμε όποιουσδήποτε n διαδοχικούς άκεραίους. Αποδείξτε ότι, αν διαιρέσουμε καθέναν από αυτούς δια n , τα υπόλοιπα, που θα πάρουμε είναι διαφορετικά μεταξύ τους. Από αυτό συμπεράνατε ότι ο ένας, ακριβώς, από τους n διαδοχικούς άκεραίους είναι διαιρετός δια n .
19. Αν $(a, b) = 1$ και $m, n \geq 1$, αποδείξτε ότι $(a^m, b^n) = 1$, με δύο τρόπους: Μία φορά χωρίς τη χρήση της ανάλυσης των a, b σε πρώτους παράγοντες και μία δεύτερη φορά, με χρήση αυτής.
20. (Γραφή άκεραίου σε b -αδικό σύστημα αριθμώσεως). Έστω άκεραίος $b > 1$. Για κάθε θετικό άκεραίο a ακολουθούμε την εξής διαδικασία. Έκτελούμε την εύκλειδεια διαίρεση του a δια b , έστω $a = ba_1 + d_0$, $0 \leq d_0 < b$. Αναδρομικά, για $k = 1, 2, \dots$ έκτελούμε την εύκλειδεια διαίρεση του a δια b , έστω $a_k = ba_{k+1} + d_k$, $0 \leq d_k < b$. Αποδείξτε ότι, για κάθε $k \geq 1$ ισχύει $a = \sum_{i=0}^{k-1} d_i b^i + a_k b^k$ και για κάποια τιμή $k = n \geq 1$, $a_n = 0$. Συμπεράνετε ότι κάθε θετικός άκεραίος a μπορεί να γραφεί με τη μορφή $d_0 + d_1 b + \dots + d_{n-1} b^{n-1}$, όπου $0 \leq d_k < b$ για κάθε $k = 0, \dots, n-1$ και $d_{n-1} > 0$. Λέμε τότε ότι γράψαμε (ή παραστήσαμε) τον a στο b -αδικό σύστημα ή στο σύστημα αρίθμησης με βάση b . Προφανώς, για $b = 10$ έχουμε τη γνωστή 10-δική παράσταση του a .
21. Έστω $a = bq + r$ με $a, b, r > 0$ (οί q, r μπορεί να παριστάνουν πηλίκο και υπόλοιπο, αντιστοίχως, της διαίρεσης του a δια b , αλλά αυτό δεν είναι απαραίτητο) και n όποιουσδήποτε. Αποδείξτε ότι υπάρχει s , τέτοιος ώστε, $n^a - 1 = (n^b - 1)s + n^r - 1$.⁴ Με τη βοήθεια αυτού αποδείξτε τα εξής:
1. $(n^a - 1, n^b - 1) = (n^b - 1, n^r - 1)$.
 2. $(n^a - 1, n^b - 1) = n^d - 1$, όπου $d = (a, b)$.
22. Υπολογίστε τους $(182, 422)$ και $(2311, 3701)$.
23. Γράψτε τον $(399, 703)$ ως γραμμικό συνδυασμό (με άκεραίους συντελεστές) των 399 και 703.
24. Υπολογίστε άκεραίες λύσεις κάθε μιās από τις εξισώσεις $547x + 632y = 1$, $398x + 600y = 2$ και $922x + 2163y = 7$, χρησιμοποιώντας κατάλληλα το θεώρημα 1.2.3.

⁴Χρησιμοποιείστε την ταυτότητα $x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \dots + x + 1)$.

25. Ὑπάρχουν ἀκέραιες λύσεις x, y τῆς ἐξίσωσης $1841x + 3647y = 1$; Δικαιολογήστε τὴν ἀπάντησή σας.
26. Δίδονται οἱ ἀκέραιοι a_1, \dots, a_{n-1}, a_n , $n \geq 3$ καὶ ὀρίζομε ἀναδρομικά: $m_2 = [a_1, a_2]$, $m_{k+1} = [m_k, a_{k+1}]$ γιὰ $2 \leq k \leq n-1$. Δεῖξτε μὲ ἐπαγωγή ἐπὶ τοῦ k ὅτι τὰ πολλαπλάσια τοῦ m_k ταυτίζονται μὲ τὰ κοινὰ πολλαπλάσια τῶν a_1, \dots, a_k , ὁπότε, εἰδικότερα, $m_k = [a_1, \dots, a_k]$.
27. Ἀποδείξτε ὅτι $(a, b) = (a + b, [a, b])$.
28. Νὰ ὑπολογισθοῦν δύο θετικοὶ ἀκέραιοι, τῶν ὁποίων τὸ ἄθροισμα εἶναι 64 980 καὶ τὸ ἐλάχιστο κοινὸ πολλαπλάσιό τους ἰσοῦται μὲ 58 639 842.
29. 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 ἐλληνιστικῶν χρόνων, ὁ ὁποῖος ἐμελέτησε συστηματικὰ τέτοιες ἐξισώσεις (ὄχι μόνον πρώτου βαθμοῦ).
- (α') Ἀποδείξτε ὅτι, ἂν ὁ (a, b) δὲν διαιρεῖ τὸν c , ἡ ἐξίσωση εἶναι ἀδύνατη.
- (β') Ἐστω $d = (a, b)$ καὶ $d|c$. Μὲ τὴ βοήθεια τῆς ἄσκησης 18 καὶ ὑποθέτωντας, χωρὶς βλάβη τῆς γενικότητος, ὅτι $b \geq 2$ (γιατὶ δὲν βλάπτεται ἡ γενικότης;), ἀποδείξτε 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 τῆς. 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 $y_1 = y_0 - k\frac{a}{d}$.
30. Ἐὰν $b_1 b_2 \neq 0$ καὶ $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, τότε, γιὰ κάθε πρῶτο p ἰσχύει $v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2)$.
Μπορεῖτε νὰ χρησιμοποιήσετε τὴν ἄσκηση 10.
31. Ἀποδείξτε 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 παρατηρήστε ὅτι ἀποδεικνύεται ἀμέσως ἡ σχέση $(a, b)[a, b] = ab$.

32. Ἐστω θετικὸς πρῶτος p καὶ θετικὸς ἀκέραιος $k < p$. Ἀποδείξτε ὅτι ὁ διωνυμικὸς συντελεστής $\binom{p}{k}$ εἶναι πολλαπλάσιο τοῦ p .

Υπόδειξη: Άρκει νά αποδείξετε ὅτι ὁ ἐκθέτης v_p τοῦ διωνυμικοῦ αὐτοῦ συντελεστή εἶναι θετικός. Χρησιμοποιήστε τὴν ταυτότητα $\binom{p}{k} = \frac{p}{k} \binom{p-1}{k-1}$ καὶ τὶς βασικὲς ιδιότητες τοῦ ἐκθέτη v_p .

33. Βρεῖτε, μὲ τὴ βοήθεια τῶν πυθαγορείων τριάδων, τύπους δύο ἀκεραίων παραμέτρων C καὶ D , πὸν νά δίνουν λύσεις τῆς διοφαντικῆς ἐξίσωσης $X^4 + Y^2 = Z^2$ μὲ X ἄρτιο (μία περίπτωση), καὶ X περιττό (δεύτερη περίπτωση).
34. Μιμηθεῖτε, μὲ μικρὲς τροποποιήσεις, τὴν ἀπόδειξη τοῦ Εὐκλείδη γιὰ τὴν ὑπαρξὴ ἀπείρων πρῶτων (πρόταση ε΄ τοῦ θεωρήματος 1.4.1) καὶ ἀποδείξτε ὅτι ὑπάρχουν ἀπειροὶ πρῶτοι τῆς μορφῆς $4k + 3$. Ἀνάλογα, ἀποδείξτε ὅτι ὑπάρχουν ἀπειροὶ πρῶτοι τῆς μορφῆς $6k + 5$.

Κεφάλαιο 2

Ίσοτιμίες

Στό κεφάλαιο αυτό, οί m, n είναι πάντοτε άκέραιοι μεγαλύτεροι τοϋ 1
Τα λατινικά γράμματα συμβολίζουν πάντα άκεραίους

2.1 Όρισμοί και βασικές ιδιότητες

Πρόταση - Όρισμός 2.1.1 *Έστω άκέραιος $m \geq 2$. Οί έξής συνθήκες είναι ισοδύναμες γιά τους άκεραίους a, b :*

1. $m|(b - a)$.
2. Υπάρχει άκέραιος k , τέτοιος ώστε $b = a + km$.
3. Το υπόλοιπο τής διαιρέσεως τοϋ a διά m είναι ίσο με το υπόλοιπο τής διαιρέσεως τοϋ b διά m .

Όταν μία από τις παραπάνω ισοδύναμες συνθήκες άληθεύει, τότε γράφομε

$$a \equiv b \pmod{m}$$

και διαβάζομε αυτή τή σχέση a ισότιμο b μέτρω m ή a ισότιμο b modulo m . Ό m λέγεται μέτρο τής ισοτιμίας $a \equiv b \pmod{m}$, οί δέ άριθμοί a, b χαρακτηρίζουται ισότιμοι μέτρω m .¹ Αυτή ή σχέση ισοτιμίας μέτρω m είναι σχέση ισοδυναμίας στο σύνολο τών άκεραίων άριθμών.

¹Εδώ είναι σαφές το πλεονέκτημα γλωσσικής οικονομίας, πού παρέχει ή χρήση τής δοτικής «μέτρω», δηλαδή, «ώς προς μέτρο». Η χρήση τοϋ λατινικού modulo είναι μάλλον κακόχη στα έλληνικά, και ή αντικατάστασή της από τή λέξη *μόδιο(ν)*, πού προτείνεται από κάποιους σύγχρονους έλληνες συγγραφείς (Ν.Μαρμαρίδης, Δ.Νταής) μοιάζει πολϋ έξεζητημένη, αν και είναι ακριβής από άποψη γλωσσικής άντιστοιχίας προς το modulo.

Άποδείξη (1) \Rightarrow (2): Η υπόθεση $m|(b - a)$ σημαίνει ότι υπάρχει k , τέτοιο ώστε $b - a = mk$, άρα $b = a + mk$.

(2) \Rightarrow (3): Έστω ότι $b = a + mk$. Αν q, r είναι, αντιστοίχως, τὸ πηλίκο καὶ τὸ υπόλοιπο τῆς διαίρεσης τοῦ a διὰ m , τότε $a = qm + r$ καὶ $0 \leq r < m$. Ὄποτε, $b = a + mk = (k + q)m + r$ καὶ ἡ σχέση ἀυτῆ, προφανῶς, λέει ὅτι, τὸ πηλίκο τῆς διαίρεσης τοῦ b διὰ m εἶναι $k + q$ καὶ τὸ υπόλοιπο (ποὺ αὐτὸ μᾶς ἐνδιαφέρει) εἶναι r . Δηλαδή, οἱ διαιρέσεις τῶν a διὰ m καὶ b διὰ m ἔχουν τὸ ἴδιο υπόλοιπο.

(3) \Rightarrow (1): Ἐξ ὑποθέσεως, οἱ διαιρέσεις τῶν a διὰ m καὶ b διὰ m ἔχουν τὸ ἴδιο υπόλοιπο, τὸ ὁποῖο ἄς συμβολίσουμε r . Έστω ὅτι τὰ ἀντίστοιχα πηλικά εἶναι q_1, q_2 . Τότε $a = mq_1 + r, b = mq_2 + r$, ὁπότε $b - a = m(q_2 - q_1)$, άρα $m|(b - a)$.

Μένει ν' ἀποδείξουμε ὅτι ἡ σχέση ἰσοτιμίας μέτρῳ m εἶναι σχέση ἰσοδυναμίας. Ἀὐτοπαθῆς ιδιότητα: $a \equiv a \pmod{m}$ σημαίνει $m|(a - a)$, σχέση προφανῶς ἀληθῆς. Συμμετρικὴ ιδιότητα: Ἄν ὑποθέσουμε ὅτι $a \equiv b \pmod{m}$, τότε $m|(b - a)$, ὁπότε καὶ $m|(a - b)$. Ἄλλὰ ἡ τελευταία σχέση σημαίνει $b \equiv a \pmod{m}$.

Μεταβατικὴ ιδιότητα: Ἄν ὑποθέσουμε ὅτι $a \equiv b \pmod{m}$ καὶ $b \equiv c \pmod{m}$, τότε $m|(b - a)$ καὶ $m|(c - b)$, άρα ὁ m διαιρεῖ τὸν $(b - a) + (c - b) = c - a$. Ἀὐτό, ἐξ ὀρισμοῦ, σημαίνει ὅτι $a \equiv c \pmod{m}$. **Ὡ.ἔ.δ.**

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

Θεώρημα 2.1.2 - Βασικὲς ιδιότητες τῶν ἰσοτιμιῶν.

α'. Ἰσοτιμίες μὲ τὸ ἴδιο μέτρο μποροῦν νὰ προστεθοῦν, νὰ ἀφαιρεθοῦν ἢ νὰ πολλαπλασιασθοῦν κατὰ 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 ἀριθμὸ.

δ'. Ἄν $f(x_1, \dots, x_n)$ εἶναι μία πολυωνυμικὴ παράσταση μὲ ἀκέραιους συντελεστῆς 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'. Τὰ δύο μέλη μιᾶς ἰσοτιμίας καὶ τὸ μέτρο μποροῦν νὰ πολλαπλασιασθοῦν μὲ τὸν ἴδιο ἀριθμὸ.

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

ζ'. Ἄν $a \equiv b \pmod{m}$ καὶ $d \geq 2$ εἶναι διαιρέτης τοῦ m , τότε $a \equiv b \pmod{d}$.

η' Ἄν $a \equiv b \pmod{m}$, τότε $(a, m) = (b, m)$.

Άποδείξη Δίνουμε συνοπτικὰ τὶς οὕτως ἢ ἄλλως ἀπλῆς ἀποδείξεις τῶν ἰσχυρισμῶν τοῦ θεωρήματος.

α'. Δίνουμε τὴν ἀπόδειξη γιὰ δύο ἰσοτιμίες $a_i \equiv b_i \pmod{m}$, ($i = 1, 2$). Γιὰ περισσότερες χρειάζεται ἀπλῆ ἐπαγωγή. Ἐχομε $b_i = a_i + k_i m$ ($i = 1, 2$) 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 $b_1 b_2 = a_1 a_2 + (a_1 k_2 + a_2 k_1 + k_1 k_2 m)m$, άρα $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

β'. Έστω $a \equiv b \pmod{m}$. Γράφομε αὐτὴ τὴν ἰσοτιμία n φορὲς καὶ πολλαπλασιάζομε αὐτὲς τὶς n τὸ πλῆθος ἰσοτιμίες κατὰ μέλη (μποροῦμε λόγω τοῦ α'), ὁπότε παίρνομε $a^n \equiv b^n \pmod{m}$.

γ'. Ἐάν $a \equiv b \pmod{m}$ καὶ k εἶναι τυχὼν ἀκέραιος, θέλομε νὰ δείξομε ὅτι $ka \equiv kb \pmod{m}$, 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 ὄρων τῆς μορφῆς $kx_1^{e_1} \cdots x_n^{e_n}$. Ἐπειδὴ μπορούμε νὰ προσθέτομε ἰσοτιμίες κατὰ μέλη (λόγῳ τοῦ α'), ἀρκεῖ νὰ δείξομε ὅτι, γιὰ κάθε τέτοιο μονώνυμο, ἰσχύει $ka_1^{e_1} \cdots a_n^{e_n} \equiv kb_1^{e_1} \cdots b_n^{e_n} \pmod{m}$. Πράγματι, ἐξ ὑποθέσεως, $a_1 \equiv b_1 \pmod{m}, \dots, a_n \equiv b_n \pmod{m}$, ἄρα, μὲ χρήση τῶν προτάσεων α', β' καὶ γ', ἔχομε: $a_1^{e_1} \equiv b_1^{e_1} \pmod{m}, \dots, a_n^{e_n} \equiv b_n^{e_n} \pmod{m}$. Πολλαπλασιάζοντας κατὰ μέλη, $a_1^{e_1} \cdots a_n^{e_n} \equiv b_1^{e_1} \cdots b_n^{e_n} \pmod{m}$ καί, μετὰ, πολλαπλασιάζοντας ἐπὶ k , $ka_1^{e_1} \cdots a_n^{e_n} \equiv kb_1^{e_1} \cdots b_n^{e_n} \pmod{m}$.

ε' Ἐστω $a \equiv b \pmod{m}$ 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, $km|(kb - ka)$, πού σημαίνει $ka \equiv kb \pmod{km}$.

ζ'. Ἐστω $a \equiv b \pmod{m}$ 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 $a_1 \equiv b_1 \pmod{m}$. 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 ζ' τοῦ θεωρήματος 1.2.2 ἔπεται ὅτι $m|(b_1 - a_1)$, δηλαδή, $a_1 \equiv b_1 \pmod{m}$.

η'. Ἡ ὑπόθεση λέει ὅτι $m|(b - a)$. Ἀλλὰ $d|m$, ἄρα $d|(b - a)$, ὁπότε $a \equiv b \pmod{d}$.

θ'. Ἀπὸ τὴν ὑπόθεση, $b = a + km$ γιὰ κάποιον ἀκέραιον k , ὁπότε, ἀρκεῖ νὰ ἐφαρμόσομε τὴν πρόταση β' τοῦ θεωρήματος 1.2.2. **ὁ.ξ.δ.**

2.2 Συστήματα υπολοίπων

Ἀπὸ τὴν πρόταση-ὄρισμὸ 2.1.1 εἶναι σαφές ὅτι, γιὰ κάθε a ὑπάρχει ἕνας ἀκριβῶς ἀκέραιος $a_0 \in \{0, 1, \dots, m - 1\}$, τέτοιος ὥστε $a \equiv a_0 \pmod{m}$. Στὴν πραγματικότητα, ὁ a_0 εἶναι τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ a διὰ m . Εἶδαμε, ἐπίσης, ὅτι ἡ σχέση ἰσοτιμίας μέτρῳ m εἶναι σχέση ἰσοδυναμίας, ἄρα ἔχει νόημα νὰ μιᾶμε γιὰ κλάσεις ἰσοδυναμίας, τίς ὁποῖες λέμε *κλάσεις ἰσοτιμίας μέτρῳ m* ἢ *κλάσεις ἰσοτιμίας modulo m* . Ἡ κλάση ἰσοτιμίας τοῦ a μέτρῳ m συμβολίζεται $a \pmod{m}$ καὶ εἶναι, φυσικά, ἕνα ἄπειρο σύνολο. Ἄρα, $a \equiv b \pmod{m} \Leftrightarrow a \pmod{m} = b \pmod{m}$. Ἐάν, ὅπως παραπάνω, a_0 εἶναι τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ a διὰ m , τότε $a \pmod{m} = a_0 \pmod{m}$, ἄρα, οἱ κλάσεις μέτρῳ m εἶναι οἱ $0 \pmod{m}, 1 \pmod{m}, \dots, m - 1 \pmod{m}$. Παράδειγμα.

Ἐστω $m = 12$. Ἡ κλάση τοῦ 45 ἀποτελεῖται ἀπὸ ὅλους (τοὺς ἄπειρους) ἀκεραίους a , γιὰ τοὺς ὁποῖους ἰσχύει $a \equiv 45 \pmod{12}$, ἄρα

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

Ἄς φαντασθοῦμε τώρα ὅτι ἀπὸ κάθε κλάση ἐπιλέγομε ἕνα, ἀκριβῶς, ἀκέραιον. Τότε σχηματίζομε ἕνα σύνολο, ἀποτελούμενο ἀπὸ m τὸ πλήθος ἀκεραίους a_1, \dots, a_m , ἀνὰ δύο ἀνισότιμους μέτρῳ m . Ἐνα τέτοιο σύνολο λέγεται *πλήρες σύστημα υπολοίπων*

μέτρῳ (ἢ modulo) m . Τὸ ἀπλούστερο, καὶ συνηθέστερα χρησιμοποιούμενο πλήρες σύστημα ὑπολοίπων εἶναι τὸ $\{0, 1, \dots, m-1\}$, ποὺ λέγεται *ἐλάχιστο μὴ ἀρνητικὸ πλήρες σύστημα*. Ἐνα ἄλλο πλήρες σύστημα ὑπολοίπων, ποὺ χρησιμοποιεῖται ἀρκετὰ συχνά, εἶναι τὸ

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

καὶ

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

Αὐτὸ λέγεται *ἀπολύτως ἐλάχιστο πλήρες σύστημα*. Παραδείγματος χάριν, τὸ ἀπολύτως ἐλάχιστο πλήρες σύστημα γιὰ $m = 12$ εἶναι $\{-5, -4, \dots, 4, 5, 6\}$ καὶ γιὰ $m = 11$ εἶναι $\{-5, -4, \dots, 4, 5\}$. 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 πλήρες 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 $0, 1, \dots, 6$.

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

Ἀπόδειξη Ἀρκεῖ νὰ δείξουμε ὅτι οἱ ἀριθμοὶ $ba_1 + c, ba_2 + c, \dots, ba_m + c$ εἶναι ἀνὰ δύο ἀνισότιμοι μέτρῳ m , στηριζόμενοι στὴν ὑπόθεση ὅτι οἱ ἀριθμοὶ a_1, a_2, \dots, 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 ζ' τοῦ θεωρήματος 2.1.2, διαιρώντας διὰ b , ποὺ εἶναι πρῶτος πρὸς τὸν m , θὰ καταλήγαμε στὴ σχέση $a_i \equiv a_j \pmod{m}$, ἢ ὁποία ἀντιφάσκει στὴν ὑπόθεση. **Ὡ.Ξ.Δ.**

Ἐὰς θεωρήσουμε τώρα κάποιον a πρῶτο πρὸς m καὶ b ὁποιοδήποτε ἀριθμὸ τῆς κλάσης $a \pmod{m}$. Ἀπὸ τὴν πρόταση η' τοῦ θεωρήματος 2.1.2 ἔπεται 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 πρῶτη πρὸς m . Ἐὰς φαντασθοῦμε τώρα ὅτι ἔχομε ἕνα πλήρες σύστημα ὑπολοίπων μέτρῳ m καὶ ἀπὸ αὐτὸ ἐπιλέγουμε ἐκείνους τοὺς ἀριθμοὺς τοῦ συστήματος, οἱ ὁποῖοι εἶναι πρῶτοι πρὸς m . Τὸ σύνολο, ποὺ λαμβάνουμε μὲ αὐτὸ τὸν τρόπο λέγεται *περιορισμένο σύστημα μέτρῳ (ἢ modulo) m* . Ἐὰν, γιὰ παράδειγμα, $m = 10$ καὶ θεωρήσουμε τὸ πλήρες σύστημα $\{15, 11, 22, 33, -11, -12, -23, 6, 14, 100\}$ (ἐλέγξτε ὅτι εἶναι ὄντως πλήρες σύστημα μέτρῳ 10), τότε τὸ περιορισμένο σύστημα ὑπολοίπων, ποὺ προκύπτει εἶναι $\{11, 33, -11, -23\}$, διότι αὐτοὶ καὶ μόνον οἱ ἀριθμοὶ τοῦ πλήρους συστήματος

είναι πρώτοι πρὸς τὸ 10. Παρατηρήστε ὅτι, γιὰ παράδειγμα, οἱ ἀριθμοὶ 7, 17, -63, πὸν ἀνήκουν στὴν κλάση $-23 \pmod{10}$, εἶναι, ἐπίσης, πρώτοι πρὸς τὸν 10.

Ἄν $\{a_1, \dots, a_m\}$ καὶ $\{b_1, \dots, b_m\}$ εἶναι πλήρη συστήματα υπόλοιπων, τότε κάθε a_i εἶναι ισότιμο μέτρω m μὲ ἀκριβῶς ἓνα b_j καὶ, ὅπως παρατηρήσαμε παραπάνω, εἶναι $(b_j, m) = 1$ ἂν, καὶ μόνο ἂν, $(a_i, m) = 1$. Συνεπῶς, ἓνα περιορισμένο σύστημα υπόλοιπων, ἀπὸ ὁποιοδήποτε πλήρες σύστημα κι ἂν προέρχεται, ἔχει τὸ ἴδιο πλῆθος ἀριθμῶν. Ἄν ἐπιλέξουμε, λοιπόν, τὸ ἐλάχιστο μὴ ἀρνητικό πλήρες σύστημα υπόλοιπων, τότε τὸ περιορισμένο σύστημα, πὸν προκύπτει ἀπὸ αὐτό, ἀποτελεῖται ἀπὸ ἐκείνους τοὺς ἀριθμοὺς $1, \dots, m-1$, οἱ ὁποῖοι εἶναι πρώτοι πρὸς τὸν m .² Τὸ πλῆθος τους συμβολίζεται $\phi(m)$. Ἡ συνάρτηση ϕ , πὸν σὲ κάθε $m \geq 2$ ἀντιστοιχεῖ τὸ πλῆθος $\phi(m)$ τῶν ἀκεραίων τοῦ συνόλου $\{1, \dots, m-1\}$, οἱ ὁποῖοι εἶναι πρώτοι πρὸς τὸν m , λέγεται *συνάρτηση ϕ τοῦ Euler*. Σύμφωνα, λοιπόν, μὲ ὅσα εἴπαμε πρὶν, κάθε περιορισμένο σύστημα υπόλοιπων περιέχει $\phi(m)$ τὸ πλῆθος ἀριθμοὺς. Τὸ θεώρημα 2.2.3 παρέχει τύπο γιὰ τὸν ὑπολογισμό τοῦ $\phi(m)$ ὅταν εἶναι γνωστὴ ἡ κανονικὴ ἀνάλυση τοῦ m .

Πρόταση 2.2.2 Ἄν a_1, a_2, \dots, a_k εἶναι περιορισμένο σύστημα υπόλοιπων μέτρω m ($k = \phi(m)$), καὶ ὁ b εἶναι πρῶτος πρὸς m , τότε ba_1, ba_2, \dots, ba_k εἶναι, ἐπίσης, περιορισμένο σύστημα υπόλοιπων μέτρω 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 ζ' τοῦ θεωρήματος 1.2.2. Μένει τώρα ν' ἀποδείξουμε ὅτι οἱ ἀριθμοὶ ba_i , $i = 1, \dots, k$ εἶναι ἀνὰ δύο ἀνισότιμοι μέτρω m . Πράγματι, ἂν $ba_i \equiv ba_j \pmod{m}$ μὲ $i \neq j$, τότε, ἀπὸ τὴν πρόταση ζ' τοῦ θεωρήματος 2.1.2 θὰ προέκυπτε $a_i \equiv a_j \pmod{m}$, ἄτοπο.

ὁ.ξ.δ.

Δίνουμε τώρα τὶς βασικὲς ιδιότητες τῆς συνάρτησης ϕ τοῦ Euler.

Θεώρημα 2.2.3 α'. Ἄν $(m, n) = 1$, τότε $\phi(mn) = \phi(m)\phi(n)$.

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

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

Προκειμένου νὰ συμπεριλάβουμε στὸ πεδίο ὀρισμοῦ τῆς ϕ καὶ τὸ 1, ὀρίζουμε $\phi(1) = 1$.

Ἀπόδειξη α'. Ἔστω M καὶ N περιορισμένα συστήματα υπόλοιπων μέτρω m καὶ n , ἀντιστοίχως. Θεωροῦμε τὸ σύνολο

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

καὶ θὰ δοῦμε κάποιες ιδιότητες τοῦ S .

(i) Ἄν $x_1, x_2 \in N$, $y_1, y_2 \in M$ καὶ $x_1 \neq x_2$ εἴτε $y_1 \neq y_2$, τότε $mx_1 + ny_1 \not\equiv mx_2 + ny_2$

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

(mod mn). Πραγματικά, ἄς ὑποθέσουμε, δίχως βλάβη τῆς γενικότητος, 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 . Ἐὰν 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 , καταλήγουμε 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 τιμὲς, ἄρα τὸ πλῆθος τῶν ἀριθμῶν τοῦ S εἶναι $\phi(n)\phi(m)$. Ὅπως εἶδαμε στὸ (i), οἱ ἀριθμοὶ αὐτοὶ εἶναι ἀνισότιμοι μὲτρω mn , ἐνῶ, λόγῳ τοῦ (ii) εἶναι πρῶτοι πρὸς τὸν mn , ἄρα ἀποτελοῦν ὑποσύνολο ἑνὸς περιορισμένου συστήματος ὑπολοίπων μὲτρω mn .

(iv) Θὰ δείξουμε τώρα ὅτι κάθε ἀριθμὸς πρῶτος πρὸς τὸν mn εἶναι ἰσότιμος μὲτρω mn μὲ κάποιον ἀπὸ τοὺς ἀριθμοὺς τοῦ S . Αὐτό, σὲ συνδυασμὸ μὲ τὸ (iii) θὰ μᾶς πείθῃ ὅτι τὸ S εἶναι ἕνα περιορισμένο σύστημα ὑπολοίπων καὶ ὄχι, ἀπλῶς, ἕνα ὑποσύνολο περιορισμένου συστήματος ὑπολοίπων. Ἐστω, λοιπόν, k πρῶτος πρὸς mn καὶ ἄς θεωρήσουμε τοὺς ἀριθμοὺς $m\ell - k$, $\ell = 0, 1, \dots, n-1$. Βάσει τῆς πρότασης 2.2.1, οἱ ἀριθμοὶ αὐτοὶ ἀποτελοῦν πλῆρες σύστημα ὑπολοίπων μὲτρω n , ἄρα γιὰ κάποιον ℓ_0 ἰσχύει $m\ell_0 - k \equiv 0 \pmod{n}$. Αὐτὴ ἢ τελευταία σχέση μᾶς λέει ὅτι ὑπάρχει z ἔτσι ὥστε $m\ell - nz = k$, ὅπου $\ell = \ell_0$. Μὲ χρῆση τῶν προτάσεων ε' καὶ β' τοῦ θεωρήματος 1.2.2 βλέπουμε ὅτι $(\ell, n) = (m\ell, n) = (m\ell - nz, n) = (k, n) = 1$, ἄρα ὁ ℓ εἶναι ἰσότιμος μὲτρω n μὲ κάποιον $x_0 \in N$. Ἀνάλογα, $(-z, m) = (-nz, m) = (m\ell - nz, m) = (k, m) = 1$, ἄρα ὁ $-z$ εἶναι ἰσότιμος μὲτρω m μὲ κάποιον $y_0 \in M$. Ἐτσι ἔχομε $\ell \equiv x_0 \pmod{n}$, ἄρα (πρόταση ε' τοῦ θεωρήματος 2.1.2) $m\ell \equiv mx_0 \pmod{mn}$ καὶ, 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, καταλήγουμε στὸ συμπέρασμα ὅτι, τὸ S μὲ πληθάρημο $\phi(m)\phi(n)$ εἶναι περιορισμένο σύστημα ὑπολοίπων μὲτρω mn . Ἀλλὰ ἕνα περιορισμένο σύστημα ὑπολοίπων μὲτρω 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 ἀνά δύο πρῶτοι μεταξύ τους. Ὄποτε, ἂν ἔχομε τὴν κανονικὴ ἀνάλυση τοῦ m , ὅπως στὸ β' τῆς ἐκφώνησης, τότε

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

καὶ ἀρκεῖ νὰ βροῦμε ἕνα γενικὸ τύπο γιὰ τὸ $\phi(p^a)$ ὅταν p πρῶτος καὶ $a \geq 1$. Αὐτό, ὅμως, εἶναι εὐκόλο: Θέλομε νὰ ὑπολογίσουμε πόσοι θετικοὶ ἀκέραιοι μικρότεροι τοῦ p^a εἶναι πρῶτοι πρὸς τὸν p^a . Εἶναι εὐκολώτερο νὰ ὑπολογίσουμε πόσοι δὲν εἶναι, διότι, ἕνας ἀριθμὸς δὲν εἶναι πρῶτος πρὸς τὸν p^a ἂν, καὶ μόνο ἂν, εἶναι πολλαπλάσιο τοῦ p . Τὰ θετικὰ πολλαπλάσια τοῦ p τὰ μικρότερα τοῦ p^a εἶναι οἱ ἀριθμοὶ $p, 2p, 3p, \dots, (p^{a-1} - 1)p$, ὅποτε, 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 είναι $(p^a - 1) - (p^{a-1} - 1) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$. Έτσι, $\phi(p^a) = p^a(1 - \frac{1}{p})$ και τώρα από την (2.1), έχουμε πολύ εύκολα τους αποδεικτέους τύπους. **ὄ.ξ.δ.**

Θεώρημα 2.2.4 *α'.* (Euler) Ἐάν $(a, m) = 1$, τότε $a^{\phi(m)} \equiv 1 \pmod{m}$.

β'. (Fermat) Ἐάν p εἶναι πρῶτος καὶ $(a, p) = 1$, τότε $a^{p-1} \equiv 1 \pmod{p}$.

Ἰσοδύναμη διατύπωση: Ἐάν p εἶναι πρῶτος, τότε $a^p \equiv a \pmod{p}$ γιὰ κάθε a .

γ'. Ἐάν $(a, m) = 1$ καὶ $\nu \equiv \mu \pmod{\phi(m)}$, τότε $a^\nu \equiv a^\mu \pmod{m}$.

Ἀπόδειξη *α'.* Ἐστω $k = \phi(m)$ καὶ $\{a_1, \dots, a_k\}$ ἔνα περιορισμένο σύστημα υπολοίπων μέτρω m . Ἀπὸ τὸ θεώρημα 2.2.2, τὸ $\{aa_1, \dots, aa_k\}$ εἶναι, ἐπίσης, περιορισμένο σύστημα υπολοίπων μέτρω m , ἄρα, καθένας ἀπὸ τοὺς ἀριθμοὺς τοῦ δευτέρου συστήματος υπολοίπων εἶναι ἰσότιμος μέτρω 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.ζ' τοῦ θεωρήματος 2.1.2), καταλήγουμε στὴν ἀποδεικτέα $a^k \equiv 1 \pmod{m}$.

β'. Ἐφαρμόζοντας τὸ *α'* μέρος γιὰ $m = p$ καὶ παρατηρώντας ὅτι, προφανῶς, $\phi(p) = p - 1$, καταλήγουμε στὴν ἀποδεικτέα σχέση.

γ'. Ὑποθέτομε, δίχως βλάβη τῆς γενικότητος, ὅτι $\nu \geq \mu$. Λόγω τῆς $\nu \equiv \mu \pmod{\phi(m)}$, συμπεραίνομε ὅτι ὑπάρχει θετικὸς ἀκέραιος ℓ , τέτοιος ὥστε $\nu = \mu + \ell\phi(m)$. Ἄρα, λόγω καὶ τοῦ θεωρήματος τοῦ Euler,

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

ὄ.ξ.δ.

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

Παράδειγμα ὑπολογισμοῦ τοῦ υπολοίπου διαιρέσεως. *Νὰ υπολογισθεῖ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 174379^{32971} διὰ 57624 .*

Ἄρκει νὰ υπολογίσουμε 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, $174379 \equiv 1507 \pmod{57624}$ καὶ, συνεπῶς, $174379^{32971} \equiv 1507^{32971} \pmod{57624}$. Πρὶν προχωρήσουμε ὑπολογίζομε ὅτι $(1507, 57624) = 1$, ἄρα μπορούμε νὰ ἐφαρμόσουμε τὸ θεώρημα τοῦ Euler μὲ $a = 1507$ καὶ $m = 57624$.

Μὲ τὴ βοήθεια τοῦ θεωρήματος 2.1, ὑπολογίζομε

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

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, $1507^{32971} \equiv 1507^{43} \pmod{57624}$.

Μέχρι στιγμής, λοιπόν,

$$174379^{32971} \equiv 1507^{43} \pmod{57624}.$$

Ο ύπολογισμός του 1507^{43} μέτρω 57624 μπορεί να γίνει με διάφορους συνδυασμούς. Ένας τρόπος, για παράδειγμα, φαίνεται παρακάτω. Οί ύπολογισμοί έχουν γίνει με κομπιουτεράκι τσέπης. Σε κάθε γραμμή, ή πιό δεξιά ίσοτιμία mod 57624 όφειλεται σε υπόλοιπο διαιρέσεως, δηλαδή, στην πρώτη γραμμή, για παράδειγμα, είναι $2271049 \equiv 23713 \pmod{57624}$ διότι το υπόλοιπο της διαίρεσης του 2271049 διά 57624 είναι 23713. Ανάλογα και στις άλλες γραμμές.

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

Συνοπῶς, τὸ ζητούμενο υπόλοιπο είναι 12091.

2.3 Ὑψωση σὲ δύναμη

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

Τὸ παραπάνω παράδειγμα μᾶς ύποδεικνύει σαφῶς τὸν παρακάτω ἀλγόριθμο. Κάνομε χρῆση τοῦ συμβολισμοῦ $[a]_m$ γιὰ νὰ δηλώσουμε τὸ υπόλοιπο τῆς διαίρεσης τοῦ a διά τοῦ $m > 1$. Ὅποτε, ὁ συμβολισμὸς στὸν ἀλγόριθμο $[a]_2$ σημαίνει 0, ἂν ὁ a εἶναι ἄρτιος καὶ 1, ἂν ὁ a εἶναι περιττός. Ἐπίσης, παρατηρήστε 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.

Εισάγεται θετικός άκέραιος N .

Έξάγονται τά δυαδικά ψηφία b_I , $I = 0, 1, 2, \dots$ τοῦ N .

Γίνεται χρήση τῶν βοηθητικῶν μεταβλητῶν I καί B .

```

I ← 0   :   B ← N
ΕΝΟΣΩ B > 0 ΕΠΑΝΑΛΑΒΕ
  bI = [B]2   :   B ← ⌊ $\frac{B}{2}$ ⌋   :   I ← I + 1
ΤΕΛΟΣ ΕΠΑΝΑΛΗΨΗΣ
ΤΕΛΟΣ

```

Ο παραπάνω άλγόριθμος περιέχεται, μάλλον κρυμμένος, στον άλγόριθμο ύψωσης σέ δύναμη, που θά περιγράψομε παρακάτω καί τοῦ όποιου ή αναλυτική περιγραφή εἶναι ή έξής:

Έστω ότι θέλομε νά ύπολογίσομε τόν a^N μέτρω m , δηλαδή, με τόν συμβολισμό στην άρχή αὐτῆς τῆς παραγράφου, θέλομε νά ύπολογίσομε τόν $[a^N]_m$. Έστω $N = (b_n \dots b_1 b_0)$: τά δυαδικά ψηφία b_i ύπολογίζονται διαδοχικά με τόν άλγόριθμο μετατροπῆς σέ δυαδική μορφή. Έπίσης, βοηθητικά, ύπολογίζονται, σέ κάθε βῆμα k , άριθμοί D_{k+1} καί A_k .

Άρχικό βῆμα 0: Ύπολόγισε

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

Βῆμα k : Έχεις ἤδη ύπολογίσει

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

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

Διαφορετικά,

Βῆμα $k + 1$: Ύπολόγισε

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

Θά δοῦμε τώρα πόσοι πολλαπλασιασμοὶ άπαιτοῦνται μέχρι νά τελειώσει ή παραπάνω διαδικασία. Κατ' άρχάς, λέγοντας «πολλαπλασιασμός» τῶν a, b , για παράδειγμα, έννοοῦμε «πολλαπλασιασμός μέτρω m » τῶν a καί b , δηλαδή, πρόκειται για τόν ύπολογισμό $[[a]_m [b]_m]_m$. Έπειδή $0 \leq [a]_m, [b]_m < m$, άπαιτεῖται ή εύρεση τοῦ ύπολοίπου τῆς διαίρεσης ένός μη άρνητικοῦ άκεραίου, μικρότερου τοῦ m^2 , δια m . Αὐτός ό ύπολογισμός δέν κοστίζει πολύ: μπορεί νά γίνει με στοιχειώδεις πράξεις, που τὸ πλήθος τους φράσσεται άπό μία σταθερά επί $(\log m)^{1.585}$. Τὸ ζήτημα αὐτὸ εἶναι πέραν τοῦ σκοποῦ αὐτῶν τῶν σημειώσεων. Πάντως, αὐτὸ, που

πρέπει να κρατήσει κανείς, είναι ότι το «κόστος» του πολλαπλασιασμού μέτρω m δεν μας προβληματίζει περισσότερο από το κόστος ενός συνήθους πολλαπλασιασμού θετικών άκεραίων μικρότερων του m .

Έπανερχόμενοι στον αλγόριθμό μας, παρατηρούμε ότι, στο αρχικό βήμα δεν κάνουμε πολλαπλασιασμό ή ύψωση σε δύναμη, ενώ το πέρασμα από το βήμα k στο βήμα $k + 1$ απαιτεί μία ύψωση στο τετράγωνο και, το πολύ, ένα πολλαπλασιασμό, δηλαδή, δύο, το πολύ, πολλαπλασιασμούς. Άρα, αν $N = (b_n \dots b_1 b_0)$, τότε ή παραπάνω διαδικασία απαιτεί $2n$, το πολύ, πολλαπλασιασμούς. Όμως, $N \geq 2^n$, άρα $n \leq \frac{\log N}{\log 2}$ και, συνεπώς,

Για τον υπολογισμό του $a^N \pmod{m}$ απαιτούνται, το πολύ, $\left\lceil 2 \frac{\log N}{\log 2} \right\rceil$ πολλαπλασιασμοί.

Η παραπάνω διαδικασία συμπυκνώνεται στον παρακάτω κομψό αλγόριθμο.

ΑΛΓΟΡΙΘΜΟΣ ΥΨΩΣΗΣ ΣΕ ΔΥΝΑΜΗ.

Εισάγονται άκεραιοι $m > 1$, $a \neq 0$, $N \geq 1$.

Έξάγεται $[a^N]_m$, δηλαδή, το υπόλοιπο της διαίρεσης του a^N δια m .

Γίνεται χρήση των βοηθητικών μεταβλητών A , B και D .

Άρχικό βήμα: $A \leftarrow 1$, $D \leftarrow a$, $B \leftarrow N$.

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

Με τον αλγόριθμο αυτόν, η διαδικασία υπολογισμού της δύναμης a^{43} , ή οποία έγινε αναλυτικά στην αρχή αυτού του έδαφίου, 'κωδικοποιείται' στον 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 κρυπτογραφική μέθοδος RSA

Θὰ δώσουμε τὴ βασική ιδέα τῆς μεθόδου RSA, πὺ ἐπινοήθηκε κατὰ τὰ τέλη τῆς δεκαετίας τοῦ '70 ἀπὸ τοὺς Rivest, Shamir, Adleman³. Διάφορες τεχνικὲς λεπτομέρειες σχετικὲς μὲ τὴν ἐφαρμογή τῆς μεθόδου στὴν πράξη δὲν θὰ μᾶς ἀπασχολήσουν ἐδῶ.

Φανταζόμαστε ὅτι ἓνα μήνυμα εἶναι μία πεπερασμένη διαδοχὴ ἀκεραίων ἀριθμῶν. Γιά παράδειγμα, ἄς ἀντιστοιχίσουμε στὸ A τὸν ἀριθμὸ 01, στὸ B τὸ 02, . . . , στὸ Ω τὸ 24 καὶ στὸ «κενὸ» τὸ 25 καὶ ἄς ἐνώνομε ἀνὰ δύο τὰ γράμματα, ὥστε νὰ σχηματίζουν 4ψήφιους ἀκεραίους. Ἔτσι, τὸ μήνυμα⁴

ΠΟΛΕΜΟΣ ΠΑΤΗΡ ΠΑΝΤΩΝ

μετατρέπεται στὸ ἐξῆς 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.ὄ.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 ἓνας, πὺ ἐπιθυμεῖ νὰ στέλνει καὶ νὰ λαμβάνει μηνύματα, ἄς ποῦμε ἢ ΑΓΝΗ, ἐπιλέγει καὶ δημοσιοποιεῖ τὸ δημόσιο κλειδί τῆς (n, e) . Ἐδῶ, $n = pq$, ὅπου $p \neq q$ εἶναι πρῶτοι, μεγαλύτεροι ἀπὸ τὸν ἀριθμὸ 2525 (= ἡ μεγαλύτερη δυνατὴ 4ψήφια συνιστώσα ἐνὸς μηνύματος μ) καὶ e εἶναι ἓνας θετικὸς ἀκέραιος πρῶτος πρὸς τὸν $\phi(n) = (p - 1)(q - 1)$. Οἱ πρῶτοι p, q εἶναι γνωστοὶ μόνο στὴν A.

Κάποια στιγμή, ὁ ΒΙΚΤΩΡ ἀποφασίζει νὰ στείλει στὴν A ἓνα μήνυμα μ . Βρίσκει σὲ κάποιο «δημόσιο κατάλογο» τὸ κλειδί (n, e) τῆς A, καὶ ἐνεργεῖ ὡς ἐξῆς: Γιά κάθε συνιστώσα a τοῦ ἀριθμοποιημένου μηνύματός του μ ὑπολογίζει τὸν ἐλάχιστο θετικὸ ἀριθμὸ τῆς κλάσης $a^e \pmod n$. Μετατρέπει ἔτσι τὸ διάνυσμα μ σ' ἓνα νέο διάνυσμα, μὲ τὸ ἴδιο πλῆθος συνιστωσῶν, ἀλλὰ πολὺ διαφορετικὲς συνιστώσες ἀπὸ τὶς ἀρχικὲς.

Γιά παράδειγμα, ἔστω ὅτι ὁ B βρίσκει στὸν δημόσιο κατάλογο ὅτι τὸ κλειδί τῆς A εἶναι $(n, e) = (49144364409017, 1365911)$. Γιά κάθε 4ψήφια συνιστώσα a τοῦ μηνύματός του, ὁ B ὑπολογίζει $a^{1365911} \pmod{49144364409017}$. Ἔτσι, τὸ μήνυμα «Πόλεμος πατὴρ πάντων» μετατρέπεται ὡς ἐξῆς. Οἱ ἰσοτιμίες ἐννοῦνται

³Ἐξ οὗ καὶ ἡ ὀνομασία RSA

⁴Οφειλόμενο στὸν Ἡράκλειτο.

mod 49144364409017 :

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

Έτσι, ο Β θα στείλει στην Α το διάνυσμα με συνιστώσες τὰ δεξιά μέλη τῶν παραπάνω 10 ἰσοτιμιῶν. Ἡ Α κατασκευάζει τὸ «ἀντικλείδι» d τοῦ κλειδιοῦ τῆς (n, e) , ὡς ἐξῆς. Ἐπειδὴ γνωρίζει ὅτι ἡ ἀνάλυση τοῦ n σὲ πρώτους παράγοντες εἶναι $3295321 \cdot 14913377$, μπορεῖ νὰ ὑπολογίσει ὅτι $\phi(n) = (3295321 - 1) \cdot (14913377 - 1) = 49144364409017$. Εἶναι, ἀπὸ ἐπιλογή τῆς Α, $(e, \phi(n)) = 1$, 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 $1 \leq d < \phi(n)$, ἀντικαθιστώντας τὸν d ἀπὸ τὸ ὑπόλοιπο τῆς διαιρέσεώς του διὰ $\phi(n)$, ἂν χρειασθεῖ. Ὁ πρακτικὸς ὑπολογισμὸς τοῦ d μπορεῖ νὰ γίνῃ 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 πολὺ, τῆς τάξεως τοῦ $\log_2 n$.

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

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

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

Γιατὶ κανεὶς ἄλλος, πλὴν τῆς Α, δὲν μπορεῖ νὰ ἀποκρυπτογραφήσῃ τὸ μήνυμα, οὔτε κἂν ὁ ἴδιος ὁ Β, 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 μόνον μέσῳ τῆς παραγοντοποίησης τοῦ n . Στὴν

πράξη, ό n είναι γινόμενο δύο τυχαίων πρώτων⁵, πού καθένας μπορεί να έχει, ως πούμε, 150 ψηφία (σέ δεκαδικό σύστημα αρίθμησης). Κανείς μέχρι σήμερα δέν μπορεί να αναλύσει σέ γινόμενο πρώτων ένα τέτοιο αριθμό n , δίχως να ξοδέψει τρείς, ή και περισσότερους, αιώνες ύπολογισμού με ισχυρούς ύπολογιστές!

2.5 Άσκησης του κεφαλαίου 2

Στις επόμενες ασκήσεις, όπου γίνεται λόγος για τα ψηφία ενός αριθμού στο δεκαδικό σύστημα αρίθμησης, να έχετε ύπ' όψει τα έξης: Άν τα ψηφία των μονάδων, δεκάδων, κλπ του αριθμού είναι a_0, a_1, \dots, a_n , τότε ό αριθμός ίσοται με $a_0 + 10a_1 + \dots + 10^n a_n$.

1. Άποδείξτε ότι, για x περιπτώ, $x^2 \equiv 1 \pmod{4}$ και $x^2 \equiv 1 \pmod{8}$. Επίσης, για y άρτιο, $y^2 \equiv 0 \pmod{4}$, ένω μέτρω 8, $y^2 \equiv 0 \pmod{8}$ ή $y^2 \equiv 4 \pmod{8}$.
2. Με τη βοήθεια της άσκησης 1 άποδείξτε τό έξης: Άν $x^2 + y^2 = z^2$ και $(x, y) = 1$, τότε, ό x, y είναι έτερότυποι (ό ένας άρτιος και ό άλλος περιπτώς).
3. Με τη βοήθεια της άσκησης 1 άποδείξτε τό έξης: Άν $x^2 + 3y^2 = z^4$ και $(x, y) = 1$, τότε ό x είναι περιπτώς και ό y είναι διαιρετός διά 4.
4. Με τη βοήθεια της άσκησης 1 άποδείξτε τό έξης: Άν ό πρώτος αριθμός p γράφεται ως άθροισμα δύο (μη μηδενικών) τετραγώνων (π.χ. $29 = 5^2 + 2^2$), τότε $p \equiv 1 \pmod{4}$. Άρα, κανείς πρώτος της μορφής $4k + 3$ δέν μπορεί να γραφεί ως άθροισμα δύο τετραγώνων.
5. Άποδείξτε ότι, για κάθε x , πού δέν διαιρείται διά 3, είναι $x^2 \equiv 1 \pmod{3}$. Με τη βοήθεια αυτού άποδείξτε ότι, αν για τόν πρώτο p ύπάρχουν μη μηδενικοί x, y , τέτοιοι ώστε $p = x^2 + 3y^2$, τότε $p \equiv 1 \pmod{6}$.
6. Άποδείξτε ότι, για κάθε x είναι $x^3 \equiv 0$ ή $\pm 1 \pmod{9}$. Με τη βοήθεια αυτού, άποδείξτε ότι ή διοφαντική εξίσωση $x^3 + 2y^3 = 5z^3$ είναι αδύνατη για μη μηδενικούς άκεραίους x, y, z με $(x, y) = 1$.
Υπόδειξη. Άν ίσχύει $x^3 + 2y^3 = 5z^3$ με $(x, y) = 1$, τότε και $x^3 + 2y^3 \equiv 5z^3 \pmod{9}$, όπου ό x, y δέν είναι και ό δύο διαιρετοί διά 3.
7. Άποδείξτε ότι, για κάθε n , ό $5n^3 + 7n^5$ είναι πολλαπλάσιο του 12.
8. *Κριτήριο διαιρετότητας διά 3 ή 9.* Κατ' αρχάς, όρίζομε τόν *πυθμένα* ενός θετικού άκεραίου, τόν όποιο θεωρούμε γραμμένο στο δεκαδικό σύστημα, ως τό άθροισμα των ψηφίων του. Για παράδειγμα, ό πυθμήν του 54678 είναι $5 + 4 + 6 + 7 + 8 = 30$.
Άποδείξτε ότι, τό ύπόλοιπο της διαίρεσης ενός αριθμού διά 3 (άντιστοίχως,

⁵Η έννοια «τυχαίος πρώτος» δέν είναι και τόσο άπλή!

διὰ 9) είναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ πυθμένος τοῦ ἀριθμοῦ διὰ 3 (ἀντιστοίχως, διὰ 9). Για παράδειγμα, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 54678 διὰ 9 εἶναι 3, καθὼς 3 εἶναι καὶ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 30 διὰ 9.

Ἐπομένως. $10 \equiv 1 \pmod{3}$ καὶ $10 \equiv 1 \pmod{9}$. Ἄν, λοιπόν, a_0, a_1, \dots, a_n εἶναι τὰ ψηφία τῶν μονάδων, δεκάδων κλπ τοῦ ἀριθμοῦ, ὑπολογίστε μὲ ποιούς ἀριθμούς εἶναι ἰσότιμος ὁ ἀριθμός, μέτρῳ 3 καὶ μέτρῳ 9.

9. *Κριτήριο διαιρετότητας διὰ 4 ἢ 25.* Ἀποδείξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 4 (ἀντιστοίχως, διὰ 25) εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ ἀριθμοῦ, ποὺ σχηματίζεται ἀπὸ τὰ δύο τελευταῖα ψηφία τοῦ ἀριθμοῦ (βάση ἀρίθμησης τὸ 10) διὰ 4 (ἀντιστοίχως, διὰ 25).
10. *Κριτήριο διαιρετότητας διὰ 8 ἢ 125.* Ἀποδείξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 8 (ἀντιστοίχως, διὰ 125) εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τῆς 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.* Ἀποδείξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 11 εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ ἀριθμοῦ, ποὺ προκύπτει ἀπὸ τὸ ἄθροισμα τῶν διψηφίων τμημάτων τοῦ ἀριθμοῦ, λαμβανομένων ἀπὸ τὰ δεξιὰ πρὸς τὰ ἀριστερά. Για 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.* Ἀποδείξτε ὅτι, τὸ ὑπόλοιπο τῆς διαίρεσης ἑνὸς ἀριθμοῦ διὰ 11 εἶναι τὸ ἴδιο μὲ τὸ ὑπόλοιπο τῆς διαίρεσης διὰ 11 τοῦ ἀριθμοῦ $a_0 - a_1 + a_2 - a_3 + \dots$, ὅπου a_0 τὸ ψηφίο τῶν μονάδων τοῦ ἀριθμοῦ, a_1 τὸ ψηφίο τῶν δεκάδων, a_2 τὸ ψηφίο τῶν ἑκατοντάδων κ. ὅ. κ. Για 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. Ἐστω πρῶτος p .
 - α'. Ἐστω $a \in \{1, \dots, p-1\}$. Μὲ τὴ βοήθεια τοῦ β' τοῦ θεωρήματος 1.2.1 ἀποδείξτε ὅτι ὑπάρχει ἕνας, ἀκριβῶς, $a' \in \{1, \dots, p-1\}$, μὲ τὴν ιδιότητα $aa' \equiv 1 \pmod{p}$. Μετά, ἀποδείξτε ὅτι, οἱ μόνες περιπτώσεις ποὺ $a' = a$ εἶναι οἱ $a = 1$ καὶ $a = p-1$.
 - β'. Ἐστω $p \geq 5$. Θεωρήστε τὸ γινόμενο $1 \cdot 2 \cdot \dots \cdot (p-2)(p-1)$ καί, βασιζόμενοι στὸ (α'), ζευγαρώστε κάθε $a \in \{2, \dots, p-2\}$ μὲ τὸ $a' \in \{2, \dots, p-2\}$ γιὰ τὸ ὁποῖο ἰσχύει $aa' \equiv 1 \pmod{p}$. Συμπεράνατε ὅτι $(p-1)! \equiv -1 \pmod{p}$. Διαπιστώστε ὅτι ἡ σχέση αὐτή, ποὺ λέγεται *θεώρημα τοῦ Wilson*, ἰσχύει καὶ γιὰ $p = 2, 3$. Ἀποδείξτε καὶ τὸ ἀντίστροφο θεώρημα: Ἄν γιὰ κάποιον ἀκέραιο p ἰσχύει $(p-1)! \equiv -1 \pmod{p}$, τότε ὁ p εἶναι πρῶτος.

14. Ἐστω ὅτι ὁ p εἶναι πρῶτος καὶ $ab' - a'b \not\equiv 0 \pmod{p}$. Ἀποδείξτε ὅτι δὲν ὑπάρχουν ἀκέραιοι x, y , πρῶτοι μεταξύ τους, πὺν νὰ ἱκανοποιοῦν συγχρόνως καὶ τὶς δύο ἰσοτιμίες $ax + by \equiv 0 \pmod{p}$ καὶ $a'x + b'y \equiv 0 \pmod{p}$. Ὑπόδειξη. Ἀπαλειψτε τὸ y ἀπὸ τὶς δύο ἰσοτιμίες καί, μετὰ, κάντε τὸ ἴδιο καὶ γιὰ τὸ x .
15. Ἀποδείξτε ὅτι, ἂν $a|b$, τότε $\phi(a)|\phi(b)$.
16. Ἐστω ὅτι ὁ $n \geq 3$ ἔχει k διαφορετικούς πρώτους διαιρέτες. Ἀποδείξτε ὅτι, ἂν ὁ n εἶναι ἄρτιος, ἀλλὰ ὄχι πολλαπλάσιο τοῦ 4, τότε $2^{k-1}|n$ ἐνῶ, γιὰ ὅλες τὶς ὑπόλοιπες τιμές τοῦ n , $2^k|n$.
17. Ἀποδείξτε ὅτι, οἱ μόνον θετικοὶ ἀκέραιοι x , γιὰ τοὺς ὁποίους ἰσχύει $\phi(x) = x/2$, εἶναι οἱ $x = 2^a$, $a \geq 1$.
18. Ἀποδείξτε ὅτι, γιὰ κάθε θετικὸ περιττὸ ἀκέραιο x ἰσχύει $\phi(x) = \phi(2x)$, ἀλλὰ ἡ σχέση αὐτὴ εἶναι ἀδύνατη γιὰ ἄρτιο x .
19. Βρεῖτε ὅλους τοὺς θετικούς ἀκεραίου x , γιὰ τοὺς ὁποίους ἰσχύει $\phi(x) = 12$.
20. Ἐστω $n \geq 1$. Γιὰ κάθε θετικὸ διαιρέτη d τοῦ n ὀρίζομε τὸ σύνολο

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

(α') Ἀποδείξτε ὅτι τὸ $A(d)$ περιέχει ἀκριβῶς $\phi(\frac{n}{d})$ ἀριθμούς.

Ὑπόδειξη. Παρατηρήστε 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') Ἄν $d_1 \neq d_2$ εἶναι θετικοὶ διαιρέτες τοῦ n , ἀποδείξτε ὅτι $A(d_1) \cap A(d_2) = \emptyset$.

(γ') Συνδυάζοντας τὰ (α') καὶ (β') ἀποδείξτε 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 3 τοῦ κεφαλαίου 1.

21. Ὑπολογίστε τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ $(12371^{128} + 34)^{172}$ διὰ 111.
22. Ἀποδείξτε 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.
23. Ἐστω p πρῶτος. Παρατηρήστε ὅτι, τὸ θεώρημα τοῦ Fermat μπορεῖ νὰ διατυπωθεῖ ὡς ἐξῆς: Γιὰ κάθε a ἰσχύει $a^p \equiv a \pmod{p}$, δίχως νὰ θέσομε τὸν περιορισμὸ ὁ p νὰ μὴ διαιρεῖ τὸν a . Μετὰ, μὲ τὴ βοήθεια τῆς ἄσκησης 32 τοῦ κεφαλαίου 1, ἀποδείξτε ὅτι $(a + b)^p \equiv a^p + b^p \pmod{p}$, γιὰ ὅλους τοὺς a, b . Ἐπίσης, ἀποδείξτε ὅτι ἂν γιὰ τὸν περιττὸ πρῶτο p ἰσχύει $a^p + b^p \equiv 0 \pmod{p}$ τότε ἰσχύει καὶ $a^p + b^p \equiv 0 \pmod{p^2}$.

24. Μετατρέψτε τὸν 749 σὲ δυαδικὸ ἀριθμὸ, ἐφαρμόζοντας τὸν ἀλγόριθμο μετατροπῆς σὲ δυαδικό.
25. Ἐφαρμόζοντας τὸν ἀλγόριθμο ὕψωσης σὲ δύναμη, ὑπολογίστε τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ 13^{370} διὰ 23.
26. Ἐστω ὅτι τὸ δημόσιο κλειδὶ τῆς A εἶναι (91,25). Ὁ B θέλει νὰ κρυπτογραφήσει καὶ νὰ στείλει στὴν A τὸ μήνυμα ΘΑ ΕΛΘΩ ΣΤΙΣ ΟΚΤΩ. Ποιὰ διαδικασία θὰ ἀκολουθήσει γιὰ νὰ κρυπτογραφήσει τὸ μήνυμα καὶ ποιὰ διαδικασία θὰ ἀκολουθήσει ἡ A, 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 μορφή» 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

Ἐστω 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 ὀρίσομε ὡς *ἐπίλυση τῆς ἰσοτιμίας* $f(x) \equiv 0 \pmod{m}$ τὴν εὔρεση ὅλων τῶν κλάσεων $a \pmod{m}$, τέτοιων ὥστε $f(a) \equiv 0 \pmod{m}$ καὶ νὰ λέμε ὅτι ἡ κλάση $a \pmod{m}$ (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 \pmod{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 Ἴσοτιμίες 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 Ἐὰν $a \neq 0$ καὶ $(a, m) = d$, τότε ἡ ἰσοτιμία $ax \equiv b \pmod{m}$ ἔχει λύση ἂν, καὶ μόνον ἂν, $d|b$. 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 ἢ $x_0 \pmod{\frac{m}{d}}$, τότε οἱ d διαφορετικὲς λύσεις τῆς $ax \equiv b \pmod{m}$ εἶναι οἱ

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

Ἀπόδειξη Ἄν ἡ $ax \equiv b \pmod{m}$ ἔχει λύση, τότε, γιὰ κάποιον $x_1 \in \mathbb{Z}$ ἔχομε $ax_1 \equiv b \pmod{m}$, ἄρα, ἀπὸ τὸ ἡ' 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, $d|b$. Θετόντας 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, τοῦλάχιστον, λύση, ἔστω τὴν $x_0 \pmod{\frac{m}{d}}$.

Ἰσχυρίζομαστε, κατ' ἀρχάς, ὅτι δὲν μπορεῖ νὰ ἔχει καὶ δεύτερη, διαφορετικὴ, λύση. Πράγματι, ἂν $x_1 \pmod{\frac{m}{d}}$ εἶναι, ἐπίσης, λύση, τότε

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

Τὸ ζ' 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 $x_1 \pmod{m}$ μία λύση τῆς $ax \equiv b \pmod{m}$. Τότε, βλέπομε πολὺ εὐκόλα ὅτι ἡ $x_1 \pmod{\frac{m}{d}}$ εἶναι λύση τῆς $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, ἄρα, ἀπὸ τὴ μοναδικότητα τῆς λύσης $x_0 \pmod{\frac{m}{d}}$, πὺν εἶδαμε 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 $0 \leq j < d$. Συνεπῶς, $x_1 = x_0 + j \frac{m}{d} + qm \equiv x_0 + j \frac{m}{d} \pmod{m}$, ἄρα, ὁ ἡ κλάση $x_1 \pmod{m}$ συμπίπτει μὲ μία ἀπὸ τὶς κλάσεις (3.1).

Μένει νὰ δείξομε ὅτι οἱ κλάσεις (3.1) εἶναι διαφορετικὲς. Πράγματι, ἂν δύο ἐξ αὐτῶν συνέπιπταν, θὰ εἶχαμε $x_0 + j_1 \frac{m}{d} \equiv x_0 + j_2 \frac{m}{d} \pmod{m}$ μὲ $0 \leq j_1 < j_2 < d$. 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, ὁμως, σημαίνει ὅτι $d|(j_2 - j_1)$, προφανῶς ἀδύνατον, ἀφοῦ $0 < j_2 - j_1 < d$.

Ὡ.ξ.δ.

Στὴν πράξη, ἡ επίλυση 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 $1 \leq a < m$. 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. Ἄν τὸ $(n + 1)$ -οστὸ ὑπόλοιπο στὴ διαδικασία τοῦ εὐκλείδειου 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 . Ἄν ὁ d δὲν διαιρεῖ τὸν b , τότε ἡ ἰσοτιμία δὲν ἔχει λύση. Ἄς υποθέσουμε, 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 συμβολισμό 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 ἀπλοῦστα ἀπὸ τὴν (3.1).

Παράδειγμα. Θὰ λύσουμε 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 ὑπολογίσουμε ἀναδρομικὰ τὰ s_{-1}, s_0, s_1, \dots , ποὺ ἀντιστοιχοῦν στὸ ζευγὸς 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 συμβολισμό 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 $x \equiv 258 + k \frac{7168}{7}, k = 0, 1, \dots, 6$, 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: *Ἐνα στρατιωτικὸ σῶμα ἔχει λιγώτερος ἀπὸ 1000 στρατιῶτες. Ἄν 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 ὀδηγοῦν φυσιολογικὰ στὸ λεγόμενον κινέζικο θεώρημα ὑπολοίπων.

Θεώρημα 3.3.1 –Κινέζικο θεώρημα ὑπολοίπων. Ἔστω ὅτι οἱ m_1, \dots, m_k εἶναι μεγαλύτεροι τοῦ 1 καὶ ἀνά δύο πρῶτοι μεταξύ τους. Τότε, γιὰ ὅποιονσδήποτε ἀκεραῖους a_1, \dots, a_k , ὑπάρχει x , τὸ ὁποῖο ἐπαληθεύει συγχρόνως ὅλες τὶς ἰσοτιμίες

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

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

Ἀπόδειξη Θέτουμε $M = m_1 m_2 \cdots m_k$ καὶ γιὰ κάθε $i = 1, \dots, k$, $M_i = M/m_i$. 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 $M_i N_i \equiv 1 \pmod{m_i}$. Ὅρίζομε 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 $i = 1, \dots, k$, $x_0 \equiv a_i \pmod{m_i}$. Πράγματι, ἀπὸ τὸν τρόπο πὸν ὀρίσθησαν τὰ M_1, \dots, M_k , βλέπομε ἀμέσως ὅτι, κάθε M_j μὲ $j \neq i$ ἔχει ὡς παράγοντά του τὸν m_i καί, συνεπῶς, εἶναι μηδενικός 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 $i = 1, \dots, k$, $x_1 \equiv a_i \equiv x_0 \pmod{m_i}$, 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, $x_1 \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$. **Ὡ.ἔ.δ.**

Παράδειγμα. Θὰ λύσομε τὸ πρόβλημα, πὸν ἀναφέραμε στὴν ἀρχὴ αὐτῆς τῆς παραγράφου. Προφανῶς, τὸ πρόβλημα ἰσοδυναμεῖ μὲ τὴν εὔρεση 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 συμβολισμό τῆς ἀπόδειξης τοῦ θεωρήματος ἔχομε $M_1 = 8 \cdot 13 = 104$, $M_2 = 15 \cdot 13 = 195$, $M_3 = 15 \cdot 8 = 120$. Ἐπίσης, $104N_1 \equiv 1 \pmod{15}$, $195N_2 \equiv 1 \pmod{8}$, $120N_3 \equiv 1 \pmod{13}$ καὶ οἱ ἰσοτιμίες αὐτὲς ἀπλοποιοῦνται ὡς ἑξῆς: $(-1)N_1 \equiv 1 \pmod{15}$, $3N_2 \equiv 1 \pmod{8}$, $3N_3 \equiv 1 \pmod{13}$. Ἡ ἐπίλυση κάθε μᾶς ἀπὸ αὐτὲς εἶναι ἀπλούστατη, 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, λόγω τῆς $0 < x < 1000$, παίρνομε $3979 < 1560k < 4979$, ἀπ' ὅπου $k = 3$ καὶ $x = -3979 + 3 \cdot 1560 = 701$.

3.4 Πολυωνυμικὲς ἰσοτιμίες μὲ ἓνα ἄγνωστο

Ἀρχικά, θὰ θεωρήσομε ὅτι τὸ μέτρο τῆς ἰσοτιμίας εἶναι ἓνας θετικός πρῶτος p .

Μία προκαταρκτικὴ ἀπλῆ, ἀλλὰ βασικὴ, 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 πολὺ, $p - 1$.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 $p - 1$. Ἐξέρομε, ἀπὸ τὸ θεώρημα τοῦ Fermat (β' τοῦ θεωρήματος 2.2.4), ὅτι, γιὰ

¹Ἐδῶ περιλαμβάνεται καὶ ἡ περίπτωση τοῦ μηδενικοῦ πολυωνύμου, τοῦ ὁποίου ὁ βαθμὸς μορεῖ νὰ ὀρισθεῖ ὡς $-\infty$.

κάθε ακέραιο a , είναι $a^p - a \equiv 0 \pmod{p}$, άρα, $f(a) \equiv 0 \pmod{p}$ αν, και μόνο αν, $g(a) \equiv 0 \pmod{p}$. Αυτό, προφανώς, σημαίνει ότι οι ισοτιμίες $f(x) \equiv 0 \pmod{p}$ και $g(x) \equiv 0 \pmod{p}$ είναι ισοδύναμες.

Θεώρημα 3.4.1 Έστω $f(X) \in \mathbb{Z}[X]$, βαθμού $n \geq 1$, του οποίου ο συντελεστής του μεγιστοβαθμίου όρου δεν διαιρείται διά p . Τότε, η ισοτιμία $f(x) \equiv 0 \pmod{p}$ έχει, τὸ πολὺ, n τὸ πλῆθος διαφορετικὲς λύσεις.²

Ἴσοδύναμη διατύπωση: Ἄν τὸ $f(X) \in \mathbb{Z}[X]$ εἶναι μὴ μηδενικὸ πολυώνυμο καὶ τὸ πλῆθος τῶν λύσεων τῆς ισοτιμίας $f(x) \equiv 0 \pmod{p}$ ὑπερβαίνει τὸν βαθμὸ τοῦ $f(X)$, τότε ὅλοι οἱ συντελεστὲς τοῦ $f(X)$ εἶναι διαιρετοὶ διά p .

Ἀπόδειξη Έστω $f(X) = a_n X^n + \dots + a_1 X + a_0$, ὅπου, ἐξ ὑποθέσεως, $(a_n, p) = 1$ καὶ ἄς ὑποθέσουμε ὅτι ἡ ισοτιμία $f(x) \equiv 0 \pmod{p}$ ἔχει $n + 1$ διαφορετικὲς λύσεις $r_1 \pmod{p}, \dots, r_{n+1} \pmod{p}$. Θὰ καταλήξουμε σὲ ἄτοπο. Τὸ γεγονός ὅτι οἱ λύσεις αὐτὲς εἶναι διαφορετικὲς, σημαίνει, φυσικὰ, $r_i \not\equiv r_j \pmod{p}$ γιὰ $i \neq j$.

Ἰσχυρισμός: Ὑπάρχουν ἀκέραιοι b_0, b_1, \dots, b_{n-1} , τέτοιοι ὥστε, νὰ ἰσχύει

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

Πράγματι, κατ' ἀρχάς, στὴν (3.4) ἄς συμβολίσουμε τὸ πολυώνυμο τῆς πρώτης γραμμῆς μὲ $g_n(X)$, τῆς δεύτερης μὲ $g_{n-1}(X) \dots$ τῆς προτελευταίας μὲ $g_1(X)$. Τὸ πολυώνυμο $g_n(X)$ εἶναι γνωστὸ, ἀφοῦ τὰ a_n, r_1, \dots, r_n εἶναι γνωστά· τὰ ὑπόλοιπα, ὅμως, πολυώνυμα $g_{n-1}(X), \dots, g_1(X)$ ἐξαρτῶνται ἀπὸ τοὺς μέχρι στιγμῆς ἀγνώστους b_{n-1}, \dots, b_1 .

Συγκρίνομε τοὺς συντελεστὲς τῶν $X^n, X^{n-1}, \dots, X, X^0$ στὰ δύο μέλη. Τοῦ X^n εἶναι a_n καὶ στὰ δύο μέλη. Ἀπὸ τὴ σύγκριση τῶν συντελεστῶν τοῦ X^{n-1} παίρνομε

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

ἄρα μπορούμε νὰ ὑπολογίσουμε τὸ b_{n-1} , τὸ ὁποῖο, πλέον, θεωρεῖται γνωστὸ, ὁπότε καὶ τὸ $g_{n-1}(X)$ εἶναι γνωστὸ.

Ἀπὸ τὴ σύγκριση τῶν συντελεστῶν τοῦ X^{n-2} παίρνομε

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

²Οἱ ἐπαίοντες θὰ ἀναγνωρίσουν ἐδῶ μία εἰδικὴ περίπτωση τοῦ γενικοῦ θεωρήματος τῆς Ἄλγεβρας, ποὺ λέει ὅτι, ἓνα πολυώνυμο βαθμοῦ n μὲ συντελεστὲς ἀπὸ ἓνα σῶμα, ἔχει, τὸ πολὺ, n διαφορετικὲς ρίζες στὸ σῶμα αὐτό. Στὴν προκειμένη περίπτωση, σῶμα εἶναι τὸ \mathbb{Z}_p (ἢ \mathbb{F}_p , κατ' ἄλλο συμβολισμό).

Από τη σχέση αυτή προσδιορίζεται και το b_{n-2} , άρα, στο έξις, και το $g_{n-2}(X)$ είναι γνωστό.

Με αυτή τη διαδικασία προχωρώντας, καταλήγουμε στον υπολογισμό όλων των b_i . Φυσικά, δεν μας ενδιαφέρει ο ακριβής υπολογισμός τους, αλλά, απλώς, ή ύπαρξή τους, που καθιστά αληθή τη σχέση (3.4). Η αντικατάσταση $X \leftarrow r_1$ στη σχέση αυτή δίνει $0 \equiv f(r_1) = b_0 \pmod{p}$. Μετά, ή αντικατάσταση $X \leftarrow r_2$ στην (3.4) δίνει $0 \equiv f(r_2) = b_0 + b_1(r_2 - r_1) \equiv 0 + b_1(r_2 - r_1) \pmod{p}$. Έπειδή, όμως, $(r_2 - r_1, p) = 1$, το ζ' του θεωρήματος 2.1.2 μας επιτρέπει να συμπεράνουμε ότι $b_1 \equiv 0 \pmod{p}$. Με τον τρόπο αυτό, οι διαδοχικές αντικαταστάσεις $X \leftarrow r_i$, $i = 3, \dots, n$ μας δίνουν, αντιστοίχως, $b_j \equiv 0 \pmod{p}$ για $j = 2, \dots, n$. Τέλος, ή αντικατάσταση $X \leftarrow r_{n+1}$ στην (3.4) δίνει, με δεδομένο ότι όλοι οι b_i είναι ισότιμοι με 0 μέτρω p , $0 \equiv f(r_{n+1}) \equiv a_n(r_{n+1} - r_1)(r_{n+1} - r_2) \cdots (r_{n+1} - r_n) \pmod{p}$. Έξ υποθέσεως, κάθε παράγωγο $r_{n+1} - r_j$, στο δεξιό μέλος, είναι πρώτος προς τον p , άρα, αναγκαστικά, συμπεραίνουμε ότι $a_n \equiv 0 \pmod{p}$, το οποίο αντιφάσκει προς την υπόθεσή μας.

ὄ.ξ.δ.

Τώρα θα εξετάσουμε την επίλυση τῆς ισοτιμίας

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

ὅπου, και πάλι, ὁ p εἶναι πρῶτος και ὁ συντελεστής τοῦ μεγιστοβαθμίου ὄρου τοῦ $f(X)$ δὲν εἶναι διαιρετὸς διὰ p . Ὁ ἐκθέτης a εἶναι τουλάχιστον 2. Θὰ δείξουμε ὅτι, ἀναδρομικά, ἂν ξέρομε νὰ λύσουμε τὴν ισοτιμία (3.5) γιὰ κάποια τιμὴ τοῦ ἐκθέτη a , τότε μπορούμε νὰ τὴν λύσουμε και γιὰ τὴν ἀμέσως ἐπόμενη τιμὴ του.

Ἡ φράση «μπορῶ νὰ λύσω μία ισοτιμία» πάντοτε σημαίνει «μπορῶ νὰ ἀποφασίσω ἂν ἔχει ἢ ὄχι λύσεις και, σὲ περίπτωση πὸν ἔχει, μπορῶ νὰ τὴν ὑπολογίσω ὅλες».

Ὡς συνήθως, συμβολίζουμε με $f^{(k)}(X)$ 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 πολυώνυμα⁴. 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.

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

⁴Ὁ τύπος τοῦ ἀναπτύγματος Taylor γιὰ πολυώνυμα εἶναι ἀνεξάρτητος ἀπὸ τὸ ἀξίωμα συνεχείας και μπορεῖ νὰ ἀποδειχθεῖ ἐπαγωγικά, δίχως χρῆση Ἀπειροστικοῦ Λογισμοῦ.

Πριν προχωρήσουμε, κάνουμε την προφανή παρατήρηση ότι, αν $x \equiv x_0 \pmod{p^a}$ είναι λύση της (3.5), τότε $x \equiv x_0 \pmod{p^{a-1}}$ είναι λύση της

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

Άρα, κάθε λύση της (3.5) προέρχεται από λύση της (3.6). Συνεπώς, όταν αναζητούμε τις λύσεις της (3.5), πρέπει να ξεκινήσουμε από μία-μία τις λύσεις της (3.6) και να δοῦμε, για κάθε μία από αυτές, αν παράγει λύσεις της (3.5) και αν ναι, πόσες.

Θεώρημα 3.4.2 Έστω $a \geq 2$ και $x_0 \pmod{p^{a-1}}$ λύση της $f(x) \equiv 0 \pmod{p^{a-1}}$.

α'. Αν $f'(x_0) \not\equiv 0 \pmod{p}$, τότε, η λύση $x_0 \pmod{p^{a-1}}$ της (3.6) παράγει μία ακριβώς λύση της (3.5).

β'. Αν $f'(x_0) \equiv 0 \pmod{p}$ και $f(x_0) \equiv 0 \pmod{p^a}$, τότε, η λύση $x_0 \pmod{p^{a-1}}$ της (3.6) παράγει p ακριβώς λύσεις της (3.5) και, συγκεκριμένα τις $x_0 + kp^{a-1} \pmod{p^a}$, $k = 0, 1, \dots, p-1$.

γ'. Αν $f'(x_0) \equiv 0 \pmod{p}$ και $f(x_0) \not\equiv 0 \pmod{p^a}$, τότε, προφανώς, η λύση $x_0 \pmod{p^{a-1}}$ της (3.6) δεν παράγει λύσεις για την (3.5).

Απόδειξη Οί τυχόν λύσεις της (3.5), που παράγονται από τη λύση $x_0 \pmod{p^{a-1}}$ της (3.6), έχουν τη μορφή $x = x_0 + yp^{a-1}$, όπου το y είναι προσδιοριστέο.

α'. Η αντικατάσταση $X \leftarrow x_0 + yp^{a-1}$ στο ανάπτυγμα Taylor του $f(X)$ μᾶς δίνει

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

διότι οί υπόλοιποι ὅροι στο δεξιό μέλος είναι της μορφής $\frac{1}{k!}f^{(k)}(x_0)y^k p^{k(a-1)}$, όπου ο εκθέτης του p είναι $k(a-1) \geq a$ και ο συντελεστής του $p^{k(a-1)}$ είναι ακέραιος. Συνεπώς, η σχέση $f(x) \equiv 0 \pmod{p^a}$ ισοδυναμεί με την

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

όπου, βέβαια, το δεξιό μέλος είναι ακέραιος, λόγω της υποθέσεως $f(x_0) \equiv 0 \pmod{p^{a-1}}$. Η παραπάνω ως προς y ισοτιμία έχει μία ακριβώς λύση $y_0 \pmod{p}$, βάσει του θεωρήματος 3.2.1. Άρα, η γενική μορφή του y είναι $y = y_0 + zp$, οπότε η γενική μορφή του x είναι $x = x_0 + (y_0 + zp)p^{a-1} \equiv x_0 + y_0 p^{a-1} \pmod{p^a}$, απ' όπου φαίνεται ότι είναι μοναδική μέτρω p^a .

β'. Όπως και στην προηγούμενη περίπτωση, καταλήγουμε στη σχέση (3.7). Λόγω των υποθέσεων $f(x_0) \equiv 0 \pmod{p^a}$ και $f'(x_0) \equiv 0 \pmod{p}$, το αριστερό μέλος είναι ισότιμο με το 0 μέτρω p^a , οποιαδήποτε τιμή κι αν έχει το y . Αν $y = zp + y_0$, όπου y_0 είναι το υπόλοιπο της εύκλειδειας διαίρεσης του y δια p , τότε, η γενική μορφή του x είναι $x = x_0 + (y_0 + zp)p^{a-1} \equiv x_0 + y_0 p^{a-1} \pmod{p^a}$, οπότε, για κάθε τιμή $y_0 = 0, 1, \dots, p-1$, παίρνουμε μία διαφορετική μέτρω p^a λύση της (3.5).

γ'. Ο ισχυρισμός είναι τετριμμένος.

ὄ.ξ.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 τέσσερις ἀκριβῶς λύσεις, τὶς $0 \pmod{7}$, $2 \pmod{7}$, $3 \pmod{7}$ καὶ $5 \pmod{7}$.

Ἐστω $x \equiv 2 \pmod{7}$. Ὑπολογίζομε ὅτι $f'(2) \equiv 0 \pmod{7}$ καὶ $f(2) \equiv 0 \pmod{7^2}$, ἄρα ἡ λύση $2 \pmod{7}$ 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 $2 + 7y_0 \pmod{7^2}$, 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 τὴν λύση $2 \pmod{7}$ τῆς $f(x) \equiv 0 \pmod{7}$ παράγονται οἱ λύσεις $16 + 7^2y_0 \pmod{7^3}$ καὶ $30 + 7^2y_0 \pmod{7^3}$ τῆς $f(x) \equiv 0 \pmod{7^3}$, ὅπου τὸ y_0 διατρέχει τὶς τιμὲς $0, 1, \dots, 6$. Παίρνομε ἔτσι τὶς ἐξῆς δεκατέσσερις λύσεις τῆς $f(x) \equiv 0 \pmod{7^3}$, ἐκ τῶν ὁποίων, οἱ πρῶτες ἑπτὰ προέρχονται ἀπὸ τὴν $16 \pmod{7^2}$ καὶ οἱ ὑπόλοιπες ἑπτὰ ἀπὸ τὴν $30 \pmod{7^2}$:

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

Ἐστω $x \equiv 3 \pmod{7}$. Τώρα $f'(3) \not\equiv 0 \pmod{7}$, ἄρα ἡ λύση $3 \pmod{7}$ 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, $y \equiv 5 \pmod{7}$. Ἐπεταί ὅτι, $x \equiv 3 + 5 \cdot 7 \equiv 38 \pmod{7^2}$. Ἡ λύση $38 \pmod{7^2}$ 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 αὕτη εἶναι ἡ μία καὶ μοναδικὴ λύση τῆς $f(x) \equiv 0 \pmod{7^3}$, ποὺ παράγεται ἀπὸ τὴν λύση $3 \pmod{7}$ 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 $98 \pmod{7^3}$ ἀπὸ τὴν πρώτη καὶ $12 \pmod{7^3}$ ἀπὸ τὴν 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 ἐξῆς: Ἐὰν $m = p_1^{a_1} \cdots p_k^{a_k}$ εἶναι ἡ κανονικὴ ἀνάλυση τοῦ m , τότε λύνομε πρῶτα κάθε μία ἀπὸ τὶς ἰσοτιμίες $f(x) \equiv 0 \pmod{p_i^{a_i}}$, $i = 1, \dots, k$. Ἐὰν, ἔστω καὶ μία ἀπὸ τὶς ἰσοτιμίες αὐτὲς δὲν ἔχει λύση, τότε, ἡ ἀρχικὴ ἰσοτιμία δὲν ἔχει λύση. Διαφορετικὰ, 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

όποιο, βάσει του «κινέζικου θεωρήματος» 3.3.1, έχει ακριβώς μία λύση $x_0 \pmod m$. Φυσικά, η τιμή x_0 εξαρτάται από την k -άδα (x_1, \dots, x_k) . Το πλήθος των λύσεων της $f(x) \equiv 0 \pmod m$ ισοϋται με τον πληθάρημο του $S_1 \times \dots \times S_k$, δηλαδή, με $|S_1| \cdot \dots \cdot |S_k|$.

Παράδειγμα. Θα λύσουμε την ισοτιμία $f(x) = x^4 + x^3 - 13x^2 + 10x + 55 \equiv 0 \pmod m$, όπου $m = 2^4 \cdot 3^3 \cdot 11^3$. Μοναδική λύση της $f(x) \equiv 0 \pmod{2^4}$ είναι η $15 \pmod{16}$. Η ισοτιμία $f(x) \equiv 0 \pmod{3^3}$ έχει τρεις λύσεις: $x \equiv 1, 10, 19 \pmod{27}$. Η ισοτιμία $f(x) \equiv 0 \pmod{11^3}$ έχει, επίσης, μία μόνο λύση, την $1265 \pmod{1331}$. Συνεπώς, το πλήθος των λύσεων της $f(x) \equiv 0 \pmod m$ είναι $1 \cdot 3 \cdot 1 = 3$, οί οποίες εύρίσκονται άντιστοιχώς, από τις έπιλύσεις των τριών συστημάτων

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

Έφαρμόζοντας το «κινέζικο θεώρημα» στα παραπάνω τρία συστήματα βρίσκουμε, άντιστοιχώς, τις λύσεις $x \equiv 461791, 270127, 78463 \pmod{2^4 \cdot 3^3 \cdot 11^3}$.

3.5 Άσκήσεις του κεφαλαίου 3

1. Να λυθεί χωριστά κάθε μία άπ' τις ισοτιμίες $412x \equiv 108 \pmod{34}$ και $33900x \equiv 56935 \pmod{2995}$. Μετά, να ύπολογισθούν όλες οί άνισότιμες μέτρω $2995 \cdot 34$ τιμές του x , οί οποίες έπαληθεύουν συγχρόνως και τις δύο ισοτιμίες.
2. Θεωρούμε τους πρώτους άριθμούς $p_1 = 29$, $p_2 = 71$ και $p_3 = 113$. Σε ό,τι ακολουθεϊ, οί δείκτες i, j, k παίρνουν τιμές άπό τό $\{1, 2, 3\}$ και είναι διαφορετικοί άνά δύο.
Νά βρεθεϊ άκέραιος a άνάμεσα στο 200000 και τό 300000, με την έξής ιδιότητα: Για κάθε $i = 1, 2, 3$, τό ύπόλοιπο της διαίρεσης του a δια p_i ισοϋται με τό ύπόλοιπο της διαίρεσης του $p_j p_k$ δια p_i .
Υπόδειξη: Ό a ικανοποιεϊ, συγχρόνως, τρεις ισοτιμίες, οί οποίες πρέπει να έπιλυθοϋν με τό «κινέζικο θεώρημα».
3. Έστω

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

Έπιλύστε την ισοτιμία $f(x) \equiv 0 \pmod{7}$, άφοϋ πρώτα βρεϊτε ένα πολυώνυμο $g(X)$, βαθμοϋ μικρότερου του 7, τέτοιο ώστε, η ισοτιμία $g(x) \equiv 0 \pmod{7}$ να έχει τις ίδιες λύσεις με την $f(x) \equiv 0 \pmod{7}$.

4. Νὰ λυθεῖ τὸ σύστημα

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

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

6. Ἐστω $p > 2$ πρῶτος. Θέτομε $s_1 = \sum_{1 \leq i \leq p-1} i$, $s_2 = \sum_{1 \leq i < j \leq p-1} ij$ καί, γενικότερα, γιὰ $k \leq p-1$, s_k εἶναι τὸ ἄθροισμα ὅλων τῶν δυνατῶν γινομένων k διαφορετικῶν ἀριθμῶν τοῦ συνόλου $\{1, 2, \dots, p-1\}$: εἰδικώτερα, $s_{p-1} = (p-1)!$. Ἀποδείξτε 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. Ὑστερα, κάνοντας χρῆση τῆς ταυτότητας

$$(X-1)(X-2) \cdots (X-p+1) = X^{p-1} - s_1 X^{p-2} + \cdots - s_{p-2} X + s_{p-1}$$

καὶ τοῦ θεωρήματος 3.4.1, ἀποδείξτε 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*, μίᾳ ἄλλῃ ἀπόδειξη τοῦ ὁποίου δίνεται στὴν ἄσκηση 13 τοῦ κεφαλαίου 2.

7. Ἐστω p πρῶτος.

α'. Ἐστω $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, ὅπου $1 \leq n < p$. Ἀποδείξτε ὅτι, ἀναγκαῖα καὶ ἱκανὴ συνθήκη γιὰ νὰ ἔχει ἡ ἰσοτιμία $f(x) \equiv 0 \pmod{p}$ n διαφορετικὲς λύσεις εἶναι ἡ ἐξῆς: Τὸ ὑπόλοιπο τῆς διαιρέσεως τοῦ $X^p - X$ διὰ τοῦ $f(X)$ εἶναι πολυώνυμο μὲ ὅλους τοὺς συντελεστὲς του διαιρετοὺς διὰ p .

Ὑπόδειξη: Ἐστω $X^p - X = f(X)g(X) + r(X)$ μὲ $\text{degr}(X) < n$. Κατ' ἀρχάς, παρατηρήστε ὅτι τὸ $g(X)$ εἶναι βαθμοῦ $p-n$. Γιὰ νὰ ἀποδείξετε ὅτι ἡ συνθήκη εἶναι ἀναγκαῖα, παρατηρήστε 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 παρατηρήστε ὅτι, ἂν ὅλοι οἱ συντελεστὲς τοῦ $r(X)$ εἶναι διαιρετοὶ διὰ p , τότε, $f(k)g(k) \equiv 0 \pmod{p}$ γιὰ κάθε $k = 0, 1, \dots, p-1$. Ἄν $f(k) \equiv 0 \pmod{p}$ γιὰ λιγώτερες ἀπὸ n τιμὲς τοῦ k , τότε \dots . Καὶ μὴ ξεχᾶστε ὅτι τὸ $g(X)$ εἶναι βαθμοῦ $p-n$.

β'. Ἐστω $a \not\equiv 0 \pmod{p}$ καὶ $n > 1$ διαιρέτης τοῦ $p-1$. Ἀποδείξτε ὅτι ἡ ἰσοτιμία $x^n \equiv a \pmod{p}$ ἔχει λύση ἂν, καὶ μόνο ἂν, $a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$. Στὴν περίπτωση δέ, ποὺ ἔχει λύση, τὸ πλῆθος τῶν διαφορετικῶν λύσεων εἶναι ἀκριβῶς n .

Υπόδειξη: Το αναγκαίο της συνθήκης είναι εύκολο. Για το ικανό θα κάνετε χρήση της ταυτότητας

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

όπου (\dots) είναι κάποιο πολυώνυμο, ή ακριβής τιμή του οποίου δεν έχει σημασία. Η ταυτότητα αυτή σ'ας δείχνει ποιό είναι το υπόλοιπο της διαίρεσης του $X^p - X$ διά του $X^n - a$ και τώρα, θα κάνετε χρήση του (α').

8. Η άσκηση αυτή δείχνει πώς μπορούμε να επεκτείνουμε στις ισοτιμίες τον κλασματικό συμβολισμό. Ό $m \geq 2$ είναι το μέτρο και όποτεδήποτε εμφανίζονται παρονομαστές σε ισοτιμίες, ή άκεραιοι με αρνητικό εκθέτη, έννοείται, δίχως να λέγεται, ότι αυτοί είναι πρώτοι προς τον m .

Οί συμβολισμοί $a^{-1} \pmod m$ και $\frac{1}{a} \pmod m$ σημαίνουν, έξ' όρισμοϋ, τή μοναδική κλάση $a' \pmod m$, για τήν όποία $aa' \equiv 1 \pmod m$. Συνακόλουθοι συμβολισμοί είναι οί $ba^{-1} \pmod m$, $a^{-1}b \pmod m$ και $\frac{b}{a} \pmod m$, πού σημαίνουν, και οί τρεῖς, τήν κλάση $a'b \pmod m$.

Άποδείξτε τις έξής ιδιότητες:

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

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

(γ') $\frac{cb}{ca} \equiv \frac{b}{a} \pmod m$.

(δ') $\frac{b_1}{a_1} + \frac{b_2}{a_2} \equiv \frac{b_1a_2 + b_2a_1}{a_1a_2} \pmod m$ και $\frac{b_1}{a_1} \cdot \frac{b_2}{a_2} \equiv \frac{b_1b_2}{a_1a_2} \pmod m$.

(ε') Για θετικό άκεραίο n , $(a^{-1})^n \equiv (a^n)^{-1} \pmod m$. Συμβολίζομε με $a^{-n} \pmod m$ τήν κλάση $(a^{-1})^n \pmod m$.

(ς') Για όποιουσδήποτε άκεραίους k, n -θετικούς, άρνητικούς ή μηδέν- ισχύουν οί σχέσεις $(a^k)^n \equiv a^{kn} \pmod m$ και $a^k a^n \equiv a^{k+n} \pmod m$.

9. Στην άσκηση αυτή γίνεται χρήση κλασματικού συμβολισμοϋ σε ισοτιμίες, όποτε πρέπει να δείτε πρώτα τήν άσκηση 8.

Για κάθε πρώτο $p \geq 5$ ισχύει $1 + \frac{1}{2} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$.

Υπόδειξη: Σύμφωνα με τήν άσκηση 8 πρέπει και άρκει να αποδειχθεῖ ότι ό αριθμητής του κλάσματος, πού προκύπτει όταν άθροίσομε τó άριστερό μέλος, διαιρείται διά p^2 . Τόν αριθμητή αυτόν συναντοϋμε στο πολυώνυμο $g(X) = (X-1)(X-2) \dots (X-p+1)$ πού; Υπολογίστε τήν τιμή $g(p)$ και χρησιμοποιείστε τήν άσκηση 6.

Κεφάλαιο 4

Τετραγωνικά ισοϋπόλοιπα

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

4.1 Ὅρισμοὶ καὶ βασικὲς ιδιότητες

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

Στὴν εἰδικώτερη περίπτωση, πού $m = p$, περιττὸς πρῶτος, ἂν ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρω p καὶ $x_0 \pmod{p}$ εἶναι μία λύση τῆς ἰσοτιμίας $x^2 \equiv a \pmod{p}$, τότε $-x_0 \pmod{p}$ εἶναι, ἐπίσης, λύση τῆς ἴδιας ἰσοτιμίας, διαφορετικὴ ἀπὸ τὴν $x_0 \pmod{p}$. 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 πολὺ, δύο διαφορετικὲς λύσεις, ἄρα, βάσει καὶ τῶν παραπάνω, ἔχει ἀκριβῶς δύο λύσεις.

Θεώρημα 4.1.1 Ἐστω περιττὸς πρῶτος p .

α'. Ἐνα περιορισμένο σύστημα ὑπολοίπων μέτρω p περιέχει ἀκριβῶς $\frac{p-1}{2}$ τὸ πλήθος τετραγωνικὰ ἰσοϋπόλοιπα, τὰ ὁποῖα εἶναι ἰσότημα μὲ τοὺς ἀριθμοὺς

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2. \quad (4.1)$$

β'. Ἐστω $(a, p) = 1$. Ἄν ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο μέτρω p , τότε

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad (4.2)$$

ένω, αν o a είναι τετραγωνικό ανισοϋπόλοιπο,

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (4.3)$$

Άποδειξη α' . Καθένας από τους αριθμούς (4.1) είναι, προφανώς, τετραγωνικό ισοϋπόλοιπο. Επίσης, οι αριθμοί αυτοί είναι ανισότιμοι μεταξύ τους. Πράγματι, αν $1 \leq \ell < k \leq \frac{p-1}{2}$ και συνέβαινε να ισχύει $k^2 \equiv \ell^2 \pmod{p}$, τότε o p θα έπρεπε να διαιρεί έναν από τους $k + \ell$ και $k - \ell$, κάτι αδύνατον, αφού και οι δύο αυτοί αριθμοί είναι θετικοί και μικρότεροι του p .

Συνεπώς, αν R είναι ένα περιορισμένο σύστημα υπολοίπων μέτρων p , τότε κάθε αριθμός k στην (4.1) είναι ισότιμος με ένα διαφορετικό αριθμό $r_k \in R$ και, φυσικά, o r_k είναι τετραγωνικό ισοϋπόλοιπο. Αντίστροφα, έστω $r \in R$ τετραγωνικό ισοϋπόλοιπο. Τότε υπάρχει $k \in \{1, \dots, p-1\}$, τέτοιος ώστε $k^2 \equiv r \pmod{p}$. Αν $1 \leq k \leq \frac{p-1}{2}$, τότε o r είναι ισότιμος προς κάποιον από τους αριθμούς (4.1)· διαφορετικά, παρατηρούμε ότι $1 \leq p-k \leq \frac{p-1}{2}$ και $r \equiv k^2 \equiv (p-k)^2 \pmod{p}$.

β' . Αν o a είναι τετραγωνικό ισοϋπόλοιπο, τότε υπάρχει x_0 , τέτοιος ώστε $a \equiv x_0^2 \pmod{p}$ και, βεβαίως, $(x_0, p) = 1$. Άρα, από το θεώρημα του Fermat (β' του θεωρήματος 2.2.4),

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

Πριν προχωρήσουμε, α ς παρατηρήσουμε ότι, για κάθε a από το σύνολο αριθμών (4.1), ισχύει ή σχέση (4.2), α ρα ή ισοτιμία

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad (4.4)$$

έχει τουλάχιστον $\frac{p-1}{2}$ το πλήθος λύσεις. Από το θεώρημα 3.4.1, δεν μπορεί να έχει περισσότερες, α ρα, οι κλάσεις των αριθμών (4.1), και μόνον αυτές, είναι οι λύσεις της ισοτιμίας (4.4). Αυτό, όμως, συνεπάγεται ότι, αν κάποιος a είναι τετραγωνικό ανισοϋπόλοιπο, τότε ή κλάση $a \pmod{p}$ δεν είναι λύση της (4.4)· Από την άλλη, το θεώρημα του Fermat, λέει ότι $a^{p-1} - 1 \equiv 0 \pmod{p}$ και, παραγοντοποιώντας το αριστερό μέλος καταλήγουμε στο συμπέρασμα ότι o p διαιρεί έναν από τους $a^{(p-1)/2} - 1$, $a^{(p-1)/2} + 1$. Το πρώτο ένδεχόμενο συνεπάγεται ότι ή $a \pmod{p}$ είναι λύση της (4.4), όποτε αποκλείεται, βάσει των δ σων μόλις είπαμε παραπάνω. Έτσι, μένει το δεύτερο ένδεχόμενο, που ισοδυναμεί, προφανώς, με τη σχέση (4.3). **ὄ.ξ.δ.**

4.2 Τὸ σύμβολο τοῦ Legendre

Στήν παράγραφο αὐτή τα λατινικά γράμματα, που δὲν εἶναι ὑποδείκτες, συμβολίζουν πάντα ἀκεραῖους πρώτους πρὸς τὸν p .

Τὸ σύμβολο Legendre τοῦ a ὡς πρὸς p ὀρίζεται ὡς ἑξῆς:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ἂν } a \text{ τετραγωνικὸ ἰσοῦπόλοιπο μέτρω } p \\ -1 & \text{ἂν } a \text{ τετραγωνικὸ ἀνισοῦπόλοιπο μέτρω } p. \end{cases}$$

Οἱ πρῶτες στοιχειώδεις ιδιότητες 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'. Ἐὰν $a \equiv b \pmod{p}$, 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 ἰσοῦπόλοιπο ἂν $p \equiv 1 \pmod{4}$ καὶ τετραγωνικὸ ἀνισοῦπόλοιπο ἂν $p \equiv 3 \pmod{4}$.

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

Ἀπόδειξη Οἱ ἰσχυρισμοὶ (α') καὶ (β') εἶναι ἐντελῶς ἄμεσες συνέπειες τῶν ὀρισμῶν.

(γ'). Προφανῆς συνδυασμὸς τοῦ ὀρισμοῦ τοῦ συμβόλου Legendre καὶ τοῦ β' τοῦ θεωρήματος 4.1.1.

(δ'). Προφανῆς συνέπεια τοῦ (γ').

(ε'). Ἐφαρμόζοντας τὸ (γ') ἔχομε

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

Τὸ ἀριστερότερο καὶ τὸ δεξιότερο μέλος τῆς παραπάνω ἰσοτιμίας εἶναι ἴσα μὲ ± 1 , ἄρα, ἀπὸ τὴν ἄσκηση 2, εἶναι ἴσα. **ῥ.ξ.δ.**

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

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

Άκόμη, τὰ $r_1, r_2, \dots, r_{p'}$ εἶναι ὅλα διαφορετικὰ μεταξὺ τους. Πράγματι, ἔστω $1 \leq k < \ell \leq p'$. 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 $ka \equiv -\ell a \pmod{p}$, δηλαδή, $(k + \ell)a \equiv 0 \pmod{p}$ · ἀδύνατον, ἀφοῦ, ἀφ' ἑνός, $(a, p) = 1$ καί, ἀφ' ἑτέρου $2 \leq k + \ell < p - 1$.

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 $r_1, r_2, \dots, r_{p'}$ εἶναι μία μετάθεση τῶν $1, 2, \dots, p'$, 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 $\left(\frac{a}{p}\right)$, ὅποτε καταλήγομε σὲ μία ἰσοτιμία, στὴν ὁποία, τὰ δύο μέλη εἶναι 1 ἢ -1. Ἄρα, ἡ ἰσοτιμία εἶναι ἰσότητα (ἄσκηση 2) καὶ καταλήγομε στὴ σχέση

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

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 , ὅποτε $\alpha = [\alpha] + \{\alpha\}$. Εἶναι σαφές ὅτι, γιὰ ὁποιοδήποτε $\alpha \in \mathbb{R}$ καὶ ὁποιοδήποτε $b \in \mathbb{Z}$, ἰσχύει $[b + \alpha] = b + [\alpha]$.

Ἐστω τώρα θετικὸς ἀκέραιος a , πρῶτος πρὸς τὸν p . Ἄν $1 \leq k \leq p'$, τότε

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

Ἄν v_k εἶναι τὸ ὑπόλοιπο τῆς εὐκλείδειας διαίρεσης τοῦ ak διὰ p , τότε, προφανῶς, $\left\{\frac{ak}{p}\right\} = \frac{v_k}{p}$ καὶ τὸ τελευταῖο κλάσμα εἶναι ἀριθμὸς τοῦ διαστήματος $[0, 0.5)$, ἢ τοῦ $(0.5, 1)$, ἀνάλογα μὲ τὸ ἂν $v_k \leq p/2$ ἢ $v_k > p/2$, ἀντιστοίχως. Ἄς παρατηρήσομε, ἐπίσης, ὅτι $v_k \leq p/2 \Leftrightarrow \sigma_k = 1$, ἐνῶ $v_k > p/2 \Leftrightarrow \sigma_k = -1$.

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

Ἄρα, συνδυάζοντας τὰ παραπάνω,

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

ὅποτε

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

Συνδυάζοντας αὐτὴ τὴ σχέση με τὴν (4.6) ὀδηγοῦμαστε στὸν πολὺ ἐνδιαφέροντα γενικὸ τύπο

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \lfloor \frac{2ak}{p} \rfloor}. \quad (4.7)$$

Με τὴ βοήθεια τοῦ τύπου (4.7) θὰ ἀποδείξουμε τὸν περίφημο νόμο τῆς τετραγωνικῆς ἀντιστροφῆς τοῦ Gauss καὶ τὸ συμπλήρωμα αὐτοῦ τοῦ νόμου, τὸ ὁποῖο καὶ θὰ ἀποδείξουμε πρῶτο, ὡς ἀπλούστερο.

Θεώρημα 4.2.2 –**Συμπλήρωμα τοῦ νόμου τετραγωνικῆς ἀντιστροφῆς.**

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

Συνεπῶς, τὸ 2 εἶναι τετραγωνικὸ ἰσοῦπόλοιπο μέτρω p γιὰ πρῶτους p τῆς μορφῆς $8n \pm 1$ καὶ τετραγωνικὸ ἀνισοῦπόλοιπο γιὰ πρῶτους p τῆς μορφῆς $8n \pm 3$.

Ἀπόδειξη Θεωροῦμε ἕναν ὁποιοδήποτε θετικὸ περιττὸ ἀκέραιο a , πρῶτο πρὸς τὸν p . Θὰ κάνουμε χρῆση τοῦ τύπου (4.7) γιὰ $\frac{a+p}{2}$ στὴ θέση τοῦ a . Ἐπίσης, θὰ κάνουμε χρῆση τῶν ἰδιοτήτων α' καὶ β' τοῦ θεωρήματος 4.2.1. Ἔχομε λοιπὸν,

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

Ἄν στὴν παραπάνω σχέση θέσουμε $a = 1$, τὸ πρῶτο ἄθροισμα στὸν ἐκθέτη τοῦ -1 (σχέση 4.9) εἶναι 0, ἀφοῦ $[k/p] = 0$ γιὰ $k = 1, \dots, p'$, 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 ἰσοῦπόλοιπο τῶν πρῶτων τῆς μορφῆς $8n \pm 1$ καὶ τετραγωνικὸ ἀνισοῦπόλοιπο τῶν πρῶτων τῆς μορφῆς $8n \pm 3$. **ὁ.ξ.δ.**

Θεώρημα 4.2.3 –**Νόμος τετραγωνικῆς ἀντιστροφῆς τοῦ Gauss.**

Ἄν p, q εἶναι διαφορετικοὶ περιττοὶ πρῶτοι, τότε

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

Συνεπῶς,

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

Άπόδειξη Θα αποδείξουμε την (4.10) υπό την εξής ισοδύναμη μορφή:

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

όπου, κατ' αναλογία με το p' , ορίζουμε $q' = \frac{q-1}{2}$.

Στηριζόμενοι στη σχέση (4.9) και την (4.8) παίρνουμε, για $a = q$,

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

καί, όμοια, εναλλάσσοντας τους ρόλους των p, q ,

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

Συνεπώς, για την απόδειξη της σχέσης (4.11) αρκεί ν' αποδειχθεί ότι

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

Η απόδειξη της σχέσης αυτής είναι πολύ απλή, αν της δώσουμε «γεωμετρική έρμηνεία». Κατ' αρχάς, σ' ένα όρθοκανονικό σύστημα άξόνων xOy , άς όρίσουμε ως *άκέραιο σημείο*, οποιοδήποτε σημείο έχει άκέραιες και τις δύο συντεταγμένες του και ως *θετικό άκέραιο σημείο*, οποιοδήποτε άκέραιο σημείο, το όποιο έχει και τις δύο συντεταγμένες του θετικές. Θεωρούμε τώρα την εϋθεία

$$\epsilon : y = \frac{q}{p}x. \quad (4.13)$$

Μία προκαταρκτική παρατήρηση είναι ότι, πάνω σε αυτή την εϋθεία δέν υπάρχει θετικό άκέραιο σημείο (x, y) με $x \leq p'$ και $y \leq q'$. βλ. άσκηση 8. Έστω θετικός άκέραιος k . Η «γεωμετρική έρμηνεία» της ποσότητας $\left[\frac{q}{p}k\right]$ είναι το πλήθος των θετικων άκεραίων σημείων, τα όποια βρίσκονται επί της εϋθείας $x = k$ και «κάτω από την εϋθεία» ϵ . βλ. άσκηση 9. Όμοίως, για θετικό άκέραιο ℓ , ή ποσότητα $\left[\frac{p}{q}\ell\right]$ δείχνει το πλήθος των θετικων άκεραίων σημείων, τα όποια βρίσκονται επί της εϋθείας $y = \ell$ και «άριστερά της εϋθείας» ϵ . βλ. άσκηση 10. Άρα, το άθροισμα στο άριστερό μέλος της σχέσης (4.11) έρμηνεύεται ως το πλήθος των θετικων άκεραίων σημείων έντός του όρθογωνίου παραλληλογράμμου, το όποιο ορίζεται από τους θετικούς ήμιάξονες και τις εϋθείες $x = p'$ και $y = q'$. βλ. άσκηση 11. Ένα τέτοιο σημείο, όμως, είναι της μορφής (x, y) με $x \in \{1, \dots, p'\}$ και $y \in \{1, \dots, q'\}$, άρα το πλήθος τους είναι $p'q'$ και αυτό ολοκληρώνει την απόδειξη της σχέσης (4.11).
ό.ξ.δ.

Ἀριθμητικὸ παράδειγμα. Ἐξετάζουμε ἂν ἡ ἰσοτιμία $x^2 \equiv 1054 \pmod{1811}$ ἔχει λύση, ὅπου ὁ ἀριθμὸς 1811 εἶναι πρῶτος. Στὸς παρακάτω ὑπολογισμοὺς, στὰ δεξιὰ κάθε ἰσότητος γράφεται ἡ ιδιότητα, τῆς ὁποίας ἔγινε χρῆση, γιὰ νὰ μεταβοῦμε ἀπὸ τὴν προηγούμενη ἰσότητα σὲ αὐτή. Ὅλοι οἱ ἀριθμοὶ στὸς «παρονομαστὲς» τῶν συμβόλων Legendre εἶναι πρῶτοι, ἄρα, σὲ κάποια βήματα ἐννοεῖται ὅτι γίνεται παραγοντοποίηση σὲ πρῶτους.

$$\begin{aligned}
 \left(\frac{1054}{1811}\right) &= \left(\frac{2}{1811}\right) \cdot \left(\frac{527}{1811}\right) && \text{(Θεώρημα 4.2.1-ε')} \\
 &= (-1) \left(\frac{527}{1811}\right) && \text{(Θεώρημα 4.2.2)} \\
 &= - \left(\frac{17}{1811}\right) \cdot \left(\frac{31}{1811}\right) && \text{(Θεώρημα 4.2.1-ε')} \\
 &= \left(\frac{1811}{17}\right) \cdot \left(\frac{1811}{31}\right) && \text{(Θεώρημα 4.2.3)} \\
 &= \left(\frac{9}{17}\right) \cdot \left(\frac{13}{31}\right) && \text{(Θεώρημα 4.2.1-β')} \\
 &= (+1) \left(\frac{13}{31}\right) && \text{(Θεώρημα 4.2.1-α')} \\
 &= \left(\frac{31}{13}\right) && \text{(Θεώρημα 4.2.3)} \\
 &= \left(\frac{5}{13}\right) && \text{(Θεώρημα 4.2.1-β')} \\
 &= \left(\frac{13}{5}\right) && \text{(Θεώρημα 4.2.3)} \\
 &= \left(\frac{-2}{5}\right) && \text{(Θεώρημα 4.2.1-β')} \\
 &= \left(\frac{-1}{5}\right) \cdot \left(\frac{2}{5}\right) && \text{(Θεώρημα 4.2.1-ε')} \\
 &= (+1)(-1) = -1 && \text{(Θεωρήματα 4.2.1-δ' καὶ 4.2.2)}
 \end{aligned}$$

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 φορές χρειάζεται νὰ γίνει παραγοντοποίηση, προκειμένου νὰ μπορέσει

νά προχωρήσει ή διαδικασία ύπολογισμοῦ, ὅπως, γιὰ παράδειγμα, ὅταν φτάνομε στὸ $\left(\frac{527}{1811}\right)$. Καὶ ἐδῶ μὲν, ὁ ἀριθμὸς 527 εἶναι μικρὸς, ὁπότε ή παραγοντοποίησή του δὲν μᾶς δημιουργεῖ ύπολογιστικὸ πρόβλημα, ἀλλὰ τί γίνεται ὅταν ἕνας ἀριθμὸς μὲ 100, ἄς ποῦμε, δεκαδικὰ ψηφία, ἐμφανίζεται στὸν «ἀριθμητῆ» τοῦ συμβόλου; Τὸ πρόβλημα τῆς παραγοντοποίησης ἑνὸς τέτοιου ἀριθμοῦ εἶναι, ἀπὸ ύπολογιστικὴ ἄποψη, πολὺ δύσκολο καί, μάλιστα, ἂν ὁ ἀριθμὸς ἔχει, ἀντὶ 100, 300 ψηφία, τότε, πολὺ πιθανὸν νὰ εἶναι καὶ ύπολογιστικῶς ἀνέφικτο. Ἡ παράκαμψη τῆς παραγοντοποίησης κατὰ τὴ διαδικασία ύπολογισμοῦ τοῦ συμβόλου Legendre ἐπιτυγχάνεται μὲ τὴ βοήθεια τοῦ συμβόλου Jacobi, τὸ ὁποῖο ἀποτελεῖ γενίκευση τοῦ συμβόλου Legendre.

Ἐστω $P = p_1 \cdots p_n$ ή ἀνάλυση τοῦ περιττοῦ ἀκεραίου P σὲ πρώτους παράγοντες. Οἱ p_1, \dots, p_n δὲν εἶναι, κατ' ἀνάγκη, διαφορετικοί. Γιὰ κάθε a πρώτο πρὸς τὸν P ὀρίζομε

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

καὶ τὸ ἀριστερὸ μέλος καλοῦμε *σύμβολο Jacobi τοῦ a ὡς πρὸς P* . Στὴν περίπτωση πού $P = p_1$, 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 ὅτι ὅλες οἱ ιδιότητες τοῦ συμβόλου Legendre, πλὴν τῆς γ' τοῦ θεωρήματος 4.2.1, ἰσχύουν καὶ γιὰ τὸ σύμβολο τοῦ Jacobi.

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

$$\beta'. \text{ Ἄν } a \equiv b \pmod{P}, \text{ τότε } \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right).$$

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

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

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

ϵ' . *Ἰσχύει ή γενίκευση τοῦ συμπληρώματος τοῦ νόμου τετραγωνικῆς ἀντιστροφῆς:*

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

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

ζ' . *Ἄν ὁ Q εἶναι περιττὸς καὶ $(P, Q) = 1$, τότε ἰσχύει ή 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,

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

Ἀπόδειξη Ἡ ἀπόδειξη τῶν α' , β' καὶ γ' ἔπεται ἀμέσως ἀπὸ τὸν ὀρισμὸ τοῦ συμβόλου Jacobi καὶ τῶν ἀντιστοίχων ἰδιοτήτων τοῦ συμβόλου Legendre.

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

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

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \equiv 1 + (a_1 + a_2 + \cdots + a_n) \begin{cases} \pmod{4} & \text{ἂν } 2|a_i \forall i \\ \pmod{16} & \text{ἂν } 4|a_i \forall i \end{cases} \quad (4.14)$$

διότι

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

καὶ στὸ δεξιὸ μέλος, ἐκτὸς ἀπὸ τὸ 1 καὶ τὸ πρῶτο ἄθροισμα, ὅλα τὰ ὑπόλοιπα ἄθροίσματα εἶναι πολλαπλάσια τοῦ 4, στὴν πρώτη περίπτωση καὶ πολλαπλάσια τοῦ 16 στὴ δεύτερη.

(δ') Μὲ τὴ βοήθεια τῆς σχέσης (4.14), τὴν ὁποία ἐφαρμόζουμε 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

$$\frac{P - 1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_n - 1}{2} \pmod{2}. \quad (4.15)$$

Κάνοντας χρῆση 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 (4.14), τὴν ὁποία ἐφαρμόζουμε γιὰ $a_i = p_i^2 - 1 \equiv 0 \pmod{4}$, ἔχομε

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

ἄρα¹

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

Κάνοντας χρήση αὐτῆς τῆς σχέσης καὶ τοῦ θεωρήματος 4.2.2, ἔχομε

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

(ζ') Θὰ ἀποδείξομε τὴν ισοδύναμη σχέση

$$(-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} = \left(\frac{Q}{P}\right) \cdot \left(\frac{P}{Q}\right), \quad (4.16)$$

βασισμένοι στὶς σχέσεις

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

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

Κάνοντας χρήση τῆς σχέσης (4.15) καὶ τῆς ὁμοίας 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,

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

ὁ.ξ.δ.

Ἀριθμητικὸ παράδειγμα. Ὑπολογίζομε ξανά τὸ $\left(\frac{1054}{1811}\right)$, δίχως νὰ καταφύγομε, σὲ κανένα βῆμα τοῦ ὑπολογισμοῦ, σὲ παραγοντοποίηση, ἐκτὸς ἀπὸ τὴν «ἐξαγωγή τοῦ 2». Αὐτὸ τὸ ἐπιτυγχάνομε μὲ χρήση τοῦ συμβόλου Jacobi. Τώρα, πλέον,

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

δὲν μᾶς ἐνδιαφέρει ἂν οἱ «παρονομαστές» τῶν συμβόλων εἶναι πρῶτοι ἀριθμοί. Φυσικά, σ' ἓνα παράδειγμα μὲ τόσο μικροὺς ἀριθμούς, αὐτὸ τὸ ὑπολογιστικὸ πλεονέκτημα τοῦ συμβόλου Jacobi –ἢ ἀποφυγὴ τῆς παραγοντοποίησης– δὲν δείχνει τόσο σημαντικό.

Στὸ δεξιότερο ἄκρο κάθε γραμμῆς σημειώνεται ποιά ἀπὸ τὶς ιδιότητες α'–ζ' τοῦ θεωρήματος 4.3.1 χρησιμοποιήθηκε.

$$\begin{aligned}
 \left(\frac{1054}{1811}\right) &= \left(\frac{2}{1811}\right) \cdot \left(\frac{527}{1811}\right) && (\gamma') \\
 &= (-1) \left(\frac{527}{1811}\right) && (\epsilon') \\
 &= \left(\frac{1811}{527}\right) && (\zeta') \\
 &= \left(\frac{230}{527}\right) && (\beta') \\
 &= \left(\frac{2}{527}\right) \cdot \left(\frac{115}{527}\right) && (\gamma') \\
 &= (+1) \left(\frac{115}{527}\right) && (\epsilon') \\
 &= - \left(\frac{527}{115}\right) && (\zeta') \\
 &= - \left(\frac{-48}{115}\right) && (\beta') \\
 &= - \left(\frac{-1}{115}\right) \cdot \left(\frac{16}{115}\right) \cdot \left(\frac{3}{115}\right) && (\gamma') \\
 &= \left(\frac{3}{115}\right) && (\delta'-\alpha') \\
 &= - \left(\frac{115}{3}\right) && (\zeta') \\
 &= - \left(\frac{1}{3}\right) && (\beta') \\
 &= -1 && (\alpha')
 \end{aligned}$$

Προσοχή! Ἄς ὑποθέσουμε ὅτι $\left(\frac{a}{p}\right) = -1$. Αὐτὸ συνεπάγεται ὅτι, γιὰ ἓνα, τουλάχιστον, πρῶτο παράγοντα τοῦ 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. Ἄν ὅμως $\left(\frac{a}{P}\right) = 1$ καὶ δὲν εἴμαστε βέβαιοι ὅτι ὁ P εἶναι πρῶτος, τότε δὲν μπορούμε νὰ συμπεράνομε ὅτι ἡ ἰσοτιμία $x^2 \equiv a \pmod{P}$ ἔχει λύση! Πράγματι, ἂν γιὰ ἄρτιο πλήθος περιττῶν πρῶτων παραγόντων p_i τοῦ P εἶναι $\left(\frac{a}{p_i}\right) = -1$, τότε,

ἐνῶ δὲν ἔχει λύση ἢ $x^2 \equiv a \pmod{P}$, εἶναι $\left(\frac{a}{P}\right) = 1$.

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

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 ἐξειδικεύσουμε τὸ πολυώνυμο $f(X)$ στὴν εἰδική, ἀλλὰ πολὺ ἐνδιαφέρουσα περίπτωση $f(X) = X^2 - b$.

Μέχρι τὸ τέλος τῆς παραγράφου, τὸ m συμβολίζει ἀκέραιο μεγαλύτερο τοῦ 1 καὶ

$$m = 2^a p_1^{a_1} \cdots p_k^{a_k} \quad (4.17)$$

εἶναι ἡ κανονικὴ ἀνάλυση τοῦ m σὲ πρώτους παράγοντες, ὅπου

- p_1, \dots, p_k εἶναι περιττοὶ πρώτοι.
- $a \geq 0, k \geq 0$, ἀλλὰ ἕνας, τουλάχιστον ἀπὸ τοὺς δύο εἶναι θετικός.

Θὰ ἀσχοληθοῦμε, λοιπόν, μὲ τὴν ἐπίλυση τῆς ἰσοτιμίας

$$x^2 \equiv b \pmod{m} \quad (4.18)$$

Χάρη στὴν ἄσκηση 17, ἂν $(b, m) > 1$, ἀναγόμεστε σὲ ὁμοιας μορφῆς ἰσοτιμία μὲ νέα b καὶ m , γιὰ τὴν ὁποία, εἴτε δὲν ὑπάρχει λύση, εἴτε ὁ νέος (b, m) εἶναι μικρότερος –ἀκριβέστερα, διαιρέτης– τοῦ ἀντίστοιχου προηγούμενου. Ἔτσι, βῆμα πρὸς βῆμα, ἂν δὲν καταλήξουμε σὲ ἀδύνατη ἰσοτιμία, θὰ φτάσουμε, ὕστερα ἀπὸ πεπερασμένο πλῆθος βημάτων, σὲ ἰσοτιμία (4.18), στὴν ὁποία $(b, m) = 1$.

Ἐπίσης, λόγῳ τοῦ *κινέζικου θεωρήματος* 3.3.1, γιὰ τὴν ἐπίλυση τῆς ἰσοτιμίας (4.18) πρέπει καὶ ἀρκεῖ νὰ μποροῦμε νὰ ἐπιλύουμε ἰσοτιμίες τῆς μορφῆς

$$x^2 \equiv b \pmod{p^a}, \quad p \text{ περιττός πρώτος, } a \geq 1, (b, p) = 1 \quad (4.19)$$

καθὼς καὶ ἰσοτιμίες τῆς μορφῆς

$$x^2 \equiv b \pmod{2^a}, \quad a \geq 1, b \text{ περιττός.} \quad (4.20)$$

Εἶναι ἀπλὸ νὰ ἀποδείξει κανεὶς ὅτι ἡ ἰσοτιμία (4.19) ἔχει ἀκριβῶς δύο λύσεις, ἢ καμία λύση, ἀνάλογα μὲ τὸ ἂν $\left(\frac{b}{p}\right) = 1$ ἢ -1 , ἀντιστοίχως· βλ. ἄσκηση 18.

Ἡ μελέτη τῆς ἰσοτιμίας (4.20) εἶναι πιὸ σύνθετη.

Θεώρημα 4.4.1 Ἀναφερόμαστε στὴν ἰσοτιμία (4.20).

Γιὰ $a = 1$, ἡ ἰσοτιμία ἔχει μίαν ἀκριβῶς λύση.

Γιὰ $a = 2$, ἡ ἰσοτιμία ἔχει λύση ἂν, καὶ μόνο ἂν, $b \equiv 1 \pmod{4}$. Ἄν ἰκανοποιεῖται αὐτὴ ἢ ἡ συνθήκη, τότε τὸ πλῆθος τῶν λύσεων τῆς ἰσοτιμίας εἶναι ἀκριβῶς 2.

Γιὰ $a \geq 3$, ἡ ἰσοτιμία ἔχει λύση ἂν, καὶ μόνο ἂν, $b \equiv 1 \pmod{8}$. Ἄν ἰκανοποιεῖται αὐτὴ ἢ ἡ συνθήκη, τότε τὸ πλῆθος τῶν λύσεων τῆς ἰσοτιμίας εἶναι ἀκριβῶς 4.

Ἐπιπλέον, στὴν περίπτωση αὐτή, ἂν $x_a \pmod{2^a}$ εἶναι μία λύση, τότε, οἱ τέσσερις διαφορετικὲς λύσεις εἶναι οἱ

$$x \equiv \pm x_a, \pm x_a + 2^{a-1} \pmod{2^a}. \quad (4.21)$$

Ἀπόδειξη Οἱ περιπτώσεις $a = 1, 2$ εἶναι τετριμμένες. Ἐστω, λοιπόν, $a \geq 3$. Ἄν ὑπάρχει ἀκέραιος x , πὺν νὰ ἰκανοποιεῖ τὴν ἰσοτιμία (4.20), τότε $x^2 \equiv b \pmod{8}$. 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 (4.20). Ἀντιστρόφως, ἔστω ὅτι $b \equiv 1 \pmod{8}$. Θὰ ἀποδείξομε ἐπαγωγικὰ ὅτι ἡ ἰσοτιμία (4.20) ἔχει λύση. Γιὰ $a = 3$, μία λύση εἶναι ἡ $1 \pmod{8}$. Ἄς ὑποθέσομε τώρα ὅτι γιὰ $a = k \geq 3$ ὑπάρχει λύση, ἔστω ἡ $x_k \pmod{2^k}$. Θέτομε $x = x_k + 2^{k-1}y$ καί, ἀντικαθιστώντας στὴν $x^2 \equiv b \pmod{2^{k+1}}$, ἔχομε

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

Ἐξ ὑποθέσεως, ὁ 2^k διαιρεῖ τὸν ἐντὸς παρενθέσεως ἀριθμὸ στοὺ ἀριστερὸ μέλος καί, ἀκόμη, $2k - 2 \geq k + 1$, ὁπότε ἡ παραπάνω ἰσοτιμία γίνεται

$$\frac{x_k^2 - b}{2^k} + x_k y \equiv 0 \pmod{2}.$$

Ἐπειδὴ ὁ x_k εἶναι περιττός, καταλήγομε, τελικὰ, στὴν

$$y \equiv \frac{b - x_k^2}{2^k} \pmod{2}.$$

Ἄρα, ἂν στὴν $x = x_k + 2^{k-1}y$ θέσομε $y = 0$ ἢ 1 , ἀναλόγως μὲ τὸ ἂν τὸ δεξιὸ μέλος τῆς παραπάνω ἰσοτιμίας εἶναι ἄρτιος ἢ περιττός ἀριθμὸς, ἀντιστοίχως, παίρνομε λύση τῆς ἰσοτιμίας $x^2 \equiv b \pmod{2^{k+1}}$.

Μένει τώρα νὰ δείξομε ὅτι, ἂν $a \geq 3$ καὶ $x_a \pmod{2^a}$ εἶναι μία λύση τῆς ἰσοτιμίας (4.20), τότε οἱ κλάσεις (4.21) εἶναι, ἐπίσης, λύσεις τῆς ἴδιας ἰσοτιμίας καί, μάλιστα, διαφορετικὲς καὶ κάθε ἀκέραιος x , πὺν ἐπαληθεύει τὴν ἰσοτιμία, ἀνήκει σὲ μία ἀπὸ αὐτὲς τὲς τέσσερις κλάσεις. Τὸ ὅτι οἱ κλάσεις αὐτὲς εἶναι λύσεις τῆς ἰσοτιμίας (4.20), μὲ δεδομένο ὅτι ἡ $x_a \pmod{2^a}$ εἶναι λύση τῆς, φαίνεται ὕστερα ἀπὸ λίγες ἀπλοῦστατες πράξεις. Ἀπλό, ἐπίσης, εἶναι νὰ δείξει κανεὶς ὅτι οἱ τέσσερις κλάσεις εἶναι διαφορετικὲς. Γιὰ παράδειγμα, ἂν ἦταν $x_a \equiv -x_a + 2^{a-1} \pmod{2^a}$, τότε θὰ ἔπρεπε $x_a \equiv 2^{a-2} \pmod{2^{a-1}}$ · ἀδύνατον, ἀφοῦ ὁ x_a εἶναι περιττός. Τὸ ἴδιο ἀπλὰ ἀποκλείεται ἡ ἰσότητα δύο ὁποιοῦνδήποτε κλάσεων (4.21).

Τέλος, ἂν $x^2 \equiv b \pmod{2^a}$ ($a \geq 3$) καὶ $x_a^2 \equiv b \pmod{2^a}$, τότε $(x + x_a)(x - x_a) \equiv 0 \pmod{2^a}$. Ἀπὸ τὴν ἄσκηση 8 τοῦ κεφαλαίου 1, ἀκριβῶς ἓνας ἀπὸ τοὺς δύο ἀκεραίους ἀριθμοὺς $(x + x_a)/2$ καὶ $(x - x_a)/2$ εἶναι περιττός. Ἄν εἶναι ὁ πρῶτος, τότε ὁ $x + x_a$ διαιρεῖται ἀπὸ τὸ 2, ἀλλὰ ὄχι ἀπὸ τὸ 4, συνεπῶς, ἡ τελευταία ἰσοτιμία μᾶς ὁδηγεῖ στοὺ συμπέρασμα ὅτι ὁ $x - x_a$ διαιρεῖται ἀπὸ τὸ 2^{a-1} . Ἄρα, $x = x_a + 2^{a-1}y$, ὁπότε $x \equiv x_a \pmod{2^a}$ ἢ $x \equiv x_a + 2^{a-1} \pmod{2^a}$, ἀνάλογα μὲ τὸ ἂν ὁ y εἶναι ἄρτιος

ή περιττός, αντίστοιχως.

Άν $\frac{x - x_a}{2}$ είναι περιττός, τότε, συλλογίζόμενοι με έντελως ανάλογο τρόπο, οδηγούμαστε στο συμπέρασμα ότι $x \equiv -x_a$ ή $-x_a + 2^{a-1} \pmod{2^a}$. **ὄ.ξ.δ.**

Στηριζόμενοι στο θεώρημα 4.4.1 και στο πρίν από την εκφώνησή του σχόλιο, μπορούμε να ξέρομε ακριβώς τὸ πλήθος τῶν λύσεων τῆς ἰσοτιμίας (4.18).

Θεώρημα 4.4.2 *Αναγκαία και ἰκανή συνθήκη για να ἔχει λύση ἡ ἰσοτιμία (4.18), ὅταν ἡ κανονικὴ ἀνάλυση τοῦ m δίδεται ἀπὸ τὴ σχέση (4.17), εἶναι να ἱκανοποιῶνται ὅλες οἱ παρακάτω συνθήκες:*

$$\left(\frac{b}{p_i}\right) = 1 \quad \text{για ὅλα τὰ } i = 1, \dots, k$$

$$b \equiv 1 \begin{cases} \pmod{4} & \text{ἂν } a = 2 \\ \pmod{8} & \text{ἂν } a \geq 3 \end{cases}$$

Στὴν περίπτωση, πὸν ἔχει λύση ἡ ἰσοτιμία, τὸ πλήθος τῶν λύσεῶν τῆς, εἶναι

$$2^k, \text{ ἂν } a = 0 \text{ ἢ } 1, \quad 2^{k+1}, \text{ ἂν } a = 2, \quad 2^{k+2}, \text{ ἂν } a \geq 3.$$

4.5 Ἀσκήσεις τοῦ κεφαλαίου 4

- Υπολογίστε ὅλα τὰ στοιχεῖα τοῦ κατ' ἀπόλυτη τιμὴ ἐλαχίστου συστήματος ὑπολοίπων μέτρῳ p , τὰ ὁποῖα εἶναι τετραγωνικὰ ἰσοϋπόλοιπα μέτρῳ p , για $p = 17$ καὶ $p = 19$, ἀντιστοίχως. Γιατὶ στὴ μία περίπτωση τὰ στοιχεῖα αὐτὰ εἶναι ἀνὰ ζεύγη ἀντίθετα καὶ στὴν ἄλλη ὄχι;
- Ἀποδείξτε τὴν ἐξῆς πολὺ ἀπλὴ, πρόταση, τῆς ὁποίας χρῆση γίνεται πολὺ συχνά: Ἄν $\epsilon, \eta \in \{-1, 1\}$ καὶ $\epsilon \equiv \eta \pmod{p}$, τότε $\epsilon = \eta$.
- Ἀποδείξτε τὴν πρόταση 4.1.1 βασιζόμενοι στὴν ἄσκηση 7 (β') τοῦ κεφαλαίου 3.
- Ἐστω $N = x^2 + y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξὺ τους. Ἀποδείξτε ὅτι ὅλοι οἱ πρῶτοι διαιρέτες τοῦ N εἶναι τῆς μορφῆς $4k + 1$.
- Ἐστω $N = x^2 - 2y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξὺ τους καὶ ὁ x εἶναι περιττός. Ἀποδείξτε ὅτι, ἂν ἕνας πρῶτος p διαιρεῖ τὸν N , τότε ὁ p εἶναι ἢ τῆς μορφῆς $8k + 1$ ἢ τῆς μορφῆς $8k + 7$.
- Ἐστω $N = x^2 + 2y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξὺ τους καὶ ὁ x εἶναι περιττός. Ἀποδείξτε ὅτι, ἂν ἕνας πρῶτος p διαιρεῖ τὸν N , τότε ὁ p εἶναι ἢ τῆς μορφῆς $8k + 1$ ἢ τῆς μορφῆς $8k + 3$.

7. Υπολογίστε την τιμή του συμβόλου $\left(\frac{7}{13}\right)$. Στη συνέχεια, για $p = 13$ και $a = 7$: Γράψτε τις σχέσεις (4.5) (6 ισοτιμίες mod 13), και επαληθεύστε τις σχέσεις (4.6) και (4.7).
Επαναλάβετε την άσκηση για $p = 19$ και $a = 5$.
8. Αν οι p, q είναι διαφορετικοί περιττοί πρώτοι, τότε δεν υπάρχουν άκεραιοι x, y , με $1 \leq x \leq p'$ και $1 \leq y \leq q'$, τέτοιοι ώστε $y = qx/p$.
9. Για $q = 23, p = 17$ και για κάθε $k = 1, 2, \dots, p' = 8$, χωριστά, επαληθεύστε τον ισχυρισμό στην απόδειξη του θεωρήματος 4.2.3 ότι $\left[\frac{q}{p}k\right]$ είναι το πλήθος των θετικών άκεραίων σημείων, τα όποια βρίσκονται επί της ευθείας $x = k$ και «κάτω από την ευθεία» (4.13).
10. Για $q = 23, p = 17$ και για κάθε $\ell = 1, 2, \dots, q' = 11$, χωριστά, επαληθεύστε τον ισχυρισμό στην απόδειξη του θεωρήματος 4.2.3 ότι $\left[\frac{p}{q}\ell\right]$ δείχνει το πλήθος των θετικών άκεραίων σημείων, τα όποια βρίσκονται επί της ευθείας $y = \ell$ και «αριστερά της ευθείας» (4.13).
11. Για $q = 23$ και $p = 17$ επαληθεύστε τον ισχυρισμό στην απόδειξη του θεωρήματος 4.2.3 ότι το άθροισμα στο αριστερό μέλος της σχέσης (4.11) ισούται με το πλήθος των θετικών άκεραίων σημείων εντός του ορθογωνίου παραλληλογράμμου, το όποιο ορίζεται από τους θετικούς ημίμαξονες και τις ευθείες $x = p'$ και $y = q'$.
12. Ο $p = 104779$ είναι πρώτος. Υπολογίστε την τιμή του συμβόλου $\left(\frac{a}{p}\right)$ για $a = 194, 120400, 18660, -14530, -1821000$ με χρήση του συμβόλου του Jacobi.
13. Αποδείξτε ότι, αν ο p είναι πρώτος > 3 , τότε $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Αποδείξτε μετά ότι ένας πρώτος p της μορφής $3k + 2$ δεν μπορεί να διαιρεί αριθμό της μορφής $x^2 + 3y^2$, όπου οι x, y είναι άκεραιοι και $(x, 3y) = 1$.
14. Έστω $P > 1$ περιττός. Έστω P_0 ο αριθμός, που σχηματίζεται από το γινόμενο όλων των διαφορετικών πρώτων διαιρετών του P , οι όποιοι εμφανίζονται με περιττό εκθέτη στην κανονική ανάλυση του P . Αποδείξτε ότι, για κάθε a πρώτο προς τον P , ισχύει $\left(\frac{a}{p}\right) = \left(\frac{a}{P_0}\right)$.
15. Έστω $P_0 = p_1 \cdots p_n$, όπου p_1, \dots, p_n είναι διαφορετικοί περιττοί πρώτοι. Αποδείξτε, με επαγωγή στο n , ότι υπάρχει b , τέτοιος ώστε $\left(\frac{b}{P_0}\right) = -1$.
Υπόδειξη. Για το επαγωγικό βήμα από το k στο $k + 1$, κάνετε το έξης: Έστω c , τέτοιος ώστε $\left(\frac{c}{p_1 \cdots p_k}\right) = -1$ και d , τέτοιος ώστε $\left(\frac{d}{p_{k+1}}\right) = 1$. Δείξτε ότι υπάρχει b , τέτοιος ώστε $b \equiv c \pmod{p_1 \cdots p_k}$ και $b \equiv d \pmod{p_{k+1}}$ και γι' αυτόν τον b , τότε, $\left(\frac{b}{p_1 \cdots p_k p_{k+1}}\right) = -1$.

16. Έστω $P > 1$ περιττός. Συνδυάστε τις δύο προηγούμενες ασκήσεις για να συμπεράνετε πρώτα ότι υπάρχει b , πρώτος προς τον P , τέτοιος ώστε $\left(\frac{b}{P}\right) = -1$ και, στη συνέχεια, αποδείξτε ότι, αν R είναι ένα περιορισμένο σύστημα υπολοίπων μέτρω P , τότε

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

Υπόδειξη. Το σύνολο $\{ab : a \in R\}$ είναι, επίσης, περιορισμένο σύστημα υπολοίπων. Αφ' ετέρου, το άθροισμα των συμβόλων Jacobi, καθώς ο «ἀριθμητής» του συμβόλου διατρέχει ένα περιορισμένο σύστημα υπολοίπων, δεν αλλάζει αν αντικαταστήσουμε αυτό το σύστημα με ένα άλλο περιορισμένο σύστημα υπολοίπων.

17. Έστω ότι έχουμε να λύσουμε την ισοτιμία $x^2 \equiv b \pmod{m}$ και οι b, m έχουν ένα κοινό πρώτο διαιρέτη p . Έστω $b = pb_1$, $m = pm_1$. Αποδείξτε ότι κάθε x , που ικανοποιεί την ισοτιμία, πρέπει να διαιρείται δια p και, μετά, θέστε $x = px_1$, οπότε η ισοτιμία θα αναχθεί στην $px_1^2 \equiv b_1 \pmod{m_1}$. Δείξτε τα εξής, σχετικά με την τελευταία ισοτιμία:

- (i) Αν $(p, m_1) = 1$, τότε αναγόμεστε σε ισοτιμία $x_1^2 \equiv b'_1 \pmod{m_1}$, όπου ο b'_1 είναι κάποιος άκεραιος με $(b'_1, m_1) = (b, m)/p$.
 (ii) Αν $(p, m_1) = p$ και $p|b_1$, τότε αναγόμεστε σε ισοτιμία $x_1^2 \equiv b_2 \pmod{m_2}$, όπου $b_2 = b_1/p$, $m_2 = m_1/p$ και $(b_2, m_2) = (b, m)/p^2$.
 (iii) Αν $(p, m_1) = p$ και ο p δεν διαιρεί τον b_1 , τότε η ισοτιμία είναι αδύνατη.

18. (α') Έστω περιττός πρώτος p , b άκεραιος πρώτος προς τον p και $a \geq 1$. Κάνοντας χρήση του θεωρήματος 3.4.2, αποδείξτε ότι η ισοτιμία $x^2 \equiv b \pmod{p^a}$ έχει ακριβώς δύο λύσεις, αν $\left(\frac{b}{p}\right) = 1$ και καμία λύση, αν $\left(\frac{b}{p}\right) = -1$.

(β') Έστω $m > 1$ και $m = p_1^{a_1} \cdots p_k^{a_k}$ ή κανονική ανάλυση του m . Έστω b άκεραιος πρώτος προς τον m . Κάνοντας χρήση του α' μέρους αυτής της άσκησης, αποδείξτε ότι, αναγκαία και ικανή συνθήκη για να έχει λύση η ισοτιμία $x^2 \equiv b \pmod{m}$ είναι: $\left(\frac{b}{p_i}\right) = 1 \forall i = 1, \dots, k$.

Στη συνέχεια, κάνοντας χρήση του κινέζικου θεωρήματος, αποδείξτε ότι, αν ικανοποιείται αυτή η συνθήκη, τότε το πλήθος των λύσεων της θεωρούμενης ισοτιμίας είναι 2^k .

19. Έχοντας υπ' όψη την άσκηση 18, λύστε κάθε μία από τις παρακάτω ισοτιμίες:

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

20. Επιλύστε την ισοτιμία $x^2 \equiv 17 \pmod{2^{13}}$.

Κεφάλαιο 5

Γεννήτορες και διακριτοί λογάριθμοι

Στό κεφάλαιο αυτό, τὸ p συμβολίζει πάντα περιττὸ πρῶτο.
Τὰ λατινικὰ γράμματα συμβολίζουν πάντα ἀκεραίους

5.1 Γεννήτορες

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

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

Οἱ βασικὲς ιδιότητες τῆς συνάρτησης ord_m περιλαμβάνονται στὴν παρακάτω πρόταση.

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

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

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 μέτρω m καὶ κάθε δύναμη τοῦ a (μὴ ἀρνητικοῦ ἐκθέτη) εἶναι ἰσότιμη μέτρω m μὲ κάποιον ἀπὸ αὐτοὺς τοὺς r τὸ πλήθος ἀριθμοῦς.

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

ὅτι ὁ r δὲν μπορεῖ νὰ εἶναι θετικός. Ἄρα, $r = 0$, ὁπότε $r|k$.

β'. Ἐστω $k \geq \ell$, 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'. Ἄν ἦταν $a^k \equiv a^\ell \pmod{m}$ μὲ $0 \leq k < \ell \leq r - 1$, τότε, σύμφωνα μὲ τὸ (β') θὰ εἴχαμε $r|(\ell - k)$, πὺν εἶναι ἀδύνατον, ἀφοῦ $1 \leq \ell - k < r$. Τέλος, ἔστω $k \geq 0$. Εἶναι $k \equiv i \pmod{r}$ γιὰ κάποιον $i \in \{0, 1, \dots, r - 1\}$ ἄρα, ἀπὸ τὸ β', $a^k \equiv a^i \pmod{m}$.

ὁ.ξ.δ.

Ἄν $\text{ord}_m(a) = \phi(m)$, τότε ὁ a χαρακτηρίζεται ὡς γεννήτορας μέτρω m .

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

Ἀπόδειξη Ἐστω ὅτι ὁ a εἶναι γεννήτορας μέτρω m , ὁπότε $\text{ord}_m(a) = \phi(m)$. 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 μέτρω m καὶ τὸ πλήθος τους εἶναι $\phi(m)$, συνεπῶς ἀποτελοῦν περιορισμένο σύστημα ὑπολοίπων μέτρω m .

Ἀντιστρόφως, ἔστω ὅτι οἱ $\phi(m)$ τὸ πλήθος ἀριθμοὶ $a, a^2, \dots, a^{\phi(m)}$ ἀποτελοῦν περιορισμένο σύστημα ὑπολοίπων μέτρω m . εἰδικώτερα, οἱ $\phi(m)$ τὸ πλήθος αὐτὲς δυνάμεις εἶναι ἀνισότιμες μέτρω m . Ἐστω τώρα ὅτι $\text{ord}_m(a) = r$. 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 πλήθος δυνάμεις τοῦ a (μὴ ἀρνητικοῦ ἐκθέτη) ἀνισότιμες μέτρω m , ἄρα, ἀπὸ τὴν παρατήρηση λίγες γραμμὲς παραπάνω, $\phi(m) \leq r$, ὁπότε $r = \phi(m)$. **ὁ.ξ.δ.**

Θεώρημα 5.1.3 α'. Γιὰ κάθε a πρῶτο πρὸς τὸν m καὶ κάθε θετικό ἀκέραιο k ἰσχύει

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

β'. Ἄν ὁ g εἶναι γεννήτορας μέτρω m , τότε ὅλοι οἱ ἀριθμοὶ g^k μὲ $1 \leq k \leq \phi(m)$ καὶ $(k, \phi(m)) = 1$ εἶναι, ἐπίσης, γεννήτορες μέτρω m , ἀνισότιμοι μεταξύ τους καὶ κάθε γεννήτορας μέτρω m εἶναι ἰσότιμος μὲ ἓναν ἀπὸ αὐτοὺς τοὺς ἀριθμοὺς. Συνεπῶς, ὑπάρχουν ἀκριβῶς $\phi(\phi(m))$ τὸ πλήθος ἀνισότιμοι γεννήτορες μέτρω m .

Ἀπόδειξη α'. Ἐστω $\text{ord}_m(a) = n$. Γιὰ κάθε θετικό ἀκέραιο ℓ , πὺν 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 $\text{ord}_m(a^k) = r$, τότε $kr = [k, n] = (\text{θεώρημα 1.3.1-α}') \frac{kn}{(k, n)}$, ἀπ' ὅπου ἡ ἀποδεικτέα σχέση $r = \frac{n}{(n, k)}$.

β'. Ἐνας ἀκέραιος b εἶναι γεννήτορας μέτρω m ἂν, καὶ μόνο ἂν, εἶναι πρῶτος πρὸς τὸν m καὶ ἡ τάξη του μέτρω m εἶναι $\phi(m)$. Βάσει τοῦ θεωρήματος 5.1.2, ἡ συνθήκη αὐτὴ ἰσοδυναμεῖ μὲ τὸ ὅτι ὁ b εἶναι ἰσότιμος μέτρω m μὲ κάποιον ἀριθμὸ g^k , ὅπου $1 \leq k \leq \phi(m)$ καὶ ἡ τάξη τοῦ g^k μέτρω m εἶναι $\phi(m)$. Βάσει τοῦ (α'),

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

Άρα, $\text{ord}_m(g^k) = \phi(m)$ αν, και μόνο αν, ϕ k είναι πρώτος προς τον $\phi(m)$.

Ανακεφαλαιώνοντας τα παραπάνω έχουμε ότι, ϕ b είναι γεννήτορας μέτρω m αν, και μόνο αν, είναι ισότιμος μέτρω m με έναν αριθμό g^k , όπου $1 \leq k \leq \phi(m)$ και $(k, \phi(m)) = 1$. Επιπλέον, από το θεώρημα 5.1.2, όλοι οι τέτοιοι αριθμοί g^k – το πλήθος τους, προφανώς, είναι $\phi(m)$ – είναι ανισότιμοι μέτρω m . **ὁ.ξ.δ.**

Θεώρημα 5.1.4 Για τὰ a και b , παρακάτω, υποθέτουμε ότι οί a, b είναι πρώτοι προς τὸ μέτρο $m > 1$ και $\text{ord}_m(a) = r$, $\text{ord}_m(b) = s$.

α'. Αν $(r, s) = 1$, τότε, $\text{ord}_m(ab) = rs$.

β'. Υπάρχει c με $\text{ord}_m(c) = [r, s]$ (=ΕΚΠ τῶν r, s).

γ'. Υπάρχει γεννήτορας μέτρω p για κάθε περιττὸ πρώτο p .

Ἀπόδειξη Θὰ κάνουμε συχνή χρήση τοῦ θεωρήματος 5.1.1 χωρίς ιδιαίτερη μνεία.

α'. Ἐστω $\text{ord}_m(ab) = t$. Ἐστω, επίσης, b_1 τέτοιος ὥστε $bb_1 \equiv 1 \pmod{m}$. Ἡ ἄσκηση 1 μᾶς λέει ὅτι $\text{ord}_m(b_1) = s$. Ἀπὸ τὴν $(ab)^t \equiv 1 \pmod{m}$ παίρνουμε ἀμέσως $a^t \equiv b_1^t \pmod{m}$. Ἐστω $c \equiv a^t \equiv b_1^t \pmod{m}$. Ἀπὸ τὸ θεώρημα 5.1.3 συμπεραίνομε ὅτι $\text{ord}_m(c) = \text{ord}_m(a^t) = \frac{r}{(r,t)}$, καθὼς ἐπίσης και $\text{ord}_m(c) = \text{ord}_m(b_1^t) = \frac{s}{(s,t)}$. Ἐξισώνοντας, παίρνουμε $r(s,t) = s(r,t)$, ἄρα $r|s(s,t)$. Ἐπειδὴ $(r, s) = 1$, ἔπεται ὅτι $r|(r,t)$, ἄρα $r|t$. Ἐντελῶς ἀνάλογα, $s|t$, ὁπότε (γ' τοῦ θεωρήματος 1.3.1) $rs|t$. Ἀπὸ τὸ ἄλλο μέρος, ὁμως, $(ab)^{rs} = (a^r)^s(b^s)^r \equiv 1^s \cdot 1^r \equiv 1 \pmod{m}$, ἄρα $t|rs$, ὁπότε, τελικά, $t = rs$.

β'. Για τὴν ἀπόδειξη θὰ κάνουμε χρήση τῶν ἐκθετῶν, στοὺς ὁποίους ἀναφερθήκαμε ἀμέσως μετὰ τὸ θεώρημα 1.4.3. Για ἀπλούστευση τοῦ συμβολισμοῦ θὰ γράφομε ord ἀντὶ ord_m . Τὸν τυπικὸ (θετικὸ) πρώτο ἀριθμὸ θὰ συμβολίζομε με q και τὸ σύμβολο $v_q(x)$ ὑπενθυμίζομε ὅτι σημαίνει τὸν ἐκθέτη τοῦ q στὸν x .

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

Θέτομε

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

και

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

Εἶναι προφανές ὅτι, για κανένα q δὲν ἔχομε συγχρόνως $\mu(q) > 0$ και $\nu(q) > 0$, ἄρα $(r_0, s_0) = 1$. Ἐπίσης, $\mu(q) + \nu(q) = \max\{v_q(r), v_q(s)\}$, ἄρα, ἀπὸ τὴν ἄσκηση 31 τοῦ κεφαλαίου 1 ἔπεται ὅτι $r_0 s_0 = [r, s]$. Εἶναι ἐπίσης προφανές ἀπὸ τὸν ὀρισμὸ τοῦ r_0 ὅτι $r_0|r$, ὁπότε ἂς θέσομε $r = r_0 r_1$ για κάποιον $r_1 \in \mathbb{N}$. Ἀνάλογα, θέτομε $s = s_0 s_1$, ὅπου $s_1 \in \mathbb{N}$. Ἀπὸ τὸ (α') τοῦ θεωρήματος 5.1.3 ἔπεται ὅτι $\text{ord}(a^{r_1}) = \frac{r}{(r, r_1)} = \frac{r}{r_1} = r_0$ και, ἀνάλογα, $\text{ord}(b^{s_1}) = s_0$. Ἐπειδὴ, τώρα, $(r_0, s_0) = 1$, τὸ (α') μᾶς λέει ὅτι $\text{ord}(a^{r_1} b^{s_1}) = r_0 s_0 = [r, s]$.

γ'. Ἐστω r ἡ μέγιστη δυνατὴ τάξη μέτρω p , δηλαδή, ὑπάρχει ἀκέραιος g με $\text{ord}_p(g) = r$, ἐνῶ $\text{ord}_p(b) \leq r$ για κάθε $b \in \mathbb{Z}$. Προφανῶς $r \leq p - 1$. Ἰσχυρίζομαστε τώρα ὅτι ἡ τάξη μέτρω p ὁποιουδήποτε ἀκεραίου διαιρεῖ τὸν r . Πράγματι, ἔστω

$\text{ord}_p(b) = s$ και ἄς ὑποθέσουμε 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 ὁποῖου ἡ τάξι μέρω p εἶναι ἴση μὲ $[r, s] > r$, ἄτοπο. Συμπεραίνομε, λοιπόν, ὅτι οἱ τάξεις τῶν $1, 2, \dots, p-1$ μέρω p εἶναι διαιρέτες τοῦ r . Αὐτό, προφανῶς, συνεπάγεται ὅτι ἡ ἰσοτιμία $x^r - 1 \equiv 0 \pmod{p}$ 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 $p-1 = r = \text{ord}_p(g)$, ὁπότε ὁ g εἶναι γεννήτορας μέρω p . **ὁ.ξ.δ.**

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

β' Ἐάν ὁ g εἶναι γεννήτορας μέρω p καὶ $g^{p-1} \not\equiv 1 \pmod{p^2}$, τότε ὁ g εἶναι γεννήτορας μέρω p^n γιὰ κάθε $n > 1$.¹

γ' Ἐάν $n \geq 1$ καὶ ὁ g εἶναι γεννήτορας μέρω p^n , τότε γεννήτορας μέρω $2p^n$ εἶναι ἐκεῖνος ἀπὸ τοὺς g καὶ $g + p^n$, ὁ ὁποῖος εἶναι περιττός.

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

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

ὅπου ὁ b_1 εἶναι κάποιος ἀκέραιος, τοῦ ὁποῖου ἡ τιμὴ δὲν μᾶς ἐνδιαφέρει. Ἄρα, $(g + px)^{p-1} = 1 + p(c + (p-1)g^{p-2}x + pb_1)$ καὶ ἂν $k \pmod{p}$ εἶναι ἡ λύση τῆς ἰσοτιμίας $(p-1)g^{p-2}x \equiv 1 - c \pmod{p}$, τότε $c + (p-1)g^{p-2}k = 1 + pb_2$ γιὰ κάποιον $b_2 \in \mathbb{Z}$, 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 $v \geq 1$ ἰσχύει μία σχέση τῆς μορφῆς

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

Γιὰ $v = 1$:

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

καὶ κάθε προσθετός στοῦ τελευταῖο ἄθροισμα \sum εἶναι πολλαπλάσιο τοῦ p^3 , διότι κάθε διωνυμικός συντελεστής στοῦ ἄθροισμα αὐτὸ εἶναι πολλαπλάσιο τοῦ p (ἄσκηση 32 τοῦ κεφαλαίου 1). Ἄρα, τὸ δεξιὸ μέλος τῆς παραπάνω σχέσης εἶναι τῆς μορφῆς $1 + p^2\ell_2$, ὅπου $\ell_2 = \ell + \{\text{ὄροι διαιρετοὶ διὰ } p\} \not\equiv 0 \pmod{p}$.

Γιὰ $v = 2$:

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

¹Στὴν 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 Σ εἶναι πολλαπλάσιο τοῦ p^4 . Ἄρα, τὸ δεξιὸ μέλος τῆς παραπάνω σχέσης εἶναι τῆς μορφῆς $1 + p^3\ell_3$, ὅπου $\ell_3 = \ell_2 + \{\text{ὄροι διαιρετοὶ διὰ } p\} \not\equiv 0 \pmod{p}$.

Ἡ ἐπαγωγικὴ ἀπόδειξη τῆς σχέσης (5.1) εἶναι τώρα ξεκάθαρη. Μὲ τὴ βοήθεια τῆς σχέσης αὐτῆς μποροῦμε νὰ ἀποδείξουμε ὅτι ὁ $g + pk$ εἶναι γεννήτορας μέτρω p^μ γιὰ κάθε $\mu \geq 1$. Κατ' ἀρχάς, ἄς κάνουμε τὴν ἀπλὴ παρατήρηση ὅτι, ἀφοῦ ὁ g εἶναι γεννήτορας μέτρω p , τὸ ἴδιο θὰ ἰσχύει καὶ γιὰ τὸν $g + pk$, ὁπότε ἡ τάξη τοῦ $g + pk$ μέτρω p εἶναι $p - 1$. Ἔστω τώρα ὅτι $\text{ord}_{p^\mu}(g + pk) = r$. Ἡ σχέση $(g + pk)^r \equiv 1 \pmod{p^\mu}$ συνεπάγεται τὴν $(g + pk)^r \equiv 1 \pmod{p}$ ἄρα, ἀφοῦ ἡ τάξη τοῦ $g + pk$ μέτρω 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 κάποιον $\nu \leq \mu - 1$. 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 εἶχαμε $(g + pk)^r = (g + pk)^{p^\nu(p-1)} \not\equiv 1 \pmod{p^\mu}$, πού ἀντιφάσκει μὲ τὸν ὀρισμὸ τοῦ r . Συνεπῶς, $\nu = \mu - 1$ καὶ $r = (p - 1)s = (p - 1)p^\nu = (p - 1)p^{\mu-1} = \phi(p^\mu)$, πού λέει, ἀκριβῶς, ὅτι ὁ $g + pk$ εἶναι γεννήτορας μέτρω p^μ .

β'. Λόγω 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'. Ἄν ὁ g εἶναι γεννήτορας μέτρω p^n , τὸ ἴδιο ἰσχύει, προφανῶς καὶ γιὰ τὸν $g + p^n$ καὶ ἕνας, ἀκριβῶς, ἀπὸ τοὺς δύο εἶναι περιττός ἀριθμὸς, τὸν ὁποῖο ἄς συμβολίσουμε μὲ g_1 . Εἶναι, ἐπίσης, $\phi(2p^n) = \phi(p^n) = (\text{ἔστω}) e$. 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 πού ἀντιφάσκει μὲ τὸ γεγονὸς ὅτι g_1 εἶναι γεννήτορας μέτρω p^n . Συνεπῶς, $\text{ord}_{2p^n}(g_1) = e = \phi(2p^n)$, δηλαδή, ὁ g_1 εἶναι, ἐπίσης, γεννήτορας μέτρω $2p^n$. **ὁ.ξ.δ.**

Σχόλιο. Ἐνα ἐπιπόλαιον κοίταγμα τοῦ θεωρήματος 5.1.5-α' δίνει τὴν ἐντύπωση ὅτι, γιὰ νὰ ὑπολογίσει κανεὶς ἕνα γεννήτορα μέτρω p^n ἢ $2p^n$, ὅταν ξέρει ἕνα γεννήτορα μέτρω p , πρέπει νὰ ὑπολογίσει τὸν τεράστιον ἀριθμὸν g^{p-1} . Λανθασμένη ἐντύπωση! Ἡ ἄσκηση 4 μᾶς λέει ὅτι, ἀρκεῖ νὰ ὑπολογίσει κανεὶς, ὅχι αὐτὸν, καθ' ἑαυτὸν, τὸν ἀριθμὸν g^{p-1} , ἀλλὰ τὴν κλάση του μέτρω p^2 καὶ ἕνα τέτοιο ἐγχείρημα, βέβαια, δὲν εἶναι δύσκολο (δὲς παράγραφο 2.3 τοῦ κεφαλαίου 2).

Μέχρι στιγμῆς ἔχομε δεῖξει ὅτι, γιὰ $m = p^n, 2p^n$, μὲ p περιττὸ πρῶτον καὶ $n \geq 1$, ὑπάρχουν γεννήτορες μέτρω m . Ἐπίσης, εἶναι φανερό ὅτι, μέτρω 2 καὶ μέτρω 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 ἐξῆς ὑποτίθενται: Ἄν $k = 1$, τότε $b \geq 2$ · ἂν $b = 0$ ἢ 1, τότε $k \geq 2$. Τότε, γιὰ κάθε a πρῶτον πρὸς τὸν m ἰσχύει

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

γ'. Για $m = 2, 4, p^n, 2p^n$, όπου p περιττός πρώτος και $n \geq 1$, υπάρχουν γεννήτορες μέτρω m . Για $m > 1$, που δεν είναι της παραπάνω μορφής, δεν υπάρχουν γεννήτορες μέτρω m .

Άποδειξη α'. Η απόδειξη γίνεται επαγωγικά. Για $b = 3$ ή αποδεικτέα γίνεται $a^2 \equiv 1 \pmod{8}$, που ισχύει. Έστω ότι ισχύει για $b = k$, τότε μπορούμε να γράψουμε $a^{2^{k-2}} = 1 + 2^k t$ για κάποιον άκεραίο t . Υψώνοντας στο τετράγωνο τα δύο μέλη παίρνουμε $a^{2^{k-1}} = 1 + 2^{k+1}t + 2^{2k}t^2 \equiv 1 \pmod{2^{k+1}}$.

β'. Βάσει του α' του θεωρήματος 2.2.3 έχουμε

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

Στο γινόμενο \prod εμφανίζεται τουλάχιστον ένας παράγων $\phi(p_i^{b_i}) = (p_i - 1)p_i^{b_i-1}$, που είναι άρτιος αριθμός, άρα ο $\phi(m)/2$ είναι άκεραίος.

Αποδεικνύομε πρώτα ότι ο

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

είναι άκεραίος. Αν $b \geq 2$, τότε ο αριθμός $\frac{1}{2} \phi(2^b) = 2^{b-2}$ είναι άκεραίος. Αν $b = 0$ ή 1 , τότε, έξ υποθέσεως, $k \geq 2$ άρα στο γινόμενο \prod εμφανίζεται ο παράγων $\phi(p_2^{b_2})$, ο οποίος είναι άρτιος, καθώς είδαμε παραπάνω. Και στις δύο περιπτώσεις, λοιπόν, ο c είναι άκεραίος.

Έστω τώρα g ένας γεννήτορας μέτρω $p_1^{b_1}$. Επειδή $(a, p_1^{b_1}) = 1$, συμπεραίνομε ότι υπάρχει s , τέτοιος ώστε $a \equiv g^s \pmod{p_1^{b_1}}$. 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' αναλογία, $a^{\phi(m)/2} \equiv 1 \pmod{p_i^{b_i}}$ για όλα τα $i = 1, \dots, k$. Ύστερα από το συμπέρασμα αυτό, το μόνο που μας μένει για ν' αποδείξομε ότι $a^{\phi(m)/2} \equiv 1 \pmod{m}$, είναι ότι $a^{\phi(m)/2} \equiv 1 \pmod{2^b}$. Για $b = 0$ δεν έχουμε τίποτε να αποδείξομε. Αν $b \geq 1$, ο a είναι περιττός, αφού $(a, m) = 1$. Για $b = 1$, αποδεικτέα σχέση είναι η τετριμμένη ισοτιμία $a^{\phi(m)/2} \equiv 1 \pmod{2}$. Για $b = 2$, $\phi(m)/2 = \prod_{i=1}^k \phi(p_i^{b_i})$ και κάθε παράγων αυτού του γινομένου (υπάρχει τουλάχιστον ένας) είναι άρτιος. Άρα, $\phi(m)/2 = 2e$, $e \in \mathbb{Z}$ και αποδεικτέα σχέση είναι η $a^{2e} \equiv 1 \pmod{4}$, ή όποια ισχύει, αφού $a^2 \equiv 1 \pmod{4}$. Για $b \geq 3$ ο $\phi(m)/2$ είναι πολλαπλάσιο του 2^{b-2} , και η αποδεικτέα σχέση έπεται άμέσως από το (α').

γ'. Ο 1 είναι γεννήτορας μέτρω 2 και ο 3 είναι γεννήτορας μέτρω 4 . Το γ του θεωρήματος 5.1.4 και το γ του θεωρήματος 5.1.5 συνεπάγονται την ύπαρξη γεννήτορα μέτρω m όταν $m = p^n$ ή $2p^n$ με p περιττό πρώτο και $n \geq 1$. Όταν ο m δεν έχει μία από αυτές τις μορφές, τότε, ή $m = 2^b$ με $b \geq 3$, ή ο m είναι όπως στο (β'). Και στις δύο περιπτώσεις ισχύει ότι, για κάθε a πρώτο προς τον

m , $a^{\phi(m)/2} \equiv 1 \pmod{m}$ (παρατηρήστε ὅτι $\phi(2^b)/2 = 2^{b-2}$), ἄρα κάθε ἀκέραιος a πρῶτος πρὸς τὸν m ἔχει τάξη μέτρω m , τὸ πολὺ, $\phi(m)/2$ καί, συνεπῶς, δὲν μπορεῖ νὰ εἶναι γεννήτορας μέτρω m . **ὀ.ξ.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 μέτρω m καὶ ἔστω g ἓνας ἀπὸ αὐτούς. Ἐστω a πρῶτος πρὸς τὸν m . Ἀπὸ τὸ θεώρημα 5.1.2 συμπεραίνομε ὅτι ὑπάρχει ἓνας μοναδικὸς $k \in \{0, 1, \dots, \phi(m) - 1\}$, τέτοιος ὥστε $a \equiv g^k \pmod{m}$. Ὁ k αὐτὸς συμβολίζεται $\text{ind}_g(a)$ καὶ λέγεται *διακριτὸς λογάριθμος τοῦ a μέτρω m , ὡς πρὸς βάση g* . Συνήθως παραλείπομε τοὺς προσδιορισμοὺς «μέτρω m » καὶ «ὡς πρὸς βάση g ». Προτιμοῦμε τὸν συμβολισμό ind ἀντὶ τοῦ \log διότι, ἀφ' ἑνός, ὑπάρχει κάποιος κίνδυνος συγχύσεως μὲ τὸν συνήθη λογάριθμο καί, ἀφ' ἑτέρου, γιατί ἡ χρήση τοῦ συμβολισμοῦ ind ἔχει ἀρκετὰ μακρὰ παράδοση στὴ Θεωρία Ἀριθμῶν.

Ἐξ ὀρισμοῦ, λοιπόν,

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

Θεώρημα 5.2.1 Ἐστω g γεννήτορας μέτρω m . Παρακάτω, τὰ a, b συμβολίζουν ἀκεραίους πρώτους πρὸς τὸν m . Γιὰ ἀπλούστευση τοῦ συμβολισμοῦ, στὰ (α')-(ζ') καὶ στὶς ἀποδείξεις τους γράφουμε ind ἀντὶ ind_g .

α'. $a \equiv b \pmod{m} \Leftrightarrow \text{ind}(a) = \text{ind}(b)$.

β'. Ἡ ἰσοτιμία $a^n \equiv 1 \pmod{m}$ ἰσοδυναμεῖ μὲ τὴν $n \text{ind}(a) \equiv 0 \pmod{\phi(m)}$.

γ'. $\text{ind}(ab) \equiv \text{ind}(a) + \text{ind}(b) \pmod{\phi(m)}$.

δ'. $\text{ind}(a^n) \equiv n \text{ind}(a) \pmod{\phi(m)}$.

ε'. $\text{ind}(1) = 0$ καὶ $\text{ind}(g) = 1$.

ζ'. $\text{ind}(-1) = \phi(m)/2$.

ζ'. Ἄν g_1 εἶναι γεννήτορας μέτρω m , τότε

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

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

Προχωροῦμε τώρα στὴν ἀπόδειξη τῶν διαφορῶν προτάσεων τοῦ θεωρήματος.

α'. Ἐστω $\text{ind}(a) = k$ καὶ $\text{ind}(b) = \ell$. 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 $0 \leq |k - \ell| < \phi(m)$, ἄρα $k = \ell$.

β'. Ἐστω $\text{ind}(a) = k$. 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'. $g^{\text{ind}(a)+\text{ind}(b)} = g^{\text{ind}(a)} g^{\text{ind}(b)} \equiv ab \equiv g^{\text{ind}(ab)} \pmod{m}$ καὶ ἡ ἀποδεικτέα προκύπτει τώρα μὲ ἐφαρμογὴ τοῦ θεωρήματος 5.1.1-β', λαμβάνοντας ὑπ' ὄψιν ὅτι $\text{ord}_m(g) = \phi(m)$.

δ'. Ἡ πρόταση (γ'), ποὺ μόλις ἀποδείξαμε, γενικεύεται μὲ προφανῆ ἐπαγωγὴ, ὡς ἐξῆς: $\text{ind}(a_1 \cdots a_n) \equiv \text{ind}(a_1) + \cdots + \text{ind}(a_n) \pmod{\phi(m)}$. Γιὰ $a_1 = \cdots = a_n = a$ παίρνομε τὴν ἀποδεικτέα.

ε'. Τετριμμένη συνέπεια τῆς σχέσης (5.2).

ζ'. Θέτομε $m = 2^j p^n$, ὅπου $j \in \{0, 1\}$, ὅποτε, 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, ὅποτε ἡ τελευταία ἰσοτιμία γράφεται ἰσοδύναμα ὡς

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

Ἀλλὰ, προφανῶς, ὁ 2^j διαιρεῖ καὶ τοὺς δύο παράγοντες στὰ δεξιά, ἐνῶ ὁ p ἀποκλείεται νὰ διαιρεῖ καὶ τοὺς δύο συγγρόνους. Ἄρα, ὁ $m = 2^j p^n$ διαιρεῖ ἢ τὸν ἕνα ἢ τὸν ἄλλο παράγοντα. Ἄν διαιροῦσε τὸν $g^{\phi(m)/2} - 1$, τότε θὰ ἐρχόμαστε σὲ ἀντίφαση μὲ τὸ ὅτι ὁ g εἶναι γεννήτορας μέτρω m . Ἄρα ὁ m διαιρεῖ τὸν ἄλλο παράγοντα,

δηλαδή, $g^{\phi(m)/2} \equiv -1 \pmod{m}$, πού σημαίνει, $\text{ind}(-1) = \phi(m)/2$.

ζ'. Θέτομε $\text{ind}_g(a) = n$, $\text{ind}_{g_1}(a) = k$, $\text{ind}_g(g_1) = \ell$, όποτε ἔχομε

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

Συνδυάζοντας τις δύο τελευταίες παίρνομε $g^{k\ell} \equiv a \pmod{m}$, ή όποία, σέ συνδυασμό με την πρώτη, μάς δίνει $g^{k\ell} \equiv g^n \pmod{m}$. Ἡ τελευταία ισοδυναμεῖ με την $n \equiv \ell k \pmod{\phi(m)}$, πού εἶναι ή ἀποδεικτέα σχέση. **ὄ.ξ.δ.**

Πίνακας 5.2: Στήν τομή τῆς στήλης τοῦ πρώτου p καί τῆς γραμμῆς τοῦ a ἐμφανίζεται ό $\text{ind}_g(a)$ όταν g εἶναι ό ἐλάχιστος γεννήτορας μέτρω p .

$a \backslash p$	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
26									19	5	12	17	17	29	25	46

συνέχεια στην ἐπόμενη σελίδα

Πίνακας 5.2 (συνέχεια από την προηγούμενη σελίδα)

$a \backslash P$	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
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

Εφαρμογές. *α'. Διωνυμικές ισοτιμίες.* Έστω ότι έχουμε να λύσουμε μία ισοτιμία $x^k \equiv a \pmod{m}$, όπου $(a, m) = 1$. Βάσει του δ' του θεωρήματος 5.2.1, η ισοτιμία αυτή είναι ισοδύναμη με την $k \operatorname{ind}(x) \equiv \operatorname{ind}(a) \pmod{\phi(m)}$. Η τελευταία γραμμική ως προς $\operatorname{ind}(x)$ ισοτιμία έχει λύση αν, και μόνο αν, $(k, \phi(m)) \mid \operatorname{ind}(a)$ (θεώρημα 3.2.1). Αν έχει λύση, τότε η επίλυσή της γίνεται απλούστατα, βάσει των ὄσων περιγράψαμε στην παράγραφο 3.2 του κεφαλαίου 3. Έχοντας υπολογίσει την κλάση $\operatorname{ind}(x) \pmod{\phi(m)}$, υπολογίζουμε με ὑψωση σὲ δύναμη (βλ. παράγραφο

2.3 του κεφαλαίου 2) την κλάση $x \pmod{m}$.

Για παράδειγμα, ἄς ἐπιλύσουμε τὴν ἰσοτιμία $x^{12} \equiv 37 \pmod{41}$. Ἡ ἰσοτιμία αὐτὴ ἰσοδυναμεῖ μὲ τὴν

$$12 \operatorname{ind}(x) \equiv \operatorname{ind}(37) \pmod{40}. \quad (5.3)$$

Ἀπὸ τὸν πίνακα 5.2 βλέπομε ὅτι $\operatorname{ind}(37) = 32$. Ὁ πίνακας αὐτὸς ἔχει συνταχθεῖ μὲ βάση τοὺς ἐλάχιστους (θετικὸς) γεννήτορες, τοὺς ὁποίους μᾶς παρέχει ὁ πίνακας 5.1, δηλαδή, στὸ παράδειγμά μας, ὁ γεννήτορας μέτρω 41 εἶναι ὁ 6. Ἐπειδὴ $(12, 40) = 4$ καὶ ὁ 4 διαιρεῖ τὸν $32 = \operatorname{ind}(37)$, 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 τέσσερις λύσεις,

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

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 πρακτικὸς, 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 ὑπολογιστικῆ. Γενικὰ μιλώντας, ἡ ἐνδεδειγμένη μέθοδος ἐπιλύσεως τῆς διωνυμικῆς ἰσοτιμίας εἶναι αὐτή, πὺ 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.* Ἐστω 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 $\operatorname{ind}(a)x \equiv \operatorname{ind}(b) \pmod{\phi(m)}$. Σύμφωνα μὲ τὸ θεώρημα 3.2.1, ἡ τελευταία ἰσοτιμία ἔχει λύσεις ἂν, καὶ μόνο ἂν, $(\operatorname{ind}(a), \phi(m)) \mid \operatorname{ind}(b)$ καί, στὴν περίπτωσι, πὺ ἡ συνθήκη αὐτὴ ἱκανοποιεῖται, τὸ πλῆθος τῶν διαφορετικῶν μέτρω $\phi(m)$ λύσεων εἶναι ἴσο μὲ $(\operatorname{ind}(a), \phi(m))$: βλ. ἄσκηση 8. Σημειώστε ὅτι, λόγω τοῦ θεωρήματος 2.2.4-γ', λύσεις τῆς ἐκθετικῆς ἰσοτιμίας, ἰσότητες μέτρω $\phi(m)$, δὲν θεωροῦνται διαφορετικῆς.

Ἄς ἐπιλύσομε, γιὰ παράδειγμα τὴν ἰσοτιμία $12^x \equiv 13 \pmod{23}$. Ἔχομε, σύμφωνα μὲ τὰ παραπάνω, $\operatorname{ind}(12)x \equiv \operatorname{ind}(13) \pmod{22}$ καὶ ἀπὸ τὸν πίνακα 5.2 βρίσκομε $\operatorname{ind}(12) = 20$, $\operatorname{ind}(13) = 14$, 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 καθιστᾷ, ἀπὸ ὑπολογιστικῆ ἄποψη, ἐξαιρετικὰ δύσκολη ἕως ἀνεφάρμοστη, γιὰ μεγάλα ἕως πολὺν μεγάλα μέτρα m . Σὲ ἀντίθεση, ὅμως, μὲ τὶς διωνυμικῆς ἰσοτιμίες, στὶς ὁποῖες παρακάμπτομε αὐτὸ τὸ ἐξαιρετικὰ σοβαρὸ

μειονέκτημα, για τις έκθετικές ισοτιμίες δεν υπάρχει, μέχρι σήμερα, πλήν ειδικών περιπτώσεων, «ύπολογιστικῶς εύκολη» μέθοδος επίλυσης. Σὲ αὐτό, ἀκριβῶς, τὸ χαρακτηριστικό τῶν έκθετικῶν ἔξισώσεων στηρίζεται ἡ ἀσφάλεια τῶν ψηφιακῶν ὑπογραφῶν καὶ τῆς ἀνταλλαγῆς κρυπτογραφικῶν κλειδιῶν

γ'. *Ἴσοῦπόλοιπα δυνάμεων.* Κατ' ἀναλογία μὲ τὰ τετραγωνικά ἰσοῦπόλοιπα, μπορούμε νὰ ὀρίσουμε ὅτι ὁ πρῶτος πρὸς τὸν m ἀκέραιος a εἶναι k -οστὸ ἰσοῦπόλοιπο μέτρω m γιὰ κάποιον ἀκέραιο $k \geq 2$ ἂν, καὶ μόνο ἂν, ἡ ἰσοτιμία $x^k \equiv a \pmod{m}$ ἔχει λύση. Ὁ ὀρισμὸς αὐτὸς ἰσχύει γιὰ ὀποιοδήποτε μέτρο m , ἀλλὰ ἐδῶ, ὅπως, ἄλλωστε, καὶ σὲ ὅλη αὐτὴ τὴν παράγραφο, θὰ ἐξετάσουμε 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 ἀθθαίρετο, ἀλλὰ σταθερό, γεννήτορα g , ὁπότε, γιὰ ἀπλοποίηση τοῦ συμβολισμοῦ, γράφομε ind ἀντὶ ind_g .*

α'. *Ὁ a εἶναι k -οστὸ ἰσοῦπόλοιπο μέτρω m ἂν, καὶ μόνο ἂν, $d \mid \text{ind}(a)$.*

β'. *Τὸ πλῆθος τῶν ἀνισοτιμῶν k -οστῶν ἰσοῦπολοίπων μέτρω m εἶναι $\frac{\phi(m)}{d}$.*

γ'. *Ὁ a εἶναι k -οστὸ ἰσοῦπόλοιπο μέτρω m ἂν, καὶ μόνο ἂν,*

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

δ'.

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

Εἰδικώτερα, ὁ a εἶναι γεννήτορας μέτρω m ἂν, καὶ μόνο ἂν, $(\phi(m), \text{ind}(a)) = 1$.

Ἀπόδειξη α'. Ἐνας ἀπλὸς συνδυασμὸς τῶν προτάσεων α' καὶ δ' τοῦ θεωρήματος 5.2.1 μᾶς δείχνει ὅτι ἡ ἰσοτιμία $x^k \equiv a \pmod{m}$ ἔχει λύση ἂν, καὶ μόνο ἂν ἔχει λύση ἡ ἰσοτιμία $k \text{ind}(x) \equiv \text{ind}(a) \pmod{\phi(m)}$. Σύμφωνα μὲ τὸ θεώρημα 3.2.1, ἡ τελευταία ἰσοτιμία ἔχει λύση ἂν, καὶ μόνο ἂν, $d \mid \text{ind}(a)$.

β'. Σύμφωνα μὲ τὸ (α'), ἀρκεῖ νὰ μετρήσουμε γιὰ πόσους ἀκεραίους a ἐνὸς περιορισμένου συστήματος ὑπολοίπων μέτρω m ἰσχύει $d \mid \text{ind}(a)$. Δεδομένου ὅτι ὁ $\text{ind}(a)$ διατρέχει τὸ σύνολο $\{0, 1, \dots, \phi(m) - 1\}$, αὐτὸ ἰσοδυναμεῖ μὲ τὸ νὰ μετρήσουμε πόσοι ἀπὸ τοὺς ἀριθμοὺς $0, 1, \dots, \phi(m) - 1$ εἶναι πολλαπλάσια τοῦ d . Ἀλλὰ αὐτὸ εἶναι ἀπλό: τὸ πλῆθος τῶν τέτοιων ἀριθμῶν εἶναι $\frac{\phi(m)}{d}$.

γ'. Σύμφωνα μὲ τὸ (α'), ὁ a εἶναι k -οστὸ ἰσοῦπόλοιπο μέτρω m ἂν, καὶ μόνο ἂν, $\text{ind}(a) \equiv 0 \pmod{d}$ καὶ ἡ ἰσοτιμία αὐτὴ εἶναι ἰσοδύναμη μὲ τὴν

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

δηλαδή, λόγω τῶν δ' καὶ ε' τοῦ θεωρήματος 5.2.1, μὲ τὴν

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

ἢ ὁποία εἶναι ἰσοδύναμη μὲ τὴν ἀποδεικτέα, λόγω τοῦ θεωρήματος 5.2.1-α'.

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

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

ἀπ' ὅπου ἔπεται ἀμέσως ἡ ἀποδεικτέα. **ῶ.ξ.δ.**

5.3 Άσκησης τοῦ κεφαλαίου 5

Στις ὑπολογιστικὲς ἀσκήσεις πρέπει νὰ κάνετε χρῆση τῶν πινάκων 5.1 καὶ 5.2

1. Ἐστω $m \geq 2$, $(a, m) = 1$. Ἐὰν $\text{ord}_m(a) = k$ καὶ $a^k \equiv 1 \pmod{m}$, τότε $\text{ord}_m(a^k) = k$.
2. Ἐστω $m \geq 2$, $(a, m) = 1$ καὶ q πρῶτος. Ἐὰν γιὰ κάποιον $k \geq 1$ ἰσχύει $a^k \equiv 1 \pmod{m}$ καὶ $a^{k-1} \not\equiv 1 \pmod{m}$ ἀποδείξτε ὅτι $\text{ord}_m(a) = q^k$.
3. Ἐστω ὅτι ὁ πρῶτος q διαιρεῖ τὸν $a^{2^m} + 1$ γιὰ κάποιον a . Ἀποδείξτε ὅτι $q \equiv 1 \pmod{2^{m+1}}$.
Ἐπίδειξη: Παρατηρήστε ὅτι $a^{2^m} \equiv -1 \pmod{q}$ καὶ ἐφαρμόστε τὴν ἀσκηση 2.
4. Ἐστω ὅτι ὁ p εἶναι περιττὸς πρῶτος καὶ ὁ g εἶναι γεννήτορας μέτρω p . Ἐστω k μὴ ἀρνητικὸς ἀκέραιος καὶ $(g + kp)^{p-1} \equiv a \pmod{p^2}$. Ἀποδείξτε ὅτι ὁ a εἶναι τῆς μορφῆς $1 + bp$ μὲ b ἀκέραιον. Ἐπιπλέον, ἂν ὁ b δὲν διαιρεῖται διὰ p , τότε ὁ $g + kp$ εἶναι γεννήτορας μέτρω p^n γιὰ κάθε $n \geq 1$.
Ἐπίδειξη: Ἐστω $(g + kp)^{p-1} = 1 + p\ell$. Ἀποδείξτε 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 ἀσκηση, 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, μέτρω p^n , γιὰ κάθε $n \geq 1$.
5. Ὑπολογίστε τὴν $\text{ord}_{43}(4)$, πρῶτα χωρὶς νὰ χρησιμοποιήσετε τὸ θεώρημα 5.2.2 καὶ μετὰ, χρησιμοποιώντας το.
6. Ὑπολογεῖστε γεννήτορες μέτρω m γιὰ $m = 2 \cdot 337^5, 191^7$.
Χρησιμοποιεῖστε τὴν ἀσκηση 4.

7. Υπολογίστε την $\text{ord}_m(a)$ στις έξης περιπτώσεις: (α') $m = 23^3$ και $a = 5^{11}$. (β') $m = 82$ και a τόν άκέραιο με $\text{ind}(a) = 10$.
8. Έστω $m > 1$ και υπάρχουν γεννήτορες μέτρω m . Αποδείξτε ότι ή έκθετική ισοτιμία $a^x \equiv b \pmod{m}$ έχει λύσεις αν, και μόνο αν, $(\text{ind}(a), \phi(m)) | b$ και, στην περίπτωση που έχει, τόν πλήθος τών διαφορετικών μέτρω $\phi(m)$ λύσεων είναι $(\text{ind}(a), \phi(m))$ ενών, μέτρω $\text{ord}_m(a)$, ή λύση είναι μοναδική. Συνεπώς, στην περίπτωση που ή ισοτιμία $a^x \equiv b \pmod{m}$ έχει λύσεις, υπάρχει ένας μοναδικός $x \in \{0, 1, \dots, \text{ord}_m(a) - 1\}$, που την έπαληθεύει.
9. Ποιοι από τούς άριθμούς 6, 27 και 37 είναι 35ες δυνάμεις μέτρω 31^2 ;
10. Αποδείξτε ότι ή έκθετική ισοτιμία $12^x \equiv 11 \pmod{47}$ είναι άδύνατη, ενών ή $12^x \equiv 21 \pmod{47}$ έχει λύσεις, τις όποιες και να υπολογίσετε.
11. Υπολογίστε όλους τούς άριθμούς του συνόλου $\{1, 2, \dots, 70\}$, οί όποιοι είναι γεννήτορες μέτρω 71.
12. Έστω περιτός πρώτος p και $n \geq 1$. Αν $S_n(p) = \sum_{k=1}^{p-1} k^n$, αποδείξτε ότι

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

Υπόδειξη. Για κάθε $k = 1, 2, \dots, p-1$ υπάρχει v , τέτοιο ώστε $k \equiv g^v \pmod{p}$.

13. Έστω πρώτος $p > 3$. Αποδείξτε ότι τόν γινόμενο τών άριθμών ενός περιορισμένου συστήματος υπολοίπων μέτρω p , οί όποιοι είναι γεννήτορες μέτρω p , είναι ισότιμο με 1 μέτρω p .
Υπόδειξη. Έστω g ένας γεννήτορας μέτρω p . Για ποιους έκθέτες k είναι και g^k γεννήτορας; Αν ό g^k είναι γεννήτορας, τόν ίδιο ισχύει και για τόν g^{p-1-k} . Επίσης, άφου $p > 3$, ό $g^{(p-1)/2}$ δέν είναι γεννήτορας.
14. Έστω p πρώτος τής μορφής $2^{2^k} + 1$.
(α') Αποδείξτε ότι οί άριθμοί ενός περιορισμένου συστήματος υπολοίπων μέτρω p , οί όποιοι είναι γεννήτορες συμπίπτουν με εκείνους, οί όποιοι είναι τετραγωνικά άνισοϋπόλοιπα.
Υπόδειξη. Έστω g γεννήτορας μέτρω p . Για ποιους έκθέτες k είναι και g^k γεννήτορας; Μετά, εφαρμόστε την πρόταση β' του θεωρήματος 4.1.1.
(β'). Χρησιμοποιείστε τόν (α') για να αποδείξετε ότι ό 7 είναι γεννήτορας μέτρω p .
Υπόδειξη. Αποδείξτε πρώτα, έπαγωγικά, και ανεξάρτητα από τή συγκεκριμένη άσκηση, ότι $2^{2^k} \equiv 2$ ή $4 \pmod{7}$, ανάλογα με τόν αν ό k είναι άρτιος ή περιτός, άντιστοίχως. Σε συνδυασμό με αυτό, θα χρειασθείτε, επίσης, τόν νόμο τής τετραγωνικής άντιστροφής του Gauss προκειμένου να αποδείξετε ότι ό 7 είναι τετραγωνικό άνισοϋπόλοιπο μέτρω p .

15. Η άσκηση αυτή περιέχει κριτήρια πιστοποίησης πρώτου, όφειλόμενα στους Maurice Borisovich Kraitichik, Derrick Henry Lehmer, Édurad Lucas, Henry Cabourn Pocklington, François Proth, John Selfridge.

Σε κάθε μία από τις επόμενες περιπτώσεις αποδείξτε ότι ο $n \geq 3$ είναι πρώτος.

- (α') (Lucas 1876) Υπάρχει a τέτοιος ώστε $a^{n-1} \equiv 1 \pmod{n}$ και $a^k \not\equiv 1 \pmod{n}$ για κάθε $k = 1, \dots, n-2$.
Υπόδειξη: Αν υπήρχε γνήσιος πρώτος διαιρέτης p του n , τότε, για κάποιο $k \in \{1, \dots, n-1\}$ θα ήταν $p \equiv a^k \pmod{n}$, οπότε οδηγηθείτε σε άτοπο.
- (β') (Lucas 1878) Υπάρχει a τέτοιος ώστε $a^{n-1} \equiv 1 \pmod{n}$ και $a^k \not\equiv 1 \pmod{n}$ για κάθε θετικό διαιρέτη k του $n-1$, μικρότερο του $n-1$.
Υπόδειξη: Ποιά είναι η τάξη του a ; Μετά εφαρμόστε το (15α').
- (γ') (Lucas-Kraitichik-Lehmer 1927) Υπάρχει a τέτοιος ώστε $a^{n-1} \equiv 1 \pmod{n}$ και $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ για κάθε πρώτο διαιρέτη q του $n-1$.
Υπόδειξη: Έστω $r = \text{ord}_n(a)$. Ισχύει $n-1 = rs$. Αν $s = 1$, εφαρμόστε το (15α'). Αν $s > 1$, θεωρήστε ένα πρώτο διαιρέτη του s και εφαρμόστε το (15β').
- (δ') (Selfridge 1967) Για κάθε πρώτο διαιρέτη q του $n-1$ υπάρχει a_q (δηλαδή, άκεραιος εξαρτώμενος από τον q) τέτοιος ώστε $a_q^{n-1} \equiv 1 \pmod{n}$ και $a_q^{(n-1)/q} \not\equiv 1 \pmod{n}$.
Υπόδειξη: Έστω ότι q_1, \dots, q_m είναι όλοι οι διαφορετικοί πρώτοι διαιρέτες του $n-1$ και a_1, \dots, a_m οι άκεραιοι a_{q_1}, \dots, a_{q_m} , που μάς εξασφαλίζει η υπόθεση. Έστω $r_i = \text{ord}_n(a_i)$, ($i = 1, \dots, m$). Διαπιστώστε πρώτα ότι υπάρχει a με $\text{ord}_n(a) = r$, όπου $r = \text{EKΠ}(r_1, \dots, r_m)$. Αποδείξτε ότι $a^{n-1} \equiv 1 \pmod{n}$ και $a^{(n-1)/q_i} \not\equiv 1 \pmod{n}$ για κάθε $i = 1, \dots, m$, οπότε εφαρμόστε το (15γ').
- (ε') (Proth 1878) Ο $n-1$ μπορεί να αναλυθεί ως $n-1 = 2^r s$, όπου $s < 2^r$ και για κάθε πρώτο διαιρέτη υπάρχει a τέτοιος ώστε $a^{(n-1)/2} \equiv -1 \pmod{n}$.
Υπόδειξη: Έστω p πρώτος διαιρέτης του n . Παρατηρήστε ότι $(a^s)^{2^{r-1}} \equiv -1 \pmod{n}$ και εφαρμόστε την άσκηση 3 για να καταλήξετε στο συμπέρασμα ότι $p \geq 1 + 2^r$. Συνεπώς, αν ο n είχε δύο πρώτους διαιρέτες (ίσους ή άνισους), τότε $n \geq (1 + 2^r)^2$, οπότε οδηγηθείτε σε αντίφαση.
- (ζ') (Pocklington 1914) Ο $n-1$ μπορεί να αναλυθεί ως $n-1 = km$, όπου $1 \leq k < m$ και $(k, m) = 1$ και για κάθε πρώτο διαιρέτη q του m υπάρχει a_q τέτοιος ώστε $a_q^{n-1} \equiv 1 \pmod{n}$ και $(a_q^{(n-1)/q} - 1, n) = 1$.
Υπόδειξη: Αν ο n είναι σύνθετος, τότε έχει ένα πρώτο διαιρέτη $p \leq \sqrt{n}$. Αν αποδειχθεί ότι $p \equiv 1 \pmod{m}$, τότε $p \geq 1 + m$ και μπορείτε εύκολα να οδηγηθείτε σε αντίφαση με την προηγούμενη άνισότητα. Για την απόδειξη της $p \equiv 1 \pmod{m}$ ακολουθήστε τα εξής βήματα. Έστω q ο τυπικός πρώτος διαιρέτης του $n-1$, $e = \nu_q(n-1)$ και $c = a_q^{(n-1)/q^e}$. Αποδείξτε, έκμεταλευόμενοι τις υποθέσεις, ότι $c^{q^e} \equiv 1 \pmod{n}$, άρα και $c^{q^e} \equiv 1 \pmod{p}$, ενώ $c^{q^{e-1}} \not\equiv 1 \pmod{p}$. Συμπεράνατε τώρα, με τη βοήθεια της άσκησης 2 ότι $q^e | p-1$.

Αυτό το συμπέρασμα θα σᾶς ἐπιτρέψει νὰ συμπεράνετε, ἂν φαντασθεῖτε τὴν κανονικὴ ἀνάλυση $q_1^{e_1} q_2^{e_2} \cdots$ τοῦ m , ὅτι $p \equiv 1 \pmod{m}$.

Εύρετήριο

- ἀκέραιο μέρος, 3
- ἀκέραιο σημείο, 58
 - θετικό, 58
- ἀλγόριθμος
 - εὐκλείδειος, 8
 - μετατροπῆς σὲ δυαδικό, 33
 - ὑψωσης σὲ δύναμη, 34
- ἀνάλυση
 - γενικευμένη κανονική, 16
 - κανονική, 15
 - σὲ πρώτους, 15
- ἀνισότιμοι ἀριθμοί, 26
- ἀνισοὑπόλοιπο
 - τετραγωνικό, 53
- ἄπειρη κάθοδος, 15
- ἀριθμός
 - ἀκέραιος, 3
 - ἄρτιος, 5
 - δυαδικός, 32
 - περιττός, 5
 - πρῶτος, 12, 13
 - ρητός, 3
 - σύνθετος, 12
 - φυσικός, 3
- bits, 32
- γεννήτορας $\text{mod } m$, 70
- διαιρέτης
 - ἀκεραίου, 3
 - κοινός, 5
 - μέγιστος κοινός, 5–8, 21
 - πρῶτος, 12, 13
 - τετριμμένος, 12
- διακριτὸς λογάριθμος, 75
- Διόφαντος, 23
- δυαδικὰ ψηφία, 32
- ἐκθέτης, 16
- ἐξίσωση
 - διοφαντική, 17, 23
- ἐπίλυση
 - ἰσοτιμίας, 41
- ἐτερότυποι ἀριθμοί, 18
- εὐκλείδεια διαίρεση, 4
- Gauss, 58
- Ἡράκλειτος, 35
- θεώρημα
 - Euler, 31
 - Fermat, 31
 - κινέζικο, ὑπολοίπων, 43
 - Wilson, 38
- ἰδεῶδες, 5
- ἰσοτιμία, 25
 - διωνυμική, 78
 - ἐκθετική, 79
 - ἰσοδύναμη μὲ ἄλλη, 41
- ἰσότιμοι ἀριθμοί, 25
- ἰσοὑπόλοιπο
 - τετραγωνικό, 53
- ἰσοὑπόλοιπο δύναμης, 80
- κλάση ἰσοτιμίας, 27
- κλειδί
 - κρυπτογραφικό, 80
- κόσκινο Ἐρατοσθένους, 14
- λύση

- ισοτιμίας, 41
- μέτρο
 - ισοτιμίας, 25
- μονάδες, 12
- πηλίκο
 - ἀκέραιο, 4
 - ἀκεραίων, 3
 - διαίρεσης, 4
- πολλαπλάσιο
 - ἀκεραίου, 3
 - ἐλάχιστο κοινό, 11, 12, 23
 - κοινό, 11
- πρῶτοι
 - ἀνὰ ζεύγη, 6
 - μεταξύ τους, 6
- πυθαγόρεια τριάδα, 17
 - πρωταρχική, 19
- RSA, 35
- σύμβολο
 - Jacobi, 60
 - Legendre, 55
- σύστημα ὑπολοίπων
 - περιορισμένο, 28
 - πλήρες, 28
 - ἀπολύτως ἐλάχιστο, 28
 - ἐλάχιστο μὴ ἀρνητικό, 28
- τάξη mod m , 69
- Taylor
 - τύπος, 46
- τετραγωνικῆς ἀντιστροφῆς
 - νόμος, 58
 - συμπλήρωμα, 57
- ὑπολογισμός
 - ὑπολοίπου διαίρεσης, 31
- ὑπολογισμός
 - ΜΚΔ, 8, 10, 21
 - ϕ συνάρτησης, 29
- ὑπόλοιπο
 - διαίρεσης, 4
- ϕ συνάρτηση Euler, 29
- ψηφιακή
 - ὑπογραφή, 80