Σημειώσεις Θεωρίας Αριθμών

Τμημα Μαθηματικων
Πανεπιστημιο Αθηνων
Αθηνα, 2013

Περιεχόμενα

Εισαγωγή

Κεφάλαιο 1

Διαιρετότητα και πρώτοι αριθμοί

1.1 Το σύνολο των ακεραίων

Η στοιχειώδης θεωρία αριθμών ασχολείται με τη μελέτη των ιδιοτήτων του συνόλου $\mathbb{N} = \{1, 2, 3, \ldots\}$ των θετικών ακεραίων (αλλιώς, φυσικών αριθμών). Θα χρειαστεί να θεωρήσουμε το $\mathbb{N}$ ως υποσύνολο του συνόλου $\mathbb{Z}$ των ακέραιων αριθμών ή και του συνόλου $\mathbb{Q}$ των ρητών αριθμών. Θα γράφουμε $\mathbb{Z}^+$ ή $\mathbb{N} \cup \{0\}$ για το σύνολο των μη αρνητικών ακεραίων. Με $\mathbb{R}$ συμβολίζουμε το σύνολο των πραγματικών αριθμών και με $\mathbb{C}$ το σύνολο των μιγαδικών αριθμών.

Η αυστηρή θεμελίωση του συνόλου $\mathbb{N}$ των φυσικών αριθμών γίνεται μέσω των αξιωμάτων του Peano. Έχοντας δεδομένο το $\mathbb{N}$ και έχοντας ορίσει τις πράξεις της πρόσθεσης και του πολλαπλασιασμού καθώς και τη διάταξη των φυσικών αριθμών, μπορούμε να δώσουμε αυστηρή κατασκευή του $\mathbb{Z}$ και του $\mathbb{Q}$. Θεωρούμε ότι ο αναγνώστης είναι εξοικειωμένος με τις ιδιότητες των πράξεων και τις ιδιότητες της διάταξης στο $\mathbb{Z}$ και στο $\mathbb{Q}$. Σε αυτή τη σύντομη παράγραφο απλώς υπενθυμίζουμε κάποιες βασικές αρχές.

Θεώρημα 1.1.1 (Αρχή του ελαχίστου)**.** *Κάθε μη κενό σύνολο S μη αρνητικών ακεραίων έχει ελάχιστο στοιχείο. Δηλαδή, υπάρχει $a \in S$ με την ιδιότητα $a \leq b$ για κάθε $b \in S$.*

Παρατήρηση 1.1.2. Η αρχή του ελαχίστου έχει ως συνέπεια την εξής πρόταση:

Δεν υπάρχει άπειρη γνησίως φθίνουσα ακολουθία μη αρνητικών ακεραίων.

Πράγματι, ας υποθέσουμε ότι υπάρχει μια ακολουθία

$$n_1 > n_2 > \cdots > n_k > n_{k+1} > \cdots$$

στο $\mathbb{Z}^+$. Από την αρχή του ελαχίστου, το σύνολο $S = \{n_k : k \in \mathbb{N}\}$ έχει ελάχιστο στοιχείο n_m για κάποιον $m \in \mathbb{N}$. Όμως $n_{m+1} < n_m$ και $n_{m+1} \in S$, πράγμα άτοπο.

Η αρχή του ελαχίστου θα χρησιμοποιηθεί αρκετές φορές στη μελέτη μας. Για το λόγο αυτό, δίνουμε κάποια πρώτα παραδείγματα εφαρμογής της (σκοπός μας δεν είναι να θεμελιώσουμε αυστηρά το σύνολο των φυσικών, αλλά να εξοικειωθούμε με το είδος των επιχειρημάτων που χρησιμοποιούνται συνήθως).

Παράδειγμα 1.1.3. Ο 1 είναι ο μικρότερος φυσικός αριθμός. Πράγματι, αν υπήρχε $a \in \mathbb{N}$ με $0 < a < 1$, τότε η ακολουθία $n_k = a^k$ θα αποτελούνταν από φυσικούς αριθμούς και θα ήταν γνησίως φθίνουσα: $n_{k+1} = a^k \cdot a < a^k \cdot 1 = n_k$. Από την προηγούμενη παρατήρηση, αυτό είναι άτοπο.

Θεώρημα 1.1.4 (Αρχιμήδεια ιδιότητα)**.** *Αν a και b είναι δύο φυσικοί αριθμοί, υπάρχει φυσικός αριθμός n τέτοιος ώστε $na \geq b$.*

Απόδειξη. Αν υποθέσουμε ότι το θεώρημα δεν ισχύει, υπάρχουν $a, b \in \mathbb{N}$ τέτοιοι ώστε $na < b$ για κάθε $n \in \mathbb{N}$. Αυτό σημαίνει ότι το σύνολο

$$S = \{b - na : \ n \in \mathbb{N}\} \tag{1.1.1}$$

αποτελείται από θετικούς ακεραίους. Από την αρχή του ελαχίστου, το S έχει ελάχιστο στοιχείο, το οποίο γράφεται στη μορφή $b - ma$ για κάποιον $m \in \mathbb{N}$. Παρατηρούμε ότι $b - (m+1)a \in S$ και

$$b - (m+1)a = (b - ma) - a < b - ma, \tag{1.1.2}$$

το οποίο είναι άτοπο. Άρα η Αρχιμήδεια ιδιότητα ισχύει. □

Παρατήρηση 1.1.5. Αν υποθέσουμε ως γνωστό ότι ο 1 είναι ο μικρότερος φυσικός αριθμός, τότε η απόδειξη είναι πολύ απλούστερη: αν πάρουμε $n = b$ έχουμε

$$a \geq 1 \Longrightarrow ba \geq b.$$

Θεώρημα 1.1.6 (Αρχή της πεπερασμένης επαγωγής)**.** *Έστω S ένα σύνολο θετικών ακεραίων με τις εξής ιδιότητες:*

(i) $1 \in S$.

(ii) Αν $k \in S$ τότε $k + 1 \in S$.

Τότε το S είναι το σύνολο όλων των φυσικών αριθμών.

Απόδειξη. Θέτουμε $T = \mathbb{N} \setminus S$ και υποθέτουμε ότι το T είναι μη κενό. Από την αρχή του ελαχίστου, το T έχει ελάχιστο στοιχείο το οποίο συμβολίζουμε με a. Αφού $1 \in S$, αναγκαστικά έχουμε $a > 1$ οπότε $a - 1 \in \mathbb{N}$. Αφού ο a ήταν το ελάχιστο στοιχείο του T, έχουμε $a - 1 \in S$. Από την υπόθεση (ii) έχουμε ότι

$$a = (a - 1) + 1 \in S. \tag{1.1.3}$$

Έτσι, καταλήγουμε σε άτοπο, άρα το T είναι το κενό σύνολο. Επομένως $S = \mathbb{N}$. □

Η αρχή της πεπερασμένης επαγωγής μας επιτρέπει να αποδεικνύουμε ότι κάποια πρόταση $P(n)$ που αφορά τους φυσικούς αριθμούς ισχύει για κάθε $n \in \mathbb{N}$. Αρκεί να ελέγξουμε ότι η $P(1)$ ισχύει (αυτή είναι η *βάση της επαγωγής*) και να αποδείξουμε τη συνεπαγωγή $P(k) \Rightarrow P(k+1)$ (αυτό είναι το *επαγωγικό βήμα*). Παραδείγματα προτάσεων που αποδεικνύονται με τη «μέθοδο της μαθηματικής επαγωγής» θα συναντάμε σε όλη τη διάρκεια του μαθήματος.

Αξίζει να αναφέρουμε δύο παραλλαγές του Θεωρήματος 1.1.6. Η απόδειξή τους αφήνεται σαν άσκηση για τον αναγνώστη (μιμηθείτε την προηγούμενη απόδειξη - χρησιμοποιήστε την αρχή του ελαχίστου).

Θεώρημα 1.1.7. *Έστω $m \in \mathbb{Z}$ και S ένα σύνολο ακεραίων με τις εξής ιδιότητες: $m \in S$ και αν $k \in S$ τότε $k+1 \in S$. Τότε $S \supseteq \{n \in \mathbb{Z} : n \geq m\} = \{m, m+1, \ldots\}$.*

Θεώρημα 1.1.8. *Έστω S ένα σύνολο θετικών ακεραίων με τις εξής ιδιότητες: $1 \in S$ και αν $1, \ldots, k \in S$ τότε $k+1 \in S$. Τότε $S = \mathbb{N}$.*

Παράδειγμα 1.1.9. Η ακολουθία των *αριθμών του Lucas* ορίζεται αναδρομικά ως εξής. Θέτουμε $a_1 = 1$, $a_2 = 3$ και, για κάθε $n \geq 3$,

$$a_n = a_{n-1} + a_{n-2}. \tag{1.1.4}$$

Σκοπός μας είναι να δείξουμε ότι υπάρχει πραγματικός αριθμός $x > 0$ με την ιδιότητα $a_n < x^n$ για κάθε $n \in \mathbb{N}$. Η απόδειξη θα δείξει ότι κάθε $x > \sqrt{3}$ (για παράδειγμα, ο $x = 7/4$) ικανοποιεί το ζητούμενο.

Θεωρούμε την πρόταση $P(n) : a_n < x^n$. Η $P(1)$ ισχύει αν $1 < x$, ενώ η $P(2)$ ισχύει αν $3 < x^2$, δηλαδή αν $\sqrt{3} < x$. Θα χρησιμοποιήσουμε την αρχή της επαγωγής στη μορφή του Θεωρήματος 1.1.7: υποθέτουμε λοιπόν ότι $k \geq 3$ και ότι οι $P(1), \ldots, P(k-1)$ ισχύουν. Ειδικότερα,

$$a_{k-1} < x^{k-1} \text{ και } a_{k-2} < x^{k-2}. \tag{1.1.5}$$

Τότε

$$a_k = a_{k-1} + a_{k-2} < x^{k-1} + x^{k-2}, \tag{1.1.6}$$

δηλαδή $a_k < x^k$ αν ισχύει η ανισότητα $x^{k-1} + x^{k-2} < x^k$, η οποία είναι ισοδύναμη με την

$$x^2 - x - 1 > 0. \tag{1.1.7}$$

Η (1.1.7) ισχύει αν ο θετικός αριθμός x είναι μεγαλύτερος από $(1+\sqrt{5})/2$. Δηλαδή το επαγωγικό επιχείρημα δουλεύει αν

$$x > \max\{1, \sqrt{3}, (1+\sqrt{5})/2\} = \sqrt{3}. \tag{1.1.8}$$

Έτσι, αν $x > \sqrt{3}$, η πρόταση $P(n)$ ισχύει για κάθε $n \in \mathbb{N}$.

1.2 Διαιρετότητα και Ευκλείδια Διαίρεση

Ορισμός 1.2.1. Έστω $a, b \in \mathbb{Z}$. Λέμε ότι ο a *διαιρεί* τον b και γράφουμε $a \mid b$, αν υπάρχει $x \in \mathbb{Z}$ τέτοιος ώστε $b = ax$. Σε αυτή την περίπτωση θα λέμε ότι ο a είναι *διαιρέτης* του b ή ότι ο b είναι *πολλαπλάσιο* του a.

Απλές συνέπειες του ορισμού είναι οι εξής:

(i) $a \mid a$ για κάθε $a \in \mathbb{Z}$.

(ii) $a \mid 0$ για κάθε $a \in \mathbb{Z}$.

(iii) $\pm 1 \mid a$ για κάθε $a \in \mathbb{Z}$.

(iv) $0 \mid a$ αν και μόνο αν $a = 0$.

(v) Αν $a \mid b$ και $b \mid c$ τότε $a \mid c$.

(vi) Αν $a \mid b$ και $a \mid c$ τότε $a \mid bx + cy$ για κάθε $x, y \in \mathbb{Z}$.

(vii) Αν $a, b \in \mathbb{Z} \setminus \{0\}$ και $a \mid b$ τότε $|a| \leq |b|$.

(viii) $a \mid \pm 1$ αν και μόνο αν $a = \pm 1$.

Η απόδειξη των παραπάνω ιδιοτήτων αφήνεται ως άσκηση.

Θεώρημα 1.2.2 (Ταυτότητα της διαίρεσης). *Υποθέτουμε ότι $a \in \mathbb{N}$ και $b \in \mathbb{Z}$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ τέτοιοι ώστε $b = aq + r$ και $0 \leq r < a$.*

Ένας απλός γεωμετρικός τρόπος για να σκεφτόμαστε την ταυτότητα της διαίρεσης είναι ο εξής: φανταζόμαστε την πραγματική ευθεία πάνω στην οποία έχουμε σημειώσει με κουκίδες τους ακεραίους. Σημειώνουμε με πιο σκούρες κουκίδες τα πολλαπλάσια του a. Διαδοχικές σκούρες κουκίδες έχουν απόσταση ακριβώς ίση με a. Τότε ένα από τα ακόλουθα συμβαίνει:

(i) Ο ακέραιος b πέφτει πάνω σε κάποια από αυτές τις σκούρες κουκίδες, οπότε ο b είναι πολλαπλάσιο του a και $r = 0$.

(ii) Ο ακέραιος b βρίσκεται ανάμεσα σε δύο διαδοχικές σκούρες κουκίδες, δηλαδή ανάμεσα σε δύο διαδοχικά πολλαπλάσια του a, και η απόσταση r ανάμεσα στον b και το μεγαλύτερο πολλαπλάσιο του a που είναι μικρότερο από τον b είναι ένας θετικός ακέραιος που δεν ξεπερνάει τον $a - 1$.

Η αυστηρή απόδειξη που θα δώσουμε παρακάτω βασίζεται σε αυτήν την ιδέα: θεωρούμε το σύνολο S των «αποστάσεων» $b - as$ του b από τις σκούρες κουκίδες που βρίσκονται αριστερά του. Εξασφαλίζουμε ότι είναι μη κενό, άρα έχει ελάχιστο στοιχείο $b - aq$. Η κουκίδα aq είναι αυτή που βρίσκεται αμέσως πριν από τον b, και η απόσταση $r = b - aq$ πρέπει να είναι μικρότερη από a.

Απόδειξη. Αποδεικνύουμε πρώτα την ύπαρξη αριθμών $q, r \in \mathbb{Z}$ που ικανοποιούν το ζητούμενο. Θεωρούμε το σύνολο

$$S = \{b - as : s \in \mathbb{Z}\} \cap \mathbb{Z}^+ \tag{1.2.1}$$

των μη αρνητικών ακεραίων της μορφής $b - as$. Το S είναι μη κενό. Πράγματι, αν $b \geq 0$ τότε $b - a \cdot 0 \in S$. Αν $b < 0$, θεωρούμε ακεραίους s της μορφής $-a \cdot n$ όπου $n \in \mathbb{N}$. Έχουμε $b - as = b + a^2 n$ και από την Αρχιμήδεια ιδιότητα υπάρχει $n \in \mathbb{N}$ τέτοιος ώστε $a^2 n \geq (-b)$.

Από την αρχή του ελαχίστου, το S έχει ελάχιστο στοιχείο, το οποίο συμβολίζουμε με r. Από τον ορισμό του S έχουμε $r \geq 0$ και υπάρχει $q \in \mathbb{Z}$ τέτοιος ώστε $b - aq = r$. Μένει να δείξουμε ότι $r < a$. Ας υποθέσουμε ότι $r \geq a$. Τότε

$$b - a(q + 1) = b - aq - a = r - a \geq 0, \tag{1.2.2}$$

δηλαδή $b - a(q + 1) \in S$. Όμως $b - a(q + 1) = r - a < r$, το οποίο είναι άτοπο αφού ο r ήταν το ελάχιστο στοιχείο του S.

Αποδεικνύουμε τώρα τη μοναδικότητα των q και r. Ας υποθέσουμε ότι

$$b = aq_1 + r_1 = aq_2 + r_2, \tag{1.2.3}$$

όπου $0 \leq r_1, r_2 < a$. Τότε

$$|r_1 - r_2| = a|q_2 - q_1|. \tag{1.2.4}$$

Αν $q_1 \neq q_2$, τότε $a|q_2 - q_1| \geq a$ ενώ $|r_1 - r_2| < a$. Έχουμε αντίφαση, άρα $q_1 = q_2$, και από την (1.2.3) έπεται ότι $r_1 = r_2$. □

Παράδειγμα 1.2.3. Από το Θεώρημα 1.2.2, κάθε ακέραιος b γράφεται μονοσήμαντα στη μορφή $b = 2q + r$, για κάποιον $q \in \mathbb{Z}$ και κάποιον $r \in \{0, 1\}$. Λέμε ότι ο b είναι *άρτιος* αν $r = 0$. Αν $r = 1$, τότε λέμε ότι ο b είναι *περιττός*. Παρατηρήστε ότι οποιαδήποτε δύναμη περιττού ακεραίου είναι περιττός ακέραιος.

Σκοπός μας είναι να δείξουμε ότι αν οι ακέραιοι x, y, z ικανοποιούν την εξίσωση

$$x^3 + 2y^3 = 4z^3 \tag{1.2.5}$$

τότε $x = y = z = 0$.

Για κάθε λύση της (1.2.5) θεωρούμε το μη αρνητικό ακέραιο

$$d := \max\{|x|, |y|, |z|\}. \tag{1.2.6}$$

Ας υποθέσουμε ότι η εξίσωση (1.2.5) έχει μια μη τετριμμένη λύση (x_1, y_1, z_1) στο $\mathbb{Z}$, δηλαδή τουλάχιστον ένας από τους x_1, y_1, z_1 είναι μη μηδενικός ακέραιος. Τότε

$$d_1 = \max\{|x_1|, |y_1|, |z_1|\} > 0. \tag{1.2.7}$$

Παρατηρούμε ότι ο $x_1^3 = 4z_1^3 - 2y_1^3$ είναι άρτιος, άρα ο x_1 είναι άρτιος. Υπάρχει λοιπόν $x_2 \in \mathbb{Z}$ τέτοιος ώστε $x_1 = 2x_2$. Αντικαθιστώντας στην (1.2.5) παίρνουμε

$$8x_2^3 + 2y_1^3 = 4z_1^3 \Longrightarrow y_1^3 = 2z_1^3 - 4x_2^3. \tag{1.2.8}$$

Έπεται ότι ο y_1 είναι άρτιος, άρα γράφεται στη μορφή $y_1 = 2y_2$ για κάποιον $y_2 \in \mathbb{Z}$. Αντικαθιστώντας στην (1.2.8) παίρνουμε

$$8y_2^3 = 2z_1^3 - 4x_2^3 \Longrightarrow z_1^3 = 4y_2^3 + 2x_2^3. \tag{1.2.9}$$

Άρα ο z_1 είναι κι αυτός άρτιος και γράφεται στη μορφή $z_1 = 2z_2$ για κάποιον $z_2 \in \mathbb{Z}$. Παρατηρούμε ότι οι x_2, y_2 και z_2 ικανοποιούν την (1.2.5) και

$$0 < d_2 = \max\{|x_2|, |y_2|, |z_2|\} = \max\{|x_1|, |y_1|, |z_1|\}/2 = d_1/2 < d_1. \tag{1.2.10}$$

Συνεχίζοντας παρόμοια κατασκευάζουμε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών αριθμών $d_1 > d_2 > \cdots > d_n > d_{n+1} > \cdots$. Αυτό είναι άτοπο από την αρχή του ελαχίστου. Άρα η μόνη λύση της (1.2.5) στο $\mathbb{Z}$ είναι η τετριμμένη $x = y = z = 0$.

Χρησιμοποιώντας την ταυτότητα της διαίρεσης και τη μέθοδο της μαθηματικής επαγωγής μπορούμε να αποδείξουμε την ύπαρξη και τη μοναδικότητα των m-αδικών αναπαραστάσεων των ακεραίων.

Θεώρημα 1.2.4. *Έστω $m \geq 2$ ένας ακέραιος. Κάθε φυσικός αριθμός n αναπαρίσταται κατά μοναδικό τρόπο στη μορφή*

$$n = a_0 + a_1 m + a_2 m^2 + \cdots + a_k m^k, \tag{1.2.11}$$

όπου k είναι ο μη αρνητικός ακέραιος για τον οποίο $m^k \leq n < m^{k+1}$, και $a_0, a_1, \ldots, a_k$ είναι ακέραιοι που ικανοποιούν τις $1 \leq a_k \leq m - 1$ και $0 \leq a_i \leq m - 1$ για κάθε $i = 0, 1, \ldots, k - 1$.

Η (1.2.11) λέγεται *m-αδική αναπαράσταση* του n. Οι ακέραιοι a_i είναι τα *ψηφία* του n με *βάση* τον m.

Απόδειξη. Θα χρησιμοποιήσουμε τη μέθοδο της μαθηματικής επαγωγής στη μορφή του Θεωρήματος 1.1.8. Αν $1 \leq n < m$ τότε η $n = a_0$ είναι η μοναδική m-αδική αναπαράσταση (1.2.11) του n (εξηγήστε γιατί). Έστω $n \geq m$ και έστω ότι ο ισχυρισμός του θεωρήματος ισχύει για κάθε θετικό ακέραιο μικρότερο του n. Θα αποδείξουμε τον ίδιο ισχυρισμό για τον n. Από την ταυτότητα της διαίρεσης του n με τον m υπάρχουν ακέραιοι q και r με $0 \leq r < m$ έτσι ώστε

$$n = r + qm. \tag{1.2.12}$$

Από την υπόθεση $n \geq m$ έχουμε $q > 0$ και συνεπώς $0 < q < qm \leq qm + r = n$. Από την υπόθεση της επαγωγής ο q αναπαρίσταται στη μορφή

$$q = a_1 + a_2 m + \cdots + a_k m^{k-1} \tag{1.2.13}$$

για μοναδικούς ακεραίους a_i με $0 \leq a_i \leq m-1$ για $i = 1, 2, \ldots, k$ και $a_k > 0$. Από τις (1.2.12) και (1.2.13), θέτοντας $r = a_0$, προκύπτει ότι ο n αναπαρίσταται στη ζητούμενη μορφή

$$n = a_0 + a_1 m + \cdots + a_{k-1} m^{k-1} + a_k m^k. \tag{1.2.14}$$

Θα δείξουμε ότι αυτή η αναπαράσταση είναι μοναδική. Έστω

$$n = b_0 + b_1 m + \cdots + b_s m^s \tag{1.2.15}$$

μια άλλη m-αδική αναπαράσταση του n, όπου $0 \leq b_j \leq m-1$ για κάθε $j = 0, 1, \ldots, s$ και $b_s \geq 1$. Από την (1.2.15) έχουμε $n = r' + mq'$ όπου $r' = b_0$ και

$$q' = b_1 + b_2 m + \cdots + b_s m^{s-1} \tag{1.2.16}$$

είναι ακέραιοι με $0 \leq r' < m$. Από τη μοναδικότητα της διαίρεσης του n με το m προκύπτει ότι $r' = r$ και $q' = q$. Η πρώτη ισότητα δίνει $b_0 = a_0$ ενώ από την υπόθεση της επαγωγής για τη μοναδικότητα της m-αδική αναπαράστασης του $q = q'$ και τις (1.2.13) και (1.2.16) προκύπτει ότι $s = k$ και $b_i = a_i$ για $i = 1, 2, \ldots, k$, όπως θέλαμε να δείξουμε.

Τέλος, αν ο n είναι στη μορφή (1.2.11) τότε από τις σχέσεις $0 \leq a_i \leq m-1$ και $1 \leq a_k \leq m-1$ προκύπτει ότι

$$m^k \leq n \leq (m-1)(1 + m + \cdots + m^k) = m^{k+1} - 1 < m^{k+1}.$$

□

Παραδείγματα 1.2.5. (α) Η 2-αδική αναπαράσταση του 100 είναι

$$100 = 1 \cdot 2^2 + 1 \cdot 2^5 + 1 \cdot 2^6.$$

(β) Η 3-αδική αναπαράσταση του 100 είναι $100 = 1 + 2 \cdot 3^2 + 1 \cdot 3^4$.

1.3 Μέγιστος κοινός διαιρέτης

Έστω a και b δύο φυσικοί αριθμοί. Οι a και b έχουν τουλάχιστον έναν κοινό διαιρέτη, τον 1. Σκοπός μας είναι να αποδείξουμε ότι υπάρχει μέγιστος φυσικός αριθμός d ο οποίος διαιρεί τους a και b. Η ιδέα πίσω από την απόδειξη που θα δώσουμε είναι να θεωρήσουμε το σύνολο I όλων των θετικών *ακεραίων συνδυασμών* $au + bv$ των a, b, όπου $u, v \in \mathbb{Z}$. Τέτοιοι θετικοί συνδυασμοί υπάρχουν: για παράδειγμα, $a = a \cdot 1 + b \cdot 0$. Η βασική παρατήρηση είναι ότι κάθε κοινός διαιρέτης k των a, b διαιρεί κάθε στοιχείο του I, άρα δεν ξεπερνάει το ελάχιστο στοιχείο του I. Αν δείξουμε ότι το ελάχιστο στοιχείο του I *είναι* κοινός διαιρέτης των a, b, τότε θα είναι ο «μέγιστος κοινός διαιρέτης» τους.

Θεώρημα 1.3.1. *Έστω $a, b \in \mathbb{N}$. Υπάρχει μοναδικός $d \in \mathbb{N}$, τέτοιος ώστε:*

(i) $d \mid a$ και $d \mid b$.

(ii) Αν για κάποιον $k \in \mathbb{N}$ έχουμε $k \mid a$ και $k \mid b$, τότε $k \mid d$. Ειδικότερα, $k \leq d$.

Επιπλέον, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $d = ax + by$.

Απόδειξη. Θεωρούμε το σύνολο

$$I = \{au + bv : \ u, v \in \mathbb{Z}\} \cap \mathbb{N}. \tag{1.3.1}$$

Είναι φανερό ότι το I είναι μη κενό, για παράδειγμα $a, b \in I$. Από την αρχή του ελαχίστου, το I έχει ελάχιστο στοιχείο d το οποίο γράφεται στη μορφή $d = ax + by$ για κάποιους $x, y \in \mathbb{Z}$.

Θα δείξουμε ότι ο d διαιρεί κάθε στοιχείο του I. Ας υποθέσουμε ότι $z = au + bv \in I$. Από την ταυτότητα της Διαίρεσης υπάρχουν $q, r \in \mathbb{Z}$ με $0 \leq r < d$ και $z = dq + r$. Παρατηρούμε ότι:

$$r = z - dq = au + bv - (ax + by)q = a(u - xq) + b(v - yq) \in I. \tag{1.3.2}$$

Αν ήταν $0 < r < d$ τότε ο r θα ήταν στοιχείο του I μικρότερο από τον d, άτοπο από τον τρόπο ορισμού του d. Άρα $r = 0$, πράγμα αποδεικνύει ότι ο d διαιρεί τον z.

Αφού $a, b \in I$, ο d διαιρεί τους a και b. Αυτός είναι ο πρώτος ισχυρισμός του θεωρήματος. Για τον δεύτερο, παρατηρούμε ότι αν $k \mid a$ και $k \mid b$ τότε

$$k \mid ax + by = d. \tag{1.3.3}$$

Για τη μοναδικότητα του d παρατηρήστε ότι αν οι φυσικοί αριθμοί d_1 και d_2 ικανοποιούν τα (i) και (ii) τότε $d_1 \mid d_2$ και $d_2 \mid d_1$. Ειδικότερα $d_1 \leq d_2$ και $d_2 \leq d_1$, άρα $d_1 = d_2$. □

Ο αριθμός d που ορίζεται από το Θεώρημα 1.3.1 καλείται *μέγιστος κοινός διαιρέτης* των a και b, και συμβολίζεται με $d = (a, b)$. Λέμε ότι δύο αριθμοί $a, b \in \mathbb{N}$ είναι *σχετικά πρώτοι* αν $(a, b) = 1$. Για παράδειγμα, οι 8 και 15 είναι σχετικά πρώτοι: $(8, 15) = 1$.

Παρατήρηση 1.3.2. Είναι χρήσιμο να θυμάται κανείς ότι ο μέγιστος κοινός διαιρέτης (a, b) των φυσικών αριθμών a και b είναι ο *ελάχιστος θετικός ακέραιος συνδυασμός* τους:

$$(a, b) = \min\{au + bv : \ u, v \in \mathbb{Z}\} \cap \mathbb{N}.$$

Ο *αλγόριθμος του Ευκλείδη* μας δίνει έναν πρακτικό τρόπο υπολογισμού του μέγιστου κοινού διαιρέτη δύο φυσικών αριθμών. Ξεκινάμε με δύο φυσικούς αριθμούς $a < b$. Από την ταυτότητα της διαίρεσης έχουμε

$$b = aq_1 + r_1$$

για κάποιους (μονοσήμαντα ορισμένους) $q_1 \in \mathbb{N}$ και $0 \leq r_1 < a$. Αν $r_1 = 0$ σταματάμε, αλλιώς γράφουμε την ταυτότητα της διαίρεσης του a με τον r_1:

$$a = r_1 q_2 + r_2,$$

για κάποιους (μονοσήμαντα ορισμένους) $q_2 \in \mathbb{N}$ και $0 \leq r_2 < r_1$. Συνεχίζουμε με τον ίδιο τρόπο. Η διαδικασία πρέπει κάποια στιγμή να καταλήξει σε υπόλοιπο $r_{n+1} = 0$. Αλλιώς, θα είχαμε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών αριθμών: $a > r_1 > r_2 > \cdots > r_n > r_{n+1} > \cdots$. Το επόμενο θεώρημα δείχνει ότι ο μέγιστος κοινός διαιρέτης των a και b είναι το τελευταίο μη μηδενικό υπόλοιπο: $(a, b) = r_n$ (αν $r_1 = 0$, τότε $a \mid b$ και $(a, b) = a$).

Θεώρημα 1.3.3. *Υποθέτουμε ότι $a, b \in \mathbb{N}$ και $a < b$. Ας υποθέσουμε ότι έχουμε βρεί $q_1, \ldots, q_{n+1} \in \mathbb{N}$ και $r_1, \ldots, r_n \in \mathbb{N}$ με $0 < r_n < r_{n-1} \cdots < r_1 < a$ και*

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ \vdots &= \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Τότε $(a, b) = r_n$.

Απόδειξη. Θα δείξουμε ότι

$$(a, b) = (a, r_1). \tag{1.3.4}$$

Θέτουμε $d_1 = (a, b)$ και $d_2 = (a, r_1)$. Έχουμε $d_1 \mid a$ και $d_1 \mid b$, άρα $d_1 \mid b - aq_1 = r_1$. Αφού $d_1 \mid a$ και $d_1 \mid r_1$, το Θεώρημα 1.3.1 δείχνει ότι

$$d_1 \mid (a, r_1) = d_2. \tag{1.3.5}$$

Από την άλλη πλευρά, $d_2 \mid a$ και $d_2 \mid r_1$, άρα $d_2 \mid aq_1 + r_1 = b$. Αφού $d_2 \mid a$ και $d_2 \mid b$, το Θεώρημα 1.3.1 δείχνει ότι

$$d_2 \mid (a, b) = d_1. \tag{1.3.6}$$

Από τις (1.3.5) και (1.3.6) συμπεραίνουμε ότι $d_1 = d_2$. Επαναλαμβάνοντας το ίδιο επιχείρημα, παίρνουμε

$$(a, b) = (a, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n). \tag{1.3.7}$$

Όμως

$$(r_{n-1}, r_n) = (r_n q_{n+1}, r_n) = r_n, \tag{1.3.8}$$

δηλαδή $(a, b) = r_n$. □

Παράδειγμα 1.3.4. Θα υπολογίσουμε τον $(391, 2533)$. Με διαδοχικές διαιρέσεις παίρνουμε

$$\begin{aligned} 2533 &= 391 \cdot 6 + 187, \\ 391 &= 187 \cdot 2 + 17, \\ 187 &= 17 \cdot 11. \end{aligned}$$

Από το Θεώρημα 1.3.3 (με $a = 391$ και $b = 2533$) συμπεραίνουμε ότι $(391, 2533) = 17$. Παρατηρήστε ότι η ίδια διαδικασία μας επιτρέπει να βρούμε ακεραίους x και y για τους οποίους $17 = 391x + 2533y$. Έχουμε

$$\begin{aligned} 17 &= 391 - 187 \cdot 2 \\ &= 391 - (2533 - 391 \cdot 6) \cdot 2 \\ &= 391 \cdot 13 + 2533 \cdot (-2), \end{aligned}$$

δηλαδή $x = 13$ και $y = -2$.

1.4 Βασικά λήμματα διαιρετότητας

Σε αυτή τη σύντομη παράγραφο αποδεικνύουμε κάποια στοιχειώδη αλλά πολύ βασικά λήμματα σχετικά με τη διαιρετότητα, τα οποία θα χρησιμοποιούμε συχνά στη συνέχεια.

Λήμμα 1.4.1. *Αν $a, b \in \mathbb{N}$ και $d = (a, b)$ τότε έχουμε $a = du$ και $b = dv$ για ακεραίους $u, v \in \mathbb{N}$ με $(u, v) = 1$.*

Απόδειξη. Εφόσον $d \mid a$ και $d \mid b$ μπορούμε να γράψουμε $a = du$ και $b = dv$ με $u, v \in \mathbb{N}$. Από το Θεώρημα 1.3.1 υπάρχουν ακέραιοι x και y τέτοιοι ώστε $d = ax + by$ και συνεπώς $d = dux + dvy$ και $1 = ux + vy$. Από την τελευταία ισότητα προκύπτει ότι κάθε κοινός διαιρέτης των u και v θα πρέπει να διαιρεί το 1 και επομένως $(u, v) = 1$. □

Λήμμα 1.4.2. *Έστω $r_1, r_2 \in \mathbb{N}$ με $(r_1, r_2) = 1$. Αν $r_1 \mid r_2 m$ για κάποιον $m \in \mathbb{N}$, τότε $r_1 \mid m$.*

Απόδειξη. Υπάρχουν ακέραιοι x και y τέτοιοι ώστε $r_1 x + r_2 y = 1$. Άρα

$$r_1 mx + r_2 my = m. \tag{1.4.1}$$

Όμως $r_1 \mid r_1 mx$ και $r_1 \mid r_2 m \Rightarrow r_1 \mid r_2 my$. Άρα $r_1 \mid (r_1 mx + r_2 my) = m$. □

Παράδειγμα 1.4.3. Αν $8 \mid 3m$ τότε $8 \mid m$.

Λήμμα 1.4.4. *Έστω $r_1, r_2 \in \mathbb{N}$ με $(r_1, r_2) = 1$. Αν $r_1 \mid m$ και $r_2 \mid m$ για κάποιον $m \in \mathbb{N}$, τότε $r_1 r_2 \mid m$.*

Απόδειξη. Υπάρχουν ακέραιοι x και y τέτοιοι ώστε $r_1 x + r_2 y = 1$. Άρα

$$r_1 mx + r_2 my = m. \tag{1.4.2}$$

Αφού $r_2 \mid m$ έχουμε $r_1 r_2 \mid r_1 mx$ και αφού $r_1 \mid m$ έχουμε $r_1 r_2 \mid r_2 my$. Άρα $r_1 r_2 \mid (r_1 mx + r_2 my) = m$. □

Παράδειγμα 1.4.5. Για να δείξουμε ότι $24 \mid m$, αρκεί να δείξουμε ότι $8 \mid m$ και $3 \mid m$.

Ένα πολύ χρήσιμο αποτέλεσμα σχετικά με τη διαιρετότητα είναι το εξής.

Λήμμα 1.4.6. *Έστω $a, b, w \in \mathbb{N}$ με $(a, b) = 1$. Αν $w \mid ab$ τότε υπάρχουν μοναδικοί φυσικοί u, v τέτοιοι ώστε $w = uv$ και $u \mid a$, $v \mid b$. Επιπλέον έχουμε $(u, v) = 1$.*

Απόδειξη. Έστω $u = (w, a)$. Από το Λήμμα 1.4.1 μπορούμε να γράψουμε $w = uv$ και $a = uv'$ για φυσικούς αριθμούς v και v' με $(v, v') = 1$. Έχουμε $uv = w \mid ab = uv'b$ και συνεπώς $v \mid v'b$. Εφόσον $(v, v') = 1$ από το Λήμμα 1.4.2 προκύπτει ότι $v \mid b$. Ας δούμε γιατί $(u, v) = 1$: ο (u, v) διαιρεί τον u, άρα διαιρεί τον a. Ομοίως ο (u, v) διαιρεί τον v, άρα διαιρεί τον b. Έπεται ότι $(u, v) \mid (a, b) = 1$, οπότε $(u, v) = 1$.

Για τη μοναδικότητα, ας υποθέσουμε ότι $w = u_1 v_1$, όπου $u_1 \mid a$ και $v_1 \mid b$. Από τις $u_1 \mid w$ και $u_1 \mid a$ βλέπουμε ότι $u_1 \mid (w, a) = u$. Επίσης από τις $u \mid a$, $v_1 \mid b$ και $(a, b) = 1$ συμπεραίνουμε όπως παραπάνω ότι $(u, v_1) = 1$. Επομένως από τη σχέση $u \mid w = u_1 v_1$ και το Λήμμα 1.4.2 προκύπτει ότι $u \mid u_1$. Άρα $u_1 = u$ και συνεπώς $v_1 = v$. □

1.5 Ανάλυση σε γινόμενο πρώτων παραγόντων

Έστω $a > 1$ ένας φυσικός αριθμός. Θα λέμε ότι ο a είναι *πρώτος* αν έχει ακριβώς δύο θετικούς διαιρέτες, τον 1 και τον a. Αν ο a δεν είναι πρώτος, θα λέγεται *σύνθετος*. Για διάφορους λόγους είναι βολικό να μην κατατάξουμε τον 1 ούτε στους πρώτους ούτε στους σύνθετους αριθμούς.

Σε ότι ακολουθεί, με το σύμβολο p θα εννοούμε πάντα κάποιον πρώτο αριθμό. Το πρώτο μας αποτέλεσμα είναι απλή συνέπεια του Λήμματος 1.4.2.

Θεώρημα 1.5.1. *Έστω $a, b \in \mathbb{N}$ και p ένας πρώτος αριθμός. Αν $p \mid ab$ τότε $p \mid a$ ή $p \mid b$.*

Απόδειξη. Έστω ότι ο p δεν διαιρεί τον a. Αφού οι μόνοι διαιρέτες του p είναι ο 1 και ο p έχουμε $(a, p) = 1$. Από το Λήμμα 1.4.2 έπεται ότι $p \mid b$. □

Με επαγωγή ως προς k παίρνουμε την εξής γενίκευση.

Θεώρημα 1.5.2. *Έστω $a_1, \ldots, a_k \in \mathbb{N}$ και p ένας πρώτος αριθμός. Αν $p \mid a_1 \cdots a_k$ τότε $p \mid a_j$ για τουλάχιστον ένα $j \in \{1, \ldots, k\}$.*

Το *θεμελιώδες θεώρημα της αριθμητικής* μας λέει ότι κάθε φυσικός αριθμός αναλύεται (ουσιαστικά) μονοσήμαντα σε γινόμενο πρώτων παραγόντων.

Θεώρημα 1.5.3. *Κάθε φυσικός αριθμός $n > 1$ αναπαρίσταται σα γινόμενο πρώτων αριθμών. Η αναπαράσταση αυτή είναι μοναδική αν αγνοήσουμε τη διάταξη των παραγόντων του γινομένου.*

Σημείωση: Κάθε πρώτος θεωρείται γινόμενο πρώτων (με έναν όρο). Ένας βασικός λόγος που δεν θεωρούμε τον 1 πρώτο είναι για να εξασφαλίσουμε τη μοναδικότητα σε αυτό το θεώρημα (αλλιώς, θα είχαμε για παράδειγμα $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3$).

Απόδειξη. Δείχνουμε πρώτα με επαγωγή ως προς n ότι κάθε ακέραιος $n \geq 2$ γράφεται σα γινόμενο πρώτων. Ο 2 είναι προφανώς γινόμενο πρώτων. Η επαγωγική υπόθεση είναι ότι κάθε $m \in \mathbb{N}$ με $2 \leq m < n$ γράφεται ως γινόμενο πρώτων. Αν ο n είναι πρώτος, δεν έχουμε τίποτα να δείξουμε. Αν ο n είναι σύνθετος, υπάρχουν $n_1, n_2 \in \mathbb{N}$ με $2 \leq n_1, n_2 < n$, τέτοιοι ώστε $n = n_1 n_2$. Από την επαγωγική υπόθεση, καθένας από τους n_1, n_2 αναπαρίσταται σα γινόμενο πρώτων, οπότε το ίδιο ισχύει και για τον $n = n_1 n_2$.

Δείχνουμε τώρα τη μοναδικότητα. Ας υποθέσουμε ότι

$$n = p_1 \cdots p_r = q_1 \cdots q_s, \tag{1.5.1}$$

όπου οι $p_1 \leq \cdots \leq p_r$ και $q_1 \leq \cdots \leq q_s$ είναι πρώτοι. Αφού $p_1 \mid q_1 \cdots q_s$, το Θεώρημα 1.5.2 δείχνει ότι υπάρχει $j \leq s$ τέτοιος ώστε $p_1 \mid q_j$. Αφού οι p_1 και q_j είναι πρώτοι, αναγκαστικά έχουμε $p_1 = q_j$. Ομοίως, αφού $q_1 \mid p_1 \cdots p_r$, υπάρχει $i \leq r$ τέτοιος ώστε $q_1 \mid p_i$, απ' όπου παίρνουμε $q_1 = p_i$. Παρατηρούμε ότι

$$p_1 = q_j \geq q_1 = p_i \geq p_1, \tag{1.5.2}$$

άρα $p_1 = q_1$. Τώρα η (1.5.1) παίρνει τη μορφή

$$p_2 \cdots p_r = q_2 \cdots q_s. \tag{1.5.3}$$

Επαναλαμβάνοντας την ίδια διαδικασία πεπερασμένες το πλήθος φορές, συμπεραίνουμε ότι $r = s$ και $p_i = q_i$ για κάθε $i = 1, \ldots, r$. □

Αν πάρουμε κατά ομάδες τους ίσους πρώτους που εμφανίζονται στην αναπαράσταση του Θεωρήματος 1.5.3, παίρνουμε αμέσως το εξής.

Θεώρημα 1.5.4. *Κάθε φυσικός αριθμός $n \geq 2$ αναπαρίσταται μονοσήμαντα στη μορφή*

$$n = p_1^{k_1} \cdots p_r^{k_r}, \tag{1.5.4}$$

όπου $p_1 < \cdots < p_r$ είναι πρώτοι αριθμοί και $k_1, \ldots, k_r \in \mathbb{N}$.

Θα λέμε ότι η αναπαράσταση της (1.5.4) είναι η *κανονική αναπαράσταση* του φυσικού αριθμού n.

1.6 Η απειρία των πρώτων αριθμών

Η πρώτη σημαντική συνέπεια του θεμελιώδους θεωρήματος της αριθμητικής είναι το *θεώρημα του Ευκλείδη* για την απειρία των πρώτων αριθμών.

Θεώρημα 1.6.1. *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Θα δώσουμε τέσσερις διαφορετικές αποδείξεις αυτού του θεωρήματος. Οι τρεις τελευταίες εξασφαλίζουν την απειρία των πρώτων, δίνουν όμως και περισσότερες πληροφορίες για την *άπειρη ακολουθία* των πρώτων αριθμών.

Πρώτη απόδειξη: Το επιχείρημα είναι αυτό που χρησιμοποίησε ο Ευκλείδης. Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι αριθμοί, οι $p_1 < \cdots < p_r$. Θεωρούμε τον φυσικό αριθμό

$$n = p_1 \cdots p_r + 1. \tag{1.6.1}$$

Ο n είναι μεγαλύτερος από 1, άρα έχει πρώτο διαιρέτη. Αφού το $\{p_1, \ldots, p_r\}$ είναι το σύνολο *όλων* των πρώτων αριθμών, υπάρχει $j \leq r$ τέτοιος ώστε $p_j \mid n$. Όμως $p_j \mid p_1 \cdots p_r$, άρα

$$p_j \mid (n - p_1 \cdots p_r) \text{ δηλαδή } p_j \mid 1. \tag{1.6.2}$$

Αυτό είναι άτοπο, άρα υπάρχουν άπειροι πρώτοι. □

Η επόμενη απόδειξη χρησιμοποιεί τους *αριθμούς του Fermat*.

Δεύτερη απόδειξη: Για κάθε $n = 0, 1, 2, \ldots$ ορίζουμε

$$F_n = 2^{2^n} + 1. \tag{1.6.3}$$

Οι αριθμοί F_n λέγονται αριθμοί του Fermat. Αφού $F_n \geq 2$ για κάθε $n \geq 0$, κάθε F_n έχει τουλάχιστον έναν πρώτο διαιρέτη q_n. Θα δείξουμε ότι

$$n \neq m \Longrightarrow (F_n, F_m) = 1. \tag{1.6.4}$$

Οποιοιδήποτε δύο αριθμοί του Fermat είναι σχετικά πρώτοι, άρα

$$n \neq m \Longrightarrow q_n \neq q_m. \tag{1.6.5}$$

(γιατί;) Έπεται ότι οι q_n, $n \geq 0$, είναι διακεκριμένοι πρώτοι, το οποίο δείχνει την απειρία των πρώτων αριθμών.

Για την απόδειξη της (1.6.3) δείχνουμε πρώτα με επαγωγή το εξής: αν $n \geq 1$, τότε

$$\prod_{j=0}^{n-1} F_j = F_n - 2. \tag{1.6.6}$$

Η (1.6.5) ισχύει αν $n = 1$: $F_0 = 3 = 5 - 2 = F_1 - 2$. Αν δεχτούμε ότι ισχύει για $n = k$, τότε

$$\begin{aligned} \prod_{j=0}^{k} F_j &= \left(\prod_{j=0}^{k-1} F_j \right) \cdot F_k = (F_k - 2) \cdot F_k \\ &= (2^{2^k} - 1)(2^{2^k} + 1) = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2, \end{aligned}$$

δηλαδή η (1.6.5) ισχύει για $n = k+1$. Έστω τώρα $0 \leq m < n$ και έστω d ένας κοινός θετικός διαιρέτης των F_m και F_n. Τότε

$$d \mid F_m \mid \prod_{j=0}^{n-1} F_j = F_n - 2, \tag{1.6.7}$$

άρα $d \mid F_n$ και $d \mid (F_n - 2)$. Έπεται ότι $d \mid 2$, άρα $d = 1$ ή $d = 2$. Αφού όλοι οι αριθμοί του Fermat είναι περιττοί, ο d δεν μπορεί να ισούται με 2. Άρα $(F_n, F_m) = 1$. □

Η πρώτη απόδειξη (του Ευκλείδη) είναι πολύ πιο σύντομη και κομψή. Κοιτάζοντας όμως τη δεύτερη απόδειξη παρατηρούμε το εξής: αν $p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots$ είναι η άπειρη ακολουθία των πρώτων αριθμών, τότε

$$p_n \leq F_{n-1} = 2^{2^{n-1}} + 1 \tag{1.6.8}$$

για κάθε $n \in \mathbb{N}$. Πράγματι, οι $F_0, F_1, \ldots, F_{n-1}$ έχουν n διακεκριμένους πρώτους διαιρέτες $p_{k_1}, \ldots, p_{k_n}$, άρα

$$p_n \leq \max\{p_{k_1}, \ldots, p_{k_n}\} \leq \max\{F_0, F_1, \ldots, F_{n-1}\} = F_{n-1}. \tag{1.6.9}$$

Η παρατήρηση αυτή μας οδηγεί στον ορισμό μιας συνάρτησης $\pi : \mathbb{R} \to \mathbb{R}$, με

$$\pi(x) = \text{ το πλήθος των πρώτων αριθμών } p \leq x. \tag{1.6.10}$$

Η π είναι αύξουσα, και βέβαια $\pi(x) = 0$ αν $x < 2$. Παρατηρούμε ότι αν $x \geq 2$ και αν $n = n(x)$ είναι ο μεγαλύτερος μη αρνητικός ακέραιος για τον οποίο $2^{2^n} + 1 \leq x$, τότε

$$\pi(x) \geq \pi\big(2^{2^n} + 1\big) \geq n + 1. \tag{1.6.11}$$

Από την άλλη πλευρά, $2^{2^{n+1}} \geq x$ άρα $\log_2(\log_2 x) \leq n + 1$. Έχουμε λοιπόν το εξής κάτω φράγμα για την $\pi(x)$.

Πρόταση 1.6.2. *Για κάθε πραγματικό αριθμό $x \geq 2$ ισχύει η ανισότητα*

$$\pi(x) \geq \log_2(\log_2 x). \tag{1.6.12}$$

Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι.

Με άλλα λόγια, η δεύτερη απόδειξη μας δίνει επιπλέον πληροφορίες για το πλήθος των πρώτων αριθμών σε ένα διάστημα της μορφής $[0, x]$, όπου x είναι ένας «μεγάλος» θετικός πραγματικός αριθμός. Η επόμενη απόδειξη που θα δώσουμε δίνει ακόμα καλύτερο κάτω φράγμα για τη συνάρτηση $\pi(x)$.

Τρίτη απόδειξη: Θεωρούμε την (ενδεχομένως πεπερασμένη) ακολουθία των πρώτων αριθμών σε αύξουσα διάταξη: $p_1 < p_2 < \cdots < p_k < \cdots$. Αν $f(t) = 1/t$, τότε για κάθε $n \geq 2$ και για κάθε $n \leq x < n + 1$ έχουμε

$$\begin{aligned} \ln x &= \int_1^x \frac{1}{t} dt \leq \int_1^2 \frac{1}{t} dt + \int_2^3 \frac{1}{t} dt + \cdots + \int_n^{n+1} \frac{1}{t} dt \\ &\leq 1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \sum_{m \in A(x)} \frac{1}{m}, \end{aligned}$$

όπου $A(x)$ είναι το σύνολο όλων των φυσικών αριθμών που *όλοι* οι πρώτοι διαιρέτες τους είναι μικρότεροι ή ίσοι από x. Το σύνολο $A(x)$ περιγράφεται με τη βοήθεια του θεμελιώδους θεωρήματος της αριθμητικής:

$$A(x) = \left\{ n = \prod_{k=1}^{\pi(x)} p_k^{r_k} : r_k \geq 0 \right\}. \tag{1.6.13}$$

Παρατηρήστε ότι ο 1 προκύπτει αν πάρουμε όλους τους εκθέτες r_k ίσους με 0. Χρησιμοποιώντας την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση ελέγχουμε ότι

$$\sum_{m \in A(x)} \frac{1}{m} = \prod_{k=1}^{\pi(x)} \left(\sum_{s=0}^{\infty} \frac{1}{p_k^s} \right). \tag{1.6.14}$$

Στην παρένθεση έχουμε μια γεωμετρική σειρά με λόγο $1/p_k$, άρα

$$\sum_{s=0}^{\infty} \frac{1}{p_k^s} = \frac{1}{1 - \frac{1}{p_k}} = \frac{p_k}{p_k - 1}. \tag{1.6.15}$$

Έπεται ότι

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}. \tag{1.6.16}$$

Από την προφανή ανισότητα $p_k \geq k+1$ βλέπουμε ότι

$$\frac{p_k}{p_k + 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}. \tag{1.6.17}$$

Επιστρέφοντας στην (1.6.15) παίρνουμε

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1. \tag{1.6.18}$$

Δηλαδή, έχουμε αποδείξει την εξής βελτίωση του Θεωρήματος 1.6.1.

Πρόταση 1.6.3. *Για κάθε πραγματικό αριθμό $x \geq 2$ ισχύει η ανισότητα*

$$\pi(x) \geq \ln x - 1. \tag{1.6.19}$$

Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι.

Η τελευταία απόδειξη που θα δώσουμε εξασφαλίζει την απειρία των πρώτων με τον εξής τρόπο: η σειρά

$$\sum_{p \in P} \frac{1}{p} \tag{1.6.20}$$

αποκλίνει (P είναι το σύνολο των πρώτων αριθμών). Επομένως, το πλήθος των προσθετέων (δηλαδή, το πλήθος των πρώτων αριθμών) αποκλείεται να είναι πεπερασμένο. Η πρώτη απόδειξη αυτού του αποτελέσματος δόθηκε από τον Euler. Επί τη ευκαιρία, υπενθυμίζουμε τον ορισμό και τις βασικές ιδιότητες της συνάρτησης του ακεραίου μέρους.

Ορισμός 1.6.4. Έστω $x \in \mathbb{R}$. Το *ακέραιο μέρος* $[x]$ του x είναι ο μοναδικός ακέραιος m που ικανοποιεί τις ανισότητες $m \leq x < m+1$. Η απεικόνιση $x \mapsto [x]$ καλείται *συνάρτηση του ακεραίου μέρους*.

Πρόταση 1.6.5. *Για κάθε $x, y \in \mathbb{R}$ ισχύουν τα εξής.*

(i) $x - 1 < [x] \leq x$ *και* $0 \leq x - [x] < 1$.

(ii) Αν $x \geq 0$, τότε ο $[x]$ ισούται με το πλήθος των φυσικών που δεν ξεπερνούν τον x. Δηλαδή

$$[x] = \sum_{1 \leq n \leq x} 1.$$

(iii) Για κάθε $k \in \mathbb{Z}$ έχουμε $[x+k] = [x] + k$.

(iv) $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$.

(v) Αν $x \in \mathbb{Z}$ τότε $[x] + [-x] = 0$, ενώ αν $x \notin \mathbb{Z}$ τότε $[x] + [-x] = -1$.

(vi) Αν $x > 0$ και $k \in \mathbb{N}$, τότε $[x/k]$ είναι το πλήθος των πολλαπλασίων του k που δεν ξεπερνούν τον x.

Η απόδειξη αυτών των ιδιοτήτων είναι απλή και αφήνεται ως άσκηση για τον αναγνώστη.

Τέταρτη απόδειξη (Erdös): Έστω $P = \{p_1, p_2, \ldots\}$ το σύνολο των πρώτων αριθμών, τους οποίους θεωρούμε σε αύξουσα διάταξη. Ας υποθέσουμε ότι η σειρά $\sum_{i\geq 1} \frac{1}{p_i}$ συγκλίνει. Τότε υπάρχει φυσικός αριθμός k με την ιδιότητα

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}. \tag{1.6.21}$$

Θα λέμε ότι οι $p_1, \ldots, p_k$ είναι οι *μικροί* πρώτοι, ενώ οι $p_{k+1}, \ldots$ είναι οι *μεγάλοι* πρώτοι. Για κάθε φυσικό αριθμό N έχουμε

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1.6.22}$$

Γράφουμε N_b για το πλήθος των φυσικών $n \leq N$ που έχουν τουλάχιστον έναν μεγάλο πρώτο διαιρέτη, και N_s για το πλήθος των φυσικών $n \leq N$ που όλοι οι πρώτοι διαιρέτες τους είναι μικροί. Από τον ορισμό των N_b και N_s έχουμε

$$N_b + N_s = N. \tag{1.6.23}$$

Παρατηρούμε ότι το πλήθος των φυσικών $n \leq N$ που είναι πολλαπλάσια κάποιου πρώτου p_i ισούται με $[N/p_i]$. Άρα χρησιμοποιώντας και την (1.6.21) παίρνουμε

$$N_b \leq \sum_{i\geq k+1} \left[\frac{N}{p_i}\right] \leq \sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1.6.24}$$

Ας δούμε τώρα πώς μπορεί κανείς να φράξει τον N_s. Κάθε φυσικός $n \leq N$ που έχει μόνο μικρούς πρώτους διαιρέτες, γράφεται στη μορφή $n = a_n b_n^2$, όπου ο a_n είναι γινόμενο διακεκριμένων πρώτων (άσκηση). Αφού αυτοί οι πρώτοι είναι κάποιοι από τους $p_1, \ldots, p_k$, έχουμε το πολύ 2^k επιλογές για τον a_n. Επιπλέον $b_n^2 \leq n \leq N$, άρα $b_n \leq \sqrt{N}$. Δηλαδή έχουμε το πολύ $\sqrt{N}$ επιλογές για τον b_n. Έπεται ότι

$$N_s \leq 2^k \sqrt{N}. \tag{1.6.25}$$

Από τις προηγούμενες τρείς σχέσεις παίρνουμε

$$N = N_b + N_s \leq \frac{N}{2} + 2^k \sqrt{N}, \tag{1.6.26}$$

δηλαδή

$$\sqrt{N} \leq 2^{k+1}. \tag{1.6.27}$$

Αυτό όμως δεν μπορεί να ισχύει για κάθε φυσικό αριθμό N: τότε το $\mathbb{N}$ θα ήταν άνω φραγμένο. Καταλήξαμε σε άτοπο, άρα η σειρά $\sum_{i\geq 1} \frac{1}{p_i}$ αποκλίνει. Ειδικότερα, υπάρχουν άπειροι πρώτοι.

Το πρόβλημα της ασυμπτωτικής συμπεριφοράς της συνάρτησης $\pi(x)$ καθώς το $x \to +\infty$ απασχόλησε έντονα τους μαθηματικούς κατά τον 19ο αιώνα. Ο Legendre (1798) έκανε την εικασία ότι για μεγάλα x ο αριθμός $\pi(x)$ είναι περίπου ίσος με

$$\pi(x) \simeq \frac{x}{\ln x - A}, \tag{1.6.28}$$

όπου $A \simeq 1.08366$. Ο Gauss πρότεινε την προσέγγιση

$$\pi(x) \simeq \int_2^x \frac{1}{\ln t} dt. \tag{1.6.29}$$

Το ολοκλήρωμα στο δεξιό μέλος είναι ουσιαστικά ίσο με $x/\ln x$ για μεγάλα x, οπότε μια ισχυρή εικασία που προκύπτει από την (1.6.28) είναι η

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1. \tag{1.6.30}$$

Ο Chebyshev (1848) έδειξε ότι αν το όριο στην (1.6.29) υπάρχει, τότε θα είναι υποχρεωτικά ίσο με 1. Λίγο αργότερα (1850) έδειξε ότι υπάρχουν δύο θετικές σταθερές c_1 και c_2 τέτοιες ώστε

$$c_1 \frac{x}{\ln x} \le \pi(x) \le c_2 \frac{x}{\ln x} \tag{1.6.31}$$

για κάθε $x \ge 2$. Δηλαδή, η σωστή τάξη μεγέθους του $\pi(x)$ είναι $x/\ln x$ (συγκρίνετε με το πολύ ασθενέστερο κάτω φράγμα $\ln x - 1$ που δίνει η Πρόταση 1.6.2).

Πολύ νωρίτερα, ο Euler (1740) είχε εισαγάγει τη συνάρτηση

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1.6.32}$$

για πραγματικές τιμές της μεταβλητής s και είχε παρατηρήσει ότι αναπαρίσταται σαν απειρογινόμενο:

$$\zeta(s) = \prod_{p\in P} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{1.6.33}$$

Ο Riemann (1860) παρατήρησε ότι αυτή η ταυτότητα θα μπορούσε να οδηγήσει σε χρήσιμα συμπεράσματα για την κατανομή των πρώτων αριθμών αν θεωρούσε κανείς τη συνάρτηση ζ σαν συνάρτηση μιας μιγαδικής μεταβλητής s και χρησιμοποιούσε τις μεθόδους της μιγαδικής ανάλυσης. Ο συμβολισμός $\zeta(s)$ οφείλεται στον Riemann, και η συνάρτηση αυτή είναι γνωστή με το όνομα «συνάρτηση Ζήτα του Riemann».

Το 1896, οι Hadamard και de la Vallée Poussin έδειξαν ανεξάρτητα και σχεδόν ταυτόχρονα ότι το όριο στην (1.6.29) υπάρχει και είναι ίσο με 1. Το αποτέλεσμα αυτό είναι γνωστό ως το «Θεώρημα των πρώτων αριθμών». Από τη δουλειά του de la Vallée Poussin έπεται ότι το ολοκλήρωμα (1.6.29) που πρότεινε ο Gauss δίνει καλύτερη προσέγγιση για την τιμή του $\pi(x)$ απ' ότι δίνει η (1.6.28), όποια τιμή κι αν δοκιμάσει κανείς για τη σταθερά A.

1.7 Μια γραμμική διοφαντική εξίσωση

Με τον όρο *διοφαντική εξίσωση* εννοούμε μια εξίσωση της μορφής

$$f(x_1, \ldots, x_k) = b, \tag{1.7.1}$$

για την οποία ψάχνουμε λύσεις στους ρητούς, τους ακέραιους ή τους μη αρνητικούς ακέραιους αριθμούς. Δηλαδή, οι τιμές των μεταβλητών $x_1, \ldots, x_k$ είναι στο $\mathbb{Q}$, το $\mathbb{Z}$ ή το $\mathbb{Z}^+$ αντίστοιχα. Συνήθως η συνάρτηση f είναι ένα πολυώνυμο με ρητούς ή ακέραιους συντελεστές.

Σε αυτή την παράγραφο θα μελετήσουμε τη γραμμική διοφαντική εξίσωση

$$a_1x_1 + \cdots + a_kx_k = b, \tag{1.7.2}$$

όπου $a_1, \ldots, a_k, b \in \mathbb{Z}$. Μας ενδιαφέρει να δούμε πότε υπάρχουν ακέραιες λύσεις της (1.7.2), δηλαδή ακέραιοι $x_1, \ldots, x_k$ οι οποίοι την ικανοποιούν. Για απλότητα υποθέτουμε ότι $k = 2$ και ότι $a_1, a_2 \in \mathbb{N}$ (η τελευταία υπόθεση δεν περιορίζει τη γενικότητα - γιατί;).

Θεώρημα 1.7.1. *Έστω a_1, a_2 φυσικοί αριθμοί. Αν $b \in \mathbb{Z}$, τότε υπάρχουν ακέραιοι x_1, x_2 τέτοιοι ώστε*

$$a_1x_1 + a_2x_2 = b \tag{1.7.3}$$

αν και μόνο αν ο b είναι πολλαπλάσιο του (a_1, a_2). Ειδικότερα, η εξίσωση έχει λύση για κάθε $b \in \mathbb{Z}$ αν και μόνο αν $(a_1, a_2) = 1$.

Απόδειξη. Θέτουμε $d = (a_1, a_2)$. Ας υποθέσουμε ότι για κάποιον $b \in \mathbb{Z}$ η εξίσωση έχει ακέραια λύση, τους x_1, x_2. Αφού $d \mid a_1$ και $d \mid a_2$, έχουμε

$$d \mid a_1x_1 + a_2x_2 = b, \tag{1.7.4}$$

δηλαδή ο b είναι πολλαπλάσιο του (a_1, a_2). Αντίστροφα, αν $b = kd$ για κάποιον $k \in \mathbb{Z}$, θα δείξουμε ότι η εξίσωση έχει ακέραια λύση. Από το Θεώρημα 1.3.1 υπάρχουν $y_1, y_2 \in \mathbb{Z}$ τέτοιοι ώστε $a_1y_1 + a_2y_2 = d$. Όμως τότε,

$$a_1(y_1k) + a_2(y_2k) = (a_1y_1 + a_2y_2)k = dk = b, \tag{1.7.5}$$

δηλαδή οι ακέραιοι $x_1 = y_1k$ και $x_2 = y_2k$ είναι μια λύση της (1.7.3).

Από την προηγούμενη ισοδυναμία, η εξίσωση έχει ακέραια λύση για κάθε $b \in \mathbb{Z}$ αν και μόνο αν $(a_1, a_2) \mid b$ για κάθε $b \in \mathbb{Z}$. Όμως ο μόνος φυσικός αριθμός που διαιρεί όλους τους ακεραίους είναι ο 1 (γιατί;). Άρα η εξίσωση έχει ακέραια λύση για κάθε $b \in \mathbb{Z}$ αν και μόνο αν $(a_1, a_2) = 1$. □

Το Θεώρημα 1.7.1 δίνει πλήρη απάντηση στο ερώτημα αν υπάρχουν λύσεις της $a_1x_1 + a_2x_2 = b$. Η απόδειξή του μας δίνει και μια μέθοδο για να βρίσκουμε μια τέτοια λύση. Έχουμε $b = (a_1, a_2)k$ για κάποιον ακέραιο k. Χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη βρίσκουμε ακεραίους y_1 και y_2 τέτοιους ώστε $a_1y_1 + a_2y_2 = (a_1, a_2)$. Τότε οι $x_1 = y_1k$ και $x_2 = y_2k$ δίνουν μια λύση.

Ένα φυσιολογικό ερώτημα είναι τώρα το εξής: πως μπορούμε να βρούμε *όλες* τις λύσεις της εξίσωσης αν γνωρίζουμε μια λύση της. Η απάντηση δίνεται από το επόμενο θεώρημα.

Θεώρημα 1.7.2. *Έστω a_1, a_2 φυσικοί αριθμοί. Αν ο $b \in \mathbb{Z}$ είναι πολλαπλάσιο του $d = (a_1, a_2)$, και αν οι ακέραιοι x_1, x_2 ικανοποιούν την*

$$a_1x_1 + a_2x_2 = b, \tag{1.7.6}$$

τότε οι ακέραιοι y_1 και y_2 είναι λύση της (1.7.6) αν και μόνο αν

$$y_1 = x_1 + (a_2/d)t \text{ και } y_2 = x_2 - (a_1/d)t \tag{1.7.7}$$

για κάποιον $t \in \mathbb{Z}$.

Απόδειξη. Έστω $t \in \mathbb{Z}$. Έχουμε

$$a_1(x_1 + (a_2/d)t) + a_2(x_2 - (a_1/d)t) = a_1x_1 + a_2x_2 + \frac{a_1a_2}{d}t - \frac{a_1a_2}{d}t = b, \quad (1.7.8)$$

δηλαδή οι $y_1 = x_1 + (a_2/d)t$ και $y_2 = x_2 - (a_1/d)t$ είναι λύση της εξίσωσης.
Αντίστροφα: ας υποθέσουμε ότι

$$a_1x_1 + a_2x_2 = b = a_1y_1 + a_2y_2 \quad (1.7.9)$$

για κάποιους ακεραίους y_1 και y_2. Τότε,

$$a_1(y_1 - x_1) = a_2(x_2 - y_2), \quad (1.7.10)$$

άρα

$$r_1(y_1 - x_1) = r_2(x_2 - y_2), \quad (1.7.11)$$

όπου $r_1 = a_1/d$ και $r_2 = a_2/d$. Από το Λήμμα 1.4.1 έχουμε $(r_1, r_2) = 1$. Αφού $r_2 \mid r_1(y_1 - x_1)$, από το Λήμμα 1.4.2 συμπεραίνουμε ότι $r_2 \mid (y_1 - x_1)$. Άρα υπάρχει $t \in \mathbb{Z}$ τέτοιος ώστε $y_1 - x_1 = r_2t$. Επιστρέφοντας στην (1.7.11) έχουμε $r_1r_2t = r_2(x_2 - y_2)$, δηλαδή $y_2 = x_2 - r_1t$. Για την τυχούσα λύση y_1, y_2 της (1.7.6) βρήκαμε $t \in \mathbb{Z}$ τέτοιον ώστε $y_1 = x_1 + r_2t = x_1 + (a_2/d)t$ και $y_2 = x_2 - r_1t = x_2 - (a_1/d)t$. Άρα όλες οι λύσεις είναι αυτής της μορφής. □

Παράδειγμα 1.7.3. Θέλουμε να βρούμε όλες τις ακέραιες λύσεις της εξίσωσης

$$172x + 20y = 1000. \quad (1.7.12)$$

Βήμα 1: Υπολογίζουμε το μέγιστο κοινό διαιρέτη των 172 και 20.

$$\begin{aligned} 172 &= 20 \cdot 8 + 12 \\ 20 &= 12 \cdot 1 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4.2 \end{aligned}$$

Άρα $(172, 20) = 4$.

Βήμα 2: Αφού $4 \mid 1000$, η εξίσωση έχει ακέραιες λύσεις.

Βήμα 3: Βρίσκουμε μια λύση της εξίσωσης.

$$\begin{aligned} 4 &= 12 - 8 = 12 - (20 - 12) = 12 \cdot 2 - 20 \\ &= (172 - 20 \cdot 8) \cdot 2 - 20 = 172 \cdot 2 - 20 \cdot 16 - 20 \\ &= 172 \cdot 2 + 20 \cdot (-17). \end{aligned}$$

Πολλαπλασιάζοντας επί 1000/4=250 παίρνουμε

$$172 \cdot 500 + 20 \cdot (-4250) = 1000.$$

Δηλαδή, μια λύση της εξίσωσης είναι οι $x_1 = 500$ και $x_2 = -4250$.

Βήμα 4: Έχουμε $r_1 = 172/4 = 43$ και $r_2 = 20/4 = 5$.

Βήμα 5: Οι λύσεις της εξίσωσης είναι τα ζευγάρια

$$y_1 = 500 + 5t \text{ και } y_2 = -4250 - 43t$$

όπου ο t διατρέχει τους ακεραίους.

Παρατήρηση 1.7.4. Ας υποθέσουμε ότι μας ζητούν τις μη αρνητικές ή τις θετικές ακέραιες λύσεις μιας γραμμικής διοφαντικής εξίσωσης. Έχοντας βρεί τη γενική μορφή των ακέραιων λύσεων της εξίσωσης, αρκεί πλέον να λύσουμε ένα σύστημα ανισώσεων. Στο συγκεκριμένο παράδειγμα, για να βρούμε τις θετικές ακέραιες λύσεις της εξίσωσης $172x + 20y = 1000$, λύνουμε το σύστημα

$$\begin{aligned} 500 + 5t &> 0 \\ -4250 - 43t &> 0 \end{aligned}$$

ως προς $t \in \mathbb{Z}$. Ζητάμε $t > -100$ και $t < -4250/43 \simeq -98.83\ldots$. Ο μοναδικός ακέραιος που ικανοποιεί τις δύο ανισότητες είναι ο $t_0 = -99$, για τον οποίο παίρνουμε τη μοναδική θετική λύση

$$x_0 = 500 + 5 \cdot (-99) = 5 \text{ και } y_0 = -4250 + 43 \cdot 99 = 7.$$

Πράγματι, $172 \cdot 5 + 20 \cdot 7 = 860 + 140 = 1000$.

1.8 Πυθαγόρειες τριάδες και το «τελευταίο θεώρημα» του Fermat

Πυθαγόρεια τριάδα είναι μια τριάδα φυσικών αριθμών x, y και z που ικανοποιούν την εξίσωση $x^2 + y^2 = z^2$. Προφανώς, αν πολλαπλασιάσουμε τους x, y και z με τον ίδιο φυσικό αριθμό k, θα πάρουμε μια νέα Πυθαγόρεια τριάδα: την $x_1 = kx$, $y_1 = ky$ και $z_1 = kz$. Θα λέμε λοιπόν ότι η Πυθαγόρεια τριάδα x, y, z είναι *πρωταρχική* αν ο μέγιστος κοινός διαιρέτης των x, y και z ισούται με 1. Το πρόβλημα που θα μας απασχολήσει είναι να βρούμε έναν τρόπο να «κατασκευάζουμε συστηματικά» πρωταρχικές Πυθαγόρειες τριάδες.

Ανάλυση: Ας υποθέσουμε ότι $x^2 + y^2 = z^2$ και ότι ο μέγιστος κοινός διαιρέτης των x, y και z ισούται με 1. Τότε οποιοιδήποτε δύο από τους x, y και z είναι σχετικά πρώτοι. Για παράδειγμα, ας υποθέσουμε ότι $d \mid x$ και $d \mid y$. Τότε $d^2 \mid x^2 + y^2 = z^2$, άρα $d \mid z$ (άσκηση). Άρα ο d είναι κοινός διαιρέτης των x, y και z, δηλαδή $d = 1$. Όμοια δείχνουμε ότι $(x, z) = 1$ και $(y, z) = 1$.

Ειδικότερα, τουλάχιστον δύο από τους x, y και z είναι περιττοί. Αν δύο από αυτούς ήταν άρτιοι, τότε δεν θα ήταν σχετικά πρώτοι. Επίσης, οι x, y και z δεν μπορούν να είναι όλοι περιττοί. Τότε ο x^2+y^2 θα ήταν άρτιος ενώ ο z^2 θα ήταν περιττός. Επομένως ακριβώς ένας από τους x, y και z είναι άρτιος.

Η επόμενη παρατήρηση είναι ότι ο z δεν μπορεί να είναι άρτιος. Αφού το τετράγωνο ενός περιττού αριθμού είναι της μορφής $4k+1$, αν ο z ήταν άρτιος θα είχαμε $z^2 = 4m$ και $x^2 + y^2 = 4s + 2$, το οποίο είναι άτοπο.

Μπορούμε λοιπόν να υποθέσουμε, αλλάζοντας τη σειρά των x και y αν χρειαστεί, ότι ισχύει το εξής.

Λήμμα 1.8.1. *Αν x, y, z είναι μια πρωταρχική Πυθαγόρεια τριάδα, τότε ο z είναι περιττός και, χωρίς βλάβη της γενικότητας, ο x είναι άρτιος και ο y περιττός.*

Γράφοντας $x^2 = z^2 - y^2$ και παραγοντοποιώντας, παίρνουμε

$$x^2 = (z + y)(z - y). \tag{1.8.1}$$

Αφού οι y, z είναι περιττοί, οι x, $z+y$ και $z-y$ είναι όλοι άρτιοι. Υπάρχουν λοιπόν φυσικοί u, v και w τέτοιοι ώστε

$$x = 2u, z + y = 2v, z - y = 2w. \tag{1.8.2}$$

Από την (1.8.1) έχουμε $4u^2 = 4vw$, δηλαδή

$$u^2 = vw. \tag{1.8.3}$$

Επίσης $(v, w) = 1$ γιατί $(v, w) \mid v + w = z$, $(v, w) \mid v - w = y$ και $(z, y) = 1$. Το επόμενο λήμμα προκύπτει εύκολα θεωρώντας τις κανονικές αναπαραστάσεις των u, v και w. Παρακάτω δίνουμε μια απόδειξη βασισμένη στο Λήμμα 1.4.6.

Λήμμα 1.8.2. *Έστω u, v και w φυσικοί αριθμοί με $u^2 = vw$ και $(v, w) = 1$. Τότε οι v και w είναι τέλεια τετράγωνα: υπάρχουν m και $s \in \mathbb{N}$ τέτοιοι ώστε $v = m^2$ και $w = s^2$.*

Απόδειξη. Έχουμε $u \mid vw$ με $(v, w) = 1$ και συνεπώς, από το Λήμμα 1.4.4, μπορούμε να γράψουμε $u = ms$ όπου m, s είναι φυσικοί αριθμοί με $m \mid v$ και $s \mid w$. Η σχέση $u^2 = vw$ γράφεται $ms = (v/m) \cdot (w/s)$ και συνεπώς ο m διαιρεί το γινόμενο των ακεραίων v/m και w/s. Προφανώς έχουμε $(m, w) = 1$, άρα και $(m, w/s) = 1$, οπότε από το Λήμμα 1.4.2 θα πρέπει $m \mid v/m$, δηλαδή $v/m^2 \in \mathbb{N}$. Όμοια $w/s^2 \in \mathbb{N}$. Συμπεραίνουμε ότι οι v/m^2 και w/s^2 είναι φυσικοί αριθμοί με γινόμενο ίσο με 1 οπότε υποχρεωτικά $v/m^2 = w/s^2 = 1$, δηλαδή $v = m^2$ και $w = s^2$. □

Οι v και w είναι λοιπόν τέλεια τετράγωνα, επομένως, υπάρχουν φυσικοί m και s τέτοιοι ώστε $v = m^2$ και $w = s^2$. Επιπλέον, αφού $(v, w) = 1$ έχουμε $(m, s) = 1$. Τώρα

$$z = v + w = m^2 + s^2 \text{ και } y = v - w = m^2 - s^2, \tag{1.8.4}$$

άρα $m > s$ και, αφού οι z, y είναι περιττοί, ο ένας από τους m, s είναι άρτιος και ο άλλος περιττός. Τέλος,

$$x^2 = z^2 - y^2 = m^4 + 2m^2s^2 + s^4 - m^4 + 2m^2s^2 - s^4 = 4m^2s^2 = (2ms)^2, \tag{1.8.5}$$

δηλαδή

$$x = 2ms. \tag{1.8.6}$$

Με άλλα λόγια, έχουμε αποδείξει το εξής.

Θεώρημα 1.8.3. *Αν μας δοθεί μια πρωταρχική Πυθαγόρεια τριάδα, μπορούμε να βρούμε φυσικούς m και s με $m > s$ και $(m, s) = 1$, τον έναν περιττό και τον άλλον άρτιο, έτσι ώστε η τριάδα να αποτελείται από τους $x = 2ms, y = m^2 - s^2$ και $z = m^2 + s^2$.*

Όπως δείχνει το επόμενο Θεώρημα, με την ανάλυση που κάναμε έχουμε καταλήξει σε έναν απλό τρόπο «κατασκευής» όλων των πρωταρχικών Πυθαγόρειων τριάδων.

Θεώρημα 1.8.4. *Έστω m και s φυσικοί αριθμοί με $m > s$ και $(m, s) = 1$. Υποθέτουμε επίσης ότι ένας από τους m, s είναι περιττός και ο άλλος άρτιος. Τότε οι αριθμοί $2ms$, $m^2 - s^2$ και $m^2 + s^2$ σχηματίζουν μια πρωταρχική Πυθαγόρεια τριάδα.*

Απόδειξη. Παρατηρούμε πρώτα ότι

$$(2ms)^2 + (m^2 - s^2)^2 = (m^2 + s^2)^2. \tag{1.8.7}$$

Αν δείξουμε ότι $(2ms, m^2 - s^2) = 1$, τότε η τριάδα θα είναι πρωταρχική (γιατί;). Ας υποθέσουμε ότι $d = (2ms, m^2 - s^2) > 1$. Τότε ο d έχει έναν πρώτο παράγοντα p, ο οποίος δεν μπορεί να ισούται με 2 γιατί διαιρεί τον περιττό αριθμό $m^2 - s^2$. Αφού $p \mid 2ms$, ο p διαιρεί κάποιον από τους m και s. Αν ο p διαιρεί τον m, τότε $p \mid m^2$ και $p \mid (m^2 - s^2)$, άρα $p \mid s^2$, δηλαδή $p \mid s$. Όμως οι m, s είναι σχετικά πρώτοι, οπότε καταλήγουμε σε άτοπο. Με τον ίδιο τρόπο καταλήγουμε σε άτοπο αν υποθέσουμε ότι ο p διαιρεί τον s. Δείξαμε ότι $(2ms, m^2 - s^2) = 1$ και συνεπώς οι $2ms$, $m^2 - s^2$, $m^2 + s^2$ σχηματίζουν πρωταρχική Πυθαγόρεια τριάδα. □

Με βάση τα δύο προηγούμενα θεωρήματα μπορούμε πολύ εύκολα να παράγουμε όλες τις πρωταρχικές Πυθαγόρειες τριάδες, ξεκινώντας από τις «μικρότερες»:

- $m = 2$ και $s = 1$: $x = 4$, $y = 3$, $z = 5$
- $m = 3$ και $s = 2$: $x = 12$, $y = 5$, $z = 13$
- $m = 4$ και $s = 1$: $x = 8$, $y = 15$, $z = 17$
- $m = 4$ και $s = 3$: $x = 24$, $y = 7$, $z = 25$
- $m = 5$ και $s = 2$: $x = 20$, $y = 21$, $z = 29$
- $m = 5$ και $s = 4$: $x = 40$, $y = 9$, $z = 41$
- $m = 6$ και $s = 1$: $x = 12$, $y = 35$, $z = 37$
- $m = 6$ και $s = 5$: $x = 60$, $y = 11$, $z = 61$
- $m = 7$ και $s = 2$: $x = 28$, $y = 45$, $z = 53$
- $m = 7$ και $s = 4$: $x = 56$, $y = 33$, $z = 65$
- $m = 7$ και $s = 6$: $x = 84$, $y = 13$, $z = 85$

και ούτω καθεξής.

Τα ορθογώνια τρίγωνα που έχουν πλευρές με μήκη x, y και z που σχηματίζουν Πυθαγόρεια τριάδα λέγονται *Πυθαγόρεια τρίγωνα* και έχουν ενδιαφέρουσες ιδιότητες. Ένα παράδειγμα είναι το εξής.

Παράδειγμα 1.8.5. Θεωρούμε ένα Πυθαγόρειο τρίγωνο με πλευρές που έχουν μήκη x, y και $z \in \mathbb{N}$. Τότε η ακτίνα ρ του εγγεγραμμένου κύκλου του τριγώνου είναι φυσικός αριθμός.

Για την απόδειξη μπορούμε να υποθέσουμε ότι $x^2 + y^2 = z^2$ και ότι η τριάδα x, y, z είναι πρωταρχική (γιατί;). Ενώνοντας το κέντρο του εγγεγραμμένου κύκλου με τις τρείς κορυφές του, χωρίζουμε το αρχικό τρίγωνο σε τρία τρίγωνα με ύψος ρ και αντίστοιχες βάσεις x, y και z. Αφού το αρχικό τρίγωνο είναι ορθογώνιο, το εμβαδόν του εκφράζεται με δύο τρόπους:

$$E = \frac{xy}{2} = \frac{\rho x}{2} + \frac{\rho y}{2} + \frac{\rho z}{2}, \tag{1.8.8}$$

δηλαδή

$$xy = \rho(x + y + z). \tag{1.8.9}$$

Από το Θεώρημα 1.8.3 υπάρχουν $m, s \in \mathbb{N}$ με $m > s$, τέτοιοι ώστε $x = 2ms$, $y = m^2 - s^2$ και $z = m^2 + s^2$. Αντικαθιστώντας στην (1.8.8) παίρνουμε

$$2ms(m^2 - s^2) = \rho(2ms + m^2 - s^2 + m^2 + s^2) = \rho \cdot 2m(m + s), \tag{1.8.10}$$

απ' όπου συμπεραίνουμε ότι

$$\rho = s(m - s) \in \mathbb{N}. \tag{1.8.11}$$

Το «τελευταίο θεώρημα» του Fermat: Η εξίσωση $x^2 + y^2 = z^2$ έχει, όπως είδαμε, άπειρες λύσεις στους φυσικούς αριθμούς. Το (αποδεδειγμένο πλέον) τελευταίο θεώρημα του Fermat είναι ο εξής ισχυρισμός.

Θεώρημα 1.8.6 (Wiles)**.** *Για κάθε $n > 2$, η εξίσωση $x^n + y^n = z^n$ δεν έχει λύση στους φυσικούς αριθμούς.*

Σκοπός μας εδώ είναι απλώς να δείξουμε την απόδειξη αυτού του ισχυρισμού στην περίπτωση $n = 4$.

Θεώρημα 1.8.7. *Η εξίσωση $x^4 + y^4 = z^4$ δεν έχει λύση στους φυσικούς αριθμούς.*

Παρατηρούμε πρώτα ότι το Θεώρημα 1.8.7 είναι άμεση συνέπεια του παρακάτω θεωρήματος.

Θεώρημα 1.8.8. *Η εξίσωση $x^4 + y^4 = z^2$ δεν έχει λύση στους φυσικούς αριθμούς.*

Πράγματι, αν οι φυσικοί x, y και z ικανοποιούν την $x^4 + y^4 = z^4$, τότε οι φυσικοί x, y και $w = z^2$ ικανοποιούν την $x^4 + y^4 = w^2$.

Για την απόδειξη του Θεωρήματος 1.8.8 θα χρησιμοποιήσουμε τη «μέθοδο της άπειρης καθόδου», η οποία περιγράφεται ως εξής: Αν θέλουμε να δείξουμε ότι δεν υπάρχει φυσικός n που να έχει κάποια ιδιότητα (P), αρκεί να αποδείξουμε την εξής συνεπαγωγή:

> Αν ο $n \in \mathbb{N}$ έχει την ιδιότητα (P), τότε υπάρχει φυσικός $m < n$ που έχει κι αυτός την ιδιότητα (P).

Τότε οδηγούμαστε σε άτοπο ως εξής. Θεωρούμε n_1 που έχει την ιδιότητα (P). Υπάρχει $n_2 < n_1$ που έχει την ιδιότητα (P), $n_3 < n_2$ που έχει την ιδιότητα (P) και ούτω καθεξής. Όμως έτσι φτιάχνουμε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών $n_1 > n_2 > \cdots > n_k > n_{k+1} > \cdots$, το οποίο είναι άτοπο.

Στην περίπτωσή μας η κατάλληλη ιδιότητα είναι η εξής: το τετράγωνο n^2 του φυσικού n γράφεται σαν άθροισμα δύο τετάρτων δυνάμεων φυσικών αριθμών. Θα υποθέσουμε ότι για κάποιον $z \in \mathbb{N}$ υπάρχουν $x, y \in \mathbb{N}$ τέτοιοι ώστε $x^4 + y^4 = z^2$ και θα βρούμε δύο άλλους φυσικούς X, Y τέτοιους ώστε $X^4 + Y^4 < x^4 + y^4 = z^2$ και $X^4 + Y^4 = w^2$ για κάποιον $w \in \mathbb{N}$. Τότε ο w έχει την ιδιότητα που περιγράψαμε και $w < z$. Σύμφωνα με τη μέθοδο της άπειρης καθόδου, καταλήγουμε σε άτοπο.

Απόδειξη. Έστω x, y, z φυσικοί αριθμοί που ικανοποιούν την $x^4 + y^4 = z^2$. Οι x^2, y^2 και z σχηματίζουν Πυθαγόρεια τριάδα και, διαιρώντας με το μέγιστο κοινό διαιρέτη τους, μπορούμε να υποθέσουμε ότι η τριάδα είναι πρωταρχική. Έπεται ότι οι x, y και z είναι ανά δύο σχετικά πρώτοι. Αλλάζοντας τη σειρά των x και y αν χρειαστεί,

μπορούμε να υποθέσουμε ότι ο x^2 (άρα και ο x) είναι άρτιος, ενώ ο y^2 (άρα και ο y) είναι περιττός. Από το Θεώρημα 1.8.3,

$$\begin{aligned} x^2 &= 2ms \\ y^2 &= m^2 - s^2 \\ z &= m^2 + s^2, \end{aligned}$$

όπου $m > s > 0$, $(m, s) = 1$ και οι m, s είναι ο ένας περιττός και ο άλλος άρτιος. Από τη δεύτερη ισότητα παίρνουμε

$$y^2 + s^2 = m^2, \tag{1.8.12}$$

και από την $(m, s) = 1$ έπεται ότι οι y, s, m σχηματίζουν πρωταρχική Πυθαγόρεια τριάδα. Ειδικότερα, συμπεραίνουμε ότι ο m είναι περιττός και ο s είναι άρτιος. Έπεται ότι

$$\begin{aligned} s &= 2ab \\ y &= a^2 - b^2 \\ m &= a^2 + b^2, \end{aligned}$$

όπου $a > b > 0$, $(a, b) = 1$ και οι a, b είναι ο ένας περιττός και ο άλλος άρτιος. Παρατηρούμε ότι

$$x^2 = 2ms = 4(ab)(a^2 + b^2) \Longrightarrow (x/2)^2 = (ab)(a^2 + b^2). \tag{1.8.13}$$

Δηλαδή το γινόμενο των ab και $a^2 + b^2$ είναι τέλειο τετράγωνο. Όμως από την $(a, b) = 1$ βλέπουμε εύκολα ότι $(ab, a^2 + b^2) = 1$. Από το Λήμμα 1.8.2 οι ab και $a^2 + b^2$ είναι τέλεια τετράγωνα. Πάλι από το Λήμμα 1.8.2, αφού $(a, b) = 1$ και ο ab είναι τέλειο τετράγωνο, καθένας από τους a και b είναι τέλειο τετράγωνο. Δηλαδή υπάρχουν X, Y και $w \in \mathbb{N}$ τέτοιοι ώστε

$$a = X^2,\ b = Y^2 \text{ και } a^2 + b^2 = w^2. \tag{1.8.14}$$

Από την (1.8.13)

$$w^2 = a^2 + b^2 = X^4 + Y^4, \tag{1.8.15}$$

δηλαδή το τετράγωνο του w γράφεται σαν άθροισμα δύο τετάρτων δυνάμεων φυσικών αριθμών, και

$$X^4 + Y^4 = a^2 + b^2 = m < m^2 + s^2 = z < z^2 = x^4 + y^4, \tag{1.8.16}$$

άρα $w < z$. Η μέθοδος της άπειρης καθόδου συμπληρώνει την απόδειξη. □

1.9 Ασκήσεις

1. (α) Δείξτε ότι

$$2 \cdot 6 \cdot 10 \cdot 14 \cdots (4n - 2) = \frac{(2n)!}{n!}$$

για κάθε $n \in \mathbb{N}$.

(β) Χρησιμοποιώντας το (α) δείξτε ότι $2^n(n!)^2 \leq (2n)!$ για κάθε $n \geq 1$.

2. Με τη μέθοδο της επαγωγής δείξτε ότι

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$$

για κάθε $n \geq 1$.

3. Αποδείξτε τις ιδιότητες (i) ως (viii) της Παραγράφου 1.2.

4. Δείξτε ότι για κάθε ακέραιο a ο $a^2 + a + 1$ διαιρεί τον $a^4 + a^2 + 1$.

5. Δείξτε ότι δεν υπάρχουν ακέραιοι m και n τέτοιοι ώστε $m^2 = n^2 + 2002$.

6. Δείξτε την εξής μορφή της ταυτότητας της διαίρεσης: αν $a, b \in \mathbb{Z}$ και $a \neq 0$, υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε $b = aq + r$ και $-|a|/2 < r \leq |a|/2$.

7. Χρησιμοποιώντας την ταυτότητα της διαίρεσης δείξτε ότι:

(α) Το τετράγωνο ενός ακεραίου είναι πάντα της μορφής $3k$ ή $3k + 1$.

(β) Το τετράγωνο ενός περιττού ακεραίου είναι πάντα της μορφής $8k + 1$.

(γ) Ο κύβος ενός ακεραίου είναι πάντα της μορφής $9k$, $9k + 1$ ή $9k + 8$.

(δ) Η τέταρτη δύναμη ενός ακεραίου είναι πάντα της μορφής $5k$ ή $5k + 1$.

8. Έστω $a, b, c \in \mathbb{N}$.

(α) Δείξτε ότι αν $3 \mid (a^2 + b^2)$ τότε $3 \mid ab$.

(β) Δείξτε ότι αν $9 \mid (a^3 + b^3 + c^3)$ τότε $3 \mid abc$.

9. Δείξτε ότι αν ένας ακέραιος είναι ταυτόχρονα τετράγωνο και κύβος (όπως για παράδειγμα ο $64 = 8^2 = 4^3$), τότε πρέπει να είναι της μορφής $7k$ ή $7k + 1$.

10. (α) Τι υπόλοιπα μπορούν να προκύψουν όταν η δέκατη δύναμη ενός ακεραίου διαιρεθεί με το 5;

(β) Τι υπόλοιπα μπορούν να προκύψουν όταν η δέκατη δύναμη ενός ακεραίου διαιρεθεί με το 25;

11. Υπάρχει θετικός ακέραιος n τέτοιος ώστε ο 2005 να διαιρεί τον $n^2 + n + 1$;

12. Δείξτε ότι κάθε θετικός ακέραιος ο οποίος στο δεκαδικό σύστημα αποτελείται από 3^n όμοια ψηφία διαιρείται με το 3^n (π.χ. ο 777 διαιρείται με το 3, ο 222222222 διαιρείται με το 9 κλπ). *Υπόδειξη*: επαγωγή στο n.

13. Ο ορισμός του μέγιστου κοινού διαιρέτη γενικεύεται ως εξής: αν $k \geq 2$ και $a_1, \ldots, a_k \in \mathbb{Z}$ και τουλάχιστον ένας από τους $a_1, \ldots, a_k$ δεν είναι μηδέν, ορίζουμε $(a_1, \ldots, a_k)$ εκείνον τον θετικό ακέραιο d που ικανοποιεί τα εξής:

(i) $d \mid a_j$ για κάθε $j = 1, \ldots, k$.

(ii) Αν $s \in \mathbb{Z}$ και $s \mid a_j$ για κάθε j, τότε $s \leq d$.

(α) Δείξτε ότι $(a_1, \ldots, a_k) = (|a_1|, \ldots, |a_k|)$ και ότι υπάρχουν ακέραιοι $x_1, \ldots, x_k$ τέτοιοι ώστε $(a_1, \ldots, a_k) = a_1x_1 + \cdots + a_kx_k$.

(β) Δείξτε ότι $((a_1, \ldots, a_{k-1}), a_k) = (a_1, \ldots, a_k)$.

14. Έστω $a, b \in \mathbb{N}$. Αν $(a, b) = ax + by$ για κάποιους $x, y \in \mathbb{Z}$, δείξτε ότι $(x, y) = 1$.

15. Για κάθε $a \in \mathbb{Z}$ δείξτε ότι

$$(2a+1, 9a+4) = 1 \text{ και } (5a+2, 7a+3) = 1.$$

16. Έστω $a, b \in \mathbb{N}$ με $(a, b) = 1$.

(α) Ποιες είναι οι δυνατές τιμές του $(a+b, ab)$;

(β) Ποιες είναι οι δυνατές τιμές του $(a+b, a^2+ab+b^2)$;

(γ) Ποιες είναι οι δυνατές τιμές του $(a+b, a^2+b^2)$;

17. Αποδείξτε τις παρακάτω ιδιότητες του μέγιστου κοινού διαιρέτη.

(α) $(a, bc) = 1$ αν και μόνο αν $(a, b) = (a, c) = 1$.

(β) Αν $(a, b) = 1$ και $c \mid b$ τότε $(a, c) = 1$.

(γ) Αν $(a, b) = 1$ τότε $(a, bc) = (a, c)$.

(δ) $(a, b) = 1$ αν και μόνο αν $(a^2, b^2) = 1$.

Σε όλα τα ερωτήματα υποθέτουμε ότι $a, b, c \in \mathbb{N}$.

18. Έστω $d, n \in \mathbb{N}$. Αν $d \mid n$, τότε $(2^d - 1) \mid (2^n - 1)$. *Υπόδειξη:* Χρησιμοποιήστε την ταυτότητα $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$.

19. Βρείτε τρία δεκαδικά ψηφία x, y, z τέτοια ώστε ο εξαψήφιος δεκαδικός αριθμός $271xyz$ να διαιρείται με το 7, με το 8 και με το 9.

20. Για κάθε $n \in \mathbb{N}$ και $0 \le k \le n$, ορίζουμε τον διωνυμικό συντελεστή

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

(α) Συμφωνούμε ότι $0! = 1$ και $\binom{0}{0} = 1$. Δείξτε ότι, για κάθε $n \in \mathbb{N}$,

$$\binom{n}{0} = \binom{n}{n} = 1$$

και

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

για κάθε $1 \le k \le n-1$.

(β) Δείξτε ότι το γινόμενο k διαδοχικών φυσικών διαιρείται με $k!$. *Υπόδειξη:* Δείξτε με επαγωγή ότι ο $\binom{n}{k}$ είναι ακέραιος.

21. (α) Αν ο n είναι πρώτος και ο k είναι ακέραιος με $1 \le k \le n-1$ δείξτε ότι ο n διαιρεί το $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

(β) Ισχύει το (α) χωρίς να υποθέσουμε ότι ο n είναι πρώτος;

22. Δείξτε ότι ο $n^4 + 4$ είναι σύνθετος για κάθε $n \ge 2$.

23. Δείξτε ότι οι τρεις φυσικοί αριθμοί $n, n+2, n+4$ δεν μπορούν να είναι ταυτόχρονα πρώτοι εκτός αν $n = 3$.

24. Βρείτε όλους τους πρώτους αριθμούς p για τους οποίους ο $8p^2 + 1$ είναι επίσης πρώτος αριθμός.

25. Έστω $p > 3$ ένας πρώτος αριθμός.

(α) Εξηγήστε γιατί $p = 6k + 1$ ή $p = 6k - 1$ για κάποιον $k \in \mathbb{N}$.

(β) Δείξτε ότι $24 \mid (p^2 - 1)$.

(γ) Δείξτε ότι $24 \mid n(n^2 - 1)$ για κάθε περιττό $n \in \mathbb{N}$.

26. Δείξτε ότι για κάθε φυσικό αριθμό $n > 2$ τουλάχιστον ένας από τους $2^n - 1$ και $2^n + 1$ είναι σύνθετος.

27. Αν p, q είναι διαδοχικοί πρώτοι μεγαλύτεροι του 2 δείξτε ότι ο $p + q$ μπορεί να γραφεί σαν γινόμενο τουλάχιστον τριών (όχι αναγκαστικά διαφορετικών) πρώτων αριθμών (π.χ. $13 + 17 = 2 \cdot 3 \cdot 5$, $17 + 19 = 2 \cdot 2 \cdot 3 \cdot 3$ και $19 + 23 = 2 \cdot 3 \cdot 7$).

28. Βρείτε όλους τους πρώτους αριθμούς μεταξύ των όρων της άπειρης ακολουθίας

$$101, 10101, 1010101, 101010101, \ldots$$

όπου $101 = 10^2 + 1, 10101 = 10^4 + 10^2 + 1$ κλπ.

29. (α) Έστω $a, b \in \mathbb{N}$ και έστω $a = \prod_{p \in P} p^{r_p}$, $b = \prod_{p \in P} p^{s_p}$ οι κανονικές αναπαραστάσεις των a, b. Δείξτε ότι $(a, b) = \prod_{p \in P} p^{k_p}$, όπου $k_p = \min\{r_p, s_p\}$ για κάθε $p \in P$.

(β) Έστω $a, b, c \in \mathbb{N}$. Αποδείξτε τα παρακάτω χωρίς να χρησιμοποιήσετε τις κανονικές αναπαραστάσεις των a, b, c.

(i) $(ab, ac) = a(b, c)$.

(ii) $(a, bc) = (a, (a, b)c)$.

(iii) $(a^2, b^2) = (a, b)^2$.

(γ) Τώρα, αποδείξτε τα ίδια πράγματα χρησιμοποιώντας τις κανονικές αναπαραστάσεις των a, b, c.

30. (α) Έστω $a, b \in \mathbb{N}$. Δείξτε ότι υπάρχει μοναδικός $m \in \mathbb{N}$ ο οποίος ικανοποιεί τα εξής:

(i) $a \mid m$ και $b \mid m$.

(ii) Αν $x \in \mathbb{N}$ και $a \mid x$, $b \mid x$, τότε $m \mid x$.

Υπόδειξη: Θεωρήστε το $S = \{x \in \mathbb{N} : a \mid x \text{ και } b \mid x\}$. Δείξτε ότι είναι μη κενό και πάρτε σαν m το ελάχιστο στοιχείο του.

(β) Ο m λέγεται *ελάχιστο κοινό πολλαπλάσιο* των a και b, και συμβολίζεται με $[a, b]$. Περιγράψτε τον $[a, b]$ με τη βοήθεια των κανονικών αναπαραστάσεων των a και b.

31. Έστω $a, b, c \in \mathbb{N}$. Ορίστε το ελάχιστο κοινό πολλαπλάσιο $[a, b, c]$ των a, b, c και δείξτε ότι:

(α) $(a, b) \cdot [a, b] = ab$. (β) $\frac{[a,b,c]^2}{[a,b][a,c][b,c]} = \frac{(a,b,c)^2}{(a,b)(a,c)(b,c)}$.

32. Δείξτε ότι $(a, b) = (a + b, [a, b])$ για κάθε $a, b \in \mathbb{N}$. Συμπεράνετε ότι αν $p \mid [a, b]$ και $p \mid a + b$, τότε $p \mid (a, b)$.

33. Έστω $a, m, n \in \mathbb{N}$ με $a > 1$. Δείξτε ότι $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

34. Δείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $4n - 1$. *Υπόδειξη:* Μιμηθείτε το επιχείρημα του Ευκλείδη.

35. Υποθέτουμε ότι ο $2^n + 1$ είναι πρώτος για κάποιον $n \geq 2$ (οι πρώτοι αυτής της μορφής λέγονται **πρώτοι του Fermat**). Δείξτε ότι ο n είναι δύναμη του 2.

36. Υποθέτουμε ότι ο $2^n - 1$ είναι πρώτος για κάποιον $n \in \mathbb{N}$ (οι πρώτοι αυτής της μορφής λέγονται **πρώτοι του Mersenne**). Δείξτε ότι ο n είναι πρώτος.

37. Έστω $n \in \mathbb{N}$, $n \geq 2$.

(α) Υποθέτουμε ότι για κάθε πρώτο $p \leq \sqrt{n}$ ο n δεν είναι πολλαπλάσιο του p. Δείξτε ότι ο n είναι πρώτος.

(β) Εξετάστε αν οι φυσικοί 509, 2093 είναι πρώτοι. Βρείτε την κανονική τους αναπαράσταση.

38. Έστω p ένας πρώτος αριθμός. Δείξτε ότι ο $\sqrt{p}$ είναι άρρητος.

39. Δείξτε ότι ο $f(n) = n^2 + n + 41$ είναι πρώτος για $n = 0, 1, \ldots, 39$. Τι συμβαίνει όταν $n = 40$;

40. Δείξτε ότι δεν υπάρχει πολυώνυμο $f(x) = a_0 + a_2 x + \cdots + a_k x^k$, $k \geq 1$, $a_k \neq 0$, με συντελεστές ακεραίους, για το οποίο όλοι οι αριθμοί $|f(n)|$, $n \geq 0$ να είναι πρώτοι.

41. Έστω $n \geq 2$. Δείξτε ότι ο $(n+1)! + k$ είναι σύνθετος για κάθε $k = 2, \ldots, n+1$. Αυτό αποδεικνύει ότι υπάρχουν οσοδήποτε μακριά διαστήματα διαδοχικών σύνθετων αριθμών.

42. Δείξτε ότι $2^n \mid (n+1)(n+2)\cdots(2n)$ για κάθε $n \in \mathbb{N}$.

43. Δείξτε ότι κάθε φυσικός αριθμός $n \geq 12$ είναι άθροισμα δύο σύνθετων αριθμών.

44. Βρείτε όλους τους πρώτους p για τους οποίους ο $29p+1$ είναι τέλειο τετράγωνο.

45. Οι πρώτοι αριθμοί p και q λέγονται δίδυμοι πρώτοι αν $|p - q| = 2$. Δείξτε ότι αν οι p, q είναι πρώτοι, τότε ο $pq + 1$ είναι τέλειο τετράγωνο αν και μόνο αν οι p και q είναι δίδυμοι πρώτοι.

46. Το «αίτημα του Bertrand», το οποίο αποδείχθηκε αληθές από τον Chebyshev το 1850, ισχυρίζεται ότι: για κάθε φυσικό $n \geq 2$ υπάρχει τουλάχιστον ένας πρώτος p τέτοιος ώστε $n < p < 2n$.

(α) Χρησιμοποιώντας το αίτημα του Bertrand δείξτε ότι για κάθε φυσικό $n \geq 3$ υπάρχει πρώτος p τέτοιος ώστε $p < n < 2p$.

(β) Χρησιμοποιώντας το αίτημα του Bertrand δείξτε ότι $p_n < 2^n$ για κάθε $n \geq 2$, όπου p_n είναι ο n-οστός πρώτος, και δώστε κάτω φράγμα για τη συνάρτηση $\pi(x)$.

47. Έστω p_n ο n-οστός πρώτος. Χρησιμοποιώντας το αίτημα του Bertrand δείξτε ότι

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

για κάθε $n \geq 3$.

48. Έστω $n \geq 2$. Δείξτε ότι ο $n!$ δεν είναι τέλειο τετράγωνο: δεν υπάρχει $m \in \mathbb{N}$ τέτοιος ώστε $n! = m^2$.

49. Αν $n \geq 2$ δείξτε ότι το άθροισμα

$$\sum_{k=1}^{n} \frac{1}{k}$$

δεν είναι ακέραιος.

50. Ποιές από τις παρακάτω διοφαντικές εξισώσεις δεν έχουν ακέραιες λύσεις; Εξηγήστε.
(α) $6x + 51y = 22$ (β) $33x + 14y = 115$ (γ) $14x + 35y = 93$.

51. Βρείτε όλες τις ακέραιες λύσεις της διοφαντικής εξίσωσης $24x + 138y = 18$.

52. Βρείτε όλες τις θετικές ακέραιες λύσεις της διοφαντικής εξίσωσης $123x + 360y = 99$.

53. Βρείτε όλες τις μη αρνητικές ακέραιες λύσεις της διοφαντικής εξίσωσης

$$2x + 7y = 53.$$

54. Βρείτε όλες τις μη αρνητικές ακέραιες λύσεις της διοφαντικής εξίσωσης

$$28x + 35y = 136.$$

55. Αν $a, b \in \mathbb{N}$ και $(a, b) = 1$, δείξτε ότι η γραμμική διοφαντική εξίσωση $ax - by = c$ έχει άπειρες το πλήθος θετικές ακέραιες λύσεις.

56. Έστω $n \geq 2$. Δείξτε ότι η εξίσωση $y^n = 2x^n$ δεν έχει λύση στους φυσικούς αριθμούς.

57. (α) Δείξτε ότι για κάθε περιττό ακέραιο $y \geq 3$ υπάρχει πρωταρχική πυθαγόρεια τριάδα (x, y, z), δηλαδή υπάρχουν σχετικώς πρώτοι θετικοί ακέραιοι x και z με $x^2 + y^2 = z^2$.
(β) Συμπεράνετε ότι υπάρχουν άπειρες πρωταρχικές Πυθαγόρειες τριάδες.

58. Βρείτε όλα τα Πυθαγόρεια τρίγωνα που το εμβαδόν τους ισούται με την περίμετρό τους.

59. Δείξτε ότι για κάθε φυσικό αριθμό n υπάρχει Πυθαγόρειο τρίγωνο που έχει την ακτίνα του εγγεγραμμένου κύκλου του ίση με n.

60. Δείξτε ότι από 52 τυχαίους ακέραιους αριθμούς μπορούν πάντοτε να επιλεγούν δύο αριθμοί το άθροισμα ή η διαφορά των οποίων διαιρείται με το 100.

61. (α) Δείξτε ότι αν επιλέξουμε τυχαία 101 αριθμούς από τους $1, 2, 3, \ldots, 200$ τότε υπάρχουν δύο μεταξύ των αριθμών που επιλέξαμε ο ένας από τους οποίους διαιρεί τον άλλο.
(β) Επιλέξτε 100 αριθμούς από τους $1, 2, 3, \ldots, 200$ έτσι ώστε να μην υπάρχουν δύο μεταξύ των αριθμών που επιλέξατε ο ένας από τους οποίους να διαιρεί τον άλλο.

62. Έστω ακέραιος $n \geq 2$. Δείξτε ότι το άθροισμα των κλασμάτων της μορφής $1/pq$, όπου p, q είναι σχετικώς πρώτοι ακέραιοι με $1 \leq p, q \leq n$ και $p + q > n$, είναι ίσο με $1/2$ (π.χ. για $n = 5$ έχουμε $1/1 \cdot 5 + 1/2 \cdot 5 + 1/3 \cdot 5 + 1/4 \cdot 5 + 1/3 \cdot 4 = 1/2$).

Υποδείξεις - απαντήσεις

1. (α) Με επαγωγή: όταν $n = 1$ η ισότητα γίνεται

$$4 \cdot 1 - 2 = 2 = \frac{2!}{1!}.$$

Υποθέτουμε ότι $2 \cdot 6 \cdot 10 \cdots (4k-2) = (2k)!/k!$. Τότε

$$\begin{aligned} 2 \cdot 6 \cdot 10 \cdots (4k-2) \cdot (4(k+1)-2) &= \frac{(2k)!}{k!} \cdot (4k+2) = \frac{(2k)!}{k!} \cdot 2(2k+1) \\ &= \frac{(2k)!}{k!} \cdot \frac{2(k+1)(2k+1)}{k+1} \\ &= \frac{(2k)!(2k+1)(2k+2)}{k!(k+1)} \\ &= \frac{(2(k+1))!}{(k+1)!}. \end{aligned}$$

(β) Από το (α), για κάθε $n \in \mathbb{N}$ έχουμε

$$\begin{aligned} \frac{(2n)!}{2^n (n!)^2} &= \frac{2 \cdot 6 \cdot 10 \cdots (4n-2)}{2^n n!} = \frac{2^n \cdot 1 \cdot 3 \cdot 5 \cdots (2n-1)}{2^n n!} \\ &= \frac{1}{1} \cdot \frac{3}{2} \cdot \frac{5}{3} \cdots \frac{2n-1}{n} \geq 1. \end{aligned}$$

Για μια διαφορετική απόδειξη ερμηνεύστε την ποσότητα $\frac{(2n)!}{(n!)^2}$ ως το πλήθος των υποσυνόλων του συνόλου $\{1, 2, \ldots, 2n\}$ με n στοιχεία.

2. Όταν $n = 1$ έχουμε $1 = 2 - 1$. Υποθέτουμε ότι

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}.$$

Τότε

$$\begin{aligned} \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} &\leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2} \\ &= 2 - \frac{k^2+k+1}{(k^2+k)(k+1)} \leq 2 - \frac{1}{k+1}. \end{aligned}$$

3. (i) Για κάθε $a \in \mathbb{Z}$ έχουμε $a = a \cdot 1$, άρα $a \mid a$.

(ii) Για κάθε $a \in \mathbb{Z}$ έχουμε $0 = a \cdot 0$, άρα $a \mid 0$.

(iii) Για κάθε $a \in \mathbb{Z}$ έχουμε $a = 1 \cdot a$ και $a = (-1) \cdot (-a)$, άρα $\pm 1 \mid a$.

(iv) Από το (ii) έχουμε $0 \mid 0$. Αντίστροφα, αν $0 \mid a$ για κάποιον $a \in \mathbb{Z}$, τότε υπάρχει $x \in \mathbb{Z}$ τέτοιος ώστε $a = 0 \cdot x$, οπότε $a = 0$.

(v) Υποθέτουμε ότι $a \mid b$ και $b \mid c$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $b = a \cdot x$ και $c = b \cdot y$. Άρα, $c = a \cdot (xy)$ και αφού $xy \in \mathbb{Z}$ συμπεραίνουμε ότι $a \mid c$.

(vi) Υποθέτουμε ότι $a \mid b$ και $a \mid c$. Τότε υπάρχουν $u, v \in \mathbb{Z}$ τέτοιοι ώστε $b = a \cdot u$ και $c = a \cdot v$. Αν $x, y \in \mathbb{Z}$, τότε $bx + cy = a \cdot (ux + vy)$ δηλαδή $a \mid bx + cy$.

(vii) Αφού $a \mid b$ και $a, b \neq 0$, υπάρχει $x \in \mathbb{Z}$ με $x \neq 0$ και $b = a \cdot x$. Τότε $|b| = |a| \cdot |x| \geq |a|$ αφού $|x| \geq 1$.

(viii) Από το (iii) έχουμε $\pm 1 \mid \pm 1$. Αντίστροφα, αν $a \mid \pm 1$ τότε $a \neq 0$ και $|a| \leq 1$ από το (η), δηλαδή $a = \pm 1$.

4. Παρατηρούμε ότι $a^4+a^2+1=(a^2+a+1)(a^2-a+1)$ και ότι $a^2-a+1\in\mathbb{Z}$ για $a\in\mathbb{Z}$.

5. Αν υπήρχαν τέτοιοι m και n τότε θα ήταν και οι δύο άρτιοι ή και οι δύο περιττοί και ο $2002=m^2-n^2=(m-n)(m+n)$ θα ήταν πολλαπλάσιο του 4, άτοπο.

6. Έστω $a,b\in\mathbb{Z}$ με $a\neq 0$. Από την ταυτότητα της διαίρεσης, υπάρχουν μοναδικοί ακέραιοι q_1 και r_1 τέτοιοι ώστε $b=|a|q_1+r_1$ και $0\leq r_1<|a|$. Αν $r_1\leq |a|/2$, παίρνουμε $q=\varepsilon q_1$ και $r=r_1$ όπου ε το πρόσημο του a. Τότε $b=aq+r$ και $-|a|/2<0\leq r\leq |a|/2$.

Έστω ότι $|a|/2<r_1<|a|$. Τότε $-|a|/2=|a|/2-|a|<r_1-|a|<0$ και $b=|a|(q_1+1)+(r_1-|a|)$, οπότε αν πάρουμε $q=\varepsilon(q_1+1)$ και $r=r_1-|a|$ έχουμε $b=aq+r$ και $-|a|/2<r<0\leq |a|/2$.

Σε κάθε περίπτωση, υπάρχουν $q,r\in\mathbb{Z}$ με $-|a|/2<r\leq |a|/2$ και $b=aq+r$. Για τη μοναδικότητα εργαζόμαστε όπως στην απόδειξη της ταυτότητας της διαίρεσης.

7. (α) Έστω $a\in\mathbb{Z}$. Ο a γράφεται στη μορφή $a=3q+r$, όπου $r\in\{0,1,2\}$. Άρα $a^2=(3q+r)^2=9q^2+6qr+r^2=3x+r^2$ για κάποιον $x\in\mathbb{Z}$. Παρατηρούμε ότι: αν $r=0$ τότε $a^2=3x$, αν $r=1$ τότε $a^2=3x+1$, ενώ αν $r=2$ τότε $a^2=3x+4=3(x+1)+1$. Σε κάθε περίπτωση, ο a^2 είναι της μορφής $3k$ ή $3k+1$.

(β) Έστω $a\in\mathbb{Z}$ περιττός. Ο a γράφεται στη μορφή $a=2q+1$ όπου $q\in\mathbb{Z}$, άρα $a^2=(2q+1)^2=4q^2+4q+1=4q(q+1)+1$. Ένας από τους q και $q+1$ είναι άρτιος και συνεπώς ο $q(q+1)=2k$ είναι άρτιος, οπότε $a^2=8k+1$ με $k\in\mathbb{Z}$.

(γ) Έστω $a\in\mathbb{Z}$. Ο a γράφεται στη μορφή $a=3q+r$, όπου $r\in\{0,1,2\}$. Άρα, $a^3=(3q+r)^3=27q^3+27q^2r+9qr^2+r^3=9x+r^3$ για κάποιον $x\in\mathbb{Z}$. Αφού $r^3=0,1$ ή 8 αν $r=0,1$ ή 2 αντίστοιχα, έχουμε το ζητούμενο.

(δ) Έστω $a\in\mathbb{Z}$. Ο a γράφεται στη μορφή $a=5q+r$, όπου $r\in\{0,1,2,3,4\}$. Άρα, $a^5=(5q+r)^4=5x+r^4$ για κάποιον $x\in\mathbb{Z}$. Παρατηρούμε ότι $0^4=0$, $1^4=1$, $2^4=16=5\cdot 3+1$, $3^4=81=5\cdot 16+1$, $4^4=256=5\cdot 51+1$. Σε κάθε περίπτωση, $r^4=0$ ή $r^4=5y+1$ για κάποιον $y\in\mathbb{Z}$. Άρα $a^4=5x$ ή $a^4=5(x+y)+1$.

8. (α) Αν κανένας από τους a και b δεν είναι πολλαπλάσιο του 3 τότε οι a^2 και b^2 είναι της μορφής $3k+1$, οπότε ο a^2+b^2 είναι της μορφής $3k+2$, δηλαδή δεν διαιρείται με 3. Αν λοιπόν $3\mid(a^2+b^2)$ τότε κάποιος από τους a και b διαιρείται με 3, οπότε $3\mid ab$.

(β) Αν κανένας από τους a,b και c δεν διαιρείται με 3 τότε οι a^3, b^3 και c^3 είναι της μορφής $9k+1$ ή $9k+8$ (Άσκηση 7). Αν όλοι είναι της μορφής $9k+1$ τότε ο $a^3+b^3+c^3$ είναι της μορφής $9k+3$, άτοπο. Αν όλοι είναι της μορφής $9k+8$ τότε ο $a^3+b^3+c^3$ είναι της μορφής $9k+24=9(k+2)+6$, άτοπο. Αν δύο είναι της μορφής $9k+1$ και ένας της μορφής $9k+8$, τότε ο $a^3+b^3+c^3$ είναι της μορφής $9k+10=9(k+1)+1$, άτοπο. Αν δύο είναι της μορφής $9k+8$ και ένας της μορφής $9k+1$, τότε ο $a^3+b^3+c^3$ είναι της μορφής $9k+17=9(k+1)+8$, άτοπο. Αν λοιπόν $9\mid(a^3+b^3+c^3)$, τότε κάποιος από τους a, b και c διαιρείται με 3, οπότε $3\mid abc$.

9. Έστω $m=a^2=b^3$ για κάποιους $a,b\in\mathbb{Z}$. Δείξτε ότι ο a^2 είναι της μορφής $7k$ ή $7k+1$ ή $7k+2$ ή $7k+4$, ενώ ο b^3 είναι της μορφής $7k$ ή $7k+1$ ή $7k+6$. Άρα το υπόλοιπο της διαίρεσης του m με 7 μπορεί να πάρει μόνο τις τιμές 0 και 1 (παραδείγματα: ο $m_1=7^6$ και ο $m_2=64$).

10. (α) Τα δυνατά υπόλοιπα είναι $0,1$ και 4. Πράγματι, αν $5\mid a$ τότε $5\mid a^{10}$. Αλλιώς (Άσκηση 6) $a=5q\pm 1$ ή $a=5q\pm 2$ με $q\in\mathbb{Z}$, οπότε $a^2=5(5q^2\pm 2q)+1=5k+1$ ή $a^2=5(5q^2\pm 4q+1)-1=5k-1$ με $k\in\mathbb{Z}$. Υψώνοντας στην πέμπτη δύναμη με το διωνυμικό τύπο προκύπτει ότι $a^{10}=(5k\pm 1)^5=5t\pm 1$ με $t\in\mathbb{Z}$.
(β) Τα δυνατά υπόλοιπα είναι $0,1$ και 24. Πράγματι, αν $5\mid a$ τότε $25\mid a^{10}$. Αλλιώς $a^2=5k\pm 1$ με $k\in\mathbb{Z}$ από το (α) και συνεπώς

$$a^{10}=(5k\pm 1)^5=(5k)^5\pm 5(5k)^4+10(5k)^3\pm 10(5k)^2+5(5k)\pm 1=25t\pm 1$$

με $t \in \mathbb{Z}$.

11. Όχι. Αν υπήρχε τέτοιος ακέραιος n τότε ο 5 θα διαιρούσε το n^2+n+1. Όμως αν $n = 5q+r$ με $q \in \mathbb{Z}$ και $r = 0, 1, 2, 3$ ή 4 τότε εύκολα βρίσκουμε ότι $n^2+n+1 = 5t+s$ με $t \in \mathbb{Z}$ και $s = 1, 3, 2, 3$ ή 1, αντίστοιχα, οπότε ο 5 δεν διαιρεί το n^2+n+1 για $n \in \mathbb{Z}$.

12. Εφαρμόζουμε επαγωγή στο n. Για $n = 1$ ισχύει διότι ο αριθμός $a+a\cdot 10+a\cdot 10^2 = 111a$ διαιρείται με το 3. Έστω ότι ο $x_{n-1} = a + a\cdot 10 + \cdots + a\cdot 10^{3^{n-1}-1}$ διαιρείται με το 3^{n-1}. Θα δείξουμε ότι ο $x_n = a + a\cdot 10 + \cdots + a\cdot 10^{3^n-1}$ διαιρείται με το 3^n. Πράγματι, αρκεί να παρατηρήσουμε ότι $x_n = (1 + 10^{3^{n-1}} + 10^{2\cdot 3^{n-1}})\, x_{n-1}$ και ότι $3 \mid 1 + 10^{3^{n-1}} + 10^{2\cdot 3^{n-1}}$, διότι κάθε δύναμη του 10 είναι της μορφής $3k+1$ με $k \in \mathbb{Z}$.

13. (α) Δείχνουμε πρώτα την ύπαρξη του $(|a_1|, \ldots, |a_k|)$. Θεωρούμε το σύνολο

$$I = \{|a_1|u_1 + \cdots + |a_k|u_k : u_i \in \mathbb{Z}\} \cap \mathbb{N}.$$

Αφού οι a_i δεν είναι όλοι μηδέν, κάποιος $|a_{i_0}| \in \mathbb{N}$. Όμως $|a_{i_0}| \in I$ (γιατί;) άρα το I είναι μη κενό. Από την αρχή του ελαχίστου, το I έχει ελάχιστο στοιχείο d το οποίο γράφεται στη μορφή $d = |a_1|x_1 + \cdots + |a_k|x_k$ για κάποιους $x_i \in \mathbb{Z}$.

Θα δείξουμε ότι ο d διαιρεί κάθε στοιχείο του I. Ας υποθέσουμε ότι $z = |a_1|u_1 + \cdots + |a_k|u_k \in I$. Υπάρχουν $q, r \in \mathbb{Z}$ με $0 \le r < d$ και $z = dq + r$. Παρατηρούμε ότι

$$r = z - dq = |a_1|(u_1 - qx_1) + \cdots + |a_k|(u_k - qx_k) \in I.$$

Αν ήταν $0 < r < d$ τότε ο r θα ήταν στοιχείο του I μικρότερο από τον d, άτοπο από τον τρόπο ορισμού του d. Άρα $r = 0$, το οποίο αποδεικνύει ότι ο d διαιρεί τον z.

Αν $a_i \neq 0$ τότε $|a_i| \in I$, επομένως $d \mid |a_i|$ για κάθε $i = 1, \ldots, k$. Αν $s \in \mathbb{N}$ και $s \mid |a_i|$ για κάθε i, τότε

$$s \mid |a_1|x_1 + \cdots + |a_k|x_k = d.$$

Ειδικότερα, $s \le d$. Η μοναδικότητα του d αποδεικνύεται εύκολα.

Για να δείξουμε ότι $(a_1, \ldots, a_k) = (|a_1|, \ldots, |a_k|)$ αρκεί να παρατηρήσουμε ότι γενικά $a \mid b$ αν και μόνο αν $a \mid |b|$, οπότε το σύνολο των κοινών θετικών διαιρετών των $a_1, \ldots, a_k$ συμπίπτει με το σύνολο των κοινών θετικών διαιρετών των $|a_1|, \ldots, |a_k|$.

(β) Θέτουμε $d_1 = ((a_1, \ldots, a_{k-1}), a_k)$ και $d = (a_1, \ldots, a_k)$. Τότε $d_1 \mid (a_1, \ldots, a_{k-1})$ και $d_1 \mid a_k$, άρα $d \mid |a_i|$ για κάθε $i \le k$. Από το (α),

$$d_1 \mid (|a_1|, \ldots, |a_k|) = (a_1, \ldots, a_k) = d.$$

Αντίστροφα, $d \mid |a_i|$ για κάθε $i \le k-1$, άρα $d \mid (|a_1|, \ldots, |a_{k-1}|) = (a_1, \ldots, a_{k-1})$. Επίσης, $d \mid |a_k|$, άρα

$$d \mid (|(a_1, \ldots, a_{k-1})|, |a_k|) = ((a_1, \ldots, a_{k-1}), a_k) = d_1.$$

Αφού $d, d_1 \in \mathbb{N}$ και $d_1 \mid d$, $d \mid d_1$, παίρνουμε $d_1 = d$.

14. Έστω $d = (a, b)$. Έχουμε $a = du$ και $b = dv$ με $u, v \in \mathbb{N}$. Η δοσμένη σχέση $d = ax + by$ γράφεται $1 = ux + vy$, από όπου προκύπτει ότι $(x, y) = 1$.

15. (α) Έστω $d = (2a+1, 9a+4)$. Τότε $d \mid 2a+1 \Rightarrow d \mid 9(2a+1) = 18a+9$ και $d \mid 9a+4 \Rightarrow d \mid 2(9a+4) = 18a+8$. Άρα $d \mid 1 = (18a+9) - (18a+8)$ και συνεπώς $d = 1$.

(β) Έστω $d = (5a+2, 7a+3)$. Τότε $d \mid 5a+2 \Rightarrow d \mid 7(5a+2) = 35a+14$ και $d \mid 7a+3 \Rightarrow d \mid 5(7a+3) = 35a+15$. Άρα $d \mid 1 = (35a+15) - (35a+14)$ και συνεπώς $d = 1$.

16. (α) Έχουμε $(a+b, ab) = 1$. Πράγματι, αν όχι τότε υπάρχει πρώτος p με $p \mid (a+b, ab)$. Τότε $p \mid a+b$ και $p \mid ab$, οπότε $p \mid a$ ή $p \mid b$. Αν $p \mid a$ τότε $p \mid (a+b) - a = b$. Ομοίως, αν $p \mid b$ τότε $p \mid a$. Συνάγουμε ότι $p \mid a$ και $p \mid b$, άρα $p \mid (a, b) = 1$, αντίφαση.

(β) Έχουμε επίσης $(a+b, a^2+ab+b^2) = 1$. Πράγματι, αν όχι τότε υπάρχει πρώτος p με $p \mid (a+b, a^2+ab+b^2)$. Τότε $p \mid a+b$ και $p \mid a^2+ab+b^2$, οπότε $p \mid a^2+ab+b^2-a(a+b) = b^2$ και συνεπώς $p \mid b$. Ομοίως $p \mid a$, άρα $p \mid (a,b) = 1$, αντίφαση.

(γ) Οι δυνατές τιμές είναι οι 1 και 2 (και λαμβάνονται π.χ. αν $a = 2$, $b = 1$ και $a = b = 1$, αντίστοιχα). Έστω $d = (a+b, a^2+b^2)$. Παρατηρούμε ότι $(a+b, a) = (b, a) = 1$ και, εφόσον $d \mid a+b$, έχουμε $(d, a) = 1$ (δες Άσκηση 17 β). Ομοίως $(d, b) = 1$ και συνεπώς $(d, ab) = 1$. Από τις $d \mid a+b$ και $d \mid a^2+b^2$ προκύπτει ότι $d \mid (a+b)^2 - (a^2+b^2) = 2ab$ και, εφόσον $(d, ab) = 1$, ότι $d \mid 2$ (Λήμμα 1.4.2), δηλαδή ότι $d = 1$ ή $d = 2$.

17. (α) Αν $(a, b) = 1$ και $(a, c) = 1$ τότε υπάρχουν $x, y, u, v \in \mathbb{Z}$ τέτοιοι ώστε $ax + by = 1$ και $au + cv = 1$. Πολλαπλασιάζοντας κατά μέλη παίρνουμε

$$a(axu + cvx + byu) + bc(yv) = 1.$$

Άρα $(a, bc) \mid 1$ απ' όπου έπεται ότι $(a, bc) = 1$. Το αντίστροφο είναι ισοδύναμο με το (β).

(β) Αν $d = (a, c)$ τότε $d \mid a$ και $d \mid c \mid b$ οπότε $d \mid (a, b) = 1$. Άρα $d = 1$.

(γ) Θέτουμε $d_1 = (a, bc)$ και $d_2 = (a, c)$. Έχουμε $d_1 \mid a$ και $(a, b) = 1$, άρα $(d_1, b) = 1$ από το (β). Από τις $d_1 \mid bc$ και $(d_1, b) = 1$ προκύπτει ότι $d_1 \mid c$ (Λήμμα 1.4.2), οπότε $d_1 \mid (a, c) = d_2$ και συνεπώς $d_1 \leq d_2$.

Αντίστροφα, $d_2 \mid a$ και $d_2 \mid c \mid bc$, άρα $d_2 \mid (a, bc) = d_1$, οπότε $d_2 \leq d_1$.

Από τις $d_1 \leq d_2$ και $d_2 \leq d_1$ συμπεραίνουμε ότι $d_1 = d_2$.

(δ) Υποθέτουμε ότι $(a^2, b^2) = d > 1$. Τότε ο d έχει έναν πρώτο διαιρέτη p. Για τον p έχουμε $p \mid d \mid a^2 \Longrightarrow p \mid a$ και $p \mid d \mid b^2 \Longrightarrow p \mid b$. Άρα $p \mid (a, b) = 1$ το οποίο είναι άτοπο. Επομένως $(a^2, b^2) = 1$.

18. Αφού $d, n \in \mathbb{N}$ και $d \mid n$, υπάρχει $k \in \mathbb{N}$ τέτοιος ώστε $n = dk$. Χρησιμοποιώντας την ταυτότητα $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$ με $x = 2^d$, παίρνουμε

$$2^n - 1 = 2^{kd} - 1 = (2^d)^k - 1 = (2^d - 1) \cdot \left(2^{d(k-1)} + 2^{d(k-2)} + \cdots + 2^d + 1\right).$$

Αφού $2^{d(k-1)} + 2^{d(k-2)} + \cdots + 2^d + 1 \in \mathbb{N}$, συμπεραίνουμε ότι $(2^d - 1) \mid (2^n - 1)$.

19. Οι $7, 8, 9$ είναι ανά δύο σχετικώς πρώτοι και συνεπώς (Λήμμα 1.4.3) ο $271xyz$ διαιρείται με καθέναν από τους αριθμούς αυτούς εάν και μόνο αν διαιρείται με το γινόμενό τους $7 \cdot 8 \cdot 9 = 504$. Έχουμε $271xyz = 271000 + xyz$ και η Ευκλείδεια διαίρεση δίνει $271000 = 504q + 352$, με $q \in \mathbb{Z}$, οπότε πρέπει $504 \mid xyz + 352$ και συνεπώς $xyz = 504 - 352 = 152$ ή $xyz = 152 + 504 = 654$.

20. (α) Παρατηρούμε ότι

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n(n-1)\cdots(n-k+1)\cdot(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!}.$$

Παίρνοντας αυτόν σαν ορισμό του $\binom{n}{k}$ στην περίπτωση $k = 0$, έχουμε

$$\binom{n}{0} = \frac{n!}{0!n!} = 1 \text{ και } \binom{n}{n} = \frac{n!}{n!0!} = 1$$

αφού $0! = 1$. Παρατηρήστε επίσης ότι

$$\binom{n}{k} = \binom{n}{n-k}.$$

Αν $n \geq 2$ και $1 \leq k \leq n-1$, τότε

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)\cdots(n-k+1)(n-k)}{k!} + \frac{(n-1)\cdots(n-k+1)}{(k-1)!} \\ &= \frac{(n-1)\cdots(n-k+1)(n-k)}{k!} + \frac{(n-1)\cdots(n-k+1)k}{k!} \\ &= \frac{(n-1)\cdots(n-k+1)[(n-k)+k]}{k!} \\ &= \frac{n(n-1)\cdots(n-k+1)}{k!} = \binom{n}{k}.\end{aligned}$$

(β) Χρησιμοποιώντας την τελευταία σχέση, δείχνουμε με επαγωγή ως προς $n \geq 2$ την εξής πρόταση $P(n)$: για κάθε $1 \leq k \leq n-1$, ο $\binom{n}{k}$ είναι ακέραιος.

Αν τώρα μας δώσουν k διαδοχικούς φυσικούς αριθμούς ($k \geq 2$) και αν n είναι ο μεγαλύτερος από αυτούς, τότε το γινόμενό τους ισούται με $Q = n \cdot (n-1)\cdots(n-k+1)$. Αφού ο

$$\binom{n}{k} = \frac{n \cdot (n-1)\cdots(n-k+1)}{k!} = \frac{Q}{k!}$$

είναι ακέραιος, συμπεραίνουμε ότι $k! \mid Q$.

21. (α) Από την Άσκηση 20 έχουμε $\binom{n}{k} = \frac{n!}{k!(n-k)!} \in \mathbb{Z}$ και συνεπώς $k!(n-k)! \mid n! = n \cdot (n-1)!$. Από την υπόθεση οι $k!(n-k)!$ και n είναι σχετικώς πρώτοι οπότε (Λήμμα 1.4.2) $k!(n-k)! \mid (n-1)!$, δηλαδή $\frac{(n-1)!}{k!(n-k)!} \in \mathbb{Z}$. Με άλλα λόγια $n \mid \frac{n!}{k!(n-k)!} = \binom{n}{k}$.

(β) Όχι, π.χ. αν $n = 4$ και $k = 2$, οπότε $\binom{n}{k} = \binom{4}{2} = 6$.

22. Γράφουμε

$$n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2+2)^2 - 4n^2 = (n^2+2n+2)(n^2-2n+2),$$

και παρατηρούμε ότι $1 < n^2+2n+2$ και $1 < n^2-2n+2$ γιατί $(n-1)^2 > 0$ αν $n \geq 2$. Άρα ο n^4+4 είναι σύνθετος για κάθε $n \geq 2$.

23. Αν $n = 1$, τότε οι 1, 3 και 5 δεν είναι όλοι πρώτοι (ο 1 δεν είναι πρώτος). Αν $n = 2$, τοτε οι 2, 4 και 6 δεν είναι όλοι πρώτοι. Στην περίπτωση $n = 3$ παίρνουμε την τριάδα των πρώτων 3, 5 και 7.

Έστω $n > 3$. Διακρίνουμε τρείς περιπτώσεις, ανάλογα με το υπόλοιπο της διαίρεσης του n με 3:

(α) Αν $n = 3k$, τότε $k > 1$ άρα ο n είναι σύνθετος.

(β) Αν $n = 3k+1$, τότε ο $n+2 = 3k+3 = 3(k+1)$ είναι σύνθετος.

(γ) Αν $n = 3k+2$, τότε ο $n+4 = 3k+6 = 3(k+2)$ είναι σύνθετος.

Σε κάθε περίπτωση, αν $n > 3$ κάποιος από τους n, $n+2$ και $n+4$ είναι σύνθετος.

24. Αν $p > 3$ τότε ο p δεν διαιρείται με το 3 και συνεπώς (Άσκηση 7 α) $p^2 = 3k+1$ με $k \in \mathbb{Z}$. Τότε ο $8p^2+1 = 24k+9$ διαιρείται με το 3 και συνεπώς δεν είναι πρώτος. Αν $p = 2$ ή $p = 3$ τότε $8p^2+1 = 33$ ή 73, αντίστοιχα, άρα $p = 3$ είναι η μόνη δυνατότητα.

25. (α) Ο p δεν μπορεί να είναι της μορφής $6k$ ή $6k+2 = 2(3k+1)$ ή $6k+3 = 3(2k+1)$ ή $6k+4 = 2(3k+2)$ γιατί θα ήταν σύνθετος. Άρα είναι της μορφής $6k+1$ ή $6k+5 = 6(k+1)-1 = 6k'-1$.

(β) Αν $p = 6k+1$ τότε $p^2-1 = 36k^2+12k = 12k(3k+1)$. Παρατηρούμε ότι ο $k(3k+1)$ είναι πάντα άρτιος (εξηγήστε, διακρίνοντας τις περιπτώσεις k =άρτιος και k =περιττός), άρα ο p^2-1 είναι πολλαπλάσιο του 24.

Αν $p = 6k-1$ τότε $p^2-1 = 36k^2-12k = 12k(3k-1)$. Παρατηρούμε, όπως πριν, ότι ο $k(3k-1)$ είναι πάντα άρτιος, άρα ο p^2-1 είναι πολλαπλάσιο του 24.

(γ) Σύμφωνα με το Λήμμα 1.4.3, αρκεί να δείξουμε ότι $3 \mid n(n^2-1)$ και $8 \mid n(n^2-1)$. Προφανώς ένας (ακριβώς) από τους $n-1$, n, $n+1$ είναι πολλαπλάσιο του 3 και συνεπώς $3 \mid n(n-1)(n+1) = n(n^2-1)$. Επίσης $8 \mid (n^2-1) \mid n(n^2-1)$ από την 'σκηση 7 β.

26. Διακρίνουμε τις περιπτώσεις $n = 2k$ και $n = 2k+1$.

(α) Αν $n = 2k$, τότε $k > 1$ αφού $n > 2$, και $2^n - 1 = (2^k)^2 - 1 = (2^k-1)(2^k+1)$. Αφού $1 < 2^k+1$ και $1 < 2^k-1$, ο 2^n-1 είναι σύνθετος.

(β) Αν $n = 2k+1$, τότε $2^n+1 = 2^{2k+1}+1 = (2+1)(2^{2k} - 2^{2k-1} + \cdots - 2 + 1)$. Αφού $1 < 3 < 2^n+1$, ο 2^n+1 είναι σύνθετος.

27. Αν όχι τότε ο $p+q$ γράφεται ως γινόμενο δύο το πολύ πρώτων. Όμως οι p, q είναι περιττοί, επομένως ο $p+q$ είναι άρτιος και συνεπώς $p+q = 2r$ για κάποιο πρώτο r. Τότε $r = (p+q)/2$ και συνεπώς $p < r < q$ ή $q < r < p$, σε αντίφαση με την υπόθεση ότι οι p και q είναι διαδοχικοί πρώτοι.

28. Ο αριθμός 101 είναι πρώτος. Θα δείξουμε ότι δεν υπάρχουν άλλοι πρώτοι στην ακολουθία. Πράγματι, οι υπόλοιποι όροι με άρτιο πλήθος ψηφίων ίσων με 1 διαιρούνται με το 101, π.χ. $10101010101 = 101 \cdot (1+10^4+10^8) = 101 \cdot 100010001$, ενώ για αυτούς με περιττό πλήθος ψηφίων ίσων με , έστω $2n+1$, έχουμε

$$\begin{aligned} 1 + 10^2 + 10^4 + \cdots + 10^{4n} &= \frac{10^{4n+2}-1}{10^2-1} = \frac{(10^{2n+1}-1)(10^{2n+1}+1)}{(10-1)(10+1)} \\ &= (1+10+10^2+\cdots+10^{2n})(1-10+10^2-\cdots+10^{2n}), \end{aligned}$$

που είναι σύνθετος αριθμός.

29. (α) Αφού $k_p \le r_p$ και $k_p \le s_p$ για κάθε $p \in P$, έχουμε $p^{k_p} \mid p^{r_p}$ και $p^{k_p} \mid p^{s_p}$ για κάθε $p \in P$. Άρα

$$\prod_{p\in P} p^{k_p} \mid \prod_{p\in P} p^{r_p} = a \text{ και } \prod_{p\in P} p^{k_p} \mid \prod_{p\in P} p^{s_p} = b,$$

οπότε

$$(*) \qquad \prod_{p\in P} p^{k_p} \mid (a,b).$$

Έστω $d = \prod_{p\in P} p^{u_p}$ ο μέγιστος κοινός διαιρέτης των a και b. Από την $q^{u_q} \mid d \mid a = \prod_{p\in P} p^{r_p}$ έπεται ότι $q^{u_q} \mid q^{r_q}$ δηλαδή $u_q \le r_q$ για κάθε $q \in P$. Ομοίως, $u_q \le s_q$ για κάθε $q \in P$. Άρα, $u_p \le k_p = \min\{r_p, s_p\}$ για κάθε $p \in P$, οπότε

$$(**) \qquad d = \prod_{p\in P} p^{u_p} \mid \prod_{p\in P} p^{k_p}.$$

Από τις $(*)$ και $(**)$ βλέπουμε ότι $(a,b) = \prod_{p\in P} p^{k_p}$.

(β-1) Έστω $d = (a,b)$. Τότε, $d \mid a$ και $d \mid b$ άρα $cd \mid ca$ και $cd \mid cb$, οπότε $cd \mid (ac, bc)$. Αντίστροφα, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $ax + by = d$, άρα $acx + bcy = cd$. Αφού $(ac,bc) \mid ac$ και $(ac,bc) \mid bc$, παίρνουμε $(ac,bc) \mid acx + bcy = cd$. Αφού $cd \mid (ac,bc)$ και $(ac,bc) \mid cd$, παίρνουμε $(ac,bc) = cd = c(a,b)$.

(β-2) Έστω $d = (a,b)$. Τότε $(a,dc) \mid a$ και $d \mid b \Longrightarrow (a,dc) \mid dc \mid bc$, άρα $(a,dc) \mid (a,bc)$. Αντίστροφα, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $d = ax + by$, άρα $dc = acx + bcy$. Τότε, $(a,bc) \mid a$ και $(a,bc) \mid bc$, άρα $(a,bc) \mid acx + bcy = dc$. Αφού $(a,bc) \mid a$ και $(a,bc) \mid dc$, παίρνουμε $(a,bc) \mid (a,dc)$.

(β-3) Υποθέτουμε πρώτα ότι $(a,b)=1$. Τότε, αν $d=(a^2,b^2)>1$ θεωρούμε έναν πρώτο $p \mid d$ και έχουμε $p \mid a^2 \Longrightarrow p \mid a$ και $p \mid b^2 \Longrightarrow p \mid b$, δηλαδή $p \mid (a,b)=1$, άτοπο. Άρα $(a^2,b^2)=1=(a,b)$.

Στη γενική περίπτωση, θέτουμε $w=(a,b)$ και γράφουμε $a=wx$ και $b=wy$ όπου $(x,y)=1$. Από το (β-1) έχουμε

$$(a^2,b^2)=(w^2x^2,w^2y^2)=w^2(x^2,y^2)=w^2=(a,b)^2,$$

γιατί $(x^2,y^2)=1$ από το προηγούμενο βήμα.

(γ) Γράφουμε $a=\prod_{p\in P}p^{r_p}$, $b=\prod_{p\in P}p^{s_p}$ και $c=\prod_{p\in P}p^{t_p}$. Τότε, $ac=\prod_{p\in P}p^{r_p+t_p}$ και $bc=\prod_{p\in P}p^{s_p+t_p}$. Άρα

$$(ac,bc)=\prod_{p\in P}p^{\min\{r_p+t_p,s_p+t_p\}}=\prod_{p\in P}p^{\min\{r_p,s_p\}}p^{t_p}=\prod_{p\in P}p^{\min\{r_p,s_p\}}\prod_{p\in P}p^{t_p}=(a,b)c.$$

Με τον ίδιο τρόπο μπορείτε να αποδείξετε τους άλλους δύο ισχυρισμούς.

30. (α) Θεωρούμε το σύνολο $S=\{x\in\mathbb{N}: a \mid x \text{ και } b \mid x\}$. Το S είναι μη κενό, αφού $ab\in S$. Άρα έχει ελάχιστο στοιχείο το οποίο συμβολίζουμε με m. Αφού $m\in S$, είναι φανερό ότι $a \mid m$ και $b \mid m$. Έστω $x\in S$. Από τον ορισμό του m έχουμε $x\geq m$. Θα υποθέσουμε ότι ο x δεν είναι πολλαπλάσιο του m και θα καταλήξουμε σε άτοπο. Από την ταυτότητα της διαίρεσης, $x=mq+r$ όπου $q\in\mathbb{N}$ και $0\leq r<m$. Αν ο x δεν είναι πολλαπλάσιο του m, τότε $r\in\mathbb{N}$ και $r<m$. Επίσης, $a \mid x-mq=r$ γιατί $a \mid x$ και $a \mid m$. Ομοίως, $b \mid r$ άρα $r\in S$. Αυτό είναι άτοπο γιατί $r<m$ και ο m ήταν το ελάχιστο στοιχείο του S. Άρα $m \mid x$ για κάθε $x\in S$.

(β) Δείξτε ότι $[a,b]=\prod_{p\in P}p^{\max\{r_p,s_p\}}$, όπου $a=\prod_{p\in P}p^{r_p}$ και $b=\prod_{p\in P}p^{s_p}$. Μιμηθείτε την απόδειξη στην Άσκηση 29 (α).

31. Ορίζουμε σαν ελάχιστο κοινό πολλαπλάσιο $[a,b,c]$ των $a,b,c\in\mathbb{N}$ το μοναδικό φυσικό αριθμό που ικανοποιεί τα εξής:

1. $a \mid [a,b,c]$, $b \mid [a,b,c]$ και $c \mid [a,b,c]$.
2. Αν $x\in\mathbb{N}$ και $a \mid x$, $b \mid x$, $c \mid x$, τότε $[a,b,c] \mid x$.

(α) Έστω $a=\prod_{p\in P}p^{a_p}$ και $b=\prod_{p\in P}p^{b_p}$. Αν $d=(a,b)$ και $m=[a,b]$, τότε $d=\prod_{p\in P}p^{d_p}$ και $m=\prod_{p\in P}p^{m_p}$. Για να δείξουμε ότι $ab=dm$, αρκεί να δείξουμε ότι για κάθε $p\in P$ ισχύει $p^{a_p}p^{b_p}=p^{d_p}p^{m_p}$ δηλαδή

$$a_p+b_p=d_p+m_p.$$

Όμως, $d_p=\min\{a_p,b_p\}$ και $m_p=\max\{a_p,b_p\}$, οπότε το ζητούμενο έπεται από την ταυτότητα

$$x+y=\min\{x,y\}+\max\{x,y\},$$

η οποία ισχύει για κάθε $x,y\in\mathbb{R}$ (εξηγήστε).

(β) Όπως στο προηγούμενο ερώτημα, γράφουμε $a=\prod_{p\in P}p^{a_p}$, $b=\prod_{p\in P}p^{b_p}$, $c=\prod_{p\in P}p^{c_p}$. Εκφράζουμε τους υπόλοιπους αριθμούς της άσκησης σαν γινόμενα δυνάμεων πρώτων με εκθέτες συναρτήσεις των a_p, b_p και c_p. Για παράδειγμα, το ελάχιστο κοινό πολλαπλάσιο των b και c γράφεται $[b,c]=\prod_{p\in P}p^{\max\{b_p,c_p\}}$. Τότε, η ισότητα που ζητάμε είναι συνέπεια της

$$\begin{aligned}&\max\{a_p,b_p,c_p\}^2\min\{a_p,b_p\}\min\{a_p,c_p\}\min\{b_p,c_p\}\\&=\min\{a_p,b_p,c_p\}^2\max\{a_p,b_p\}\max\{a_p,c_p\}\max\{b_p,c_p\}\end{aligned}$$

για κάθε $p\in P$. Λόγω συμμετρίας μπορούμε να υποθέσουμε ότι $a_p\leq b_p\leq c_p$, οπότε η ζητούμενη ισότητα ανάγεται στην

$$c_p^2a_p^2b_p=a_p^2b_pc_p^2$$

η οποία ισχύει.

32. Παρατηρούμε πρώτα ότι αν $(a,b)=1$ τότε $(a+b,[a,b])=1$. Πράγματι, από την 'σκηση 31 έχουμε $[a,b]=ab$ και $(a+b,ab)=1$ από την 'σκηση 16 α. Για τη γενική περίπτωση γράφουμε $a=dx$, $b=dy$ όπου $d=(a,b)$ και $(x,y)=1$. Τότε

$$(a+b,[a,b])=\big(dx+dy,\frac{d^2xy}{d}\big)=d(x+y,xy)=d=(a,b),$$

αφού $(x+y,xy)=1$. Η τελευταία πρόταση προκύπτει αμέσως.

33. Θα δείξουμε ότι αν $m=qn+r$ όπου $m\geq n$, $q,r\in\mathbb{Z}$ και $0\leq r<n$ τότε

$$(a^m-1,a^n-1)=(a^n-1,a^r-1).$$

Αν $d=(a^n-1,a^r-1)$, τότε χρησιμοποιώντας την $a^n-1\mid a^{qn}-1$ βλέπουμε ότι

$$d\mid a^r(a^{qn}-1)+(a^r-1)=a^{qn+r}-1=a^m-1,$$

άρα $d\mid(a^m-1,a^r-1)$. Αντίστροφα, αν $d_1=(a^m-1,a^n-1)$, έχουμε $d_1\mid a^n-1\mid a^{qn}-1$, άρα

$$d_1\mid a^m-1-a^r(a^{qn}-1)=a^r-1.$$

Επομένως $d_1\mid(a^n-1,a^r-1)=d$.

Τώρα χρησιμοποιούμε τον αλγόριθμο του Ευκλείδη. Υποθέτουμε ότι $m\geq n$. Αν $n\mid m$ το συμπέρασμα είναι προφανές, αλλιώς μπορούμε να βρούμε $q_1,\ldots,q_{n+1}\in\mathbb{N}$ και $r_1,\ldots,r_n\in\mathbb{N}$ με $0<r_n<r_{n-1}<\cdots<r_1<n$ έτσι ώστε

$$\begin{aligned}
m &= nq_1+r_1,\\
n &= r_1q_2+r_2,\\
r_1 &= r_2q_3+r_3,\\
\vdots &= \vdots\\
r_{n-2} &= r_{n-1}q_n+r_n,\\
r_{n-1} &= r_nq_{n+1},
\end{aligned}$$

και $(m,n)=r_n$. Ο προηγούμενος συλλογισμός δείχνει ότι

$$\begin{aligned}
(a^m-1,a^n-1) &= (a^n-1,a^{r_1}-1)=(a^{r_1}-1,a^{r_2}-1)=\cdots=(a^{r_{n-1}}-1,a^{r_n}-1)\\
&= a^{r_n}-1=a^{(m,n)}-1.
\end{aligned}$$

34. Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι της μορφής $4n-1$, οι $q_1,q_2,\ldots,q_N$ (υπάρχει τουλάχιστον ένας τέτοιος πρώτος, ο 3). Θεωρούμε τον αριθμό

$$S=4q_1q_2\ldots q_N-1.$$

Ο S είναι μεγαλύτερος από 1, άρα έχει κανονική ανάλυση $S=p_1^{r_1}\cdots p_k^{r_k}$ σε γινόμενο πρώτων διαιρετών, όπου $r_j\geq1$ και όλοι οι p_j είναι περιττοί αφού ο S είναι περιττός. Αν όλοι οι p_j ήταν της μορφής $4k+1$, τότε το γινόμενό τους θα ήταν κι αυτό της μορφής $4k+1$ (γιατί;) ενώ ο S είναι της μορφής $4k-1$. Άρα ο S έχει τουλάχιστον έναν πρώτο διαιρέτη p της μορφής $4n-1$.

Αφού $q_1,q_2,\ldots,q_N$ είναι όλοι οι πρώτοι της μορφής $4n-1$, συμπεραίνουμε ότι $p=q_i$ για κάποιον $i\leq N$. Όμως τότε, $p\mid4q_1q_2\ldots q_N$ και $p\mid S$, άρα $p\mid S-4q_1q_2\ldots q_N=1$, το οποίο είναι άτοπο. Το άτοπο δείχνει ότι υπάρχουν άπειροι πρώτοι της μορφής $4n-1$.

35. Υποθέτουμε ότι ο 2^n+1 είναι πρώτος για κάποιον $n \geq 2$. Αν ο n δεν είναι δύναμη του 2, τότε γράφεται μονοσήμαντα στη μορφή $n = 2^k s$, όπου $s > 1$ περιττός φυσικός. Αν $x = 2^{2^k}$ τότε

$$2^n + 1 = x^s + 1 = (x+1)(x^{s-1} - x^{s-2} + \cdots - x + 1).$$

Αφού $1 < x+1 < x^s+1$, ο 2^n+1 είναι σύνθετος. Καταλήξαμε σε άτοπο, άρα ο n είναι δύναμη του 2.

36. Υποθέτουμε ότι ο 2^n-1 είναι πρώτος για κάποιον $n \geq 2$. Αν ο n δεν είναι πρώτος, τότε υπάρχουν $d, k > 1$ τέτοιοι ώστε $n = dk$. Από την Άσκηση 18

$$2^d - 1 \mid 2^n - 1.$$

Αφού $1 < 2^d - 1 < 2^n - 1$, ο 2^n-1 είναι σύνθετος. Καταλήξαμε σε άτοπο, άρα ο n είναι πρώτος.

Σημείωση: Δεν ισχύει το αντίστροφο. Ο $p = 11$ είναι πρώτος, αλλά ο $2^{11} - 1 = 2047 = 23 \cdot 89$ είναι σύνθετος.

37. (α) Υποθέτουμε ότι ο n είναι σύνθετος. Τότε, υπάρχουν $1 < k \leq m < n$ τέτοιοι ώστε $n = km$. Από την $k \leq m$ έπεται ότι $n \geq k^2$ δηλαδή $k \leq \sqrt{n}$. Αφού $k \geq 2$, ο k έχει έναν πρώτο διαιρέτη p. Τότε, $p \mid k \mid n$ και $p \leq k \leq \sqrt{n}$.

(β) Έχουμε $[\sqrt{509}] = 22$. Σύμφωνα με το (α), αν ο 509 είναι σύνθετος θα διαιρείται με κάποιον πρώτο $p \leq 22$, δηλαδή με κάποιον από τους $2, 3, 5, 7, 11, 13, 17, 19$. Κάνοντας οκτώ διαιρέσεις βλέπουμε ότι ο 509 είναι πρώτος.

Ομοίως, $[\sqrt{2093}] = 45$. Παρατηρούμε ότι $2093 = 7 \cdot 299$. Για να βρούμε την ανάλυση του 299, θεωρούμε τον $[\sqrt{299}] = 17$. Παρατηρούμε ότι $299 = 13 \cdot 23$ και ότι οι 13 και 23 είναι πρώτοι. Άρα η κανονική αναπαράσταση του 2093 είναι $2093 = 7 \cdot 13 \cdot 23$.

38. Ας υποθέσουμε ότι $\sqrt{p} = m/n$ για κάποιους $m, n \in \mathbb{N}$. Αν $r = m/(m,n)$ και $s = n/(m,n)$, τότε $\sqrt{p} = r/s$ και $(r,s) = 1$. Τότε, $p = r^2/s^2$ δηλαδή $p \mid ps^2 = r^2$. Αφού ο p είναι πρώτος, παίρνουμε $p \mid r$, άρα $r = px$ για κάποιον $x \in \mathbb{N}$. Επιστρέφοντας στην $ps^2 = r^2$ έχουμε $ps^2 = p^2x^2 \Longrightarrow px^2 = s^2$. Όπως πριν, $p \mid px^2 = s^2$, άρα $p \mid s$. Όμως τότε $p \mid (r,s) = 1$, άτοπο. Άρα ο $\sqrt{p}$ είναι άρρητος.

39. Χρησιμοποιώντας την Άσκηση 37 μπορείτε να ελέγξετε ότι ο n^2+n+41 είναι πρώτος για $n = 0, 1, \ldots, 39$ (θα χρειαστούν πολλές πράξεις!). Όμως,

$$f(40) = 40^2 + 40 + 41 = 40^2 + 2 \cdot 40 + 1 = (40+1)^2 = 41^2,$$

δηλαδή ο $f(40)$ είναι σύνθετος.

40. Υποθέτουμε ότι για το πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_k x^k$, $k \geq 1$, $a_k \neq 0$, έχουμε $|f(n)| =$πρώτος για κάθε n. Ειδικότερα,

$$|f(1)| = p$$

όπου p πρώτος. Παρατηρούμε ότι για κάθε $s \in \mathbb{N}$,

$$f(1+sp) = a_0 + a_1(1+sp) + \cdots + a_k(1+sp)^k = a_0 + a_1 \cdot 1 + \cdots + a_k \cdot 1^k + Bp = f(1) + Bp,$$

όπου $B \in \mathbb{Z}$. Άρα $p \mid f(1) + Bp = f(1+sp) \mid |f(1+sp)|$. Όμως $|f(1+sp)| = q \in P$ από την υπόθεση, και αφού $p \mid q$ έπεται ότι $p = q$. Δηλαδή,

$$|f(1+sp)| = p$$

για κάθε $s \in \mathbb{N}$. Αυτό είναι άτοπο, αφού $\lim_{s\to\infty} |f(1+sp)| = \infty$ (η f είναι πολυώνυμο βαθμού $k \geq 1$, άρα $\lim_{x\to\infty} |f(x)| = \infty$).

41. Για κάθε $k = 2, \ldots, n+1$ έχουμε $k \mid (n+1)!$ και $k \mid k$, άρα $k \mid (n+1)! + k$. Δηλαδή ο $(n+1)! + k$ είναι σύνθετος για κάθε $k = 2, \ldots, n+1$.

Οι $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$ είναι n διαδοχικοί σύνθετοι φυσικοί αριθμοί.

42. Με επαγωγή: αν $n = 1$ ζητάμε την $2^1 \mid 2$, η οποία προφανώς ισχύει.

Υποθέτουμε ότι $2^k \mid (k+1)(k+2)\cdots(2k)$, δηλαδή $(k+1)(k+2)\cdots(2k) = 2^k m$ για κάποιον $m \in \mathbb{N}$. Θα δείξουμε ότι ο $(k+2)(k+3)\cdots(2k+2)$ είναι πολλαπλάσιο του 2^{k+1}. Γράφουμε

$$\begin{aligned}(k+2)(k+3)\cdots(2k+2) &= (k+2)(k+3)\cdots(2k)(2k+1)(2k+2)\\ &= 2(k+1)(k+2)(k+3)\cdots(2k)(2k+1)\\ &= 2\cdot 2^k m\cdot(2k+1)\\ &= 2^{k+1}m(2k+1).\end{aligned}$$

Άρα $2^{k+1} \mid (k+1)(k+2)\cdots(2k)$.

43. Υποθέτουμε πρώτα ότι ο n είναι άρτιος, δηλαδή $n = 2k$ για κάποιον $k \geq 6$. Τότε

$$n = 2(k-3) + 6$$

και οι $2(k-3)$, 6 είναι σύνθετοι αριθμοί. Έστω τώρα ότι ο n είναι περιττός. Γράφουμε

$$n = (n-9) + 9$$

και παρατηρούμε ότι ο $9 = 3^2$ είναι σύνθετος και ο $n-9$ είναι άρτιος μεγαλύτερος ή ίσος του 4, άρα σύνθετος. Σε κάθε περίπτωση, ο $n \geq 12$ γράφεται σαν άθροισμα δύο σύνθετων αριθμών.

Σημείωση: Είναι σωστό ότι κάθε άρτιος αριθμός $n \geq 4$ γράφεται σαν άθροισμα δύο πρώτων αριθμών; Αυτό είναι ένα από τα πιο γνωστά ανοικτά προβλήματα της θεωρίας των αριθμών, η **εικασία του Goldbach**.

44. Ας υποθέσουμε ότι για κάποιον πρώτο p ισχύει $29p + 1 = s^2$, όπου $s \in \mathbb{N}$. Τότε

$$29p = s^2 - 1 = (s-1)(s+1).$$

Παρατηρούμε ότι $(s+1) \mid 29p$ και ότι οι μόνοι διαιρέτες του $29p$ είναι οι 1, p, 29 και $29p$ (γιατί ο 29 είναι πρώτος). Υπάρχουν λοιπόν τα εξής ενδεχόμενα:

(α) $s + 1 = 1$, το οποίο απορρίπτεται γιατί $s > 0$.

(β) $s + 1 = 29p$, το οποίο απορρίπτεται γιατί τότε $s - 1 = 1$ άρα $s = 2$ και τότε $29p = 2^2 - 1 = 3$, το οποίο είναι άτοπο.

(γ) $s + 1 = 29$, το οποίο απορρίπτεται γιατί τότε $27 = s - 1 = p$, το οποίο δεν μπορεί να συμβαίνει αφού ο p είναι πρώτος.

(δ) $s + 1 = p$, οπότε $s - 1 = 29$ άρα $p = 29 + 2 = 31$.

Ο $p = 31$ είναι πρώτος και $29 \cdot 31 + 1 = 900 = 30^2$. Από τη συζήτηση που προηγήθηκε, ο 31 είναι ο μόνος πρώτος για τον οποίο ο $29p + 1$ είναι τέλειο τετράγωνο.

45. Έστω ότι οι p και q είναι δίδυμοι πρώτοι. Μπορούμε να υποθέσουμε ότι $q = p + 2$. Τότε

$$pq + 1 = p(p+2) + 1 = p^2 + 2p + 1 = (p+1)^2,$$

δηλαδή ο $pq + 1$ είναι τέλειο τετράγωνο.

Αντίστροφα: υποθέτουμε ότι οι p, q είναι πρώτοι και ότι $pq + 1 = s^2$ για κάποιον $s \in \mathbb{N}$. Τότε $pq = s^2 - 1 = (s-1)(s+1)$, και αφού οι μόνοι διαιρέτες του p; είναι οι 1, p, q και pq, υπάρχουν τα εξής ενδεχόμενα:

(α) $s+1=1$, το οποίο απορρίπτεται γιατί $s>0$.

(β) $s+1=pq$, το οποίο απορρίπτεται γιατί τότε $s-1=1$ άρα $s=2$ και τότε $pq=2^2-1=3$, το οποίο είναι άτοπο αφού ο 3 είναι πρώτος.

(γ) $s+1=p$, οπότε $q=s-1=p-2$, δηλαδή $|p-q|=2$.

(δ) $s+1=q$, οπότε $p=s-1=q-2$, δηλαδή $|p-q|=2$.

Είδαμε ότι αν οι p,q είναι πρώτοι και $pq+1=s^2$, τότε συμβαίνει ένα από τα (γ) και (δ). Σε καθεμία από αυτές τις δύο περιπτώσεις, $|p-q|=2$.

46. (α) Έστω p ο μεγαλύτερος πρώτος που είναι μικρότερος από τον n. Υποθέτουμε ότι $2p\leq n$ και θα καταλήξουμε σε άτοπο. Από το αίτημα του Bertrand υπάρχει πρώτος q με $p<q<2p$ (πάρτε στη θέση του n τον p). Τότε

$$p<q<2p\leq n,$$

δηλαδή, ο q είναι πρώτος μικρότερος από τον n και $q>p$. Αυτό είναι άτοπο αφού ο p ήταν ο μεγαλύτερος πρώτος «κάτω» από τον n.

(β) Με επαγωγή, αρχίζοντας από $n=2$: $p_2=3<4=2^2$. Υποθέτουμε ότι $p_k<2^k$. Από το αίτημα του Bertrand, ανάμεσα στον 2^k και στον 2^{k+1} υπάρχει πρώτος p_j. Αφού $p_k<2^k$ και $p_j>2^k$, έχουμε $j>k$ (αν ήταν $j\leq k$ θα είχαμε $p_j\leq p_k<2^k$). Άρα $k+1\leq j$, το οποίο σημαίνει ότι

$$p_{k+1}\leq p_j<2^{k+1}.$$

Αυτό αποδεικνύει το επαγωγικό βήμα.

Έστω $x\geq 4$. Υπάρχει μοναδικός $k\geq 2$ τέτοιος ώστε $2^k\leq x<2^{k+1}$. Τότε από την $p_k<2^k$ έχουμε $\pi(2^k)\geq k$ και αφού η π είναι αύξουσα, παίρνουμε

$$\pi(x)\geq\pi(2^k)\geq k.$$

Από την άλλη πλευρά,

$$x<2^{k+1}\Longrightarrow\log_2 x<k+1.$$

'ρα

$$\pi(x)\geq k>\log_2 x-1.$$

47. Με επαγωγή ως προς n. Για $n=3$ ζητάμε την $5\leq 2+3$ η οποία ισχύει. Υποθέτουμε ότι

$$p_k\leq p_1+p_2+\cdots+p_{k-1}$$

για κάποιον $k\geq 3$. Υπάρχει πρώτος p_j με $p_k<p_j<2p_k$ και, όπως στην προηγούμενη άσκηση, έχουμε $j>k$ άρα $p_{k+1}\leq p_j<2p_k$. Από την επαγωγική υπόθεση έπεται ότι

$$p_{k+1}<2p_k=p_k+p_k\leq p_1+p_2+\cdots+p_{k-1}+p_k.$$

Αυτό αποδεικνύει το επαγωγικό βήμα.

48. Υποθέτουμε πρώτα ότι ο n είναι άρτιος. Τότε $n/2\in\mathbb{N}$ και από το αίτημα του Bertrand υπάρχει πρώτος p με $n/2<p<n$. Παρατηρούμε ότι ο p δεν διαιρεί κανέναν $x\leq n$ εκτός από τον εαυτό του: τα πολλαπλάσια του p είναι οι αριθμοί $p,2p,3p,\ldots$, και έχουμε $kp>n$ για κάθε $k\geq 2$.

Άρα στην κανονική αναπαράσταση του $n!=2\cdot 3\cdots n$ ο p θα εμφανίζεται με εκθέτη 1, δηλαδή με περιττό εκθέτη. Τότε, ο $n!$ δεν μπορεί να είναι τέλειο τετράγωνο: αν ήταν, όλοι οι πρώτοι διαιρέτες του θα είχαν άρτιο εκθέτη, άρα και ο p.

Αν $n=2s+1$, βρίσκουμε πρώτο p με $s<p<2s$. Πάλι, $p\geq s+1$ άρα $2p\geq 2s+2>n$, οπότε εφαρμόζεται το προηγούμενο επιχείρημα: ο p δεν διαιρεί κανέναν $x\leq n$ εκτός από τον εαυτό του, άρα ο εκθέτης του είναι 1 στην κανονική αναπαράσταση του $n!$.

49. Έστω $n \geq 2$. Υπάρχει μοναδικός $s \geq 1$ τέτοιος ώστε $2^s \leq n < 2^{s+1}$. Επίσης, ορίζουμε B το γινόμενο όλων των περιττών φυσικών $m \leq n$. Παρατηρήστε ότι ο B είναι περιττός. Ας υποθέσουμε ότι $\sum_{k=1}^{n} \frac{1}{k} \in \mathbb{N}$. Τότε

$$\sum_{k=1}^{n} \frac{2^{s-1}B}{k} = 2^{s-1}B \sum_{k=1}^{n} \frac{1}{k} \in \mathbb{N}.$$

Αν $k \leq n$ και $k \neq 2^s$, τότε ο k γράφεται μονοσήμαντα στη μορφή $k = 2^l m$, όπου $0 \leq l < s$ και ο m είναι περιττός (γιατί;). Άρα $k \mid 2^{s-1}B$. Έπεται ότι

$$\frac{B}{2} = \frac{2^{s-1}B}{2^s} = \sum_{k=1}^{n} \frac{2^{s-1}B}{k} - \sum_{k \neq 2^s} \frac{2^{s-1}B}{k} \in \mathbb{N}.$$

Αυτό είναι άτοπο αφού ο B είναι περιττός.

50. (α) Ο μέγιστος κοινός διαιρέτης των 6 και 51 είναι ο $(6, 51) = 3$. Αφού ο 3 δεν διαιρεί τον 22, η εξίσωση δεν έχει ακέραιες λύσεις.

(β) Ο μέγιστος κοινός διαιρέτης των 33 και 14 είναι ο $(33, 14) = 1$. Αφού $1 \mid 115$, η εξίσωση έχει ακέραιες λύσεις.

(γ) Ο μέγιστος κοινός διαιρέτης των 14 και 35 είναι ο $(14, 35) = 7$. Αφού ο 7 δεν διαιρεί τον 93, η εξίσωση δεν έχει ακέραιες λύσεις.

51. Υπολογίζουμε πρώτα το μέγιστο κοινό διαιρέτη των 24 και 138.

$$\begin{aligned} 138 &= 24 \cdot 5 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 \end{aligned}$$

'ρα $(24, 138) = 6$. Αφού $6 \mid 18$, η εξίσωση έχει ακέραιες λύσεις. Βρίσκουμε μια λύση της εξίσωσης.

$$\begin{aligned} 6 &= 24 - 18 = 24 - (138 - 24 \cdot 5) = 24 - 138 + 24 \cdot 5 \\ &= 24 \cdot 6 + 138 \cdot (-1). \end{aligned}$$

Πολλαπλασιάζοντας επί 18/6=3 παίρνουμε

$$24 \cdot 18 + 138 \cdot (-3) = 18.$$

Δηλαδή, μια λύση της εξίσωσης είναι οι $x_0 = 18$ και $y_0 = -3$.

Έχουμε $r_1 = 24/6 = 4$ και $r_2 = 138/6 = 23$. Άρα οι λύσεις της εξίσωσης είναι τα ζευγάρια

$$x = 18 + 23t \text{ και } y = -3 - 4t$$

όπου ο t διατρέχει τους ακεραίους.

52. Υπολογίζουμε πρώτα το μέγιστο κοινό διαιρέτη των 123 και 360.

$$\begin{aligned} 360 &= 123 \cdot 2 + 114 \\ 123 &= 114 \cdot 1 + 9 \\ 114 &= 9 \cdot 12 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 \end{aligned}$$

'ρα $(123, 360) = 3$. Αφού $3 \mid 99$, η εξίσωση έχει ακέραιες λύσεις. Βρίσκουμε μια λύση της εξίσωσης.

$$\begin{aligned} 3 &= 9 - 6 = 9 - (114 - 9 \cdot 12) = 9 \cdot 13 - 114 = (123 - 114) \cdot 13 - 114 \\ &= 123 \cdot 13 - 114 \cdot 14 = 123 \cdot 13 - (360 - 123 \cdot 2) \cdot 14 \\ &= 123 \cdot 41 + 360(-14). \end{aligned}$$

Πολλαπλασιάζοντας επί 99/3=33 παίρνουμε

$$123 \cdot 1353 + 360 \cdot (-462) = 99.$$

Δηλαδή μια λύση της εξίσωσης είναι οι $x_0 = 1353$ και $y_0 = -462$. Έχουμε $r_1 = 123/3 = 41$ και $r_2 = 360/3 = 120$. Άρα οι λύσεις της εξίσωσης είναι τα ζευγάρια

$$x = 1353 + 120t \text{ και } y = -462 - 41t$$

όπου ο t διατρέχει τους ακεραίους. Για να βρούμε τις θετικές ακέραιες λύσεις της $123x + 360y = 99$, λύνουμε το σύστημα

$$\begin{aligned} 1353 + 120t &> 0 \\ -462 - 41t &> 0 \end{aligned}$$

ως προς $t \in \mathbb{Z}$. Ζητάμε $t > -1353/120 \Rightarrow t \geq -11$ και $t < -462/41 \Rightarrow t \leq -12$, άρα δεν υπάρχει θετική λύση της εξίσωσης.

53. Ο μέγιστος κοινός διαιρέτης των 2 και 7 ισούται με 1, άρα η εξίσωση έχει ακέραιες λύσεις. Για να βρούμε μια λύση της εξίσωσης, γράφουμε $1 = 2 \cdot (-3) + 7 \cdot 1$ και πολλαπλασιάζοντας επί 53 παίρνουμε

$$2 \cdot (-159) + 7 \cdot 53 = 53.$$

Δηλαδή, μια λύση της εξίσωσης είναι οι $x_0 = -159$ και $y_0 = 53$. Άρα οι λύσεις της εξίσωσης είναι τα ζευγάρια

$$x = -159 + 7t \text{ και } y = 53 - 2t$$

όπου ο t διατρέχει τους ακεραίους. Για να βρούμε τις μη αρνητικές ακέραιες λύσεις της $2x + 7y = 53$, λύνουμε το σύστημα

$$\begin{aligned} -159 + 7t &\geq 0 \\ 53 - 2t &\geq 0 \end{aligned}$$

ως προς $t \in \mathbb{Z}$. Ζητάμε $t \geq 159/7 \Rightarrow t \geq 23$ και $t \leq 53/2 \Rightarrow t \leq 26$, άρα υπάρχουν τέσσερις μη αρνητικές λύσεις της εξίσωσης:

$$\begin{aligned} x = 23 &\quad , \quad y = 1 \\ x = 16 &\quad , \quad y = 3 \\ x = 9 &\quad , \quad y = 5 \\ x = 2 &\quad , \quad y = 7. \end{aligned}$$

54. Ο μέγιστος κοινός διαιρέτης των 28 και 35 είναι ο 7, ο οποίος δεν διαιρεί τον 136. Άρα η εξίσωση δεν έχει ακέραιες λύσεις.

55. Θεωρούμε την εξίσωση $ax + bw = c$. Αφού $(a, b) = 1$, η εξίσωση έχει ακέραιες λύσεις. Επίσης, αν x, w είναι μια λύση της $ax + bw = c$, τότε οι $x, y = -w$ είναι λύση της $ax - by = c$.

Έστω x_0, w_0 μια λύση της $ax + bw = c$. Τότε, οι λύσεις αυτής της εξίσωσης είναι της μορφής $x = x_0 + bt$ και $w = w_0 - at$, όπου ο t διατρέχει τους ακεραίους. Θέτουμε $y_0 = -w_0$. Τότε οι x_0, y_0 είναι λύση της $ax - by = c$, και για κάθε $t \in \mathbb{Z}$, οι $x = x_0 + bt$

και $y = -(w_0 - at) = y_0 + at$ δίνουν όλες τις λύσεις της $ax - by = c$. Παρατηρούμε ότι $a, b > 0$, άρα υπάρχει $t_0 \in \mathbb{N}$ τέτοιος ώστε: για κάθε $t \geq t_0$ να έχουμε $x_0 + bt > 0$ και $y_0 + at > 0$ (από την Αρχιμήδεια ιδιότητα: ο t_0 θα εξαρτάται από τους x_0 και y_0). Άρα, η $ax - by = c$ έχει άπειρες το πλήθος θετικές ακέραιες λύσεις: τις $x = x_0 + bt$, $y = y_0 + at$ για $t = t_0, t_0 + 1, \ldots$.

56. Υποθέτουμε ότι υπάρχουν $x, y \in \mathbb{N}$ τέτοιοι ώστε $y^n = 2x^n$. Αν $d = (x, y)$, τότε υπάρχουν $r, s \in \mathbb{N}$ με $x = rd$, $y = sd$ και $(r, s) = 1$. Αντικαθιστώντας στην $y^n = 2x^n$ έχουμε $s^n = 2r^n$ και $(r, s) = 1$. Τότε, $r^n \mid s^n$, απ' όπου παίρνουμε $r \mid s$. Αφού $(r, s) = 1$, αναγκαστικά $r = 1$ και $s^n = 2$. Ειδικότερα $2 \mid s^n \Rightarrow 2 \mid s$. Όμως τότε, $s \geq 2$ άρα $s^n > 2$ αφού $n \geq 2$. Καταλήξαμε σε άτοπο, άρα η $y^n = 2x^n$ δεν έχει λύση στους φυσικούς αριθμούς.

57. (α) Έστω $y = 2a + 1$. Έχουμε $y = (a + 1)^2 - a^2$ με $(a + 1, a) = 1$ και συνεπώς η τριάδα (x, y, z) με $x = 2a(a + 1)$ και $z = a^2 + (a + 1)^2$ είναι πρωταρχική πυθαγόρεια τριάδα, σύμφωνα με το Θεώρημα 1.8.2.

(β) Προκύπτει αμέσως από το (α).

58. Υποθέτουμε ότι το Πυθαγόρειο τρίγωνο αντιστοιχεί σε κάποια τριάδα x, y, z. Τότε υπάρχουν d και $m > s$ με $(m, s) = 1$, ο ένας άρτιος και ο άλλος περιττός, τέτοιοι ώστε $x = 2msd$, $y = (m^2 - s^2)d$, $z = (m^2 + s^2)d$ και $d = (x, y, z)$. Αφού το εμβαδόν του τριγώνου ισούται με την περίμετρό του, έχουμε

$$xy = 2(x + y + z) \Longrightarrow 2ms(m^2 - s^2)d^2 = 4m(m + s)d,$$

άρα

$$ds(m - s) = 2.$$

Αφού ο $m - s$ είναι περιττός και διαιρεί τον 2, έχουμε $m - s = 1$. Επίσης, $s = 1$ ή $s = 2$. Για $s = 2$ παίρνουμε $d = 1$ και $m = 3$, δηλαδή την τριάδα $x = 12$, $y = 5$ και $z = 13$. Για $s = 1$ παίρνουμε $m = 2$ και $d = 2$, δηλαδή την τριάδα $x = 8$, $y = 6$, $z = 10$.

59. Αν x, y, z είναι οι ζητούμενες πλευρές του τριγώνου και n η ακτίνα του εγγεγραμμένου κύκλου, πρέπει να ισχύει η

$$(*) \qquad 2n = x + y - z.$$

Πράγματι, υπάρχουν d και $m > s$ με $(m, s) = 1$, ο ένας άρτιος και ο άλλος περιττός, τέτοιοι ώστε $x = 2msd$, $y = (m^2 - s^2)d$, $z = (m^2 + s^2)d$ και $d = (x, y, z)$. Τότε

$$x + y - z = (2ms + m^2 - s^2 - m^2 - s^2)d = (2ms - 2s^2)d = 2s(m - s)d.$$

Από την άλλη πλευρά, είδαμε ότι η ακτίνα του εγγεγραμμένου κύκλου ισούται με $s(m - s)d$, κι αυτό αποδεικνύει την $(*)$.

Ζητάμε λοιπόν μια Πυθαγόρεια τριάδα με $x + y - z = 2n$. Δοκιμάστε τους $y = 2n + 1$, $x = 2n^2 + 2n$ και $z = 2n^2 + 2n + 1$:

$$(2n^2 + 2n + 1)^2 = (2n^2 + 2n)^2 + 2(2n^2 + 2n) + 1 = (2n^2 + 2n)^2 + (2n + 1)^2$$

και

$$2n + 1 + 2n^2 + 2n - (2n^2 + 2n + 1) = 2n.$$

60. Καθένας από τους 52 ακεραίους αφήνει υπόλοιπο 0, 50 ή $\pm 1, \pm 2, \ldots, \pm 49$ διαιρούμενος με το 100. Αν δύο ακέραιοι, έστω οι x και y, αφήνουν το ίδιο υπόλοιπο τότε $100 \mid x - y$. Αν όχι τότε τουλάχιστον 50 από τους 52 ακεραίους αφήνουν υπόλοιπα ± 1, $\pm 2, \ldots, \pm 49$, όλα ανά δύο διαφορετικά μεταξύ τους, άρα δύο από αυτούς, έστω οι z και w, αφήνουν υπόλοιπα i και $-i$ για κάποιο $i \in \{1, 2, \ldots, 49\}$. Τότε $100 \mid z + w$.

61. (α) Έστω $n_1, n_2, \ldots, n_{101}$ οι δοσμένοι ακέραιοι. Γράφουμε $n_i = 2^{r_i} q_i$ με $r_i \in \mathbb{Z}^+$ και $q_i \in \mathbb{N}$ περιττό (δες επίσης Άσκηση 49) για κάθε i. Εφόσον $1 \leq n_i \leq 200$ οι $q_1, q_2, \ldots, q_{101}$ ανήκουν στο σύνολο $\{1, 3, \ldots, 199\}$ άρα παίρνουν 100 δυνατές διαφορετικές τιμές. Συνεπώς έχουμε υποχρεωτικά $q_i = q_j$ για κάποια $i \neq j$. Τότε $n_i = 2^{r_i} q$ και $n_j = 2^{r_j} q$ με $q_i = q_j = q$ και $n_i \mid n_j$ αν $r_i \leq r_j$ ενώ $n_j \mid n_i$ αν $r_j \leq r_i$.

(β) Οι ακέραιοι $101, 102, \ldots, 200$ έχουν αυτή την ιδιότητα.

62. Αν a_n είναι το άθροισμα αυτό τότε $a_2 = 1/2$ και συνεπώς αρκεί να δείξουμε ότι $a_{n-1} = a_n$ για κάθε $n \geq 3$. Παρατητούμε ότι το a_n προκύπτει από το a_{n-1} προσθέτοντας τα κλάσματα της μορφής $\frac{1}{p \cdot q}$ με $1 \leq p, q \leq n$, $(p, q) = 1$ και $p = n$ ή $q = n$ και αφαιρώντας αυτά της μορφής $\frac{1}{p \cdot q}$ με $1 \leq p, q \leq n$, $(p, q) = 1$ και $p + q = n$. Όμως για $p + q = n$ έχουμε

$$\frac{1}{p \cdot n} + \frac{1}{q \cdot n} = \frac{p + q}{p \cdot q \cdot n} = \frac{1}{p \cdot q}$$

και οι συνθήκες $(p, n) = 1$, $(q, n) = 1$ και $(p, q) = 1$ είναι ανά δύο ισοδύναμες. Συμπεραίνουμε ότι $a_n - a_{n-1} = 0$ για $n \geq 3$.

Κεφάλαιο 2

Ισοτιμίες

2.1 Εισαγωγή

Ορισμός 2.1.1. Έστω $m \in \mathbb{N}$. Αν $a, b \in \mathbb{Z}$, θα λέμε ότι ο a είναι *ισότιμος* (ή *ισοδύναμος* ή *ισοϋπόλοιπος*) με τον b ως προς m και θα γράφουμε $a \equiv b \pmod{m}$ αν $m \mid (a-b)$.

Παράδειγμα 2.1.2. Θέτουμε $m = 7$. Ελέγξτε ότι

$$3 \equiv 24 \pmod{7},\ -31 \equiv 11 \pmod{7},\ -15 \equiv -64 \pmod{7}.$$

Η ισοτιμία (mod m) είναι σχέση ισοδυναμίας, όπως δείχνει η επόμενη απλή πρόταση.

Πρόταση 2.1.3. *Έστω $m \in \mathbb{N}$ και $a, b, c \in \mathbb{Z}$.*

(i) $a \equiv a \pmod{m}$.

(ii) Αν $a \equiv b \pmod{m}$, *τότε* $b \equiv a \pmod{m}$.

(iii) Αν $a \equiv b \pmod{m}$ *και* $b \equiv c \pmod{m}$, *τότε* $a \equiv c \pmod{m}$.

Θυμηθείτε ότι αν $m \in \mathbb{N}$ και $a \in \mathbb{Z}$, τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ τέτοιοι ώστε $a = mq + r$ και $0 \leq r < m$. Από τον ορισμό που δώσαμε, οι a και r είναι ισότιμοι ως προς m. Λέμε ότι ο r είναι το *ελάχιστο υπόλοιπο του a ως προς m* και ότι ο a *ανήκει στην κλάση του r ως προς m* (ο a ανήκει στην κλάση $r \pmod{m}$). Υπάρχουν λοιπόν m κλάσεις mod m, οι $r \pmod{m}$, $r = 0, 1, \ldots, m-1$.

Πρόταση 2.1.4. *Έστω $m \in \mathbb{N}$ και έστω $a, b \in \mathbb{Z}$. Τότε, $a \equiv b \pmod{m}$ αν και μόνο αν οι a και b ανήκουν στην ίδια κλάση υπολοίπων ως προς m.*

Απόδειξη. Υποθέτουμε πρώτα ότι $a \equiv b \pmod{m}$ και ότι ο a ανήκει στην κλάση $r \pmod{m}$ για κάποιον $0 \leq r < m$. Αυτό σημαίνει ότι $a = mq + r$ για κάποιον $q \in \mathbb{Z}$. Από την άλλη πλευρά, αφού $a \equiv b \pmod{m}$, έχουμε $m \mid (a-b)$ δηλαδή υπάρχει $s \in \mathbb{Z}$ τέτοιος ώστε $b = a + ms$. Έπεται ότι $b = a + ms = m(q+s) + r$, δηλαδή ο b ανήκει κι αυτός στην κλάση $r \pmod{m}$.

Αντίστροφα, αν υποθέσουμε ότι οι a και b ανήκουν στην ίδια κλάση $r \pmod{m}$, τότε υπάρχουν $q, s \in \mathbb{Z}$ τέτοιοι ώστε $a = mq + r$ και $b = ms + r$. Όμως τότε $a - b = m(q-s)$, δηλαδή $m \mid (a-b)$. Άρα $a \equiv b \pmod{m}$. □

Με άλλα λόγια, κάθε φυσικός m ορίζει μια σχέση ισοδυναμίας στο $\mathbb{Z}$, την

$$a \sim b \Longleftrightarrow a \equiv b \pmod{m},$$

οι δε κλάσεις ισοδυναμίας είναι ακριβώς οι κλάσεις $r \pmod{m}$ που αποτελούνται από όλους τους ακεραίους που η διαίρεση τους με m αφήνει υπόλοιπο r, για $r = 0, 1, \ldots, m-1$.

Οι επόμενες δύο προτάσεις δίνουν βασικές ιδιότητες των ισοτιμιών, τις οποίες θα χρησιμοποιούμε συχνά στη συνέχεια.

Πρόταση 2.1.5. *Έστω $m \in \mathbb{N}$ και έστω $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Αν $a_1 \equiv b_1 \pmod{m}$ και $a_2 \equiv b_2 \pmod{m}$, τότε*

(i) $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

(ii) $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(iii) $a_1^k \equiv b_1^k \pmod{m}$ *για κάθε* $k \in \mathbb{N}$.

Απόδειξη. *(i)* Από την υπόθεση έχουμε $m \mid (a_1 - b_1)$ και $m \mid (a_2 - b_2)$, άρα $m \mid (a_1 - b_1) + (a_2 - b_2)$, δηλαδή $m \mid (a_1 + a_2) - (b_1 + b_2)$.

(ii) Έχουμε $a_1 a_2 - b_1 b_2 = (a_1 - b_1)a_2 + b_1(a_2 - b_2)$. Αν λοιπόν $m \mid (a_1 - b_1)$ και $m \mid (a_2 - b_2)$, τότε $m \mid (a_1 a_2 - b_1 b_2)$.

(iii) Προκύπτει εύκολα από το (ii) με επαγωγή. □

Πρόταση 2.1.6. *Έστω $m \in \mathbb{N}$ και $a, b, c \in \mathbb{Z}$ με $c \neq 0$.*

(i) Αν $ac \equiv bc \pmod{m}$, τότε $a \equiv b \pmod{m/(c,m)}$.

(ii) Αν $ac \equiv bc \pmod{m}$ και $(c, m) = 1$, τότε $a \equiv b \pmod{m}$.

Απόδειξη. *(i)* Έστω $d = (c, m)$. Έχουμε $m \mid c(a-b)$, άρα $\frac{m}{d} \mid \frac{c}{d} \cdot (a-b)$. Όμως $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$ από το Λήμμα 1.4.1, και συνεπώς $\frac{m}{d} \mid a - b$ από το Λήμμα 1.4.2, δηλαδή $a \equiv b \pmod{m/(c,m)}$.

(ii) Άμεση συνέπεια του (i). □

2.2 Συστήματα υπολοίπων και το μικρό θεώρημα του Fermat

Έστω $m \in \mathbb{N}$. Το σύνολο $M = \{0, 1, \ldots, m-1\}$ καλείται *ελάχιστο πλήρες σύστημα υπολοίπων ως προς m*. Ο όρος «πλήρες σύστημα» εξηγείται από το γεγονός ότι κάθε ακέραιος a είναι ισότιμος με ακριβώς ένα στοιχείο του M ως προς m. Πιο γενικά, ένα σύνολο S ακεραίων λέγεται *πλήρες σύστημα υπολοίπων ως προς m* αν για κάθε ακέραιο a υπάρχει μοναδικό $x \in S$ με την ιδιότητα $x \equiv a \pmod{m}$). Για παράδειγμα, το σύνολο $S = \{2, 4, 6\}$ είναι ένα πλήρες σύστημα υπολοίπων ως προς 3.

Λήμμα 2.2.1. *Ένα σύνολο S ακεραίων είναι πλήρες σύστημα υπολοίπων ως προς m αν και μόνο αν το S έχει m στοιχεία και $x \not\equiv y \pmod{m}$ αν $x \neq y$ στο S.*

Απόδειξη. Έστω ότι το S ακεραίων είναι πλήρες σύστημα υπολοίπων ως προς m. Για κάθε $i \in M$ υπάρχει στοιχείο $x_i \in S$ τέτοιο ώστε $x_i \equiv i \pmod m$. Έχουμε $\{x_0, x_1, \ldots, x_{m-1}\} \subseteq S$ και για $i \neq j$ στο M ισχύει $i \not\equiv j \pmod m$ και συνεπώς $x_i \not\equiv x_j \pmod m$. Μένει να δείξουμε ότι το S έχει το πολύ m στοιχεία, αφού από αυτό έπεται ότι $S = \{x_0, x_1, \ldots, x_{m-1}\}$. Πράγματι, αν το S είχε περισσότερα από m στοιχεία τότε αναγκαστικά δύο από αυτά, έστω x και y, θα είχαν το ίδιο ελάχιστο υπόλοιπο διαιρούμενα με το m και συνεπώς $x \equiv y \pmod m$, σε αντίθεση με την υπόθεση.

Αντίστροφα έστω ότι $S = \{x_0, x_1, \ldots, x_{m-1}\}$ με $x_i \not\equiv x_j \pmod m$ για $i \neq j$ και έστω $a \in \mathbb{Z}$. Υπάρχει το πολύ ένας δείκτης i με $x_i \equiv a \pmod m$ διότι στην αντίθετη περίπτωση θα είχαμε $x_i \equiv a \pmod m$ και $x_j \equiv a \pmod m$ για διαφορετικούς δείκτες i και j και συνεπώς $x_i \equiv x_j \pmod m$, σε αντίθεση με την υπόθεση. Από την άλλη υπάρχει τουλάχιστον ένας τέτοιος δείκτης i. Πράγματι από τους $m+1$ ακεραίους $a, x_0, \ldots, x_{m-1}$ υπάρχουν αναγκαστικά δύο που αφήνουν το ίδιο ελάχιστο υπόλοιπο διαιρούμενοι με το m και συνεπώς είναι ισότιμοι ως προς m. Από την υπόθεση μας για το S ένας από αυτούς πρέπει να είναι ο a, οπότε $x_i \equiv a \pmod m$ για κάποιο i. □

Θεωρούμε το σύνολο $M^* = \{a \in M : (a, m) = 1\}$. Συμβολίζουμε με $\phi(m)$ το πλήθος των στοιχείων του M^*. Ένα σύνολο T ακεραίων καλείται *ανηγμένο σύστημα υπολοίπων ως προς* m αν όλα τα στοιχεία του T είναι σχετικώς πρώτα προς τον m και για κάθε ακέραιο a σχετικώς πρώτο προς τον m υπάρχει μοναδικό $x \in T$ με την ιδιότητα $x \equiv a \pmod m$. Για παράδειγμα, το σύνολο $S = \{1, 15\}$ είναι ένα ανηγμένο σύστημα υπολοίπων ως προς 4. Παρατηρήστε ότι $(x, m) = (y, m)$ αν $x \equiv y \pmod m$ και ότι το M^* είναι ανηγμένο σύστημα υπολοίπων ως προς m. Με αυτά ως δεδομένο η απόδειξη του επόμενου λήμματος είναι πανομοιότυπη με αυτή του Λήμματος 2.2.1 και παραλείπεται.

Λήμμα 2.2.2. *Ένα σύνολο T ακεραίων είναι ανηγμένο σύστημα υπολοίπων ως προς m αν και μόνο αν το T έχει $\phi(m)$ στοιχεία, όλα σχετικά πρώτα προς τον m, και $x \not\equiv y \pmod m$ αν $x \neq y$ στο T.*

Από το Λήμμα 2.2.2 έπεται ότι όλα τα ανηγμένα συστήματα υπολοίπων ως προς m έχουν το ίδιο πλήθος στοιχείων $\phi(m)$. Η συνάρτηση $\phi : \mathbb{N} \to \mathbb{N}$ καλείται *συνάρτηση του Euler*. Έτσι, για $m \in \mathbb{N}$ το $\phi(m)$ είναι το πλήθος των $a \in \{1, 2, \ldots, m\}$ με $(a, m) = 1$. Για παράδειγμα έχουμε $\phi(6) = 2$, $\phi(12) = 4$ και $\phi(p) = p - 1$ για κάθε πρώτο p. Γενικότερα ισχύει το ακόλουθο λήμμα.

Λήμμα 2.2.3. *Για κάθε πρώτο p και $r \in \mathbb{N}$ έχουμε $\phi(p^r) = p^{r-1}(p-1)$.*

Απόδειξη. Ένας τυχαών ακέραιος a δεν είναι σχετικώς πρώτος προς τον p^r αν και μόνο αν ο a είναι πολλαπλάσιο του p. Συνεπώς για $a \in \{1, 2, \ldots, p^r\}$ έχουμε $(a, p^r) = 1$ αν και μόνο αν ο a δεν είναι ένας από τους p^{r-1} ακεραίους $p \cdot k,\ k \in \{1, 2, \ldots, p^{r-1}\}$, οπότε $\phi(p^r) = p^r - p^{r-1}$. □

Πρόταση 2.2.4. *Έστω $m \in \mathbb{N}$ και $k \in \mathbb{Z} \setminus \{0\}$ με $(k, m) = 1$.*

(i) Όταν ο x διατρέχει ένα πλήρες σύστημα υπολοίπων ως προς m, ο kx διατρέχει κι αυτός ένα πλήρες σύστημα υπολοίπων ως προς m.

(ii) Όταν ο x διατρέχει ένα ανηγμένο σύστημα υπολοίπων ως προς m, ο kx διατρέχει κι αυτός ένα ανηγμένο σύστημα υπολοίπων ως προς m.

Απόδειξη. (*i*) Έστω S ένα πλήρες σύστημα υπολοίπων ως προς m. Προφανώς το kS έχει m στοιχεία, όσα και το S. Επίσης αν $x, y \in S$ και $kx \equiv ky \pmod{m}$, τότε από την υπόθεση $(k, m) = 1$ και την Πρόταση 2.1.6 έχουμε $x \equiv y \pmod{m}$, άρα $x = y$. Συμπεραίνουμε ότι το σύνολο $kS := \{kx : x \in S\}$ αποτελείται από m ακεραίους που ανά δύο είναι ανισότιμοι ως προς m και συνεπώς, από το Λήμμα 2.2.1, το kS είναι ένα πλήρες σύστημα υπολοίπων ως προς m.

(*ii*) Έστω T ένα ανηγμένο σύστημα υπολοίπων ως προς m. Όπως και στο (i) βλέπουμε ότι το kT έχει τόσα στοιχεία όσα και το T, δηλαδή $\phi(m)$, τα οποία είναι ανά δύο μη ισότιμα ως προς m. Επιπλέον, από την $(k, m) = 1$ έπεται ότι $(kx, m) = 1$ για κάθε $x \in T$, δηλαδή τα στοιχεία του kT είναι σχετικά πρώτα προς τον m. Άρα, από το Λήμμα 2.2.2, το kT είναι ένα ανηγμένο σύστημα υπολοίπων ως προς m. □

Πρόταση 2.2.5. *Έστω $m, n \in \mathbb{N}$ με $(m, n) = 1$.*

(i) Όταν ο x διατρέχει ένα πλήρες σύστημα υπολοίπων ως προς m και ο y διατρέχει ένα πλήρες σύστημα υπολοίπων ως προς n, ο $nx + my$ διατρέχει ένα πλήρες σύστημα υπολοίπων ως προς mn.

(ii) Όταν ο x διατρέχει ένα ανηγμένο σύστημα υπολοίπων ως προς m και ο y διατρέχει ένα ανηγμένο σύστημα υπολοίπων ως προς n, ο $nx + my$ διατρέχει ένα ανηγμένο σύστημα υπολοίπων ως προς mn.

Απόδειξη. (*i*) Έστω $S_1 = \{x_1, \ldots, x_m\}$ ένα πλήρες σύστημα υπολοίπων ως προς m και $S_2 = \{y_1, \ldots, y_n\}$ ένα πλήρες σύστημα υπολοίπων ως προς n. Αν $nx_i + my_j \equiv nx_r + my_s \pmod{mn})$, τότε $nx_i \equiv nx_r \pmod{m}$ (γιατί;). Αφού $(m, n) = 1$, έπεται ότι $x_i \equiv x_r \pmod{m}$, δηλαδή $x_i = x_r$. Όμοια βλέπουμε ότι $y_j = y_s$. Αυτό αποδεικνύει ότι το σύνολο $S = \{nx + my : x \in S_1, y \in S_2\}$ αποτελείται από mn ακεραίους οι οποίοι ανά δύο δεν είναι ισότιμοι ως προς mn. Άρα, από το Λήμμα 2.2.1, το S είναι ένα πλήρες σύστημα υπολοίπων ως προς mn.

(*ii*) Έστω $T_1 = \{x_1, \ldots, x_{\phi(m)}\}$ ένα ανηγμένο σύστημα υπολοίπων ως προς m, $T_2 = \{y_1, \ldots, y_{\phi(n)}\}$ ένα ανηγμένο σύστημα υπολοίπων ως προς n και έστω $T = \{nx+my : x \in T_1, y \in T_2\}$. Για $x \in T_1$ και $y \in T_2$ έχουμε

$$(nx + my, m) = (nx, m) = (x, m) = 1$$

και

$$(nx + my, n) = (my, n) = (y, n) = 1$$

διότι $(m, n) = 1$. Από τις δύο προηγούμενες σχέσεις και την $(m, n) = 1$ βλέπουμε ότι $(nx + my, mn) = 1$, δηλαδή τα στοιχεία του T είναι σχετικά πρώτα προς τον mn. Έστω τώρα τυχών ακέραιος a με $(a, mn) = 1$. Έχουμε $(a, m) = (a, n) = 1$ ενώ, από την Πρόταση 2.2.4 (ii), τα nT_1 και mT_2 είναι ανηγμένα συστήματα υπολοίπων ως προς m και n, αντίστοιχα. Συνεπώς υπάρχουν $x \in T_1$ και $y \in T_2$ με $a \equiv nx \pmod{m}$ και $a \equiv my \pmod{n}$. Προκύπτει ότι $a \equiv nx + my \pmod{mn}$ με $nx + my \in T$. Επιπλέον το $nx + my$ είναι το μοναδικό στοιχείο του T ισότιμο με το a ως προς mn διότι τα στοιχεία του T είναι ανά δύο ανισότιμα ως προς mn (η απόδειξη είναι ακριβώς στο πρώτο μέρος). Συνεπώς το T είναι ανηγμένο σύστημα υπολοίπων ως προς mn. □

Πόρισμα 2.2.6. *Αν $m, n \in \mathbb{N}$ και $(m, n) = 1$ τότε $\phi(mn) = \phi(m)\phi(n)$.*

Απόδειξη. Από την Πρόταση 2.2.5 (ii) προκύπτει ότι υπάρχει ανηγμένο σύστημα υπολοίπων ως προς mn με $\phi(m)\phi(n)$ στοιχεία και το ζητούμενο προκύπτει από το Λήμμα 2.2.2. □

Για παράδειγμα έχουμε $\phi(24) = \phi(3)\phi(8) = 2 \cdot 4 = 8$ και $\phi(pq) = (p-1)(q-1)$ για διακεκριμένους πρώτους p και q. Μια συνάρτηση ορισμένη στο $\mathbb{N}$ με την ιδιότητα του Πορίσματος 2.2.6 καλείται *πολλαπλασιαστική*. Θα μελετήσουμε εκτενέστερα τις πολλαπλασιαστικές συναρτήσεις στο επόμενο κεφάλαιο.

Θεώρημα 2.2.7. *Έστω $n \geq 2$ με κανονική αναπαράσταση την $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Τότε*

$$\phi(n) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right). \tag{2.2.1}$$

Απόδειξη. Η πρώτη ισότητα έπεται άμεσα από το Λήμμα 2.2.3, το Πόρισμα 2.2.6 και την παρατήρηση $(p_i^{k_i}, p_j^{k_j}) = 1$ για $i \neq j$. Για τη δεύτερη ισότητα παρατηρούμε ότι

$$\prod_{j=1}^{r} p_j^{k_j} \cdot \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{r} p_j^{k_j} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1). \tag{2.2.2}$$

□

Εφαρμογή της Πρότασης 2.2.4 είναι το Θεώρημα Fermat-Euler.

Θεώρημα 2.2.8. *Έστω $m \in \mathbb{N}$ και $a \in \mathbb{Z} \setminus \{0\}$ τέτοιος ώστε $(a, m) = 1$. Τότε*

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{2.2.3}$$

Απόδειξη. Έστω $T = \{x_1, \ldots, x_{\phi(m)}\}$ ένα ανηγμένο σύστημα υπολοίπων ως προς m. Από την Πρόταση 2.2.4 (ii), το σύνολο $aT = \{ax_1, \ldots, ax_{\phi(m)}\}$ είναι κι αυτό ένα ανηγμένο σύστημα υπολοίπων ως προς m. Από την Πρόταση 2.1.5 (ii) παίρνουμε

$$x_1 \cdots x_{\phi(m)} \equiv (ax_1) \cdots (ax_{\phi(m)}) = a^{\phi(m)} x_1 \cdots x_{\phi(m)} \pmod{m}. \tag{2.2.4}$$

Όμως $(x_i, m) = 1$ για κάθε $i = 1, \ldots, \phi(m)$, άρα $(x_1 \cdots x_{\phi(m)}, m) = 1$. Από την (2.2.4) και την Πρόταση 2.1.6 (ii) έπεται το ζητούμενο. □

Ειδική περίπτωση του Θεωρήματος 2.2.8 είναι το «μικρό θεώρημα του Fermat».

Θεώρημα 2.2.9. *Έστω p ένας πρώτος αριθμός και $a \in \mathbb{Z}$. Αν ο p δεν διαιρεί τον a τότε $a^{p-1} \equiv 1 \pmod{p}$.*

Απόδειξη. Αφού ο p είναι πρώτος και δεν διαιρεί τον a, έχουμε ότι $(a, p) = 1$ και $\phi(p) = p - 1$. Το ζητούμενο έπεται από το θεώρημα Fermat-Euler με $m = p$. □

2.3 Γραμμικές ισοτιμίες

Το γενικό πρόβλημα με το οποίο θα ασχοληθούμε σε αυτήν και την επόμενη παράγραφο είναι το εξής. Δίνονται ένα πολυώνυμο $f : \mathbb{Z} \to \mathbb{Z}$ με ακέραιους συντελεστές και ένας φυσικός αριθμός m. Μας ενδιαφέρει το πλήθος των λύσεων της ισοτιμίας $f(x) \equiv 0 \pmod{m}$: με αυτό εννοούμε το πλήθος των στοιχείων x ενός πλήρους συστήματος υπολοίπων ως προς m τα οποία ικανοποιούν την ισοτιμία.

Αυτό είναι και το ενδιαφέρον ερώτημα, γιατί αν x είναι ένας ακέραιος που ικανοποιεί την $f(x) \equiv 0 \pmod m$ και $y \equiv x \pmod m$, τότε $f(y) \equiv 0 \pmod m$. Πράγματι, αν $f(z) = c_k z^k + \cdots + c_1 z + c_0$ όπου $c_i \in \mathbb{Z}$ και $c_k \neq 0$, από την $y \equiv x \pmod m$ έχουμε

$$y^i \equiv x^i \pmod m, \text{ άρα } c_i y^i \equiv c_i x^i \pmod m \tag{2.3.1}$$

για κάθε $i = 0, 1, \ldots, k$ και προσθέτοντας τις ισοτιμίες παίρνουμε

$$f(y) \equiv f(x) \pmod m. \tag{2.3.2}$$

Μας ενδιαφέρει λοιπόν να δούμε πόσες λύσεις «μη ισότιμες ως προς m» υπάρχουν.

Σε αυτή την παράγραφο θα ξεκινήσουμε με τη μελέτη των γραμμικών ισοτιμιών (την περίπτωση που $f(z) = az - b$). Η πλήρης απάντηση στο πρόβλημα δίνεται από το επόμενο θεώρημα.

Θεώρημα 2.3.1. *Έστω $m \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Η ισοτιμία*

$$ax \equiv b \pmod m \tag{2.3.3}$$

έχει λύσεις αν και μόνο αν $(a, m) \mid b$. Τότε, το πλήθος των λύσεων ισούται με $d = (a, m)$ και όλες οι λύσεις ανήκουν στην ίδια κλάση υπολοίπων ως προς m/d.

Απόδειξη. Ο $x \in \mathbb{Z}$ ικανοποιεί την $ax \equiv b \pmod m$ αν και μόνο αν υπάρχει $y \in \mathbb{Z}$ τέτοιος ώστε $ax - b = my$, δηλαδή αν και μόνο αν η γραμμική διοφαντική εξίσωση $ax - my = b$ έχει ακέραιες λύσεις. Το Θεώρημα 1.7.1 δείχνει ότι αυτό συμβαίνει αν και μόνο αν $(a, m) \mid b$. Αυτό αποδεικνύει το πρώτο μέρος του θεωρήματος.

Έστω ότι $d = (a, m) \mid b$ και έστω x_1, x_2 δύο λύσεις της (2.3.3). Τότε $m \mid a(x_1 - x_2)$, απ' όπου έπεται ότι $\frac{m}{d} \mid \frac{a}{d}(x_1 - x_2)$. Αφού $(a/d, m/d) = 1$ (Λήμμα 1.4.1), αυτό σημαίνει ότι $(m/d) \mid x_1 - x_2$. Δηλαδή όλες οι λύσεις της (2.3.3) ανήκουν στην ίδια κλάση υπολοίπων ως προς m/d.

Μένει να δείξουμε ότι το πλήθος των λύσεων της ισοτιμίας ισούται με d. Σταθεροποιούμε μία λύση x_0 και θεωρούμε τους ακεραίους

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}. \tag{2.3.4}$$

Για κάθε $0 \leq s \leq d - 1$ έχουμε

$$a\left(x_0 + \frac{ms}{d}\right) = ax_0 + \frac{as}{d} \cdot m \equiv ax_0 \equiv b \pmod m, \tag{2.3.5}$$

δηλαδή όλοι αυτοί οι ακέραιοι ικανοποιούν την (2.3.3). Θα δείξουμε ότι ανήκουν σε διαφορετικές κλάσεις υπολοίπων ως προς m. Αν για κάποιους $0 \leq s_1, s_2 \leq d - 1$ ισχύει

$$x_0 + \frac{m}{d} s_1 \equiv x_0 + \frac{m}{d} s_2 \pmod m \tag{2.3.6}$$

τότε $m \mid \frac{m}{d}(s_1 - s_2)$, δηλαδή $d \mid (s_1 - s_2)$, το οποίο μπορεί να συμβεί μόνο αν $s_1 = s_2$ αφού $|s_1 - s_2| < d$.

Βρήκαμε d το πλήθος λύσεις ανισότιμες ως προς m, άρα η (2.3.3) έχει τουλάχιστον d λύσεις. Θα δείξουμε ότι κάθε άλλη λύση είναι ισότιμη με κάποια από αυτές ως προς m, το οποίο θα ολοκληρώσει την απόδειξη. Όπως είδαμε, κάθε άλλη λύση είναι της μορφής $x_0 + \frac{m}{d} r$ για κάποιον $r \in \mathbb{Z}$. Από τον αλγόριθμο της διαίρεσης, υπάρχουν μοναδικοί $q \in \mathbb{Z}$ και $0 \leq s < d$ τέτοιοι ώστε $r = qd + s$. Τότε,

$$x_0 + \frac{m}{d} r = x_0 + \frac{m}{d}(qd + s) = x_0 + \frac{sm}{d} + mq \equiv x_0 + \frac{sm}{d} \pmod m, \tag{2.3.7}$$

δηλαδή ανήκει στην ίδια κλάση υπολοίπων ως προς m με κάποια από τις d λύσεις στην (2.3.4). □

Παραδείγματα 2.3.2. Η απόδειξη του προηγούμενου θεωρήματος δίνει ταυτόχρονα έναν αλγόριθμο υπολογισμού των λύσεων. Θα τον εφαρμόσουμε σε δύο παραδείγματα.

(α) Να λυθεί η γραμμική ισοτιμία $5x \equiv 2 \pmod{26}$.

Παρατηρούμε ότι $d = (5, 26) = 1$. Άρα η ισοτιμία έχει ακριβώς μία λύση. Για να τη βρούμε, αρκεί να λύσουμε τη γραμμική διοφαντική εξίσωση $5x - 26y = 2$. Γράφουμε $1 = 5 \cdot (-5) - 26 \cdot (-1)$ και πολλαπλασιάζοντας επί 2 παίρνουμε $5 \cdot (-10) - 26 \cdot (-2) = 2$, δηλαδή $5 \cdot (-10) \equiv 2 \pmod{26}$. Η μοναδική λύση είναι η $-10 \pmod{26}$ ή, αλλιώς, η $16 \pmod{26}$.

(β) Να λυθεί η γραμμική ισοτιμία $6x \equiv 15 \pmod{21}$.

Παρατηρούμε ότι $d = (6, 21) = 3 \mid 15$. Άρα η ισοτιμία έχει ακριβώς τρείς λύσεις. Για να βρούμε μία από αυτές, αρκεί να λύσουμε τη γραμμική διοφαντική εξίσωση $6x - 21y = 15$. Γράφουμε $3 = 6 \cdot (-3) - 21 \cdot (-1)$ και πολλαπλασιάζοντας επί 5 παίρνουμε $6 \cdot (-15) - 21 \cdot (-5) = 15$, δηλαδή $6 \cdot (-15) \equiv 15 \pmod{21}$. Άρα μία λύση είναι η $-15 \pmod{21}$, ή αλλιώς, η $6 \pmod{21}$. Έχουμε $m/d = 21/3 = 7$, άρα οι τρείς λύσεις της ισοτιμίας είναι οι

$$6 \pmod{21},\ 13 \pmod{21},\ 20 \pmod{21}.$$

Το επόμενο αποτέλεσμα, το *Κινέζικο θεώρημα υπολοίπων*, μας δίνει μέθοδο υπολογισμού κοινής λύσης ενός συστήματος γραμμικών ισοτιμιών. Η χρησιμότητά του γίνεται κατανοητή από την εξής πρόταση.

Πρόταση 2.3.3. *Έστω $f : \mathbb{Z} \to \mathbb{Z}$ πολυώνυμο με ακέραιους συντελεστές και έστω $m_1, m_2, \ldots, m_r$ φυσικοί αριθμοί, σχετικά πρώτοι ανά δύο. Αν $m = m_1 m_2 \cdots m_r$, τότε κάθε λύση της*

$$f(x) \equiv 0 \pmod{m}$$

είναι λύση του συστήματος

$$\begin{aligned} f(x) &\equiv 0 \pmod{m_1}, \\ f(x) &\equiv 0 \pmod{m_2}, \\ &\vdots \\ f(x) &\equiv 0 \pmod{m_r} \end{aligned}$$

και αντιστρόφως.

Απόδειξη. Αν $f(x) \equiv 0 \pmod{m}$, έχουμε $m \mid f(x)$. Όμως, $m_i \mid m$ για κάθε $i = 1, \ldots, r$, άρα $m_i \mid f(x)$. Έπεται ότι $f(x) \equiv 0 \pmod{m_i}$ για κάθε $i = 1, \ldots, r$.

Αντίστροφα, αν ο x είναι λύση του συστήματος $f(x) \equiv 0 \pmod{m_i}$, τότε $m_i \mid f(x)$ για κάθε $i = 1, \ldots, r$. Αφού οι m_i είναι ανά δύο σχετικά πρώτοι, το γινόμενο $m = m_1 m_2 \cdots m_r$ διαιρεί κι αυτό τον $f(x)$. Άρα $f(x) \equiv 0 \pmod{m}$. □

Σύμφωνα με την Πρόταση 2.3.3, αν $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, προκειμένου να λύσουμε την $f(x) \equiv 0 \pmod{m}$ αρκεί να βρούμε όλες τις λύσεις των $f(x) \equiv 0 \pmod{p_i^{k_i}}$ και,

κατόπιν, για κάθε r-άδα $(c_1, \ldots, c_r)$ λύσεων αυτών των r ισοτιμιών να βρούμε κλάση $x \pmod m$ η οποία να ικανοποιεί το σύστημα

$$\begin{aligned} x &\equiv c_1 \pmod{p_1^{k_1}}, \\ x &\equiv c_2 \pmod{p_2^{k_2}}, \\ &\vdots \quad \equiv \quad \vdots \\ x &\equiv c_r \pmod{p_r^{k_r}}. \end{aligned}$$

Τότε, η κλάση $x \pmod m$ θα ικανοποιεί ταυτόχρονα τις $f(x) \equiv 0 \pmod{p_i^{k_i}}$, και από την Πρόταση 2.3.3 θα είναι λύση της $f(x) \equiv 0 \pmod m$.

Το Κινέζικο θεώρημα υπολοίπων εξασφαλίζει ότι κάθε σύστημα γραμμικών ισοτιμιών όπως παραπάνω έχει μοναδική λύση.

Θεώρημα 2.3.4. *Έστω $m_1, m_2, \ldots, m_r$ φυσικοί αριθμοί με $(m_i, m_j) = 1$ αν $i \neq j$. Αν $m = m_1 m_2 \cdots m_r$, τότε για κάθε $c_1, \ldots, c_r \in \mathbb{Z}$ το σύστημα*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1}, \\ x &\equiv c_2 \pmod{m_2}, \\ &\vdots \quad \equiv \quad \vdots \\ x &\equiv c_r \pmod{m_r} \end{aligned}$$

έχει μοναδική λύση $x \pmod m$.

Απόδειξη. Για κάθε $i = 1, \ldots, r$ ορίζουμε $M_i = m/m_i$. Τότε

(i) αν $j \neq i$ έχουμε $m_j \mid M_i$,

(ii) $(M_i, m_i) = 1$ για κάθε i.

Λόγω της δεύτερης ιδιότητας, η γραμμική ισοτιμία

$$M_i y \equiv 1 \pmod{m_i} \tag{2.3.8}$$

έχει μοναδική λύση, την $b_i \pmod{m_i}$. Ορίζουμε

$$x = c_1 M_1 b_1 + \cdots + c_r M_r b_r. \tag{2.3.9}$$

Για κάθε $i = 1, \ldots, r$ έχουμε

$$c_i M_i b_i \equiv c_i \pmod{m_i} \tag{2.3.10}$$

λόγω της $M_i b_i \equiv 1 \pmod{m_i}$, και

$$c_j M_j b_j \equiv 0 \pmod{m_i} \tag{2.3.11}$$

αν $j \neq i$, λόγω της $m_j \mid M_j$. Προσθέτοντας παίρνουμε

$$x = c_1 M_1 b_1 + \cdots + c_r M_r b_r \equiv c_i \pmod{m_i} \tag{2.3.12}$$

για κάθε $i = 1, \ldots, r$. Δηλαδή, ο x είναι λύση του συστήματος. Αν y είναι μια άλλη λύση τότε $m_i \mid (x - y)$ για κάθε i, και αφού οι m_i είναι ανά δύο σχετικά πρώτοι συμπεραίνουμε ότι $m = m_1 m_2 \cdots m_r \mid (x - y)$. Άρα η λύση x είναι μοναδική modulo m: $x \equiv y \pmod m$. □

2.4 Πολυωνυμικές ισοτιμίες

Υποθέτουμε ότι $f(x) = c_n x^n + \cdots + c_1 x + c_0$ είναι ένα πολυώνυμο βαθμού $n \geq 2$ με ακέραιους συντελεστές c_i ($c_n \neq 0$). Έστω $m = p_1^{k_1} \cdots p_r^{k_r}$ ένας φυσικός μεγαλύτερος ή ίσος του 2. Από την Πρόταση 2.3.3, για να λύσουμε την ισοτιμία $f(x) \equiv 0 \pmod{m}$ αρκεί να λύσουμε τις

$$f(x) \equiv 0 \pmod{p_i^{k_i}},\ i = 1, \ldots, r. \tag{2.4.1}$$

Το Θεώρημα που ακολουθεί δίνει έναν αλγόριθμο με τον οποίο μπορούμε να αναχθούμε από το πρόβλημα της επίλυσης της $f(x) \equiv 0 \pmod{p^k}$ στο απλούστερο πρόβλημα της επίλυσης της $f(x) \equiv 0 \pmod{p}$.

Θα χρειαστούμε ένα απλό λήμμα.

Λήμμα 2.4.1. *Έστω $f(x) = c_n x^n + \cdots + c_1 x + c_0$ ένα πολυώνυμο βαθμού $n \geq 2$ με ακέραιους συντελεστές c_i ($c_n \neq 0$). Για κάθε $a, b \in \mathbb{Z}$ έχουμε*

$$f(a+b) = f(a) + bf'(a) + b^2 s, \tag{2.4.2}$$

όπου $s \in \mathbb{Z}$ και $f'(a)$ είναι η παράγωγος της f στο a.

Απόδειξη. Έστω $g(x) = f(a+x)$. Το $g(x)$ είναι πολυώνυμο στο x με ακεραίους συντελεστές και συνεπώς

$$g(x) = g(0) + g'(0)x + x^2 h(x) \tag{2.4.3}$$

για κάποιο πολυώνυμο $h(x)$ με ακεραίους συντελεστές. Προφανώς έχουμε $g(b) = f(a+b)$, $g(0) = f(a)$ και $g'(0) = f'(a)$ οπότε για $x = b$ η (2.4.3) δίνει τη (2.4.2) με $s = h(b) \in \mathbb{Z}$. □

Θεώρημα 2.4.2. *Έστω $f(x) = c_n x^n + \cdots + c_1 x + c_0$ ένα πολυώνυμο βαθμού $n \geq 2$ με ακέραιους συντελεστές c_i ($c_n \neq 0$), και έστω p πρώτος αριθμός και $k \geq 2$. Τότε η κλάση $x \pmod{p^k}$ είναι λύση της $f(x) \equiv 0 \pmod{p^k}$ αν και μόνο αν $x = z + yp^{k-1}$ για κάποιους ακεραίους $0 \leq z < p^{k-1}$ και $0 \leq y < p$ οι οποίοι ικανοποιούν τις*

$$f(z) \equiv 0 \pmod{p^{k-1}} \tag{2.4.4}$$

και

$$\frac{f(z)}{p^{k-1}} + yf'(z) \equiv 0 \pmod{p}. \tag{2.4.5}$$

Απόδειξη. Έστω ακέραιος x με $0 \leq x < p^k$. Από τον αλγόριθμο της διαίρεσης υπάρχουν μοναδικοί ακέραιοι y και z τέτοιοι ώστε $x = yp^{k-1} + z$ και $0 \leq z < p^{k-1}$. Παρατηρήστε ότι αναγκαστικά ισχύει $0 \leq y < p$ (γιατί;). Από το Λήμμα 2.4.1 υπάρχει $s \in \mathbb{Z}$ τέτοιος ώστε

$$f(x) = f(z + yp^{k-1}) = f(z) + yp^{k-1} f'(z) + (yp^{k-1})^2 s. \tag{2.4.6}$$

Όμως $p^k \mid p^{2k-2}$ (αφού $2k - 2 \geq k$) και συνεπώς η ισοτιμία $f(x) \equiv 0 \pmod{p^k}$ είναι ισοδύναμη με την

$$f(z) + yp^{k-1} f'(z) \equiv 0 \pmod{p^k}. \tag{2.4.7}$$

Εφόσον $p^{k-1} \mid p^k$ από την (2.4.6) προκύπτει ότι $p^{k-1} \mid f(z)$, δηλαδή η (2.4.4), και συνεπώς και η (2.4.5), διαιρώντας τη (2.4.6) με p^{k-1}. Αντίστροφα αν ισχύουν οι (2.4.4) και (2.4.5) τότε

$$f(z) + yp^{k-1} f'(z) = p^{k-1},\ \left(\frac{f(z)}{p^{k-1}} + yf'(z)\right) \equiv 0 \pmod{p^k}, \tag{2.4.8}$$

επομένως ισχύει η (2.4.6), άρα και η $f(x) \equiv 0 \pmod{p^k}$. □

Ας υποθέσουμε ότι μας δίνεται μια ισοτιμία της μορφής $f(x) \equiv 0 \pmod{p^k}$, όπου $k \geq 2$. Με διαδοχικές εφαρμογές του Θεωρήματος 2.4.2 μπορούμε να αναχθούμε στην επίλυση της ισοτιμίας $f(x) \equiv 0 \pmod{p}$ και κάποιων γραμμικών ισοτιμιών (παραδείγματα θα δοθούν στις ασκήσεις). Περνάμε λοιπόν φυσιολογικά στο πρόβλημα της επίλυσης ισοτιμιών της μορφής $f(x) \equiv 0 \pmod{p}$, όπου p είναι ένας πρώτος αριθμός. Το πρώτο μας αποτέλεσμα δείχνει ότι μπορούμε πάντα να υποθέτουμε ότι ο βαθμός του f είναι μικρότερος από p.

Πρόταση 2.4.3. *Έστω $f : \mathbb{Z} \to \mathbb{Z}$ ένα πολυώνυμο με ακέραιους συντελεστές. Υπάρχει πολυώνυμο $g : \mathbb{Z} \to \mathbb{Z}$ με ακέραιους συντελεστές και βαθμό μικρότερο από p, τέτοιο ώστε*

$$f(x) \equiv g(x) \pmod{p}$$

για κάθε $x \in \mathbb{Z}$.

Απόδειξη. Έστω $f(x) = c_n x^n + \cdots + c_1 x + c_0$ ένα πολυώνυμο με ακέραιους συντελεστές και $c_n \neq 0$. Έστω ότι $n \geq p$ (αλλιώς δεν έχουμε τίποτα να δείξουμε). Ισχυριζόμαστε ότι για κάθε $p \leq j \leq n$ υπάρχει $1 \leq r = r(j) \leq p-1$ τέτοιος ώστε $x^j \equiv x^{r(j)} \pmod{p}$ για κάθε $x \in \mathbb{Z}$. Για το σκοπό αυτό παρατηρούμε ότι ο j γράφεται μονοσήμαντα στη μορφή $j = (p-1)q(j) + r(j)$ όπου $q(j), r(j) \in \mathbb{N}$ και $1 \leq r(j) \leq p-1$ (αυτό είναι απλή συνέπεια του αλγόριθμου της διαίρεσης). Τότε, αν $(x,p) = 1$ έχουμε

$$x^j = (x^{p-1})^{q(j)} x^{r(j)} \equiv 1^{q(j)} x^{r(j)} = x^{r(j)} \pmod{p}$$

από το μικρό θεώρημα του Fermat, ενώ αν $p \mid x$ έχουμε

$$x^j \equiv 0 \equiv x^{r(j)} \pmod{p}.$$

Τώρα για κάθε $x \in \mathbb{Z}$ έχουμε

$$f(x) = \sum_{j=p}^{n} c_j x^j + \sum_{j=0}^{p-1} c_j x^j \equiv \sum_{j=p}^{n} c_j x^{r(j)} + \sum_{j=0}^{p-1} c_j x^j = g(x) \pmod{p}$$

και το πολυώνυμο g έχει προφανώς βαθμό μικρότερο από p. □

Στη συνέχεια λοιπόν μπορούμε να σκεφτόμαστε ότι ο βαθμός του πολυωνύμου f είναι μικρότερος από p.

Θεώρημα 2.4.4 «Lagrange». *Έστω $f(x) = c_n x^n + \cdots + c_1 x + c_0$ ένα πολυώνυμο με ακέραιους συντελεστές και έστω p ένας πρώτος αριθμός. Υποθέτουμε ότι ο p δεν διαιρεί το συντελεστή c_n. Τότε η ισοτιμία $f(x) \equiv 0 \pmod{p}$ έχει το πολύ n λύσεις.*

Απόδειξη. Με επαγωγή ως προς το βαθμό n του πολυωνύμου. Αν $n = 0$, θέλουμε απλώς να δείξουμε ότι δεν ισχύει η $c_0 \equiv 0 \pmod{p}$, το οποίο είναι αληθές αφού, από την υπόθεση, ο p δεν διαιρεί τον $c_n = c_0$.

Αν $n = 1$, θέλουμε να δείξουμε ότι η γραμμική ισοτιμία $c_1 x \equiv -c_0 \pmod{p}$ έχει το πολύ μία λύση. Όμως ο p δεν διαιρεί τον c_1, άρα $d = (c_1, p) = 1$ και το ζητούμενο έπεται από το Θεώρημα 2.3.1.

Υποθέτουμε ότι το Θεώρημα ισχύει για κάθε πολυώνυμο βαθμού μικρότερου από n και θεωρούμε ένα πολυώνυμο $f(x) = c_n x^n + \cdots + c_1 x + c_0$ βαθμού n. Θα υποθέσουμε

ότι η $f(x) \equiv 0 \pmod{p}$ έχει $n+1$ λύσεις $x_0, x_1, \ldots, x_n$ ανισότιμες ως προς p και θα καταλήξουμε σε άτοπο. Παρατηρούμε ότι για κάθε $x \in \mathbb{Z}$,

$$f(x) - f(x_0) = (c_n x^n + \cdots + c_1 x + c_0) - (c_n x_0^n + \cdots + c_1 x_0 + c_0) = (x - x_0)g(x),$$

όπου g πολυώνυμο με ακέραιους συντελεστές, το οποίο έχει βαθμό μικρότερο ή ίσο από $n-1$. Όμως, για κάθε $j = 1, \ldots, n$ έχουμε

$$(x_j - x_0)g(x_j) = f(x_j) - f(x_0) \equiv 0 \pmod{p},$$

και αφού ο πρώτος p δεν διαιρεί τον $x_j - x_0$ συμπεραίνουμε ότι

$$g(x_j) \equiv 0 \pmod{p}$$

για κάθε $j = 1, \ldots, n$. Όμως τότε η ισοτιμία $g(x) \equiv 0 \pmod{p}$ έχει τουλάχιστον n λύσεις ανισότιμες ως προς p, το οποίο είναι αδύνατο από την υπόθεση της επαγωγής (παρατηρήστε ότι το g έχει συντελεστή του μεγιστοβάθμιου όρου τον c_n). □

Θεώρημα 2.4.5. *Έστω $f(x) = c_n x^n + \cdots + c_1 x + c_0$ ένα πολυώνυμο με ακέραιους συντελεστές και έστω p ένας πρώτος αριθμός. Αν η ισοτιμία $f(x) \equiv 0 \pmod{p}$ έχει περισσότερες από n λύσεις τότε $p \mid c_j$ για κάθε $j = 0, 1, \ldots, n$.*

Απόδειξη. Έχουμε $p \mid c_n$: διαφορετικά, από το Θεώρημα του Lagrange η ισοτιμία $f(x) \equiv 0 \pmod{p}$ θα είχε το πολύ n λύσεις. Αφού $p \mid c_n$ έχουμε

$$g(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \equiv f(x) \pmod{p}$$

για κάθε $x \in \mathbb{Z}$. Άρα η ισοτιμία $g(x) \equiv 0 \pmod{p}$ έχει περισσότερες από n λύσεις, και όπως πριν βλέπουμε ότι $p \mid c_{n-1}$. Συνεχίζοντας όμοια, βλέπουμε ότι όλοι οι συντελεστές $c_n, c_{n-1}, \ldots, c_1, c_0$ είναι πολλαπλάσια του p. □

Συνέπεια του Θεωρήματος 2.4.5 είναι το Θεώρημα του Wilson.

Θεώρημα 2.4.6. *Για κάθε πρώτο αριθμό p ισχύει*

$$(p-1)! \equiv -1 \pmod{p}.$$

Πρώτη απόδειξη: Το ζητούμενο είναι προφανές αν $p = 2$. Μπορούμε λοιπόν να υποθέσουμε ότι ο p είναι περιττός πρώτος. Θεωρούμε το πολυώνυμο

$$f(x) = (x^{p-1} - 1) - \prod_{k=1}^{p-1}(x - k).$$

Ο βαθμός του f είναι $p-2$ (παρατηρήστε ότι οι δυνάμεις x^{p-1} στα $x^{p-1} - 1$ και $\prod_{k=1}^{p-1}(x-k)$ αλληλοαναιρούνται). Από το μικρό θεώρημα του Fermat, για κάθε $k = 1, \ldots, p-1$ έχουμε

$$f(k) \equiv k^{p-1} - 1 \equiv 0 \pmod{p}$$

και συνεπώς η ισοτιμία $f(x) \equiv 0 \pmod{p}$ έχει περισσότερες από $p-2$ λύσεις. Επομένως ο p διαιρεί όλους τους συντελεστές του πολυωνύμου. Ειδικότερα, διαιρεί το σταθερό όρο $c_0 = -1 - (-1)^{p-1}(p-1)! = -1 - (p-1)!$, το οποίο σημαίνει ότι $-1 \equiv (p-1)! \pmod{p}$. □

Δεύτερη απόδειξη: Παρατηρούμε ότι για κάθε $a \in \mathbb{Z}$ με $(a,p)=1$ η ισοτιμία $ax \equiv 1 \pmod{p}$ έχει μοναδική λύση $x \pmod{p}$ και ότι υποχρεωτικά $(x,p)=1$. Συνεπώς σε κάθε $a \in \{1,2,\ldots,p-1\}$ αντιστοιχεί μοναδικό $b \in \{1,2,\ldots,p-1\}$ με $ab \equiv 1 \pmod{p}$. Με αυτόν τον τρόπο στο $b \in \{1,2,\ldots,p-1\}$ αντιστοιχεί προφανώς το a και, επιπλέον, έχουμε $a=b$ αν και μόνο αν $a^2 \equiv 1 \pmod{p}$, δηλαδή $p \mid (a-1)(a+1)$, που σημαίνει $a=1$ ή $a=p-1$. Συμπερασματικά, τα στοιχεία του $\{2,3,\ldots,p-2\}$ χωρίζονται σε ζεύγη (a,b) με $ab \equiv 1 \pmod{p}$ και συνεπώς $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. □

Παρατήρηση 2.4.7. Αντίστροφα, ας υποθέσουμε ότι για κάποιο φυσικό αριθμό $n \geq 2$ ισχύει $(n-1)! \equiv -1 \pmod{n}$. Τότε $(n-1)!+1 = nx$ για κάποιον $x \in \mathbb{N}$. Αν ο n δεν είναι πρώτος, τότε έχει ένα πρώτο διαιρέτη p. Αφού $p < n$, ο p διαιρεί και τον $(n-1)!$, άρα $p \mid 1$, άτοπο. Αυτή η παρατήρηση σε συνδυασμό με το θεώρημα του Wilson δείχνει ότι ένας φυσικός αριθμός n είναι πρώτος *αν και μόνο αν* ικανοποιεί την $(n-1)! \equiv -1 \pmod{n}$. Δίνει δηλαδή κριτήριο για το αν ο n είναι πρώτος ή όχι.

2.5 Ασκήσεις

1. Δείξτε ότι $7 \mid (3^{2n+1} + 2^{n+2})$ για κάθε $n \in \mathbb{N}$.

2. Βρείτε όλους του θετικούς ακεραίους n για τους οποίους ο 5 διαιρεί το $1^n + 2^n + 3^n + 4^n$.

3. Δείξτε ότι αν $a \equiv b \pmod{n_1}$ και $a \equiv c \pmod{n_2}$ τότε $b \equiv c \pmod{n}$, όπου $n = (n_1, n_2)$.

4. Έστω $m > 2$. Δείξτε ότι οι $1^2, 2^2, \ldots, m^2$ δεν σχηματίζουν πλήρες σύστημα υπολοίπων ως προς m.

5. Έστω p πρώτος αριθμός και $a \in \mathbb{Z}$. Δείξτε ότι αν ο p δεν διαιρεί τους a και $a-1$ τότε ο p διαιρεί το $1 + a + a^2 + \cdots + a^{p-2}$.

6. Βρείτε όλους τους φυσικούς n για τους οποίους $n^{13} \equiv n \pmod{1365}$.

7. Βρείτε το μεγαλύτερο θετικό ακέραιο ο οποίος διαιρεί το $n^5 - n$ για κάθε $n \in \mathbb{N}$.

8. Αν p και q είναι διακεκριμένοι πρώτοι, δείξτε ότι

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

9. Έστω p πρώτος και $a, b \in \mathbb{N}$. Δείξτε ότι $(a+b)^p \equiv a^p + b^p \pmod{p}$.

10. Έστω $p > 2$ πρώτος και $a, b \in \mathbb{N}$. Δείξτε ότι αν $a^p + b^p \equiv 0 \pmod{p}$, τότε $a^p + b^p \equiv 0 \pmod{p^2}$.

11. Χρησιμοποιώντας το Θεώρημα του Euler, βρείτε τα τρία τελευταία δεκαδικά ψηφία του 3^{1205}.

12. Έστω ακέραιος a και $n \in \mathbb{N}$. Δείξτε ότι υπάρχει θετικός ακέραιος m τέτοιος ώστε $n \mid a^m - 1$ αν και μόνο αν $(a,n)=1$.

13. Δείξτε ότι για ακεραίους $n \geq 10$ τα δέκα τελευταία δεκαδικά ψηφία των 2^n και $2^{n+7.812.500}$ συμπίπτουν. *Υπόδειξη*: $7.812.500 = 4 \cdot 5^9$.

14. (α) Δείξτε ότι $\phi(2^{2^n}-1) = \prod_{i=0}^{n-1} \phi(2^{2^i}+1)$ για κάθε $n \in \mathbb{N}$.
(β) Βρείτε όλους τους θετικούς ακεραίους n για τους οποίους ισχύει $\phi(2^{2^n}-1) = 2^{2^n-1}$.

15. Βρείτε όλους τους θετικούς ακεραίους n για τους οποίους ισχύει $\phi(n!) = 2^n$.

16. Να λυθούν οι γραμμικές ισοτιμίες

$$140x \equiv 133 \pmod{301} \quad \text{και} \quad 34x \equiv 60 \pmod{98}.$$

17. Να λυθεί το σύστημα γραμμικών ισοτιμιών

$$x \equiv 5 \pmod 6, \quad x \equiv 4 \pmod{11}, \quad x \equiv 3 \pmod{17}.$$

18. Ένα καλάθι περιέχει n αυγά. Αν βγάλουμε τα αυγά από το καλάθι παίρνοντας $2, 3, 4, 5$ ή 6 κάθε φορά, στο καλάθι απομένουν $1, 2, 3, 4$ ή 5 αυγά αντίστοιχα. Αν παίρνουμε 7 αυγά κάθε φορά, τότε δεν περισσεύει κανένα. Ποιός είναι ο μικρότερος δυνατός αριθμός αυγών που μπορεί να περιέχει το καλάθι;

19. Έστω p ένας πρώτος και έστω ότι $(a, p) = 1$ για κάποιο φυσικό a. Δείξτε ότι η κλάση $x \equiv a^{p-2}b \pmod p$ είναι λύση της γραμμικής ισοτιμίας $ax \equiv b \pmod p$.

Χρησιμοποιώντας το παραπάνω, λύστε τις ισοτιμίες $6x \equiv 5 \pmod{11}$ και $3x \equiv 17 \pmod{29}$.

20. (α) Δείξτε ότι μεταξύ τριών διαδοχικών ακεραίων είναι πάντοτε δυνατόν να επιλεγεί ένας ο οποίος είναι σχετικά πρώτος με καθέναν από τους άλλους δύο.

(β) Δείξτε ότι μεταξύ πέντε διαδοχικών ακεραίων είναι πάντοτε δυνατόν να επιλεγεί ένας ο οποίος είναι σχετικά πρώτος με καθέναν από τους άλλους τέσσερις.

(γ) Δείξτε ότι μεταξύ δέκα διαδοχικών ακεραίων είναι πάντοτε δυνατόν να επιλεγεί ένας ο οποίος είναι σχετικά πρώτος με καθέναν από τους άλλους εννέα.

(δ) Να εξετάσετε αν μεταξύ δεκαέξι διαδοχικών ακεραίων είναι πάντοτε δυνατόν να επιλεγεί ένας ο οποίος είναι σχετικά πρώτος με καθέναν από τους άλλους δεκαπέντε.

(ε) Να εξετάσετε αν μεταξύ είκοσι διαδοχικών ακεραίων είναι πάντοτε δυνατόν να επιλεγεί ένας ο οποίος είναι σχετικά πρώτος με καθέναν από τους άλλους δεκαεννέα.

21. Να λυθεί η ισοτιμία $7x^4 + 19x + 25 \equiv 0 \pmod{27}$.

22. Έστω p ένας περιττός πρώτος και έστω $q = (p-1)/2$. Δείξτε ότι

$$(q!)^2 + (-1)^q \equiv 0 \pmod p.$$

23. Αν ο p είναι πρώτος δείξτε ότι ο ακέραιος $[\frac{(p-1)!}{p}]$ είναι άρτιος.

24. (α) Δείξτε ότι αν ο m είναι σύνθετος και $m \geq 6$, τότε $m \mid (m-1)!$.

(β) Βρείτε όλους τους φυσικούς n για τους οποίους ο $(n-1)!+1$ είναι δύναμη του n.

25. Βρείτε όλους τους πρώτους αριθμούς p για τους οποίους ο $\frac{2^{p-1}-1}{p}$ είναι ίσος με το τετράγωνο ενός ακεραίου.

Υποδείξεις - απαντήσεις

1. Παρατηρούμε ότι $9 \equiv 2 \pmod 7$, άρα

$$3^{2n+1} = 3 \cdot 3^{2n} = 3 \cdot 9^n \equiv 3 \cdot 2^n \pmod 7.$$

Επομένως

$$3^{2n+1} + 2^{n+2} = 3 \cdot 9^n + 4 \cdot 2^n \equiv 3 \cdot 2^n + 4 \cdot 2^n = 7 \cdot 2^n \equiv 0 \pmod 7,$$

δηλαδή $7 \mid (3^{2n+1} + 2^{n+2})$.

2. Ο 5 διαιρεί το $1^n + 2^n + 3^n + 4^n$ εάν και μόνο αν ο n είναι περιττός ή $n \equiv 2 \pmod 4$. Πράγματι, αν ο n είναι περιττός τότε

$$1^n + 2^n + 3^n + 4^n \equiv 1^n + 2^n + (-2)^n + (-1)^n = 0 \pmod 5.$$

Αν $n = 2m$ με $m \in \mathbb{Z}$ τότε

$$1^n+2^n+3^n+4^n \equiv 1^n+2^n+(-2)^n+(-1)^n = 2(1+2^n) = 2(1+4^m) \equiv 2(1+(-1)^m) \pmod 5$$

και συνεπώς $1^n + 2^n + 3^n + 4^n \equiv 0 \pmod 5$ αν και μόνο αν ο m είναι περιττός, δηλαδή $n = 2m \equiv 2 \pmod 4$.

3. Αφού $n = (n_1, n_2)$ έχουμε

$$n \mid n_1 \mid a - b \ \text{ και } \ n \mid n_2 \mid a - c.$$

'ρα $n \mid (a - b) - (a - c) = c - b$, δηλαδή $b \equiv c \pmod n$.

4. Οι $1^2, 2^2, \ldots, m^2$ είναι m το πλήθος. Αν σχημάτιζαν πλήρες σύστημα υπολοίπων ως προς m θα έπρεπε να είναι ανισότιμοι mod m. Όμως $m - 1 > 1$ γιατί $m > 2$, και

$$(m-1)^2 = m^2 - 2m + 1 \equiv 1 = 1^2 \pmod m.$$

5. Από το μικρό Θεώρημα του Fermat έχουμε $p \mid a^{p-1} - 1 = (a-1)(a^{p-2} + \cdots + a^2 + a + 1)$. Όμως $(p, a - 1) = 1$ από την υπόθεση, άρα $p \mid a^{p-2} + \cdots + a^2 + a + 1$.

6. Παρατηρούμε ότι $1365 = 3 \cdot 5 \cdot 7 \cdot 13$. Αφού $\phi(3) = 2$, $\phi(5) = 4$, $\phi(7) = 6$ και $\phi(13) = 12$, έχουμε

$$\phi(3),\ \phi(5),\ \phi(7),\ \phi(13) \ \mid \ 12.$$

Από το θεώρημα του Euler, για κάθε $n \in \mathbb{N}$ έχουμε

$$\begin{aligned} n^{13} &= (n^2)^6 \cdot n \equiv n \pmod 3 \\ n^{13} &= (n^4)^3 \cdot n \equiv n \pmod 5 \\ n^{13} &= (n^6)^2 \cdot n \equiv n \pmod 7 \\ n^{13} &= n^{12} \cdot n \equiv n \pmod{13}. \end{aligned}$$

Αφού ο $n^{13} - n$ διαιρείται με τους πρώτους $3, 5, 7, 13$, θα διαιρείται και με το γινόμενό τους. Συνεπώς η

$$n^{13} \equiv n \pmod{1365}$$

ισχύει για κάθε φυσικό n.

7. Έστω d ο ακέραιος αυτός. Προφανώς $d \mid 2^5 - 2 = 30$, άρα $d \leq 30$. Όμως ο 30 διαιρεί το $n^5 - n$ για κάθε $n \in \mathbb{N}$ διότι $5 \mid n^5 - n$ από το μικρό Θεώρημα του Fermat ενώ προφανώς

$2 \mid n(n-1)$ και $3 \mid n(n-1)(n+1)$, άρα $2\cdot 3 \mid n(n-1)(n+1)(n^2+1) = n(n^4-1) = n^5 - n$. Συμπεραίνουμε ότι $d = 30$.

8. Αφού $(p,q) = 1$, από το μικρό θεώρημα του Fermat έχουμε

$$p^{q-1} \equiv 1 \pmod{q} \ \text{ και } \ q^{p-1} \equiv 1 \pmod{p}.$$

Άρα

$$p^{q-1} + q^{p-1} \equiv p^{q-1} \equiv 1 \pmod{q} \ \text{ και } \ p^{q-1} + q^{p-1} \equiv q^{p-1} \equiv 1 \pmod{p}.$$

Από τις $p, q \mid (p^{q-1} + q^{p-1}) - 1$ έπεται ότι $pq \mid (p^{q-1} + q^{p-1}) - 1$, δηλαδή το ζητούμενο.

9. Από το μικρό θεώρημα του Fermat έχουμε

$$(a+b)^p \equiv a + b \pmod{p}$$

(αν $(a+b, p) = 1$ τότε $(a+b)^{p-1} \equiv 1 \pmod{p}$ άρα $(a+b)^p \equiv a+b \pmod{p}$, ενώ αν $p \mid a+b$ τότε και τα δύο μέλη είναι στην κλάση $0 \pmod{p}$). Ομοίως $a^p \equiv a \pmod{p}$ και $b^p \equiv b \pmod{p}$, άρα

$$a^p + b^p \equiv a + b \equiv (a+b)^p \pmod{p}.$$

10. Από την προηγούμενη άσκηση, αν $a^p + b^p \equiv 0 \pmod{p}$ τότε $(a+b)^p \equiv 0 \pmod{p}$. Δηλαδή $p \mid (a+b)^p$, άρα $p \mid a+b$ (ο p είναι πρώτος). Έπεται ότι

$$p^2 \mid p^p \mid (a+b)^p,$$

δηλαδή $(a+b)^p \equiv 0 \pmod{p^2}$.

11. Έχουμε $\phi(1000) = 400$ και $(3, 1000) = 1$ άρα, από το Θεώρημα Fermat-Euler, $3^{400} \equiv 1 \pmod{1000}$. Προκύπτει ότι $3^{1205} = 3^5 \cdot (3^{400})^3 \equiv 3^5 \cdot 1^3 \equiv 3^5 = 243 \pmod{1000}$ και συνεπώς τα τρία τελευταία δεκαδικά ψηφία του 3^{1205} είναι τα 243.

12. Έστω $n \mid a^m - 1$ και $d = (a, n)$. Έχουμε $d \mid a$, άρα $d \mid a^m$, και $d \mid n \mid a^m - 1$ οπότε $d \mid a^m - 1$ και συνεπώς $d \mid a^m - (a^m - 1) = 1$, δηλαδή $d = 1$. Αντίστροφα, αν $(a, n) = 1$ τότε $n \mid a^m - 1$ με $m = \phi(n) \in \mathbb{N}$, από το Θεώρημα Fermat-Euler.

13. Αρκεί να δείξουμε ότι $10^{10} \mid 2^{n+4\cdot 5^9} - 2^n$. Προφανώς $2^{10} \mid 2^{n+4\cdot 5^9} - 2^n$ για $n \geq 10$. Επίσης, από το Θεώρημα Fermat-Euler έχουμε $5^{10} \mid 2^n(2^{\phi(5^{10})} - 1) = 2^n(2^{4\cdot 5^9} - 1) = 2^{n+4\cdot 5^9} - 2^n$ και συνεπώς $10^{10} = 2^{10} \cdot 5^{10} \mid 2^{n+4\cdot 5^9} - 2^n$ για $n \geq 10$.

14. (α) Γνωρίζουμε από τη σχέση (1.6.5) ότι

$$2^{2^n} - 1 = \prod_{i=0}^{n-1} (2^{2^i} + 1).$$

Η προτεινόμενη ισότητα προκύπτει αμέσως από την πολλαπλασιαστικότητα της συνάρτησης του Euler.
(β) Οι ζητούμενοι ακέραιοι είναι οι $n = 1, 2, 3, 4, 5$. Από το (α) συμπεραίνουμε ότι η προτεινόμενη εξίσωση είναι ισοδύναμη με την εξίσωση

$$\prod_{i=0}^{n-1} \phi(2^{2^i} + 1) = 2^{2^n - 1}.$$

Είναι γνωστό ότι για $i = 5$ ο ακέραιος $2^{2^i} + 1 = 2^{2^5} + 1$ διαιρείται με το 641 και συνεπώς ο $\phi(2^{2^5} + 1)$ διαιρείται με το 640 που δεν είναι δύναμη του 2. Άρα υποχρεωτικά $n \leq 5$. Για $n \leq 5$ οι ακέραιοι $2^{2^i} + 1$ με $0 \leq i \leq n-1$ είναι πρώτοι και συνεπώς

$$\prod_{i=0}^{n-1} \phi(2^{2^i} + 1) = \prod_{i=0}^{n-1} 2^{2^i} = 2^{1+2+2^2+\cdots+2^{n-1}} = 2^{2^n-1}.$$

15. Έχουμε $\phi(n!) = 2^n$ μόνο για $n = 5$. Πράγματι αν $n \geq 6$ τότε το $n!$ διαιρείται με το $3 \cdot 6$ και συνεπώς για τη μεγαλύτερη δύναμη 3^r του 3 που διαιρεί το $n!$ ισχύει $r \geq 2$. Το $\phi(n!)$ διαιρείται με το $\phi(3^r) = 2 \cdot 3^{r-1}$ και συνεπώς $3 \mid \phi(n!)$, οπότε το $\phi(n!)$ δεν είναι δύναμη του 2. Για $n = 1, 2, 3, 4, 5$ βρίσκουμε $\phi(n!) = 1, 1, 2, 8, 32$, αντίστοιχα.

16. (α) Παρατηρούμε ότι $(140, 301) = 7 \mid 133$. Άρα η $140x \equiv 133 \pmod{301}$ έχει 7 λύσεις οι οποίες ανήκουν στην ίδια κλάση ως προς $301/7 = 43$. Για να βρούμε μία λύση, χρησιμοποιούμε τον Ευκλείδειο αλγόριθμο: έχουμε

$$\begin{aligned} 301 &= 2 \cdot 140 + 21 \\ 140 &= 6 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7, \end{aligned}$$

άρα

$$7 = 21 - 14 = 21 - 140 + 6 \cdot 21 = 7 \cdot 21 - 140 = 7 \cdot (301 - 2 \cdot 140) - 140 = 7 \cdot 301 - 15 \cdot 140.$$

Πολλαπλασιάζοντας επί 19 παίρνουμε

$$140 \cdot (-285) + 301 \cdot 133 = 133,$$

δηλαδή

$$140 \cdot 16 \equiv 140 \cdot (-285) \equiv 133 (\mathrm{mod}\ 301).$$

Μια λύση της ισοτιμίας είναι η $x_1 = 16 \pmod{301}$, οπότε οι λύσεις είναι

$$16 \pmod{301},\ 59 \pmod{301},\ 102 \pmod{301},\ 145 \pmod{301},$$

$$188 \pmod{301},\ 231 \pmod{301},\ 274 \pmod{301}.$$

(β) Παρατηρούμε ότι $(34, 98) = 2 \mid 60$. Άρα η $34x \equiv 60 \pmod{98}$ έχει 2 λύσεις οι οποίες ανήκουν στην ίδια κλάση ως προς $98/2 = 49$. Για να βρούμε μία λύση, χρησιμοποιούμε τον Ευκλείδειο αλγόριθμο: έχουμε

$$\begin{aligned} 98 &= 2 \cdot 34 + 30 \\ 34 &= 1 \cdot 30 + 4 \\ 30 &= 7 \cdot 4 + 2 \\ 4 &= 2 \cdot 2, \end{aligned}$$

άρα

$$2 = 30 - 7 \cdot 4 = 30 - 7 \cdot 34 + 7 \cdot 30 = 8 \cdot 30 - 7 \cdot 34 = 8 \cdot 98 - 23 \cdot 34.$$

Πολλαπλασιάζοντας επί 30 παίρνουμε

$$34 \cdot (-690) + 98 \cdot 240 = 60,$$

δηλαδή

$$34 \cdot (-4) \equiv 34 \cdot (-690) \equiv 60 (\mathrm{mod}\ 98).$$

Μια λύση της ισοτιμίας είναι η $x_1 = -4 \pmod{98}$, οπότε οι λύσεις είναι

$$45 \pmod{98},\ 94 \pmod{98}.$$

17. Ορίζουμε $M_1 = 11 \cdot 17 = 187$, $M_2 = 6 \cdot 17 = 102$ και $M_3 = 6 \cdot 11 = 66$. Οι ισοτιμίες $187y \equiv 1 \pmod 6$, $102y \equiv 1 \pmod{11}$ και $66y \equiv 1 \pmod{17}$ έχουν τις λύσεις $b_1 = 1$, $b_1 = 4$ και $b_1 = 8$, αντίστοιχα. Προκύπτει ότι ο

$$x = c_1 M_1 b_1 + c_2 M_2 b_2 + c_3 M_3 b_3 = 5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot 4 + 3 \cdot 66 \cdot 8 = 4151$$

είναι λύση του συστήματος. Δηλαδή λύση είναι η κλάση $785 \pmod{1122}$.

18. Λύστε το σύστημα

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 0 \pmod 7, \end{aligned}$$

χρησιμοποιώντας το Κινέζικο θεώρημα υπολοίπων και βρείτε τη μικρότερη θετική λύση του συστήματος. Απάντηση: $x = 119$.

19. Αφού $(a, p) = 1$ έχουμε $a^{p-1} \equiv 1 \pmod p$. Αν λοιπόν $x \equiv a^{p-2} b \pmod p$, τότε

$$ax \equiv a^{p-1} b \equiv b \pmod p.$$

Από το παραπάνω βλέπουμε εύκολα ότι:
(α) Η ισοτιμία $6x \equiv 5 \pmod{11}$ έχει λύση την $x \equiv 6^9 \cdot 5 \pmod{11}$. Αφού $6^3 = 216 \equiv 7 \pmod{11}$, έχουμε $6^9 \equiv 7^3 = 343 \equiv 2 \pmod{11}$. Άρα $6^9 \cdot 5 \equiv 10 \pmod{11}$ είναι η λύση.
(β) Η ισοτιμία $3x \equiv 17 \pmod{29}$ έχει λύση την $x \equiv 3^{27} \cdot 17 \pmod{29}$. Τώρα $3^{27} = 27^9 = (-2)^9 = 2^5 \cdot (-16) \equiv 3 \cdot (-16) = -48 \equiv 10 \pmod{29}$, άρα

$$3^{27} \cdot 17 \equiv 170 \equiv 25 \pmod{29}$$

είναι η λύση.

20. (α) Μεταξύ των $n-1, n$ και $n+1$ ο n είναι σχετικώς πρώτος και προς τον $n-1$ και προς τον $n+1$.
(β) Αν δύο ακέραιοι, έστω οι $x < y$, από τους $n, n+1, n+2, n+3, n+4$ έχουν κοινό διαιρέτη το d τότε ο d διαιρεί και τη διαφορά $y - x$. Όμως $1 \le y - x \le 4$ και συνεπώς $d = 2, 3$ ή 4, άρα οι x, y ή είναι και οι δύο άρτιοι ή και οι δύο πολλαπλάσια του 3. Εύκολα βλέπει κανείς ότι μεταξύ των $n, n+1, n+2, n+3, n+4$ υπάρχει πάντοτε κάποιος που δεν είναι ούτε άρτιος ούτε πολλαπλάσιο του 3. Αυτός είναι σχετικώς πρώτος προς καθένα από τους υπόλοιπους.
(γ) Προκύπτει με παρόμοιο (αλλά πιο πολύπλοκο) σκεπτικό με το (β).
(δ) Ομοίως με το (γ).
(ε) Αυτό δεν είναι πάντοτε δυνατό. Από το Κινέζικο Θεώρημα υπολοίπων το σύστημα

$$\begin{aligned} x \equiv 0 \pmod 2 \quad & x + 6 \equiv 0 \pmod 7 \quad & x \equiv 0 \pmod{17} \\ x \equiv 0 \pmod 3 \quad & x + 7 \equiv 0 \pmod{11} \quad & x \equiv 0 \pmod{19} \\ x + 1 \equiv 0 \pmod 5 \quad & x + 5 \equiv 0 \pmod{13} \end{aligned}$$

έχει μονοδική λύση x ως προς $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ και για κάθε τέτοια λύση x οι x, $x+2$, $x+4, \ldots, x+18$ διαιρούνται με το 2, οι x, $x+3$, $x+6, \ldots, x+18$ διαιρούνται με το

3, οι $x+1$, $x+6$, $x+11$ και $x+16$ διαιρούνται με το 5, οι $x+6$ και $x+13$ διαιρούνται με το 7, οι $x+7$ και $x+18$ διαιρούνται με το 11, οι $x+5$ και $x+18$ διαιρούνται με το 13, οι x και $x+17$ διαιρούνται με το 17 και οι x και $x+19$ διαιρούνται με το 19, οπότε καθένας από τους $x, x+1, \ldots, x+19$ έχει κοινό διαιρέτη με κάποιον από τους υπόλοιπους.

21. Απάντηση: $x \equiv 16 \pmod{27}$.

22. Παρατηρούμε ότι $p-k \equiv -k \pmod{p}$ για κάθε $k = 1, \ldots, q = \frac{p-1}{2}$. Άρα

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

από το θεώρημα του Wilson, δηλαδή $p \mid 1+(-1)^q(q!)^2$. Έπεται ότι

$$p \mid (-1)^q\big(1+(-1)^q(q!)^2\big) = (-1)^q + (q!)^2,$$

με άλλα λόγια $(q!)^2 + (-1)^q \equiv 0 \pmod{p}$.

23. Μπορούμε να υποθέσουμε ότι $p \geq 3$. Από το Θεώρημα του Wilson έχουμε $(p-1)! = -1 + np$ για κάποιο $n \in \mathbb{N}$ και συνεπώς

$$[\frac{(p-1)!}{p}] = [\frac{np-1}{p}] = n-1.$$

Όμως ο $np-1 = (p-1)!$ είναι προφανώς άρτιος, άρα ο n περιττός και ο $n-1 = [\frac{(p-1)!}{p}]$ άρτιος.

24. (α) Γράφουμε τον m στη μορφή $m = a \cdot b$ όπου $1 < a \leq b < m$. Αν $a < b$ τότε οι a και b είναι δύο από τους φυσικούς που εμφανίζονται στο γινόμενο $(m-1)! = 1 \cdot 2 \cdots (m-1)$ και συνεπώς $m = a \cdot b \mid (m-1)!$. Αν $a = b$ τότε $a \geq 3$ και συνεπώς $2a < a^2 = m$ οπότε οι a και $2a$ εμφανίζονται στο γινόμενο $(m-1)! = 1 \cdot 2 \cdots (m-1)$ το οποίο διαιρείται με το $a \cdot 2a = 2m$.

(β) Οι μόνοι θετικοί ακέραιοι με την ιδιότητα αυτή είναι οι $n = 2, 3$ και 5. Για αυτό αρκεί να δείξουμε ότι ο $(n-1)!+1$ δεν είναι δύναμη του n αν $n \geq 6$. Έστω αντιθέτως ότι $n \geq 6$ και $(n-1)!+1 = n^k$ για κάποιο θετικό ακέραιο k. Η προηγούμενη σχέση μπορεί να γραφεί ως

$$(n-2)! = n^{k-1} + \cdots + n^2 + n + 1.$$

Προφανώς ο $(n-1)!$ είναι άρτιος, άρα ο $(n-1)!+1 = n^k$ είναι περιττός και συνεπώς ο n είναι περιττός και ο $m = n-1$ είναι άρτιος με $m \geq 6$. Από το ερώτημα (α) προκύπτει ότι $n-1 = m \mid (m-1)! = (n-2)!$ και επομένως ότι $n-1 \mid = n^{k-1} + \cdots + n^2 + n + 1$. Παρατηρώντας ότι $n^i \equiv 1 \pmod{n-1}$ για κάθε i προκύπτει ότι $n-1 \mid k$. Τότε όμως $n-1 \leq k$ και $n^k \geq n^{n-1} > (n-1)^{n-1} + 1 > (n-1)! + 1$, σε αντίφαση με την υπόθεση.

25. Θα δείξουμε ότι οι μόνοι τέτοιοι πρώτοι είναι οι $p = 3$ και $p = 7$. Έστω $2^{p-1} - 1 = pk^2$ με $k \in \mathbb{N}$. Προφανώς $p > 2$, άρα ο $p-1$ είναι άρτιος και μπορούμε να γράψουμε

$$(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = pk^2.$$

Θέτοντας $u = 2^{\frac{p-1}{2}} - 1$ και $v = 2^{\frac{p-1}{2}} + 1$ έχουμε $uv = pk^2$ και $(u, v) = 1$. Αφού ο p είναι πρώτος πρέπει $p \mid u$ ή $p \mid v$. Στην πρώτη περίπτωση έχουμε $u/p \cdot v = k^2$ και $(u/p, v) = 1$ οπότε από το Λήμμα 1.8.2 προκύπτει ότι οι u/p και v είναι τέλεια τετράγωνα, οπότε $v = r^2$ με $r \in \mathbb{N}$. Ομοίως στη δεύτερη περίπτωση έχουμε $u = r^2$ με $r \in \mathbb{N}$. Αν $2^{\frac{p-1}{2}} + 1 = r^2$ τότε $2^{\frac{p-1}{2}} = r^2 - 1 = (r-1)(r+1)$ και συνεπώς οι $r-1$ και $r+1$ είναι και οι δύο δυνάμεις του 2. Η μόνη δυνατότητα είναι η $r = 3$, οπότε $(p-1)/2 = 3$ και $p = 7$. Έστω $2^{\frac{p-1}{2}} - 1 = r^2$, δηλαδή $2^{\frac{p-1}{2}} = r^2 + 1$. Προφανώς ο r είναι περιττός, άρα $r^2 + 1 \equiv 2 \pmod{4}$. Συνεπώς ο $2^{\frac{p-1}{2}}$ δεν διαιρείται με το 4 και υποχρεωτικά $(p-1)/2 = 1$, δηλαδή $p = 3$.

Κεφάλαιο 3

Αριθμητικές συναρτήσεις

3.1 Εισαγωγή

Ορισμός 3.1.1. Κάθε συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ καλείται *αριθμητική συνάρτηση*. Επιπλέον, λέμε ότι μια αριθμητική συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ είναι *πολλαπλασιαστική* αν για κάθε ζευγάρι φυσικών αριθμών m, n με $(m, n) = 1$ ισχύει

$$f(mn) = f(m)f(n). \tag{3.1.1}$$

Παραδείγματα 3.1.2. Οι παρακάτω αριθμητικές συναρτήσεις παίρνουν τιμές στο $\mathbb{N}$ ή στο $\mathbb{Z}$ και δίνουν μια πρώτη ιδέα για το είδος των αριθμητικών συναρτήσεων που παρουσιάζουν ενδιαφέρον στη θεωρία των αριθμών.

(α) Η συνάρτηση $U : \mathbb{N} \to \mathbb{N}$ με $U(n) = 1$ για κάθε $n \in \mathbb{N}$. Η U είναι προφανώς πολλαπλασιαστική: για την ακρίβεια, $U(mn) = 1 = U(m)U(n)$ για κάθε $m, n \in \mathbb{N}$. Η U είναι *πλήρως πολλαπλασιαστική*.

(β) Η συνάρτηση $I : \mathbb{N} \to \mathbb{N}$ με $I(n) = n$ για κάθε $n \in \mathbb{N}$. Η I είναι προφανώς πλήρως πολλαπλασιαστική: για κάθε $m, n \in \mathbb{N}$ έχουμε $I(mn) = mn = I(m)I(n)$.

(γ) Η συνάρτηση $d : \mathbb{N} \to \mathbb{N}$, όπου $d(n)$ είναι το πλήθος των θετικών διαιρετών του n. Παρατηρήστε ότι

$$d(n) = \sum_{k|n} 1. \tag{3.1.2}$$

(δ) Η συνάρτηση $\sigma : \mathbb{N} \to \mathbb{N}$, όπου $\sigma(n)$ είναι το άθροισμα των θετικών διαιρετών του n. Παρατηρήστε ότι

$$\sigma(n) = \sum_{k|n} k. \tag{3.1.3}$$

(ε) Η συνάρτηση του Euler $\phi : \mathbb{N} \to \mathbb{N}$, όπου $\phi(n)$ είναι το πλήθος των φυσικών $x \leq n$ που είναι σχετικά πρώτοι με τον n.

(στ) Η συνάρτηση $\nu : \mathbb{N} \to \mathbb{Z}^+$, όπου $\nu(n)$ είναι το πλήθος των διακεκριμένων πρώτων παραγόντων στην κανονική αναπαράσταση του n.

(ζ) Η συνάρτηση $\mu : \mathbb{N} \to \mathbb{Z}$, που ορίζεται από την

$$\mu(n) = \begin{cases} 0, & \text{αν ο } n \text{ διαιρείται με κάποιο τέλειο τετράγωνο } m^2 > 1 \\ (-1)^{\nu(n)}, & \text{αν } n = p_1 p_2 \dots p_{\nu(n)}, \text{ όπου } p_i \text{ διακεκριμένοι πρώτοι} \end{cases}$$

είναι μια αριθμητική συνάρτηση. Η μ καλείται *συνάρτηση του Möbius*.

Σε αυτό το Κεφάλαιο θα μελετήσουμε τις βασικές αριθμητικές συναρτήσεις και τις μεταξύ τους σχέσεις. Ένα πρώτο ερώτημα είναι αν οι συναρτήσεις που μόλις ορίσαμε είναι πολλαπλασιαστικές. Το επόμενο θεώρημα δίνει ένα γενικό κριτήριο που θα μας φανεί αρκετά χρήσιμο.

Θεώρημα 3.1.3. *Υποθέτουμε ότι η συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ είναι πολλαπλασιαστική. Τότε η συνάρτηση $g : \mathbb{N} \to \mathbb{C}$ που ορίζεται από την*

$$g(n) = \sum_{k|n} f(k) \tag{3.1.4}$$

είναι επίσης πολλαπλασιαστική.

Απόδειξη. Έστω $m, n \in \mathbb{N}$ με $(m, n) = 1$. Ας υποθέσουμε ότι $k \mid mn$. Από το Λήμμα 1.4.5, ο k γράφεται μονοσήμαντα στη μορφή $k = k_1k_2$ όπου $k_1 \mid m$, και $k_2 \mid n$. Αντίστροφα, αν $k_1 \mid m$ και $k_2 \mid n$ τότε ο $k = k_1k_2$ διαιρεί τον mn. Με άλλα λόγια η απεικόνιση που στέλνει ένα ζευγάρι διαιρετών των m και n στο γινόμενό τους είναι ένα προς ένα και επί του συνόλου των διαιρετών του mn:

> Καθώς οι k_1, k_2 «διατρέχουν» τους διαιρέτες των m, n, ο k_1k_2 «διατρέχει» τους διαιρέτες του mn.

Μπορούμε λοιπόν να γράψουμε

$$g(mn) = \sum_{k|mn} f(k) = \sum_{k_1|m} \sum_{k_2|n} f(k_1k_2). \tag{3.1.5}$$

Παρατηρούμε ότι αν $k_1 \mid m$ και $k_2 \mid n$ τότε $(k_1, k_2) = 1$. Αφού η f είναι πολλαπλασιαστική, έχουμε $f(k_1k_2) = f(k_1)f(k_2)$. Επιστρέφοντας στην (3.1.5) παίρνουμε

$$g(mn) = \sum_{k_1|m} \sum_{k_2|n} f(k_1)f(k_2) = \left(\sum_{k_1|m} f(k_1) \right) \left(\sum_{k_2|n} f(k_2) \right) = g(m)g(n), \tag{3.1.6}$$

δηλαδή η g είναι πολλαπλασιαστική. □

3.2 Οι συναρτήσεις d και σ

Το γεγονός ότι οι d και σ είναι πολλαπλασιαστικές συναρτήσεις είναι άμεση συνέπεια του Θεωρήματος 3.1.3.

Θεώρημα 3.2.1. *Οι συναρτήσεις d και σ είναι πολλαπλασιαστικές.*

Απόδειξη. Έχουμε

$$d(n) = \sum_{k|n} 1 = \sum_{k|n} U(k) \text{ και } \sigma(n) = \sum_{k|n} k = \sum_{k|n} I(k). \tag{3.2.1}$$

Αφού οι U και I είναι πολλαπλασιαστικές, το συμπέρασμα έπεται από το Θεώρημα 3.1.3. □

Το Θεώρημα 3.2.1 μας επιτρέπει να δώσουμε «τύπο» για τις $d(n)$ και $\sigma(n)$ συναρτήσει της κανονικής αναπαράστασης του n. Παρατηρήστε ότι αν f είναι μια πολλαπλασιαστική συνάρτηση και $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ ένας φυσικός μεγαλύτερος από 1, τότε

$$f(n) = f(p_1^{k_1})f(p_2^{k_2})\cdots f(p_r^{k_r}). \tag{3.2.2}$$

Η ισότητα αυτή αποδεικνύεται με βάση την παρατήρηση ότι $(p_1^{k_1}, p_2^{k_2}\cdots p_r^{k_r}) = 1$ και απλή επαγωγή. Αν λοιπόν θέλουμε να δώσουμε τύπο για την f, αρκεί να υπολογίσουμε την τιμή $f(p^k)$ όπου p πρώτος και $k \in \mathbb{N}$.

Θεώρημα 3.2.2. *Έστω $n \geq 2$ και έστω $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ η κανονική του αναπαράσταση. Τότε*

$$d(n) = \prod_{j=1}^{r}(1 + k_j) \tag{3.2.3}$$

και

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1}\frac{p_2^{k_2+1} - 1}{p_2 - 1}\cdots\frac{p_r^{k_r+1} - 1}{p_r - 1}. \tag{3.2.4}$$

Απόδειξη. Οι διαιρέτες ενός φυσικού της μορφής p^k είναι οι $1, p, p^2, \ldots, p^k$. Επομένως

$$d(p^k) = k + 1 \tag{3.2.5}$$

και

$$\sigma(p^k) = 1 + p + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}. \tag{3.2.6}$$

Αφού οι d και σ είναι πολλαπλασιαστικές συναρτήσεις, από την (3.2.2) έχουμε

$$d(n) = \prod_{j=1}^{r} d(p_j^{k_j}) = \prod_{j=1}^{r}(1 + k_j) \tag{3.2.7}$$

και

$$\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\cdots\sigma(p_r^{k_r}) = \frac{p_1^{k_1+1} - 1}{p_1 - 1}\frac{p_2^{k_2+1} - 1}{p_2 - 1}\cdots\frac{p_r^{k_r+1} - 1}{p_r - 1} \tag{3.2.8}$$

για κάθε $n \geq 2$ με κανονική αναπαράσταση την $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Αν $n = 1$ τότε $d(n) = 1$ και $\sigma(n) = 1$. □

Ορισμός 3.2.3. Ένας φυσικός αριθμός n καλείται *τέλειος* αν $\sigma(n) = 2n$, δηλαδή αν το άθροισμα των *γνήσιων διαιρετών* του n (των διαιρετών του που είναι μικρότεροι από αυτόν) ισούται με n.

Παραδείγματα τέλειων αριθμών μας δίνουν οι $n = 6$ και $n = 28$ (παρατηρήστε ότι $6 = 1 + 2 + 3$ και $28 = 1 + 2 + 4 + 7 + 14$). Δεν είναι γνωστό αν υπάρχουν περιττοί τέλειοι αριθμοί. Το επόμενο όμως θεώρημα δίνει πλήρη περιγραφή των άρτιων τέλειων αριθμών.

Θεώρημα 3.2.4 (Ευκλείδης -Euler)**.** *Έστω $m \in \mathbb{N}$ τέτοιος ώστε ο $2^m - 1$ να είναι πρώτος. Τότε, ο $2^{m-1}(2^m - 1)$ είναι τέλειος αριθμός. Κάθε άρτιος τέλειος αριθμός είναι αυτής της μορφής.*

Παρατήρηση 3.2.5. Στην Άσκηση 1.29 είδαμε ότι αν ο $2^m - 1$ είναι πρώτος, τότε ο m είναι πρώτος. Δηλαδή, οι άρτιοι τέλειοι αριθμοί είναι οι φυσικοί της μορφής $2^{p-1}(2^p - 1)$ όπου p πρώτος και $2^p - 1$ πρώτος.

Απόδειξη. Υποθέτουμε πρώτα ότι $n = 2^{m-1}(2^m - 1)$, όπου ο $2^m - 1$ είναι πρώτος. Παρατηρούμε ότι $(2^{m-1}, 2^m - 1) = 1$ και χρησιμοποιώντας το γεγονός ότι η σ είναι πολλαπλασιαστική παίρνουμε

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = \frac{2^m - 1}{2 - 1} \cdot 2^m \tag{3.2.9}$$

αφού $\sigma(p) = p + 1$ για κάθε πρώτο p. Άρα

$$\sigma(n) = 2 \cdot 2^{m-1}(2^m - 1) = 2n, \tag{3.2.10}$$

το οποίο δείχνει ότι ο n είναι τέλειος.

Αντίστροφα, ας υποθέσουμε ότι n είναι ένας άρτιος τέλειος αριθμός. Τότε ο n γράφεται στη μορφή $n = 2^{m-1}k$, όπου $m > 1$ και ο k είναι περιττός. Θα δείξουμε ότι $k = 2^m - 1$ και ότι ο k είναι πρώτος. Αφού ο n είναι τέλειος και $(2^{m-1}, k) = 1$, έχουμε

$$2n = \sigma(n) = \sigma(2^{m-1})\sigma(k) = (2^m - 1)\sigma(k), \tag{3.2.11}$$

δηλαδή

$$\sigma(k) = \frac{2^m k}{2^m - 1} = k + \frac{k}{2^m - 1}. \tag{3.2.12}$$

Αφού $\sigma(k) \in \mathbb{N}$, βλέπουμε ότι ο $k/(2^m - 1)$ είναι φυσικός και βέβαια διαιρεί τον k. Στο δεξιό μέλος της (3.2.12) έχουμε το άθροισμα δύο θετικών διαιρετών του k ενώ στο αριστερό μέλος έχουμε το άθροισμα όλων των θετικών διαιρετών του k. Αναγκαστικά, οι k και $k/(2^m - 1)$ είναι οι μόνοι θετικοί διαιρέτες του k, δηλαδή ο k είναι πρώτος και $k/(2^m - 1) = 1$, το οποίο δείχνει ότι $k = 2^m - 1$. Έπεται ότι $n = 2^{m-1}(2^m - 1)$ με τον $2^m - 1$ πρώτο. □

Το επόμενο πρόβλημα που θα μας απασχολήσει είναι να δώσουμε φράγματα για τη συνάρτηση $d(n)$. Παρατηρήστε ότι για κάθε πρώτο p έχουμε $d(p) = 2$ και αφού υπάρχουν οσοδήποτε μεγάλοι πρώτοι αριθμοί, η $d(n)$ συμπεριφέρεται μάλλον ακανόνιστα όταν το $n \to \infty$. Το ερώτημα είναι λοιπόν να δοθούν άνω φράγματα για την $d(n)$.

Το πρώτο μας αποτέλεσμα δείχνει ότι δεν μπορούμε να περιμένουμε λογαριθμικό άνω φράγμα.

Θεώρημα 3.2.6. *Για κάθε $k \in \mathbb{N}$ και κάθε $C > 0$ υπάρχει $n \in \mathbb{N}$ τέτοιος ώστε*

$$d(n) > C(\ln n)^k. \tag{3.2.13}$$

Απόδειξη. Θέλουμε να κατασκευάσουμε φυσικούς n με μεγάλο (σε σχέση με το n) πλήθος διαιρετών. Θεωρούμε τους $(k+1)$ μικρότερους πρώτους αριθμούς $p_1 < p_2 < \cdots < p_k < p_{k+1}$ και δοκιμάζουμε φυσικούς n της μορφής

$$n = (p_1 p_2 \cdots p_k p_{k+1})^m,$$

όπου ο m θα επιλεγεί κατάλληλα. Από το Θεώρημα 3.2.2 έχουμε

$$d(n) = \prod_{j=1}^{k+1}(m+1) = (m+1)^{k+1} \tag{3.2.14}$$

και

$$C(\ln n)^k = Cm^k\big(\ln(p_1p_2\cdots p_{k+1})\big)^k. \tag{3.2.15}$$

Αν

$$m^{k+1} > Cm^k\big(\ln(p_1p_2\cdots p_{k+1})\big)^k, \tag{3.2.16}$$

το οποίο εξασφαλίζεται αν επιλέξουμε $m > C\big(\ln(p_1p_2\cdots p_{k+1})\big)^k$, διότι τότε θα έχουμε $d(n) = (m+1)^{k+1} > m^{k+1} > C(\ln n)^k$. □

Υπάρχουν λοιπόν φυσικοί με πλήθος διαιρετών μεγαλύτερο από οποιαδήποτε δοσμένη δύναμη του λογαρίθμου τους. Από την άλλη πλευρά, το πλήθος των διαιρετών ενός φυσικού δεν μπορεί να είναι πολύ μεγάλο.

Θεώρημα 3.2.7. *Για κάθε $\epsilon > 0$ υπάρχει σταθερά $C(\epsilon) > 0$ τέτοια ώστε*

$$d(n) \le C(\epsilon)n^\epsilon \tag{3.2.17}$$

για κάθε $n \in \mathbb{N}$. Δηλαδή, το πλήθος των διαιρετών του n «φράσσεται» από n^ϵ.

Απόδειξη. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $0 < \epsilon < 1$. Για κάθε $n \ge 2$ με κανονική αναπαράσταση την $n = p_1^{k_1}\cdots p_r^{k_r}$, έχουμε

$$\frac{d(n)}{n^\epsilon} = \frac{1+k_1}{p_1^{\epsilon k_1}}\cdots\frac{1+k_r}{p_r^{\epsilon k_r}}. \tag{3.2.18}$$

Οι $p_1,\dots,p_r$ χωρίζονται σε δύο ομάδες. Αν κάποιος p_j ικανοποιεί την $2 \le p_j < 2^{1/\epsilon}$, τότε

$$\frac{1+k_j}{p_j^{\epsilon k_j}} \le \frac{1+k_j}{2^{\epsilon k_j}} = \frac{1+k_j}{e^{(\ln 2)\epsilon k_j}} < \frac{1+k_j}{1+(\ln 2)\epsilon k_j} < \frac{1}{(\ln 2)\epsilon}, \tag{3.2.19}$$

διότι $1 + (\ln 2)\epsilon k_j > (\ln 2)\epsilon(1+k_j)$. Αν πάλι $p_j \ge 2^{1/\epsilon}$, τότε

$$\frac{1+k_j}{p_j^{\epsilon k_j}} \le \frac{1+k_j}{2^{k_j}} \le 1. \tag{3.2.20}$$

Από τις προηγούμενες σχέσεις βλέπουμε ότι

$$\frac{d(n)}{n^\epsilon} \le \prod_{\{p\in P:p<2^{1/\epsilon}\}} \frac{1}{(\ln 2)\epsilon} =: C(\epsilon), \tag{3.2.21}$$

όπου η σταθερά $C(\epsilon)$ εξαρτάται μόνο από το ϵ: αν μας δοθεί το ϵ βρίσκουμε πόσοι πρώτοι δεν ξεπερνούν τον $2^{1/\epsilon}$ και υψώνουμε τον $1/[\epsilon(\ln 2)]$ σε αυτή τη δύναμη. □

Για το άθροισμα $\sigma(n)$ των θετικών διαιρετών του n έχουμε το εξής απλό άνω φράγμα.

Θεώρημα 3.2.8. *Για κάθε $n \in \mathbb{N}$ ισχύει η ανισότητα*

$$\sigma(n) \le n(1+\ln n). \tag{3.2.22}$$

Απόδειξη. Γράφουμε

$$\sigma(n) = \sum_{k|n} k = \sum_{k|n} \frac{n}{k} \le n\sum_{s=1}^{n}\frac{1}{s}, \tag{3.2.23}$$

χρησιμοποιώντας την παρατήρηση ότι ο n/k διατρέχει τους θετικούς διαιρέτες του n όταν ο k διατρέχει τους θετικούς διαιρέτες του n. Όμως

$$\sum_{s=1}^{n} \frac{1}{s} \leq 1 + \int_1^2 \frac{dt}{t} + \cdots + \int_{n-1}^{n} \frac{dt}{t} = 1 + \int_1^n \frac{dt}{t} = 1 + \ln n, \tag{3.2.24}$$

άρα $\sigma(n) \leq n(1 + \ln n)$. □

3.3 Η συνάρτηση του Möbius

Η συνάρτηση $\mu : \mathbb{N} \to \mathbb{Z}$ του Möbius ορίζεται από την

$$\mu(n) = \begin{cases} 0, & \text{αν ο } n \text{ διαιρείται με κάποιο τέλειο τετράγωνο } m^2 > 1 \\ (-1)^{\nu(n)}, & \text{αν } n = p_1 p_2 \dots p_{\nu(n)}, \text{ όπου } p_i \text{ διακεκριμένοι πρώτοι} \end{cases}.$$

Παρατηρήστε ότι στην περίπτωση $n = 1$ έχουμε $\nu(1) = 0$, οπότε $\mu(1) = (-1)^0 = 1$. Επίσης, από τον τρόπο ορισμού της μ έχουμε $\mu(n) = 0$ αν και μόνο αν υπάρχει πρώτος p τέτοιος ώστε $p^2 \mid n$. Ένας φυσικός αριθμός n λέγεται *ελεύθερος τετραγώνων* αν δεν υπάρχει πρώτος που το τετράγωνό του να διαιρεί τον n. Με αυτή την ορολογία, ο n είναι ελεύθερος τετραγώνων αν και μόνο αν $\mu(n) = \pm 1$.

Για να κατανοήσει κανείς το κίνητρο για τον ορισμό της συνάρτησης του Möbius, πρέπει να μελετήσει βαθύτερα τη συνάρτηση ζήτα του Riemann (βλέπε §1.6). Η συνάρτηση μ ορίζεται έτσι ώστε, με τη βοήθειά της, να «αντιστρέφεται» η συνάρτηση ζήτα: πιο συγκεκριμένα, τελείως τυπικά, ισχύει η ταυτότητα

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) \cdot \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right) = 1 \tag{3.3.1}$$

για κάθε s. Πράγματι,

$$\begin{aligned} \left(\sum_{m=1}^{\infty} \frac{1}{m^s} \right) \cdot \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{k^s} \right) &= \sum_{n=1}^{\infty} \sum_{\{k,m : km=n\}} \frac{\mu(k)}{n^s} \\ &= \sum_{n=1}^{\infty} \left(\sum_{k \mid n} \mu(k) \right) \frac{1}{n^s}, \end{aligned}$$

οπότε η (3.3.1) ισχύει αν δείξουμε ότι

$$\sum_{k \mid n} \mu(k) = \begin{cases} 1, & \text{αν } n = 1, \\ 0, & \text{αν } n > 1 \end{cases}.$$

Στη συνέχεια θα δείξουμε τις βασικές ιδιότητες της συνάρτησης του Möbius (ανάμεσά τους και αυτή την ταυτότητα).

Πρόταση 3.3.1. *Η συνάρτηση του Möbius είναι πολλαπλασιαστική.*

Απόδειξη. Έστω $m, n \in \mathbb{N}$ με $(m, n) = 1$. Αν κάποιος από τους m και n δεν είναι ελεύθερος τετραγώνων, τότε το ίδιο ισχύει και για τον mn, άρα $\mu(mn) = 0 = \mu(m)\mu(n)$. Αν οι m και n είναι ελεύθεροι τετραγώνων, τότε οι διακεκριμένοι πρώτοι παράγοντες των m και n είναι διαφορετικοί, γιατί $(m, n) = 1$. Άρα ο mn είναι επίσης ελεύθερος τετραγώνων και $\nu(mn) = \nu(m) + \nu(n)$. Έπεται ότι

$$\mu(mn) = (-1)^{\nu(mn)} = (-1)^{\nu(m)+\nu(n)} = (-1)^{\nu(m)}(-1)^{\nu(n)} = \mu(m)\mu(n). \quad (3.3.2)$$

Σε κάθε περίπτωση, $(m, n) = 1 \Rightarrow \mu(mn) = \mu(m)\mu(n)$. Άρα η μ είναι πολλαπλασιαστική συνάρτηση. □

Η επόμενη πρόταση αποδεικνύει τη βασική ταυτότητα που ικανοποιεί η συνάρτηση μ.

Πρόταση 3.3.2. *Για κάθε $n \in \mathbb{N}$ έχουμε*

$$\sum_{k|n} \mu(k) = \begin{cases} 1, & \text{αν } n = 1, \\ 0, & \text{αν } n > 1 \end{cases}.$$

Απόδειξη. Θεωρούμε τη συνάρτηση

$$g(n) = \sum_{k|n} \mu(k). \quad (3.3.3)$$

Αφού η μ είναι πολλαπλασιαστική, το Θεώρημα 3.1.3 δείχνει ότι η g είναι πολλαπλασιαστική. Αν p είναι ένας πρώτος αριθμός, τότε για κάθε $k \geq 1$ έχουμε

$$g(p^k) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) = 1 + (-1) + 0 + \cdots + 0 = 0 \quad (3.3.4)$$

(αν $k = 1$ έχουμε μόνο τους δύο πρώτους όρους στο άθροισμα). Αφού η g είναι πολλαπλασιαστική, αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι ένας φυσικός μεγαλύτερος ή ίσος του 2, τότε

$$g(n) = g(p_1^{k_1}) g(p_2^{k_2}) \cdots g(p_r^{k+r}) = 0. \quad (3.3.5)$$

Τέλος, $g(1) = \mu(1) = 1$. □

Χρησιμοποιώντας την Πρόταση 3.3.2 μπορούμε να αποδείξουμε τον *τύπο αντιστροφής του Möbius*.

Θεώρημα 3.3.3 (Ο τύπος αντιστροφής του Möbius)**.** *Έστω $f : \mathbb{N} \to \mathbb{C}$ μια αριθμητική συνάρτηση. Ορίζουμε $g : \mathbb{N} \to \mathbb{C}$ με*

$$g(n) = \sum_{k|n} f(k). \quad (3.3.6)$$

Τότε

$$f(n) = \sum_{k|n} \mu(k) g\left(\frac{n}{k}\right) = \sum_{k|n} \mu\left(\frac{n}{k}\right) g(k) \quad (3.3.7)$$

για κάθε $n \in \mathbb{N}$.

Απόδειξη. Γράφουμε

$$\begin{aligned}\sum_{k|n}\mu(k)g\left(\frac{n}{k}\right) &= \sum_{k|n}\mu(k)\left(\sum_{d|\frac{n}{k}}f(d)\right)=\sum_{\{k,d:kd|n\}}\mu(k)f(d)\\ &= \sum_{d|n}f(d)\left(\sum_{k|\frac{n}{d}}\mu(k)\right)\\ &= f(n),\end{aligned}$$

γιατί, από την Πρόταση 3.3.2, έχουμε $\sum_{k|\frac{n}{d}}\mu(k)=0$ εκτός αν $d=n$ οπότε το άθροισμα αυτό ισούται με 1. Η δεύτερη ισότητα είναι φανερή: αρκεί να παρατηρήσετε ότι ο n/k διατρέχει τους διαιρέτες του n όταν ο k διατρέχει τους διαιρέτες του n. □

Ισχύει και το αντίστροφο:

Θεώρημα 3.3.4. *Έστω $g:\mathbb{N}\to\mathbb{C}$ μια αριθμητική συνάρτηση. Αν για την $f:\mathbb{N}\to\mathbb{C}$ ισχύει*

$$f(n)=\sum_{k|n}\mu\left(\frac{n}{k}\right)g(k) \tag{3.3.8}$$

για κάθε $n\in\mathbb{N}$, τότε

$$g(n)=\sum_{k|n}f(k) \tag{3.3.9}$$

για κάθε $n\in\mathbb{N}$.

Απόδειξη. Γράφουμε

$$\begin{aligned}\sum_{k|n}f(k) &= \sum_{k|n}f\left(\frac{n}{k}\right)=\sum_{k|n}\left(\sum_{d|\frac{n}{k}}\mu\left(\frac{n}{kd}\right)g(d)\right)\\ &= \sum_{d|n}g(d)\left(\sum_{k|\frac{n}{d}}\mu\left(\frac{n/d}{k}\right)\right)=\sum_{d|n}g(d)\left(\sum_{k|\frac{n}{d}}\mu(k)\right)\\ &= g(n),\end{aligned}$$

χρησιμοποιώντας πάλι την Πρόταση 3.3.2. □

Ένα άμεσο πόρισμα του τύπου αντιστροφής του Möbius είναι το αντίστροφο του Θεωρήματος 3.1.3.

Πόρισμα 3.3.5. *Έστω $f:\mathbb{N}\to\mathbb{C}$ μια αριθμητική συνάρτηση. Αν η συνάρτηση $g:\mathbb{N}\to\mathbb{C}$ που ορίζεται από την*

$$g(n)=\sum_{k|n}f(k) \tag{3.3.10}$$

είναι πολλαπλασιαστική, τότε η f είναι πολλαπλασιαστική.

Απόδειξη. Από τον τύπο αντιστροφής του Möbius,

$$f(n) = \sum_{k|n} \mu(k) g\left(\frac{n}{k}\right). \tag{3.3.11}$$

Έστω $m, n \in \mathbb{N}$ με $(m,n) = 1$. Παρατηρούμε ότι: όταν οι k_1, k_2 διατρέχουν τους θετικούς διαιρέτες των m, n αντίστοιχα, τότε ο $k_1 k_2$ διατρέχει τους θετικούς διαιρέτες του mn. Επίσης, $(k_1, k_2) = 1$ και $(m/k_1, n/k_2) = 1$, αφού $(m,n) = 1$. Χρησιμοποιώντας και το γεγονός ότι οι μ, g είναι πολλαπλασιαστικές, γράφουμε

$$\begin{aligned}
f(mn) &= \sum_{k|mn} \mu(k) g\left(\frac{mn}{k}\right) \\
&= \sum_{k_1|m} \sum_{k_2|n} \mu(k_1 k_2) g\left(\frac{m}{k_1} \cdot \frac{n}{k_2}\right) \\
&= \sum_{k_1|m} \sum_{k_2|n} \mu(k_1)\mu(k_2) g\left(\frac{m}{k_1}\right) g\left(\frac{n}{k_2}\right) \\
&= \left(\sum_{k_1|m} \mu(k_1) g\left(\frac{m}{k_1}\right)\right) \cdot \left(\sum_{k_2|n} \mu(k_2) g\left(\frac{n}{k_2}\right)\right) \\
&= f(m) f(n),
\end{aligned}$$

άρα η f είναι πολλαπλασιαστική. □

Παρατήρηση 3.3.6 (πάνω στην άθροιση)**.** Στις προηγούμενες αποδείξεις χρειάστηκε να αλλάξουμε τη σειρά της άθροισης για αθροίσματα της μορφής

$$\sum_{k|n} \sum_{d|\frac{n}{k}} A(k,d), \tag{3.3.12}$$

όπου A μια συνάρτηση ορισμένη στο $mbN \times \mathbb{N}$. Για να υπολογίσουμε το παραπάνω άθροισμα, πρώτα αθροίζουμε τις τιμές της $A(k,\cdot)$ πάνω από όλους τους θετικούς διαιρέτες του n/k, όπου k σταθεροποιημένος θετικός διαιρέτης του n. Το πρώτο αυτό άθροισμα εξαρτάται από το k, και κατόπιν αθροίζουμε πάνω από όλους τους θετικούς διαιρέτες του n. Παρατηρήστε ότι αν $d \mid (n/k)$ τότε ο d είναι διαιρέτης του n. Αν λοιπόν $d \mid n$, στο παραπάνω άθροισμα συμμετέχουν οι τιμές $A(k,d)$ που αντιστοιχούν στους φυσικούς k για τους οποίους $k \mid n$ και $d \mid (n/k)$. Αυτοί είναι ακριβώς οι φυσικοί k που ικανοποιούν την $k \mid (n/d)$ (γιατί;). Θα καταλήξουμε λοιπόν στο ίδιο ακριβώς αποτέλεσμα αν υπολογίσουμε το

$$\sum_{d|n} \sum_{k|\frac{n}{d}} A(k,d). \tag{3.3.13}$$

Η ισότητα

$$\sum_{k|n} \sum_{d|\frac{n}{k}} A(k,d) = \sum_{d|n} \sum_{k|\frac{n}{d}} A(k,d) \tag{3.3.14}$$

χρησιμοποιήθηκε αρκετές φορές σε αυτή την παράγραφο (βλέπε τις αποδείξεις των Θεωρημάτων 3.3.3 και 3.3.4).

3.4 Η συνάρτηση του Euler

Υπενθυμίζουμε ότι η συνάρτηση του Euler $\phi : \mathbb{N} \to \mathbb{N}$ ορίζεται ως εξής: για κάθε $n \in \mathbb{N}$ θέτουμε $\phi(n)$ το πλήθος των $x \in \{1, \ldots, n\}$ για τους οποίους $(x, n) = 1$. Το γεγονός ότι η ϕ είναι πολλαπλασιαστική συνάρτηση είναι συνέπεια της επόμενης παρατήρησης.

Θεώρημα 3.4.1. *Για κάθε φυσικό αριθμό n ισχύει η ταυτότητα*

$$\sum_{k|n} \phi(k) = n. \tag{3.4.1}$$

Απόδειξη. Για κάθε θετικό διαιρέτη k του n θεωρούμε το σύνολο

$$B_k = \{x : 1 \leq x \leq n \text{ και } (x, n) = k\}. \tag{3.4.2}$$

Τα σύνολα B_k είναι ξένα και η ένωσή τους είναι το $\{1, \ldots, n\}$. Αν λοιπόν συμβολίσουμε με $|A|$ το πλήθος των στοιχείων ενός πεπερασμένου συνόλου A, τότε

$$\sum_{k|n} |B_k| = n. \tag{3.4.3}$$

Για κάθε θετικό διαιρέτη k του n θεωρούμε τώρα το σύνολο

$$C_k = \{y : 1 \leq y \leq n/k \text{ και } (y, n/k) = 1\}. \tag{3.4.4}$$

Παρατηρούμε ότι $x \in B_k$ αν και μόνο αν $x/k \in C_k$. Πράγματι, αν $x \in B_k$ τότε $x \leq n$ και $(x, n) = k$, άρα $x/k \in \mathbb{N}$, $x/k \leq n/k$, και $(x/k, n/k) = (x, n)/k = 1$. Αντίστροφα, αν $y \in C_k$, τότε $ky \leq n$ και $(ky, n) = (ky, k(n/k)) = k(y, n/k) = k$, δηλαδή $ky \in B_k$. Επομένως, η απεικόνιση $g_k : B_k \to C_k$ με $g_k(x) = x/k$ είναι ένα προς ένα και επί. Από τον ορισμό του C_k έπεται ότι

$$|B_k| = |C_k| = \phi\left(\frac{n}{k}\right) \tag{3.4.5}$$

για κάθε k. Επιστρέφοντας στην (3.4.3) παίρνουμε

$$\sum_{k|n} \phi(k) = \sum_{k|n} \phi\left(\frac{n}{k}\right) = \sum_{k|n} |C_k| = \sum_{k|n} |B_k| = n, \tag{3.4.6}$$

που ήταν το ζητούμενο. □

Πόρισμα 3.4.2. *Η συνάρτηση ϕ είναι πολλαπλασιαστική.*

Απόδειξη. Η συνάρτηση $I(n) = n$ είναι πολλαπλασιαστική, οπότε το συμπέρασμα έπεται άμεσα από το Θεώρημα 3.4.1 και το Πόρισμα 3.3.5. □

Πόρισμα 3.4.3. *Για κάθε φυσικό αριθμό n ισχύει η ταυτότητα*

$$\phi(n) = \sum_{k|n} \mu(k)\frac{n}{k} = n\sum_{k|n} \frac{\mu(k)}{k}. \tag{3.4.7}$$

Απόδειξη. Άμεση συνέπεια του τύπου αντιστροφής του Möbius (Θεώρημα 3.3.3). □

Αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική αναπαράστασης του n, ο τύπος

$$\phi(n) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1) \tag{3.4.8}$$

του Θεωρήματος 2.2.7 μπορεί να προκύψει διαφορετικά ως εξής.

Απόδειξη (Θεωρήμα 2.2.7). Αρκεί να δείξουμε την πρώτη ισότητα. Θα χρησιμοποιήσουμε το Πόρισμα 3.4.3 και το γεγονός ότι η ϕ είναι πολλαπλασιαστική. Αν p είναι ένας πρώτος αριθμός και $k \geq 1$, τότε

$$\phi(p^k) = p^k \sum_{d|p^k} \frac{\mu(d)}{d} = p^k \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p}\right) = p^k \left(1 - \frac{1}{p}\right), \tag{3.4.9}$$

γιατί $\mu(1) = 1$, $\mu(p) = -1$ και $\mu(p^s) = 0$ αν $s \geq 2$. Έπεται ότι αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \geq 2$, τότε

$$\phi(n) = \prod_{j=1}^{r} p_j^{k_j} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{r} p_j^{k_j} \cdot \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right). \tag{3.4.10}$$

Η τελευταία ισότητα ολοκληρώνει την απόδειξη. □

Τέλος δίνουμε κάποιες εκτιμήσεις για την $\phi(n)$. Παρατηρήστε ότι $\phi(n) \leq n - 1$ για κάθε $n \geq 2$, με ισότητα αν ο n είναι πρώτος. Αυτό είναι λοιπόν το καλύτερο γενικό άνω φράγμα που μπορούμε να δώσουμε. Στην αντίθετη κατεύθυνση, παρατηρούμε ότι από τον ορισμό των συναρτήσεων ϕ και σ, αυτό που περιμένει κανείς είναι ότι η τιμή $\phi(n)$ θα είναι μεγάλη σε σχέση με το n αν ο n έχει «λίγους» διαιρέτες, δηλαδή αν το άθροισμα $\sigma(n)$ των διαιρετών του n είναι «μικρό» σε σχέση με το n. Το επόμενο θεώρημα δείχνει ότι οι δύο συναρτήσεις «ισορροπούν» με μεγάλη ακρίβεια: το γινόμενο $\phi(n)\sigma(n)$ είναι πάντα «περίπου ίσο» με n^2.

Θεώρημα 3.4.4. *Για κάθε φυσικό αριθμό n ισχύουν οι ανισότητες*

$$\frac{1}{2} < \frac{\phi(n)\sigma(n)}{n^2} \leq 1. \tag{3.4.11}$$

Απόδειξη. Στην περίπτωση $n = 1$ είναι $\phi(n) = \sigma(n) = 1$, οπότε έχουμε ισότητα στο δεξιό μέλος. Υποθέτουμε λοιπόν ότι $n \geq 2$ και θεωρούμε την κανονική αναπαράσταση $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Τότε

$$\sigma(n) = \prod_{j=1}^{r} \frac{p_j^{k_j+1} - 1}{p_j - 1} \tag{3.4.12}$$

και

$$\phi(n) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1), \tag{3.4.13}$$

άρα

$$\sigma(n)\phi(n) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j^{k_j+1} - 1) = \prod_{j=1}^{r} p_j^{2k_j} \left(1 - \frac{1}{p_j^{k_j+1}}\right), \tag{3.4.14}$$

δηλαδή

$$\sigma(n)\phi(n) = n^2 \prod_{j=1}^{r} \left(1 - \frac{1}{p_j^{k_j+1}}\right). \tag{3.4.15}$$

Το γινόμενο στο δεξιό μέλος είναι προφανώς μικρότερο ή ίσο από 1, άρα

$$\frac{\sigma(n)\phi(n)}{n^2} \leq 1. \tag{3.4.16}$$

Για την αριστερή ανισότητα του θεωρήματος, παρατηρούμε ότι

$$\begin{aligned} \prod_{j=1}^{r} \left(1 - \frac{1}{p_j^{k_j+1}}\right) &\geq \prod_{j=1}^{r} \left(1 - \frac{1}{p^2}\right) \geq \prod_{m=2}^{n} \left(1 - \frac{1}{m^2}\right) \\ &= \prod_{m=2}^{n} \frac{m+1}{m} \cdot \prod_{m=2}^{n} \frac{m-1}{m} = \frac{n+1}{2} \cdot \frac{1}{n} = \frac{n+1}{2n} > \frac{1}{2}, \end{aligned}$$

απ' όπου προκύπτει η $\sigma(n)\phi(n)/n^2 > 1/2$. □

Σε συνδυασμό με το άνω φράγμα $\sigma(n) \leq n(1 + \ln n)$ του Θεωρήματος 3.2.8, παίρνουμε αμέσως ένα κάτω φράγμα για την $\phi(n)$.

Πόρισμα 3.4.5. *Για κάθε $n \in \mathbb{N}$ ισχύει η ανισότητα*

$$\phi(n) > \frac{n}{2(1 + \ln n)}. \tag{3.4.17}$$

Απόδειξη. Από το Θεώρημα 3.4.4 και το Θεώρημα 3.2.8 έχουμε

$$\frac{1}{2} < \frac{\sigma(n)\phi(n)}{n^2} \leq \frac{\phi(n)n(1 + \ln n)}{n^2} \tag{3.4.18}$$

για κάθε $n \in \mathbb{N}$. □

3.5 Ασκήσεις

1. Δείξτε ότι

$$\prod_{k|n} k = n^{d(n)/2}.$$

2. Δείξτε ότι ο $d(n)$ είναι περιττός αν και μόνο αν ο n είναι τέλειο τετράγωνο.

3. Δείξτε ότι

$$\sum_{k|n} d(k)^3 = \left(\sum_{k|n} d(k)\right)^2.$$

4. Δείξτε ότι $d(n) \leq d(2^n - 1)$ για κάθε φυσικό n.

5. (α) Δείξτε ότι $d(n) < 2\sqrt{n}$ για κάθε $n \in \mathbb{N}$.
(β) Βρείτε όλους τους θετικούς ακεραίους n για τους οποίους ισχύει $d(2n) = n$.

6. Υποθέτουμε ότι ο n είναι σύνθετος. Δείξτε ότι $\sigma(n) > n + \sqrt{n}$.

7. Δείξτε ότι ο μόνος ελεύθερος τετραγώνων τέλειος φυσικός αριθμός είναι ο 6.

8. Έστω n ένας τέλειος αριθμός. Δείξτε ότι

$$\sum_{k|n} \frac{1}{k} = 2.$$

9. Έστω ότι υπάρχει κάποιος περιττός τέλειος φυσικός n. Δείξτε ότι ο n έχει τουλάχιστον δύο πρώτους παράγοντες και ότι ακριβώς ένας από τους πρώτους παράγοντες του n έχει περιττό εκθέτη στην κανονική αναπαράσταση του n.

10. Έστω $a \in \mathbb{N}$ ελεύθερος τετραγώνων με άρτιο πλήθος πρώτων παραγόντων: δηλαδή, $a = p_1 p_2 \cdots p_k$, όπου p_i διακεκριμένοι πρώτοι και k άρτιος. Θεωρούμε όλους τους θετικούς διαιρέτες k του a που είναι μικρότεροι από $\sqrt{a}$. Δείξτε ότι

$$\sum_{k} \mu(k) = 0.$$

11. Δείξτε ότι η συνάρτηση $f(n) = (-1)^{n-1}$ είναι πολλαπλασιαστική και υπολογίστε το άθροισμα

$$h(n) = \sum_{k|n} (-1)^{k-1} \mu\left(\frac{n}{k}\right)$$

για κάθε $n \in \mathbb{N}$.

12. Δείξτε ότι

$$\sum_{k|n} \mu(k) d\left(\frac{n}{k}\right) = 1$$

και ότι

$$\sum_{k|n} \mu(k) \sigma\left(\frac{n}{k}\right) = n$$

για κάθε $n \in \mathbb{N}$.

13. Δείξτε ότι

$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$$

για κάθε $n \in \mathbb{N}$.

14. Δείξτε ότι

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} k = \frac{n\phi(n)}{2}$$

για κάθε $n \in \mathbb{N}$.

15. Δείξτε ότι $\phi(n)d(n) \geq n$ για $n \in \mathbb{N}$.

16. Βρείτε όλους τους θετικούς ακεραίους $n \leq 30$ για τους οποίους $\phi(n) = d(n)$.

17. Αν $6 \mid n$ δείξτε ότι $\phi(n) \leq n/3$.

18. Έστω $n \in \mathbb{N}$ με την ιδιότητα $\phi(n) \mid n$. Δείξτε ότι $n = 2^a 3^b$ για κάποιους $a, b \in \mathbb{Z}^+$.

19. Υποθέτουμε ότι $p_1 < p_2 < \cdots < p_N$ είναι όλοι οι πρώτοι αριθμοί. Δείξτε ότι $\phi(p_1 p_2 \cdots p_N) = 1$ και καταλήξτε σε άτοπο (έτσι, παίρνετε άλλη μια απόδειξη για την απειρία των πρώτων αριθμών).

20. Δείξτε ότι

$$\sum_{k|n} \sigma(k)\phi\left(\frac{n}{k}\right) = nd(n)$$

για κάθε $n \in \mathbb{N}$.

21. Δείξτε ότι $\sigma(n) + \phi(n) = nd(n)$ αν και μόνο αν ο n είναι πρώτος.

22. Έστω $f : \mathbb{N} \to \mathbb{C}$ πολλαπλασιαστική αριθμητική συνάρτηση. Αν $m, n \in \mathbb{N}$, $d = (m, n)$ και $D = mn/d$ δείξτε ότι

$$f(m)f(n) = f(d)f(D).$$

Υπόδειξη: θεωρήστε την κανονική αναπαράσταση των m, n.

Υποδείξεις - απαντήσεις

1. Όταν ο k διατρέχει τους θετικούς διαιρέτες του n, τότε ο n/k διατρέχει κι αυτός τους θετικούς διαιρέτες του n. Άρα

$$\left(\prod_{k|n} k\right)^2 = \prod_{k|n} k \cdot \prod_{k|n} \frac{n}{k} = \prod_{k|n} n = n^{d(n)},$$

αφού το πλήθος των θετικών διαιρετών του n ισούται με $d(n)$. Έπεται το ζητούμενο.

2. Αν $n = 1$, τότε $d(n) = 1$ και το ζητούμενο ισχύει: ο 1 είναι τέλειο τετράγωνο και ο $d(1)$ περιττός. Υποθέτουμε λοιπόν ότι $n \geq 2$ και ότι $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική αναπαράσταση του n. Τότε,

$$d(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1),$$

άρα ο $d(n)$ είναι περιττός αν και μόνο αν όλοι οι k_j είναι άρτιοι (αν κάποιος k_j είναι περιττός τότε ο $d(n)$ διαιρείται με τον άρτιο $k_j + 1$, δηλαδή είναι άρτιος). Από την άλλη πλευρά, όλοι οι k_j είναι άρτιοι αν και μόνο αν ο n είναι τέλειο τετράγωνο. Πράγματι, αν $k_j = 2s_j$ τότε $n = m^2$ όπου $m = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$. Το αντίστροφο ελέγχεται εντελώς ανάλογα.

3. Ορίζουμε τις αριθμητικές συναρτήσεις

$$A(n) = \sum_{k|n} d(k)^3 \quad \text{και} \quad B(n) = \sum_{k|n} d(k).$$

Δείχνουμε πρώτα ότι οι A και B είναι πολλαπλασιαστικές: αν $(m, n) = 1$, τότε για $r = 1, 3$ έχουμε

$$\begin{aligned} \sum_{k|mn} d(k)^r &= \sum_{k_1|m} \sum_{k_2|n} d(k_1 k_2)^r = \sum_{k_1|m} \sum_{k_2|n} d(k_1)^r d(k_2)^r \\ &= \left(\sum_{k_1|m} d(k_1)^r\right) \left(\sum_{k_2|n} d(k_2)^r\right), \end{aligned}$$

όπου χρησιμοποιήσαμε το ότι η d είναι πολλαπλασιαστική και το ότι όταν οι k_1, k_2 διατρέχουν τους θετικούς διαιρέτες των m, n αντίστοιχα, τότε ο $k_1 k_2$ διατρέχει τους θετικούς διαιρέτες του mn, και $(k_1, k_2) = 1$ αφού $(m, n) = 1$.

Αφού η B είναι πολλαπλασιαστική, το ίδιο ισχύει και για την B^2. Αρκεί λοιπόν να ελέγξουμε ότι $A(p^k) = B^2(p^k)$. Έχουμε:

$$A(p^k) = d(1)^3 + d(p)^3 + \cdots + d(p^k)^3 = 1^3 + 2^3 + \cdots + (k+1)^3$$

και

$$B^2(p^k) = \left(d(1) + d(p) + \cdots + d(p^k)\right)^2 = (1 + 2 + \cdots + (k+1))^2 .$$

Όμως,

$$1^3 + 2^3 + \cdots + (k+1)^3 = \frac{(k+1)^2(k+2)^2}{4} = (1 + 2 + \cdots + (k+1))^2 ,$$

το οποίο αποδεικνύει το ζητούμενο.

4. Έστω A το σύνολο των θετικών διαιρετών του n και B το σύνολο των θετικών διαιρετών του $2^n - 1$. Ορίζουμε μια απεικόνιση $g : A \to B$ με $g(k) = 2^k - 1$. Η g είναι καλά ορισμένη: αν $k \mid n$ τότε $(2^k - 1) \mid (2^n - 1)$. Η g είναι προφανώς ένα προς ένα, άρα το A έχει το πολύ τόσα στοιχεία όσα έχει το B. Με άλλα λόγια, $d(n) \leq d(2^n - 1)$.

5. (α) Παρατηρούμε ότι αν $d \mid n$ τότε $d \leq \sqrt{n}$ ή $n/d \leq \sqrt{n}$ (διαφορετικά θα είχαμε $n = \sqrt{n}\sqrt{n} < d \cdot (n/d) = n$) και συνεπώς $d \in \{1, 2, \ldots, [\sqrt{n}]\}$ ή $n/d \in \{1, 2, \ldots, [\sqrt{n}]\}$. Προκύπτει ότι το πλήθος $d(n)$ των θετικών διαιρετών του n δεν ξεπερνά το διπλάσιο του πλήθους των στοιχείων του $\{1, 2, \ldots, [\sqrt{n}]\}$, επομένως $d(n) \leq 2\sqrt{n}$. Εύκολα βλέπουμε από τα παραπάνω ότι η περίπτωση της ισότητας δεν υφίσταται.

(β) Αν $d(2n) = n$, από το (α) έχουμε $n = d(2n) < 2\sqrt{2n}$, άρα $\sqrt{n} < 2\sqrt{2}$ ή $n < 8$. Οι λύσεις με $n < 8$ είναι οι $n = 4$ και $n = 6$.

6. Ο n είναι σύνθετος, άρα υπάρχουν $m \geq s > 1$ τέτοιοι ώστε $n = ms$. Ειδικότερα, $n \leq m^2$ δηλαδή $m \geq \sqrt{n}$. Έπεται ότι

$$\sigma(n) \geq n + m + 1 \geq n + \sqrt{n} + 1 > n + \sqrt{n}.$$

7. Υποθέτουμε ότι ο $n = p_1 \cdots p_r$ είναι τέλειος, όπου $p_1 < \cdots < p_r$ (παρατηρήστε ότι $r \geq 2$: ένας πρώτος αριθμός δεν μπορεί να είναι τέλειος). Αφού ο n είναι τέλειος, έχουμε $\sigma(n) = 2n$ δηλαδή

$$(p_1 + 1) \cdots (p_r + 1) = 2p_1 \cdots p_r.$$

Δείχνουμε πρώτα ότι $p_1 = 2$. Αν όχι, τότε το αριστερό μέλος διαιρείται με 4 (γιατί κάθε $p_i + 1$ είναι άρτιος και $r \geq 2$) ενώ η μεγαλύτερη δύναμη του 2 που διαιρεί το δεξιό μέλος είναι ο 2 (το γινόμενο $p_1 \cdots p_r$ είναι περιττός αριθμός). Αυτό οδηγεί σε άτοπο. Αφού $p_1 = 2$, έχουμε

$$3(p_2 + 1) \cdots (p_r + 1) = 4p_2 \cdots p_r.$$

Αφού $3 \mid 4p_2 \cdots p_r$, υπάρχει $2 \leq i \leq r$ τέτοιος ώστε $3 \mid p_i$, το οποίο μπορεί να συμβεί μόνο αν $p_i = 3$ (ο p_i είναι πρώτος). Άρα $p_2 = 3$. Αν υπήρχε κι άλλος πρώτος διαιρέτης, π.χ. ο p_3, του n τότε θα είχαμε $(p_3 + 1) \mid 4p_2 \cdots p_r$, οπότε $(p_3 + 1) \mid 4$ το οποίο αποκλείεται γιατί $p_3 + 1 \geq 5 + 1 = 6$ ή $(p_3 + 1) \mid p_i$ για κάποιον $i \geq 3$ το οποίο αποκλείεται γιατί ο $p_3 + 1$ είναι άρτιος ενώ όλοι οι p_i, $i \geq 3$ περιττοί.

Άρα ο n πρέπει να έχει μόνο δύο πρώτους διαιρέτες, τους $p_1 = 2$ και $p_2 = 3$. Εύκολα ελέγχουμε ότι ο $n = 2 \cdot 3 = 6$ είναι τέλειος, άρα αυτός είναι ο μοναδικός ελεύθερος τετραγώνων τέλειος αριθμός.

8. Αφού ο n είναι τέλειος, έχουμε

$$\sigma(n) = \sum_{k \mid n} k = 2n.$$

Όμως

$$\sum_{k \mid n} k = \sum_{k \mid n} \frac{n}{k} = n \sum_{k \mid n} \frac{1}{k}.$$

Από τις δύο προηγούμενες σχέσεις βλέπουμε ότι

$$\sum_{k \mid n} \frac{1}{k} = 2.$$

9. Έστω $n = p_1^{k_1} \cdots p_r^{k_r}$ τέλειος αριθμός, όπου $p_1 < \cdots < p_r$ περιττοί πρώτοι. Δείχνουμε πρώτα ότι $r \geq 2$. Αν ήταν $n = p^k$, όπου $p \geq 3$, θα είχαμε

$$\sigma(n) = 2n \Longrightarrow \frac{p^{k+1} - 1}{p - 1} = 2p^k,$$

απ' όπου θα παίρναμε $p^{k+1} = 2p^k - 1$ και συνεπώς ότι $p \mid 1$, πράγμα αδύνατο.

Ο n έχει λοιπόν τουλάχιστον δύο (περιττούς) πρώτους διαιρέτες. Αφού ο n είναι τέλειος, έχουμε

$$(1+p_1+\cdots+p_1^{k_1})\cdots(1+p_r+\cdots+p_r^{k_r})=2p_1^{k_1}\cdots p_r^{k_r}.$$

Παρατηρούμε ότι αν ο k_i είναι περιττός τότε ο $s_i=1+p_i+\cdots+p_i^{k_i}$ είναι άρτιος, ενώ αν ο k_i είναι άρτιος τότε ο s_i είναι περιττός (ο s_i είναι άθροισμα k_i+1 περιττών αριθμών). Άρα το αριστερό μέλος διαιρείται με 2^x αν x από τους k_i είναι περιττοί, και είναι περιττός αριθμός αν όλοι οι k_i είναι άρτιοι. Αφού το δεξιό μέλος είναι της μορφής $2\times m$ με τον m περιττό, αναγκαστικά έχουμε $x=1$ (γιατί;). Δηλαδή ακριβώς ένας από τους p_i έχει περιττό εκθέτη στην κανονική αναπαράσταση του n.

10. Παρατηρούμε ότι για κάθε θετικό διαιρέτη d του a ισχύει $\mu(d)=\mu(a/d)$. Πράγματι: ο d είναι της μορφής $p_{i_1}\cdots p_{i_s}$ και ο a/k της μορφής $p_{j_1}\cdots p_{j_r}$ όπου $s+r=k$ δηλαδή άρτιος αριθμός (κάποιοι από τους πρώτους διαιρέτες του a σχηματίζουν τον d και οι υπόλοιποι τον a/d). Τότε

$$\mu(d)\mu(a/d)=(-1)^s(-1)^r=(-1)^k=1,$$

δηλαδή οι $\mu(d)$ και $\mu(a/d)$ είναι ομόσημοι. Αφού $\mu(d),\mu(a/d)=\pm1$, έπεται ότι $\mu(d)=\mu(a/d)$.

Θέτουμε $A=\{d\mid a:d<\sqrt{a}\}$ και $B=\{u\mid a:u>\sqrt{a}\}$. Ο a δεν είναι τέλειο τετράγωνο, άρα το $A\cup B$ είναι το σύνολο όλων των θετικών διαιρετών του a. Επιπλέον, $B=\{a/d:d\in A\}$ γιατί αν d είναι ένας θετικός διαιρέτης του a μικρότερος από $\sqrt{a}$, τότε ο a/d είναι θετικός διαιρέτης του a μεγαλύτερος από $\sqrt{a}$ και αντιστρόφως. Από την Πρόταση 2.3.2 έχουμε

$$\sum_{d|a}\mu(d)=0.$$

Όμως

$$\sum_{d|a}\mu(d)=\sum_{d\in A}\mu(d)+\sum_{d\in B}\mu(d)=2\sum_{d\in A}\mu(d).$$

Άρα

$$\sum_{\{d|a:d<\sqrt{a}\}}\mu(d)=0.$$

11. Έστω $m,n\in\mathbb{N}$ με $(m,n)=1$. Θέλουμε να δείξουμε ότι

$$(-1)^{mn-1}=(-1)^{m-1}(-1)^{n-1}$$

δηλαδή ότι ο $mn-m-n+1=(m-1)(n-1)$ είναι άρτιος. Αυτό δεν θα μπορούσε να ισχύει μόνο αν οι m,n ήταν και οι δύο άρτιοι, το οποίο αποκλείεται αφού υποθέσαμε ότι $(m,n)=1$. Άρα η $f(n)=(-1)^{n-1}$ είναι πολλαπλασιαστική. Η συνάρτηση

$$h(n)=\sum_{k|n}(-1)^{k-1}\mu\left(\frac{n}{k}\right)=\sum_{k|n}f(k)\mu\left(\frac{n}{k}\right)$$

είναι πολλαπλασιαστική (γιατί οι f,μ είναι πολλαπλασιαστικές, έχουμε χρησιμοποιήσει αρκετές φορές αυτό το επιχείρημα). Υπολογίζουμε πρώτα την τιμή $h(p^k)$, όπου p πρώτος και $k\geq1$. Έχουμε

$$\begin{aligned}h(p^k)&=\mu(p^k)+(-1)^{p-1}\mu(p^{k-1})+\cdots+(-1)^{p^{k-1}-1}\mu(p)+(-1)^{p^k-1}\mu(1)\\&=(-1)^{p^{k-1}-1}(-1)+(-1)^{p^k-1}=(-1)^{p^{k-1}}+(-1)^{p^k-1}.\end{aligned}$$

Όμως αν ο p είναι περιττός πρώτος τότε ο p^{k-1} είναι περιττός και ο p^k-1 είναι άρτιος, ενώ αν $p=2$ και $k>1$ έχουμε το αντίθετο. Συνεπώς $h(p^k)=0$ εκτός αν $p=2$ και $k=1$, οπότε $h(2)=-2$. Αφού η h είναι πολλαπλασιαστική, για κάθε $n\geq3$ έχουμε $h(n)=0$. Τέλος $h(1)=(-1)^0\mu(1)=1$.

12. Έχουμε $d(n) = \sum_{k|n} U(k)$, όπου $U(k) = 1$ για $k \in \mathbb{N}$. Από τον τύπο αντιστροφής του Möbius παίρνουμε

$$1 = U(n) = \sum_{k|n} \mu(k) d\left(\frac{n}{k}\right).$$

Με εντελώς ανάλογο τρόπο η σχέση $\sigma(n) = \sum_{k|n} I(k)$, όπου $I(k) = k$, δίνει

$$n = I(n) = \sum_{k|n} \mu(k) \sigma\left(\frac{n}{k}\right).$$

13. Και τα δύο μέλη της προτεινόμενης ισότητας είναι πολλαπλασιαστικές συναρτήσεις του n και συνεπώς αρκεί να δείξουμε ότι ταυτίζονται όταν ο n είναι δύναμη πρώτου. Αν $n = p^r$ τότε

$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = 1 + \frac{(-1)^2}{p-1} = \frac{p}{p-1} = \frac{n}{\phi(n)}.$$

14. Παρατηρούμε ότι αν $1 \le k \le n$ τότε $(k, n) = 1$ αν και μόνο αν $(n - k, n) = 1$. Άρα

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} k = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} (n-k).$$

Έπεται ότι

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} k = \frac{1}{2}\left(\sum_{\substack{k=1 \\ (k,n)=1}}^{n} k + \sum_{\substack{k=1 \\ (k,n)=1}}^{n} (n-k) \right) = \frac{1}{2} \sum_{\substack{k=1 \\ (k,n)=1}}^{n} n = \frac{n\phi(n)}{2}.$$

15. Αν $n = p^r$ με p πρώτο και $r \ge 1$ τότε

$$\phi(n)d(n) = \phi(p^r)d(p^r) = p^{r-1}(p-1)(r+1) \ge p^{r-1}2(p-1) \ge p^{r-1} \cdot p = p^r = n.$$

Αν $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ γενικότερα τότε

$$\phi(n)d(n) = \phi(p_1^{r_1})d(p_1^{r_1}) \cdot \phi(p_2^{r_2})d(p_2^{r_2}) \cdots \phi(p_s^{r_s})d(p_s^{r_s}) \ge p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} = n.$$

16. Απάντηση: $n = 1, 3, 8, 10, 18, 24, 30$.

17. Έχουμε $n = 2^r 3^s m$ με $r, s \ge 1$ και $(m, 6) = 1$ οπότε $\phi(n) = \phi(2^r)\phi(3^s)\phi(m) = 2^{r-1} \cdot 2 \cdot 3^{s-1}\phi(m) \le 2^r 3^{s-1} m = n/3$.

18. Θα υποθέσουμε ότι $n = 2^a 3^b p_3^{k_3} \cdots p_r^{k_r}$, όπου $a, b \ge 0$ και $k_i > 0$, είναι η κανονική αναπαράσταση του n, και θα καταλήξουμε σε άτοπο. Αν $a, b > 0$, έχουμε

$$\phi(n) = 2^{a-1} 3^{b-1} \cdot 2 \cdot p_3^{k_3 - 1}(p_3 - 1) \cdots p_r^{k_r - 1}(p_r - 1),$$

και από την υπόθεση,

$$2^a 3^{b-1}(p_3 - 1) \cdots (p_r - 1) \mid 2^a 3^b p_3 \cdots p_r.$$

Όμως, η μεγαλύτερη δύναμη του 2 που διαιρεί το δεξιό μέλος είναι 2^a ενώ το αριστερό μέλος διαιρείται με 2^{a+1} αφού οι $p_3 - 1, \ldots, p_r - 1$ είναι άρτιοι (εξηγήστε).

Έστω ότι $n = 2^a p_3^{k_3} \cdots p_r^{k_r}$, όπου $a > 0$, $p_i \ge 5$ και $k_i > 0$. Όπως πριν, παίρνουμε

$$2^{a-1}(p_3 - 1) \cdots (p_r - 1) \mid 2^a p_3 \cdots p_r \Longrightarrow (p_3 - 1) \cdots (p_r - 1) \mid 2 p_3 \cdots p_r.$$

Όμως τότε $(p_3-1) \mid 2p_2 \cdots p_r$, το οποίο είναι άτοπο γιατί θα είχαμε $(p_3-1) \mid 2$ ή $(p_3-1) \mid p_j$ για κάποιον j, άτοπο αφού ο $p_3 - 1$ είναι άρτιος και μεγαλύτερος ή ίσος του 4.

Με ανάλογο τρόπο καταλήγουμε σε άτοπο αν υποθέσουμε ότι $n = 3^b p_3^{k_3} \cdots p_r^{k_r}$, όπου $b > 0$, $p_i \geq 5$ και $k_i > 0$ ή $n = p_3^{k_3} \cdots p_r^{k_r}$, όπου $p_i \geq 5$ και $k_i > 0$.

19. Έστω $1 < x < p_1 p_2 \cdots p_N$. Τότε ο x έχει τουλάχιστον έναν πρώτο διαιρέτη, ο οποίος είναι κάποιος από τους p_i, $i = 1, \ldots, N$ (έχουμε υποθέσει ότι αυτοί είναι όλοι οι πρώτοι). Άρα $(x, p_1 p_2 \ldots p_N) > 1$. Έπεται ότι

$$\phi(p_1 p_2 \ldots p_N) = 1$$

(από όλους τους $1 \leq x \leq p_1 p_2 \ldots p_N$, μόνο ο 1 είναι σχετικά πρώτος προς τον $p_1 p_2 \ldots p_N$). Από την άλλη πλευρά, η ϕ είναι πολλαπλασιαστική, άρα

$$\phi(p_1 p_2 \ldots p_N) = \phi(p_1)\phi(p_2) \ldots \phi(p_N) \geq \phi(2)\phi(3) = 1 \cdot 2 = 2$$

(οι πρώτοι δύο από τους $p_1, \ldots, p_N$ είναι οι $p_1 = 2$ και $p_2 = 3$). Καταλήξαμε σε άτοπο, άρα υπάρχουν άπειροι πρώτοι αριθμοί.

20. Χρησιμοποιώντας το γεγονός ότι οι ϕ, σ και d είναι πολλαπλασιαστικές συναρτήσεις, ελέγχουμε ότι οι $nd(n)$ και $h(n) = \sum_{k|n} \sigma(k)\phi\left(\frac{n}{k}\right)$ είναι πολλαπλασιαστικές συναρτήσεις. Αρκεί λοιπόν να ελέγξουμε ότι $h(p^r) = p^r d(p^r)$. Έχουμε

$$\begin{aligned} h(p^r) &= \sigma(1)\phi(p^r) + \sigma(p)\phi(p^{r-1}) + \cdots + \sigma(p^{r-1})\phi(p) + \sigma(p^r)\phi(1) \\ &= 1 \cdot p^{r-1}(p-1) + (1+p)p^{r-2}(p-1) + \cdots + (1+p+\cdots+p^{r-1})(p-1) \\ &\quad +(1+p+\cdots+p^r) \\ &= (p^r - p^{r-1}) + (p^r - p^{r-2}) + \cdots (p^r - 1) + (1+p+\cdots+p^{r-1}) + p^r \\ &= (r+1)p^r = p^r d(p^r). \end{aligned}$$

21. Αν ο n είναι πρώτος, τότε $\sigma(n) = n+1$, $\phi(n) = n-1$ και $d(n) = 2$. Άρα

$$\sigma(n) + \phi(n) = n + 1 + n - 1 = 2n = nd(n).$$

Αντίστροφα, αν υποθέσουμε ότι $\sigma(n) + \phi(n) = nd(n)$, από την προηγούμενη άσκηση έχουμε

$$\sigma(n) + \phi(n) = \sigma(n)\phi(1) + \sigma(1)\phi(n) = \sum_{k|n} \sigma(k)\phi\left(\frac{n}{k}\right).$$

Από την τελευταία ισότητα γίνεται φανερό ότι το άθροισμα στο δεξιό μέλος αποτελείται μόνο από τους δύο όρους που εμφανίζονται στο αριστερό μέλος (αλλιώς, το δεξιό μέλος θα ήταν γνήσια μεγαλύτερο). Όμως αυτό σημαίνει ότι ο n έχει μόνο δύο θετικούς διαιρέτες: τον 1 και τον n. Δηλαδή, ο n είναι πρώτος.

22. Γράφουμε $m = \prod_{i=1}^t p_i^{r_i}$ και $n = \prod_{i=1}^t p_i^{r_i}$ όπου $p_1,\ p_2, \ldots, p_t$ είναι διακεκριμένοι πρώτοι και r_i, s_i είναι μή αρνητικοί ακέραιοι. Τότε $d = (m,n) = \prod_{i=1}^t p_i^{\alpha_i}$ και $D = mn/d = \prod_{i=1}^t p_i^{\beta_i}$ όπου $\alpha_i = \min\{r_i, s_i\}$ και $\beta_i = \min\{r_i, s_i\}$. Παρατηρώντας ότι $\{r_i, s_i\} = \{\alpha_i, \beta_i\}$ για κάθε i, από την πολλαπλασιαστικότητα της f έχουμε

$$\begin{aligned} f(m)f(n) &= \prod_{i=1}^t f(p_i^{r_i}) \prod_{i=1}^t f(p_i^{s_i}) \\ &= \prod_{i=1}^t f(p_i^{\alpha_i}) \prod_{i=1}^t f(p_i^{\beta_i}) \\ &= f(d)f(D). \end{aligned}$$

Κεφάλαιο 4

Ο τετραγωνικός νόμος αντιστροφής

4.1 Η τάξη ενός ακεραίου ως προς n

Έστω $n > 1$ ένας φυσικός αριθμός. Το θεώρημα του Euler μας λέει ότι αν $a \in \mathbb{Z}$ και $(a, n) = 1$, τότε

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{4.1.1}$$

όπου ϕ είναι η συνάρτηση του Euler. Επομένως υπάρχουν πάντα δυνάμεις του a που είναι ισότιμες με 1 ως προς n.

Ορισμός 4.1.1. Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Η *τάξη* του a ως προς n είναι ο μικρότερος φυσικός k για τον οποίο $a^k \equiv 1 \pmod{n}$. Παρατηρήστε ότι ο 1 έχει τάξη 1 ως προς κάθε n.

Παράδειγμα 4.1.2. Ας υποθέσουμε ότι $n = 7$ και $a = 2$. Υπολογίζοντας τις δυνάμεις του 2 παίρνουμε τις ισοτιμίες

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1,\ 2^4 \equiv 2,\ 2^5 \equiv 4,\ 2^6 \equiv 1,\ \ldots$$

ως προς 7. Επομένως ο 2 έχει τάξη 3 ως προς 7.

Παρατηρήσεις 4.1.3. (α) Αν $a \equiv b \pmod{n}$ τότε $a^s \equiv b^s \pmod{n}$ για κάθε $s \geq 1$. Έπεται εύκολα ότι οι a και b έχουν την ίδια τάξη ως προς n.

(β) Αν $(a, n) = d > 1$, τότε η γραμμική ισοτιμία

$$ax \equiv 1 \pmod{n} \tag{4.1.2}$$

δεν έχει λύση. Αυτό όμως σημαίνει ότι δεν υπάρχει $s \geq 1$ τέτοιος ώστε $a^s \equiv 1 \pmod{n}$: γιατί τότε, ο $x = a^{s-1}$ θα ήταν λύση της (4.1.2). Αυτός είναι ο λόγος που απαιτούμε την $(a, n) = 1$ προκειμένου να ορίσουμε την τάξη του a ως προς n.

(γ) Στο παράδειγμα που δώσαμε παραπάνω, η τάξη του $a = 2$ ήταν $k = 3$, ενώ $\phi(n) = \phi(7) = 6$. Δηλαδή $k \mid \phi(n)$. Αυτό ισχύει τελείως γενικά όπως δείχνει το επόμενο θεώρημα.

Θεώρημα 4.1.4. *Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Αν ο a έχει τάξη k ως προς n, τότε*

$$a^s \equiv 1 \pmod{n} \text{ αν και μόνο αν } k \mid s. \tag{4.1.3}$$

Ειδικότερα, $k \mid \phi(n)$.

Απόδειξη. Αν $s = kx$ για κάποιον φυσικό x, τότε από την $a^k \equiv 1 \pmod{n}$ παίρνουμε

$$a^s = (a^k)^x \equiv 1^x = 1 \pmod{n}. \tag{4.1.4}$$

Αντίστροφα, ας υποθέσουμε ότι $a^s \equiv 1 \pmod{n}$. Γράφουμε $s = kq + r$ όπου $0 \leq r < k$. Τότε $a^{kq} \equiv 1 \pmod{n}$, άρα

$$a^r \equiv a^{kq} a^r = a^s \equiv 1 \pmod{n}. \tag{4.1.5}$$

Αφού η τάξη του a είναι k και $0 \leq r < k$, αναγκαστικά έχουμε $r = 0$. Δηλαδή ο s είναι πολλαπλάσιο του k.

Ειδικότερα, αφού $a^{\phi(n)} \equiv 1 \pmod{n}$ συμπεραίνουμε ότι $k \mid \phi(n)$. □

Παρατηρήσεις 4.1.5. (α) Σύμφωνα με το Θεώρημα 4.1.4, αν για παράδειγμα θέλουμε να βρούμε την τάξη του 2 ως προς 13, αρκεί να δοκιμάσουμε τους εκθέτες $s = 1, 2, 3, 4, 6, 12$ (τους διαιρέτες του $\phi(13) = 12$). Μπορείτε να επαληθεύσετε ότι η τάξη του 2 ως προς 13 είναι ίση με $k = 12$.

(β) Ένα «αντίστροφο ερώτημα» που προκύπτει από το Θεώρημα 4.1.4 είναι το εξής. Δίνονται $n > 1$ και $k \mid \phi(n)$. Είναι σωστό ότι υπάρχει πάντα $a \in \mathbb{Z}$ με $(a, n) = 1$ ο οποίος έχει τάξη ίση με k; Η απάντηση είναι αρνητική: αν $n = 12$ τότε $\phi(12) = 4$. Οι κλάσεις που είναι πρώτες προς τον 12 είναι οι $1, 5, 7, 11 \pmod{12}$. Παρατηρούμε ότι $1^1 \equiv 1 \pmod{12}$ και $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$. Δηλαδή ενώ $4 \mid \phi(12)$, δεν υπάρχει $a \in \mathbb{Z}$ ο οποίος να έχει τάξη ίση με 4.

Θεώρημα 4.1.6. *Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Αν ο a έχει τάξη k ως προς n, τότε $a^i \equiv a^j \pmod{n}$ αν και μόνο αν $i \equiv j \pmod{k}$.*

Απόδειξη. Υποθέτουμε πρώτα ότι $i > j$ και $a^i \equiv a^j \pmod{n}$. Τότε $n \mid a^j(a^{i-j} - 1)$ και αφού $(a^j, n) = 1$ βλέπουμε ότι $n \mid (a^{i-j} - 1)$. Αφού $a^{i-j} \equiv 1 \pmod{n}$, το Θεώρημα 4.1.4 δείχνει ότι $k \mid (j - i)$, δηλαδή $j \equiv i \pmod{k}$. Αντίστροφα, αν $i = j + kq$ τότε $a^i = (a^k)^q a^j \equiv 1^k a^j = a^j \pmod{n}$. □

Πόρισμα 4.1.7. *Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Αν ο a έχει τάξη k ως προς n, τότε οι $a, a^2, \ldots, a^k$ είναι ανισότιμοι* mod n.

Το επόμενο ερώτημα που θα μας απασχολήσει είναι αν μπορούμε αμέσως να υπολογίσουμε την τάξη του a^s ως προς n αν γνωρίζουμε την τάξη του a ως προς n.

Θεώρημα 4.1.8. *Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Αν ο a έχει τάξη k ως προς n, τότε η τάξη του a^s ως προς n ισούται με $k/(k, s)$.*

Απόδειξη. Γράφουμε $d = (k, s)$ και συμβολίζουμε με r την τάξη του a^s. Από το Λήμμα 1.4.1 υπάρχουν $k_1, s_1 \in \mathbb{N}$ με $(k_1, s_1) = 1$ τέτοιοι ώστε $k = k_1 d$ και $s = s_1 d$. Παρατηρούμε ότι

$$(a^s)^{k_1} = (a^{s_1 d})^{k/d} = (a^k)^{s_1} \equiv 1 \pmod{n}. \tag{4.1.6}$$

Από το Θεώρημα 4.1.4,

$$r \mid k_1 = \frac{k}{d} = \frac{k}{(k,s)}. \tag{4.1.7}$$

Από την άλλη πλευρά, αφού

$$a^{sr} = (a^s)^r \equiv 1 \pmod{n} \tag{4.1.8}$$

έχουμε $k \mid sr$ δηλαδή $k_1 d \mid s_1 dr$. Αυτό σημαίνει ότι $k_1 \mid s_1 r$ και αφού $(k_1, s_1) = 1$ συμπεραίνουμε ότι $k/(k,s) = k/d = k_1 \mid r$. □

Πόρισμα 4.1.9. *Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a,n) = 1$. Αν ο a έχει τάξη k ως προς n, τότε ο a^s έχει κι αυτός τάξη k ως προς n αν και μόνο αν $(k,s) = 1$.*

4.2 Πρωταρχικές ρίζες

Ορισμός 4.2.1. Έστω $n > 1$ και $a \in \mathbb{Z}$ με $(a,n) = 1$. Ο a λέγεται *πρωταρχική ρίζα* του n αν η τάξη του a ως προς n είναι ίση με $\phi(n)$.

Παρατήρηση 4.2.2. Είναι εύκολο να ελέγξετε ότι ο 3 είναι πρωταρχική ρίζα του 7. Η τάξη του είναι ίση με $6 = \phi(7)$. Γενικότερα, θα δούμε ότι αν ο n είναι πρώτος τότε έχει πρωταρχικές ρίζες.

Υπάρχουν σύνθετοι αριθμοί που έχουν πρωταρχικές ρίζες: για παράδειγμα, ο $9 = 3^2$ έχει πρωταρχική ρίζα τον 2. Θα δούμε όμως ότι οι «περισσότεροι» φυσικοί δεν έχουν πρωταρχικές ρίζες. Ακριβέστερα, οι μόνοι φυσικοί που έχουν πρωταρχικές ρίζες είναι οι $2, 4, p^k, 2p^k$ όπου p περιττός πρώτος και $k \geq 1$.

Πριν προχωρήσουμε στην απόδειξη αυτών των ισχυρισμών, ας δούμε μια απλή εφαρμογή των πρωταρχικών ριζών.

Πρόταση 4.2.3. *Αν $(a,n) = 1$ και ο a είναι πρωταρχική ρίζα του n, τότε οι ακέραιοι $a, a^2, \ldots, a^{\phi(n)}$ σχηματίζουν ένα πλήρες ανηγμένο σύστημα υπολοίπων ως προς n.*

Απόδειξη. Από το Πόρισμα 4.1.7 οι $a, a^2, \ldots, a^{\phi(n)}$ είναι ανισότιμοι ως προς n. Το πλήθος τους ισούται με $\phi(n)$ και από την $(a,n) = 1$ έπεται ότι είναι όλοι σχετικά πρώτοι προς τον n. Άρα, σχηματίζουν ένα πλήρες ανηγμένο σύστημα υπολοίπων ως προς n. □

Δείχνουμε πρώτα ότι κάθε πρώτος p έχει πρωταρχικές ρίζες. Η μέθοδος σχετίζεται με μια απλή συνέπεια του θεωρήματος του Lagrange.

Λήμμα 4.2.4. *Έστω p περιττός πρώτος και $d \mid (p-1)$. Τότε η ισοτιμία*

$$x^d - 1 \equiv 0 \pmod{p} \tag{4.2.1}$$

έχει ακριβώς d λύσεις.

Απόδειξη. Έχουμε $p-1=dk$ για κάποιον φυσικό k. Άρα

$$x^{p-1}-1=(x^d-1)g(x), \tag{4.2.2}$$

όπου $g(x)=x^{d(k-1)}+\cdots+x^d+1$ είναι ένα πολυώνυμο βαθμού $dk-d=p-1-d$. Από το μικρό θεώρημα του Fermat, η $x^{p-1}-1\equiv 0 \pmod p$ έχει ακριβώς $p-1$ λύσεις. Από το θεώρημα του Lagrange, η $g(x)\equiv 0 \pmod p$ έχει το πολύ $p-1-d$ λύσεις.

Όμως από την (4.2.2) βλέπουμε ότι κάθε λύση της $x^{p-1}-1\equiv 0 \pmod p$ που δεν είναι λύση της $g(x)\equiv 0 \pmod p$ είναι λύση της $x^d-1\equiv 0 \pmod p$ (χρησιμοποιήστε το γεγονός ότι ο p είναι πρώτος). Έπεται ότι η $x^d-1\equiv 0 \pmod p$ έχει τουλάχιστον $p-1-(p-1-d)=d$ λύσεις. Τέλος, από το Θεώρημα του Lagrange, το πλήθος των λύσεων της $x^d-1\equiv 0 \pmod p$ είναι το πολύ ίσο με d και αυτό ολοκληρώνει την απόδειξη. □

Θεώρημα 4.2.5. *Έστω p περιττός πρώτος και έστω $d \mid (p-1)$. Τότε υπάρχουν $\phi(d)$ ακέραιοι, ανισότιμοι ως προς p, οι οποίοι έχουν τάξη ίση με d.*

Απόδειξη. Για κάθε $d \mid (p-1)$ θέτουμε $\psi(d)$ το πλήθος των $x\in S_p:=\{1,\dots,p-1\}$ που έχουν τάξη ίση με d. Αφού $\phi(p)=p-1$, η τάξη κάθε στοιχείου x του S_p είναι διαιρέτης του $p-1$. Δηλαδή, οι διαιρέτες d του $p-1$ επάγουν μια διαμέριση του S_p. Με άλλα λόγια,

$$p-1=\sum_{d\mid p-1}\psi(d). \tag{4.2.3}$$

Από την άλλη πλευρά, το Θεώρημα 3.4.1 δείχνει ότι

$$p-1=\sum_{d\mid p-1}\phi(d). \tag{4.2.4}$$

Αν δείξουμε ότι $\psi(d)\le\phi(d)$ για κάθε $d\mid p-1$ τότε οι (4.2.3) και (4.2.4) δείχνουν ότι $\psi(d)=\phi(d)$ για κάθε $d\mid p-1$, δηλαδή τον ισχυρισμό του Θεωρήματος.

Διακρίνουμε δύο περιπτώσεις:

(α′) Αν $\psi(d)=0$ τότε προφανώς $\psi(d)\le\phi(d)$.

(β′) Έστω ότι $\psi(d)>0$. Τότε υπάρχει $a\in S_p$ ο οποίος έχει τάξη ίση με d. Οι φυσικοί $a,a^2,\dots,a^d$ είναι ανισότιμοι ως προς p και για κάθε $s=1,\dots,d$ έχουμε

$$(a^s)^d=(a^d)^s\equiv 1 \pmod p. \tag{4.2.5}$$

Δηλαδή, οι $a,a^2,\dots,a^d$ είναι όλες οι λύσεις της $x^d-1\equiv 0 \pmod p$.

Από τα παραπάνω έπεται ότι αν $x\in S_p$ και η τάξη του x ως προς p είναι ίση με d, τότε ο x είναι λύση της $x^d-1\equiv 0 \pmod p$ άρα πρέπει να ανήκει στην κλάση κάποιου a^s, $s=1,\dots,d$. Με άλλα λόγια, $\psi(d)$ είναι το πλήθος των a^s, $1\le s\le d$ που έχουν τάξη ίση με d. Όμως, το Θεώρημα 4.1.8 δείχνει ότι ο a^s έχει τάξη d αν και μόνο αν $d/(d,s)=d$, δηλαδή $(d,s)=1$. Το πλήθος των $1\le s\le d$ που ικανοποιούν την $(d,s)=1$ είναι εξ' ορισμού ίσο με $\phi(d)$. Άρα σε αυτή την περίπτωση έχουμε $\psi(d)=\phi(d)$. □

Θεώρημα 4.2.6. *Κάθε περιττός πρώτος p έχει πρωταρχικές ρίζες.*

Απόδειξη. Από το προηγούμενο θεώρημα υπάρχουν $\phi(p-1) = \phi(\phi(p))$ ακέραιοι, ανισότιμοι ως προς p, οι οποίοι έχουν τάξη ίση με $p-1$. Καθένας από αυτούς είναι πρωταρχική ρίζα του p. □

Το επόμενο θεώρημα δείχνει ποιοί φυσικοί αριθμοί έχουν πρωταρχικές ρίζες.

Θεώρημα 4.2.7. *Αν ο $n > 1$ έχει πρωταρχικές ρίζες, τότε $n = 2$ ή $n = 4$ ή $n = p^k$ ή $n = 2p^k$, όπου p περιττός πρώτος και $k \geq 1$.*

Απόδειξη. Θεωρούμε την κανονική αναπαράσταση $n = p_1^{k_1} \cdots p_r^{k_r}$ του n και θέτουμε $m_i = p_i^{k_i}$ για $i = 1, \ldots, r$. Επίσης θεωρούμε το ελάχιστο κοινό πολλαπλάσιο των $\phi(m_i)$

$$L = [\phi(m_1), \ldots, \phi(m_r)]. \tag{4.2.6}$$

Έχουμε

$$\phi(n) = \phi(m_1) \cdots \phi(m_r), \tag{4.2.7}$$

άρα $L \mid \phi(n)$.

Υποθέτουμε ότι ο a είναι πρωταρχική ρίζα του n. Παρατηρούμε ότι $(a, m_i) = 1$ για κάθε i, άρα $a^{\phi(m_i)} \equiv 1 \pmod{m_i}$ από το θεώρημα του Euler. Έπεται ότι $a^L \equiv 1 \pmod{m_i}$ για κάθε $i = 1, \ldots, r$ και αφού οι m_i είναι ανά δύο σχετικά πρώτοι συμπεραίνουμε ότι

$$a^L \equiv 1 \pmod{n}. \tag{4.2.8}$$

Από την άλλη πλευρά, ο a είναι πρωταρχική ρίζα του n άρα η τάξη του a ως προς n είναι $\phi(n)$. Από την (4.2.8) παίρνουμε $\phi(n) \mid L$ και συνεπώς

$$\phi(n) = \phi(m_1) \cdots \phi(m_r) = L = [\phi(m_1), \ldots, \phi(m_r)]. \tag{4.2.9}$$

Για να ισχύει η (4.2.9), οι $\phi(m_i)$ πρέπει να είναι ανά δύο σχετικά πρώτοι (γιατί;). Αυτός ο περιορισμός είναι πολύ ισχυρός. Πράγματι, αν ο n είχει δύο περιττούς πρώτους διαιρέτες p_i και p_j, τότε ο $\phi(m_i) = \phi(p_i^{k_i}) = p_i^{k_i - 1}(p_i - 1)$ θα ήταν άρτιος και ομοίως για τον $\phi(m_j)$. 'ρα ο n μπορεί να έχει μία από τις παρακάτω μορφές:

(i) $n = p^k$, όπου p περιττός πρώτος και $k \geq 1$.

(ii) $n = 2^s p^k$, όπου p περιττός πρώτος και $s, k \geq 1$. Αν όμως $s \geq 2$ τότε ο $\phi(2^s) = 2^{s-1}$ είναι άρτιος και δεν μπορεί να είναι σχετικά πρώτος με τον $\phi(p^k) = p^{k-1}(p-1)$. Δηλαδή η μόνη δυνατή περίπτωση εδώ είναι η $n = 2p^k$.

(iii) $n = 2^s$, όπου $s \geq 1$. Παρατηρούμε ότι οι $2, 4$ έχουν πρωταρχικές ρίζες: ο 1 είναι πρωταρχική ρίζα του 2 και ο 3 πρωταρχική ρίζα του 4 (γιατί;). Θα δείξουμε ότι αυτές είναι οι μόνες «δυνάμεις του 2» που έχουν πρωταρχικές ρίζες, αποδεικνύοντας ότι αν $s \geq 3$ τότε, για κάθε περιττό $a \in \mathbb{Z}$,

$$a^{\frac{\phi(2^s)}{2}} \equiv 1 \pmod{2^s} \tag{4.2.10}$$

(οι περιττοί ακέραιοι είναι οι μόνοι υποψήφιοι για πρωταρχικές ρίζες μιας δύναμης του 2). Παρατηρήστε ότι $\phi(2^s)/2 = 2^{s-2}$. Έστω a περιττός. Για $s = 3$ έχουμε

$$a^2 \equiv 1 \pmod{8} \tag{4.2.11}$$

(Άσκηση 7 β του Κεφαλαίου 1). Υποθέτουμε ότι

$$a^{2^{r-2}} \equiv 1 \pmod{2^r} \tag{4.2.12}$$

Τότε $a^{2^{r-2}} = 1 + t \cdot 2^r$, άρα

$$a^{2^{r-1}} = (1 + t \cdot 2^r)^2 = 1 + t \cdot 2^{r+1} + t^2 \cdot 2^{2r} \equiv 1 \pmod{2^{r+1}}. \tag{4.2.13}$$

Αυτό αποδεικνύει τον ισχυρισμό μας με επαγωγή.

Συνοψίζοντας τα συμπεράσματα των (i)-(iii) έχουμε ότι οι μόνοι φυσικοί $n > 1$ που θα μπορούσαν να έχουν πρωταρχικές ρίζες είναι οι $n = 2$ ή $n = 4$ ή $n = p^k$ ή $n = 2p^k$, όπου p περιττός πρώτος και $k \geq 1$. □

Παρατήρηση 4.2.8. Αντίστροφα αποδεικνύεται ότι οι $n = 2$, $n = 4$, $n = p^k$, $n = 2p^k$, όπου p περιττός πρώτος και $k \geq 1$, έχουν όλοι πρωταρχικές ρίζες (η απόδειξη παραλείπεται).

4.3 Τετραγωνικά υπόλοιπα και το σύμβολο του Legendre

Έστω p ένας περιττός πρώτος και έστω $a, b, c \in \mathbb{Z}$ με $(a, p) = 1$. Θεωρούμε την ισοτιμία

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{4.3.1}$$

Αφού $(a, p) = 1$ και ο p είναι περιττός, έχουμε $(4a, p) = 1$. Άρα η (4.3.1) είναι ισοδύναμη με την

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}. \tag{4.3.2}$$

Όμως

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac), \tag{4.3.3}$$

οπότε θέτοντας $y = 2ax + b$ και $s = b^2 - 4ac$ αναγόμαστε στην επίλυση της απλούστερης τετραγωνικής ισοτιμίας $y^2 \equiv s \pmod{p}$. Αν αυτή έχει λύσεις y, κατόπιν αρκεί να λύσουμε τη γραμμική ισοτιμία $2ax + b \equiv y \pmod{p}$ ως προς x.

Το πρόβλημα λοιπόν με το οποίο θα ασχοληθούμε σε αυτή την παράγραφο είναι το εξής. Δίνονται ένας περιττός πρώτος p και ένας ακέραιος a και θέλουμε να δούμε πόσες λύσεις έχει η ισοτιμία

$$x^2 \equiv a \pmod{p}. \tag{4.3.4}$$

Μπορούμε αμέσως να κάνουμε κάποιες απλές παρατηρήσεις. Από το θεώρημα του Lagrange, η (4.3.4) έχει το πολύ δύο λύσεις. Επίσης, αν $p \mid a$ τότε η μοναδική λύση της (4.3.4) είναι η $x \equiv 0 \pmod{p}$.

Αν τώρα $(a, p) = 1$ και υπάρχει x_0 τέτοιος ώστε $x_0^2 \equiv a \pmod{p}$, τότε

$$(p - x_0)^2 = p^2 - 2px_0 + x_0^2 \equiv x_0^2 \equiv a \pmod{p}. \tag{4.3.5}$$

Επίσης, οι x_0 και $p - x_0$ είναι ανισότιμοι mod p: αλλιώς θα είχαμε $p \mid 2x_0$, το οποίο είναι άτοπο αφού $(x_0, p) = 1$ και ο p είναι περιττός.

Ο προηγούμενος συλλογισμός δείχνει ότι αν $(a, p) = 1$ τότε η (4.3.4) έχει δύο λύσεις ή καμμία λύση.

Ορισμός 4.3.1. Έστω p ένας περιττός πρώτος και έστω $a \in \mathbb{Z}$ με $(a, p) = 1$. Λέμε ότι ο a είναι *τετραγωνικό υπόλοιπο* του p αν η $x^2 \equiv a \pmod{p}$ έχει (δύο) λύσεις. Αλλιώς, λέμε ότι ο a δεν είναι τετραγωνικό υπόλοιπο του p.

Παράδειγμα 4.3.2. Θέλουμε να δούμε ποιά είναι τα τετραγωνικά υπόλοιπα του 13. Αρκεί να βρούμε τα υπόλοιπα της διαίρεσης των τετραγώνων των $1, 2, \ldots, 12$ με το 13. Παρατηρούμε ότι

$$\begin{aligned} 1^2 \equiv 12^2 &\equiv 1 \pmod{13} \\ 2^2 \equiv 11^2 &\equiv 4 \pmod{13} \\ 3^2 \equiv 10^2 &\equiv 9 \pmod{13} \\ 4^2 \equiv 9^2 &\equiv 3 \pmod{13} \\ 5^2 \equiv 8^2 &\equiv 12 \pmod{13} \\ 6^2 \equiv 7^2 &\equiv 10 \pmod{13}. \end{aligned}$$

Άρα τα τετραγωνικά υπόλοιπα του 13 είναι οι $1, 3, 4, 9, 10, 12 \pmod{13}$. Παρατηρήστε ότι υπάρχουν $6 = \frac{13-1}{2}$ τετραγωνικά υπόλοιπα του 13. Επίσης, τα υπόλοιπα της διαίρεσης των $1^2, 2^2, \ldots, 6^2 = \left(\frac{13-1}{2}\right)^2$ με 13 είναι διαφορετικά ανά δύο (και μας δίνουν όλα τα τετραγωνικά υπόλοιπα του 13). Οι παρατηρήσεις αυτές ισχύουν τελείως γενικά, όπως δείχνει το επόμενο θεώρημα.

Θεώρημα 4.3.3. *Έστω p ένας περιττός πρώτος. Υπάρχουν ακριβώς $(p-1)/2$ ανισότιμα ως προς p τετραγωνικά υπόλοιπα του p, τα οποία αναπαρίστανται από τους*

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

Απόδειξη. Τα τετραγωνικά υπόλοιπα του p είναι οι ακέραιοι που ανήκουν στις κλάσεις υπολοίπων

$$1^2, 2^2, \ldots, (p-1)^2 \pmod{p} \tag{4.3.6}$$

Όμως η κλάση κάθε τετραγωνικού υπολοίπου εμφανίζεται ακριβώς δύο φορές στη λίστα (4.3.6). Συνεπώς υπάρχουν ακριβώς $(p-1)/2$ ανισότιμα ως προς p τετραγωνικά υπόλοιπα του p. Τέλος έχουμε $(p-i)^2 \equiv i^2 \pmod{p}$ για $1 \leq i \leq (p+1)/2$ οπότε οι $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ είναι αναγκαστικά ανά δύο ανισότιμοι ως προς p (διαφορετικά θα υπήρχαν λιγότερες από $(p-1)/2$ κλάσεις τετραγωνικών υπολοίπων ως προς p). □

Το επόμενο θεώρημα (*κριτήριο του Euler*) μας δίνει, τουλάχιστον θεωρητικά, έναν τρόπο να αποφασίζουμε αν ο a είναι ή δεν είναι τετραγωνικό υπόλοιπο του p.

Θεώρημα 4.3.4. *Έστω p ένας περιττός πρώτος και έστω $a \in \mathbb{Z}$ με $(a, p) = 1$. Ο a είναι τετραγωνικό υπόλοιπο του p αν και μόνο αν*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{4.3.7}$$

Σε αντίθετη περίπτωση, ισχύει αναγκαστικά η

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{4.3.8}$$

Απόδειξη. Υποθέτουμε πρώτα ότι ο a είναι τετραγωνικό υπόλοιπο του p. Τότε υπάρχει x με $(x, p) = 1$ ο οποίος ικανοποιεί την $x^2 \equiv a \pmod{p}$. Έπεται ότι

$$x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{4.3.9}$$

Όμως $x^{p-1} \equiv 1 \pmod p$ από το μικρό θεώρημα του Fermat, οπότε προκύπτει η (4.3.7). Για την αντίστροφη κατεύθυνση παρατηρούμε πρώτα ότι η

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p \tag{4.3.10}$$

έχει ακριβώς $p-1$ λύσεις από το μικρό θεώρημα του Fermat. Ορίζουμε

$$\begin{aligned} A &= \{a : 1 \le a \le p-1 \text{ και } a \text{ τετραγωνικό υπόλοιπο του } p\}, \\ B &= \{a : 1 \le a \le p-1 \text{ και } a \text{ όχι τετραγωνικό υπόλοιπο του } p\}, \\ C &= \{a : 1 \le a \le p-1 \text{ και } a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p\}, \\ D &= \{a : 1 \le a \le p-1 \text{ και } a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p\}. \end{aligned}$$

Παρατηρούμε ότι $A \cup B = \{1, \dots, p-1\}$ και καθένα από τα A, B έχει ακριβώς $(p-1)/2$ στοιχεία από το Θεώρημα 4.3.3. Από την (4.3.10) γίνεται φανερό ότι $C \cup D = \{1, \dots, p-1\}$: αν $1 \le a \le p-1$ τότε

$$p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1), \tag{4.3.11}$$

άρα

$$p \mid a^{\frac{p-1}{2}} - 1 \text{ ή } p \mid a^{\frac{p-1}{2}} + 1 \tag{4.3.12}$$

και, επιπλέον, μόνο μία από τις παραπάνω σχέσεις μπορεί να ισχύει, αλλιώς θα είχαμε $p \mid 2$ (γιατί;) το οποίο είναι αδύνατο. Επίσης, το θεώρημα του Lagrange μας εξασφαλίζει ότι καθένα από τα C, D έχει το πολύ $(p-1)/2$ στοιχεία. Συνδυάζοντας με τα προηγούμενα συμπεραίνουμε ότι καθένα από τα C, D έχει ακριβώς $(p-1)/2$ στοιχεία (εναλλακτικά, ο τελευταίος ισχυρισμός είναι άμεση συνέπεια του Λήμματος 4.2.4).

Τέλος, από το πρώτο μέρος της απόδειξης έχουμε $A \subseteq C$, άρα $D \subseteq B$. Συγκρίνοντας πληθαρίθμους παίρνουμε $A = C$ και $B = D$ που είναι ακριβώς το ζητούμενο. □

Ορισμός 4.3.5. Έστω p ένας περιττός πρώτος και έστω $a \in \mathbb{Z}$ με $(a, p) = 1$. Το *σύμβολο του Legendre* $\left(\frac{a}{p}\right)$ ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{αν ο } a \text{ είναι τετραγωνικό υπόλοιπο του } p \\ -1, & \text{αν ο } a \text{ δεν είναι τετραγωνικό υπόλοιπο του } p \end{cases}.$$

Αν $p \mid a$ θέτουμε $\left(\frac{a}{p}\right) = 0$. Με αυτή τη σύμβαση, για κάθε $a \in \mathbb{Z}$ ο αριθμός $1 + \left(\frac{a}{p}\right)$ ισούται με το πλήθος των λύσεων της $x^2 \equiv a \pmod p$.

Οι βασικές ιδιότητες του συμβόλου Legendre αποδεικνύονται στην επόμενη πρόταση.

Πρόταση 4.3.6. *Έστω p ένας περιττός πρώτος και έστω $a, b \in \mathbb{Z}$ με $(a, p) = (b, p) = 1$. Ισχύουν τα εξής:*

(i) *Αν $a \equiv b \pmod p$ τότε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) $\left(\frac{a^2}{p}\right) = 1$.

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

(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(v) $\left(\frac{1}{p}\right) = 1$ *και* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Απόδειξη. *(i)* Αν $a \equiv b \pmod p$) τότε οι ισοτιμίες $x^2 \equiv a \pmod p$ και $x^2 \equiv b \pmod p$ έχουν ακριβώς τις ίδιες λύσεις, δηλαδή ο a είναι τετραγωνικό υπόλοιπο του p αν και μόνο αν ο b είναι τετραγωνικό υπόλοιπο του p.

(ii) Η $x^2 \equiv a^2 \pmod p$ έχει προφανή λύση την $x = a$. Αφού $(a, p) = 1$ έχουμε και $(a^2, p) = 1$. Άρα ο a^2 είναι τετραγωνικό υπόλοιπο του p.

(iii) Έχουμε $\left(\frac{a}{p}\right) = 1$ αν και μόνο αν ο a είναι τετραγωνικό υπόλοιπο του p, το οποίο από το κριτήριο του Euler ισχύει αν και μόνο αν $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Εντελώς ανάλογα, έχουμε $\left(\frac{a}{p}\right) = -1$ αν και μόνο αν $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Σε κάθε περίπτωση,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p. \tag{4.3.13}$$

(iv) Χρησιμοποιώντας το προηγούμενο συμπέρασμα βλέπουμε ότι

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p. \tag{4.3.14}$$

Αφού

$$p \mid \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{ και } \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \in \{-2, 0, 2\} \tag{4.3.15}$$

αναγκαστικά έχουμε

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{4.3.16}$$

(v) Η πρώτη ισότητα είναι συνέπεια του (ii) αφού $1 = 1^2$. Για τη δεύτερη παρατηρούμε ότι

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p \tag{4.3.17}$$

και χρησιμοποιούμε όπως πριν το γεγονός ότι

$$p \mid \left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} \in \{-2, 0, 2\} \tag{4.3.18}$$

και ο p είναι περιττός. □

Οι ιδιότητες που αποδείξαμε στην Πρόταση 4.3.6 είναι πολύ χρήσιμες για τον υπολογισμό συμβόλων του Legendre.

Παράδειγμα 4.3.7. Θέλουμε να δούμε αν η ισοτιμία $x^2 \equiv -38 \pmod{13}$ έχει λύσεις. Προσπαθούμε να υπολογίσουμε το

$$\left(\frac{-38}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{38}{13}\right) = (-1)^{\frac{13-1}{2}}\left(\frac{38}{13}\right) = \left(\frac{38}{13}\right). \tag{4.3.19}$$

Ως εδώ χρησιμοποιήσαμε τις ιδιότητες (iv) και (v). Τώρα, χρησιμοποιώντας την (i) παίρνουμε

$$\left(\frac{38}{13}\right) = \left(\frac{12}{13}\right) \tag{4.3.20}$$

και χρησιμοποιώντας τις (iv) και (ii) βλέπουμε ότι

$$\left(\frac{12}{13}\right) = \left(\frac{2^2 \cdot 3}{13}\right) = \left(\frac{2^2}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right). \tag{4.3.21}$$

Αρκεί λοιπόν να υπολογίσουμε το $\left(\frac{3}{13}\right)$. Όμως,

$$\left(\frac{3}{13}\right) \equiv 3^6 = (27)^2 \equiv 1 \pmod{13}, \tag{4.3.22}$$

άρα

$$\left(\frac{-38}{13}\right) = \left(\frac{3}{13}\right) = 1, \tag{4.3.23}$$

δηλαδή η ισοτιμία έχει δύο λύσεις.

Το επόμενο θεώρημα (*Λήμμα του Gauss*) δίνει μια άλλη ερμηνεία στο σύμβολο του Legendre.

Θεώρημα 4.3.8. *Έστω p ένας περιττός πρώτος και a ένας ακέραιος με $(a,p)=1$. Θεωρούμε το σύνολο*

$$S = \left\{a, 2\cdot a, \ldots, \frac{p-1}{2}\cdot a\right\}. \tag{4.3.24}$$

Αν n είναι το πλήθος των στοιχείων του S που αφήνουν υπόλοιπο μεγαλύτερο από $p/2$ στη διαίρεσή τους με τον p, τότε

$$\left(\frac{a}{p}\right) = (-1)^n. \tag{4.3.25}$$

Απόδειξη. Είναι εύκολο να ελέγξετε ότι οι $a, 2\cdot a, \ldots, \frac{p-1}{2}\cdot a$ είναι πρώτοι προς τον p και ανισότιμοι ως προς p. Επομένως τα υπόλοιπα της διαίρεσής τους με p χωρίζονται σε δύο ομάδες:

(α′) τα $r_1, \ldots, r_m$ τα οποία ικανοποιούν την $0 < r_i < p/2$.

(β′) τα $s_1, \ldots, s_n$ τα οποία ικανοποιούν την $p/2 < s_j < p$

(ο $p/2$ δεν είναι ακέραιος, άρα δεν μπορεί να είναι υπόλοιπο). Οι r_i και s_j ανήκουν σε διαφορετικές κλάσεις ως προς p, άρα

$$m + n = \frac{p-1}{2}, \tag{4.3.26}$$

όσος δηλαδή είναι ο πληθάριθμος του S. Θεωρούμε τώρα τους αριθμούς $r_i, p - s_j$, οι οποίοι ανήκουν όλοι στο σύνολο $\{1, \ldots, (p-1)/2\}$. Παρατηρούμε ότι

$$r_i \neq p - s_j \tag{4.3.27}$$

για κάθε $i = 1, \ldots, m$ και $j = 1, \ldots, n$. Πράγματι, υπάρχουν $u, v \in \{1, \ldots, (p-1)/2\}$ τέτοιοι ώστε $r_i \equiv ua \pmod{p}$ και $s_j \equiv va \pmod{p}$. Αν $r_i = p - s_j$, τότε

$$p = r_i + s_j \mid (u+v)a \tag{4.3.28}$$

και αφού $(a,p)=1$ πρέπει να ισχύει η $p \mid (u+v)$, το οποίο αποκλείεται αφού $2 \leq u+v \leq p-1$. Έπεται ότι το σύνολο $\{r_1,\ldots,r_m,p-s_1,\ldots,p-s_n\}$ συμπίπτει με το $\{1,\ldots,(p-1)/2\}$. Αυτό έχει ως συνέπεια (γιατί;) την

$$\left(\frac{p-1}{2}\right)! = r_1\cdots r_m(p-s_1)\cdots(p-s_n) \equiv (-1)^n r_1\cdots r_m s_1\cdots s_n \pmod p. \tag{4.3.29}$$

Από την άλλη πλευρά, οι r_i, s_j αντιστοιχούν στις κλασεις υπολοίπων των στοιχείων του S. Άρα

$$r_1\cdots r_m s_1\cdots s_n \equiv \prod_{u=1}^{(p-1)/2}(ua) = a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p. \tag{4.3.30}$$

Από τις (4.3.29) και (4.3.30) βλέπουμε ότι

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p \tag{4.3.31}$$

και αφού $\left(\left(\frac{p-1}{2}\right)!,p\right)=1$ παίρνουμε

$$(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod p. \tag{4.3.32}$$

Έπεται ότι

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p \tag{4.3.33}$$

από την Πρόταση 4.3.6(iii). □

Μια πρώτη εφαρμογή του Λήμματος του Gauss δίνει το επόμενο θεώρημα, στο οποίο υπολογίζεται η τιμή του συμβόλου $\left(\frac{2}{p}\right)$.

Θεώρημα 4.3.9. *Αν p είναι περιττός πρώτος τότε*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{4.3.34}$$

Δηλαδή, $\left(\frac{2}{p}\right)=1$ αν $p=8k\pm1$ και $\left(\frac{2}{p}\right)=-1$ αν $p=8k\pm3$.

Απόδειξη. Από το Λήμμα του Gauss έχουμε

$$\left(\frac{2}{p}\right) = (-1)^n, \tag{4.3.35}$$

όπου n το πλήθος των $x \in S=\{2,4,6,\ldots,p-1\}$ που αφήνουν υπόλοιπο μεγαλύτερο από $p/2$ στη διαίρεσή τους με p. Αφού όλα τα στοιχεία του S ικανοποιούν την $0<x<p$, αρκεί να μετρήσουμε πόσα από αυτά είναι μεγαλύτερα από $p/2$. Δηλαδή ρωτάμε για ποιά $1\leq k\leq (p-1)/2$ ισχύει $2k>p/2$ ή ισοδύναμα $k>p/4$. Προφανώς,

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right]. \tag{4.3.36}$$

Διακρίνουμε τέσσερις περιπτώσεις (ο p είναι περιττός):

(α′) Αν $p = 8k + 1$, τότε

$$n = \frac{8k}{2} - \left[\frac{8k+1}{4}\right] = 4k - 2k = 2k.$$

(β′) Αν $p = 8k + 3$, τότε

$$n = \frac{8k+2}{2} - \left[\frac{8k+3}{4}\right] = (4k+1) - 2k = 2k + 1.$$

(γ′) Αν $p = 8k + 5$, τότε

$$n = \frac{8k+4}{2} - \left[\frac{8k+5}{4}\right] = (4k+2) - (2k+1) = 2k + 1.$$

(δ′) Αν $p = 8k + 7$, τότε

$$n = \frac{8k+6}{2} - \left[\frac{8k+7}{4}\right] = (4k+3) - (2k+1) = 2k + 2.$$

Επομένως $(-1)^n = 1$ όταν $p = 8k \pm 1$ και $(-1)^n = -1$ όταν $p = 8k \pm 3$. Τέλος, παρατηρήστε ότι ο $\frac{p^2-1}{8}$ είναι άρτιος όταν $p = 8k \pm 1$ και περιττός όταν $p = 8k \pm 3$, οπότε το συμπέρασμα μπορεί να διατυπωθεί ενιαία μέσω της (4.3.34). □

Κλείνουμε την παράγραφο αυτή με μια εφαρμογή στο εξής πρόβλημα. Ποιοι πρώτοι γράφονται ως άθροισμα των τετραγώνων δύο ακεραίων; Για παράδειγμα οι $2 = 1^2+1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$ και $17 = 1^2 + 4^2$ έχουν αυτή την ιδιότητα ενώ οι $3, 7, 11$ και 19 όχι.

Λήμμα 4.3.10. *Αν p είναι περιττός ακέραιος και $p = a^2 + b^2$ για ακεραίους a, b τότε $p \equiv 1 \pmod 4$.*

Απόδειξη. Προφανώς ένας από τους a, b είναι άρτιος και ο άλλος περιττός. Έστω ότι ο a είναι άρτιος και ο b περιττός. Τότε $a^2 \equiv 0 \pmod 4$ και $b^2 \equiv 1 \pmod 4$ οπότε $p = a^2 + b^2 \equiv 1 \pmod 4$. □

Για πρώτους p ισχύει και το αντίστροφο του Λήμματος 4.3.10.

Θεώρημα 4.3.11. *Ένας περιττός πρώτος p γράφεται στη μορφή $p = a^2 + b^2$ για ακεραίους a, b αν και μόνο αν $p \equiv 1 \pmod 4$.*

Απόδειξη. Έστω ότι $p \equiv 1 \pmod 4$. Παρατηρούμε ότι ο $(p-1)/2$ είναι άρτιος και συνεπώς

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1,$$

οπότε ο -1 είναι τετραγωνικό υπόλοιπο του p. Άρα υπάρχει $t \in \mathbb{Z}$ με $t^2 \equiv -1 \pmod p$. Θεωρούμε τους ακεραίους $xt - y$ με $x, y \in \{0, 1, \ldots, [\sqrt{p}]\}$. Τα δυνατά ζεύγη (x, y) είναι σε πλήθος $([\sqrt{p}] + 1])^2 > (\sqrt{p})^2 = p$ ενώ υπάρχουν p κλάσεις υπολοίπων ως προς p. Επομένως για δύο διαφορετικά ζεύγη (x_1, y_1) και (x_2, y_2) έχουμε

$$x_1 t - y_1 \equiv x_2 t - y_2 \pmod p.$$

Υποθέτοντας ότι $x_1 \geq x_2$ έχουμε $0 \leq x_1 - x_2 \leq [\sqrt{p}] < \sqrt{p}$ και ομοίως $|y_1 - y_2| < \sqrt{p}$. Έστω $x = x_1 - x_2$ και $y = y_1 - y_2$. Από την επιλογή των x_i, y_i και τα παραπάνω έχουμε $xt \equiv y \pmod{p}$ και $0 < x^2 + y^2 < 2p$. Από την επιλογή του t έχουμε $x^2 + y^2 \equiv -x^2t^2 + y^2 \equiv 0 \pmod{p}$. Όμως ο p είναι το μοναδικό πολλαπλάσιο του p μεταξύ του 0 και του $2p$ οπότε αναγκαστικά $x^2 + y^2 = p$. Το αντίστροφο προκύπτει από το Λήμμα 4.3.10. □

4.4 Ο τετραγωνικός νόμος αντιστροφής

Έστω p και q δύο περιττοί πρώτοι. Τότε τα σύμβολα του Legendre $\left(\frac{p}{q}\right)$ και $\left(\frac{q}{p}\right)$ ορίζονται και τα δύο. Ο *τετραγωνικός νόμος αντιστροφής* μας επτρέπει να υπολογίζουμε το ένα από τα δύο αν γνωρίζουμε την τιμή του άλλου. Ισχύει πάντα η ισότητα

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{4.4.1}$$

Όπως θα δούμε, συνδυάζοντας αυτό το αποτέλεσμα με τα αποτελέσματα της προηγούμενης παραγράφου, μπορούμε εύκολα και γρήγορα να αποφασίζουμε αν ο a είναι τετραγωνικό υπόλοιπο του περιττού πρώτου p για κάθε ακέραιο a με $(a, p) = 1$.

Θα δώσουμε μια απόδειξη του τετραγωνικού νόμου αντιστροφής που βασίζεται στην εξής συνέπεια του Λήμματος του Gauss.

Λήμμα 4.4.1. *Αν p είναι ένας περιττός πρώτος και a είναι ένας περιττός ακέραιος με $(a, p) = 1$, τότε*

$$\left(\frac{a}{p}\right) = (-1)^N, \tag{4.4.2}$$

όπου

$$N = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right]. \tag{4.4.3}$$

Απόδειξη. Όπως στην απόδειξη του Θεωρήματος 4.3.8, θεωρούμε το σύνολο

$$S = \left\{a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a\right\}. \tag{4.4.4}$$

Για κάθε $k = 1, \ldots, (p-1)/2$ γράφουμε

$$ka = q_k p + t_k, \tag{4.4.5}$$

όπου $q_k \in \mathbb{Z}$ και $1 \leq t_k \leq p - 1$. Τότε,

$$\left[\frac{ka}{p}\right] = q_k \tag{4.4.6}$$

για κάθε k, άρα

$$ka = [ka/p]\, p + t_k. \tag{4.4.7}$$

Με το συμβολισμό της απόδειξης του Θεωρήματος 4.3.8, αν $t_k < p/2$ τότε ο t_k είναι ένας από τους $r_1, \ldots, r_m$, ενώ αν $t_k > p/2$, ο t_k είναι ένας από τους $s_1, \ldots, s_n$.

Προσθέτοντας λοιπόν κατά μέλη παίρνουμε

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} [ka/p]\, p + \sum_{i=1}^{n} r_i + \sum_{j=1}^{n} s_j. \tag{4.4.8}$$

Όμως, στην απόδειξη του Θεωρήματος 4.3.8 είδαμε ότι οι $r_1, \ldots, r_m, p-s_1, \ldots, p-s_n$ είναι μια αναδιάταξη των $1, 2, \ldots, (p-1)/2$. Άρα

$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} (p - s_j) = pn + \sum_{i=1}^{m} r_i - \sum_{j=1}^{n} s_j. \tag{4.4.9}$$

Αφαιρώντας τις δύο τελευταίες ισότητες κατά μέλη, παίρνουμε

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p \left(\sum_{k=1}^{(p-1)/2} [ka/p] - n \right) + 2 \sum_{j=1}^{n} s_j. \tag{4.4.10}$$

Τώρα χρησιμοποιούμε το γεγονός ότι οι p και a είναι περιττοί: παίρνοντας κλάσεις ως προς 2 στην (4.4.10) έχουμε

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2} [ka/p] - n \right) \pmod 2, \tag{4.4.11}$$

δηλαδή

$$n \equiv N = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p} \right] \pmod 2. \tag{4.4.12}$$

Άρα

$$\left(\frac{a}{p} \right) = (-1)^n = (-1)^N, \tag{4.4.13}$$

όπου η πρώτη ισότητα είναι ακριβώς το συμπέρασμα του Θεωρήματος 4.3.8. □

Θεώρημα 4.4.2 (Τετραγωνικός νόμος αντιστροφής, Gauss)**.** *Αν p και q είναι διακεκριμένοι περιττοί πρώτοι, τότε*

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}. \tag{4.4.14}$$

Απόδειξη. Θεωρούμε το ορθογώνιο στο xy-επίπεδο που έχει κορυφές τα $(0,0)$, $(p/2,0)$, $(0,q/2)$ και $(p/2,q/2)$. Με R συμβολίζουμε το εσωτερικό του ορθογωνίου (δεν συμπεριλαμβάνονται οι πλευρές του).

Μετράμε το πλήθος των σημείων (n,m) με ακέραιες συντεταγμένες τα οποία ανήκουν στο R. Αφού οι p και q είναι περιττοί, έχουμε $(n,m) \in R$ αν και μόνο αν ικανοποιούνται οι $1 \le n \le (p-1)/2$ και $1 \le m \le (q-1)/2$. Δηλαδή το πλήθος αυτών των σημείων είναι

$$L = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{4.4.15}$$

Τώρα θεωρούμε τη διαγώνιο του R που συνδέει τα $(0,0)$ και $(p/2,q/2)$. Η εξίσωση αυτής της ευθείας είναι $y = (q/p)x$, δηλαδή $py = qx$. Αν κάποιο από τα σημεία (n,m)

ανήκε στη διαγώνιο, θα είχαμε $pm = qn$. Αφού $(p, q) = 1$ θα παίρναμε $q \mid m$ και $p \mid n$, το οποίο είναι αδύνατο αφού $1 \leq n \leq (p-1)/2$ και $1 \leq m \leq (q-1)/2$. Άρα τα σημεία (n, m) ανήκουν σε ένα από τα δύο τρίγωνα T_1 (κάτω από τη διαγώνιο) και T_2 (πάνω από τη διαγώνιο) στα οποία χωρίζει η διαγώνιος το R.

Τώρα, ξαναμετράμε τα ακέραια σημεία (n, m) του R ως εξής. Για κάθε σημείο $(k, 0)$, $1 \leq k \leq (p-1)/2$, τα ακέραια σημεία που βρίσκονται στην κατακόρυφη που ορίζει το $(k, 0)$ και μέσα στο T_1 είναι εκείνα τα (k, y) για τα οποία $0 < y < kq/p$. Άρα, το πλήθος τους είναι ίσο με $[kq/p]$. Προσθέτοντας ως προς k βλέπουμε ότι το πλήθος των ακεραίων σημείων στο T_1 ισούται με

$$\sum_{k=1}^{(p-1)/2} [kq/p]. \tag{4.4.16}$$

Εντελώς ανάλογα βλέπουμε ότι το πλήθος των ακεραίων σημείων στο T_2 ισούται με

$$\sum_{l=1}^{(q-1)/2} [lp/q]. \tag{4.4.17}$$

Άρα, το πλήθος L των ακεραίων σημείων στο R ικανοποιεί την

$$L = \frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} [kq/p] + \sum_{l=1}^{(q-1)/2} [lp/q]. \tag{4.4.18}$$

Από το Λήμμα 4.4.1 βλέπουμε ότι

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\sum_{l=1}^{(q-1)/2}[lp/q]}(-1)^{\sum_{k=1}^{(p-1)/2}[kq/p]} \\ &= (-1)^{\sum_{l=1}^{(q-1)/2}[lp/q]+\sum_{k=1}^{(p-1)/2}[kq/p]} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \end{aligned}$$

Αυτός είναι ακριβώς ο τετραγωνικός νόμος αντιστροφής. □

Παράδειγμα 4.4.3. Υπολογίζουμε το σύμβολο του Legendre $\left(\frac{196}{23}\right)$: Διαδοχικά έχουμε

$$\left(\frac{196}{23}\right) = \left(\frac{12}{23}\right) \tag{4.4.19}$$

γιατί $196 = 23 \cdot 8 + 12$, και

$$\left(\frac{12}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{3}{23}\right) = \left(\frac{3}{23}\right). \tag{4.4.20}$$

Αρκεί λοιπόν να υπολογίσουμε το $\left(\frac{3}{23}\right)$. Από τον τετραγωνικό νόμο αντιστροφής,

$$\left(\frac{3}{23}\right)\left(\frac{23}{3}\right) = (-1)^{11} = -1. \tag{4.4.21}$$

Επίσης,

$$\left(\frac{23}{3}\right) = \left(\frac{2}{3}\right) \equiv 2 \equiv -1 \pmod 3 \tag{4.4.22}$$

δηλαδή

$$\left(\frac{23}{3}\right) = -1. \tag{4.4.23}$$

Άρα,

$$\left(\frac{196}{23}\right) = (-1)\left(\frac{23}{3}\right) = 1. \tag{4.4.24}$$

4.5 Ασκήσεις

1. (α) Βρείτε όλα τα δυνατά υπόλοιπα του $3^n \pmod 8$ για $n \in \mathbb{N}$.

(β) Βρείτε όλα τα ζεύγη (m, n) μη αρνητικών ακεραίων για τα οποία ισχύει $2^m - 3^n = 1$.

2. Αποδείξτε τις παρακάτω προτάσεις:

(α) Αν ο a έχει τάξη $2k$ ως προς τον περιττό πρώτο p, τότε $a^k \equiv -1 \pmod p$.

(β) Αν ο a έχει τάξη $n-1$ ως προς τον n, τότε ο n είναι πρώτος.

3. Έστω $n \geq 1$. Δείξτε ότι όλοι οι περιττοί πρώτοι διαιρέτες του n^2+1 είναι της μορφής $4k+1$.

4. Βρείτε μια πρωταρχική ρίζα του 17.

5. Έστω r μια πρωταρχική ρίζα του n. Δείξτε ότι ο r^k είναι πρωταρχική ρίζα του n αν και μόνο αν $(k, \phi(n)) = 1$.

6. Έστω r μια πρωταρχική ρίζα του περιττού πρώτου p. Δείξτε ότι:

(α) Αν $p \equiv 1 \pmod 4$ τότε ο $-r$ είναι επίσης πρωταρχική ρίζα του p.

(β) Αν $p \equiv 3 \pmod 4$ τότε ο $-r$ έχει τάξη $(p-1)/2$ ως προς p.

7. Να λυθούν οι τετραγωνικές ισοτιμίες

$$x^2 + 7x + 10 \equiv 0 \pmod{11}$$

και

$$5x^2 + 6x + 1 \equiv 0 \pmod{23}.$$

8. Αν ο $p = 2^k + 1$ είναι πρώτος, δείξτε ότι κάθε ακέραιος που δεν είναι τετραγωνικό υπόλοιπο του p είναι πρωταρχική ρίζα του p.

9. Υπολογίστε την τιμή των συμβόλων του Legendre

$$\left(\frac{19}{23}\right), \left(\frac{-23}{59}\right), \left(\frac{20}{31}\right), \left(\frac{18}{43}\right), \left(\frac{-72}{131}\right).$$

10. Έστω p ένας περιττός πρώτος και a ένας ακέραιος με $(a, p) = 1$. Δείξτε ότι η Διοφαντική εξίσωση

$$x^2 + py + a = 0$$

έχει ακέραια λύση αν και μόνο αν $\left(\frac{-a}{p}\right) = 1$.

11. (α) Έστω p ένας περιττός πρώτος και έστω $a, b \in \mathbb{Z}$ πρώτοι προς τον p. Δείξτε ότι τουλάχιστον ένας από τους a, b και ab είναι τετραγωνικό υπόλοιπο του p.

(β) Δείξτε ότι για κάθε πρώτο p υπάρχει $n \in \mathbb{N}$ τέτοιος ώστε

$$p \mid (n^2-2)(n^2-3)(n^2-6).$$

12. Αν ο περιττός πρώτος p ικανοποιεί την $p \equiv 1 \pmod 4$, δείξτε ότι

$$\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) = 0.$$

Υπόδειξη: $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$.

13. Έστω p ένας περιττός πρώτος. Αν $\left(\frac{a}{p}\right) = -1$, δείξτε ότι

$$\sum_{k \mid a} k^{\frac{p-1}{2}} \equiv 0 \pmod p.$$

14. Αν οι p και q είναι περιττοί πρώτοι και ικανοποιούν την $p = q + 4x$ για κάποιον ακέραιο x, δείξτε ότι

$$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right).$$

15. Να λυθεί η τετραγωνική ισοτιμία $x^2 \equiv 11 \pmod{35}$.

16. Να βρεθούν όλοι οι περιττοί πρώτοι p για τους οποίους $\left(\frac{-3}{p}\right) = 1$.

17. Να βρεθούν όλοι οι περιττοί πρώτοι που έχουν τετραγωνικό υπόλοιπο τον 5.

18. Έστω p ένας περιττός πρώτος. Αν $p \equiv 1 \pmod 4$, δείξτε ότι

$$\sum_{k=1}^{p-1} k \left(\frac{k}{p}\right) = 0$$

και

$$\sum_{\substack{k=1 \\ (k/p)=1}}^{p-1} k = \frac{p(p-1)}{4}.$$

19. Έστω p πρώτος αριθμός. Αν $p \equiv 3 \pmod 4$ δείξτε ότι

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

Υπόδειξη: $\left(\frac{p-k}{p}\right) = -\left(\frac{k}{p}\right)$.

20. Δείξτε ότι η τάξη του 2 ως προς 5^n είναι ίση με $4 \cdot 5^{n-1}$ για κάθε $n \in \mathbb{N}$.

Υποδείξεις - απαντήσεις

1. (α) Τα δυνατά υπόλοιπα είναι τα $1, 3$. Πράγματι για $n \in \mathbb{N}$ έχουμε $3^{2n} = 9^n \equiv 1^n = 1 \pmod 8$ και $3^{2n+1} = 3 \cdot 3^{2n} \equiv 3 \cdot 1 = 3 \pmod 8$.
(β) Αν $m \geq 3$ τότε $3^n = 2^m - 1 \equiv -1 \equiv 7 \pmod 8$, το οποίο είναι αδύνατο από το (α). Συνεπώς $m \leq 2$ οπότε οι μόνες λύσεις είναι οι $(m, n) = (1, 0)$ και $(2, 1)$.

2. (α) Από την υπόθεση έχουμε

$$p \mid a^{2k} - 1 = (a^k - 1)(a^k + 1).$$

Όμως ο p δεν μπορεί να διαιρεί τον $a^k - 1$ (ο a θα είχε τάξη μικρότερη ή ίση του k ενώ έχουμε υποθέσει ότι η τάξη του ως προς p είναι ίση με $2k$). Άρα $p \mid a^k + 1$, το οποίο σημαίνει ότι $a^k \equiv -1 \pmod p$.

(β) Αν ο n είναι σύνθετος, τότε $\phi(n) < n - 1$ (γιατί;). Από το θεώρημα του Euler, αν $(a, n) = 1$ τότε $a^{\phi(n)} \equiv 1 \pmod n$, άρα ο a έχει τάξη κάποιον διαιρέτη του $\phi(n)$, δηλαδή κάποιον φυσικό γνήσια μικρότερο του $n - 1$.

3. Έστω p ένας περιττός πρώτος διαιρέτης του $n^2 + 1$. Τότε $n^2 \equiv -1 \pmod p$, άρα

$$n^4 = (n^2)^2 \equiv (-1)^2 = 1 \pmod p.$$

Έπεται ότι η τάξη του n ως προς p ισούται με 4 (γιατί;). Άρα $4 \mid \phi(p) = p - 1$, οπότε υπάρχει $k \in \mathbb{Z}$ τέτοιος ώστε $p - 1 = 4k$.

4. Ο 3 είναι πρωταρχική ρίζα του 17. Αν r είναι η τάξη του 3 ως προς 17 τότε (Θεώρημα 4.1.1) $r \mid \phi(17) = 16$. Όμως $3^1 \equiv 3 \pmod{17}$, $3^2 \equiv 9 \pmod{17}$, $3^4 \equiv 13 \pmod{17}$ $3^8 \equiv 13^2 \equiv (-4)^2 = 16 \pmod{17}$, οπότε υποχρεωτικά $r = 16$.

5. Ξέρουμε ότι η τάξη του r^k ως προς n είναι ίση με $d/(k, d)$ όπου d η τάξη του r ως προς n. Αφού ο r είναι πρωταρχική ρίζα του n έχουμε $d = \phi(n)$. Δηλαδή η τάξη του r^k ως προς n είναι ίση με $\phi(n)/(k, \phi(n))$. Ο r^k θα είναι κι αυτός πρωταρχική ρίζα του n αν και μόνο αν $\phi(n)/(k, \phi(n)) = \phi(n)$, δηλαδή αν και μόνο αν $(k, \phi(n)) = 1$.

6. (α) Έστω k η τάξη του $-r$ ως προς p. Τότε $k \mid \phi(p) = p - 1$ και δεν μπορούμε να έχουμε $k = (p - 1)/2$ γιατί ο $(p - 1)/2$ είναι άρτιος οπότε θα είχαμε

$$r^{(p-1)/2} = (-r)^{(p-1)/2} \equiv 1 \pmod p,$$

το οποίο δεν ισχύει αφού ο r είναι πρωταρχική ρίζα του p. Αν λοιπόν $k \neq p - 1$, τότε $k < (p - 1)/2$ οπότε $2k < p - 1$ και

$$r^{2k} = [(-r)^k]^2 \equiv 1^2 = 1 \pmod p,$$

το οποίο είναι πάλι άτοπο. Έπεται ότι $k = p - 1$, δηλαδή ο $-r$ είναι πρωταρχική ρίζα του p.

(β) Όπως πριν βλέπουμε ότι η τάξη k του $-r$ ως προς p δεν μπορεί να είναι μικρότερη από $(p - 1)/2$. Επίσης ο $(p - 1)/2$ είναι περιττός, άρα

$$(-r)^{(p-1)/2} = -r^{(p-1)/2}.$$

Αρκεί λοιπόν να δείξουμε ότι $r^{(p-1)/2} \equiv -1 \pmod p$. Αυτό προκύπτει από την

$$p \mid r^{p-1} - 1 = (r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1).$$

Ο p δεν διαιρεί τον $r^{(p-1)/2} - 1$ (γιατί η τάξη του r ως προς p είναι $p - 1$), άρα $p \mid r^{(p-1)/2} + 1$.

7. (α) Η $x^2+7x+10\equiv 0 \pmod{11}$ είναι ισοδύναμη με την

$$4x^2+28x+40=(2x+7)^2-9\equiv 0 \pmod{11}$$

γιατί $(4,11)=1$. Θέτουμε $y=2x+7$ και λύνουμε την $y^2\equiv 9 \pmod{11}$ η οποία έχει τις προφανείς λύσεις $y\equiv 3 \pmod{11}$ και $y\equiv -3 \pmod{11}$. Αρκεί λοιπόν να λύσουμε τις

$$2x+7\equiv 3 \pmod{11} \text{ και } 2x+7\equiv -3 \pmod{11}$$

ή, ισοδύναμα, τις

$$2x\equiv -4\equiv 7 \pmod{11} \text{ και } 2x\equiv -10\equiv 1 \pmod{11}.$$

Οι λύσεις τους είναι οι $x\equiv 9 \pmod{11}$ και $x\equiv 6 \pmod{11}$.

(β) Όμοια.

8. Έστω ότι ο ακέραιος a δεν είναι τετραγωνικό υπόλοιπο του p και έστω r η τάξη του a ως προς p. Από το Θεώρημα 4.1.1 έχουμε $r \mid \phi(p)=p-1=2^k$ ενώ το κριτήριο του Euler (Θεώρημα 4.3.2) δίνει $a^{2^{k-1}}\equiv -1 \pmod{p}$. Από την τελευταία σχέση και την ισοτιμία $a^{2^r}\equiv 1 \pmod{p}$ προκύπτει $r>2^{k-1}$ (γιατί;) και συνεπώς υποχρεωτικά $r=2^k=p-1$.

9. Χρησιμοποιούμε τις βασικές ιδιότητες του συμβόλου του Legendre και τον τετραγωνικό νόμο αντιστροφής.

(α) $\left(\frac{19}{23}\right)=(-1)^{9\cdot 11}\left(\frac{23}{19}\right)=-\left(\frac{4}{19}\right)=-\left(\frac{2^2}{19}\right)=-1$.

(β) $\left(\frac{-23}{59}\right)=(-1)^{29}\left(\frac{23}{59}\right)=-(-1)^{11\cdot 29}\left(\frac{59}{23}\right)=\left(\frac{13}{23}\right)=(-1)^{6\cdot 11}\left(\frac{23}{13}\right)=\left(\frac{10}{13}\right)=\left(\frac{2}{13}\right)\left(\frac{5}{13}\right)=-\left(\frac{5}{13}\right)=-\left(\frac{13}{5}\right)=-\left(\frac{3}{5}\right)=-\left(\frac{5}{3}\right)=-\left(\frac{2}{3}\right)=1$.

(γ) $\left(\frac{20}{31}\right)=\left(\frac{2^2}{31}\right)\left(\frac{5}{31}\right)=\left(\frac{5}{31}\right)=(-1)^{2\cdot 15}\left(\frac{31}{5}\right)=\left(\frac{31}{5}\right)=\left(\frac{1}{5}\right)=1$.

Τα υπόλοιπα σύμβολα του Legendre υπολογίζονται με τον ίδιο τρόπο.

10. Αν υπάρχουν ακέραιοι x,y τέτοιοι ώστε $x^2+py+a=0$, τότε $x^2+a\equiv 0 \pmod{p}$ δηλαδή η τετραγωνική ισοτιμία $x^2\equiv -a \pmod{p}$ έχει λύσεις. Επομένως, $\left(\frac{-a}{p}\right)=1$.

Αντίστροφα, αν $\left(\frac{-a}{p}\right)=1$, τότε υπάρχει $x\in\mathbb{Z}$ τέτοιος ώστε $x^2\equiv -a \pmod{p}$, δηλαδή $p \mid x^2+a$. Άρα υπάρχει ακέραιος y τέτοιος ώστε $x^2+a=py$. Έπεται ότι $x^2+p(-y)+a=0$.

11. (α) Αφού οι a,b είναι πρώτοι προς τον p ισχύει και η $(ab,p)=1$. Γνωρίζουμε ότι

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Αφού οι τρείς αυτοί αριθμοί παίρνουν τις τιμές ± 1, δεν μπορούν να είναι όλοι ίσοι με -1. 'ρα κάποιο από τα τρία σύμβολα του Legendre παίρνει την τιμή 1, δηλαδή τουλάχιστον ένας από τους a,b και ab είναι τετραγωνικό υπόλοιπο του p.

(β) Αν $p\neq 2,3$, παίρνουμε $a=2$ και $b=3$ στο (α). Κάποιος από τους $2,3$ και $2\cdot 3=6$ είναι τεραγωνικό υπόλοιπο του p. Άρα υπάρχει $n\in\mathbb{N}$ τέτοιος ώστε

$$p \mid n^2-2 \text{ ή } p \mid n^2-3 \text{ ή } p \mid n^2-6.$$

Σε κάθε περίπτωση,

$$p \mid (n^2-2)(n^2-3)(n^2-6).$$

Αν $p=2$ ή $p=3$ το ζητούμενο ισχύει με $n=2$ ή $n=3$ αντίστοιχα.

12. Ο $(p-1)/2$ είναι άρτιος, άρα για κάθε $a=1,\ldots,(p-1)/2$ έχουμε

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

Από το κριτήριο του Euler έπεται ότι

$$\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right).$$

Επομένως,

$$2\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right) + \sum_{a=1}^{(p-1)/2}\left(\frac{p-a}{p}\right) = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right).$$

Όμως το σύμβολο $\left(\frac{a}{p}\right)$ παίρνει τις τιμές 1 και -1 από $(p-1)/2$ φορές καθώς το a κινείται από 1 ως $p-1$ (οι μισές τιμές του a είναι τετραγωνικά υπόλοιπα του p και οι άλλες μισές όχι). Άρα το τελευταίο άθροισμα είναι ίσο με μηδέν. Έπεται το ζητούμενο.

13. Όταν ο k διατρέχει τους διαιρέτες του a, ο k/a διατρέχει τους διαιρέτες του a και

$$\left(\frac{k}{p}\right)\left(\frac{a/k}{p}\right) = \left(\frac{a}{p}\right) = -1, \text{ άρα } \left(\frac{k}{p}\right) = -\left(\frac{a/k}{p}\right).$$

Άρα

$$2\sum_{k|a}\left(\frac{k}{p}\right) = \sum_{k|a}\left(\frac{k}{p}\right) + \sum_{k|a}\left(\frac{a/k}{p}\right) = 0.$$

Επίσης, από το κριτήριο του Euler,

$$\sum_{k|a} k^{\frac{p-1}{2}} \equiv \sum_{k|a}\left(\frac{k}{p}\right) \pmod p.$$

Άρα

$$\sum_{k|a} k^{\frac{p-1}{2}} \equiv 0 \pmod p.$$

14. Έχουμε

$$\left(\frac{x}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{2^2}{p}\right) = \left(\frac{4x}{p}\right) = \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

και ομοίως

$$\left(\frac{x}{q}\right) = \left(\frac{4x}{q}\right) = \left(\frac{p-q}{q}\right) = \left(\frac{p}{q}\right).$$

Από τα παραπάνω και το νόμο αντιστροφής του Gauss προκύπτει ότι

$$\left(\frac{x}{p}\right)\left(\frac{x}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}+\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{\frac{p+1}{2}\cdot\frac{q-1}{2}} = 1$$

διότι $p \equiv q \pmod 4$ από την υπόθεση και συνεπώς ένας από τους $\frac{p+1}{2}$, $\frac{q-1}{2}$ είναι άρτιος.

15. Η δοσμένη ισοτιμία είναι ισοδύναμη με το σύστημα των ισοτιμιών $x^2 \equiv 1 \pmod 5$ και $x^2 \equiv 4 \pmod 7$. Οι ισοτιμίες αυτές έχουν λύσεις $x \equiv \pm 1 \pmod 5$ και $x \equiv \pm 2 \pmod 7$ αντίστοιχα και οδηγούν στις λύσεις $x \equiv \pm 16, \pm 26 \pmod{35}$ της αρχικής ισοτιμίας.

16. Πρέπει $(p, 3) = 1$ και

$$1 = \left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

οπότε πρέπει και αρκεί $p \equiv 1 \pmod 3$.

17. Πρέπει $(p,5)=1$ και

$$1=\left(\frac{5}{p}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right)=\left(\frac{p}{5}\right)$$

οπότε $p\equiv\pm1 \pmod 5$.

18. Όπως στην Άσκηση 12 έχουμε $\left(\frac{k}{p}\right)=\left(\frac{p-k}{p}\right)$ για κάθε ακέραιο k. Συνεπώς

$$\begin{aligned}2\sum_{k=1}^{p-1}k\left(\frac{k}{p}\right) &= \sum_{k=1}^{p-1}k\left(\frac{k}{p}\right)+\sum_{k=1}^{p-1}(p-k)\left(\frac{p-k}{p}\right)\\ &= \sum_{k=1}^{p-1}k\left(\frac{k}{p}\right)+\sum_{k=1}^{p-1}(p-k)\left(\frac{k}{p}\right)\\ &= p\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)=0\end{aligned}$$

από όπου προκύπτει η πρώτη από τις προτεινόμενες ισότητες. Θέτοντας

$$A_p=\sum_{\substack{k=1\\(k/p)=1}}^{p-1}k,\qquad B_p=\sum_{\substack{k=1\\(k/p)=-1}}^{p-1}k$$

η ισότητα αυτή γράφεται $A_p-B_p=0$. Προφανώς όμως $A_p+B_p=\frac{p(p-1)}{2}$ οπότε $A_p=B_p=\frac{p(p-1)}{4}$.

19. Έχουμε

$$\left(\frac{p-k}{p}\right)=\left(\frac{-k}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{k}{p}\right)=-\left(\frac{k}{p}\right)$$

για κάθε ακέραιο k και συνεπώς

$$\begin{aligned}2\sum_{k=1}^{p-1}k^2\left(\frac{k}{p}\right) &= \sum_{k=1}^{p-1}k^2\left(\frac{k}{p}\right)+\sum_{k=1}^{p-1}(p-k)^2\left(\frac{p-k}{p}\right)\\ &= \sum_{k=1}^{p-1}k^2\left(\frac{k}{p}\right)-\sum_{k=1}^{p-1}(p-k)^2\left(\frac{k}{p}\right)\\ &= \sum_{k=1}^{p-1}(2kp-p^2)\left(\frac{k}{p}\right)=2p\sum_{k=1}^{p-1}k\left(\frac{k}{p}\right)\end{aligned}$$

διότι $\sum_{k=1}^{p-1}p^2\left(\frac{k}{p}\right)=0$.

20. Θα χρησιμοποιήσουμε επαγωγή στο n. Για $n=1$ ο 2 έχει πράγματι τάξη 4 ως προς 5. Έστω ότι η πρόταση ισχύει για τον n αλλά όχι για τον $n+1$. Έστω k η τάξη του 2 ως προς 5^{n+1} οπότε $k\mid\phi(5^{n+1})=4\cdot5^n$ και $k<4\cdot5^n$. Έχουμε $2^k\equiv1 \pmod{5^{n+1}}$ και συνεπώς $2^k\equiv1 \pmod{5^n}$, άρα η τάξη του 2 ως προς 5^n, που είναι ίση με $4\cdot5^{n-1}$ από την υπόθεση της επαγωγής, διαιρεί το k. Από τις σχέσεις $4\cdot5^{n-1}\mid k$, $k\mid4\cdot5^n$ και $k<4\cdot5^n$ προκύπτει ότι $k=4\cdot5^{n-1}$. Από το Θεώρημα Fermat-Euler ο $2^{4\cdot5^{n-2}}-1$ διαιρείται με το 5^{n-1} αλλά όχι με το 5^n (αλλιώς η πρόταση δεν θα ίσχυε για τον n), συνεπώς μπορούμε να γράψουμε $2^{4\cdot5^{n-2}}=1+5^{n-1}q$ με $q\in\mathbb{N}$ σχετικώς πρώτο προς το 5. Από την ταυτότητα

$$(a+b)^5=a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

προκύπτει

$$\begin{aligned} 2^{4\cdot 5^{n-1}} - 1 &= (2^{4\cdot 5^{n-2}})^5 - 1 = (1+5^{n-1}q)^5 - 1 \\ &= 5^{n+1}(5^{4n-6}q^5 + 5^{3n-4}q^4 + 2\cdot 5^{2n-3}q^3 + 2\cdot 5^{n-2}q^2) + 5^n q \end{aligned}$$

και συνεπώς ο $2^{4\cdot 5^{n-1}} - 1$ δεν διαιρείται με το 5^{n+1}, πράγμα το οποίο αντιφάσκει στο ότι ο 2 έχει τάξη $k = 4\cdot 5^{n-1}$ ως προς 5^{n+1}. Η αντίφαση αυτή ολοκληρώνει το επαγωγικό βήμα.