Παρασκευάς Αλβανός
Δημήτριος Πουλάκης

Επανάληψη στη Θεωρία Αριθμών

Συνοπτική Θεωρία, Μεθοδολογία, Ασκήσεις

ΚΑΛΛΙΠΟΣ
ανοικτές ακαδημαϊκές εκδόσεις

Εθνικό Πρόγραμμα Ανάπτυξης 2021-2025

Παρασκευάς Αλβανός
ΕΔΙΠ τμήματος Μαθηματικών ΑΠΘ

Δημήτριος Πουλάκης
Καθηγητής Τμήματος Μαθηματικών ΑΠΘ

Επανάληψη στη Θεωρία Αριθμών

Συνοπτική Θεωρία, Μεθοδολογία, Ασκήσεις

ΚΑΛΛΙΠΟΣ
ανοικτές ακαδημαϊκές εκδόσεις

Επανάληψη στη Θεωρία Αριθμών
Συνοπτική Θεωρία, Μεθοδολογία, Ασκήσεις

Συγγραφή

Παρασκευάς Αλβανός

Δημήτριος Πουλάκης

Συντελεστές έκδοσης

Γλωσσική Επιμέλεια: Δημήτριος Καλλιάρας

Γραφιστική Επιμέλεια: Αλεξάνδρα Θεοδωράκη

ISBN: 978-618-85370-3-3

ΚΑΛΛΙΠΟΣ

Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

www.kallipos.gr

Αφιερώνεται στην κόρη μου Κωνσταντίνα
που τεσσάρων χρονών
μου ζήτησε να της μάθω μαθηματικά
Π. Αλβανός

Αφιερώνεται στη σύζυγό μου Πετρούλα
και στην κόρη μου Ηγησώ
Δ. Πουλάκης

Εισαγωγή

Το παρόν σύγγραμμα είναι μία συλλογή ασκήσεων Θεωρίας Αριθμών η οποία απευθύνεται κυρίως σε προπτυχιακούς φοιτητές ή σε απόφοιτους Τμημάτων Μαθηματικών οι οποίοι επιθυμούν να εμβαθύνουν στο αντικείμενο. Είναι δυνατόν να χρησιμοποιηθεί ως βοήθημα κατά την διδασκαλία ενός μαθήματος Θεωρίας Αριθμών, για προετοιμασία σε εξετάσεις ή φοιτητικούς διαγωνισμούς, καθώς και για αυτοδιδασκαλία.

Στην αρχή κάθε κεφαλαίου δίνονται βασικά αποτελέσματα χωρίς απόδειξη με τις σχετικές αναφορές και κατόπιν αυτά χρησιμοποιούνται σε ασκήσεις διαβαθμισμένης δυσκολίας. Στη προτελευταία ενότητα κάθε κεφαλαίου παρατίθενται κάποιες συνδυαστικές ασκήσεις, καθώς και ασκήσεις ιδιαίτερης δυσκολίας. Στην τελευταία ενότητα κάθε κεφαλαίου παρατίθενται οι εντολές και ο τρόπος επίλυσης υπολογιστικών ασκήσεων με την χρήση του υπολογιστικού πακέτου Maple. ΄Αλλα γνωστά προγράμματα τα οποία μπορεί να χρησιμοποιηθούν για την επίλυση υπολογιστικών ασκήσεων στη Θεωρία Αριθμών είναι το Mathematica, το MAGMA και το SAGE το οποίο είναι ανοικτό.

Το σύγγραμμα αυτό περιέχει δέκα κεφάλαια τα οποία είναι αφιερωμένα στα Συστήματα Αριθμών, Διαιρετότητα, Αριθμητικές Συναρτήσεις, Ισοτιμίες, Γραμμικές Ισοτιμίες και Συστήματα, Πολυωνυμικές Ισοτιμίες και Αρχικές Ρίζες, Τετραγωνικά Υπόλοιπα, Παράσταση Ακεραίων από Τετραγωνικές Μορφές, Διοφαντικές Εξισώσεις και Συνεχή Κλάσματα.

Θα χρησιμοποιούμε τα συνήθη σύμβολα της Θεωρίας Συνολων: $\in$, $\subseteq$, $\subset$, $\cap$ και $\cup$. Αν X και Y είναι υποσύνολα του ίδιου συνόλου, τότε συμβολίζουμε με $X \setminus Y$ το σύνολο των στοιχείων του X που δεν ανήκουν στο Y. Ας είναι $f : A \to B$ μία απεικόνιση. Υπενθυμίζουμε ότι η f καλείται ένεση, αν για κάθε $x, y \in A$ με $x \neq y$ έχουμε $f(x) \neq f(y)$ και έφεση αν για κάθε $z \in B$ υπάρχει $x \in A$ με $f(x) = z$. Επίσης, η f καλείται αμφίεση, αν είναι ένεση και έφεση. Θα συμβολίζουμε με $\mathbb{N}$ το σύνολο των φυσικών αριθμών $\{0, 1, 2, \ldots\}$ και με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών. Επίσης, με $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ θα συμβολίζουμε τα σύνολα των ρητών, πραγματικών και μιγαδικών αριθμών, αντίστοιχα.

Περιεχόμενα

Κεφάλαιο 1

Συστήματα Αριθμών

Θέτοντας ως σημείο εκκίνησης τους πραγματικούς αριθμούς και τις ιδιότητές τους, ένα μεγάλο μέρος των κλασικών μαθηματικών (αναλυτική γεωμετρία, ακολουθίες, διαφορικές εξισώσεις, απειροστικός λογισμός κ.α.) μπορεί να αναπτυχθεί επαγωγικά. Οι μαθηματικοί του 19ου αιώνα όπως οι Weierstrass, Dedekind και Cantor που ασχολήθηκαν με την κατασκευή του συνόλου των πραγματικών αριθμών $\mathbb{R}$ κατέληγαν πάντα στο σύνολο των φυσικών αριθμών $\mathbb{N}$. Έτσι έγινε σαφές ότι ολόκληρος ο τομέας των καθαρών μαθηματικών μπορεί να κατασκευαστεί αυστηρά ξεκινώντας από τη θεωρία των φυσικών αριθμών. Ο Dedekind αρχικά και ο Peano στη συνέχεια έδειξαν πως ολόκληρη η θεωρία των φυσικών αριθμών θα μπορούσε να προέλθει από μερικά βασικά αξιώματα [2].

Το πρώτο κεφάλαιο αποτελεί μία εισαγωγή για την θεωρία αριθμών. Σε αυτό ορίζονται τα βασικά αριθμητικά σύνολα (φυσικοί, ακέραιοι) και εισάγονται απαραίτητες αλγεβρικές έννοιες όπως η σχέση ισοδυναμίας και οι αλγεβρικές δομές.

1.1 Φυσικοί Αριθμοί

Η ευρύτερα αποδεκτή αξιωματικοποίηση των φυσικών αριθμών είναι αυτή του Peano η οποία δόθηκε στα 1882.

Αξιώματα Peano Το σύστημα των φυσικών αριθμών είναι ένα σύνολο $\mathbb{N}$ εφοδιασμένο με μία απεικόνιση $\sigma : \mathbb{N} \to \mathbb{N}$ και ένα στοιχείο $0 \in \mathbb{N}$ έτσι, ώστε να ισχύουν τα εξής:

1) Η απεικόνιση σ είναι ένεση.
2) $0 \notin \sigma(\mathbb{N})$
3) Αν $S \subseteq \mathbb{N}$ με $0 \in S$ και $\sigma(x) \in S$ $\forall x \in S$, τότε $S = \mathbb{N}$.

Έτσι, το σύνολο $\mathbb{N}$ είναι απλώς το σύνολο

$$\{0, \sigma(0), \sigma(\sigma(0)), \ldots\}.$$

Θέτοντας $\sigma(0) = 1$, $\sigma(1) = 2, \ldots$ καταλήγουμε στη καθιερωμένη γραφή των φυσικών αριθμών.

Τα παραπάνω αξιώματα δεν διατυπώθηκαν ακριβώς έτσι από τον Peano. Για παράδειγμα ο Peano ξεκινούσε με τον αριθμό 1 ως τον πρώτο φυσικό αριθμό ενώ σήμερα είναι πλέον αποδεκτό να θεωρείται το 0 ως ο πρώτος φυσικός αριθμός.

Στο σύνολο των φυσικών ορίζουμε την *πρόσθεση* «+» μεταξύ δύο φυσικών x και y ως εξής:

$$x + 0 = x, \quad x + \sigma(y) = \sigma(x + y).$$

Επίσης, ορίζουμε τον *πολλαπλασιασμό* «·» μεταξύ δύο φυσικών x και y ως εξής:

$$x \cdot 0 = 0, \quad x \cdot \sigma(y) = \sigma(x + y).$$

Το αποτέλεσμα της πρόσθεσης το καλούμε *άθροισμα* και το αποτέλεσμα του πολλαπλασιασμού *γινόμενο*.

Οι προτάσεις που ακολουθούν είναι συνέπεια των αξιωμάτων του Peano.

Πρόταση 1.1. *Για κάθε $x, y, z \in \mathbb{N}$ ισχύουν τα εξής:*

$\alpha)$ $x + (y + z) = (x + y) + z$, $x(yz) = (xy)z$ (*προσεταιριστική ιδιότητα*),
$\beta)$ $x + y = y + x$, $xy = yx$ (*αντιμεταθετική ιδιότητα*),
$\gamma)$ $x(y + z) = xy + xz$ (*επιμεριστική ιδιότητα*),
$\delta)$ $x + y = x + z \Rightarrow y = z$, *και* $xy = xz$ *με* $x \neq 0 \Rightarrow y = z$ (*νόμος διαγραφής*),
$\varepsilon)$ $x + y = 0 \Leftrightarrow x = y = 0$,
$\sigma\tau)$ $xy = 0 \Leftrightarrow x = 0$ *ή* $y = 0$.

Απόδειξη. Βλέπε [3, Κεφάλαιο 1, Πρόταση 2.1, 2.2], [4, Κεφάλαιο 1, Πρόταση 1.6, 1.5]. □

Ορισμός 1.1. Ας είναι $x, y \in \mathbb{N}$. Ο φυσικός x καλείται *μικρότερος* του y και γράφεται $x < y$ αν υπάρχει $k \in \mathbb{N}$ με $k \neq 0$ τέτοιο ώστε $y = x + k$. Στην προκειμένη περίπτωση ο y καλείται *μεγαλύτερος* του m.

Πρόταση 1.2 (Νόμος της τριχοτομίας)**.** *Για κάθε $x, y \in \mathbb{N}$ ισχύει ακριβώς μία από τις παρακάτω σχέσεις:*

$$x < y, \quad x = y, \quad x > y.$$

Απόδειξη. Βλέπε [3, Κεφάλαιο 1, Πρόταση 2.3], [4, Κεφάλαιο 1, Πρόταση 1.7]. □

Αν έχουμε $m, n \in \mathbb{N}$ με $m = n$ ή $m < n$, τότε γράφουμε $m \leq n$ ή $n \geq m$.

Πρόταση 1.3. *Ας είναι $m, n, k \in \mathbb{N}$. Τότε, ισχύουν τα εξής:*

$\alpha)$ $m \leq m$.
$\beta)$ $m \leq n$ *και* $n \leq m \Rightarrow m = n$.
$\gamma)$ $m \leq n$ *και* $n \leq k \Rightarrow m \leq k$.

Απόδειξη. Βλέπε [4, Κεφάλαιο 1, Πρόταση 1.8]. □

Ορισμός 1.2. Ας είναι S μη κενό υποσύνολο του $\mathbb{N}$ και $s \in S$ τέτοιο, ώστε $s \leq x$, για κάθε $x \in S$. Τότε, το s καλείται *ελάχιστο στοιχείο* του S.

Πρόταση 1.4 (Αρχή της καλής διάταξης)**.** *Κάθε μη κενό υποσύνολο του $\mathbb{N}$ έχει μοναδικό ελάχιστο στοιχείο.*

Απόδειξη. Βλέπε [3, Κεφάλαιο 1, Πρόταση 2.4], [4, Κεφάλαιο 1, Πρόταση 1.8]. □

Το τρίτο αξίωμα του Peano είναι γνωστό ως το *αξίωμα της μαθηματικής επαγωγής* και αποτελεί ένα πολύ χρήσιμο εργαλείο για τις αποδείξεις προτάσεων και θεωρημάτων. Στη συνέχεια παρουσιάζουμε την διαδικασία χρήσης της μαθηματικής επαγωγής καθώς και δύο ισοδύναμες εκφράσεις της. Η βασική διαδικασία χωρίζεται σε τρία βήματα: το *βασικό βήμα* (Β.Β.), την *επαγωγική υπόθεση* (Ε.Υ.) και το *επαγωγικό βήμα* (Ε.Β.).

Αρχή της Μαθηματικής Επαγωγής (Α). Έστω $P(n)$ μία πρόταση που εξαρτάται από το n και θέλουμε να αποδείξουμε ότι είναι αληθής για κάθε φυσικό $n \geq n_0$. Η διαδικασία απόδειξης έχει ως εξης:
Β.Β.) Αποδεικνύουμε ότι η πρόταση είναι αληθής για $n = n_0$.
Ε.Υ.) Υποθέτουμε ότι ισχύει για $n = k$, όπου $k > n_0$.
Ε.Β.) Αποδεικνύουμε ότι ισχύει για $n = k + 1$.

Αρχή της Μαθηματικής Επαγωγής (Β). Έστω $P(n)$ μία πρόταση που εξαρτάται από το n και θέλουμε να αποδείξουμε ότι είναι αληθής για κάθε φυσικό $n \geq n_0$. Η διαδικασία απόδειξης έχει ως εξης:
Β.Β.) Αποδεικνύουμε ότι η πρόταση είναι αληθής για $n = n_0$.
Ε.Υ.) Υποθέτουμε ότι ισχύει για καθε n με $n_0 < n < k$.
Ε.Β.) Αποδεικνύουμε ότι ισχύει για $n = k$.

Απόδειξη των παραπάνω μορφών μαθηματικής επαγωγής, ο ενδιαφερόμενος αναγνώστης μπορεί να βρει στο [3, Κεφάλαιο 1, Πρόταση 2.5 και 2.6] και στο [4, Κεφάλαιο 1, Πρόταση 1.10 και 1.11].

Δισδιάστατη Μαθηματική Επαγωγή (Α). Έστω $P(n, m)$ μία πρόταση που εξαρτάται από τα n και m θέλουμε να αποδείξουμε ότι είναι αληθής για κάθε $n, m \in \mathbb{N}$. Η διαδικασία απόδειξης έχει ως εξης:

- Αποδεικνύουμε ότι η πρόταση είναι αληθής για $n = 0$, $m = 0$.
- Υποθέτουμε ότι ισχύει για $n = k$, $m = 0$, όπου $k > 0$.
- Αποδεικνύουμε ότι ισχύει για $n = k + 1$, $m = 0$.
- Υποθέτουμε ότι ισχύει για κάθε n και $m = k$, όπου $k > 0$.
- Αποδεικνύουμε ότι ισχύει για κάθε n και $m = k + 1$.

Δισδιάστατη Μαθηματική Επαγωγή (Β). Έστω $P(n, m)$ μία πρόταση που εξαρτάται από τα n και m θέλουμε να αποδείξουμε ότι είναι αληθής για κάθε $n, m \in \mathbb{N}$. Η διαδικασία απόδειξης έχει ως εξης:

- Αποδεικνύουμε ότι η πρόταση είναι αληθής για $n = m = 0$.
- Υποθέτουμε ότι ισχύει για $n + m = k$, όπου $k > 0$.
- Αποδεικνύουμε ότι ισχύει για $n + m = k + 1$.

Ασκήσεις

Αρχικά θα δούμε ασκήσεις που αφορούν γνωστές βασικές ιδιότητες των φυσικών αριθμών.

΄Ασκηση 1.1. *Ας είναι $m, n, k \in \mathbb{N}$. Τότε, ισχύουν τα εξής:*

α) $m < n$ *και* $n < k \Rightarrow m < k$.

β) $m < n \Leftrightarrow m + k < n + k$.

γ) Αν $k \neq 0$, *τότε* $m = n \Leftrightarrow mk = nk$.

δ) Αν $k \neq 0$ *και* $m < n \Rightarrow km < kn$.

Απόδειξη. α) Καθώς $m < n$ και $n < k$, υπάρχουν $s, t \in \mathbb{N}$ τέτοια, ώστε $n = m + s$ και $k = n + t$. Από τις δύο ισότητες έχουμε $k = m + s + t$ και επομένως $k > m$.

β) Ας είναι $m + k < n + k$. ΄Αρα, υπάρχει $s \in \mathbb{N}$ έτσι, ώστε $m + k = n + k + s$. Από την αντιμεταθέτική ιδότητα προκύπτει $m + k = n + s + k$ και από το νόμο της διαγραφής παίρνουμε $m = n + s$, απ΄ όπου $m < n$. Ας είναι $m < n$. Οπότε, υπάρχει $s \in \mathbb{N}$ έτσι, ώστε $m = n + s$. Θα δείξουμε ότι για κάθε φυσικό k ισχύει:

$$m + k = n + s + k.$$

Για $k = 0$ έχουμε:

$$m + 0 = m = n + s = n + s + 0.$$

Ας υποθέσουμε ότι ισχύει για $k = \nu$. Τότε $m + \nu = n + s + \nu$ και επομένως

$$\sigma(m + \nu) = \sigma(n + s + \nu),$$

απ΄ όπου έχουμε:

$$m + \nu + \sigma(0) = n + s + \nu + \sigma(0)$$

ή ισοδύναμα

$$m + \nu + 1 = n + s + \nu + 1.$$

΄Αρα, η προς απόδειξη σχέση ισχύει για κάθε φυσικό k. ΄Ετσι, παίρνουμε $m + k < n + k$.

γ) Αν $mk = nk$, τότε από το νόμο της διαγραφής προκύπτει άμεσα το ζητούμενο. Ας είναι $m = n$. Θα δείξουμε επαγωγικά ότι $mk = nk$, για κάθε $k > 0$. Για $k = 1$ έχουμε

$$m \cdot 1 = n \cdot 1 \Rightarrow m \cdot \sigma(0) = n \cdot \sigma(0) \Rightarrow m \cdot 0 + m = n \cdot 0 + n \Rightarrow 0 + m = 0 + n,$$

και επομένως $m = n$. Ας υποθέσουμε ότι η προς απόδειξη σχέση ισχύει για $k = \nu$. Θα δείξουμε ότι ισχύει για $k = \nu + 1$. Πράγματι, η επιμεριστική ιδιότητα δίνει:

$$m(k + 1) = n(k + 1) \Rightarrow mk + m = nk + n.$$

Από την υπόθεση της επαγωγής έχουμε $mk = nk$ και επομένως ο νόμος της διαγραφής συνεπάγεται το ζητούμενο.

δ) Καθώς έχουμε $m < n$, υπάρχει φυσικός $l \neq 0$ με $m + l = n$. Από το (γ) έπεται ότι $k(m + l) = kn$, απ΄ όπου $km + kl = kn$. Επειδή ισχύει $k \neq 0$ και $l \neq 0$, η Πρόταση 1.1(στ) δίνει $kl \neq 0$. ΄Ετσι, παίρνουμε ότι $km < kn$. □

Στην συνέχεια θα δούμε ασκήσεις κάνοντας χρήση μία εκ των τριών πρώτων ισοδύναμων εκφράσεων της αρχής της μαθηματικής της επαγωγής.

΄Ασκηση 1.2. *Ας είναι n φυσικός ≥ 1.*

α) *Θέτουμε*

$$T_n = 1 + 2 + \cdots + n.$$

Να δειχθεί ότι ισχύει

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

β) *Θέτουμε*

$$C_n = 1 + 3 + \cdots + (2n-1).$$

Να δειχθεί ότι ισχύει

$$C_n = n^2.$$

γ) *Θέτουμε*

$$P_n = 1 + 4 + \cdots + (3n-2).$$

Να δειχθεί ότι ισχύει

$$P_n = \frac{1}{2}n(3n-1).$$

δ) *Θέτουμε*

$$\Pi_n = 1 + 3 + 6 + \cdots + \frac{1}{2}n(n+1).$$

Να δειχθεί ότι ισχύει

$$\Pi_n = \frac{1}{6}n(n+1)(n+2).$$

Απόδειξη. Βασικό εργαλείο στην απόδειξη των παραπάνω σχέσεων είναι η χρήση της μεθόδου της επαγωγής.

α) Για $n = 1$ ισχύει. Ας υποθέσουμε ότι ισχύει για $n = k$, δηλαδή,

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

Θα δείξουμε ότι ισχύει για $n = k + 1$. Έχουμε:

$$\begin{aligned} T_{k+1} &= \frac{1}{2}(k+1)(k+2) \\ &= \frac{1}{2}(k+1)k + (k+1) \\ &= 1 + 2 + \cdots + k + (k+1). \end{aligned}$$

Άρα, η σχέση ισχύει για κάθε $n \geq 1$.

β) Για $n = 1$ ισχύει. Ας υποθέσουμε ότι ισχύει για $n = k$, δηλαδή, $C_k = k^2$. Θα δείξουμε ότι ισχύει για $n = k + 1$. Έχουμε:

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

Επομένως, η σχέση ισχύει για κάθε $n \geq 1$.

γ) Για $n = 1$ ισχύει. Ας υποθέσουμε ότι ισχύει για $n = k$, δηλαδή,

$$P_k = \frac{1}{2}k(3k-1).$$

Θα δείξουμε ότι ισχύει για $n = k+1$. Έχουμε:

$$\begin{aligned} P_{k+1} &= \frac{1}{2}(k+1)(3(k+1)-1) \\ &= \frac{1}{2}k(3k+2) + \frac{1}{2}(3k+2) \\ &= \frac{1}{2}k(3k-1) + 3\frac{1}{2}k + \frac{1}{2}(3k+2) \\ &= 1 + 4 + \cdots + (3k-2) + 3k + 1. \end{aligned}$$

Συνεπώς, η σχέση ισχύει για κάθε $n \geq 1$.

δ) Για $n = 1$ ισχύει. Ας υποθέσουμε ότι ισχύει για $n = k$, δηλαδή,

$$\Pi_k = \frac{1}{6}k(k+1)(k+2).$$

Θα δείξουμε ότι ισχύει για $n = k+1$. Έχουμε:

$$\begin{aligned} \Pi_{k+1} &= \frac{1}{6}(k+1)(k+2)(k+3) \\ &= \frac{1}{6}(k+1)(k+2)k + \frac{1}{6}(k+1)(k+2)3 \\ &= 1 + 3 + 6 + \cdots + \frac{1}{2}k(k+1) + \frac{1}{2}(k+1)(k+2). \end{aligned}$$

Άρα η σχέση ισχύει για κάθε $n \geq 1$. □

Άσκηση 1.3. *Να δειχθεί ότι για κάθε θετικό ακέραιο n ισχύουν τα εξής:*

α)
$$\sum_{k=1}^{n} k = \frac{1}{2}n(n+1),$$

β)
$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1),$$

γ)
$$\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2,$$

δ)
$$\sum_{k=1}^{n} k^4 = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1),$$

ε)

$$\sum_{k=1}^{n} k^5 = \frac{1}{12} n^2 (n+1)^2 (2n^2 + 2n - 1)$$

στ)

$$\sum_{k=1}^{n} k^6 = \frac{1}{42} n(n+1)(2n+1)(3n^4 + 6n^3 - 3n + 1),$$

ζ)

$$\sum_{k=1}^{n} k^7 = \frac{1}{24} n^2 (n+1)^2 (3n^4 + 6n^3 - n^2 - 4n + 2),$$

η)

$$\sum_{k=1}^{n} k^8 = \frac{1}{90} n(n+1)(2n+1)(5n^6 + 15n^5 + 5n^4 - 15n^3 - n^2 + 9n - 3),$$

θ)

$$\sum_{k=1}^{n} k^9 = \frac{1}{20} n^2 (n+1)^2 (n^2 + n - 1)(2n^4 + 4n^3 - n^2 - 3n + 3),$$

ι)

$$\sum_{k=1}^{n} k^{10} = \frac{1}{66} n(n+1)(2n+1)(n^2 + n - 1)(3n^6 + 9n^5 + 2n^4 - 11n^3 + 3n^2 + 10n - 5).$$

Απόδειξη. Όλες οι περιπτώσεις αποδεικνύονται επαγωγικά με τον ίδιο τρόπο. Ενδεικτικά θα επιλύσουμε την περίπτωση (ε).

Για $n = 1$ ισχύει. Ας υποθέσουμε ότι ισχύει για $n = s$. Θα δείξουμε ότι ισχύει για $n = s + 1$. Έχουμε:

$$\sum_{k=1}^{s+1} k^5 = \sum_{k=1}^{s} k^5 + (s+1)^5 = \frac{s^2 (s+1)^2 (2s^2 + 2s - 1)}{12} + (s+1)^5.$$

Εύκολα αποδεικνύεται ότι ισχύει

$$s^2 (s+1)^2 (2s^2 + 2s - 1) + 12(s+1)^5 = (s+1)^2 (s+2)^2 \Big(2(s+1)^2 + 2(s+1) - 1\Big).$$

Επομένως, η σχέση ισχύει για κάθε θετικό ακέραιο n. □

Στη συνέχεια, θα αποδείξουμε με την χρήση της μαθηματικής επαγωγής κάποιες ανισοτικές σχέσεις.

Άσκηση 1.4. *Να δειχθεί ότι ισχύει* $2^n > n + 1$, *για κάθε φυσικό* $n \geq 2$.

Απόδειξη. Αρχικά θα δείξουμε ότι ισχύει για $n = 2$. Πράγματι, για $n = 2$ έχουμε

$$2^2 > 2 + 1,$$

το οποίο προφανώς ισχύει. Ας υποθέσουμε ότι ισχύει για $n = k$. Θα δείξουμε ότι ισχύει για $n = k + 1$. Πράγματι, καθώς $k > 0$, έχουμε:

$$2^{k+1} = 2^k \cdot 2 > (k+1) \cdot 2 = 2k + 2 > k + 2.$$

□

΄Ασκηση 1.5. *Να δειχθεί ότι ισχύει $2^n > n^2$, για κάθε φυσικό $n \geq 5$.*

Απόδειξη. Αρχικά θα δείξουμε ότι ισχύει για $n = 5$. Για $n = 5$, έχουμε $2^5 = 32 > 25 = 5^2$ το οποίο αληθεύει. Υποθέτουμε ότι ισχύει για $n = k$. Θα δείξουμε ότι η ανισότητα αληθεύει και για $n = k + 1$. Καθώς $k > 5$, έχουμε:

$$(k-1)^2 > 2 \Longrightarrow k^2 - 2k + 1 > 2 \Longrightarrow k^2 > 2k + 1.$$

΄Ετσι, παίρνουμε:

$$2^{k+1} = 2 \cdot 2^k > 2k^2 = k^2 + k^2 > k^2 + 2k + 1 = (k+1)^2.$$

□

΄Ασκηση 1.6. *Να δειχθεί ότι ισχύει $n! > 2^n$, για κάθε φυσικό $n \geq 4$.*

Απόδειξη. Για $n = 4$, έχουμε:

$$4! = 24 > 16 = 2^4.$$

Υποθέτουμε ότι ισχύει για $n = k$, δηλαδή, ότι $k! > 2^k$. Θα δείξουμε ότι ισχύει και για $n = k + 1$. Πράγματι, έχουμε:

$$(k+1)! = k!\,(k+1) > 2^k(k+1) > 2^k\, 2 = 2^{k+1}.$$

□

΄Ασκηση 1.7. *Ας είναι $x \in \mathbb{R}$ με $0 < x < 1$. Να δειχθεί ότι για κάθε φυσικό $n \geq 2$, ισχύει:*

$$(1-x)^n > 1 - nx.$$

Απόδειξη. Για $n = 2$, καθώς $x \neq 0$, παίρνουμε:

$$(1-x)^2 = 1 - 2x + x^2 > 1 - 2x.$$

Ας υποθέσουμε ότι η ανισότητα ισχύει για $n > 2$. Θα δείξουμε ότι ισχύει και για $n + 1$. ΄Εχουμε:

$$\begin{aligned}(1-x)^{n+1} &= (1-x)^n(1-x) > \\ &(1-nx)(1-x) = 1 - nx - x + nx^2 > 1 - nx - x = 1 - (n+1)x.\end{aligned}$$

□

Στις επόμενες τρεις ασκήσεις θα αποδείξουμε επαγωγικά σχέσεις που περιέχουν την αναδρομική ακολουθία του Fibonacci (F_n). Υπενθυμίζουμε ότι η ακολουθία Fibonacci δίνεται από τις σχέσεις

$$F_1 = 1,\ F_2 = 1 \quad \text{και} \quad F_n = F_{n-1} + F_{n-2},\ \ \forall n \geq 3.$$

΄Ασκηση 1.8. *Ας είναι (F_n) η ακολουθία του Fibonacci και $\phi = \frac{1+\sqrt{5}}{2}$ η χρυσή τομή. Να δειχθεί ότι, για κάθε φυσικό $n \geq 1$, ισχύει:*

$$F_n \geq \phi^{n-2}.$$

Απόδειξη. Για $n = 1$, ισχύει $F_1 = 1 > 1/\phi$. Επίσης, για $n = 2$, έχουμε $F_2 = 1 \geq 1 = \phi^{2-2}$. Στη συνέχεια, υποθέτουμε ότι η ανισότητα αληθεύει, για κάθε n με $2 < n < k$. Θα δείξουμε ότι ισχύει και για $n = k$. Πράγματι, έχουμε:

$$F_k = F_{k-1} + F_{k-2} \geq \phi^{k-3} + \phi^{k-4} = \phi^{k-2}(\phi^{-1} + \phi^{-2}) = \phi^{k-2}.$$

□

΄Ασκηση 1.9. *Ας είναι (F_n) η ακολουθία του Fibonacci. Να δειχθεί ότι, για κάθε $n \geq 1$, ισχύει:*

$$F_{n+2} - 1 = \sum_{i=1}^{n} F_i.$$

Απόδειξη. Για $n = 1$ έχουμε:

$$F_3 - 1 = 2 - 1 = 1 = F_1.$$

Υποθέτουμε ότι ισχύει για κάθε n με $1 < n < k$. Θα δείξουμε ότι ισχύει και για $n = k$. Πράγματι, έχουμε:

$$\sum_{i=1}^{k} F_i = F_k + \sum_{i=1}^{k-1} F_i = F_k + F_{(k-1)+2} - 1 = F_k + F_{k+1} - 1 = F_{k+2} - 1.$$

□

΄Ασκηση 1.10. *Ας είναι (F_n) η ακολουθία του Fibonacci. Να δειχθεί ότι, για κάθε $n \geq 1$, ισχύει:*

$$F_n < \left(\frac{7}{4}\right)^n.$$

Απόδειξη. Για $n = 1$, έχουμε:

$$F_1 = 1 < \left(\frac{7}{4}\right)^1,$$

το οποίο ισχύει. Επιπλέον, για $n = 2$, έχουμε:

$$F_2 = 1 < \frac{49}{16} = \left(\frac{7}{4}\right)^2,$$

το οποίο ισχύει. Υποθέτουμε ότι ισχύει για κάθε n με $2 < n < k$. Θα δείξουμε ότι ισχύει και για $n = k$. Πράγματι, για κάθε $k \geq 3$, έχουμε:

$$F_k = F_{k-1} + F_{k-2} < \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2} = \left(\frac{7}{4}\right)^{k-2} \frac{11}{4} < \left(\frac{7}{4}\right)^k.$$

□

Ας σημειωθεί ότι στην προηγουμένη άσκηση χρησιμοποιήθηκε η Αρχή Μαθηματικής Επαγωγής (Β) με $n_0 = 2$. Τέλος παρουσιάζουμε και μια άσκηση όπου κάνουμε χρήση της δισδιάστατης μαθηματικής επαγωγής. Υπενθυμίζουμε τον συμβολισμό

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

όπου $n, k \in \mathbb{N}$ με $0 \leq k \leq n$. Η ποσότητα αυτή δίνει το πλήθος των συνδυασμών n αντικειμένων ανά k.

΄Ασκηση 1.11. *Ας είναι A ένα σύνολο με $n \geq 2$ στοιχεία. Να δείχθουν τα εξής:*
α) Το πλήθος των υποσυνόλων του A με δύο στοιχεία είναι $\binom{n}{2}$.
β) Το πλήθος των υποσυνόλων του A με $m \geq 2$ στοιχεία είναι $\binom{n}{m}$.

Απόδειξη. (α) ΄Εστω $n = 2$. Προφανώς ένα σύνολο A με δύο στοιχεία έχει ακριβώς ένα υποσύνολό με δύο στοιχεία, που είναι το ίδιο το σύνολο A. Από την άλλη πλευρά, έχουμε ότι $\binom{2}{2} = 1$. Οπότε, για $n = 2$ ισχύει. Ας υποθέσουμε ότι η πρόταση αληθεύει για $n = k$, δηλαδή, τα υποσύνολα με δύο στοιχεία ενός συνόλου με k στοιχεία είναι $\binom{k}{2}$. Θα δείξουμε ότι τα υποσύνολα με δύο στοιχεία ενός συνόλου με $n = k + 1$ στοιχεία είναι $\binom{k+1}{2}$. Ας είναι $A = \{a_1, \ldots, a_k, a_{k+1}\}$ και $B \subseteq A$ με $|B| = 2$. Αν $a_{k+1} \notin B$ τότε $B \subseteq \{a_1, \ldots, a_k\}$ και, σύμφωνα με την υπόθεση της επαγωγής, υπάρχουν $\binom{k}{2}$ το πλήθος διαφορετικά τέτοια σύνολα B. Αν $a_{k+1} \in B$, τότε το B είναι της μορφής $\{a_{k+1}, a_i\}$, όπου $i = 1, \ldots, n$, και επομένως υπάρχουν k το πλήθος διαφορετικά τέτοια σύνολα B. ΄Αρα υπάρχουν

$$k + \binom{k}{2} = k + \frac{k!}{2!(k-2)!} = \frac{2!(k-1)!k + k!(k-1)}{2!(k-1)!} = \frac{(k+1)!}{2!(k-1)!} = \binom{k+1}{2}$$

το πλήθος υποσύνολα με δύο στοιχεία.

(β) Σύμφωνα με το (α), η σχέση ισχύει για κάθε $n \geq 2$ και $m = 2$. Υποθέτουμε ότι ισχύει για κάθε υποσύνολο B του A με $|B| = m$ και $m < k \leq n$. Θα δείξουμε ότι η πρόταση ισχύει για $m = k$. Ας είναι $A = \{a_1, \ldots, a_n\}$ και $B \subseteq A$ με $|B| = k$. Αν $a_n \notin B$ τότε $B \subseteq \{a_1, \ldots, a_{n-1}\}$ και, σύμφωνα με την υπόθεση της επαγωγής, υπάρχουν $\binom{n-1}{k}$ το πλήθος διαφορετικά υποσύνολα B του A με $a_n \notin B$. Αν $a_n \in B$, τότε $B = \{a_n, a_{i_1}, \ldots, a_{i_{k-1}}\}$, όπου $i_j \in \{1, \ldots, n-1\}$. Δηλαδή, υπάρχουν $\binom{n-1}{k-1}$ το πλήθος διαφορετικά υποσύνολα B του A με $a_n \in B$. Οπότε αρκεί να αποδείξουμε ότι

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

Πράγματι, έχουμε:

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

□

Ασκήσεις με την χρήση της μαθηματικής επαγωγής υπάρχουν σε όλα τα κεφάλαια που ακολουθούν καθώς αποτελεί ένα από τα βασικά εργαλεία της Θεωρίας Αριθμών.

1.2 Σχέσεις Ισοδυναμίας

Οι σχέσεις ισοδυναμίας παίζουν ιδιαιτέρως σημαντικό ρόλο τόσο στη Θεωρία Αριθμών όσο και στην Άλγεβρα γενικότερα.

Ορισμός 1.3. Έστω σύνολο $\Sigma \neq \emptyset$ και S ένα υποσύνολο του $\Sigma \times \Sigma$. Το S καλείται *σχέση ισοδυναμίας* στο Σ, αν έχει τις εξής ιδιότητες:
1) $(x, x) \in S$, για κάθε $x \in \Sigma$ (*ανακλαστική*).
2) Αν $(x, y) \in S$, τότε έχουμε $(y, x) \in S$, για κάθε $x, y \in \Sigma$ (*συμμετρική*).
3) Αν $(x, y) \in S$, $(y, z) \in S$, τότε ισχύει $(x, z) \in S$, για κάθε $x, y, z \in \Sigma$ (*μεταβατική*).

Συνήθως αντί για $(x, y) \in S$ γράφουμε xSy ή $x \equiv y\ (S)$, όταν το S παραπέμπει σε σχέση ισοδυναμίας και το διαβάζουμε «x σε σχέση με το y» ή «x ισοδύναμο με το y ως προς S», αντίστοιχα.

Ορισμός 1.4. Δύο στοιχεία τα οποία συνδέονται με μία σχέση ισοδυναμίας S καλούνται *ισοδύναμα* ως προς S. Το σύνολο

$$[a] = \{x \in \Sigma \mid x \equiv a\ (S)\}$$

καλείται *κλάση ισοδυναμίας* του a. Το σύνολο

$$\Sigma/S = \{[x] \mid x \in \Sigma\}$$

καλείται *σύνολο πηλίκο* του Σ με την S.

Πρόταση 1.5. *Ας είναι S μία σχέση ισοδυναμίας στο Σ και $x, y \in \Sigma$. Τότε, έχουμε:*
α) $[x] \cap [y] = \emptyset \Rightarrow [x] = [y]$.
β) $[x] \equiv [y]\ (S) \Leftrightarrow [x] = [y]$.

Απόδειξη. [4, Κεφάλαιο 1, Πρόταση 1.13, Πρόταση 1.15] ή [3, Κεφάλαιο 1, Πρόταση 3.1, Πρόταση 3.2]. □

Ορισμός 1.5. Ας είναι U ένα σύνολο και $\{U_a\}_{a \in A}$ μια οικογένεια υποσυνόλων του U. Η οικογένεια $\{U_a\}_{a \in A}$ καλείται *διαμέριση* του U, αν ισχύουν τα εξής:
1) $U_a \neq \emptyset$, για κάθε $a \in A$.
2) $\bigcup_{a \in A} U_a = U$.
3) $U_i \neq U_j$, για κάθε ζεύγος δεικτών i, j με $i \neq j$.

Πρόταση 1.6. *Ας είναι $\{U_a\}_{a \in A}$ μια διαμέριση του Σ. Να δείξετε ότι η σχέση η οποία ορίζεται ως εξής:*

$$x \equiv y\ (S) \Leftrightarrow x \text{ και } y \text{ ανηκουν στο ίδιο σύνολο } U_a$$

είναι μια σχέση ισοδυναμίας στο Σ της οποίας οι κλάσεις της είναι τα σύνολα U_a.

Απόδειξη. [4, Κεφάλαιο 1, Πρόταση 1.14]. □

Όταν το πλήθος των κλάσεων ισοδυναμίας είναι μη πεπερασμένο, τότε μπορούμε μόνο να τις περιγράψουμε. Όταν το πλήθος των κλάσεων ισοδυναμίας είναι σχετικά μικρό, τότε μπορούμε και να τις προσδιορίσουμε. Η διαδικασία που ακολουθούμε

είναι η εξής: Ας είναι S μια σχέση ισοδυναμίας στο σύνολο Σ. Παίρνουμε αρχικά ένα στοιχείο $a_1 \in \Sigma$ (κάποιο που να μας βολεύει για τους υπολογισμούς ή τυχαία) και υπολογίζουμε την κλάση ισοδυναμίας του $[a_1]$. Εφόσον η κλάση του a_1 δεν είναι ίση με το Σ, στη συνέχεια παίρνουμε ένα στοιχείο $a_2 \in \Sigma$ που να μην ανήκει στο $[a_1]$ και υπολογίζουμε την κλαση του. Αν $[a_1] \cup [a_2] \neq \Sigma$, τότε παίρνουμε ένα στοιχείο $a_2 \in \Sigma$ που να μην ανήκει στο $[a_1] \cup [a_2]$ κ.ο.κ.. Συνεχίζουμε την διαδικασία μέχρι να καταλήξουμε στην ισότητα

$$[a_1] \cup [a_2] \cup \cdots \cup [a_k] = \Sigma,$$

οπότε και έχουμε προσδιορίσει όλες τις διαφορετικές κλάσεις ισοδυναμίας, δηλαδή όλα τα διαφορετικά στοιχεία του $\Sigma/(S)$.

Ασκήσεις

΄Ασκηση 1.12. *Να δειχθεί ότι η σχέση*

$$x \equiv y \ (S) \iff x - y \in \mathbb{Z}$$

είναι μία σχέση ισοδυναμίας στο $\mathbb{R}$ *και να προσδιοριστούν οι κλάσεις* $[0]$ *και* $[\sqrt{3}]$.

Απόδειξη. Για κάθε $x \in \mathbb{R}$ έχουμε $x - x = 0 \in \mathbb{Z}$ και επομένως $x \equiv x \ (S)$. ΄Αρα, η σχέση S είναι ανακλαστική.

Ας είναι $x, y \in \mathbb{R}$ με $x \equiv y \ (S)$. Τότε $x - y \in \mathbb{Z}$ και επομένως $y - x = -(x - y) \in \mathbb{Z}$. ΄Αρα $y \equiv x \ (S)$ και κατά συνέπεια η σχέση S είναι συμμετρική.

Τέλος, η σχέση S είναι μεταβατική. Πράγματι, αν $x, y, z \in \mathbb{R}$, με $x \equiv y \ (S)$ και $y \equiv z \ (S)$, τότε $x - y \in \mathbb{Z}$ και $y - z \in \mathbb{Z}$, απ΄ όπου παίρνουμε $x - z \in \mathbb{Z}$. ΄Αρα $x \equiv z \ (S)$.

Από το ορισμό της κλάσης ισοδυναμίας προκύπτει:

$$[0] = \{x \in \mathbb{R} \mid x \equiv 0 \ (S)\} = \{x \in \mathbb{R} \mid x \in \mathbb{Z}\} = \mathbb{Z}$$

και

$$[\sqrt{3}] = \{x \in \mathbb{R} \mid x \equiv \sqrt{3} \ (S)\} = \{x \in \mathbb{R} \mid x - \sqrt{3} \in \mathbb{Z}\} = \{x + \sqrt{3} \mid x \in \mathbb{Z}\}.$$

□

΄Ασκηση 1.13. *Να δειχθεί ότι η σχέση*

$$x \equiv y \ (S) \iff \exists\, k \in \mathbb{Z} \text{ τέτοιο, ώστε } x - y = 2k$$

είναι μία σχέση ισοδυναμίας στο $\mathbb{Z}$ *και να προσδιοριστούν όλες οι κλάσεις ισοδυναμίας της.*

Απόδειξη. Για κάθε $x \in \mathbb{Z}$ έχουμε $x - x = 0 = 2 \cdot 0$ και επομένως $x \equiv x \ (S)$. ΄Αρα, η σχέση S είναι ανακλαστική.

Ας είναι $x, y \in \mathbb{Z}$, με $x \equiv y \ (S)$. Τότε, υπάρχει $k \in \mathbb{Z}$ με $x - y = 2k$, απ΄ όπου έχουμε $y - x = 2(-k)$ και επομένως $y \equiv x \ (S)$. ΄Αρα, η σχέση S είναι συμμετρική.

Ας είναι $x, y, z \in \mathbb{Z}$ με $x \equiv y \ (S)$ και $y \equiv z \ (S)$. Τότε, υπάρχουν $k_1, k_2 \in \mathbb{Z}$ με $x - y = 2k_1$ και $y - z = 2k_2$ και επομένως έχουμε $x - z = 2(k_1 + k_2)$. Καθώς $k_1 + k_2 \in \mathbb{Z}$, παίρνουμε $x \equiv z \ (S)$. Συνεπώς, η σχέση S είναι μεταβατική.

Κάθε ακέραιος είναι άρτιος ή περιττός. Επομένως, για κάθε ακέραιο x έχουμε $x \equiv 0\ (S)$ ή $x \equiv 1\ (S)$. Συνεπώς, έχουμε μόνο τις εξής δύο κλάσεις ισοδυναμίας:

$$[0] = \{x \in \mathbb{Z} \mid x \equiv 0\ (S)\} = \{x \in \mathbb{Z} \mid \exists\, k \in \mathbb{Z} : x = 2k\} = \{x \in \mathbb{Z} \mid x \text{ άρτιος}\}$$

και

$$[1] = \{x \in \mathbb{Z} \mid x \equiv 1\ (S)\} = \{x \in \mathbb{Z} \mid \exists\, k \in \mathbb{Z} : x = 2k+1\} = \{x \in \mathbb{Z} \mid x \text{ περιττός}\}.$$

□

΄Ασκηση 1.14. *Ας είναι Σ ένα μη κενό σύνολο και A ένα υποσύνολό του. Ορίζουμε μια σχέση S στο Σ ως εξής:*

$$x \equiv y\ (S) \iff x = y \text{ ή } x, y \in A.$$

Να δειχτεί ότι η S είναι μια σχέση ισοδυναμίας και να προσδιορισμούν οι κλάσεις ισοδυναμίας των στοιχείων του Σ.

Απόδειξη. Καθώς για κάθε $x \in \Sigma$ ισχύει $x = x$, έχουμε $x \equiv x\ (S)$ και επομένως η σχέση S είναι ανακλαστική.

Ας είναι $x, y \in \Sigma$ με $x \equiv y\ (S)$. Τότε, $x = y$ ή $x, y \in A$ και επομένως $y \equiv x\ (S)$. ΄Αρα, η σχέση S είναι συμμετρική.

Ας είναι $x, y, z \in \Sigma$ με $x \equiv y\ (S)$ και $y \equiv z\ (S)$. Τότε, $x = y$ ή $x, y \in A$ και $y = z$ ή $y, z \in A$. Αν $x = y$, τότε $x = z$ ή $x, z \in A$ και κατά συνέπεια $x \equiv z\ (S)$. Επίσης, αν $x, y \in A$, τότε $x, z \in A$ και επομένως $x \equiv z\ (S)$. ΄Αρα, η σχέση S είναι μεταβατική. Συνεπώς, η S είναι σχέση ισοδυναμίας.

Ας είναι $x \in \Sigma$. Αν $x \notin A$, τότε $[x] = \{x\}$ και αν $x \in A$, τότε $[x] = A$. □

Στην συνέχεια θα δούμε μερικές σχέσεις ισοδυναμίας σε σύνολα που είναι καρτεσιανά γινόμενα.

΄Ασκηση 1.15. *Να δειχθεί ότι η σχέση*

$$(x_1, y_1) \equiv (x_2, y_2)\ (S) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2$$

είναι μία σχέση ισοδυναμίας στο $\mathbb{R}^2$ και να περιγραφούν οι κλάσεις ισοδυναμίας αλγεβρικά και γεωμετρικά.

Απόδειξη. Για κάθε $(x, y) \in \mathbb{R}^2$ ισχύει $x^2 + y^2 = x^2 + y^2$ και επομένως $(x, y) \equiv (x, y)\ (S)$. ΄Αρα, η σχέση S είναι ανακλαστική.

Ας είναι $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ με $(x_1, y_1) \equiv (x_2, y_2)\ (S)$. Τότε, $x_1^2 + y_1^2 = x_2^2 + y_2^2$ και επομένως $x_2^2 + y_2^2 = x_1^2 + y_1^2$. ΄Αρα, έχουμε $(x_2, y_2) \equiv (x_1, y_1)\ (S)$ και επομένως η σχέση S είναι συμμετρική.

Ας είναι $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$ με $(x_1, y_1) \equiv (x_2, y_2)\ (S)$ και $(x_2, y_2) \equiv (x_3, y_3)\ (S)$. Τότε, $x_1^2 + y_1^2 = x_2^2 + y_2^2$ και $x_2^2 + y_2^2 = x_3^2 + y_3^2$, απ΄ όπου $(x_1, y_1) \equiv (x_3, y_3)\ (S)$. ΄Αρα, η σχέση S είναι μεταβατική. Επομένως, η S είναι σχέση ισοδυναμίας.

Η κλάση ισοδυναμίας ενός ζεύγους $(x_0, y_0) \in \mathbb{R}^2$ είναι το σύνολο

$$[(x_0, y_0)] = \{(x, y) \in \mathbb{R}^2 \mid (x, y) \equiv (x_0, y_0)\ (S)\} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = x_0^2 + y_0^2\},$$

δηλαδή, η κλάση ισοδυναμίας του (x_0, y_0) αποτελείται από τα σημεία ενός κύκλου με κέντρο την αρχή των αξόνων και ακτίνα $\sqrt{x_0^2 + y_0^2}$. □

΄Ασκηση 1.16. *Ας είναι $A = \{1, 2, 3\}$ και $B = A \times A$. Θεωρούμε την σχέση S στο B η οποία ορίζεται ως εξής:*

$$(x_1, y_1) \equiv (x_2, y_2)\ (S) \iff x_1 + y_1 = x_2 + y_2.$$

Να δειχθεί οτι η S είναι σχέση ισοδυναμίας και να προσδιοριστούν οι κλάσεις της.

Απόδειξη. Για κάθε $(x, y) \in B$ ισχύει $x + y = x + y$ και επομένως $(x, y) \equiv (x, y)\ (S)$. ΄Αρα, η σχέση S είναι ανακλαστική.

Ας είναι $(x_1, y_1), (x_2, y_2) \in B$ με $(x_1, y_1) \equiv (x_2, y_2)\ (S)$. Τότε, έχουμε $x_1 + y_1 = x_2 + y_2$ και επομένως $x_2 + y_2 = x_1 + y_1$. ΄Αρα, $(x_2, y_2) \equiv (x_1, y_1)\ (S)$ και κατά συνέπεια η σχέση S είναι συμμετρική.

Ας είναι $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in B$ με $(x_1, y_1) \equiv (x_2, y_2)\ (S)$ και $(x_2, y_2) \equiv (x_3, y_3)\ (S)$. Τότε, έχουμε $x_1+y_1 = x_2+y_2$ και $x_2+y_2 = x_3+y_3$, απ΄ όπου έπεται $x_1+y_1 = x_3+y_3$. ΄Ετσι, έχουμε $(x_1, y_1) \equiv (x_3, y_3)\ (S)$ και επομένως η σχέση S είναι μεταβατική. Επομένως, η S είναι σχέση ισοδυναμίας.

Η κλάση ισοδυναμίας ενός ζεύγους $(x_0, y_0) \in B$ είναι το σύνολο

$$[(x_0, y_0)] = \{(x, y) \in B \mid (x, y) \equiv (x_0, y_0)\ (S)\} = \{(x, y) \in B \mid x + y = x_0 + y_0\},$$

δηλαδή, η κλάση ισοδυναμίας του (x_0, y_0) αποτελείται από τα ζεύγη (x, y) του B που έχουν ίδιο άθροισμα συντεταγμένων. Επομένως, οι κλάσεις ισοδυναμίας της S είναι:

$$\begin{aligned}
&[(1,1)] = \{(1,1)\},\\
&[(1,2)] = \{(1,2),(2,1)\},\\
&[(1,3)] = \{(1,3),(2,2),(3,1)\},\\
&[(2,3)] = \{(3,2),(2,3)\},\\
&[(3,3)] = \{(3,3)\}.
\end{aligned}$$

□

΄Ασκηση 1.17. *Ας είναι $B = \mathbb{R} \times \mathbb{R}$ και (S) σχέση στο B, η οποία ορίζεται ως εξής:*

$$(x_1, y_1) \equiv (x_2, y_2)\ (S) \iff 2(x_1 - x_2) = y_1 - y_2.$$

Να δειχθεί ότι η (S) είναι σχέση ισοδυναμίας και να περιγραφούν αλγεβρικά και γεωμετρικά οι κλάσεις της.

Απόδειξη. Για κάθε $(x, y) \in B$ έχουμε $2(x-x) = 0 = y-y$ και επομένως $(x, y) \equiv (x, y)\ (S)$. ΄Αρα, η σχέση S είναι ανακλαστική.

Αν $(x_1, y_1), (x_2, y_2) \in B$ με $(x_1, y_1) \equiv (x_2, y_2)\ (S)$, τότε έχουμε $2(x_1 - x_2) = y_1 - y_2$ και επομένως $2(x_2 - x_1) = y_2 - y_1$, απ΄ όπου $(x_2, y_2) = (x_1, y_1)\ (S)$. Επομένως, η σχέση (S) είναι συμμετρική.

Ας είναι $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in B$ με $(x_1, y_1) \equiv (x_2, y_2)\ (S)$ και $(x_2, y_2) \equiv (x_3, y_3)\ (S)$. Τότε, έχουμε $2(x_1 - x_2) = y_1 - y_2$ και $2(x_2 - x_3) = y_2 - y_3$, απ΄ όπου παίρνουμε $2(x_1 - x_3) = y_1 - y_3$ και κατά συνέπεια $(x_1, y_1) \equiv (x_3, y_3)\ (S)$. ΄Αρα, η σχέση (S) είναι μεταβατική. Συνεπώς, η (S) είναι σχέση ισοδυναμίας.

Η κλάση ισοδυναμίας ενός ζεύγους (x_0, y_0) είναι το σύνολο:

$$\begin{aligned}[(x_0, y_0)] &= \{(x, y) \in B \mid (x, y) \equiv (x_0, y_0)\ (S)\} \\ &= \{(x, y) \in B \mid 2(x - x_0) = y - y_0\} \\ &= \{(x, y) \in B \mid y = 2x - 2x_0 + y_0\}.\end{aligned}$$

Δηλαδή, η κλάση ισοδυναμίας του ζεύγους (x_0, y_0) αποτελείται από τα σημεία της ευθείας $y = 2x - 2x_0 + y_0$ του καρτεσιανού επιπέδου. Επομένως, οι κλάσεις ισοδυναμίας της σχέσης S είναι όλες οι ευθείες του καρτεσιανού επιπέδου με κλίση 2. □

΄Ασκηση 1.18. *Θεωρούμε την εξής σχέση στο* $\mathbb{R}^3$*:*

$$(x_1, y_1, z_1) \equiv (x_2, y_2, z_2)\ (S) \iff x_1 - x_2 = 3y_1 - 3y_2.$$

Να δειχθεί ότι η S *είναι μία σχέση ισοδυναμίας στο* $\mathbb{R}^3$ *και να περιγραφούν αλγεβρικά και γεωμετρικά οι κλάσεις της.*

Απόδειξη. Ας είναι $(x, y, z) \in \mathbb{R}^3$. Τότε, ισχύει $x - x = 0 = 3y - 3y$ και επομένως $(x, y, z) \equiv (x, y, z)\ (S)$. ΄Αρα, η σχέση S είναι ανακλαστική.

Ας είναι $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{R}^2$ με $(x_1, y_1, z_1) \equiv (x_2, y_2, z_2)\ (S)$. Τότε $x_1 - x_2 = 3y_1 - 3y_2$, απ΄ όπου $x_2 - x_1 = 3y_2 - 3y_1$ και επομένως $(x_2, y_2, z_2) \equiv (x_1, y_1, z_1)\ (S)$. ΄Αρα, η σχέση S είναι συμμετρική.

Ας είναι $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) \in \mathbb{R}^2$, με $(x_1, y_1, z_1) \equiv (x_2, y_2, z_2)\ (S)$ και $(x_2, y_2, z_2) \equiv (x_3, y_3, z_3)\ (S)$ τότε $x_1 - x_2 = 3y_1 - 3y_2$, $x_2 - x_3 = 3y_2 - 3y_3$, απ΄ όπου $x_1 - x_3 = 3y_1 - 3y_3$. ΄Αρα $(x_1, y_1, z_1) \equiv (x_3, y_3, z_3)\ (S)$ και επομένως η σχέση S είναι μεταβατική.

Η κλάση ισοδυναμίας μίας τριάδας (x_0, y_0, z_0) είναι το σύνολο:

$$\begin{aligned}[(x_0, y_0, z_0)] &= \{(x, y, z) \in \mathbb{R}^3 \mid (x, y, z) \equiv (x_0, y_0, z_0)\ (S)\} \\ &= \{(x, y, z) \in \mathbb{R}^3 \mid x - 3y = x_0 - 3y_0\}.\end{aligned}$$

Δηλαδή, κάθε κλάση ισοδυναμίας αποτελείται από τα σημεία του επιπέδου στο τρισδιάστατο χώρο που τέμνει το επίπεδο των αξόνων x και y κάθετα και η τομή τους είναι η ευθεία $x - 3y = x_0 - 3y_0$. □

1.3 Ακέραιοι

"Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk" φέρεται να έχει πει ο Leopold Kronecker, δηλαδή, «ο Θεός έφτιαξε τους ακέραιους, όλα τα υπόλοιπα είναι ανθρώπινη δουλειά».

Ας είναι S η σχέση ισοδυναμίας στο σύνολο $\mathbb{N} \times \mathbb{N}$ η οποία ορίζεται ως εξής: για κάθε $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ έχουμε

$$(a, b) \equiv (c, d)\ (S) \iff a + d = b + c.$$

Ορισμός 1.6. Το σύνολο πηλίκο $\mathbb{N} \times \mathbb{N}/S$ καλείται *σύνολο των ακεραίων* και συμβολίζεται με $\mathbb{Z}$ και τα στοιχεία του καλούνται *ακέραιοι*.

Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε τις πράξεις της πρόσθεσης «+» και του πολλαπλασιασμού «·» ως εξής:

$$[(a,b)] + [(c,d)] = [(a+c, b+d)],$$
$$[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)].$$

Ας σημειωθεί ότι τα αποτελέσματα αυτών των πράξεων είναι ανεξάρτητα από τους αντιπροσώπους των κλάσεων οι οποίες χρησιμοποιήθηκαν. Συχνά όταν γράφουμε το γινόμενο των αριθμών παραλείπουμε το σύμβολο του πολλαπλασιασμού. Για κάθε $x, y, z \in \mathbb{Z}$ ισχύουν τα εξής:

α) $x + (y+z) = (x+y) + z$, $x(yz) = (xy)z$ (προσεταιριστικός νόμος).
β) $x + y = y + x$, $xy = yx$ (αντιμεταθετικός νόμος).
γ) $x(y+z) = xy + xz$ (επιμεριστικός νόμος).

Για τις κλάσεις $[(0,0)]$ και $[(1,0)]$ ισχύουν τα εξής:

$$[(a,b)] + [(0,0)] = [(a,b)] \quad \text{και} \quad [(a,b)] \cdot [(1,0)] = [(a,b)],$$

για κάθε $[(a,b)] \in \mathbb{Z}$. Επίσης, για κάθε $[(a,b)] \in \mathbb{Z}$, έχουμε:

$$[(a,b)] + [(b,a)] = [(a+b, a+b)] = [(0,0)].$$

Ο $[(b,a)]$ καλείται *αντίθετος* του $[(a,b)]$ και συμβολίζεται με $-[(a,b)]$.

Ορισμός 1.7. Ο ακέραιος $[(a,b)]$ καλείται *μικρότερος* (αντ. *μεγαλύτερος*) του $[(c,d)]$ και γράφουμε $[(a,b)] < [(c,d)]$ (αντ. $[(a,b)] > [(c,d)]$) αν και μόνον αν ισχύει $a+d < b+c$ (αντ. $a+d > b+c$). Ένας ακέραιος x καλείται *θετικός*, αν ισχύει $x > 0$ και *αρνητικός*, αν $x < 0$.

Συμβολίζουμε συνήθως με $\mathbb{Z}^+$ το σύνολο των θετικών ακεραίων. Αν $x, y \in \mathbb{Z}$ με $x = y$ ή $x < y$, τότε γράφουμε $x \leq y$ ή $y \geq x$. Οι διαφορετικές κλάσεις του $\mathbb{Z}$ είναι οι εξής:

$$[(n,0)], [(0,0)], [(0,n)], \quad n \in \mathbb{N}.$$

Θεωρούμε την απεικόνιση $\varphi : \mathbb{N} \to \mathbb{Z}$ με $\varphi(n) = [(n,0)]$, για κάθε $n \in \mathbb{N}$. Η απεικόνιση φ είναι ένεση και για κάθε $m, n \in \mathbb{N}$ έχουμε:

α) $\varphi(m+n) = \varphi(m) + \varphi(n)$,
β) $\varphi(mn) = \varphi(m)\varphi(n)$,
γ) $m < n \Rightarrow \varphi(m) < \varphi(n)$.

Έτσι, μπορούμε να ταυτίζοντας τον φυσικό αριθμό n με την κλάση $[(n,0)]$ μπορούμε να θεωρήσουμε το $\mathbb{N}$ ως υποσύνολο του $\mathbb{Z}$. Απλοποιώντας την γραφή για τα στοιχεία του $\mathbb{Z}$ γράφουμε $-n$, 0, n, αντί $[(0,n)]$, $[(0,0)]$, $[(n,0)]$, αντίστοιχα (όπου $n \in \mathbb{N} \setminus \{0\}$), παίρνουμε την συνήθη γραφή των ακεραίων αριθμών.

Για περισσότερες πληροφορίες σχετικά με την κατασκευή ακεραίων ο αναγνώστης μπορεί να συμβουλευτεί στα συγγράμματα [1, Κεφάλαιο 2], [3, Ενότητα 1.4] και [4, Ενότητα 2.1], ενώ στο [3, Ενότητα 1.5] υπάρχει ο τρόπος κατασκευής του συνόλου των ρητών αριθμών το οποίο περιγράφουμε ως εξής:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Στη συνέχεια θα δούμε κάποιες ασκήσεις που αφορούν γνωστές ιδιότητες των ακεραίων αριθμών.

Ασκήσεις

΄Ασκηση 1.19. *Ας είναι $x, y, z \in \mathbb{Z}$. Να δειχθεί ότι ισχύουν τα εξής:*

α) $x0 = 0$.
β) $xy = 0 \Rightarrow x = 0$ *ή* $y = 0$.
γ) $x + y = x + z \Rightarrow y = z$.
δ) $x \neq 0$ *και* $xy = xz \Rightarrow y = z$.

Απόδειξη. α) Ας είναι $x \geq 0$. Το x αντιστοιχεί στην κλάση $[(x, 0)]$ και το 0 στην κλάση $[(0, 0)]$. Οπότε, έχουμε:

$$x\,0 = [(x, 0)]\,[(0, 0)] = [(x \cdot 0 + 0 \cdot 0, x \cdot 0 + 0 \cdot 0)] = [(0, 0)] = 0.$$

Αν $x < 0$, τότε το x αντιστοιχεί στην κλάση $[(0, x)]$. Ομοίως συμπεραίνουμε ότι ισχύει $x0 = 0$.

β) Ας είναι $x > 0$ και $y > 0$. Τότε $x = [(m, 0)]$ και $y = [(n, 0)]$, όπου $m, n \in \mathbb{N}$. Από την σχέση $xy = 0$, έχουμε

$$[(m, 0)]\,[(n, 0)] = [(0, 0)],$$

απ΄ όπου $[(mn, 0)] = [(0, 0)]$. ΄Ετσι, έχουμε $mn = 0$ και επομένως η Πρόταση 1.1(στ) δίνει $m = 0$ ή $n = 0$. ΄Αρα, ισχύει $x = 0$ ή $y = 0$. Αν $x > 0$ και $y < 0$, τότε $x = [(m, 0)]$ και $y = [(0, n)]$, όπου $m, n \in \mathbb{N}$. Από την ισότητα $xy = 0$, έχουμε

$$[(m, 0)]\,[(0, n)] = [(0, 0)],$$

απ΄ όπου έπεται $[(0, mn)] = [(0, 0)]$. ΄Ετσι, παίρνουμε $mn = 0$ και επομένως προκύπτει όπως και προηγουμένως ότι $x = 0$ ή $y = 0$. Τέλος, αν $x > 0$ και $y < 0$, τότε ομοίως προκύπτει το ζητούμενο.

γ) Ας είναι $x = [(a, b)]$, $y = [(c, d)]$ και $z = [(e, f)]$, όπου $a, b, c, d, e, f \in \mathbb{N}$. Από την ισότητα $x + y = x + z$ έχουμε:

$$[(a + c, b + d)] = [(a + e, b + f)]$$

ή

$$(a + c) + (b + f) = (b + d) + (a + e).$$

Χρησιμοποιώντας την Πρόταση 1.1, οι νόμοι του προσεταιρισμού και αντιμετάθεσης δίνουν:

$$(a + b) + (c + f) = (a + b) + (e + d).$$

Στη συνέχεια, ο νόμος διαγραφής δίνει $c + f = e + d$, απ΄ όπου έπεται $[(c, d)] = [(e, f)]$, δηλαδή $y = z$.

δ) Ας είναι $y = [(c, d)]$ και $z = [(e, f)]$, όπου $c, d, e, f \in \mathbb{N}$. Πρώτα, ας υποθέσουμε ότι $x = [(n, 0)]$, όπου $n > 0$. Από την ισότητα $xy = xz$ παίρνουμε:

$$[(nc, nd)] = [(ne, nf)].$$

΄Ετσι, έχουμε $nc + nf = nd + ne$ και επομένως οι νόμοι της επιμεριστικότητας και διαγραφής δίνουν $c + f = d + e$, απ΄ όπου προκύπτει $y = z$. Στη συνέχεια, αν $x = [(0, n)]$, όπου $n > 0$, με τον ίδιο τρόπο καταλήγουμε στο ζητούμενο. □

΄Ασκηση 1.20. *Ας είναι $a, b \in \mathbb{Z}$. Να δειχθεί ότι ισχύει $a < b$ αν και μόνον αν υπάρχει φυσικός $k > 0$ τέτοιος, ώστε $a + k = b$.*

Απόδειξη. Ας είναι $a = [(\alpha, \beta)]$ και $b = [(\gamma, \delta)]$, όπου $\alpha, \beta, \gamma, \delta \in \mathbb{N}$. Ισχύει:

$$a < b \Longleftrightarrow \alpha + \delta < \beta + \gamma.$$

Από την άλλη πλευρά, έχουμε:

$$\alpha + \delta < \beta + \gamma \Longleftrightarrow \exists\, \kappa \neq 0 \quad \text{με} \quad \alpha + \delta + \kappa = \beta + \gamma.$$

Η τελευταία όμως ισότητα ισχύει αν και μόνον αν

$$[(\alpha + \kappa, \beta)] = [(\gamma, \delta)],$$

ή ισοδύναμα

$$[(\alpha, \beta)] + [(\kappa, 0)] = [(\gamma, \delta)].$$

Δείξαμε λοιπόν ότι $a < b$ αν και μόνον αν υπάρχει φυσικός $k > 0$ τέτοιος, ώστε $a + k = b$. □

΄Ασκηση 1.21. *Ας είναι $a, b \in \mathbb{Z}$. Τότε ισχύει μονο μία από τις παρακάτω σχέσεις:*

$$a < b \quad \text{ή} \quad a = b \quad \text{ή} \quad a > b.$$

Απόδειξη. Ας είναι $a = [(\alpha, \beta)]$ και $b = [(\gamma, \delta)]$, όπου $\alpha, \beta, \gamma, \delta \in \mathbb{N}$. Τότε, από την Πρόταση 1.2 έχουμε:

$$\alpha + \delta < \beta + \gamma \quad \text{ή}\ \alpha + \delta = \beta + \gamma \quad \text{ή}\ \alpha + \delta < \beta + \gamma.$$

΄Αρα, ισχύει:

$$a < b \quad \text{ή} \quad a = b \quad \text{ή} \quad a > b.$$

□

΄Ασκηση 1.22. *Ας είναι $a, b, c \in \mathbb{Z}$. Να δειχθεί ότι ισχύουν τα εξής:*

α) *Αν $a < b$ και $b < c$, τότε $a < c$.*

β) *Αν $a < b$, τότε $a + c < b + c$.*

γ) *Αν $a < b$ και $c \neq 0$, τότε $ac < bc$ αν $c > 0$ και $ac > bc$ αν $c < 0$.*

Απόδειξη. Ας είναι $a = [(\alpha, \beta)]$, $b = [(\gamma, \delta)]$ και $c = [(\epsilon, \zeta)]$, όπου $\alpha, \beta, \gamma, \delta, \epsilon, \zeta \in \mathbb{N}$.

α) Από τις σχέσεις $a < b$ και $b < c$ έχουμε:

$$\alpha + \delta < \beta + \gamma \quad \text{και} \quad \gamma + \zeta < \delta + \epsilon.$$

Εφαρμόζοντας την ΄Ασκηση 1.1(β) παίρνουμε:

$$\alpha + \delta + \gamma + \zeta < \beta + \gamma + \gamma + \zeta$$

και

$$\beta + \gamma + \gamma + \zeta < \beta + \gamma + \delta + \epsilon.$$

Συνδυάζοντας τις δύο ανισότητες, η ΄Ασκηση 1.1(α) δίνει:

$$\alpha + \delta + \gamma + \zeta < \beta + \gamma + \delta + \epsilon.$$

Στη συνέχεια, από την ΄Ασκηση 1.1(β) έχουμε:

$$\alpha + \zeta < \beta + \epsilon.$$

Συνεπώς, ισχύει $a < c$.

β) Από την ανισότητα $a < b$ έχουμε:

$$\alpha + \delta < \beta + \gamma.$$

΄Ετσι, η ΄Ασκηση 1.1(β) δίνει:

$$\alpha + \delta + \epsilon + \zeta < \beta + \gamma + \epsilon + \zeta.$$

Καθώς $a + c = [(\alpha + \epsilon, \beta + \zeta)]$ και $b + c = [(\gamma + \epsilon, \delta + \zeta)]$, παίρνουμε

$$a + c < b + c.$$

γ) Καθώς $c > 0$, έχουμε $c = [(n, 0)]$, με $n > 0$. ΄Ετσι, παίρνουμε:

$$ac = [(\alpha n, \beta n)] \quad \text{και} \quad bc = [(\gamma n, \delta n)].$$

Από την ανισότητα $a < b$ έχουμε:

$$\alpha + \delta < \beta + \gamma.$$

Χρησιμοποιώντας την ΄Ασκηση 1.1(δ), παίρνουμε:

$$(\alpha + \delta)n < (\beta + \gamma)n.$$

΄Ετσι, έχουμε:

$$\alpha n + \delta n < \beta n + \gamma n.$$

Επομένως, έχουμε $ac < bc$.

Στη συνέχεια, υποθέτουμε ότι $c < 0$. Επομένως $c = [(0, n)]$, με $n > 0$. ΄Ετσι, έχουμε:

$$ac = [(\beta n, \alpha n)] \quad \text{και} \quad bc = [(\delta n, \gamma n)].$$

Η σχέση $a < b$ ισοδυναμεί με την ανισότητα

$$\alpha + \delta < \beta + \gamma.$$

Χρησιμοποιώντας την ΄Ασκηση 1.1(δ), παίρνουμε:

$$(\alpha + \delta)n < (\beta + \gamma)n$$

ή

$$\alpha n + \delta n < \beta n + \gamma n.$$

΄Ετσι, παίρνουμε $bc < ac$. □

΄Ασκηση 1.23. *Ας είναι $a \in \mathbb{Z}$ και $\mathbb{Z}_a$ το σύνολο των ακεραίων με στοιχεία μεγαλύτερα ή ίσα του a. Να δειχθεί ότι κάθε μη κενό υποσύνολο S του $\mathbb{Z}_a$ περιέχει ένα ελάχιστο στοιχείο, δηλαδή ένα στοιχείο $s \in S$ τέτοιο, ώστε $s \leq x$, για κάθε $x \in S$.*

Απόδειξη. Αν $S \subseteq \mathbb{N}$, τότε, σύμφωνα με την Πρόταση 1.4, το S έχει ελάχιστο στοιχείο. Ας υποθέσουμε ότι $S \nsubseteq \mathbb{N}$. Τότε, έχουμε $a < 0$. Παρατηρούμε ότι οι αριθμοί του $\mathbb{Z}_a$ οι οποίοι είναι αρνητικοί είναι οι εξής:

$$a, a+1, \ldots, a+(-a-1) = -1.$$

Επίσης, έχουμε:

$$a < a+1 < \ldots < -2 < -1.$$

Ο μικρότερος από αυτούς που ανήκει στο σύνολο S είναι και το ελάχιστο στοιχείο του S. □

1.4 Αλγεβρικές Δομές

Οι αλγεβρικές δομές έχουν κυρίαρχο ρόλο στον τομέα της ΄Αλγεβρας. Για παράδειγμα, αν γνωρίζουμε ότι ένα σύνολο A έχει κάποια συγκεκριμένη αλγεβρική δομή, τότε κάθε αποτέλεσμα που είναι γνωστό σχετικά με αυτήν ισχύει αυτόματα για το A. Σε αυτή την ενότητα θα δώσουμε τις έννοιες βασικών δομών και ασκήσεις επί των βασικών τους ιδιοτήτων. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να συμβουλευτεί το [1, 4].

Ορισμός 1.8. Ας είναι G ένα μη κενό σύνολο. Καλούμε *πράξη* επί του G μία απεικόνιση $* : G \times G \to G$. Αν $(x, y) \in G \times G$, τότε θα συμβολίζουμε με $x * y$ την εικόνα του ζεύγους (x, y). Λέμε ότι:

α) η πράξη $*$ είναι *προσεταιριστική* στο G, αν για κάθε $x, y, z \in G$ ισχύει:

$$x * (y * z) = (x * y) * z,$$

β) η πράξη $*$ είναι *αντιμεταθετική* στο G, αν για κάθε $x, y \in G$ ισχύει:

$$x * y = y * y,$$

γ) η πράξη $*$ έχει *ουδέτερο στοιχείο* στο G, αν υπάρχει $e \in G$, τέτοιο ώστε για κάθε $x \in G$

$$x * e = x = e * x,$$

δ) ένα στοιχείο $x \in G$ έχει *συμμετρικό*, αν υπάρχει $x' \in G$ τέτοιο, ώστε

$$x * x' = e = x' * x.$$

Το ζεύγος $(G, *)$ καλείται *ημιομάδα* αν η πράξη $*$ είναι προσεταιριστική στην G, *μονοειδές* αν επιπλέον η πράξη έχει ουδέτερο στοιχείο και *ομάδα* αν επιπλέον κάθε στοιχείο του G έχει συμμετρικό. Αν η πράξη είναι αντιμεταθετική, τότε η ημιομάδα (αντίστοιχα μονοειδές, ομάδα) $(G, *)$ καλείται αντιμεταθετική (αντίστοιχα αντιμεταθετικό, αβελιανή ή αντιμεταθετική). Το e καλείται *ουδέτερο στοιχείο* της πράξης $*$ και το x' *συμμετρικό* του x ως προς την πράξη $*$.

Ας σημειωθεί ότι αν μία πράξη έχει ουδέτερο στοιχείο, τότε αυτό είναι μοναδικό. Επίσης, το συμμετρικό ενός στοιχείου, αν υπάρχει είναι μοναδικό.

Όταν η πράξη μιας ομάδος συμβολίζεται ως πρόσθεση, τότε το συμμετρικό στοιχείο καλείται *αντίθετο* και το ουδέτερο στοιχείο *μηδενικό*. Όταν η πράξη μιας ομάδος συμβολίζεται ως πολλαπλασιασμός, τότε το συμμετρικό στοιχείο καλείται *αντίστροφο* και το ουδέτερο στοιχείο *μοναδιαίο*.

Ορισμός 1.9. Ας είναι A ένα μη κενό σύνολο και $+, \cdot$ δύο πράξεις επί του A. Η τριάδα $(A, +, \cdot)$ καλείται δακτύλιος, αν ισχύουν οι παρακάτω ιδιότητες :

α) Το ζεύγος $(A, +)$ είναι αντιμεταθετική ομάδα.

β) Το ζεύγος $(A \setminus \{0\}, \cdot)$ είναι μονοειδές.

γ) Για κάθε $x, y, z \in A$ ισχύει $x \cdot (y + z) = x \cdot y + x \cdot z$ και $(y + z) \cdot x = y \cdot x + z \cdot x$.

Αν η πράξη " $\cdot$ " είναι αντιμεταθετική, τότε ο δακτύλιος $(A, +, \cdot)$ καλείται *αντιμεταθετικός*. Αν το ζεύγος $(A \setminus \{0\}, \cdot)$ είναι αντιμεταθετική ομάδα, τότε ο δακτύλιος καλείται *σώμα*.

Αρχικά θα δούμε μερικές ασκήσεις που αφορούν τις ιδιότητες των πράξεων. Για να αποδείξουμε ότι μία πράξη $*$ είναι προσεταιριστική ή αντιμεταθετική σε ένα σύνολο A το αποδεικνύουμε σύμφωνα με τον ορισμό ενώ για να αποδείξουμε ότι δεν είναι προσεταιριστική ή αντιμεταθετική παραθέτουμε ένα αντιπαράδειγμα. Για τον προσδιορισμό, αν υπάρχει, του ουδέτερου στοιχείου e επιλύουμε την εξίσωση $x * e = x$ για κάθε $x \in A$ ως προς e και αν η πράξη δεν είναι αντιμεταθετική, τότε αντικαθιστούμε τις λύσεις της προηγούμενης εξίσωσης στην $e * x = x$ για να δούμε αν υπάρχει κάποια που την ικανοποιεί. Παρόμοια για να προσδιορίσουμε τα στοιχεία που έχουν συμμετρικό επιλύουμε την $x * x' = e$ ως προς x' και αν η πράξη δεν είναι αντιμεταθετική, τότε βλέπουμε ποιες από αυτές τις λύσεις επαληθεύουν την $x' * x = e$ για να δούμε αν υπάρχει κάποια που την ικανοποιεί.

Ασκήσεις

Άσκηση 1.24. *Ας είναι A μη κενό σύνολο και $*$ μία πράξη στο A. Να εξεταστεί, αν η πράξη $*$ είναι προσεταιριστική, αντιμεταθετική, αν έχει ουδέτερο στοιχείο και να προσδιοριστούν τα στοιχεία που έχουν συμμετρικό στις παρακάτω περιπτώσεις:*

α) $A = \mathbb{Q}$ *και* $a * b = a - b$.

β) $A = \mathbb{Q}$ *και* $a * b = ab$.

γ) $A = \mathbb{Z}^+$ *και* $a * b = \max\{a, b\}$.

δ) $A = \mathbb{Z}^+$ *και* $a * b = \min\{a, b\}$.

ε) $A = \mathbb{Z} \times \mathbb{Z}$ *και* $(a, b) * (c, d) = (a + c, b + d)$.

στ) $A = \mathbb{R} \times \mathbb{R} \setminus \{(0, 0)\}$ *και* $(a, b) * (c, d) = (ac - bd, ad + bc)$.

Απόδειξη. α) Η πράξη $*$ δεν είναι προσεταιριστική. Πράγματι, έχουμε

$$(7 * 3) * 1 = (7 - 3) * 1 = 4 * 1 = 4 - 1 = 3$$

και

$$7 * (3 * 1) = 7 * (3 - 1) = 7 * 2 = 7 - 2 = 5.$$

Έτσι, έχουμε $(7 * 3) * 1 \neq 7 * (3 * 1)$ και επομένως η πράξη $*$ δεν είναι προσεταιριστική. Επίσης, παρατηρούμε ότι $3 * 1 = 3 - 1 = 2$ και $1 * 3 = 1 - 3 = -2$. Καθώς $3 * 1 \neq 1 * 3$, η

πράξη $*$ δεν είναι αντιμεταθετική. Αν e είναι ουδέτερο στοιχείο για την πράξη $*$, τότε για κάθε ρητό x έχουμε $x * e = x = e * x$. Τότε $x - e = x$ και $e - x = x$. Από την πρώτη ισότητα παίρνουμε $e = 0$ και από την δεύτερη $-x = x$, για κάθε ρητό x, το οποίο είναι άτοπο. Άρα, η πράξη $*$ δεν έχει ουδέτερο στοιχείο.

β) Ο συνήθης πολλαπλασιασμός στο σύνολο των ρητών είναι πράξη προσεταιριστική, αντιμεταθετική, έχει ως ουδέτερο στοιχείο το 1 και κάθε μη μηδενικός ρητός x έχει συμμετρικό στοιχείο τον αριθμό $1/x$.

γ) Ας είναι $m, n, k \in A$. Τότε, έχουμε:

$$m * (n * k) = m * (\max\{n, k\}) = \max\{m, \max\{n, k\}\} = \max\{m, n, k\}$$

και

$$(m * n) * k = (\max\{m, n\}) * k = \max\{\max\{m, n\}, k\} = \max\{m, n, k\}.$$

Άρα, ισχύει $m * (n * k) = (m * n) * k$ και επομένως ισχύει η προσεταιριστική ιδιότητα. Επίσης, ισχύει:

$$m * n = \max\{m, n\} = n * m$$

και επομένως η πράξη $*$ είναι αντιμεταθετική. Ένας θετικός ακέραιος e είναι ουδέτερο στοιχείο για την πράξη $*$ αν και μόνον αν για κάθε $m \in A$ ισχύει:

$$m * e = m = e * m$$

ή

$$\max\{m, e\} = m,$$

το οποίο ισοδυναμεί με $e \leq m$. Άρα, ο ακέραιος 1 είναι το ουδέτερο στοιχείο για την πράξη $*$. Ένα στοιχείο $m \in A$ έχει συμμετρικό $m' \in A$ αν και μόνον αν ισχύει:

$$m * m' = 1 \Longleftrightarrow \max\{m, m'\} = 1.$$

Έτσι, έχουμε $m = m' = 1$. Άρα, το μοναδικό στοιχείο του A το οποίο έχει συμμετρικό είναι το 1.

δ) Ας είναι $m, n, k \in A$. Τότε, έχουμε:

$$m * (n * k) = m * (\min\{n, k\}) = \min\{m, \min\{n, k\}\} = \min\{m, n, k\}$$

και

$$(m * n) * k = (\min\{m, n\}) * k = \min\{\max\{m, n\}, k\} = \min\{m, n, k\}.$$

Άρα, ισχύει $m * (n * k) = (m * n) * k$ και επομένως ισχύει η προσεταιριστική ιδιότητα. Επιπλέον, έχουμε:

$$m * n = \max\{m, n\} = n * m$$

και επομένως η πράξη $*$ είναι αντιμεταθετική. Αν e είναι ουδέτερο στοιχείο για την πράξη $*$, τότε έχουμε:

$$m * e = m = e * m,$$

ή

$$\min\{m, e\} = m.$$

Για $m = e + 1$, προκύπτει ότι $\min\{e + 1, e\} = e + 1$ το οποίο είναι άτοπο. Άρα, η πράξη $*$ δεν έχει ουδέτερο στοιχείο.

ε) Ας είναι $(a,b),(c,d),(e,f) \in A$. Τότε, έχουμε:

$$((a,b)*(c,d))*(e,f) = (a+c,b+d)*(e,f) = ((a+c)+e,(b+d)+f) = \\ (a+(c+e),b+(d+f)) = (a,b)*(c+d,e+f) = (a,b)*((c,d)*(e,f)).$$

΄Αρα, ισχύει η προσεταιριστική ιδιότητα για την πράξη $*$. Επίσης, ισχύει:

$$(a,b)*(c,d) = (a+c,b+d) = (c+a,d+b) = (c,d)*(a,b).$$

Επομένως, η πράξη $*$ είναι αντιμεταθετική. Το ζεύγος $(0,0)$ είναι το ουδέτερο στοιχείο, καθώς για κάθε $(a,b) \in A$ έχουμε:

$$(a,b)*(0,0) = (a+0,b+0) = (a,b).$$

Τέλος, κάθε στοιχείο (a,b) έχει ως συμμετρικό το ζεύγος $(-a,-b)$. Πράγματι, έχουμε:

$$(a,b)*(-a,-b) = (a+(-a),b+(-b)) = (0,0).$$

στ) Ας είναι $(a,b),(c,d),(e,f) \in A$. Τότε, έχουμε:

$$\begin{aligned} ((a,b)*(c,d))*(e,f) &= (ac-bd,ad+bc)*(e,f) \\ &= ((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e) \\ &= (ace-bde-adf-bcf,acf-bdf+ade+bce) \end{aligned}$$

και

$$\begin{aligned} (a,b)*((c,d)*(e,f)) &= (a,b)*(ce-df,cf+de) \\ &= (a(ce-df)-b(cf+de),a(cf+de)+b(ce-df)) \\ &= (ace-bde-adf-bcf,acf-bdf+ade+bce). \end{aligned}$$

Οπότε, έχουμε

$$((a,b)*(c,d))*(e,f) = (a,b)*((c,d)*(e,f))$$

και επομένως η πράξη $*$ είναι προσεταιριστική. Επίσης, έχουμε:

$$(a,b)*(c,d) = (ac-bd,ad+bc) = (ca-bd,da+cb) = (c,d)*(a,b).$$

΄Αρα, η πράξη $*$ είναι αντιμεταθετική. Το ζεύγος $(1,0)$ είναι ουδέτερο στοιχείο, καθώς για κάθε $(a,b) \in A$ ισχύει:

$$(a,b)*(1,0) = (a\cdot 1-b\cdot 0,a*0+b*1) = (a,b).$$

Στη συνέχεια θα δείξουμε ότι κάθε $(a,b) \in A$ έχει συμμετρικό. Πράγματι, το ζεύγος $(c,d) \in A$ είναι συμμετρικό του (a,b), αν και μόνον αν, έχουμε $(a,b)*(c,d) = (1,0)$ που ισοδυναμεί με $(ac-bd,ad+bc) = (1,0)$. Δηλαδή, το (c,d) είναι συμμετρικό του (a,b), αν και μόνον αν, έχουμε:

$$ac-bd = 1 \quad \text{και} \quad ad+bc = 0.$$

Ας είναι $b \neq 0$. Τότε, πολλαπλασιάζοντας την πρώτη από τις προηγούμενες ισότητες με b, παίρνουμε $abc - b^2d = b$. Από την δεύτερη ισότητα έχουμε $bc = -ad$ και έτσι παίρνουμε $-a^2d - b^2d = b$, απ΄ όπου προκύπτει:

$$d = -\frac{b}{a^2 + b^2}.$$

Αντικαθιστώντας την τιμή στη πρώτη ισότητα, παίρνουμε:

$$c = \frac{a}{a^2 + b^2}.$$

Αντιστρόφως, υπολογίζουμε:

$$(a, b)\left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right) = (1, 0).$$

΄Αρα, το συμμετρικό του (a, b) είναι το ζεύγος

$$\left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right).$$

Αν $b = 0$, τότε $a \neq 0$ και εύκολα βλέπουμε ότι το συμμετρικό του $(a, 0)$ είναι το ζεύγος $(1/a, 0)$. □

΄Ασκηση 1.25. *Ας είναι E ένα μη κενό σύνολο και $\mathcal{P}(E)$ το δυναμοσύνολό του. Ας είναι A και B υποσύνολα του E. Η διαφορά του B από το A είναι το σύνολο*

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Θεωρούμε την πράξη $*$ στο $\mathcal{R}(E)$ η οποία ορίζεται ως εξής:

$$A * B = A \setminus B, \quad \forall (A, B) \in \mathcal{R}(E)^2.$$

Να εξεταστεί αν η πράξη $*$ είναι προσεταιριστική ή αντιμεταθετική.

Απόδειξη. Η πράξη $*$ δεν είναι προσεταιριστική. Για να το δείξουμε θεωρούμε το σύνολο $E = \{1, 2, 3, 4\}$ και τα υποσύνολά του $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ και $C = \{1, 2\}$. ΄Εχουμε:

$$A * (B * C) = A \setminus (B \setminus C) = A \setminus \{3, 4\} = \{1, 2\}$$

και

$$A * (B * C) = (A \setminus B) \setminus C = \{1\} \setminus C = \emptyset.$$

Οπότε, ισχύει $A*(B*C) \neq A*(B*C)$ και επομένως η πράξη $*$ δεν είναι προσεταιριστική.

Η πράξη $*$ δεν είναι αντιμεταθετική. Πράγματι, ας θεωρήσουμε το σύνολο $E = \{1, 2, 3\}$ και τα υποσύνολά του $A = \{1, 2\}$ και $B = \{1, 3\}$. ΄Εχουμε:

$$A * B = A \setminus B = \{2\} \quad \text{και} \quad B * A = B \setminus A = \{3\}.$$

΄Αρα $A * B \neq B * A$ και επομένως η πράξη δεν είναι αντιμεταθετική. □

΄Ασκηση 1.26. *Να δειχθεί ότι η πράξη $a * b = a + b - ab$ στο $\mathbb{R}$ είναι προσεταιριστική, αντιμεταθετική και έχει ουδέτερο στοιχείο.*

Απόδειξη. Θα δείξουμε πρώτα ότι η πράξη ast είναι προσεταιριστική. Ας είναι $a, b, c \in \mathbb{R}$. Τότε, έχουμε:

$$a * (b * c) = a * (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - bc - ab - ac + abc$$

και

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc.$$

΄Αρα, ισχύει $a * (b * c) = (a * b) * c$ και επομένως η πράξη είναι προσεταιριστική.

Στη συνέχεια θα δείξουμε ότι η πράξη $*$ είναι αντιμεταθετική. Πράγματι, για $a, b \in \mathbb{R}$ έχουμε:

$$a * b = a + b - ab = b + a - ab = b * a.$$

Συνεπώς, η πράξη είναι αντιμεταθετική.

Ένα στοιχείο $e \in \mathbb{R}$ είναι ουδέτερο για την πράξη ast αν και μόνον αν για κάθε $a \in \mathbb{R}$ ισχύει:

$$a * e = a = e * a,$$

ή

$$a + e - ae = a = e + a - ae$$

το οποίο είναι ισοδύναμο με την ισότητα $ae = e$ ή $e(a - 1) = 0$. Παίρνοντας $a = 2$, προκύπτει $e = 0$. Αντιστρόφως, έχουμε $0(a - 1) = 0$, για κάθε $a \in \mathbb{R}$. Επομένως, το 0 είναι το ουδέτερο στοιχείο της πράξης $*$. □

Στη συνέχεια θα δούμε μερικές ασκήσεις που αφορούν τις βασικές αλγεβρικές δομές.

΄Ασκηση 1.27. *Να δειχθεί ότι το σύνολο*

$$G = \{2^m \mid m \in \mathbb{Z}\}$$

με πράξη τον συνήθη πολλαπλασιασμό αποτελεί ομάδα.

Απόδειξη. Ας είναι $x, y \in G$. Τότε $x = 2^m$ και $y = 2^n$, όπου $m, n \in \mathbb{Z}$. ΄Εχουμε $xy = 2^{m+n}$ και $m + n \in \mathbb{Z}$. ΄Αρα $xy \in G$. Ο πολαπλασιασμός των ρητών είναι προσεταιριστική πράξη. Το ουδέτερο στοιχείο είναι ο αριθμός $1 = 2^0$ ο οποίος ανήκει στο G. Επίσης, το συμμετρικό ένος στοιχείου $x = 2^m$ είναι το $x^{-1} = 2^{-m}$ το οποίο ανήκει επίσης στο G. ΄Αρα, το ζεύγος $(G, \cdot)$ αποτελεί ομάδα. □

΄Ασκηση 1.28. *Ας είναι $G = \mathbb{Q} \setminus \{-1/2\}$. Ορίζουμε μια πράξη επί του G ως εξής:*

$$x * y = x + 2xy + y, \ \forall x, y \in G.$$

Να δειχθεί ότι το ζεύγος $(G, *)$ είναι αβελιανή ομάδα.

Απόδειξη. Πρώτα παρατηρούμε ότι αν $x, y \in \mathbb{Q}$ με $x * y = -1/2$, τότε

$$y + 2xy + x = -\frac{1}{2} \iff 2x(y + \frac{1}{2}) + y + \frac{1}{2} = 0 \iff (y + \frac{1}{2})(2x + 1) = 0.$$

Έτσι, έχουμε $x = -1/2$ ή $y = -1/2$. Άρα, αν $x, y \in G$, τότε $x * y \in G$.

Η πράξη είναι προσεταιριστική. Πράγματι, για κάθε $x, y, z \in G$ έχουμε

$$\begin{aligned}(x * y) * z &= (x + 2xy + y) * z \\ &= x + 2xy + y + 2(x + 2xy + y)z + z \\ &= x + y + z + 2xz + 2yz + 2xy + 4xyz\end{aligned}$$

και

$$\begin{aligned}x * (y * z) &= x * (y + 2yz + z) \\ &= x + 2x(y + 2yz + z) + (y + 2yz + z) \\ &= x + y + z + 2xz + 2yz + 2xy + 4xyz,\end{aligned}$$

απ'οπου παίρνουμε

$$(x * y) * z = x * (y * z).$$

Επίσης, για κάθε $x, y \in G$, έχουμε:

$$x * y = x + 2xy + y = y + 2xy + x = y * x.$$

Επομένως, η πράξη $*$ είναι αντιμεταθετική.

Τέλος, για κάθε $x \in G$, έχουμε:

$$x * e = x = e * x \iff x + 2xe + e = x = e + 2ex + x \iff e(1 + 2x) = 0.$$

Η τελευταία ισότητα ισοδυναμεί με $e = 0$ και επομένως το 0 είναι το ουδέτερο στοιχείο για την πράξη.

Ας είναι $x \in G$. Ας υποθέσουμε ότι υπάρχει $f \in A$ τέτοιο, ώστε να ισχύει $x * f = 0$ ή $x + 2xf + f = 0$, απ΄ όπου ισοδύναμα παίρνουμε:

$$f = -\frac{x}{2x + 1}.$$

Οπότε, το $-x/(2x + 1)$ είναι το συμμετρικό στοιχείο του x. Συνεπώς, το ζεύγος $(G, *)$ είναι ομάδα. □

Άσκηση 1.29. *Ας είναι X ένα μη κενό σύνολο. Συμβολίζουμε με $S(X)$ το σύνολο των αμφιέσεων του X στο X. Να δείχθεί ότι το σύνολο $S(X)$ με πράξη την σύνθεση απεικονίσεων αποτελεί ομάδα.*

Απόδειξη. Ας είναι $f, g \in S(X)$. Θα δείξουμε ότι η σύνθεση $g \circ f$ είναι αμφίεση. Πράγματι, αν $x, y \in X$ με $(g \circ f)(x) = (g \circ f)(y)$, τότε $g(f(x)) = g(f(y)$ και, καθώς η g είναι ένεση, έχουμε $f(x) = f(y)$. Η f είναι επίσης ένεση και κατά συνέπεια παίρνουμε $x = y$. Άρα, η $g \circ f$ είναι ένεση. Αν $z \in X$, τότε υπάρχει $y \in X$ με $z = g(y)$ γιατί η g είναι έφεση. Επίσης, καθώς η f είναι έφεση, υπάρχει $x \in X$ με $y = f(x)$. Άρα, έχουμε

$z = g(f(x)) = (g \circ f)(x)$ και επομένως η $g \circ f$ είναι έφεση. Συνεπώς, η $g \circ f$ είναι αμφίεση.

Ας είναι $f, g, h \in S(X)$. Αν $z \in X$, τότε έχουμε:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x).$$

΄Ετσι, ισχύει $(f \circ g) \circ h = f \circ (g \circ h)$ και επομένως η σύνθεση απεικονίσεων είναι πράξη προσεταιριστική.

Συμβολίζουμε με I_X την ταυτοτική απεικόνιση του X, δηλαδή για κάθε $x \in X$ ισχύει $I_X(x) = x$. ΄Ετσι, για κάθε $f \in S(X)$ και $x \in X$, έχουμε:

$$(f \circ I_X)(x) = f(I_X(x)) = f(x) = I_X(f(x)) = (I_X \circ f)(x).$$

΄Αρα, ισχύει $f \circ I_X = f = I_X \circ f$. Συνεπώς, η απεικόνιση I_X είναι το ουδέτερο στοιχείο για την σύνθεση απεικονίσεων.

Τέλος, για κάθε αμφίεση f, η αντίστροφη απεικόνισή της f^{-1} είναι επίσης αμφίεση. Πράγματι, αν $x, y \in X$ με $f^{-1}(x) = f^{-1}(y)$, τότε $f(f^{-1}(x)) = f(f^{-1}(y))$, απ΄ όπου $(f \circ f^{-1})(x) = (f \circ f^{-1})(y)$ και επομένως $I_X(x) = I_X(y)$, δηλαδή $x = y$. ΄Αρα, η f^{-1} είναι ένεση. Επίσης, αν $z \in X$, τότε

$$z = I_X(z) = (f^{-1} \circ f)(z) = f^{-1}(f(z)).$$

΄Αρα, η f^{-1} είναι έφεση. Επομένως, η f^{-1} είναι αμφίεση και κατά συνέπεια κάθε στοιχείο του $S(X)$ έχει συμμετρικό στοιχείο. ΄Αρα, το ζεύγος $(S(X), \circ)$ είναι ομάδα. □

΄Ασκηση 1.30. *Σε κάθε δακτύλιο A ισχύει:*

$$(-x)y = x(-y) = -xy, \quad \forall x, y \in A.$$

Απόδειξη. ΄Εχουμε:

$$\begin{aligned} (-x)y = x(-y) &\iff (-x)y + xy = x(-y) + xy \\ &\iff (-x + x)y = x(-y + y) \\ &\iff 0y = x0 \end{aligned}$$

το οποίο ισχύει. Ομοίως έχουμε:

$$(-x)y = -xy \iff (-x)y + xy = -xy + xy \iff (-x + x)y = 0 \iff 0y = 0,$$

το οποίο ισχύει. □

΄Ασκηση 1.31. *Ας είναι K ένα σώμα και 0_K, 1_K τα ουδέτερα στοιχεία για την πρόσθεση και τον πολλαπλασιασμό του K, με $0_K \neq 1_K K$. Αν ισχύει*

$$-x = x^{-1}, \quad \forall x \in K \setminus \{0_K\},$$

τότε δειχθεί ότι $K = \{0_K, 1_K\}$.

Απόδειξη. Έχουμε $-1_K = 1_K^{-1} = 1_K$ και επομένως $1_K + 1_K = 0_K$. Ας υποθέσουμε ότι υπάρχει $x \in K \setminus \{0_K, 1_K\}$. Καθώς $x \neq 1_K = -1_K$, έχουμε $x + 1_K \neq 0_K$ και επομένως ισχύει $-(x + 1_K) = (x + 1_K)^{-1}$, απ΄ όπου παίρνουμε $(x + 1_K)^2 + 1_K = 0_K$. Έτσι, προκύπτει:

$$x^2 + x + x + 1_K + 1_K = 0_K.$$

Καθώς έχουμε $1_K + 1_K = 0_K$ και

$$x + x = 1_K x + 1_K x = (1_K + 1_K)x = 0_K x = 0_K,$$

παίρνουμε $x^2 = 0_K$. Επειδή $x \neq 0_K$, πολλαπλασιάζουμε την προηγουμένη ισότητα με x^{-1} και παίρνουμε $x = 0_K$ που είναι άτοπο. Άρα, ισχύει $K = \{0_K, 1_K\}$. □

΄Ασκηση 1.32. *Να δειχθεί ότι το σύνολο*

$$A = \left\{ \frac{a}{2^n} \in \mathbb{Q} \mid a \in \mathbb{Z},\ n \in \mathbb{Z} \right\}$$

εφοσιασμένο με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού αποτελεί αντιμεταθετικό δακτύλιο. Να βρεθούν τα αντιστρέψιμα στοιχεία του.

Απόδειξη. Ας είναι $x, y \in A$. Τότε $x = a/2^m$, $y = b/2^m$, όπου $a, b \in \mathbb{Z}$ και $m, n \in \mathbb{Z}$. Πρώτα θα δείξουμε ότι $x + y \in A$. Διακρίνουμε τις εξής περιπτώσεις:

α) $m, n \in \mathbb{N}$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $m \geq n$. Τότε, έχουμε:

$$x + y = \frac{a}{2^m} + \frac{b}{2^n} = \frac{a + b2^{m-n}}{2^m}.$$

Καθώς $a + b2^{m-n} \in \mathbb{Z}$, έπεται ότι $x + y \in A$.

β) $m = -k$, $n = -l$, όπου $k, l \in \mathbb{N}$. Τότε, έχουμε:

$$x + y = \frac{a}{2^m} + \frac{b}{2^n} = a2^k + b2^l.$$

Καθώς $a2^k + b2^l \in \mathbb{Z}$, παίρνουμε $x + y \in A$.

γ) $m \in \mathbb{N}$, $n = -l$, όπου $l \in \mathbb{N}$. Τότε, ισχύει:

$$x + y = \frac{a}{2^m} + \frac{b}{2^n} = \frac{a}{2^m} + b2^l = \frac{a + b2^{m+l}}{2^m}.$$

Έχουμε $a + b2^{m+l} \in \mathbb{Z}$ και κατά συνέπεια $x + y \in A$.

Επίσης, έχουμε $xy \in A$. Πράγματι, ισχύει:

$$xy = \frac{a}{2^m}\ \frac{b}{2^n} = \frac{ab}{2^{m+n}}.$$

Έτσι, είναι προφανές ότι $xy \in A$.

Παρατηρούμε ότι οι αριθμοί 0 και 1 ανήκουν στο A. Έπίσης, για κάθε στοιχείο $x = a/2^m$ του A, το αντίθετό του $-x = (-a)/2^m$ είναι επίσης στοιχείο του A. Οι συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{Q}$ είναι προσεταιριστικές, αντιμεταθετικές, προσεταιριστικές. Οι αριθμοί 0 και 1 είναι τα ουδέτερα στοιχεία για

την πρόσθεση και πολλαπλασιασμό, αντίστοιχα. Επίσης, ισχύει ο επιμεριστικός του πολλαπλασιασμού ως προς την πρόσθεση. Επομένως, η τριάδα $(A, +, \cdot)$ αποτελεί αντιμεταθετικό δακτύλιο.

Ένα στοιχείο $x = a/2^m$ του A είναι αντιστρέψιμο αν και μόνον αν το στοιχείο $x^{-1} = 2^m/a$ ανήκει επίσης στο A, δηλαδή, αν και μόνον αν $a = \pm 2^n$. Άρα, ένα στοιχείο $x \in A$ είναι αντιστρέψιμο αν και μόνον αν $x = \pm 2^k$, όπου $k \in \mathbb{Z}$. □

Άσκηση 1.33. *Να δειχθεί ότι το σύνολο*

$$\mathbb{Z}[\sqrt{3}] = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\right\}$$

εφοδιασμένο με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού αποτελεί δακτύλιο.

Απόδειξη. Ας είναι $x, y \in \mathbb{Z}[\sqrt{3}]$. Τότε $x = a + b\sqrt{3}$ και $y = c + d\sqrt{3}$, όπου $a, b, c, d \in \mathbb{Z}$. Έχουμε:

$$x + y = (a + b) + (c + d)\sqrt{3} \quad \text{και} \quad xy = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Οι αριθμοί $a + b$, $c + d$, $ac + 3bd$, $ad + bc$ και επομένως $x + y, xy \in \mathbb{Z}[\sqrt{3}]$.

Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι προσεταιριστικές και αντιμεταθετικές μέσα στο $\mathbb{R}$. Επιπλέον, για κάθε $x, y, z \in \mathbb{R}$ ισχύει:

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{και} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Καθώς $\mathbb{Z}[\sqrt{3}] \subseteq \mathbb{R}$, οι ιδιότητες αυτές ισχύουν και για τα στοιχεία του $\mathbb{Z}[\sqrt{3}]$.

Το ουδέτερο στοιχείο για την πρόσθεση είναι το $0 = 0 + 0\sqrt{3}$ το οποίο ανήκει στο $\mathbb{Z}[\sqrt{3}]$. Επίσης, αν $x \in \mathbb{Z}[\sqrt{3}]$, τότε $x = a + b\sqrt{3}$ και επομένως $-x = (-a) + (-b)\sqrt{3}$. Καθώς $-a, -b \in \mathbb{Z}$, έχουμε $-x \in \mathbb{Z}[\sqrt{3}]$. Συνεπώς, το αντίθετο κάθε στοιχείου του $\mathbb{Z}[\sqrt{3}]$ ανήκει στο $\mathbb{Z}[\sqrt{3}]$. Επιπλέον, το ουδέτερο στοιχείο για τον πολλαπλασιασμό είναι το $1 = 1 + 0\sqrt{3}$ το οποίο ανήκει στο $\mathbb{Z}[\sqrt{3}]$. □

Άσκηση 1.34. *Ας είναι $(A, +, \cdot)$ ένας δακτύλιος. Στο σύνολο $\mathbb{Z} \times A$ ορίζουμε τις εξής πράξεις:*

$$(m, a) \oplus (n, b) = (m + n, a + b),$$
$$(m, a) \otimes (n, b) = (mn, na + mb + ab).$$

Να δειχθεί ότι η τριάδα $(\mathbb{Z} \times A, \oplus, \otimes)$ αποτελεί δακτύλιο.

Απόδειξη. Παρατηρούμε αμέσως ότι το αποτέλεσμα των παραπάνω πράξεων είναι στοιχείο του $\mathbb{Z} \times A$. Θα δείξουμε πρώτα ότι το ζεύγος $(\mathbb{Z} \times A, \oplus)$ αποτελεί αντμεταθετική ομάδα. Για κάθε $(r, a), (s, b), (t, c) \in \mathbb{Z} \times A$ έχουμε:

$$\begin{aligned}((r, a) \oplus (s, b)) \oplus (t, c) &= (r + s, a + b) \oplus (t, c) \\ &= (r + s + t, a + b + c) \\ &= (r, a) \oplus (s + t, b + c) \\ &= (r, a) \oplus ((s, b) \oplus (t, c)).\end{aligned}$$

΄Αρα, ισχύει η προσεταιριστική ιδιότητα. Συμβολίζουμε με 0_A το ουδέτερο στοιχείο της ομάδας $(A, +)$. Το ζεύγος $(0, 0_A)$ είναι το ουδέτερο στοιχείο της πράξης $\oplus$. Πράγματι, για κάθε $(r, a) \in \mathbb{Z} \times A$ έχουμε

$$(r, a) \oplus (0, 0_A) = (r + 0, a + 0_A) = (r, a)$$

και

$$(0, 0_A) \oplus (r, a) = (0 + r, 0_A + a) = (r, a).$$

΄Αρα, πράγματι το $(0, 0_A)$ είναι το ουδέτερο στοιχείο της πράξης $\oplus$. Ας είναι $(r, a) \in \mathbb{Z} \times A$. Θεωρούμε το στοιχείο $(-r, -a)$. ΄Εχουμε:

$$(r, a) \oplus (-r, -a) = (r + (-r), a + (-a)) = (0, 0_A)$$

και

$$(-r, -a) \oplus (r, a) = ((-r) + r, (-a) + a) = (0, 0_A).$$

Επομένως, το $(-r, -a)$ είναι το αντίθετο στοιχείο του (r, a). Τέλος, για κάθε $(r, a), (s, b) \in \mathbb{Z} \times A$ ισχύει:

$$(r, a) \oplus (s, b) = (r + s, a + b) = (s + r, b + a) = (s, b) \oplus (r, a).$$

Συνεπώς, το ζεύγος $(\mathbb{Z} \times A, \oplus)$ είναι μία αντιμεταθετική ομάδα.

Στην συνέχεια θα δείξουμε ότι το ζεύγος $(\mathbb{Z} \times A, \otimes)$ είναι ένα μονοειδές. Για κάθε $(r, a), (s, b), (t, c) \in \mathbb{Z} \times A$ έχουμε:

$$\begin{aligned}
((r, a) \otimes (s, b)) \otimes (t, c) &= (rs, ab) \otimes (t, c) \\
&= ((rs)t, (ab)c) \\
&= (r(st), a(bc)) \\
&= (r, a) \otimes (st, bc) \\
&= (r, a) \otimes ((s, b) \otimes (t, c)).
\end{aligned}$$

΄Αρα, ισχύει η προσεταιριστική ιδιότητα. Ας είναι 1_A το ουδέτερο στοιχείο για τον πολλαπλασιασμό του A. ΄Εχουμε:

$$(r, a) \otimes (1, 1_A) = (r \cdot 1, a \cdot 1_A) = (r, a)$$

και

$$(1, 1_A) \otimes (r, a) = (1 \cdot r, 1_A \cdot a) = (r, a).$$

΄Ετσι, βλέπουμε ότι το ζεύγος $(1, 1_A)$ είναι το ουδέτερο στοιχείο για την πράξη $\otimes$. Συνεπώς, το ζεύγος $(\mathbb{Z} \times A, \otimes)$ είναι ένα μονοειδές.

Τέλος, αν $(r, a), (s, b), (t, c) \in \mathbb{Z} \times A$, τότε έχουμε:

$$\begin{aligned}
(t, c) \otimes ((r, a) \oplus (s, b)) &= (t, c) \otimes (r + s, a + b) \\
&= (t(r + s), c(a + b)) \\
&= (tr + ca, ca + cb) \\
&= (tr, ca) \oplus (ca, cb) \\
&= ((t, c) \otimes (r, a)) \oplus ((t, c) \otimes (s, b)).
\end{aligned}$$

Επομένως, η τριάδα $(\mathbb{Z} \times A, \oplus, \otimes)$ αποτελεί δακτύλιο. □

1.5 Συνδυαστικές Ασκήσεις

΄Ασκηση 1.35. *Να δειχθεί ότι, για κάθε $n \in \mathbb{N}$, ο αριθμός*

$$A = \left(3 + \sqrt{5}\right)^n + \left(3 - \sqrt{5}\right)^n$$

είναι άρτιος.

Απόδειξη. Θεωρούμε την πρόταση:

$$P(n) = \left(3 + \sqrt{5}\right)^n + \left(3 - \sqrt{5}\right)^n.$$

Για $n = 0$ και $n = 1$ προφανώς ισχύει. Ας υποθέσουμε ότι ισχύει για κάθε $n < k$. Θα δείξουμε ότι ισχύει για $n = k$. Θέτουμε $a = 3 + \sqrt{5}$ και $b = 3 - \sqrt{5}$. Οι αριθμοί a και b είναι ρίζες της εξίσωσης $x^2 - 6b + 4 = 0$ και επομένως ισχύει $a^2 = 6a - 4$ και $b^2 = 6b - 4$. ΄Εχουμε:

$$\begin{aligned} P(k) &= a^k + b^k = a^{k-2}(6a - 4) + b^{k-2}(6b - 4) \\ &= 6(a^{k-1} + b^{k-1}) - 4(a^{k-2} + b^{k-2}) = 6P(k-1) - 4P(k-2). \end{aligned}$$

Από την υπόθεση έχουμε ότι $P(k-1)$ και $4P(k-2)$ είναι άρτιοι, άρα και $P(k)$ άρτιος.

Εδώ αξίζει να σημειώσουμε ότι στο πρώτο βήμα της επαγωγικής διαδικασίας δεν αρκεστήκαμε στην απόδειξη της πρότασης για $n = 0$ αλλά αναφέρουμε ότι ισχύει και για $n = 1$. Αυτό έγινε διότι η σχέση $P(k) = 6P(k-1) - 4P(k-2)$ δεν έχει νόημα για $k = 1$ και επιπλέον θα χρειαζόταν περαιτέρω δικαιολόγηση γιατί ισχύει η πρόταση $P(2)$. □

΄Ασκηση 1.36. (*International Mathematical Olympiad 1972*) *Να δειχθεί ότι, για κάθε $n, m \in \mathbb{N}$, ο αριθμός $(2m)!(2n)!$ είναι πολλαπλάσιος του $m!n!(m+n)!$.*

Απόδειξη. Θεωρούμε την πρόταση:

$$P(m,n) = \frac{(2m)!(2n)!}{m!n!(m+n)!} \in \mathbb{Z}.$$

Θα χρησιμοποιήσουμε την «Δισδιάστατη Μαθηματική Επαγωγή - Β». Προφανώς, ισχύει $P(0,0) = 1$, και επομένως για $m = n = 0$ αληθεύει. Ας υποθέσουμε ότι ισχύει για κάθε $m = k-1$, $n = 0$. Θα δείξουμε ότι ισχύει και για $m = k$, $n = 0$. Πράγματι, έχουμε:

$$P(k,0) = \frac{(2k)!}{2k!} = \frac{2k(2k-1)(2k-2)!}{2k(k-1)!} = (2k-1)P(k-1,0).$$

Από την υπόθεση της επαγωγής συνεπάγεται ότι ο αριθμός αυτός είναι ακέραιος. Ας υποθέσουμε τώρα ότι η πρόταση ισχύει για κάθε φυσικό m και $n = k-1$. Θα

δείξουμε ότι ισχύει για κάθε φυσικό m και $n = k$. Έχουμε:

$$\begin{aligned}4P(m,n-1) - P(m+1,n-1) &= \\ &= 4\frac{(2m)!(2n-2)!}{m!(n-1)!(m+n-1)!} - \frac{(2m+2)!(2n-2)!}{(m+1)!(n-1)!(m+n)!} \\ &= \frac{4(2m)!(2n-2)!n(m+n)}{m!n!(m+n)!} - \frac{2(2m+1)(2m)!(2n-2)!n}{m!n!(m+n)!} \\ &= \frac{(2m)!(2n-2)!(4n(m+n)-2(2m+1)n}{m!n!(m+n)!} = \frac{(2m)!(2n)!}{m!n!(m+n)!} = P(m,n).\end{aligned}$$

Από την υπόθεση της επαγωγής, έχουμε ότι οι αριθμοί $P(m,k-1)$, $P(m+1,k-1)$ είναι ακέραιοι, απ΄ όπου έπεται ότι ο αριθμός $P(m,k)$ είναι επίσης ακέραιος. □

΄Ασκηση 1.37. (*International Mathematical Olympiad 1982*) *Ας είναι* $f : \mathbb{Z}^+ \to \mathbb{N}$ *απεικόνιση τέτοια, ώστε για κάθε* $m, n \in \mathbb{Z}^+$ *να ισχύει*

$$f(m+n) - f(m) - f(n) \in \{0,1\}$$

και επιπλέον $f(2) = 0$, $f(3) > 0$, $f(9999) = 3333$. *Να υπολογιστεί η τιμή* $f(1982)$.

Απόδειξη. Πρώτα θα δείξουμε ότι $f(3) = 1$. Πράγματι, για $m = n = 1$ έχουμε ότι

$$f(2) - f(1) - f(1) = k \Longrightarrow -2f(1) = k,$$

όπου $k \in \{0,1\}$. Καθώς $f(1) \in \mathbb{N}$, παίρνουμε $f(1) = 0$. Επιπλέον, για $m = 2$ και $n = 1$ έχουμε ότι

$$f(3) - f(2) - f(1) = k \Longrightarrow f(3) = k,$$

όπου $k \in \{0,1\}$. ΄Ετσι, η ανισότητα $f(3) > 0$ δίνει $f(3) = 1$.

Στην συνέχεια θα αποδείξουμε επαγωγικά ότι $f(3s) \geq s$, για κάθε $s \geq 1$. Για $s = 1$ είδαμε ότι ισχύει. Ας υποθέσουμε ότι ισχύει για $s = n$, δηλαδή ότι $f(3n) \geq n$. Θα δείξουμε ότι ισχύει για $s = n+1$. Πράγματι, έχουμε:

$$f(3n+3) = f(3) + f(3n) + k = f(3n) + k + 1 \geq n + k + 1 \geq n + 1.$$

΄Αρα, ισχύει $f(3s) \geq s$, για κάθε $s \geq 1$.

Αν ισχύει $f(3s_0) > s_0$ για κάποιο $s_0 < 3333$, τότε για κάθε $t > s_0$ έχουμε:

$$f(3t) = f(3(t-s_0) + 3s_0) = f(3(t-s_0)) + f(3s_0) + k > t - s_0 + s_0 + k \geq t$$

όπου $k \in \{0,1\}$. ΄Ετσι, για $t = 3333$ έχουμε $f(9999) > 3333$ το οποίο δεν ισχύει. Επομένως, έχουμε $f(3s) = s$, για κάθε $s \leq 3333$.

Τέλος, θα δείξουμε ότι $f(3s+1) = f(3s+2) = s$, για κάθε $s \leq 1110$. Πράγματι, έχουμε:

$$f(3s+1) = f(3s) + f(1) + k \Longrightarrow f(3s+1) = s + k.$$

Επιπλέον, κάνοντας χρήση των σχέσεων $f(3s) = s$ και $f(m+n) \geq f(m) + f(n)$ έχουμε:

$$3s + 1 = f(9s+3) \geq f(6s+2) + f(3s+1) \geq 3 \cdot f(3s+1).$$

΄Αρα, $f(3s+1) < s+1$ και καθώς $f(3s+1) = s+k$ συνεπάγεται ότι $f(3s+1) = s$. Ομοίως αποδεικύουμε και ότι $f(3s+2) = s$. ΄Ετσι, προκύπτει:

$$f(1982) = f(3 \cdot 660 + 2) = 660.$$

□

Βιβλιογραφία

[1] S. MacLane and G. Birkhoff (1971). Algèbre, Stuctures Fondamentales, Gauthier-Villars, Paris.

[2] Dasgupta A. (2013). Set Theory: With an Introduction to Real Point Sets. Springer Verlag.

[3] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

[4] Πουλάκης, Δ. (2014). ΄Άλγεβρα. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 2

Διαιρετότητα

Το κεφάλαιο αυτό περιέχει ασκήσεις που αφορούν τις βασικές ιδιότητες της διαίρεσης ακεραίων, του μέγιστου κοινού διαιρέτη, του ελάχιστου κοινού πολλαπλασίου και των πρώτων αριθμών. Επιπλέον, παρουσιάζεται ένα από τα σημαντικότερα εργαλεία της Θεωρίας Αριθμών που είναι ο Ευκλείδειος αλγόριθμος. Ο Ευκλείδειος αλγόριθμος παρουσιάστηκε αρχικά από τον Ευκλείδη στα «Στοιχεία» του για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο ακεραίων, αλλά βρίσκει και αλλού εφαρμογές όπως στην επίλυση γραμμικών ισοτιμιών, Διοφαντικών εξισώσεων, στα συνεχή κλάσματα κ.α.

2.1 Διαίρεση Ακεραίων

Ας είναι a και b ακέραιοι.

Ορισμός 2.1. Λέμε ότι ο a *διαιρεί* τον b και γράφουμε $a \mid b$ αν υπάρχει $c \in \mathbb{Z}$ έτσι, ώστε $b = ac$. Τότε, ο a καλείται *διαιρέτης* του b και ο b *πολλαπλάσιο* του a. Αν ο a δεν διαιρεί τον b, τότε γράφουμε $a \nmid b$.

Παρατηρούμε αμέσως ότι αν $0 \mid b$, τότε $b = 0$ και για κάθε $a \in \mathbb{Z}$ ισχύει $a \mid a$ και $a \mid 0$. Επίσης, για κάθε $a, b \in \mathbb{Z}$ ισχύουν τα εξης:

$$a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b.$$

Μερικές βασικές ιδιότητες δίνονται στην παρακάτω πρόταση:

Πρόταση 2.1. *Ας είναι $a, b, c \in \mathbb{Z}$. Τότε ισχύουν τα εξής:*
α) Αν $a \mid b$ και $b \mid c$, τότε $a \mid c$.
β) Αν $a \mid b$ και $c \mid d$, τότε $ac \mid bd$.
γ) Αν $a \mid b$ και $a \mid c$, τότε $a \mid bx + cy$, για κάθε $x, y \in \mathbb{Z}$.
δ) Αν $a \mid b$ και $b \neq 0$, τότε $|a| \leq |b|$.
ε) Αν $a \mid b$ και $b \mid a$, τότε $|a| = |b|$.

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 1.1], [7, Κεφάλαιο 2, Πρόταση 2.1] ή [5, Πρόταση 1.2.2, εδώ]. □

Ασκήσεις

Η άσκηση που ακολουθεί αποδεικνύει ότι το γινόμενο n διαδοχικών ακεραίων διαιρείται από το $n!$ και επομένως από το n. Είναι μία βασική ιδιότητα των ακεραίων που θα χρησιμοποιήσουμε αρκετές φορές στην συνέχεια.

΄Ασκηση 2.1. *Ας είναι a και b θετικοί ακέραιοι. Τότε, έχουμε:*
α) $a!b! \mid (a+b)!$.
β) $b! \mid (a+1)\cdots(a+b)$.
γ) *Το γινόμενο b διαδοχικών ακεραίων διαιρείται από το $b!$.*

Απόδειξη. α) Θα εφαρμόσουμε την μέθοδο της μαθηματικής επαγωγής επί του αθροίσματος $n = a+b$. Για $n = 2$, έχουμε $a = b = 1$ και επομένως η σχέση ισχύει. Ας υποθέσουμε τώρα ότι αληθεύει για $n = k$, θα δείξουμε ότι ισχύει για $n = k+1$. Ας είναι $a+b = k+1$. Καθώς $(a-1)+b = k$ και $a+(b-1) = k$, έχουμε:

$$(a-1)!b! \mid (a+b-1)! \quad \text{και} \quad a!(b-1)! \mid (a+b-1)!,$$

αντίστοιχα. Οπότε, ο ακέραιος $a!b!$ διαιρεί τους $(a+b-1)!a$ και $(a+b-1)!b$. Καθώς ισχύει:

$$(a+b)! = (a+b-1)!(a+b) = (a+b-1)!a + (a+b-1)!b,$$

παίρνουμε $a!b! \mid (a+b)!$ και επομένως η προς απόδειξη σχέση αληθεύει και για $n = k+1$, απ΄ όπου έχουμε το αποτέλεσμα.

β) Από την (α) έπεται αμέσως ότι $b! \mid (a+1)\cdots(a+b)$.

γ) Ας είναι A το γινόμενο b διαδοχικών θετικών ακεραίων. Αν το A είναι γινόμενο b διαδοχικών θετικών ακεραίων, τότε από το (β) έχουμε ότι $b! \mid A$. Αν το A είναι γινόμενο b διαδοχικών αρνητικών ακεραίων, τότε $A = (-1)^b|A|$. Έτσι, από το (β) έχουμε ότι $b! \mid |A|$, απ΄ όπου $b! \mid (-1)^b|A|$ και επομένως $b! \mid A$. Τέλος, στην περίπτωση που οι διαθοχικοί ακέραιοι δεν είναι όλοι θετικοί ή αρνητικοί, τότε ανάμεσα τους είναι το 0. ΄Αρα $A = 0$ και επομένως $b! \mid A$. □

΄Ασκηση 2.2. *Για κάθε θετικό ακέραιο n, ισχύουν τα εξής:*
α) $7 \mid 3^{2n+1} + 2^{n+2}$.
β) $16 \mid 3^{4n+1} - 2\cdot 3^{2n} - 1$.
γ) $169 \mid 3^{3n+3} - 26n - 27$.

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του n και στις τρεις περιπτώσεις.

α) Θέτουμε $A(n) = 3^{2n+1} + 2^{n+2}$. ΄Εχουμε $A(1) = 3^{2+1} + 2^{1+2} = 35$ και επομένως $7 \mid A(1)$. Υποθέτουμε ότι ισχύει $7 \mid A(k)$. Για $n = k+1$ έχουμε:

$$A(k+1) = 3^{2k+3} + 2^{k+3} = 9\cdot 3^{2k+1} + 2\cdot 2^{k+2} = 2A(k) + 7\cdot 3^{2k+1}.$$

Καθώς $7 \mid A(k)$, παίρνουμε $7 \mid A(k+1)$. Συνεπώς, η προς απόδειξη σχέση ισχύει.

β) Θέτουμε $B(n) = 3^{4n+1} - 2\cdot 3^{2n} - 1$. Είναι $B(1) = 3^5 - 2\cdot 3^2 - 1 = 224$ και επομένως $16 \mid B(1)$. Υποθέτουμε ότι ισχύει $16 \mid B(k)$. ΄Εχουμε:

$$\begin{aligned} B(k+1) &= 3^{4k+5} - 2\cdot 3^{2k+2} - 1 = 3^4\cdot 3^{4k+1} - 9\cdot 2\cdot 3^{2k} - 1 = 81\cdot 3^{4k+1} - 18\cdot 3^{2k} - 1 \\ &= 80\cdot 3^{4k+2} + 3^{4k+2} - 16\cdot 3^{2k} - 2\cdot 3^{2k} - 1 = B(k) + 80\cdot 3^{4k+1} - 16\cdot 3^{2k}. \end{aligned}$$

Η υπόθεση επαγωγής δίνει $16 \mid B(k)$ και επομένως παίρνουμε $16 \mid B(k+1)$. Έτσι, η προς απόδειξη σχέση ισχύει για κάθε θετικό ακέραιο.

γ) Θέτουμε $C(n) = 3^{3n+3} - 26n - 27$. Είναι $C(1) = 3^6 - 26 - 27 = 676$ και επομένως $169 \mid C(1)$. Υποθέτουμε ότι ισχύει $169 \mid C(k)$. Παίρνουμε την διαφορά:

$$C(k+1) - C(k) = 3^{3k+6} - 3^{3k+3} - 26 = 3^{3k+3}(3^3 - 1) - 26 = 26\,(27^{k+1} - 1).$$

Επιπλέον, ισχύει:

$$27^{k+1} - 1 = (27-1) \cdot (27^k + \cdots + 27 + 1) = 26 \cdot (27^k + \cdots + 27 + 1).$$

Έτσι, προκύπτει $169 \mid C(k+1) - C(k)$. Καθώς $169 \mid C(k)$, παίρνουμε $169 \mid C(k+1)$. □

Άσκηση 2.3. *Να προσδιοριστούν όλοι οι ακέραιοι $a \neq 3$ οι οποίοι ικανοποιούν την σχέση $a - 3 \mid a^3 - 3$.*

Απόδειξη. Ας είναι a ακέραιος με $a \neq 3$ τέτοιος, ώστε $a - 3 \mid a^3 - 3$. Γράφουμε:

$$a^3 - 3 = a^3 - 3^3 + 3^3 - 3 = (a-3)(a^2 + 3a + 9) + 24.$$

Έτσι, βλέπουμε ότι $a - 3 \mid 24$, απ΄ όπου προκύπτει:

$$a - 3 = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24.$$

Επομένως, έχουμε:

$$a = -21, -9, -5, -3, -1, 0, 1, 2, 4, 5, 6, 7, 9, 11, 15, 27.$$

□

Άσκηση 2.4. *Ας είναι n θετικός ακέραιος και $n = a_m \cdots a_0$ η συνήθης παράστασή του στο δεκαδικό σύστημα, δηλαδή $a_0, \ldots, a_m \in \{0, \ldots, 9\}$ και $a_m \neq 0$. Τότε, ισχύουν τα εξής:*

α) $2 \mid n \Leftrightarrow 2 \mid a_0$.
β) $4 \mid n \Leftrightarrow 4 \mid a_1 a_0$.
γ) $5 \mid n \Leftrightarrow 5 \mid a_0$.
δ) $25 \mid n \Leftrightarrow 25 \mid a_1 a_0$.
ε) $3 \mid n \Leftrightarrow 3 \mid a_m + \cdots + a_0$.
στ) $9 \mid n \Leftrightarrow 9 \mid a_m + \cdots + a_0$.
ζ) $11 \mid n \Leftrightarrow 11 \mid a_0 - a_1 + \cdots + (-1)^m a_m$.

Απόδειξη. Έχουμε $n = a_m 10^m + \cdots + a_1 10 + a_0$.

α) Καθώς $2 \mid 10, \ldots, 2 \mid 10^m$, ισχύει $2 \mid n$ αν και μόνον αν $2 \mid a_0$.

β) Έχουμε $4 \mid 100, \ldots, 4 \mid 10^m$ και επομένως $4 \mid n$ αν και μόνον αν $4 \mid a_1 10 + a_0$.

γ) Εργαζόμαστε όπως στο (α).

δ) Εργαζόμαστε όπως στο (β).

ε) Θα δείξουμε πρώτα ότι $10^j = 9k_j + 1$, όπου k_j ακέραιος για κάθε $j \in \mathbb{Z}^+$. Για $j = 1$ έχουμε $10 = 9 \cdot 1 + 1$ και επομένως ισχύει. Υποθέτουμε ότι για $j = m$ ισχύει. Για $j = m + 1$, έχουμε:

$$10^{m+1} = 10 \cdot 10^m = 10(9k_m + 1) = 9(10k_m + 1) + 1.$$

Συνεπώς, η προς απόδειξη ισότητα ισχύει γα κάθε $j = 1, 2, \ldots$. Άρα, έχουμε:

$$n = a_m 10^m + \cdots + 10a_1 + a_0 = \\ a_m(9k_m + 1) + \cdots + a_1(9k_1 + 1) + a_0 = 9(a_m k_m + \cdots + a_1 k_1) + a_m + \cdots + a_0.$$

Έτσι, βλέπουμε ότι $3 \mid n$ αν και μόνον αν $3 \mid a_m + \cdots + a_0$.

στ) Η παραπάνω ισότητα

$$n = 9(a_m k_m + \cdots + a_1 k_1) + a_m + \cdots + a_0$$

συνεπάγεται επίσης ότι $9 \mid n$ αν και μόνον αν $9 \mid a_m + \cdots + a_0$.

ζ) Έχουμε:

$$n = a_m 10^m + \cdots + 10a_1 + a_0 = a_m(11 - 1)^m + \cdots + (11 - 1)a_1 + a_0.$$

Από τον τύπο του διωνύμου του Νεύτωνα [6, Πρόταση 6.2, σελ. 27], παίρνουμε:

$$(11 - 1)^k = 11 \cdot A_k + (-1)^k \quad (k = 1, \ldots, m),$$

όπου A_k ακέραιος. Τότε, προκύπτει:

$$n = 11 \cdot (a_m A_m + \cdots + a_1 A_1) + \sum_{i=0}^{m} a_i (-1)^i.$$

Άρα, έχουμε $11 \mid n$ αν και μόνον αν $11 \mid a_0 + a_1 - a_2 + \cdots + (-1)^m a_m$. □

2.2 Ευκλείδεια Διαίρεση

Ένα από τα πλέον βασικά θεωρήματα της Θεωρίας Αριθμών γνωστό ως *Θεώρημα της διαίρεσης με υπόλοιπο* ή *Ευκλείδεια διαίρεση* είναι το εξής:

Θεώρημα 2.1. *Ας είναι a, b ακέραιοι με $b \neq 0$. Τότε, υπάρχει μοναδικό ζεύγος ακεραίων q, r τέτοιο, ώστε να ισχύει:*

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

Απόδειξη. Βλέπε ένα από τα συγγράμματα [6, Κεφάλαιο 3, Θεώρημα 2.1], [7, Κεφάλαιο 2, Θεώρημα 2.1] [4, Κεφάλαιο 1], [5, Θεώρημα 1.2.3, εδώ]. □

Οι ακέραιοι q και r καλούνται *πηλίκο* και *υπόλοιπο* της διαίρεσης του a με τον b, αντίστοιχα. Σύμφωνα με το παραπάνω θεώρημα, ένας ακέραιος a είναι της μορφής $a = 2k$ ή $a = 2k + 1$. Στην πρώτη περίπτωση ο a καλείται *άρτιος*, ενώ στη δεύτερη *περιττός*. Από το Θεώρημα 2.1 προκύπτει και το παρακάτω πόρισμα

Πόρισμα 2.1. *Ας είναι a, b ακέραιοι με $b \neq 0$. Τότε, υπάρχει μοναδικό ζεύγος ακεραίων q, r τέτοιο, ώστε να ισχύει:*

$$a = bq + r \quad \text{και} \quad -\tfrac{1}{2}|b| < r \leq \tfrac{1}{2}|b|.$$

Απόδειξη. Βλέπε [5, Πόρισμα 1.2.4, εδώ]. □

Ασκήσεις

Οι πρώτες τρεις ασκήσεις είναι εφαρμογές του Θεωρήματος 2.1.

΄Ασκηση 2.5. *Να υπολογιστεί το πηλίκο q και το υπόλοιπο r της Ευκλείδειας διαίρεσης του a με το b, όπου*
α) $a = -124$, $b = 34$.
β) $a = 453$, $b = -42$.

Απόδειξη. Για τον υπολογισμό του πηλίκου το μόνο που θα πρέπει να προσέξουμε είναι ότι $0 \leq r < |b|$.
α) Ισχύει:

$$-124 = -4 \cdot 34 + 12.$$

΄Αρα, έχουμε $q = -4$ και $r = 12$.
β) Ισχύει:

$$453 = 11 \cdot (-42) + 9$$

΄Ετσι, προκύπτει $q = 11$ και $r = 9$. □

΄Ασκηση 2.6. *Να βρεθεί ο θετικός ακέραιος a, ο οποίος διαιρούμενος με τον 53 δίνει πηλίκο ένα πολλαπλάσιο του 7 και υπόλοιπο το τετράγωνο του πηλίκου.*

Απόδειξη. Ας είναι q και r το πηλίκο και το υπόλοιπο της διαίρεσης του a με τον 53. Τότε $q = 7q'$, όπου q' ακέραιος, και $r = q^2 < 53$. Επομένως, έχουμε:

$$0 \leq 49\, q'^2 < 53,$$

απ΄ όπου έπεται $q' = 1$ και κατά συνέπεια $q = 7$. ΄Αρα $a = 53 \cdot 7 + 49 = 420$. □

΄Ασκηση 2.7. *Να δειχθεί ότι για κάθε θετικό ακέραιο n ο ακέραιος $3n^2 - 1$ δεν είναι τετράγωνο ακεραίου.*

Απόδειξη. Ας υποθέσουμε ότι υπάρχει ακέραιος n τέτοιος, ώστε $3n^2 - 1 = k^2$, όπου k είναι ακέραιος. Σύμφωνα με το Θεώρημα 2.1, έχουμε $k = 3q + r$, όπου q ακέραιος και $r \in \{0, 1, 2\}$. Αν $r = 0$, τότε $3n^2 - 1 = 9q^2$, απ΄ όπου παίρνουμε $3 \mid 1$ που είναι άτοπο. Αν $r = 1$, τότε έχουμε $3n^2 - 1 = (3q + 1)^2$ και επομένως $3n^2 - 1 = 9q^2 + 6q + 1$, απ΄ όπου έπεται $3 \mid 2$ που είναι άτοπο. Τέλος, ας είναι $r = 2$. Τότε $3n^2 - 1 = (3q + 2)^2$, απ΄ όπου παίρνουμε $3n^2 - 1 = 9q^2 + 6q + 4$ και επομένως $3 \mid 5$ που είναι άτοπο. □

Μία βασική τεχνική απόδειξης σχέσεων μεταξύ ακεραίων είναι να διακρίνουμε τις περιπτώσεις όπου ο ακέραιος διαιρείται ή όχι από το 2. Δηλαδή αν είναι άρτιος ή περιττός.

΄Ασκηση 2.8. *Ας είναι $P(X) = a_n X^n + \cdots + a_1 X + a_0$ ένα πολυώνυμο με ακέραιους συντελεστές. Αν οι ακέραιοι $P(0)$ και $P(1)$ είναι περιττοί, τότε να δειχθεί ότι η εξίσωση $P(X) = 0$ δεν έχει ακεραία λύση.*

Απόδειξη. Ας υποθέσουμε ότι ρ είναι ακέραιος με $P(\rho) = 0$. Τότε, έχουμε:

$$P(X) = (X - \rho)Q(X),$$

όπου $Q(X)$ είναι πολυώνυμο με ακέραιους συντελεστές. Έτσι, παίρνουμε $P(1) = (1-\rho)Q(1)$ και $P(0) = \rho Q(0)$. Καθώς οι ακέραιοι $P(0)$ και $P(1)$ είναι περιττοί, οι $1-\rho$ και ρ είναι επίσης περιττοί και κατά συνέπεια ο ρ είναι ταυτόχρονα άρτιος και περιττός που είναι άτοπο. □

΄Ασκηση 2.9. *Να δειχθεί ότι δεν υπάρχουν ακέραιοι x και y έτσι ώστε να ισχύει:*

$$5x^3 - 4y^2 - 6xy + 15x + 6y - 5 = 0.$$

Απόδειξη. Ας είναι x και y ακέραιοι τέτοιοι ώστε να ισχύει η παραπάνω ισότητα. Τότε, έχουμε:

$$5(x^3 + 3x - 1) = 4y^2 + 6xy - 6y,$$

απ΄ όπου έπεται ότι ο ακέραιος $x^3 + 3x - 1$ είναι άρτιος. Από την άλλη πλευρά, αν ο x είναι περιττός, τότε ο $x^3 + 3x - 1$ είναι περιττός και αν ο x είναι άρτιος, τότε πάλι ο $x^3 + 3x - 1$ είναι περιττός. ΄Αρα, σε κάθε περίπτωση $5(x^3 + 3x - 1)$ είναι περιττός που είναι άτοπο. □

2.3 Μέγιστος Κοινός Διαιρέτης

Ας είναι $a_1, \ldots, a_n$ ακέραιοι από τους οποίους ένας τουλάχιστον δεν είναι μηδέν. Ας είναι D το σύνολο των θετικών ακεραίων d με $d \mid a_1, \ldots, d \mid a_n$. Το σύνολο D δεν είναι κενό καθώς $1 \in D$. Αν $d \in D$, τότε υπάρχει $a_i \neq 0$ και $d \mid a_i$ και επομένως $d \leq |a_i|$. ΄Αρα, το σύνολο D είναι πεπερασμένο.

Ορισμός 2.2. Το μέγιστο στοιχείο του D καλείται *μέγιστος κοινός διαιρέτης* των $a_1, \ldots, a_n$ και συμβολίζεται με $(a_1, \ldots, a_n)$. Αν $(a_1, \ldots, a_n) = 1$, τότε οι ακέραιοι $a_1, \ldots, a_n$ καλούνται *πρώτοι μεταξύ τους*. Επίσης, αν $(a_i, a_j) = 1$ για κάθε $i, j \in \{1, \ldots, n\}$ με $i \neq j$, τότε οι οι ακέραιοι $a_1, \ldots, a_n$ καλούνται *πρώτοι μεταξύ τους ανά δύο*.

Παρατηρούμε ότι $(a_1, \ldots, a_n) = (|a_1|, \ldots, |a_n|)$ και $(a_1, \ldots, a_n) = (0, a_1, \ldots, a_n)$. Αν οι ακέραιοι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε είναι και πρώτοι μεταξύ τους. Το αντίστροφο δεν συμβαίνει. Π.χ. έχουμε $(15, 10, 6) = 1$ ενώ $(15, 10) = 5$, $(15, 6) = 3$ και $(10, 6) = 2$.

Θεώρημα 2.2. *Ας είναι $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και $d = (a_1, \ldots, a_n)$. Τότε, υπάρχουν ακέραιοι $k_1, \ldots, k_n$ έτσι, ώστε να ισχύει:*

$$k_1 a_1 + \cdots + k_n a_n = d.$$

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Θεώρημα 3.1] ή [7, Κεφάλαιο 2, Θεώρημα 2.2] ή [4, Κεφάλαιο 1]. □

Η ισότητα του προηγουμένου θεωρήματος είναι γνωστή ως ταυτότητα του Bézout. Για $n = 2$ έχουμε:

Πόρισμα 2.2. *Ας είναι a, b μη μηδενικοί ακέραιοι και $d = (a, b)$. Τότε, υπάρχουν ακέραιοι x_0, y_0 έτσι, ώστε να ισχύει:*

$$ax_0 + by_0 = d.$$

Απόδειξη. Βλέπε [5, Πρόταση 1.5.3, εδώ] □

Πόρισμα 2.3. *Ας είναι $a_1, \dots, a_n$ μη μηδενικοί ακέραιοι. Έχουμε $(a_1, \dots, a_n) = d$ αν και μόνον αν ισχύουν τα εξής:*

α) $d \mid a_1, \dots, d \mid a_n$.

β) Αν δ είναι θετικός ακέραιος με $\delta \mid a_1, \dots, \delta \mid a_n$, τότε $\delta \mid d$.

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πόρισμα 3.1] ή [6, Κεφάλαιο 2, Πόρισμα 2.1] □

Μερικές βασικές ιδιότητες του μέγιστου κοινού διαιρέτη δίνονται στις παρακάτω προτάσεις.

Πρόταση 2.2. *Αν $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ με $(a_1, \dots, a_n) = d$, τότε ισχύουν τα εξής:*

α) $(la_1, \dots, la_n) = |l|\, d$, *όπου* $l \in \mathbb{Z} \setminus \{0\}$.

β) $(a_1/d, \dots, a_n/d) = 1$.

γ) $d = (a_1 + l_2 a_2 + \cdots + l_n a_n, a_2, \dots, a_n)$, *όπου* $l_2, \dots, l_n \in \mathbb{Z}$.

δ) $d = (a_1, \dots, a_k, (a_{k+1}, \dots, a_n))$, *με* $1 < k < n$.

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 3.1] ή [7, Κεφάλαιο 2, Πρόταση 2.3]. □

Πρόταση 2.3. *Ας είναι a, b, c μη μηδενικοί ακέραιοι. Αν $a \mid bc$ και $\mu\kappa\delta(a, b) = 1$, τότε $a \mid c$.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 3.3 και Πρόταση 3.2] ή [7, Κεφάλαιο 2, Πρόταση 2.2]. □

Τέλος, παραθέτουμε τον *Ευκλείδειο αλγόριθμο* και τον *εκτεταμένο Ευκλείδειο αλγόριθμο*, δύο εξαιρετικά χρήσιμα εργαλεία όχι μόνο για την Θεωρία Αριθμών αλλά για τους περισσότερους τομείς των μαθηματικών.

Ευκλείδειος Αλγόριθμος. Έστω $a, b \in \mathbb{Z}$ και έστω χωρίς περιορισμό της γενικότητας ότι $a > b > 0$. Θέτω $r_0 = a$ και $r_1 = b$. Ισχύει ότι

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, \ 0 \le r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, \ 0 \le r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, \ 0 \le r_n < r_{n-1} \\
r_{n-1} &= q_n r_n
\end{aligned}$$

Εκτεταμένος Ευκλείδειος Αλγόριθμος. Η κατάστρωση των παραπάνω ισοτήτων μας επιτρέπει να προσδιορίσουμε ένα ζεύγος ακεραίων x_0 και y_0 οι οποίοι επαληθεύουν την ισότητα του Πορίσματος 2.2. Έχουμε:

$$\begin{aligned}
r_n &= r_{n-2} - q_{n-1} r_{n-1} \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2}) \\
&\vdots \\
&= x_0 r_0 + y_0 r_1
\end{aligned}$$

όπου $x_0, y_0 \in \mathbb{Z}$. Ο Ευκλείδειος αλγόριθμος μαζί με αυτή την διαδικασία καλούνται *Εκτεταμένος Ευκλείδειος Αλγόριθμος*.

Έτσι, μπορούμε να υπολογίσουμε τον μέγιστο κοινό διαιρέτη d των a, b καθώς και ακεραίους x_0 και y_0 με $ax_0 + by_0 = d$ [6, Κεφάλαιο 2, Ενότητα 4] ή [7, Κεφάλαιο 2, Ενότητα 4].

Ασκήσεις

Η πρώτη άσκηση είναι μια εφαρμογή του Ευκλειδείου αλγόριθμου και του εκτεταμένου Ευκλείδειου αλγορίθμου.

Άσκηση 2.10. *Να βρεθεί ο μέγιστος κοινός διαιρέτης των αριθμών 4523 και 2037 και να γραφεί ως γραμμικός συνδυασμός αυτών.*

Απόδειξη. Εφαρμόζουμε τον Ευκλείδειο αλγόριθμο για τους αριθμούς 4523 και 2037. Έχουμε:

$$\begin{aligned} 4523 &= 2 \cdot 2037 + 449, \\ 2037 &= 4 \cdot 449 + 241, \\ 449 &= 1 \cdot 241 + 208, \\ 241 &= 1 \cdot 208 + 33, \\ 208 &= 6 \cdot 33 + 10, \\ 33 &= 3 \cdot 10 + 3, \\ 10 &= 3 \cdot 3 + 1. \end{aligned}$$

Έτσι, παίρνουμε $(4523, 2037) = 1$.

Από την άλλη πλευρά, έχουμε:

$$1 = 10 - 3 \cdot 3 = 10 - 3(33 - 3 \cdot 10) = -3 \cdot 33 + 10 \cdot 10 =$$

$$-3 \cdot 33 + 10(208 - 6 \cdot 33) = 10 \cdot 208 - 63 \cdot 33 = 10 \cdot 208 - 63(241 - 1 \cdot 208) =$$

$$-63 \cdot 241 + 73 \cdot 208 = -63 \cdot 241 + 73(449 - 1 \cdot 241) = 73 \cdot 449 - 136 \cdot 241 =$$

$$73 \cdot 449 - 136(2037 - 4 \cdot 449) = -136 \cdot 2037 + 617 \cdot 449 =$$

$$-136 \cdot 2037 + 617(4523 - 2 \cdot 2037) = 617 \cdot 4523 - 1370 \cdot 2037.$$

Επομένως

$$617 \cdot 4523 - 1370 \cdot 2037 = 1.$$

□

Στις επόμενες δύο ασκήσεις αποδεικνύουμε σχέσεις κάνοντας χρήση των σχέσεων διαιρετότητας. Επισημαίνουμε ότι το σύνολο των ρητών περιγράφεται ως εξής:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0,\ (a, b) = 1 \right\}.$$

Ένα κλάσμα a/b με $a, b \in \mathbb{Z}$ και $b \neq 0$, καλείται *ανάγωγο* αν $(a, b) = 1$.

΄Ασκηση 2.11. *Ας είναι a και b ακέραιοι με $(a,b)=1$ και $8a+13b\neq 0$. Να δειχθεί ότι το κλάσμα*

$$\frac{3a+5b}{8a+13b}$$

είναι ανάγωγο.

Απόδειξη. Θέτουμε $d=(3a+5b, 8a+13b)$. Θα δείξουμε ότι $d=1$. Έχουμε $d \mid 3a+5b$ και $d \mid 8a+13b$. Τότε ισχύει $d \mid 8(3a+5b)$ και $d \mid 3(8a+13b)$, απ΄ όπου παίρνουμε:

$$d \mid 8(3a+5b)-3(8a+13b).$$

Καθώς η διαφορά του δεξιού μέλους της παραπάνω σχέσης ισούται με b, έχουμε $d \mid b$. Επίσης, ισχύει $d \mid 13(3a+5b)$ και $d \mid 5(8a+13b)$, απ΄ όπου προκύπτει:

$$d \mid 13(3a+5b)-5(8a+13b).$$

Η διαφορά του δεξιού μέλους της παραπάνω σχέσης ισούται με $-a$ και επομένως $d \mid a$. Από τις σχέσεις $d \mid a$ και $d \mid b$ παίρνουμε $d \mid (a,b)$ και κατά συνέπεια $d=1$. □

΄Ασκηση 2.12. *Κάθε ακέραιος >6 μπορεί να γραφεί ως άθροισμα δύο ακεραίων >1 που είναι πρώτοι μεταξύ τους.*

Απόδειξη. Αν n είναι περιττός >6, τότε $n=2+(n-2)$, όπου $n-2$ είναι περιττός >1 και επομένως $(2,n-2)=1$. Ας υποθέσουμε στη συνέχεια ότι ο n είναι άρτιος >6. Διακρίνουμε τις εξής περιπτώσεις:

α) $n=4k$, όπου k ακέραιος ≥ 2. Τότε $n=(2k-1)+(2k+1)$, όπου $2k+1>2k-1$. Αν υπάρχει ακέραιος $d\geq 2$ με $d \mid 2k-1$ και $d \mid 2k+1$, τότε, ισχύει:

$$d \mid (2k-1)-(2k-1) \Longrightarrow d \mid -2.$$

Επομένως $d=2$. Αυτό όμως είναι άτοπο γιατί οι ακέραιοι $2k-1$ και $2k+1$ είναι περιττοί. ΄Αρα $d=1$.

β) $n=4k+2$, όπου k ακέραιος ≥ 2. Τότε $n=(2k+3)+(2k-1)$, όπου $2k+3>2k-1>1$. Αν υπάρχει ακέραιος $d\geq 2$ με $d \mid 2k+3$ και $d \mid 2k-1$, τότε, ισχύει:

$$d \mid (2k+3)-(2k-1) \Longrightarrow d \mid 4.$$

Επομένως $d=2$ ή $d=4$ που είναι άτοπο γιατί οι ακέραιοι $2k-1$ και $2k+3$ είναι περιττοί. ΄Αρα $d=1$. □

Μία τεχνική για την απόδειξη ισότητας φυσικών a και b είναι να αποδειχθεί ότι $a \mid b$ και ότι $b \mid a$. Οι επόμενες δύο ασκήσεις είναι εφαρμογή αυτής της τεχνικής.

΄Ασκηση 2.13. *Ας είναι a, b και c περιττοί ακέραιοι. Να δειχθεί ότι ισχύει:*

$$(a,b,c)=\left(\frac{a+b}{2},\frac{b+c}{2},\frac{a+c}{2}\right).$$

Απόδειξη. Θέτουμε $d = (a, b, c)$ και

$$\delta = \left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{a+c}{2}\right).$$

Θα δείξουμε ότι $d = \delta$.

Έχουμε:

$$\delta \Big| \frac{a+b}{2}, \quad \delta \Big| \frac{b+c}{2}, \quad \delta \Big| \frac{a+c}{2},$$

απ'οπου, παίρνουμε:

$$\delta \Big| \frac{a+b}{2} + \frac{b+c}{2} - \frac{a+c}{2},$$
$$\delta \Big| \frac{b+c}{2} + \frac{a+c}{2} - \frac{a+b}{2},$$
$$\delta \Big| \frac{a+b}{2} + \frac{a+c}{2} - \frac{b+c}{2}.$$

Έτσι, προκύπτει $\delta \mid b$, $\delta \mid c$, $\delta \mid a$, αντίστοιχα, και επομένως $\delta \mid d$.

Αντιστρόφως, έχουμε $d \mid a+b$, $d \mid b+c$ και $d \mid a+c$. Καθώς οι ακέραιοι a, b και c είναι περιττοί, οι $a+b$, $b+c$ και $a+c$ είναι άρτιοι και κατά συνέπεια οι αριθμοί $\kappa = (a+b)/2$, $\lambda = (b+c)/2$, $\mu = (a+c)/2$ ακέραιοι. Επομένως, έχουμε $d \mid 2\kappa$, $d \mid 2\lambda$ και $d \mid 2\mu$. Επειδή ο ακέραιος d είναι περιττός, έχουμε $(d, 2) = 1$ και κατά συνέπεια η Πρόταση 2.3 δίνει:

$$d \Big| \frac{a+b}{2}, \quad d \Big| \frac{b+c}{2}, \quad d \Big| \frac{a+c}{2},$$

απ΄ όπου έχουμε $d \mid \delta$. Επειδή οι ακέραιοι d και δ είναι θετικοί, οι σχέσεις $\delta \mid d$ και $d \mid \delta$ δίνουν $d = \delta$. □

΄Ασκηση 2.14. *Να δειχθεί ότι για κάθε ζεύγος ακεραίων a και n με $a > 1$ και $n \geq 1$ ισχύει:*

$$(a-1, n) = \left(\frac{a^n - 1}{a-1}, a-1\right).$$

Απόδειξη. Θέτουμε $d = (a-1, n)$ και $\delta = ((a^n-1)/(a-1), a-1)$. Επίσης, παρατηρούμε ότι ισχύει:

$$\frac{a^n - 1}{a-1} = a^{n-1} + \cdots + a + 1 = (a^{n-1} - 1) + \cdots + (a-1) + n.$$

Έχουμε $d \mid a-1$ και $d \mid n$. Για κάθε θετικό ακέραιο k ισχύει $a-1 \mid a^k - 1$ και επομένως η παραπάνω ισότητα δίνει $d \mid (a^n-1)/(a-1)$. ΄Αρα, ισχύει $d \mid \delta$.

Από την άλλη πλευρά, έχουμε $\delta \mid (a^n-1)/(a-1)$ και $\delta \mid a-1$. Οπότε, από την παραπάνω ισότητα παίρνουμε $\delta \mid n$. Επομένως, έχουμε $\delta \mid d$. Καθώς οι ακέραιοι d και δ είναι θετικοί, οι σχέσεις $\delta \mid d$ και $d \mid \delta$ δίνουν $d = \delta$. □

Τέλος, παρατίθεται μία θεωρητική άσκηση με την ακολουθία Fibonacci και μία με την χρήση των τύπων Vieta.

΄Ασκηση 2.15. *Η ακολουθία του Fibonacci (F_n) ορίζεται ως εξής:*

$$F_1 = F_2 = 1 \quad \textit{και} \quad F_{n+1} = F_n + F_{n-1}, \quad \textit{για κάθε } n \geq 2.$$

Να δειχθεί ότι ισχύει $(F_n, F_{n+1}) = 1$, *για κάθε* $n \geq 1$.

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του n. Για $n = 1$, έχουμε $(F_1, F_2) = (1, 1) = 1$. Υποθέτουμε ότι για $n = k$ ισχύει $(F_k, F_{k+1}) = 1$. Για $n = k + 1$, έχουμε:

$$F_{k+2} = F_{k+1} + F_k.$$

Έτσι, χρησιμοποιώντας την υπόθεση της επαγωγής, παίρνουμε:

$$(F_{k+2}, F_{k+1}) = (F_{k+1} + F_k, F_{k+1}) = (F_k, F_{k+1}) = 1.$$

Συνεπώς, ισχύει $(F_n, F_{n+1}) = 1$, για κάθε $n \geq 1$. □

Άσκηση 2.16. *Ας είναι* a *και* b *θετικοί ακέραιοι τέτοιοι, ώστε ο αριθμός*

$$A = \frac{a^3 + 1}{b + 1} + \frac{b^3 + 1}{a + 1}$$

να είναι ακέραιος. Να δειχθεί ότι καθένας από τους δύο όρους του αθροίσματος είναι ακέραιος.

Απόδειξη. Αν μόνον ο ένας από τους δύο όρους του αθροίσματος είναι ακέραιος και ο άλλος όχι, τότε ο αριθμός A δεν είναι ακέραιος που είναι άτοπο. Ας υποθέσουμε ότι και οι δύο όροι του αθροίσματος δεν είναι ακέραιοι. Οι δύο αυτοί όροι είναι ρίζες της εξίσωσης

$$x^2 - Ax + B = 0,$$

όπου

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

Άρα, $A, B \in \mathbb{Z}$.

Αν $x = r/s$, όπου $r, s \in \mathbb{Z}$ με $(r, s) = 1$, είναι μία ρίζα της παραπάνω εξίσωσης, τότε έχουμε:

$$r^2 - Ars + Bs^2 = 0 \Longrightarrow r^2 = (Ar - Bs) \cdot s.$$

Έχουμε $s \mid r^2$ και καθώς $(r, s) = 1$ παίρνουμε $s \mid 1$, απ' όπου έπεται $s = \pm 1$. Επομένως, οι ρίζες της εξίσωσης είναι ακέραιοι και κατά συνέπεια τα κλάσματα

$$\frac{a^3 + 1}{b + 1} \quad \text{και} \quad \frac{b^3 + 1}{a + 1}$$

είναι επίσης ακέραιοι. □

2.4 Ελάχιστο Κοινό Πολλαπλάσιο

Ας είναι $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Ας είναι M το σύνολο των θετικών ακεραίων m με $a_1 \mid m, \ldots, a_n \mid m$. Ο ακέραιος $|a_1 \cdots a_n|$ ανήκει στο M και επομένως $M \neq \emptyset$.

Ορισμός 2.3. Το μικρότερο στοιχείο του συνόλου M καλείται *ελάχιστο κοινό πολλαπλάσιο* των $a_1, \ldots, a_n$ και συμβολίζεται με $[a_1, \ldots, a_n]$.

Παρατηρούμε ότι $[|a_1|, \ldots, |a_n|] = [a_1, \ldots, a_n]$.

Πρόταση 2.4. *Ας είναι $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Ο θετικός ακέραιος m είναι το ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$, αν και μόνον αν, ισχύει:*

α) $a_1 \mid m, \ldots, a_n \mid m$.

β) *Αν μ είναι θετικός ακέραιος με $a_1 \mid \mu, \ldots, a_n \mid \mu$, τότε $m \mid \mu$.*

Απόδειξη. Βλέπε [6, Πρόταση 5.1]. □

Στην παρακάτω προτάση δίνονται δύο βασικές ιδιότητες του ελαχίστου κοινού πολλαπλασίου.

Πρόταση 2.5. *Ας είναι $\lambda, a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και $m = [a_1, \ldots, a_n]$. Τότε, ισχύουν τα εξής:*

α) $[\lambda a_1, \ldots, \lambda a_n] = |\lambda| m$.

β) $(m/a_1, \ldots, m/a_n) = 1$.

γ) $m = [a_1, \ldots, a_k, [a_{k+1}, \ldots, a_n]]$, *με* $1 < k < n$.

Απόδειξη. Βλέπε [6, Πρόταση 5.2 και Πρόταση 5.3]. □

Ασκήσεις

΄Ασκηση 2.17. *Ας είναι a, b, c θετικοί ακέραιοι. Τότε, ισχύει:*

$$[a, b, c] = [[a, b], [a, c]].$$

Απόδειξη. Από την Πρόταση 2.5(γ) ισχύει:

$$[[a, b], [a, c]] = [[a, b], a, c] = [a, b, a, c] = [a, b, c].$$

□

΄Ασκηση 2.18. *Ας είναι a, b μη μηδενικοί ακέραιοι. Τότε, ισχύει:*

$$[a, b] = (a, b) \iff |a| = |b|.$$

Απόδειξη. Αν $|a| = |b|$, τότε $a = \pm b$, οπότε έχουμε

$$[a, b] = [a, \pm a] = |a| \cdot [1, \pm 1] = |a|$$

και

$$(a, b) = (a, \pm a) = |a| \cdot (1, \pm 1) = |a|$$

.

Αντιστρόφως, ας υποθέσουμε ότι $[a, b] = (a, b) = d$. Καθώς $d = (a, b)$, έπεται $d \mid a$ και $d \mid b$. Επίσης, επειδή $d = [a, b]$, παίρνουμε $a \mid d$ και $b \mid d$. Επομένως, ισχύει $|a| = |d|$ και $|b| = |d|$, απ΄ όπου έχουμε $|a| = |b|$. □

2.5 Πρώτοι Αριθμοί

Ορισμός 2.4. Ένας θετικός ακέραιος $p > 1$ καλείται *πρώτος,* αν οι μόνοι διαιρέτες του είναι οι ακέραιοι ± 1 και $\pm p$. Ένας πρώτος αριθμός που είναι διαιρέτης ενός ακεραίου n καλείται *πρώτος διαιρέτης* ή *πρώτος παράγοντας* του n. Ένας θετικός ακέραιος > 1 που δεν είναι πρώτος καλείται *σύνθετος*.

Παρατηρούμε ότι ένας ακέραιος $n > 1$ είναι σύνθετος αν και μόνον αν $n = ab$, με $1 < a \leq b < n$.

Θεώρημα 2.3. *Το πλήθος των πρώτων αριθμών είναι άπειρο.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Θεώρημα 6.1] ή [5, Πρόταση 1.3.3, εδώ] □

Πρόταση 2.6. *Κάθε σύνθετος ακέραιος > 1 έχει ένα πρώτο διαιρέτη p με $p < \sqrt{a}$.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 6.2] ή [5, Πρόταση 1.3.4, εδώ] □

Η πρόταση αυτή δίνει αμέσως το παρακάτω αποτέλεσμα που μπορεί να χρησιμοποιηθεί για να διαπιστωθεί ότι ένας θετικός ακέραιος είναι πρώτος.

Πόρισμα 2.4. *Αν ο ακέραιος $a > 1$ δεν διαιρείται από κανένα πρώτο p με $p \leq \sqrt{a}$, τότε ο a είναι πρώτος.*

Το παρακάτω θεώρημα είναι από τα σπουδαιότερα θεωρήματα της Θεωρίας Αριθμών και είναι γνωστό ως το *Θεμελιώδες Θεώρημα της Αριθμητικής*.

Θεώρημα 2.4. *Κάθε ακέραιος > 1 γράφεται ως γινόμενο πρώτων με μοναδικό τρόπο αν παραβλέψουμε την τάξη των πρώτων στο γινόμενο.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Θεώρημα 7.1] ή [5, Θεώρημα 1.7.1, εδώ] ή [4, Κεφάλαιο 1]. □

Έτσι, κάθε ακέραιος $a > 1$ γράφεται ως γινόμενο

$$a = p_1^{a_1} \cdots p_k^{a_k},$$

όπου $p_1, \ldots, p_k$ είναι διαφορετικοί πρώτοι και $a_1, \ldots, a_k$ θετικοί ακέραιοι. Η γραφή αυτή του a καλείται *πρωτογενής ανάλυση* του a.

Χρησιμοποιώντας την πρωτογενή ανάλυση ενός θετικού ακεραίου μπορούμε να βρούμε εύκολα τους διαιρέτες του, όπως δείχνει η παρακάτω πρόταση.

Πρόταση 2.7. *Ας είναι a ακέραιος > 1 και $a = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής ανάλυση του. Ο ακέραιος d διαιρεί τον a αν και μόνον αν $d = p_1^{b_1} \cdots p_k^{b_k}$ με $0 \leq b_i \leq a_i$ $(i = 1, \ldots, k)$.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 7.1]. □

Ένα πολύ χρήσιμο πόρισμα για τις ασκήσεις είναι το εξής:

Πρόταση 2.8. *Ας είναι $m \geq 2$, $b_1, \ldots, b_m \in \mathbb{Z}^+$ πρώτοι μεταξύ τους ανά δύο και ας είναι $a \in \mathbb{Z}$ έτσι, ώστε να ισχύει:*

$$a^n = b_1 \cdots b_m.$$

Τότε, για κάθε $i \in \{1, \ldots, m\}$ υπάρχει $c_i \in \mathbb{Z}^+$ με $b_i = c_i^n$.

Απόδειξη. [5, Πόρισμα 1.7.7, εδώ] □

Εάν η πρωτογενής ανάλυση δύο ακεραίων είναι γνωστή, τότε υπολογίζουμε εύκολα τον μέγιστο κοινό τους διαιρέτη και το ελάχιστο κοινό τους πολλαπλάσιο με την παρακάτω πρόταση.

Πρόταση 2.9. *Ας είναι $a_1, \ldots, a_n$ ακέραιοι > 1 με πρωτογενείς αναλύσεις*

$$a_i = p_1^{a_{i1}} \cdots p_k^{a_{ik}} \quad (i = 1, \ldots, n),$$

όπου $p_1, \ldots, p_k$ διαφορετικοί πρώτοι και $a_{i1}, \ldots, a_{ik}$ ακέραιοι ≥ 0. Τότε, έχουμε:

$$(a_1, \ldots, a_n) = p_1^{d_1} \cdots p_k^{d_k}, \quad [a_1, \ldots, a_n] = p_1^{m_1} \cdots p_k^{m_k},$$

όπου

$$d_j = \min\{a_{1j}, \ldots, a_{nj}\} \quad \text{και} \quad m_j = \max\{a_{1j}, \ldots, a_{nj}\}, \quad (j = 1, \ldots, k).$$

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 8.1 και Πρόταση 8.3]. □

Πόρισμα 2.5. *Ας είναι $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και m θετικός ακέραιος. Τότε έχουμε:*

$$(a_1^m, \ldots, a_n^m) = (a_1, \ldots, a_n)^m, \quad [a_1^m, \ldots, a_n^m] = [a_1, \ldots, a_n]^m.$$

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πόρισμα 8.1 και Πόρισμα 8.4]. □

Από την πρωτογενή ανάλυση ακεραίου έχουμε τα παρακάτω αποτελέσματα.

Πρόταση 2.10. *Ας είναι $a, b_1, \ldots, b_n$ ακέραιοι > 1 και οι $b_1, \ldots, b_n$ πρώτοι μεταξύ τους ανά δύο. Τότε, ισχύει:*

$$(a, b_1 \cdots b_n) = (a, b_1) \cdots (a, b_n).$$

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 8.2]. □

Πόρισμα 2.6. *Ας είναι $a, b_1, \ldots, b_n$ ακέραιοι > 1 και οι $b_1, \ldots, b_n$ πρώτοι μεταξύ τους ανά δύο. Αν $b_1 \mid a, \ldots, b_n \mid a$, τότε $b_1 \cdots b_n \mid a$.*

Πρόταση 2.11. *Ας είναι $a, b \in \mathbb{Z}$. Τότε ισχύει:*

$$(a, b)[a, b] = |ab|.$$

Απόδειξη. Βλέπε [6, Κεφάλαιο 2, Πρόταση 8.4] ή [5, Πρόταση 1.5.14, εδώ]. □

Ασκήσεις

Για τον υπολογισμό με το χέρι της πρωτογενούς ανάλυσης ενός ακεραίου τα βασικά μας εργαλία είναι τα κριτήρια διαιρετότητας των ακεραίων (΄Ασκηση 2.4) και η Πρόταση 2.6.

΄Ασκηση 2.19. *Να βρεθεί η πρωτογενής ανάλυση των ακεραίων* 23678, 78771, 1235328, 6745689.

Απόδειξη. Βλέπουμε αρχικά ότι το 23678 διαιρείται με το 2 οπότε έχω $23678 = 2 \cdot 11839$. Το 11839 δεν εμπίπτει σε κάποιους από τα γνωστά κριτήρια διαιρετότητας. Οπότε, καθώς $\sqrt{11839} < 110$, θα πρέπει να δούμε αν οι πρώτοι ακέραιοι μικρότεροι του 110 διαιρούν το 11839. Μετά από μια επίπονη διαδικασία, καταλήγουμε ότι το 11839 είναι πρώτος. Άρα, η πρωτογενής ανάλυση του 23678 είναι η $2 \cdot 11839$.

Βλέπουμε αρχικά ότι το 78771 διαιρείται με το 3 οπότε έχω $78771 = 3 \cdot 26257$. Στη συνέχεια παρατηρούμε ότι το 26257 διαιρείται με το 11 καθώς $7 - 5 + 2 - 6 + 2 = 0$. Οπότε έχουμε ότι $26257 = 11 \cdot 2387$. Βλέπουμε ότι και το 2387 διαιρείται με το 11 και έχουμε ότι $2387 = 11 \cdot 217$. Τώρα, εύκολα βλέπουμε ότι $217 = 7 \cdot 31$ και καθώς το 31 είναι πρώτος, η πρωτογενής ανάλυση του 78771 είναι η $3 \cdot 7 \cdot 11^2 \cdot 31$.

Με ανάλογο τρόπο καταλήγουμε στο ότι $1235328 = 2^7 \cdot 3 \cdot 3217$ και $6745689 = 3^2 \cdot 41 \cdot 101 \cdot 181$. □

Άσκηση 2.20. *Να εξεταστεί αν οι ακέραιοι* 1457, 1627 *είναι πρώτοι.*

Απόδειξη. Καθώς $\sqrt{1457} < 39$ αρκεί να ελέγξουμε αν το 1457 διαιρείται με κάποιον πρώτο μικρότερο του 39. Εκτελώντας τις διαιρέσεις διαπιστώνουμε ότι ο πρώτος 31 διαιρεί τον 1457 και κατά συνέπεια ο ακέραιος 1457 δεν είναι πρώτος.

Ομοίως, καθώς $\sqrt{1627} < 41$, αρκεί να ελέγξουμε αν ο ακέραιος 1627 διαιρείται με κάποιον πρώτο μικρότερο του 41. Εκτελώντας τις διαιρέσεις διαπιστώνουμε ότι κανένας πρώτος μικρότερος του 41 δεν διαιρεί τον 1457 και έται ο 1457 είναι πρώτος. □

Η ταυτότητα

$$a^4 + 4b^4 = \left((a+b)^2 + b^2\right)\left((a-b)^2 + b^2\right),$$

οφείλεται στη Sophie Germain η οποία είναι γνωστή για την συμβολή της στη Θεωρία Αριθμών και ειδικότερα στην απόδειξη του τελευταίου Θεωρήματος του Fermat. Η άσκηση που ακολουθεί είναι μια εφαρμογή αυτής της ταυτότητας.

Άσκηση 2.21. *Να δειχθεί ότι για κάθε ακέραιο $m \geq 2$ ο ακέραιος m^4+4 είναι σύνθετος.*

Απόδειξη. Έχουμε:

$$m^4 + 4 = (m^2+2)^2 - (2m)^2 = (m^2+2m+2)(m^2-2m+2).$$

Καθώς $m \geq 2$, ισχύει:

$$m^2 + 2m + 2 > m^2 - 2m + 2 \geq 2.$$

Επομένως, ο ακέραιος $m^4 + 4$ είναι σύνθετος. Ας σημειωθεί ότι για $m = 1$ έχουμε $m^4 + 4 = 5$. □

Στην βιβλιογραφία γίνεται αναφορά σε πρώτους με ιδιαίτερη μορφή (π.χ. Mersenne, Fermat κ.α.). Στην συνέχεια θα δούμε ασκήσεις με ιδιότητες πρώτων ιδιαίτερης μορφής.

Άσκηση 2.22. *Να βρεθούν όλοι οι πρώτοι της μορφής*

$$\frac{n(n+1)}{2} - 1$$

όπου n ακέραιος > 1.

Απόδειξη. Ας υποθέσουμε ότι $n = 2k + 1$, $k \in \mathbb{Z}^+$. Τότε, έχουμε:

$$\frac{n(n+1)}{2} - 1 = \frac{(2k+1)(2k+2)}{2} - 1 = (2k+1)(k+1) - 1 = 2k^2 + 3k = k(2k+3).$$

Για $k > 1$, ο ακέραιος αυτός είναι σύνθετος, ενώ για $k = 1$ παίρνουμε τον πρώτο 5.

Ας υποθέσουμε στη συνέχεια ότι $n = 2k$, $k \in \mathbb{Z}^+$. Τότε, έχουμε:

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

Αν ο k είναι περιττός, τότε ο παραπάνω ακέραιος είναι άρτιος. Καθώς ο μόνος πρώτος άρτιος είναι το 2, η μόνη δυνατή περίπτωση είναι $2k^2 + k - 1 = 2$ η οποία προκύπτει για $k = 1$. Αν $k = 2l$, όπου $l \in \mathbb{Z}^+$, τότε παίρνουμε:

$$2k^2 + k - 1 = 8l^2 + 2l - 1 = 9l^2 - (l^2 - 2l + 1) = (3l)^2 - (l-1)^2 = (2l+1)(4l-1).$$

Επομένως, σ΄ αυτή την περίπτωση έχουμε ένα σύνθετο ακέραιο. Συνεπώς, οι μόνοι πρώτοι της ζητούμενης μορφής είναι οι 2 και 5. □

΄Ασκηση 2.23. *Να δειχθεί ότι αν ο ακέραιος $A = 1 \cdots 1$ είναι πρώτος και το πλήθος των δεκαδικών του ψηφίων είναι n, τότε ο n είναι επίσης πρώτος. Ισχύει το αντίστροφο;*

Απόδειξη. Ας υποθέσουμε ότι ο n είναι σύνθετος. Τότε $n = kl$ και k, l είναι ακέραιοι με $1 < k, l < n$. Θέτουμε $B = 1 \cdots 1$, όπου το πλήθος των ψηφίων του B είναι ίσο με k, και έχουμε:

$$A = B \cdot 10^{n-k} + B \cdot 10^{n-2k} + \cdots + B \cdot 10^{n-(l-1)k} + B = B(10^{n-k} + 10^{n-2k} + \cdots + 10^{n-(l-1)k} + 1).$$

Επομένως, ο A είναι σύνθετος. ΄Ατοπο, και κατά συνέπεια ο n είναι πρώτος.

Το αντίστροφο δεν ισχύει. Για παράδειγμα, έχουμε $111 = 3 \cdot 37$ και $n = 3$. □

΄Ασκηση 2.24. *Να δειχθεί ότι αν n είναι θετικός ακέραιος τέτοιος, ώστε ο $P = 2^n + 1$ είναι πρώτος, τότε ο n είναι δύναμη του 2. ΄Ενας πρώτος αυτής της μορφής καλείται πρώτος του Fermat.*

Απόδειξη. Ας υποθέσουμε ότι $n = aq$, όπου q πρώτος ≥ 3 και $a \in \mathbb{Z}^+$. Τότε, έχουμε:

$$2^{aq} + 1 = (2^a + 1)((2^a)^{q-1} - (2^a)^{q-2} + \cdots + (-1)^{q-1}).$$

Καθώς $2^{aq} + 1 > 2^a + 1 > 1$ και $2^a + 1 \mid P$, ο P είναι σύνθετος. Αυτό όμως είναι άτοπο. ΄Αρα, ο n δεν έχει πρώτο διαιρέτη > 2 και κατά συνέπεια $n = 2^m$, όπου m θετικός ακέραιος. □

΄Ασκηση 2.25. *Να προσδιοριστούν οι πρώτοι αριθμοί x και y για τους οποίους ο αριθμός $x^{x+1} + y^{y+1}$ είναι πρώτος.*

Απόδειξη. Αν οι πρώτοι x και y είναι περιττοί, τότε ο ακέραιος $x^{x+1} + y^{y+1}$ είναι άρτιος > 2 και κατά συνέπεια σύνθετος. ΄Αρα $x = 2$ ή $y = 2$. Ας υποθέσουμε ότι $x = 2$ και y περιττός πρώτος. Τότε, ο $(y+1)/2$ είναι θετικός ακέραιος και ισχύει:

$$x^{x+1} + y^{y+1} = 8 + (y^{(y+1)/2})^2.$$

Αν $y > 3$, τότε υπάρχει θετικός ακέραιος k τέτοιος, ώστε να ισχύει:

$$y^{(y+1)/2} = 3k+1 \ \text{ ή } \ 3k+2.$$

Από την άλλη πλευρά έχουμε:

$$(3k+2)^2 = 3(3k^2+4k+1)+1 \quad \text{και} \quad (3k+1)^2 = 3(3k^2+2k)+1.$$

Επομένως, ισχύει:

$$y^{y+1} = 3m+1,$$

όπου m ακέραιος. Έτσι, παίρνουμε:

$$8 + y^{y+1} = 8 + 3m + 1 = 3(m+3)$$

και κατά συνέπεια ο ακέραιος $8 + y^{y+1}$ δεν είναι πρώτος. Τέλος, αν $y = 3$, τότε $2^3 + 3^4 = 89$ που είναι πρώτος. Άρα, οι ζητουμένοι ακέραιοι είναι $x = 2$ και $y = 3$. □

Άσκηση 2.26. *Να δειχθεί ότι το πλήθος των πρώτων της μορφής $4k+3$, όπου k θετικός ακέραιος, είναι άπειρο.*

Απόδειξη. Ας υποθέσουμε ότι $p_1, \ldots, p_m$ είναι όλοι οι πρώτοι της μορφής $4k+3$. Θεωρούμε τον ακέραιο:

$$A = 4p_1 \cdots p_m - 1.$$

Ο ακέραιος A είναι της μορφής $4k+3$, καθώς έχουμε $A = 4(p_1 \cdots p_m - 1) + 3$. Αν ο A είναι πρώτος, τότε ο A είναι κάποιος από τους $p_1, \ldots, p_m$. Καθώς όμως για κάθε $i = 1, \ldots, m$ έχουμε $A > p_i$, καταλήγουμε σε άτοπο. Άρα, ο A είναι σύνθετος.

Παρατηρούμε ότι το γινόμενο δύο ακεραίων της μορφής $4k+1$ είναι ακέραιος της ίδιας μορφής. Πραγματι, αν $4k_1+1$ και $4k_2+1$ είναι δύο ακέραιοι, τότε έχουμε:

$$(4k_1+1)(4k_2+1) = 4(4k_1k_2 + k_1 + k_2) + 1.$$

Επομένως, ο A θα έχει τουλάχιστον έναν πρώτο διαιρέτη p της μορφής $4k+3$. Οπότε, $p = p_j$ για κάποιο $j \in \{1, \ldots, m\}$. Άρα, έχουμε $p \mid A$ και $p \mid p_1 \cdots p_m$, απ' όπου έπεται $p \mid 1$ που είναι άτοπο. Συνεπώς, το πλήθος των πρώτων της μορφής $4k+3$ είναι άπειρο. □

Άσκηση 2.27. *Αν οι αριθμοί p και $8p-1$ είναι πρώτοι, τότε να δειχθεί ότι ο $8p+1$ είναι σύνθετος.*

Απόδειξη. Οι αριθμοί $8p-1$, $8p$, $8p+1$ είναι διαδοχικοί και κατά επομένως, σύμφωνα με την Άσκηση 2.1(β), ένας από αυτούς διαιρείται από τον 3. Αν $3 \mid 8p$, τότε, καθώς $(3,8) = 1$, έχουμε $3 \mid p$ και επομένως $p = 3$. Έτσι, παίρνουμε $8p+1 = 25$ που είναι σύνθετος. Ας υποθέσουμε ότι $p > 3$. Αν $3 \mid 8p-1$, τότε προκύπτει $3 = 8p-1$ γιατί ο $8p-1$ είναι πρώτος. Έτσι, έχουμε $p = 1/2$ που είναι άτοπο. Άρα ισχύει $3 \mid 8p+1$ και $8p+1 > 25$. Συνεπώς, ο αριθμός $8p+1$ είναι σύνθετος. □

Στη συνέχεια, θα δούμε την χρήση των ιδιοτήτων των πρώτων αριθμών στην απόδειξη ανισοτικών σχέσεων και στην εύρεση ακεραίων λύσεων σε εξισώσεις.

Άσκηση 2.28. *Ας είναι $p_1, p_2, \ldots$ η ακολουθία των πρώτων αριθμών. Να δειχθούν τα εξής:*

α) $p_n \leq p_1 \cdots p_{n-1} + 1$.

β) $p_n \leq 2^{2^{n-1}}$.

Απόδειξη. α) Θεωρούμε τον θετικό ακέραιο $A = p_1 \cdots p_{n-1} + 1$. Τότε, υπάρχει ένας πρώτος p_m με $p_m \mid A$ και επομένως $p_m \leq A$. Αν $p_m = p_i$, για κάποιο $i \in \{1, \ldots, n-1\}$, τότε παίρνουμε $p_m \mid 1$ που είναι άτοπο. Άρα, έχουμε $p_n \leq p_m$. Έτσι, προκύπτει $p_n \leq p_m \leq p_1 \cdots p_{n-1} + 1$.

β) Θα εφαρμόσουμε επαγωγή επί του n. Για $n = 1$, έχουμε $2^{2^{n-1}} = 2$ και $p_1 = 2$. Ας υποθέσουμε ότι η πρόταση ισχύει για κάθε $k < n$. Χρησιμοποιώντας την σχέση (α) έχουμε:

$$p_n \leq p_1 \cdots p_{n-1} + 1 \leq 2^{1+2+\cdots+2^{n-2}} + 1 = 2^{2^{n-1}-1} + 1 \leq 2^{2^{n-1}}.$$

□

Άσκηση 2.29. *Να βρεθούν οι ακέραιες θετικές λύσεις της εξίσωσης*

$$3^x + 3^y + 3^z = 2457,$$

όπου x, y, z είναι θετικοί ακέραιοι με $x < y < z$.

Απόδειξη. Η πρωτογενής ανάλυση του 2457 είναι: $2457 = 3^3 \cdot 7 \cdot 13$. Τότε, έχουμε:

$$3^x(1 + 3^{y-x} + 3^{z-x}) = 3^3 \cdot 7 \cdot 13.$$

Καθώς $3 \nmid 1 + 3^{y-x} + 3^{z-x}$, έπεται $x = 3$. Έτσι, προκύπτει:

$$1 + 3^{y-3} + 3^{z-3} = 7 \cdot 13,$$

απ' όπου έχουμε:

$$3^{y-3} + 3^{z-3} = 90 = 2 \cdot 3^2 \cdot 5.$$

Επομένως, παίρνουμε:

$$3^{y-3}(1 + 3^{z-y}) = 2 \cdot 3^2 \cdot 5.$$

Επειδή $3 \nmid 1 + 3^{z-y}$, προκύπτει $y = 5$. Οπότε, έχουμε:

$$1 + 3^{z-5} = 2 \cdot 5,$$

απ' όπου έπεται $3^{z-5} = 3^2$ και κατά συνέπεια $z = 7$. Άρα, έχουμε μοναδική λύση, την $(x, y, z) = (3, 5, 7)$. □

Άσκηση 2.30. *Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει:*

$$30 \mid n^5 - n.$$

Απόδειξη. Έχουμε $30 = 2 \cdot 3 \cdot 5$. Καθώς οι αριθμοί 2, 3 και 5 είναι πρώτοι μεταξύ τους ανά δύο, σύμφωνα με τη Πόρισμα 2.6, αρκεί να δείξουμε ότι $2 \mid n^5 - n$, $3 \mid n^5 - n$ και $5 \mid n^5 - n$. Γράφουμε

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n-1)n(n+1)(n^2 + 1).$$

Οι ακέραιοι $n-1$, n και $n+1$ είναι διαδοχικοί και επομένως από την ΄Ασκηση 2.1 έχουμε ότι $2 \mid n^5 - n$ και $3 \mid n^5 - n$. Στη συνέχεια, θα δείξουμε με επαγωγή επί του n ότι ισχύει $5 \mid n^5 - n$. Για $n = 0$, έχουμε $5 \mid 0$. Υποθέτουμε ότι η σχέση ισχύει για $n = k$, δηλαδή έχουμε $5 \mid k^5 - k$. Για $n = k+1$, έχουμε:

$$(k+1)^5 - (k+1) = (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - (k+1) = k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k).$$

Καθώς ισχύει $5 \mid k^5 - k$, παίρνουμε $5 \mid (k+1)^5 - (k+1)$. Συνεπώς, ισχύει $30 \mid n^5 - n$, για κάθε $n \in \mathbb{N}$. □

2.6 Συνδυαστικές Ασκήσεις

Στις πρώτες τέσσερεις ασκήσεις θα δούμε τεχνικές που αφορούν στον προσδιορισμό ακεραίων.

΄Ασκηση 2.31. *Ας είναι a θετικός ακέραιος τέτοιος, ώστε η διαίρεση του με τους 624 και 301 αφήνει υπόλοιπο 16. Να βρεθεί ο ακέραιος a.*

Απόδειξη. Από το Θεώρημα 2.1 έπεται ότι υπάρχουν ακέραιοι q_1, q_2 έτσι, ώστε:

$$a = 624\,q_1 + 16 \quad \text{και} \quad a = 301 q_2 + 16.$$

Οπότε, έχουμε:

$$624\,q_1 = 301 q_2.$$

Στη συνέχεια χρησιμοποιούμε τον Ευκλείδειο αλγόριθμο για να βρούμε των μέγιστο κοινό διαιρέτη των ακεραίων 624 και 301. ΄Εχουμε:

$$\begin{aligned} 624 &= 301 \cdot 2 + 22, \\ 301 &= 22 \cdot 13 + 15, \\ 22 &= 15 \cdot 1 + 7, \\ 15 &= 7 \cdot 2 + 1. \end{aligned}$$

΄Αρα $(624, 301) = 1$. Καθώς έχουμε $624 \mid 301 q_2$ και $(624, 301) = 1$, προκύπτει $624 \mid q_2$ και επομένως $q_2 = 624x$, όπου x ακέραιος. Συνεπώς, οι ζητούμενοι ακέραιοι είναι της μορφής $a = 624 \cdot 301x + 16$. □

΄Ασκηση 2.32. *Να προσδιοριστούν τα ψηφία a και b ώστε ο ακέραιος $A = 62ab427$ να διαιρείται από το 99.*

Απόδειξη. Καθώς $99 = 9 \cdot 11$, έχουμε $99 \mid A$ αν και μόνον αν $9 \mid A$ και $11 \mid A$. Σύμφωνα με την ΄Ασκηση 2.4, έχουμε $9 \mid A$ αν και μόνον αν $9 \mid 21 + a + b$ και $11 \mid A$ αν και μόνον αν $11 \mid 13 + a - b$. Οπότε, παίρνουμε:

$$\begin{aligned} 9 \mid A &\iff 9 \mid 3 + a + b, \\ 11 \mid A &\iff 11 \mid 2 + a - b. \end{aligned}$$

Επομένως, έχουμε:

$$a + b = 9l - 3, \quad a - b = 11k - 2,$$

όπου k και l είναι ακέραιοι. Λύνουμε το παραπάνω γραμμικό σύστημα ως προς a και b, και προκύπτει:

$$a = \frac{1}{2}(9l + 11k - 5), \quad b = \frac{1}{2}(9l - 11k - 1).$$

Επειδή $a, b \in \{0, 1, \ldots, 9\}$, έχουμε:

$$0 \leq a + b \leq 18, \quad -9 \leq a - b \leq 9$$

απ΄ όπου:

$$0 \leq 9l - 3 \leq 18, \quad -9 \leq 11k - 2 \leq 9.$$

΄Ετσι, παίρνουμε:

$$\frac{1}{3} \leq l \leq \frac{7}{3}, \quad \frac{-7}{11} \leq k \leq 1.$$

Συνεπώς, $l = 1, 2$ και $k = 0, 1$.

Καθώς οι a και b είναι ακέραιοι, οι αριθμοί $9l + 11k - 5$ και $9l - 11k - 1$ είναι άρτιοι. Αυτό όμως συμβαίνει όταν αμφότεροι οι k, l δεν είναι άρτιοι ή περιττοί. ΄Αρα, έχουμε τις εξής περιπτώσεις:
α) $l = 1$, $k = 0$. Τότε $a = 2$ και $b = 4$.
β) $l = 2$, $k = 1$. Τότε $a = 12$ και $b = 3$. Η περίπτωση όμως αυτή απορρίπτεται γιατί ο a είναι > 9.
Συνεπώς, ο ζητούμενος ακέραιος είναι ο $A = 6224427$. □

΄Ασκηση 2.33. *Να προσδιοριστούν οι τιμές που μπορεί να πάρει ο ρητός αριθμός x έτσι, ώστε ο αριθμός $A = 3x^2 - 5x$ να είναι ακέραιος.*

Απόδειξη. Αν $x \in \mathbb{Z}$, τότε $A \in \mathbb{Z}$. Ας είναι $x = a/b$, με $a, b \in \mathbb{Z}$, $b > 1$, $(a, b) = 1$ και ας υποθέσουμε ότι ο αριθμός

$$A = \frac{3a^2 - 5ab}{b^2}$$

είναι ακέραιος. Τότε $b^2 \mid 3a^2 - 5ab$ και επομένως $b \mid a(3a - 5b)$. Καθώς $(a, b) = 1$, έχουμε $b \mid 3a - 5b$ και επομένως $b \mid 3a$. ΄Ετσι, προκύπτει $b \mid 3$ και κατά συνέπεια $b = 3$ γιατί $b > 1$. Τότε, έχουμε:

$$A = \frac{3a^2 - 15a}{3^2} = \frac{a(a-5)}{3}.$$

Επίσης, καθώς $(a, b) = 1$ και $b = 3$, παίρνουμε $3 \nmid a$. Επομένως, έχουμε $3 \mid a - 5$ και κατά συνέπεια $a = 3k + 5$, όπου $k \in \mathbb{Z}$. Αντιστρόφως, για κάθε $k \in \mathbb{Z}$ ισχύει:

$$A = 3\left(\frac{3k+5}{3}\right)^2 - 5\left(\frac{3k+5}{3}\right) = 3k^2 + 5k.$$

Συνεπώς, οι ζητούμενοι αριθμοί είναι όλοι οι ακέραιοι και οι αριθμοί της μορφής $x = (3k + 5)/3$, όπου $k \in \mathbb{Z}$. □

΄Ασκηση 2.34. *Να βρεθούν οι πρώτοι p για τους οποίους ο αριθμός $(2^{p-1} - 1)/p$ είναι τέλειο τετράγωνο ακεραίου.*

Απόδειξη. Ας είναι ακέραιος A τέτοιος, ώστε $(2^{p-1}-1)/p = A^2$. Αν $p = 2$, τότε έχουμε $A^2 = (2^{p-1}-1)/p = 1/2$ που είναι άτοπο. Άρα $p \geq 3$. Οπότε, έχουμε:

$$\frac{1}{p}(2^{(p-1)/2}-1)(2^{(p-1)/2}+1) = A^2.$$

Αν q είναι πρώτος με $q \mid 2^{(p-1)/2}-1$ και $q \mid 2^{(p-1)/2}+1$, τότε $q = 2$. Καθώς οι ακέραιοι $2^{(p-1)/2} \pm 1$ είναι περιττοί, καταλήγουμε σε άτοπο. Άρα, έχουμε $(2^{(p-1)/2}-1, 2^{(p-1)/2}+1) = 1$. Έτσι, ο πρώτος p διαιρεί μόνον έναν από τους $2^{(p-1)/2} \pm 1$. Επομένως, έχουμε τις εξής περιπτώσεις:

α) $p \mid 2^{(p-1)/2}-1$. Καθώς $((2^{(p-1)/2}-1)/p, 2^{(p-1)/2}+1) = 1$, έχουμε $2^{(p-1)/2}+1 = C^2$, όπου $C = 2n+1$ και n ακέραιος. Επομένως, ισχύει:

$$2^{(p-1)/2} = C^2 - 1 = 4n(n+1).$$

Αν $n > 1$, τότε ο n ή ο $n+1$ έχει ένα περιττό διαιρέτη. Καθώς το αριστερό μέλος της παραπάνω ισότητας δεν έχει περιττό παράγοντα καταλήγουμε σε άτοπο. Αν $n = 1$, τότε $2^{(p-1)/2} = 8$, απ' όπου παίρνουμε $p = 7$. Από την άλλη πλευρά, έχουμε $(2^{7-1}-1)/7 = 3^2$.

β) $p \mid 2^{(p-1)/2}+1$. Τότε, ομοίως έχουμε $2^{(p-1)/2}-1 = B^2$, όπου $B = 2m+1$ και m ακέραιος. Έτσι, παίρνουμε:

$$2^{(p-1)/2} = B^2 + 1 = 4m(m+1) + 2.$$

Αν $(p-1)/2 \geq 2$, τότε ισχύει:

$$2^{(p-1)/2-1} = 2m(m+1) + 1,$$

απ' όπου $2 \mid 1$ που είναι άτοπο. Άρα $(p-1)/2 = 1$ και επομένως $p = 3$. Επίσης, βλέπουμε ότι $(2^{3-1}-1)/3 = 1$.

Επομένως, οι ζητούμενοι πρώτοι είναι οι 3 και 7. □

Οι επόμενες εννέα ασκήσεις αφορούν σχέσεις με ΕΚΠ και ΜΚΔ ακεραίων.

Άσκηση 2.35. *Ας είναι a και b ακέραιοι με $(a,b) = 1$. Να δειχθεί ότι ισχύει:*

$$(a^2+b^2, a+b) = 1 \text{ ή } 2.$$

Απόδειξη. Ας είναι $(a^2+b^2, a+b) = d$. Τότε, έχουμε:

$$d \mid a^2+b^2 \quad \text{και} \quad d \mid a+b.$$

Από την δεύτερη σχέση παίρνουμε $d \mid (a+b)(a-b)$. Οπότε, έχουμε $d \mid a^2+b^2 \pm (a^2-b^2)$, και επομένως $d \mid 2a^2$ και $d \mid 2b^2$, απ' όπου $d \mid (2a^2, 2b^2)$. Από την Πρόταση 2.2(α) και Πόρισμα 2.5, έχουμε:

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

Άρα $d = 1$ ή 2. □

Άσκηση 2.36. *Να δειχθεί ότι για κάθε φυσικό m ισχύει:*

$$(2^m+3^m, 2^{m+1}+3^{m+1}) = 1.$$

Απόδειξη. Έχουμε:

$$(2^m + 3^m, 2^{m+1} + 3^{m+1}) = \\ (2^m + 3^m, 2^{m+1} + 3^{m+1} - 2(2^m + 3^m)) = (2^m + 3^m, 3^m) = (2^m, 3^m) = (2,3)^m = 1.$$

□

Άσκηση 2.37. *Ας είναι a, m, n θετικοί ακέραιοι και $a > 1$. Να προσδιοριστούν οι μέγιστοι κοινοί διαιρέτες $d = (a^m - 1, a^n + 1)$ και $d' = (a^m + 1, a^n + 1)$.*

Απόδειξη. Ας είναι i και j οι μεγαλύτεροι θετικοί ακέραιοι έτσι, ώστε $2^i \mid m$ και $2^j \mid n$. Θα δείξουμε ότι ισχύει:

$$d = \begin{cases} a^{(m,n)} + 1, & \text{αν } i = j, \\ 1, & \text{αν } i \neq j \text{ και } a \text{ άρτιος}, \\ 2, & \text{αν } i \neq j \text{ και } a \text{ περιττός} \end{cases}$$

και

$$d' = \begin{cases} a^{(m,n)} + 1, & \text{αν } i > j, \\ 1, & \text{αν } i \leq j \text{ και } a \text{ άρτιος}, \\ 2, & \text{αν } i \leq j \text{ και } a \text{ περιττός}. \end{cases}$$

Θέτουμε:

$$b = a^{(m,n)}, \quad r = m/(m,n) \quad s = n/(m,n).$$

Έτσι, έχουμε $d = (b^r + 1, b^s + 1)$ και $(r,s) = 1$. Σύμφωνα με το Θεώρημα 2.2, υπάρχουν θετικοί ακέραιοι e και f με $er - fs = 1$. Επίσης, καθώς $d \mid b^r + 1$ και $d \mid b^s + 1$, υπάρχουν $k, l \in \mathbb{Z}$ με $b^r + 1 = dk$ και $b^s + 1 = dl$.

Αν $i = j$, τότε $2^i \mid (m,n)$ και $2^j \mid (m,n)$ και επομένως οι ακέραιοι r και s είναι περιττοί. Οπότε, ένας από τους e, f πρέπει να είναι άρτιος και ο άλλος περιττός. Λόγω συμμετρίας, μπορούμε να υποθέσουμε ότι ο e είναι περιττός και ο f άρτιος. Τότε, επειδή ο e είναι περιττός και ο f άρτιος, έχουμε:

$$(b^r)^e = (dk - 1)^e = ud - 1 \quad \text{και} \quad (b^s)^f = (dl - 1)^f = vd + 1,$$

όπου $u, v \in \mathbb{Z}$. Οπότε, παίρνουμε:

$$ud - 1 = (b^r)^e = b^{1+sf} = b(vd + 1),$$

απ΄ όπου προκύπτει:

$$(u - bv)d = b + 1.$$

Άρα, έχουμε $d \mid b + 1$. Από την άλλη πλευρά, καθώς οι οι ακέραιοι r και s είναι περιττοί, παίρνουμε $b + 1 \mid b^r + 1$, $b + 1 \mid b^s + 1$ και κατά συνέπεια $b + 1 \mid d$. Έτσι, καθώς οι ακέραιοι d και $b + 1$ είναι θετικοί, έχουμε $d = b + 1$.

Ας είναι $i \neq j$. Τότε, ο ένας από τους r, s είναι άρτιος και ο άλλος περιττός. Λόγω συμμετρίας, μπορούμε να υποθέσουμε ότι ο r είναι άρτιος και ο s περιττός. Τότε, υπάρχουν $y, z \in \mathbb{Z}$ έτσι, ώστε να έχουμε:

$$(b^r)^s = (dk - 1)^s = yd - 1 \quad \text{και} \quad (b^s)^r = (dl - 1)^r = zd + 1.$$

Επομένως, ισχύει $yd - 1 = zd + 1$, απ΄ όπου παίρνουμε $d \mid 2$. Καθώς όμως $2 \mid d$ αν και μόνον αν ο a είναι περιττός, παίρνουμε το ζητούμενο.

Για τον μέγιστο κοινό διαιρέτη d', χρησιμοποιώντας την Πρόταση 2.2(γ), παίρνουμε:

$$d' = (a^m - 1, a^n + 1) = (a^m + a^n, a^n + 1).$$

Καθώς ισχύει $(a, a^k + 1) = 1$, όπου k θετικός ακέραιος, από την Πρόταση 2.10, έχουμε:

$$\begin{aligned}(a^m + a^n, a^n + 1) &= (a^{\min\{m,n\}}(a^{|m-n|} + 1), a^n + 1) = \\ &(a^{|m-n|} + 1, a^n + 1)(a^{\min\{m,n\}}, a^n + 1) = (a^{|m-n|} + 1, a^n + 1).\end{aligned}$$

Αν $i > j$ (αντίστοιχα, $i < j$), τότε ο 2^j (αντίστοιχα 2^i) είναι η μεγαλύτερη δύναμη του 2 που διαιρεί τον $|m - n|$. Επίσης, αν $i = j$, τότε η μεγαλύτερη δύναμη του 2 που διαιρεί τον $|m - n|$ είναι $> 2^i$. Έτσι, ο τύπος για τον d μας δίνει τον τύπο για τον d'. □

΄Ασκηση 2.38. *Ας είναι a και b μη μηδενικοί ακέραιοι και $m, n \in \mathbb{N}$. Να δειχθεί ότι ισχύει:*

$$[a^{m+n}, a^m b^n, b^{m+n}] = [a, b]^{m+n}.$$

Απόδειξη. Από την Πρόταση 2.5 και Πόρισμα 2.5, έχουμε:

$$[a^{m+n}, a^m b^n, b^{m+n}] = [[a^{m+n}, b^{m+n}], a^m b^n] = [[a, b]^{m+n}, a^m b^n].$$

Από την άλλη πλευρά, έχουμε $a \mid [a, b]$ και $b \mid [a, b]$. Επομένως, ισχύει:

$$a^m \mid [a, b]^m \quad \text{και} \quad b^n \mid [a, b]^n,$$

απ΄ όπου έπεται $a^m b^n \mid [a, b]^{m+n}$. Άρα, παίρνουμε:

$$[[a, b]^{m+n}, a^m b^n] = [a, b]^{m+n}.$$

Συνδυάζοντας τις παραπάνω δύο ισότητες προκύπτει το αποτέλεσμα. □

΄Ασκηση 2.39. *Ας είναι a, b, c θετικοί ακέραιοι τέτοιοι, ώστε να έχουμε:*

$$(a, b, c)[a, b, c] = abc.$$

Να δειχθεί ότι ισχύει:

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

Απόδειξη. Γράφουμε:

$$a = p_1^{a_1} \cdots p_k^{a_k}, \quad b = p_1^{b_1} \cdots p_k^{b_k}, \quad c = p_1^{c_1} \cdots p_k^{c_k},$$

όπου $p_1, \ldots, p_k$ είναι διαφορετικοί πρώτοι και a_i, b_i, c_i ακέραιοι ≥ 0 $(i = 1, \ldots, k)$. Τότε, έχουμε:

$$(a, b, c) = \prod_{i=1}^{k} p_i^{\min\{a_i, b_i, c_i\}}, \quad [a, b, c] = \prod_{i=1}^{k} p_i^{\max\{a_i, b_i, c_i\}}.$$

Έτσι, η ισότητα $(a, b, c)[a, b, c] = abc$ δίνει:

$$\min\{a_i, b_i, c_i\} + \max\{a_i, b_i, c_i\} = a_i + b_i + c_i \quad (i = 1, \ldots, k).$$

Ας υποθέσουμε ότι $a_i \geq b_i \geq c_i$. Τότε, παίρνουμε $a_i + b_i + c_i = a_i + c_i$ και επομένως $b_i = 0$. Επειδή $b_i \geq c_i$, έπεται $c_i = 0$. Άρα, ο πρώτος p_i δεν διαιρεί τους b και c. Έτσι, βλέπουμε ότι για κάθε i, ο πρώτος p_i δεν διαιρεί δύο από τους a, b και c. Συνεπώς, παίρνουμε:

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

□

Άσκηση 2.40. *Ας είναι a, b, c τρεις μη μηδενικοί ακέραιοι. Να δειχθεί ότι ισχύει:*

$$([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)].$$

Απόδειξη. Ας είναι

$$a = p_1^{a_1} \cdots p_k^{a_k}, \quad b = p_1^{b_1} \cdots p_k^{b_k}, \quad c = p_1^{c_1} \cdots p_k^{c_k},$$

όπου $p_1, \ldots, p_k$ διαφορετικοί πρώτοι και $a_i \geq 0$, $b_i \geq 0$, $c_i \geq 0$ $(i = 1, \ldots, k)$. Έχουμε:

$$[a, b] = \prod_{i=1}^{k} p_i^{\max\{a_i, b_i\}}, \quad [b, c] = \prod_{i=1}^{k} p_i^{\max\{b_i, c_i\}}, \quad [a, c] = \prod_{i=1}^{k} p_i^{\max\{a_i, c_i\}}$$

και

$$(a, b) = \prod_{i=1}^{k} p_i^{\min\{a_i, b_i\}}, \quad (b, c) = \prod_{i=1}^{k} p_i^{\min\{b_i, c_i\}}, \quad (a, c) = \prod_{i=1}^{k} p_i^{\min\{a_i, c_i\}}.$$

Η προς απόδειξη ισότητα ισχύει, αν και μόνον αν, για κάθε $i = 1, \ldots, k$ έχουμε:

$$\min\{\max\{a_i, b_i\}, \max\{b_i, c_i\}, \max\{a_i, c_i\}\} = \max\{\min\{a_i, b_i\}, \min\{b_i, c_i\}, \min\{a_i, c_i\}\}.$$

Μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι $a_1 \geq b_i \geq c_i$. Τότε, έχουμε:

$$\min\{\max\{a_i, b_i\}, \max\{b_i, c_i\}, \max\{a_i, c_i\}\} = \min\{a_i, b_i, a_i\} = b_i$$

και

$$\max\{\min\{a_i, b_i\}, \min\{b_i, c_i\}, \min\{a_i, c_i\}\} = \max\{b_i, c_i, c_i\} = b_i.$$

Επομένως, η παραπάνω ισότητα και κατά συνέπεια η προς απόδειξη σχέση ισχύει. □

Άσκηση 2.41. (*Πρώτη Μαθηματική Ολυμπιάδα, ΗΠΑ, 1972*) *Ας είναι a, b, c θετικοί ακέραιοι. Να δειχθεί ότι ισχύει:*

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

Απόδειξη. Ας είναι

$$a = p_1^{a_1} \cdots p_k^{a_k}, \quad b = p_1^{b_1} \cdots p_k^{b_k}, \quad c = p_1^{c_1} \cdots p_k^{c_k},$$

όπου $p_1, \ldots, p_k$ διαφορετικοί πρώτοι και $a_i \geq 0$, $b_i \geq 0$, $c_i \geq 0$ $(i = 1, \ldots, k)$. Έχουμε:

$$[a,b] = \prod_{i=1}^{k} p_i^{\max\{a_i,b_i\}}, \quad [b,c] = \prod_{i=1}^{k} p_i^{\max\{b_i,c_i\}}, \quad [a,c] = \prod_{i=1}^{k} p_i^{\max\{a_i,c_i\}}$$

και

$$[a,b,c] = \prod_{i=1}^{k} p_i^{\max\{a_i,b_i,c_i\}}.$$

Οπότε, παίρνουμε:

$$\frac{[a,b,c]}{[a,b][b,c][c,a]} = \prod_{i=1}^{k} p_i^{2\max\{a_i,b_i,c_i\}-\max\{a_i,b_i\}-\max\{b_i,c_i\}-\max\{c_i,a_i\}}.$$

Από την άλλη πλευρά, έχουμε:

$$(a,b) = \prod_{i=1}^{k} p_i^{\min\{a_i,b_i\}}, \quad (b,c) = \prod_{i=1}^{k} p_i^{\min\{b_i,c_i\}}, \quad (a,c) = \prod_{i=1}^{k} p_i^{\min\{a_i,c_i\}}$$

και

$$(a,b,c) = \prod_{i=1}^{k} p_i^{\min\{a_i,b_i,c_i\}}.$$

Έτσι, παίρνουμε:

$$\frac{(a,b,c)^2}{(a,b)(b,c)(c,a)} = \prod_{i=1}^{k} p_i^{2\min\{a_i,b_i,c_i\}-\min\{a_i,b_i\}-\min\{b_i,c_i\}-\min\{c_i,a_i\}}.$$

Η προς απόδειξη ισότητα αληθεύει, αν και μόνον αν, για κάθε $i = 1, \ldots, k$ έχουμε:

$$\begin{aligned}\max\{a_i,b_i,c_i\} - \max\{a_i,b_i\} - \max\{b_i,c_i\} - \max\{b_i,c_i\} = \\ \min\{a_i,b_i,c_i\} - \min\{a_i,b_i\} - \min\{b_i,c_i\} - \min\{b_i,c_i\}.\end{aligned}$$

Μπορούμε να υποθέσουμε, δίχως βλάβη της γενικότητας, ότι $a_i \geq b_i \geq c_i$. Τότε, έχουμε:

$$2\max\{a_i,b_i,c_i\} - \max\{a_i,b_i\} - \max\{b_i,c_i\} - \max\{c_i,a_i\} = 2a_i - a_i - b_i - a_i = -b_i$$

και

$$2\min\{a_i,b_i,c_i\} - \min\{a_i,b_i\} - \min\{b_i,c_i\} - \min\{c_i,a_i\} = 2c_i - b_i - c_i - c_i = -b_i$$

και επομένως προκύπτει η παραπάνω ισότητα. Συνεπώς, η προς απόδειξη σχέση ισχύει. □

Άσκηση 2.42. *Ας είναι a, b, c τρεις μη μηδενικοί ακέραιοι με* $(a,b) = (b,c) = (a,c) = 1$. *Να δειχθεί ότι ισχύει*

$$(ab + bc + ac, abc) = 1.$$

Απόδειξη. Θέτουμε $d = (ab + bc + ac, abc)$. Ας υποθέσουμε ότι $d > 1$ και p είναι ένας πρώτος διαιρέτης του d. Άρα, έχουμε $p \mid ab + bc + ac$ και $p \mid abc$. Από την σχέση $p \mid abc$ έπεται ότι $p \mid a$ ή $p \mid b$ ή $p \mid c$. Υποθέτουμε ότι $p \mid a$. Από τις σχέσεις $p \mid a$ και $p \mid ab + bc + ac$, παίρνουμε $p \mid bc$ και κατά συνέπεια $p \mid b$ ή $p \mid c$. Επομένως, έχουμε $p \mid a$ και $p \mid b$ ή $p \mid a$ και $p \mid c$. Έτσι, παίρνουμε $p \mid (a, b)$ ή $p \mid (a, c)$. Καθώς $(a, b) = (a, c) = 1$ καταλήγουμε σε άτοπο. Άρα, ισχύει $d = 1$. □

Άσκηση 2.43. *Να προσδιοριστούν οι θετικοί ακέραιοι $a \leq b$ που επαληθεύουν τις σχέσεις $ab = 480$ και $[a, b] = 240$.*

Απόδειξη. Θέτουμε $(a, b) = d$. Τότε, υπάρχουν ακέραιοι x και y με $(x, y) = 1$ και $a = dx$, $b = dy$. Σύμφωνα με την Πρόταση 2.11, έχουμε:

$$(a, b)[a, b] = |ab|,$$

απ΄ όπου προκύπτει:

$$240d = d^2xy.$$

Επομένως, έπεται $240 = dxy$. Από την άλλη πλευρά, έχουμε $ab = 480$, απ΄ όπου $d^2xy = 480$. Οπότε, από τις ισότητες $240 = dxy$ και $d^2xy = 480$ παίρνουμε $d = 2$. Επομένως, έχουμε $xy = 120$. Στη συνέχεια θα προσδιορίσουμε όλους τους θετικούς ακεραίους $x \leq y$ με $xy = 120$ και $(x, y) = 1$. Εύκολα διαπιστώνουμε ότι τα ζεύγη με αυτή την ιδιότητα είναι τα εξής:

$$(1, 120), (3, 40), (5, 24), (8, 15).$$

Άρα, τα ζητούμενα ζεύγη είναι:

$$(a, b) = (2, 240), (6, 80), (10, 48), (16, 30).$$

□

Τέλος θα δούμε ασκήσεις που προτείνονται από ξένα περιοδικά ή από διεθνείς διαγωνισμούς.

Άσκηση 2.44. (*E.10523 [1996, 426] AMM 105, 8, 773-774.*) *Να βρεθούν όλες οι τετράδες $(a, b, c, d) \in \mathbb{Z}^4$ με $1 < a < b < c < d$ για τις οποίες ισχύει:*

$$(a - 1)(b - 1)(c - 1)(d - 1) \mid abcd - 1.$$

Απόδειξη. Θέτουμε:

$$y = (a - 1)(b - 1)(c - 1)(d - 1) \quad \text{και} \quad x = abcd - 1.$$

Παρατηρούμε αμέσως ότι $y < x$. Ας υποθέσουμε τώρα ότι $y \mid x$. Ας είναι $a \geq 5$. Τότε, ισχύει:

$$\frac{x}{y} < \frac{a}{a-1}\,\frac{b}{b-1}\,\frac{c}{c-1}\,\frac{d}{d-1} = \left(1 + \frac{1}{a-1}\right)\left(1 + \frac{1}{b-1}\right)\left(1 + \frac{1}{c-1}\right)\left(1 + \frac{1}{d-1}\right).$$

Καθώς $a \geq 5$, $b \geq 6$, $c \geq 7$ και $c \geq 8$, παίρνουμε:

$$\frac{x}{y} \leq \frac{5}{4}\,\frac{6}{5}\,\frac{7}{6}\,\frac{8}{7} = 2.$$

Επειδή $y \mid x$, έχουμε $x/y \in \mathbb{Z}$ και επομένως $x/y = 1$. Άρα $y = x$ που είναι άτοπο.

Αν κάποιος από τους a, b, c, d είναι άρτιος, τότε ο x είναι περιττός. Οπότε, ο y είναι περιττός και κατά συνέπεια οι ακέραιοι a, b, c, d είναι όλοι άρτιοι. ;ρα, οι ακέραιοι a, b, c, d είναι είτε όλοι άρτιοι, είτε όλοι περιττοί.

Στη συνέχεια, ας είναι $a = 4$. Τότε ο x είναι περιττός και οι ακέραιοι b, c, d άρτιοι. Έτσι, έχουμε:

$$\frac{x}{y} \leq \frac{4}{3}\,\frac{6}{5}\,\frac{8}{7}\,\frac{10}{9} < 3.$$

Καθώς $x/y \in \mathbb{Z}$, έχουμε $x/y = 1$ ή 2. Επειδή $y < x$, παίρνουμε $x = 2y$ και επομένως ο x είναι άρτιος που είναι άτοπο.

Ας είναι $a = 3$. Τότε, οι ακέραιοι b, c και d είναι περιττοί. Οπότε, έχουμε:

$$\frac{x}{y} \leq \frac{3}{2}\,\frac{5}{4}\,\frac{7}{6}\,\frac{9}{8} < 3.$$

Έτσι, καθώς $y < x$, παίρνουμε $x/y = 2$. Από την ισότητα $x = 3bcd - 1$, έπεται $3 \mid x+1$. Επίσης, αν κάποιος από τους ακέραιους $b-1$, $c-1$, $d-1$ διαιρείται από τον 3, τότε $3 \mid x$. Η σχέση αυτή σε συνδυασμό με την $3 \mid x+1$ δίνουν $3 \mid 1$ που είναι άτοπο. Άρα, κανένας από τους $b-1$, $c-1$, $d-1$ δεν διαιρείται από τον 3. Αν $b \neq 5$, τότε $b \geq 9$, $c \geq 11$ και $d \geq 15$. Έτσι, παίρνουμε:

$$\frac{x}{y} \leq \frac{3}{2}\,\frac{9}{8}\,\frac{11}{10}\,\frac{13}{12} < 2$$

που είναι άτοπο. Άρα, έχουμε $b = 5$. Καθώς $x/y = 2$, προκύπτει:

$$15cd - 1 = x = 2y = 16(c-1)(d-1),$$

απ΄ όπου έπεται ότι $(c-16)(d-16) = 239$. Καθώς ο ακέραιος 239 είναι πρώτος και $c < d$, παίρνουμε $c = 17$ και $d = 255$. Άρα, έχουμε $(a,b,c,d) = (3,5,17,255)$.

Τέλος, ας είναι $a = 2$. Τότε, οι ακέραιοι b, c και d άρτιοι και ο x/y περιττός. Έχουμε:

$$\frac{x}{y} \leq \frac{2}{1}\,\frac{4}{3}\,\frac{6}{5}\,\frac{8}{7} < 4.$$

Καθώς ισχύει $x \neq y$ και ο x/y είναι περιττός, παίρνουμε $x/y = 3$. Άρα, έχουμε $3 \mid x$ και επομένως κανένας από τους b, c και d δεν διαιρείται από τον 3. Αν $b > 4$, τότε ισχύει:

$$\frac{x}{y} \leq \frac{2}{1}\,\frac{8}{7}\,\frac{10}{9}\,\frac{14}{13} < 3$$

που είναι άτοπο. Άρα $b = 4$, απ΄ όπου έχουμε:

$$8cd - 1 = x = 3y = 9(c-1)(d-1).$$

Έτσι, προκύπτει $(c-9)(d-9) = 71$ και ο 71 είναι πρώτος. Οπότε, παίρνουμε $c = 10$ και $d = 80$. Συνεπώς, έχουμε $(a,b,c,d) = (2,4,10,80)$. □

΄Ασκηση 2.45. (*E.10597 [1997, 457] AMM 106, 5, σελ. 474.*) *Ας είναι* $d_1, \ldots, d_n$ $(n \geq 3)$ *θετικοί ακέραιοι με* $(d_1, \ldots, d_n) = 1$ *και* $d_i \mid d_1 + \cdots + d_n$ $(1 = 1, \ldots, n)$.
α) Να δειχθεί ότι $d_1 \cdots d_n \mid (d_1 + \cdots + d_n)^{n-2}$.
β) Να δοθεί ένα παράδειγμα n *ακεραίων* $d_1, \ldots, d_n$ *τέτοιων, ώστε ο εκθέτης* $n-2$ *να είναι ο μικρότερος δυνατός ώστε να ισχύει η προηγούμενη σχέση διαιρετότητας.*

Απόδειξη. α) Ας είναι p πρώτος με $p \mid d_1 \cdots d_n$ και p^k η μεγαλύτερη δύναμη του p έτσι, ώστε να υπάρχει j με $p^k \mid d_j$. Καθώς $d_j \mid d_1 + \cdots + d_n$, έπεται $p^k \mid d_1 + \cdots + d_n$ και επομένως $p^{k(n-2)} \mid (d_1 + \cdots + d_n)^{n-2}$. Από την αλλη πλευρά, επειδή $(d_1, \ldots, d_n) = 1$, υπάρχει δείκτης s με $p \nmid d_s$. Οπότε, από την σχέση $p \mid d_1 + \cdots + d_n$ συνεπάγεται ότι υπάρχει και ένας άλλος δείκτης r με $r \neq s$ και $p \nmid d_r$. ΄Αρα, αν p^a είναι η μεγαλύτερη δύναμη του p που διαιρεί τον $d_1 \cdots d_n$, τότε $a \leq k(n-2)$. Συνεπώς, ισχύει $d_1 \cdots d_n \mid (d_1 + \cdots + d_n)^{n-2}$.

β) Ας είναι $d_1 = 1$, $d_2 = n-1$ και $d_i = n$ $(i = 3, \ldots, n)$. Τότε, έχουμε:

$$d_1 + \cdots + d_n = 1 + (n-1) + (n-2)n = (n-1)n.$$

Επίσης, για κάθε $i = 1, \ldots, n$, ισχύει $d_i \mid d_1 + \cdots + d_n$ και $(d_1, \ldots, d_n) = 1$. Από την άλλη πλευρά, έχουμε:

$$d_1 \cdots d_n = n^{n-2}(n-1).$$

Καθώς $(n, n-1) = 1$, η μικρότερη δύναμη του $n(n-1)$ που διαιρείται από το $n^{n-2}(n-1)$ είναι ο ακέραιος $((n-1)n)^{n-2}$. ΄Ετσι, βλέπουμε ότι ο εκθέτης $n-2$ δεν είναι δυνατόν να γίνει μικρότερος.

΄Αλλα τέτοια παραδείγματα δίνονται από τους ακεραίους $d_1 = 1$, $d_2 = 2$, $d_i = 3 \cdot 2^{i-3}$ $(i = 2, \ldots, n-1)$ και $d_1 = 1$, $d_i = 2$ $(i = 3, \ldots, n)$, $d_n = 2n - 3$. □

΄Ασκηση 2.46. (*E.*3005 [1983, 400], *AMM, Vol.* 94, 1, 1987) *Ας είναι* n *ένας ακέραιος* ≥ 5. *Να δειχθεί ότι ο* n *είναι πρώτος, αν και μόνον αν, κάθε φορά που γράφουμε τον* n *ως άθροισμα θετικών ακεραίων* $n = n_1 + n_2 + n_3 + n_4$, *έχουμε* $n_{i_1} n_{i_2} \neq n_{i_3} n_{i_4}$, *για κάθε μετάθεση* i_1, i_2, i_3, i_4 *των* $1, 2, 3, 4$.

Απόδειξη. Ας υποθέσουμε ότι ο n είναι σύνθετος. Τότε, καθώς $n \geq 5$, υπάρχουν θετικοί ακέραιοι a, b έτσι, ώστε να ισχύει:

$$n = (a+1)(b+1).$$

Επομένως, έχουμε:

$$n = ab + a + b + 1.$$

Επίσης, θέτοντας $n_1 = ab$, $n_2 = a$, $n_3 = b$ και $n_4 = 1$, παίρνουμε:

$$n_1 n_4 = n_2 n_3.$$

Στη συνέχεια, ας υποθέσουμε ότι ο n είναι πρώτος και ότι υπάρχουν θετικοί ακέραιοι n_1, n_2, n_3, n_4 τέτοιοι, ώστε να ισχύει:

$$n = n_1 + n_2 + n_3 + n_4 \quad \text{και} \quad n_1 n_2 = n_3 n_4.$$

Θεωρούμε το κλάσμα $r/s = n_1/n_4 = n_2/n_3$, όπου r, s είναι θετικοί ακέραιοι με $(r, s) = 1$. Επομένως, έχουμε:

$$n_1 s = n_4 r \quad \text{και} \quad n_2 s = r n_3.$$

Καθώς $(r,s) = 1$, παίρνουμε $r \mid n_1$ και $r \mid n_2$. Οπότε, έχουμε $n_1 = kr$ και $n_2 = hr$, όπου k και h θετικοί ακέραιοι. Αντικαθιστώντας στις παραπάνω ισότητες, παίρνουμε:

$$n_3 = hs \quad \text{και} \quad n_4 = ks.$$

΄Ετσι, παίρνουμε:

$$n = n_1 + n_2 + n_3 + n_4 = kr + hr + ks + hs = (h + k)(r + s)$$

και επομένως ο n είναι σύνθετος που είναι άτοπο. □

2.7 Θεωρία Αριθμών με Maple

΄Οπως και σε κάθε κεφάλαιο η ενότητα αυτή είναι αφιερωμένη στις ασκήσεις των προηγούμενων ενοτήτων που μπορούν να επιλυθούν με Maple.

΄Ασκηση 2.47. *Να βρεθεί ο μέγιστος κοινός διαιρέτης των αριθμών 4523 και 2037 και να γραφεί ως γραμμικός συνδυασμός αυτών.*

Απόδειξη. Ο υπολογισμός του μέγιστου κοινού διαιρέτη γίνεται με μία εντολή:

```
gcd(4523,2037);
```

$$1$$

Υπάρχει, όμως, και η εντολή igcdex η οποία υπολογίζει και τα s και t για τα οποία ισχύει

$$4523s + 2037t = (4523, 2037).$$

```
igcdex(4523, 2037, 's', 't');
s;
t;
```

$$1$$
$$617$$
$$-1370$$

□

΄Ασκηση 2.48. *Ας είναι a θετικός ακέραιος τέτοιος, ώστε η διαίρεση του με τους 624 και 301 αφήνει υπόλοιπο 16. Να βρεθεί ο ακέραιος a.*

Απόδειξη. Για τον προσδιορισμό των a θα επιλύσουμε το σύστημα εξισώσεων

$$\begin{aligned} a &= 624q_1 + 16, \\ a &= 301q_2 + 16, \end{aligned}$$

όπου a, q_1, q_2 ακέραιοι. Για τον υπολογισμό των ακεραίων a, q_1, q_2 που ικανοποιούν τις παραπάνω εξισώσεις θα χρησιμοποιήσουμε την εντολή isolve η οποία υπολογίζει ακέραιες λύσεις:

```
isolve({a = 624*q1 + 16, a = 301*q2 + 16}, x);
          {a = 16 + 187824 x, q1 = 301 x, q2 = 624 x}
```

Εύκολα παρατηρούμε ότι τα a που ικανοποιούν τις αρχικές συνθήκες είναι οι ακέραιοι της μορφής $16 + 187824x$, όπου x μη αρνητικός ακέραιος. □

Κάνοντας κάποιος μια μικρή αναζήτηση στο διαδίκτυο, θα βρει πολύ εύκολα αρκετές ιστοσελίδες που υπολογίζουν τις πρωτογενείς αναλύσεις ακεραίων. Εμείς για τις επόμενες δύο ασκήσεις χρησιμοποιούμε τις εντολές ifactor και isprime

΄Ασκηση 2.49. *Να βρεθεί η πρωτογενής ανάλυση των ακεραίων* 23678, 78771, 1235328, 6745689.

Απόδειξη.

```
ifactor(23678);
                          (2) (11839)
ifactor(78771);
                                   2
                        (3) (7) (11)  (31)
ifactor(1235328);
                           7
                         (2)  (3) (3217)
ifactor(6745689);
                         2
                      (3)  (41) (101) (181)
```

□

΄Ασκηση 2.50. *Να εξεταστεί αν οι ακέραιοι* 1457, 1627 *είναι πρώτοι.*

Απόδειξη.

```
isprime(1457);
                             false
isprime(1627);
                              true
```

□

Βιβλιογραφία

[1] Apostol, T. (1986) Εισαγωγή στην Αναλυτική Θεωρία Αριθμών, Gunteberg.

[2] Baker, A. (1984) A Concise Introduction to the Theory o Numbers, Cambridge University Press.

[3] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[4] Hurwitz, A. (1981). Μαθήματα Αριθμοθεωρίας του A. Hurwitz επεξεργασμένα από τον Ν. Κριτικό. Αθήνα: Έκδόσεις Γ. Α. Πνευματικού.

[5] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[6] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

[7] Πουλάκης, Δ. (2014). Άλγεβρα. Θεσσαλονίκη: Εκδόσεις Ζήτη.

[8] Πουλάκης, Δ. (2015). Υπολογιστική Θεωρία Αριθμών. Συνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, http://www.kallipos.gr.

Κεφάλαιο 3

Αριθμητικές Συναρτήσεις

Το κεφάλαιο αυτό περιέχει ασκήσεις οι οποίες αφορούν την οικογένεια των αριθμητικών συναρτήσεων και την πράξη του ενελικτικού γινομένου. Ειδικότερα, επικεντρώνεται σε ένα βασικό υποσύνολο των αριθμητικών συναρτήσεων, τις πολλαπλασιαστικές συναρτήσεις και ιδιαίτερα σε τέσσερις βασικές πολλαπλασιαστικές συναρτήσεις, την σ, η οποία δίνει το άθροισμα των θετικών διαιρετών ενός θετικού ακεραίου, την τ, η οποία δίνει το πλήθος των θετικών διαιρετών ενός θετικού ακεραίου και τέλος τις συναρτήσεις μ του Mobious και ϕ του Euler. Τέλος, δίνονται ασκήσεις στις ειδικές κατηγορίες των τέλειων αριθμών, των φίλων αριθμών καθώς και στη γενίκευση τους, τους κοινωνικούς αριθμοούς.

3.1 Ενελικτικό Γινόμενο

Στην πρώτη ενότητα του κεφαλαίου αυτού εισάγουμε το σύνολο των αριθμητικών συναρτήσεων και μία διμελής πράξη σε αυτό.

Ορισμός 3.1. Μία συνάρτηση με πεδίο ορισμού το σύνολο $\mathbb{Z}^+$ και πεδίο τιμών το σύνολο $\mathbb{C}$ καλείται *αριθμητική*.

Θα συμβολίζουμε με $\mathcal{A}$ το σύνολο των αριθμητικών συναρτήσεων. Τρία σημαντικά παραδείγματα αριθμητικών συναρτήσεων είναι τα εξής:

α) Η συνάρτηση $\tau : \mathbb{Z}^+ \to \mathbb{Z}^+$, όπου $\tau(n)$ είναι το πλήθος των φυσικών διαιρετών του n.

β) Η συνάρτηση $\sigma : \mathbb{Z}^+ \to \mathbb{Z}^+$, όπου $\sigma(n)$ είναι το άθροισμα των φυσικών διαιρετών του n.

γ) Η ταυτοτική συνάτηση $i : \mathbb{Z}^+ \to \mathbb{Z}^+$, με $i(n) = n$, $\forall\, n \in \mathbb{Z}^+$.

Ορισμός 3.2. Ας είναι $f, g \in \mathcal{A}$. Η αριθμητική συνάρτηση $f * g$ που ορίζεται από την σχέση

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \quad \forall x \in \mathbb{Z}^+,$$

(όπου το d διατρέχει το σύνολο των θετικών διαιρετών του n) καλείται *ενελικτικό γινόμενο* ή *γινόμενο κατά Dirichlet* των f και g.

Έτσι, στο σύνολο $\mathcal{A}$ ορίζεται η πράξη $*$ που την καλούμε *ενελικτικό πολλαπλασιασμό* ή *πολλαπλασιασμό κατά Dirichlet*. Ο ενελικτικός πολλαπλασιασμός είναι πράξη προσεταιριστική, αντιμεταθετική και έχει ουδέτερο στοιχείο [13, Πρόταση 1.1]. Το ουδέτερο στοιχείο είναι η συνάρτηση ε που ορίζεται ως εξής:

$$\varepsilon(1) = 1 \quad \text{και} \quad \varepsilon(n) = 0, \ \forall n \geq 2.$$

Ας είναι $f \in \mathcal{A}$. Μία συνάρτηση $g \in \mathcal{A}$ καλείται *ενελικτική αντίστροφος* της f αν ισχύει:

$$f * g = \epsilon = g * f.$$

Ας υποθέσουμε ότι υπάρχει και μία δευτερη συνάρτηση h τέτοια, ώστε να ισχύει:

$$f * h = \epsilon = h * f.$$

Τότε, έχουμε:

$$g = g * \epsilon = g * (f * h) = (g * f) * h = \epsilon * h = h.$$

Συνεπώς, αν η ενελικτική αντίστροφος μίας αριθμητικής συνάρτησης f υπάρχει, τότε αυτή είναι μοναδική και συμβολίζεται με f^*. Η πρόταση που ακολουθεί μας δίνει μια ικανή και αναγκαία συνθήκη ώστε μια αριθμητική συνάρτηση να έχει ενελικτική αντίστροφο και έναν τρόπο για να υπολογίζουμε τις τιμές της.

Πρόταση 3.1. *Ας είναι f αριθμητική συνάρτηση. Η f έχει ενελικτική αντίστροφος αν και μονον αν $f(1) \neq 0$. Οι τιμές της f^* δίνονται από τους εξής αναγωγικούς τύπους:*

$$f^*(1) = \frac{1}{f(1)}$$

και για κάθε $n > 1$,

$$f^*(n) = -\frac{1}{f(1)} \sum_{d|n,\, d<n} f(n/d) f^*(d).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 1.2]. □

Ασκήσεις

΄Ασκηση 3.1. *Ας είναι $f : \mathbb{Z}^+ \to \mathbb{R}$ αριθμητική συνάρτηση τέτοια, ώστε να ισχύει $f(1) = 1999$ και*

$$f(1) + \cdots + f(n) = n^2 f(n), \quad \forall\, n \in \mathbb{Z}^+.$$

Να υπολογιστεί η τιμή $f(1999)$, να αιτιολογηθεί γιατί η f έχει ενελικτική αντίστροφο και να υπολογιστεί η τιμή $f^*(1999)$.

Απόδειξη. Θα προσδιορίσουμε ένα κλειστό τύπο ο οποίος θα μας δίνει τις τιμές της f. ΄Εχουμε:

$$f(1) + \cdots + f(n) = n^2 f(n) \quad \text{και} \quad f(1) + \cdots + f(n-1) = (n-1)^2 f(n-1).$$

Συνδυάζοντας τις δύο ισότητες, παίρνουμε:

$$(n-1)^2 f(n-1) + f(n) = n^2 f(n),$$

απ΄ όπου

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

΄Ετσι, έχουμε:

$$f(n) = \frac{n-1}{n+1} f(n-1).$$

Εφαρμόζοντας διαδοχικά αυτό τον τύπο προκύπτει:

$$f(n) = \frac{n-1}{n+1}\,\frac{n-2}{n} \cdots \frac{2}{4}\,\frac{1}{3} f(1) = \frac{2}{n(n+1)} 1999.$$

΄Ετσι, για $n = 1999$, παίρνουμε:

$$f(1999) = \frac{2}{1999 \cdot 2000}\, 1999 = \frac{1}{1000}.$$

Καθώς $f(1) \neq 0$, η συνάρτηση f έχει ενελικτική αντίστροφο. Ο αριθμός 1999 είναι πρώτος και επομένως οι μόνοι θετικοί διαιρέτες του 1999 είναι το 1 και το 1999. Οπότε, έχουμε ότι

$$\begin{aligned}(f * f^*)(1999) = \epsilon(1999) &\iff \sum_{d|1999} f^*(d) f\left(\frac{n}{d}\right) = 0 \\ &\iff f^*(1999)f(1) + f^*(1)f(1999) = 0.\end{aligned}$$

΄Αρα,

$$f^*(1999) = -\frac{f^*(1)f(1999)}{f(1)} = -\frac{f(1999)}{f(1)^2} = -\frac{1}{1999^2 \cdot 1000}.$$

□

3.2 Πολλαπλασιαστικές Συναρτήσεις

Στη συνέχεια θα ασχοληθούμε με ένα σημαντικό υποσύνολο των αριθμητικών συναρτήσεων το οποίο είναι οι πολλαπλασιαστικές συναρτήσεις.

Ορισμός 3.3. Μία μη-μηδενική αριθμητική συνάρτηση f καλείται *πολλαπλασιαστική* αν για κάθε $m, n \in \mathbb{Z}^+$ με $(m, n) = 1$ ισχύει:

$$f(mn) = f(m)f(n).$$

Η f καλείται *πλήρως πολλαπλασιαστική,* αν για κάθε $m, n \in \mathbb{Z}$ ισχύει:

$$f(mn) = f(m)f(n).$$

Θα συμβολίζουμε με $\mathcal{M}$ το σύνολο των πολλαπλασιαστικών συναρτήσεων. Οι αριθμητικές συναρτήσεις τ και σ που αναφέραμε στην προηγούμενη ενότητα είναι πολλαπλασιαστικές αλλά δεν είναι πλήρως πολλαπλασιαστικές [13, Κεφάλαιο 3, Παράδειγμα 2.3, Παράδειγμα 2.5] ή [12, Πρόταση 3.1.1, εδώ].

Για κάθε $f \in \mathcal{M}$ ισχύει $f(1) = 1$. Πράγματι, καθώς η f είναι μη-μηδενική υπάρχει $m \in \mathbb{Z}^+$ με $f(m) \neq 0$. Τότε, έχουμε:

$$f(m) = f(m \cdot 1) = f(m)f(1),$$

απ΄ όπου έπεται $f(1) = 1$. Έτσι, σύμφωνα με την Πρόταση 3.1, έχουμε ότι κάθε πολλαπλασιαστική συνάρτηση έχει ενελικτική αντίστροφο.

Πρόταση 3.2. *Ας είναι f μία πολλαπλασιαστική συνάρτηση και $a_1, \ldots, a_n$ θετικοί ακέραιοι πρώτοι μεταξύ τους ανά δύο. Τότε, έχουμε:*

$$f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 2.1]. □

Συνέπεια του ορισμού της πολλαπλασιαστικής συνάρτησης και της Πρότασης 3.2 είναι τα πορίσματα που ακολουθούν.

Πόρισμα 3.1. *Ας είναι $f \in \mathcal{M}$ και n ακέραιος > 1 με πρωτογενή ανάλυση $n = p_1^{a_1} \cdots p_k^{a_k}$. Τότε, ισχύει:*

$$f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k}).$$

Πόρισμα 3.2. *Ας είναι $f, g \in \mathcal{M}$. Αν για κάθε πρώτο p και κάθε θετικό ακέραιο a έχουμε $f(p^a) = g(p^a)$, τότε $f = g$.*

Πόρισμα 3.3. *Ας είναι $f \in \mathcal{M}$. Η f είναι πλήρως πολλαπλασιαστική συνάρτηση αν και μόνον αν για κάθε πρώτο p και κάθε θετικό ακέραιο a ισχύει $f(p^a) = f(p)^a$.*

Ας είναι n ακέραιος > 1 με πρωτογενή ανάλυση $n = p_1^{a_1} \cdots p_k^{a_k}$. Τότε, από το Πόρισμα 3.1 έχουμε:

$$\tau(n) = (a_1 + 1) \cdots (a_k + 1) \tag{3.1}$$

και

$$\sigma(n) = \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{a_i}) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}. \tag{3.2}$$

Οι παρακάτω προτάσεις μας δίνουν τρόπους παραγωγής καινούργιων πολλαπλασιαστικών συναρτήσεων.

Πρόταση 3.3. *Ας είναι $f, g \in \mathcal{M}$. Τότε ισχύουν τα εξής:*

α) Το (συνηθισμένο) γινόμενο fg των f και g, που ορίζεται από την σχέση

$$(fg)(n) = f(n)g(n), \quad \text{για κάθε } n \in \mathbb{Z}^+,$$

είναι πολλάπλασιαστική συνάρτηση.

β) Αν $g(n) \neq 0$, για κάθε $n \in \mathbb{Z}^+$, τότε το πηλίκο f/g των f και g, που ορίζεται από την σχέση

$$(f/g)(n) = f(n)/g(n), \quad \text{για κάθε } n \in \mathbb{Z}^+,$$

είναι πολλαπλασιαστική συνάρτηση.

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 2.2]. □

Πρόταση 3.4. *Το ενελικτικό γινόμενο δύο πολλαπλασιαστικών συναρτήσεων είναι πολλαπλασιαστική συνάρτηση.*

Απόδειξη. [13, Κεφάλαιο 3, Πρόταση 2.3]. □

Πόρισμα 3.4. *Ας είναι f αριθμητική συνάρτηση και F η αριθμητική συνάρτηση που ορίζεται από την σχέση*

$$F(n) = \sum_{d|n} f(d), \quad \forall\, n \in \mathbb{Z}^+.$$

Αν η συνάρτηση f είναι πολλαπλασιαστική, τότε και η F είναι πολλαπλασιαστική.

Πρόταση 3.5. *Η ενελικτική αντίστροφος μίας πολλαπλασιαστική συνάρτησης είναι πολλαπλασιαστική.*

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 2.4]. □

Ασκήσεις

Για να εξετάσουμε αν κάποια αριθμητική συνάρτηση είναι πολλαπλασιαστική, μπορούμε να χρησιμοποιήσουμε τον ορισμό ή τις Προτάσεις 3.3, 3.4 και 3.5. Για να αποδείξουμε ότι μια αριθμητική συνάρτηση δεν είναι πολλαπλασιαστική αρκεί να δώσουμε ένα αντιπαράδειγμα.

΄Ασκηση 3.2. *Ας είναι η συνάρτηση*

$$\gamma : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+, \;\; n \longmapsto \gamma(n),$$

όπου $\gamma(n)$ το γινόμενο των φυσικών διαιρετών του n. Να δειχθούν τα εξής:

α) Η συνάρτηση γ δεν είναι πολλάπλασιαστική.

β) $\gamma(n) = n^{\tau(n)/2}$.

γ) $\gamma(n) = n^2$ και $n > 1$ αν και μόνον αν $n = p^3$ ή $n = pq$, όπου p, q διακεκριμμένοι πρώτοι.

Απόδειξη. α) Θα αποδείξουμε ότι η γ δεν είναι πολλαπλασιαστική δίνοντας ένα αντιπαράδειγμα. Για $m = 2$ και $n = 3$ έχουμε ότι

$$\gamma(2) = 1 \cdot 2 = 2, \;\; \gamma(3) = 1 \cdot 3 = 3, \;\; \gamma(6) = 1 \cdot 2 \cdot 3 \cdot 6 = 36.$$

Καθώς $\gamma(2) \cdot \gamma(3) \neq \gamma(6)$, έχουμε ότι η γ δεν είναι πολλαπλασιαστική.

β) Πρώτα παρατηρούμε ότι αν d είναι ένας θετικός διαιρέτης του n, τότε n/d είναι επίσης ένας θετικός διαιρέτης του n. ΄Ετσι, η αντιστοιχία $d \mapsto n/d$ ορίζει μία αμφίεση του συνόλου των θετικών διαιρετών $D(n)$ του n στον εαυτόν του. Οποτε, αν $d_1, \ldots, d_{\tau(n)}$ είναι όλα τα στοιχεία του $D(n)$, τότε έχουμε:

$$\gamma(n) = d_1 \cdots d_{\tau(n)} = \frac{n}{d_1} \cdots \frac{n}{d_{\tau(n)}},$$

απ΄ όπου παίρνουμε $\gamma(n)^2 = n^{\tau(n)}$. Άρα, ισχύει $\gamma(n) = n^{\tau(n)/2}$.

γ) Από την β) έχουμε ότι $\gamma(n) = n^2$ αν και μόνον αν $\tau(n) = 4$. Ας είναι $n > 1$ και $n = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής ανάλυση του, Τότε έχουμε:

$$\tau(n) = (a_1 + 1) \cdots (a_k + 1).$$

Ας υποθέσουμε ότι $\tau(n) = 4$. Αν $k > 2$, τότε $\tau(n) > 4$ που είναι άτοπο. Για $k = 2$, έχουμε ότι $4 = (a_1 + 1)(a_2 + 1)$ από όπου προκύπτει ότι $a_1 = a_2 = 1$, οπότε, $n = p_1 p_2$. Ομοίως προκύπτει ότι για $k = 1$, $n = p_1^3$. Αντιστρόφως, αν $n = p_1 p_2$, τότε έχουμε $\tau(n) = 4$. Επίσης, αν $n = p_1^3$, τότε $\tau(n) = 4$. □

΄Ασκηση 3.3. *Να προσδιοριστεί η συνάρτηση* τ^*.

Απόδειξη. Η συνάρτηση τ είναι πολλαπλασιαστική και επομένως ισχύει $\tau^*(1) = 1$. Από την σχέση $\tau * \tau^* = \epsilon$, εχουμε $(\tau * \tau^*)(p^k) = 0$, για κάθε πρώτο p και $k \in \mathbb{Z}^+$. Για $k = 1$, έχουμε:

$$\tau^*(p)\tau(1) + \tau^*(1)\tau(p) = 0,$$

απ΄ όπου $\tau^*(p) = -2$. Για $k = 2$, έχουμε:

$$\tau^*(p^2)\tau(1) + \tau^*(p)\tau(p) + \tau^*(1)\tau(p^2) = 0,$$

απ΄ όπου $\tau^*(p^2) = 1$. Τέλος, για $k = 3$, παίρνουμε:

$$\tau^*(p^3)\tau(1) + \tau^*(p^2)\tau(p) + \tau^*(p)\tau(p^2) + \tau^*(1)\tau(p^3) = 0,$$

και επομένως $\tau^*(p^3) = 0$.

Στη συνέχεια, υποθέτουμε ότι ισχύει $\tau^*(p^k) = 0$ για $k = 4, \ldots, m$. Τότε, έχουμε:

$$\sum_{d|p^m} \tau^*(d)\tau(p^m/d) = 0.$$

΄Ετσι, παίρνουμε:

$$\tau^*(p^k)\tau(1) + \tau^*(p^2)\tau(p^{k-2}) + \tau^*(p)\tau(p^{k-1}) + \tau^*(1)\tau(p^k) = 0$$

και επομένως προκύπτει:

$$\tau^*(p^k) = -(k-1) + 2k - (k+1) = 0.$$

΄Αρα, ισχύει $\tau^*(p^k) = 0$, για κάθε $k \geq 3$.

Σύμφωνα με την Πρόταση 3.5, η συνάρτηση τ^* είναι πολλαπλασιαστική. Επομένως έχουμε:

$$\tau^*(n) = \begin{cases} 1, & \text{αν } n = 1, \\ 0, & \text{αν υπάρχει πρώτος } p \text{ τέτοιος ώστε } p^3 \mid n, \\ (-2)^k, & n = p_1 \cdots p_k b^2, \text{όπου } b \text{ είναι ακέραιος ελεύθερος τετραγώνου} \\ & \text{και } p_i \nmid b, \ (i = 1, \ldots, k). \end{cases}$$

□

Στις ασκήσεις που ακολουθούν παρουσιάζουμε κάποιες τεχνικές για να υπολογίζουμε ακεραίους που ικανοποιούν κάποιες σχέσεις.

΄Ασκηση 3.4. *Να βρεθούν όλα τα ζεύγη θετικών ακεραίων m και n με $\tau(m) = 10$, $\tau(n) = 21$ και $(m, n) = 18$.*

Απόδειξη. Αν $m = p_1^{a_1} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση του m, τότε:

$$\tau(m) = \tau(p_1^{a_1} \cdots p_s^{a_s}) = (a_1 + 1) \cdots (a_s + 1) = 10.$$

Καθώς $10 = 2 \cdot 5$, έχουμε $s \leq 2$. Αν $s = 2$, τότε $m = p_1 p_2^4$ και αν $s = 1$, τότε $m = p_1^9$. Ομοίως, αν $n = q_1^{b_1} \cdots q_t^{b_t}$ η πρωτογενής ανάλυση του n, τότε έχουμε:

$$\tau(n) = \tau(q_1^{b_1} \cdots q_t^{b_t}) = (b_1 + 1) \cdots (b_t + 1) = 21 = 3 \cdot 7,$$

απ΄ όπου προκύπτει $n = q_1^{20}$ ή $n = q_1^2 q_2^6$.

Καθώς $(m, n) = 18 = 2 \cdot 3^2$, συνεπάγεται ότι και ο m και ο n έχουν και το 3 και το 2 ως παράγοντες. ΄Αρα, ο m θα είναι της μορφής $p_1 p_2^4$ όπου ή ο p_1 θα είναι το 2 και ο p_2 θα είναι το 3 ή το αντίστροφο. Ομοίως, ο n θα είναι της μορφής $q_1^2 q_2^6$ όπου ή ο q_1 θα είναι το 2 και ο q_2 θα είναι το 3 ή το αντίστροφο. ΄Ετσι, προκύπτουν οι εξής περιπτώσεις:

$$\begin{aligned}
p_1 = 2, p_2 = 3, q_1 = 2, q_2 = 3 &\implies (m, n) = (2 \cdot 3^4, 2^2 \cdot 3^6) = 2 \cdot 3^4 \neq 18, \\
p_1 = 2, p_2 = 3, q_1 = 3, q_2 = 2 &\implies (m, n) = (2 \cdot 3^4, 3^2 \cdot 2^6) = 2 \cdot 3^2 = 18, \\
p_1 = 3, p_2 = 2, q_1 = 2, q_2 = 3 &\implies (m, n) = (3 \cdot 2^4, 2^2 \cdot 3^6) = 2^2 \cdot 3 \neq 18, \\
p_1 = 3, p_2 = 2, q_1 = 3, q_2 = 2 &\implies (m, n) = (3 \cdot 2^4, 3^2 \cdot 2^6) = 2^4 \cdot 3 \neq 18.
\end{aligned}$$

΄Αρα, οι μόνες επιλογές για τους ακεραίους m και n είναι: $m = 2 \cdot 3^4 = 162$ και $n = 3^2 \cdot 2^6 = 576$. □

΄Ασκηση 3.5. *Να βρεθούν οι θετικοί ακέραιοι για τους οποίους ισχύει $\sigma(n) = 12$.*

Απόδειξη. Καθώς $\sigma(n) > n$ αρκεί να ελέγξουμε μόνο τους θετικούς ακεραίους $n \leq 11$. ΄Ετσι έχουμε:

$$\begin{aligned}
&\sigma(2) = 1 + 2 = 3, && \sigma(3) = 1 + 3 = 4, \\
&\sigma(4) = 1 + 2 + 4 = 7, && \sigma(5) = 1 + 5 = 6, \\
&\sigma(6) = 1 + 2 + 3 + 6 = 12, && \sigma(7) = 1 + 7 = 8, \\
&\sigma(8) = 1 + 2 + 4 + 8 = 15, && \sigma(9) = 1 + 3 + 9 = 13, \\
&\sigma(10) = 1 + 2 + 5 + 10 = 18, && \sigma(11) = 1 + 11 = 12.
\end{aligned}$$

΄Αρα $\sigma(n) = 12$ μόνο για $n = 6, 11$. □

΄Ασκηση 3.6. *Να βρεθούν όλοι οι θετικοί ακέραιοι k για τους οποίους υπάρχει $n \in \mathbb{Z}^+$ έτσι, ώστε να ισχύει $\tau(n^2)/\tau(n) = k$.*

Απόδειξη. Ας είναι k θετικός ακέραιος για τον οποίον υπάρχει $n \in \mathbb{Z}^+$ έτσι, ώστε να έχουμε $\tau(n^2)/\tau(n) = k$. Αν $n = p_1^{a_1} \cdots p_s^{a_s}$ είναι η πρωτογενής ανάλυση του n, τότε, ο ακέραιος $\tau(n^2) = (2a_1 + 1) \cdots (2a_s + 1)$, είναι περιττός και κατά συνέπεια ο k είναι

περιττός. Θα αποδείξουμε με επαγωγή ότι κάθε θετικός περιττός k γράφεται με την μορφή $k = \tau(n^2)/\tau(n)$, όπου $n \in \mathbb{Z}^+$.

Για $k = 1$, έχουμε $1 = \tau(1^2)/\tau(1)$. Υποθέτουμε ότι η προς απόδειξη πρόταση ισχύει για τους περιττούς $2l - 1$ με $l = 1, \ldots, \nu$. Θα δείξουμε ότι ισχύει και για $k = 2\nu + 1$. Γράφουμε

$$k = 2(\nu + 1) - 1 = 2^r m - 1,$$

όπου m περιττός. Καθώς $m < k$, από την υπόθεση της επαγωγής, έπεται ότι υπάρχει $n_0 \in \mathbb{Z}^+$ έτσι, ώστε να ισχύει $\tau(n_0^2)/\tau(n_0) = m$.

Ας είναι $p_0, \ldots, p_{r-1}$ διακεκριμμένοι πρώτοι οι οποίοι δεν διαιρούν τον n_0. Θέτουμε:

$$x_0 = (2^r - 1)m - 1, \quad x_i = 2^i x_0 \quad (1, \ldots, r).$$

Παρατηρούμε ότι:

$$2x_0 + 1 = x_1 + 1, \quad 2x_1 + 1 = x_2 + 1, \quad 2x_{r-1} + 1 = x_r + 1.$$

Θεωρούμε τον ακέραιο

$$n = p_0^{x_0} \cdots p_{r-1}^{x_{r-1}} n_0.$$

Τότε, έχουμε:

$$\begin{aligned}
\frac{\tau(n^2)}{\tau(n)} &= \frac{(2x_0 + 1) \cdots (2x_{r-1} + 1)}{(x_0 + 1) \cdots (x_{r-1} + 1)} \frac{\tau(n_0^2)}{\tau(n_0)} \\
&= \frac{(x_1 + 1) \cdots (x_r + 1)}{(x_0 + 1) \cdots (x_{r-1} + 1)} m \\
&= \frac{x_r + 1}{x_0 + 1} m \\
&= \frac{2^r x_0 + 1}{2^r - 1} \\
&= \frac{2^r (x_0 + 1)}{2^r - 1} - 1 \\
&= \frac{2^r (2^r - 1)m}{2^r - 1} - 1 \\
&= 2^r m - 1 = k.
\end{aligned}$$

□

Στη συνέχεια, παρατίθενται κάποιες αποδεικτικές ασκήσεις που αφορούν σε ιδιότητες και σχέσεις των βασικών πολλαπλασιαστικών συναρτήσεων τ και σ.

΄Ασκηση 3.7. *Ας είναι $n \in \mathbb{Z}^+$. Ο $\tau(n)$ είναι περιττός, αν και μόνον αν, ο n είναι τέλειο τετράγωνο.*

Απόδειξη. Ας είναι $n = m^2$, με $m \in \mathbb{Z}^+$. Αν $m = p_1^{a_1} \cdots p_s^{a_s}$ είναι η πρωτογενής ανάλυση του m, τότε η πρωτογενής ανάλυση του n είναι:

$$n = p_1^{2a_1} \cdots p_s^{2a_s}$$

και επομένως

$$\tau(n) = (2a_1 + 1)\cdots(2a_s + 1),$$

δηλαδή, ο $\tau(n)$ είναι περιττός.

Αντιστρόφως, ας είναι ο $\tau(n)$ περιττός και $n = q_1^{b_1}\cdots q_k^{b_k}$ η πρωτογενής ανάλυση του n. Τότε, έχουμε:

$$\tau(n) = (b_1 + 1)\cdots(b_k + 1).$$

Αν υπάρχει ένας τουλάχιστον b_i περιττός, τότε ο $b_i + 1$ θα είναι άρτιος και επομένως ο $\tau(n)$ θα είναι άρτιος που είναι άτοπο. Άρα, έχουμε $b_i = 2c_i$, με $c_i \in \mathbb{Z}^+$, $(i = 1, \ldots, k)$. Οπότε, ισχύει:

$$n = (q_1^{c_1}\cdots q_k^{c_k})^2.$$

Συνεπώς, ο n είναι τέλειο τετράγωνο. □

Άσκηση 3.8. *Ας είναι ακέραιος $n > 1$ και $p_1^{a_1}\cdots p_s^{a_s}$ η πρωτογενής ανάλυση του. Τότε, έχουμε:*

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right)$$

Απόδειξη. Η παραπάνω διπλή ανισότητα είναι ισοδύναμη με την σχέση:

$$1 > \frac{p_1^{a_1}\cdots p_s^{a_s}}{\sigma(p_1^{a_1})\cdots\sigma(p_s^{a_s})} > \left(\frac{p_1 - 1}{p_1}\right)\cdots\left(\frac{p_s - 1}{p_s}\right).$$

Για κάθε $i = 1, \ldots, s$ ισχύει:

$$\frac{p_i^{a_i}}{\sigma(p_i^{a_i})} = \frac{p_i^{a_i}}{1 + p_i + \cdots + p_i^{a_i}} < 1.$$

Οπότε και το γινόμενο όλων των $p_i^{a_i}/\sigma(p_i^{a_i})$ είναι μικρότερο της μονάδος και έτσι αποδεικνύεται η πρώτη ανισοτική σχέση.

Για την δεύτερη ανισοτική σχέση αρκεί να δείξουμε:

$$\frac{p_i^{a_i}}{\sigma(p_i^{a_i})} > \left(\frac{p_i - 1}{p_i}\right)$$

για κάθε $i = 1, \ldots, s$. Αναπτύσσοντας το $\sigma(p_i^{a_i})$, η παραπάνω ανίσωση γίνεται:

$$\frac{p_i^{a_i}}{1 + p_i + \cdots + p_i^{a_i}} > \frac{p_i - 1}{p_i} \iff p_i^{a_1+1} > p_i^{a_1+1} - 1$$

το οποίο προφανώς ισχύει. □

Άσκηση 3.9. *Ο $\sigma(n)$ είναι περιττός αν και μόνον αν ο n είναι τέλειο τετράγωνο ή διπλάσιο τελείου τετραγώνου.*

Απόδειξη. Διακρίνουμε δύο περιπτώσεις. Ο n να είναι άρτιος ή περιττός. Αν $n = 1$ τότε προφανώς ισχύει. Ας είναι ο n περιττός > 1 και $p_1^{a_1} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση του. Τότε, για κάθε $i = 1, \ldots, s$ έχουμε $p_i \neq 2$. Καθώς, ισχύει

$$\sigma(n) = \sigma(p_1^{a_1} \cdots p_s^{a_s}) = \sigma(p_1^{a_1}) \cdots \sigma(p_s^{a_s}) = (1 + p_1 + \cdots + p_1^{a_1}) \cdots (1 + p_s + \cdots + p_s^{a_s}).$$

Ο $\sigma(n)$ είναι περιττός, αν και μόνο αν όλοι οι παράγοντες $1+p_i+\cdots+p_i^{a_i}$ είναι περιττοί. Το άθροισμα $1 + p_i + \cdots + p_i^{a_i}$ είναι περιττός, αν και μονον αν, ο a_i είναι άρτιος (ως άθροισμα περιττού πλήθους περιττών). Σ΄ αυτή την περίπτωση, έχουμε $a_i = 2c_i$, με $c_i \in \mathbb{Z}^+$ $(i = 1, \ldots, s)$. Θέτοντας $m = p_1^{c_1} \cdots p_s^{c_s}$, παίρνουμε $n = m^2$. Έτσι, αν ο n είναι περιττός, τότε ο $\sigma(n)$ είναι περιττός αν και μόνον αν $n = m^2$, $m \in \mathbb{Z}^+$.

Ας υποθέσουμε τώρα ότι ο n είναι άρτιος και $2^{b_1} q_2^{b_2} \cdots q_t^{b_t}$ η πρωτογενής ανάλυση του, όπου $q_i > 2$ $(i = 2, \ldots, t)$. Έχουμε:

$$\begin{aligned}\sigma(n) &= \sigma(2^{b_1} q_2^{b_2} \cdots q_t^{b_t}) = \sigma(2^{b_1})\sigma(q_2^{b_2}) \cdots \sigma(q_t^{b_t}) \\ &= (1 + 2 + \cdots + 2^{b_1})(1 + q_2 + \cdots + q_2^{b_2}) \cdots (1 + q_t + \cdots + q_t^{b_t}).\end{aligned}$$

Καθως ο παράγοντας $1 + 2 + \cdots + 2^{b_1}$ είναι περιττός, έχουμε ότι ο $\sigma(n)$ είναι περιττός αν και μόνον αν οι παράγοντες $1 + q_i + \cdots + q_i^{b_i}$ $(i = 2, \ldots, t)$ είναι περιττοί το οποίο συμβαίνει αν και μόνον αν $b_i = 2d_i$ με $d_i \in \mathbb{Z}^+$ $(i = 2, \ldots, t)$. Επιπλέον, έχουμε $b_1 = 2d_1 + e$, όπου $d_1 \in \mathbb{Z}^+$ και $e = 0$ ή 1. Θέτουμε $m = 2^{d_1} q_2^{d_2} \cdots q_t^{d_t}$. Τότε, έχουμε $n = 2^e m^2$. Έτσι, αν ο n είναι άρτιος, τότε ο $\sigma(n)$ είναι περιττός αν και μόνον αν $n = m^2$ ή $n = 2m^2$, $m \in \mathbb{Z}^+$. □

΄Ασκηση 3.10. *Για κάθε $n \in \mathbb{Z}^+$ ισχύει:*

$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d) \right)^2.$$

Απόδειξη. Η συνάρτηση τ είναι πολλαπλασιαστική. Σύμφωνα με την Πρόταση 3.3, η συνάρτηση τ^3 είναι επίσης πολλαπλασιαστική. Στη συνέχεια το Πόρισμα 3.5 συνεπάγεται ότι η συνάρτηση F που ορίζεται από την σχέση

$$F(n) = \sum_{d|n} \tau(d)^3, \quad \forall\, n \in \mathbb{Z}^+,$$

είναι πολλαπλασιαστική. Από την άλλη πλευρά, το Πόρισμα 3.5 δίνει ότι η συνάρτηση g που ορίζεται από την σχέση

$$g(n) = \sum_{d|n} \tau(d), \quad \forall\, n \in \mathbb{Z}^+,$$

είναι πολλαπλασιαστική. Στη συνέχεια, από την Πρόταση 3.3 έχουμε ότι η συνάρτηση $G = g^2$ είναι πολλαπλασιαστική. Έτσι, σύμφωνα με το Πόρισμα 3.2, καθώς οι F και G είναι πολλαπλασιαστικές, για να αποδείξουμε ότι $F = G$, αρκεί να αποδείξουμε ότι για κάθε πρώτο p και κάθε θετικό ακέραιο a ισχύει $F(p^a) = G(p^a)$.

Έχουμε:

$$\begin{aligned} F(p^a) &= \sum_{d|p^a} \tau(d)^3 \\ &= \tau(1)^3 + \tau(p)^3 + \cdots + \tau(p^a)^3 \\ &= 1^3 + 2^3 + \cdots + (a+1)^3 \end{aligned}$$

και

$$\begin{aligned} G(p^a) &= \left(\sum_{d|p^a} \tau(d) \right)^2 \\ &= (\tau(1) + \tau(p) + \cdots + \tau(p^a))^2 \\ &= (1 + 2 + \cdots + (a+1))^2. \end{aligned}$$

Στη συνέχεια θα δείξουμε επαγωγικά ότι ισχύει η ισότητα:

$$1^3 + 2^3 + \cdots + a^3 = (1 + 2 + \cdots + a)^2.$$

Για $a = 1$ η σχέση προφανώς ισχύει. Υποθέτουμε ότι η παραπάνω ισότητα ισχύει για $a = k$. Θα δείξουμε ότι ισχύει για $a = k + 1$. Έχουμε:

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

Άρα, η προς απόδειξη ισότητα ισχύει και κατά συνέπεια έχουμε $F(p^a) = G(p^a)$. Επομένως $F = G$. □

3.3 Η Συνάρτηση μ του Mobious

Η συνάρτηση μ του Mobious ορίζεται ως εξής:

$$\mu(n) = \begin{cases} 1, & \text{αν } n = 1, \\ 0, & \text{αν υπάρχει πρώτος } p \text{ τέτοιος ώστε } p^2 \mid n, \\ (-1)^k, & n = p_1 p_2 \cdots p_k, \text{ όπου } p_i \neq p_j \text{ για κάθε } i \neq j. \end{cases}$$

Η συνάρτηση μ είναι πολλαπλασιαστική [13, Κεφάλαιο 3, Ενότητα 4]. Μερικές ιδιότητες της μ δίνονται στις παρακατω προτάσεις.

Πρόταση 3.6. *Για κάθε $n \in \mathbb{Z}^+$ ισχύει:*

$$\sum_{d|n} \mu(d) = \varepsilon(n)$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 4.1]. □

Πρόταση 3.7. *Για κάθε θετικό ακέραιο $n > 1$ με πρωτογενή ανάλυση $n = p_1^{a_1} \cdots p_k^{a_k}$ και κάθε $f \in \mathcal{M}$ ισχύει:*

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_k)).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 4.2]. □

Το παρακατω βασικό θεώρημα είναι γνωστό ως *τύπος αντιστροφής του Mobious.*

Θεώρημα 3.1. *Ας είναι f και g αριθμητικές συναρτήσεις. Τότε, έχουμε:*

$$g(n) = \sum_{d|n} f(d), \quad \forall\, n \in \mathbb{Z}^+$$

αν και μόνον αν ισχύει:

$$f(n) = \sum_{d|n} \mu(d) g(n/d), \quad \forall\, n \in \mathbb{Z}^+.$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Θεώρημα 4.1]. □

Πόρισμα 3.5. *Ας είναι f και g αριθμητικές συναρτήσεις τέτοιες, ώστε να ισχύει:*

$$g(n) = \sum_{d|n} f(d), \quad \forall\, n \in \mathbb{Z}^+.$$

Τότε, η συνάρτηση f είναι πολλαπλασιαστική, αν και μόνον αν, η g είναι πολλαπλασιαστική.

Μία γνωστή αριθμητική συνάρτηση είναι η συνάρτηση Λ του Mangoldt η οποία ορίζεται ως εξής:

$$\Lambda(n) = \begin{cases} \log p, & n = p^m, \text{ όπου } p \text{ πρώτος και } m \text{ θετικός ακέραιος,} \\ 0, & \text{οπουδήποτε αλλού.} \end{cases}$$

Η συνάρτηση Λ του Mangoldt είναι ιδιαιτέρως ενδιαφέρουσα, καθώς σχετίζεται με την συνάρτηση ζ του Riemann [8, Σελ.28], [3, Σελ.50].

Ασκήσεις

΄Ασκηση 3.11. *Να δειχθούν τα εξής:*

α) *Η συνάρτηση Λ του Mangoldt δεν είναι πολλαπλασιαστική.*

β) $\log n = \sum_{d|n} \Lambda(d)$.

γ) $\Lambda(d) = \sum_{d|n} \mu(d) \log(n/d) = -\sum_{d|n} \mu(d) \log(d),\ \forall n \in \mathbb{Z}^+$.

Απόδειξη. α) Από τον ορισμό της συνάρτησης Λ έχουμε $\Lambda(1) = 0$. Καθώς για κάθε πολλαπλασιαστική συνάρτηση f ισχύει $f(1) = 1$, έπεται ότι η Λ δεν είναι πολλαπλασιαστική.

β) Ας είναι $n > 1$ και $p_1^{a_1} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση του n. Έχουμε:

$$\sum_{d|n} \Lambda(d) = \sum_{0 \le b_i \le a_i} \Lambda(p_1^{b_1} \cdots p_s^{b_s}) = \sum_{b_1=1}^{a_1} \Lambda(p_1^{b_1}) + \cdots + \sum_{b_s=1}^{a_s} \Lambda(p_s^{b_s})$$

(από τον ορισμό της συνάρτησης Λ έπεται ότι όλοι οι υπόλοιποι όροι είναι μηδέν). Έτσι, προκύπτει:

$$\begin{aligned} \sum_{d|n} \Lambda(n) &= a_1 \log p_1 + \cdots + a_s \log p_s \\ &= \log p_1^{a_1} + \cdots + \log p_s^{a_s} = \log n. \end{aligned}$$

γ) Εφαρμόζοντας το Θεώρημα 3.1 στη σχέση β) παίρνουμε:

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right).$$

Εφαρμόζοντας απλές ιδιότητες λογαρίθμων, έχουμε:

$$\Lambda(n) = \sum_{d|n} \mu(d)(\log n - \log d) = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d.$$

Για $n > 1$, από την Πρόταση 3.6 έχουμε:

$$\sum_{d|n} \mu(d) = 0.$$

Έτσι, προκύπτει:

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log(d).$$

□

Στη συνέχεια θα δούμε μερικές ασκήσεις που σχετίζονται με τις ιδιότητες της συνάρτησης του Mobious.

Άσκηση 3.12. *Για κάθε $n \in \mathbb{Z}^+$ ισχύει ότι*

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

Απόδειξη. Οι αριθμοί n, $n+1$, $n+2$, $n+3$ είναι τέσσερεις διαδοχικοί ακέραιοι και επομένως ένας τουλάχιστον από αυτούς διαιρείται με το 4. Αυτός που διαιρείται με το 4, δεν είναι ελεύθερος τετραγώνου και επομένως η εικόνα του μέσω της μ είναι 0. Έτσι, έχουμε:

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

□

΄Ασκηση 3.13. *Ας είναι $n \in \mathbb{Z}^+$, $n \geq 3$. Τότε ισχύει:*

$$\sum_{k=1}^{n} \mu(k!) = 1.$$

Απόδειξη. Για κάθε $k \geq 4$, ο $k!$ διαιρείται από τον 4 και επομένως $\mu(k!) = 0$. ΄Ετσι έχουμε:

$$\sum_{k=1}^{n} \mu(k!) = \mu(1) + \mu(1 \cdot 2) + \mu(1 \cdot 2 \cdot 3) = 1 + (-1)^1 + (-1)^2 = 1$$

□

΄Ασκηση 3.14. *Ας είναι $n \in \mathbb{Z}^+$, $n \geq 2$ και r το πλήθος των πρώτων διαιρετών του n. Τότε, έχουμε:*

$$\sum_{d|n} |\mu(d)| = 2^r.$$

Απόδειξη. Ας είναι f η συνάρτηση με $f(n) = |\mu(n)|$, για κάθε $n \in \mathbb{Z}^+$. Αν $m, n \in \mathbb{Z}^+$ με $(m, n) = 1$, τότε, έχουμε:

$$|\mu(mn)| = |\mu(m)\mu(n)| = |\mu(m)||\mu(n)|.$$

Επομενως, η συνάρτηση f είναι πολλαπλασιαστική. Από το Πόρισμα 3.5 έπεται ότι η συνάρτηση F, με

$$F(n) = \sum_{d|n} f(d), \quad \forall\, n \in \mathbb{Z}^+,$$

είναι πολλαπλασιαστική. Αν p είναι πρώτος και $a \in \mathbb{Z}^+$, τότε έχουμε:

$$F(p^a) = \sum_{d|p^a} |\mu(d)| = |\mu(1)| + |\mu(p)| + |\mu(p^2)| + \cdots + |\mu(p^a)| = 2.$$

Ας είναι τώρα $n = p_1^{a_1} \cdots p_r^{a_r}$ η πρωτογενής ανάλυση. Καθώς η συνάρτηση F είναι πολλαπλασιαστική, παίρνουμε:

$$F(n) = F(p_1^{a_1}) \cdots F(p_r^{a_r}) = 2^r.$$

□

Τέλος, θα δούμε μια εφαρμογή του Θεωρήματος 3.1, δηλαδή, του τύπου της αντιστροφής του Mobious.

΄Ασκηση 3.15. *Ας είναι $q \in \mathbb{C}$ και w μία αριθμητική συνάρτηση τέτοια, ώστε να ισχύει*

$$q^n = \sum_{d|n} dw(d).$$

α) Να βρεθεί η τιμή $w(24)$ συναρτήσει του q.
β) Αν $q \in \mathbb{Z}$, τότε να δειχθεί ότι $w(24) \in \mathbb{Z}$.

Απόδειξη. α) Εφαρμόζοντας το Θεώρημα 3.1, παίρνουμε:

$$nw(n) = \sum_{d|n} q^d \mu(n/d).$$

΄Αρα, έχουμε:

$$\begin{aligned} 24w(24) &= \sum_{d|24} q^d \mu(n/d) \\ &= q\mu(24) + q^2\mu(12) + q^3\mu(8) + q^4\mu(6) + \\ &\quad q^6\mu(4) + q^8\mu(3) + q^{12}\mu(2) + q^{24}\mu(1) \\ &= q^4 - q^8 - q^{12} + q^{24}. \end{aligned}$$

Επομένως, παίρνουμε:

$$w(24) = \frac{1}{24}(q^4 - q^8 - q^{12} + q^{24}).$$

β) Ας είναι $q \in \mathbb{Z}$ και $S = q^4 - q^8 - q^{12} + q^{24}$. Θα δείξουμε ότι $24 \mid S$. Αν $3 \mid q$, τότε $3 \mid S$. Αν $3 \nmid q$, τότε $q = 3k + l$ με $l = 1$ ή 2. ΄Εχουμε:

$$q^4 = (3k + l)^4 = 3A + 1,$$

όπου A θετικός ακέραιος. Ομοίως, παίρνουμε:

$$q^8 = (3A + 1)^2 = 3B + 1, \quad q^{12} = (3A + 1)^3 = 3C + 1, \quad q^{24} = (3C + 1)^2 = 3D + 1,$$

όπου B, C, D θετικοί ακέραιοι. ΄Αρα, ισχύει $S = 3(A - B - C + D)$ και επομένως $3 \mid S$. Συνεπώς, σε κάθε περίπτωση έχουμε $3 \mid S$.

Αν $2 \mid q$, τότε $8 \mid S$. Ας είναι είναι τώρα $q = 2a + 1$. Τότε, έχουμε:

$$q^4 = (2a + 1)^4 = 8E + 1,$$

όπου E θετικός ακέραιος, απ΄ όπου παίρνουμε:

$$q^8 = (8E + 1)^2 = 8F + 1, \quad q^{12} = (8E + 1)^3 = 8G + 1, \quad q^{24} = (8G + 1)^2 = 8H + 1,$$

όπου F, G, H θετικοί ακέραιοι. Επομένως, έχουμε $S = 8(E - F - G + H)$. ΄Ετσι, ισχύει $8 \mid S$. Καθώς $(3, 8) = 1$, έπεται $24 \mid S$ και κατά συνέπεια $w(24) \in \mathbb{Z}$. □

3.4 Η Συνάρτηση ϕ του Euler

Η συνάρτηση $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$, όπου $\phi(n)$ είναι το πλήθος των θετικών διαιρετών k του n με $(k, n) = 1$, είναι γνωστή ως συνάρτηση του Euler. Το θεώρημα που ακολουθεί οφείλεται στον Gauss.

Θεώρημα 3.2. *Για κάθε $n \in \mathbb{Z}^+$ ισχύει:*

$$n = \sum_{d|n} \phi(d).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Θεώρημα 5.1] ή [12, Πρόταση 4.2.5, εδώ]. □

Η συνάρτηση ϕ είναι πολλαπλασιαστική [12, Πρόταση 4.2.6, εδώ]. Αν η πρωτογενής ανάλυση ενός θετικού ακεραίου n είναι γνωστή, τότε η τιμή $\phi(n)$ υπολογίζεται εύκολα, όπως δείχνει η παρακάτω πρόταση.

Πρόταση 3.8. *Ας είναι n ακέραιος > 1 και $n = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής του ανάλυση. Τότε, έχουμε:*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 5.1] ή [12, Πρόταση 4.2.7, εδώ]. □

Πόρισμα 3.6. *Για κάθε ακέραιο $n > 2$, ο ακέραιος $\phi(n)$ είναι άρτιος.*

Απόδειξη. Βλέπε [12, Πρόταση 4.2.8, εδώ]. □

Ασκήσεις

Αρχικά θα δούμε μερικές ασκήσεις στις οποίες ζητείται ο προσδιορισμός του συνόλου των ακεραίων οι οποίοι επαληθεύουν ορισμένες σχέσεις με την συνάρτηση ϕ.

΄Ασκηση 3.16. *Να βρεθούν όλοι οι θετικοί ακέραιοι n για τους οποίους ισχύει $\phi(n) = n/2$.*

Απόδειξη. Για $n = 1$ η σχέση δεν ισχύει. Ας είναι $n \geq 2$ τέτοιος, ώστε να ισχύει $\phi(n) = n/2$. Τότε ο n είναι άρτιος. ΄Ετσι, έχουμε $n = 2^k m$ όπου m περιττός και $k \in \mathbb{Z}^+$. Οπότε, παίρνουμε:

$$\phi(n) = \frac{n}{2} \Rightarrow \phi(2^k)\phi(m) = \frac{2^k m}{2}$$

απ΄ όπου έπεται $2^{k-1}m = 2^{k-1}\phi(m)$. ΄Αρα, έχουμε $m = \phi(m)$ και επομένως $m = 1$. Συνεπώς, $n = 2^k$. Αντίστροφα, αν $n = 2^k$, τότε $\phi(2^k) = 2^{k-1} = 2^k/2$. □

΄Ασκηση 3.17. *Να βρεθούν όλοι οι θετικοί ακέραιο n για τους οποίους ισχύει $\phi(n) = \phi(2n)$.*

Απόδειξη. Αν ο n είναι περιττός, τότε $(2, n) = 1$ και επομένως έχουμε:

$$\phi(2n) = \phi(2)\phi(n) = \phi(n).$$

Αν n είναι άρτιος, τότε $n = 2^k m$, όπου m περιττός και $k \in \mathbb{Z}^+$. ΄Ετσι, έχουμε:

$$\phi(n) = \phi(2n) \iff \phi(2^k)\phi(m) = \phi(2^{k+1})\phi(m) \iff 2^{k-1} = 2^k$$

που είναι αδύνατο. ΄Αρα, ισχύει $\phi(n) = \phi(2n)$ μόνο για κάθε περιττό θετικό ακέραιο n. □

΄Ασκηση 3.18. *Να βρεθούν όλοι οι θετικοί ακέραιοι n για τους οποίους ισχύει $\phi(n) = 16$.*

Απόδειξη. Ας είναι n με $\phi(n) = 16$ και $n = p_1^{a_1} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση του n. Τότε, έχουμε:

$$p_1^{a_1-1} \cdots p_s^{a_s-1}(p_1 - 1) \cdots (p_s - 1) = 2^4.$$

Έτσι, οι ακέραιοι $p_i - 1$ είναι κάποιοι από τους $1, 2, 4, 8, 16$ και κατά συνέπεια $p_i \in \{2, 3, 5, 17\}$ (η περίπτωση $p_i = 9$ απορίπτεται γιατί ο p_i είναι πρώτος). Άρα, έχουμε $n = 2^{a_1}3^{a_2}5^{a_3}17^{a_4}$. Αν $a_2 > 1$, τότε $3 \mid 16$ που είναι άτοπο. ;ρα $a_2 \leq 1$. Με τον ίδιο τρόπο συμπεραίνουμε ότι $a_3 \leq 1$ και $a_4 \leq 1$. Επίσης, έχουμε $a_1 \leq 5$. Διακρίνουμε τις εξής περιπτώσεις:

α) $a_1 = 0$. Τότε $n = 3^{a_2}5^{a_3}17^{a_4}$, με $a_i \leq 1$ $(i = 2, 3, 4)$. Οπότε, από την ισότητα $\phi(n) = 16$ έπεται ότι $a_2 = a_3 = 0$ και $a_4 = 1$. Άρα, $n = 17$.

β) $a_1 = 1$. Τότε $n = 2 \cdot 3^{a_2}5^{a_3}17^{a_4}$, με $a_i \leq 1$ $(i = 2, 3, 4)$. Έχουμε $\phi(n) = \phi(3^{a_2}5^{a_3}17^{a_4})$ και επομένως από την προηγούμενη περίπτωση παίρνουμε $a_2 = a_3 = 0$ και $a_4 = 1$. Έτσι, έχουμε $n = 2 \cdot 17 = 34$.

γ) $a_1 = 2$. Τότε $n = 4 \cdot 3^{a_2}5^{a_3}17^{a_4}$, με $a_i \leq 1$ $(i = 2, 3, 4)$. Από την ισότητα $\phi(n) = 16$ παίρνουμε $a_2 = 1$, $a_3 = 1$ και $a_4 = 0$. Επομένως, έχουμε $n = 60$.

δ) $a_1 = 3$. Τότε $n = 8 \cdot 3^{a_2}5^{a_3}17^{a_4}$, με $a_i \leq 1$ $(i = 2, 3, 4)$. Από την ισότητα $\phi(n) = 16$ προκύπτει $a_2 = 0$, $a_3 = 1$ και $a_4 = 0$. Συνεπώς, έχουμε $n = 40$.

ε) $a_1 = 4$. Τότε $n = 16 \cdot 3^{a_2}5^{a_3}17^{a_4}$, με $a_i \leq 1$ $(i = 2, 3, 4)$. Σ΄ αυτή την περίπτωση έχουμε $a_2 = 1$ και $a_3 = a_4 = 0$. Άρα $n = 48$.

στ) $a_1 = 5$. Τότε $n = 32 \cdot 3^{a_2}5^{a_3}17^{a_4}$, με $a_i \leq 1$ $(i = 2, 3, 4)$. Έτσι, έχουμε $a_2 = a_3 = a_4 = 0$. Άρα $n = 32$.

Συνεπώς, οι θετικοί ακέραιοι n για τους οποίους ισχύει $\phi(n) = 16$ είναι οι 17, 34, 60, 40, 48 και 32. □

Άσκηση 3.19. *Να προσδιοριστούν όλοι ακέραιοι $n \in \mathbb{Z}^+$ για τους οποίους ισχύει:*

$$\phi(3n) = \phi(4n) = \phi(6n).$$

Απόδειξη. Γράφουμε $n = 2^a3^bm$, όπου $a \geq 0$, $b \geq 0$ και $m \in \mathbb{Z}^+$ με $(m, 6) = 1$. Επομένως, έχουμε:

$$3n = 2^a3^{b+1}m, \quad 4n = 2^{a+2}3^bm, \quad 6n = 2^{a+1}3^{b+1}m.$$

Τότε:

$$\phi(3n) = \phi(2^a3^{b+1}m) = \phi(2^a)2 \cdot 3^b\phi(m),$$
$$\phi(4n) = \phi(2^{a+2}3^bm) = 2^{a+1}\phi(3^b)\phi(m),$$
$$\phi(6n) = \phi(2^{a+1}3^{b+1}m) = 2^{a+1}3^b\phi(m).$$

Έτσι, έχουμε:

$$\phi(3n) = \phi(4n) = \phi(6n) \iff \phi(2^a)2 \cdot 3^b = 2^{a+1}\phi(3^b) = 2^{a+1}3^b.$$

Ας υποθέσουμε ότι ισχύουν οι ισότητες του δεύτερου σκέλους της ισοδυναμίας. Τότε, η ισότητα $2^{a+1}\phi(3^b) = 2^{a+1}3^b$ έπεται $\phi(3^b) = 3^b$, απ΄ όπου $3^b = 1$ και επομένως $b = 0$. Η ισότητα $\phi(2^a)2 \cdot 3^b = 2^{a+1}3^b$ δίνει $\phi(2^a) = 2^a$, απ΄ όπου $2^a = 1$ και κατά συνέπεια $a = 0$. Άρα $(n, 6) = 1$. Από την άλλη πλευρά, αν $(n, 6) = 1$, τότε οι ισότητες του δεύτερου σκέλους της παραπάνω ισοδυναμίας ισχύουν. Συνεπώς, οι ζητούμενοι ακέραιοι είναι όλοι οι θετικοί ακέραιοι n με $(n, 6) = 1$. □

Στις ασκήσεις που ακολουθούν αποδεικνύονται ιδιότητες της συνάρτησης ϕ του Euler.

΄Ασκηση 3.20. *Ας είναι $n \in \mathbb{Z}^+$ και d θετικός διαιρέτης του n. Να δειχθεί ότι $\phi(d) \mid \phi(n)$.*

Απόδειξη. Ας είναι $n = p_1^{a_1} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση του n. Τότε, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $d = p_1^{b_1} \cdots p_r^{b_r}$, με $r \leq s$ και $b_i \leq a_i$ $(i = 1, \ldots, r)$. Οπότε, έχουμε:

$$\phi(n) = p_1^{a_1-1} \cdots p_s^{a_s-1}(p_1 - 1) \cdots (p_s - 1)$$

και

$$\phi(d) = p_1^{b_1-1} \cdots p_r^{b_r-1}(p_1 - 1) \cdots (p_r - 1).$$

΄Ετσι, παίρνουμε:

$$\phi(n) = \phi(d)p_1^{a_1-b_1} \cdots p_r^{a_r-b_r} p_{r+1}^{a_{r+1}} \cdots p_s^{a_s}(p_{r+1} - 1) \cdots (p_s - 1).$$

Συνεπώς, ισχύει $\phi(d) \mid \phi(n)$. □

΄Ασκηση 3.21. *Ας είναι n ακέραιος > 1. Αν $\phi(n) \mid n - 1$, τότε να δειχθεί ότι ο n είναι ελεύθερος τετραγώνου.*

Απόδειξη. Ας είναι $p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής ανάλυση του n. Αρκεί να δείξουμε ότι $a_1 = \cdots = a_k = 1$. Από την σχέση $\phi(n) \mid n - 1$, έχουμε ότι

$$p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1 - 1) \cdots (p_k - 1) \mid n - 1.$$

Αν υπάρχει i με $a_i \geq 2$, τότε $p_i \mid n - 1$. Καθώς $p_i \mid n$, παίρνουμε $p_i \mid 1$. ΄Ατοπο, άρα για κάθε $i = 1, \ldots, k$, έχουμε $a_i = 1$ και επομένως ο n είναι ελεύθερος τετραγώνου. □

΄Ασκηση 3.22. *Ας είναι n σύνθετος ακέραιος > 1. Να δειχθεί ότι ισχύει:*

$$\phi(n) \leq n - \sqrt{n}.$$

Απόδειξη. Ας είναι $n = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής ανάλυση του n. Καθώς $0 < 1 - 1/p_i < 1$ $(i = 1, \ldots, k)$, παίρνουμε:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \leq n\left(1 - \frac{1}{p_1}\right).$$

Επιπλέον, ας υποθέσουμε ότι ο p_1 είναι ο μικρότερος πρώτος διαιρέτης του n. Τότε, έχουμε $p_1 < \sqrt{n}$ και επομένως προκύπτει:

$$1 - \frac{1}{p_1} \leq 1 - \frac{1}{\sqrt{n}}.$$

΄Ετσι, παίρνουμε:

$$\phi(n) \leq n - \sqrt{n}.$$

□

΄Ασκηση 3.23. *Ας είναι n ακέραιος > 1 και S το άθροισμα των θετικών ακεραίων που είναι πρώτοι προς τον n και μικρότεροι από τον n. Να δειχθεί ότι ισχύει:*

$$S = \frac{1}{2}\, n\phi(n).$$

Απόδειξη. Ας είναι A το σύνολο όλων των θετικών ακεραίων a με $a < n$ και $(n, a) = 1$. Τότε $|A| = \phi(n)$. Αν $a \in A$, τότε $n - a < n$ και $(n - a, n) = (a, n) = 1$ και επομένως $n - a \in A$. Εύκολα βλέπουμε ότι η αντιστοιχία $a \mapsto n - a$ ορίζει μία αμφίεση του A επί του A. ΄Ετσι, όταν ο a διατρέχει το σύνολο A, ο $n - a$ διατρέχει επίσης το σύνολο A. Οπότε, έχουμε:

$$S = \sum_{a\in A} a = \sum_{a\in A} (n - a) = n\phi(n) - S,$$

απ΄ όπου έπεται $S = n\phi(n)/2$. □

Η προηγούμενη άσκηση μας δίνει να καταλάβουμε γιατί το $\phi(n)$ είναι για $n \geq 3$ είναι άρτιος. Βλέπουμε πως οι θετικοί ακέραιοι που είναι μικρότεροι από το n και είναι πρώτοι με το n εμφανίζονται σε ζεύγη, δηλαδή, a και $n - a$.

΄Ασκηση 3.24. *Ας είναι n θετικός ακέραιος. Να δειχθεί ότι ισχύει:*

$$\sum_{d|n} (-1)^{n/d}\phi(d) = \begin{cases} 0, & \text{αν ο } n \text{ είναι άρτιος,} \\ -n, & \text{αν ο } n \text{ είναι περιττός.} \end{cases}$$

Απόδειξη. Ας υποθέσουμε ότι ο n είναι περιττός. Τότε, κάθε διαιρέτης του n είναι περιττός, και επομένως το Θεώρημα 3.2 δίνει:

$$\sum_{d|n} (-1)^{n/d}\phi(d) = -\sum_{d|n} \phi(d) = -n.$$

Στη συνέχεια, ας υποθέσουμε ότι ο n είναι άρτιος. ΄Αρα, $n = 2^k m$, όπου $k \geq 1$ και m περιττός ακέραιος. Ας είναι $d_1, \ldots, d_r$ όλοι οι θετικοί διαιρέτες του m. Τότε, όλοι οι θετικοί διαιρέτες του n είναι:

$$d_1, \ldots, d_r, 2d_1, \ldots, 2d_r, \ldots, 2^k d_1, \ldots, 2^k d_r.$$

΄Εχουμε:

$$\begin{aligned}
\sum_{d|n} (-1)^{n/d}\phi(d) &= \sum_{j=0}^{k}\sum_{i=1}^{r} (-1)^{n/2^j d_i}\phi(2^j d_i) \\
&= \sum_{j=0}^{k-1}\sum_{i=1}^{r} \phi(2^j d_i) - \sum_{i=1}^{r} \phi(2^k d_i) \\
&= \sum_{j=0}^{k-1}\sum_{i=1}^{r} \phi(2^j)\phi(d_i) - \sum_{i=1}^{r} \phi(2^k)\phi(d_i) \\
&= \left(\sum_{i=1}^{r} \phi(d_i)\right)\left(\sum_{j=0}^{k-1} \phi(2^j) - \phi(2^k)\right).
\end{aligned}$$

Καθώς όμως

$$\sum_{j=0}^{k-1} \phi(2^j) - \phi(2^k) = \cancel{1} + \cancel{2} - \cancel{1} + \cancel{2^2} - \cancel{2} + \cdots + 2^{k-1} - \cancel{2^{k-2}} - 2^k + 2^{k-1} = 0,$$

παίρνουμε

$$\sum_{d|n} (-1)^{n/d} \phi(d) = 0.$$

□

3.5 Τέλειοι, Φίλοι και Κοινωνικοί Αριθμοί

Σε αυτήν την ενότητα θα δούμε τρία υποσύνολα ακεραίων αριθμών, τους τέλειους, τους φίλους και τους κοινωνικούς αριθμούς. Η μελέτη των τέλειων και των φίλων αριθμών ξεκινάει από τα αρχαία χρόνια. Στις αρχές του 20ου αιώνα ο Βέλγος μαθηματικός Paul Poulet όρισε το σύνολο των κοινωνικών αριθμών ως γενίκευση των τέλειων και φίλων αριθμών. Στις μέρες μας υπάρχουν πολλά ανοικτά ερωτήματα γύρω από τους τέλειους, φίλους και κοινωνικούς αριθμούς, όπως για παραδειγμα αν υπάρχουν άπειροι τέλειοι, φίλοι ή κοινωνικοί αριθμοί, αν υπάρχουν περιττοί τέλειοι αριθμοί, αν υπάρχουν ζεύγη φίλων αριθμών που να είναι πρώτοι μεταξύ τους και πολλά άλλα. Η ευκολία στο να καταλάβει ακόμα και ένας μαθητής γυμνασίου τη ζητούμενη εικασία καθιστά την απόδειξη των εικασιών αυτών ιδιαιτέρως ελκυστική για το ευρύ κοινό.

Ορισμός 3.4. Ας είναι n θετικός ακέραιος. Ο ακέραιος n καλείται *τέλειος*, αν ισχύει:

$$\sigma(n) = 2n.$$

Η παρακάτω πρόταση μας παρέχει μια ικανή και αναγκαία συνθήκη για να είναι ένας θετικός ακέραιος τέλειος.

Πρόταση 3.9. *Ο άρτιος θετικός ακέραιος n είναι τέλειος αν και μόνον αν ισχύει:*

$$n = 2^k(2^{k+1} - 1),$$

όπου $k \in \mathbb{Z}^+$ και ο $2^{k+1} - 1$ είναι πρώτος.

Απόδειξη. Βλέπε [13, Κεφάλαιο 3, Πρόταση 6.1] ή [12, Πρόταση 3.2.1, Πρόταση 3.2.2, εδώ] □

Ένας πρώτος της μορφής $2^k - 1$ καλείται *πρώτος του Mersenne* . Εύκολα αποδεικνύεται ότι αν $2^k - 1$ πρώτος, τότε k πρώτος. Έτσι προκύπτει το παρακάτω πόρισμα.

Πόρισμα 3.7. *Ο άρτιος θετικός ακέραιος n είναι τέλειος αν και μόνον αν ισχύει:*

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

όπου p και $2^p - 1$ είναι πρώτοι.

Ο μικρότερος τέλειος αριθμός είναι ο 6 εφόσον

$$\sigma(6) = 1 + 2 + 3 + 6 = 12,$$

ενώ ο μεγαλύτερος γνωστός μέχρι το 2016 ήταν ο $n = 2^{k-1}(2^k - 1)$ όπου $k = 74.207.281$ και έχει 44.677.235 ψηφία [6].

Ορισμός 3.5. Ας είναι $m, n \in \mathbb{Z}^+$. Οι ακέραιοι m και n καλούνται *φίλοι αριθμοί,* αν ισχύει:

$$\sigma(m) = m + n = \sigma(n).$$

Το μικρότερο ζεύγος φίλων αριθμών (m, n) είναι το $(220, 284)$ εφόσον

$$\sigma(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 + 220 = 504$$

και

$$\sigma(284) = 1 + 2 + 4 + 71 + 142 + 284 = 504.$$

Ορισμός 3.6. Αν η ακολουθία $\{n_i\}$ όπου

$$n_1 = n, \;\; n_2 = \sigma(n_1) - n_1, \;\; n_3 = \sigma(n_2) - n_2, \ldots$$

είναι περιοδική με περίοδο t τότε ο n καλείται κοινωνικός αριθμός με περίοδο t.

Εύκολα διαπιστώνουμε ότι αν η περίοδος του n είναι 2 τότε ο n είναι τέλειος αριθμός, ενώ αν η περίοδος του n είναι 3 τότε οι n_1 και n_2 είναι φίλοι αριθμοί. Για παράδειγμα ο 1.264.460 είναι ο μικρότερος κοινωνικός αριθμός με περίοδο 4, ο 12.496 είναι ο μικρότερος κοινωνικός αριθμός με περίοδο 5 και ο 21.548.919.483 είναι ο μικρότερος κοινωνικός αριθμός με περίοδο 6.

Ασκήσεις

Στις ασκήσεις που ακολουθούν, αποδεικνύονται κάποιες ιδιότητες των τέλειων και φίλων αριθμών.

΄Ασκηση 3.25. *Ας είναι n τέλειος αριθμός. Να δειχθεί ότι ισχύει:*

$$\sum_{d|n} \frac{1}{d} = 2.$$

Απόδειξη. Ας είναι $D = \{d_1, \ldots, d_{\tau(n)}\}$ το σύνολο των θετικών διαιρετών του n. Παρατηρούμε ότι αν $d \in D$, τότε ο ακέραιος n/d είναι επίσης θετικός διαιρέτης του n και επομένως $D = \{n/d_1, \ldots, n/d_{\tau(n)}\}$. ΄Ετσι, έχουμε:

$$2n = \sigma(n) = \frac{n}{d_1} + \cdots + \frac{n}{d_{\tau(n)}} = n\left(\frac{1}{d_1} + \cdots + \frac{1}{d_{\tau(n)}}\right) = n \sum_{d|n} \frac{1}{d},$$

απ΄ όπου προκύπτει:

$$\sum_{d|n} \frac{1}{d} = 2.$$

□

΄Ασκηση 3.26. *Ας είναι n και m φίλοι αριθμοί, με τον m άρτιο και τον n περιττό. Να δειχθεί ότι $n = a^2$ και $m = b^2$ ή $m = 2b^2$ για κάποια $a, b \in \mathbb{N}$.*

Απόδειξη. Εφόσον οι n και m είναι φίλοι αριθμοί, έχουμε:

$$\sigma(m) = m + n = \sigma(n).$$

Καθώς ο m είναι άρτιος και ο n περιττός συνεπάγεται ότι οι $\sigma(m)$ και $\sigma(n)$ είναι περιττοί. Από την ΄Ασκηση 3.9 έχουμε ότι οι m και n είναι είτε τέλεια τετράγωνα είτε το διπλάσιο τέλειου τετραγώνου. Εφόσον όμως το n είναι περιττός, μόνο τέλειο τετράγωνο μπορεί να είναι. □

΄Ασκηση 3.27. *Ας είναι $n = 2^{k-1}(2^k - 1)$, όπου $k > 1$ και $2^k - 1$ πρώτος, ένας άρτιος τέλειος αριθμός. Να δειχθούν τα εξής:*

α) $n = 1 + 2 + 3 + \cdots + 2^k - 1$,
β) $\phi(n) = 2^{k-1}(2^{k-1} - 1)$,
γ) $\gamma(n) = n^k$.

Απόδειξη. α) Εφαρμόζοντας τον τύπο αθροίσματος αριθμητικής προόδου για τους $2^k - 1$ πρώτους όρους με πρώτο όρο το 1 και διαφορά προόδου το 1, έχουμε:

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

β) Καθώς ο $2^k - 1$ είναι περιττός, θα είναι πρώτος με τον 2^{k-1}. Καθώς ο $2^k - 1$ είναι πρώτος, έχουμε $\phi(2^k - 1) = 2^k - 2$. ΄Ετσι, παίρνουμε:

$$\phi(n) = \phi(2^{k-1}(2^k - 1)) = \phi(2^{k-1})\phi(2^k - 1) = 2^{k-2}(2^k - 2) = 2^{k-1}(2^{k-1} - 1).$$

γ) Από την ΄Ασκηση 3.2 έχουμε ότι $\gamma(n) = n^{\tau(n)/2}$. Από την άλλη πλευρά, καθώς η συνάρτηση τ είναι πολλαπλασιαστική και ο $2^k - 1$ πρώτος, παίρνουμε:

$$\tau(n) = \tau(2^k - 1)\tau(2^{k-1}) = 2(k - 1 + 1) = 2k.$$

Επομένως, $\gamma(n) = n^k$. □

΄Οπως αναφέρθηκε στην αρχή της ενότητας ένα από τα άλυτα προβλήματα της Θεωρίας Αριθμών που σχετίζονται με τους τέλειους αριθμούς είναι η ύπαρξη των περιττών τέλειων αριθμοί. Καθώς το ερώτημα αυτό παραμένει ακόμη αναπάντητο, πολλοί ερευνητές ασχολήθηκαν με την μορφή που θα πρέπει να έχει ένας περιττός πρώτος. Το πρώτο σημαντικό αποτέλεσμα προέρχεται από τον Euler.

΄Ασκηση 3.28. *Ας είναι n περιττός τέλειος αριθμός με πρωτογενή ανάλυση $n = p_1^{a_1} \cdots p_k^{a_k}$. Να δειχθεί ότι υπάρχει δείκτης i με $a_i = 4b + 1$, όπου $k \in \mathbb{Z}^+$, και οι a_j $(j = 1, \ldots, k,\ j \neq i)$ είναι όλοι άρτιοι. Επίσης, έχουμε $p_i = 4A + 1$, με $A \in \mathbb{Z}^+$.*

Απόδειξη. Καθώς ο n είναι τέλειος, ισχύει $\sigma(n) = 2n$, απ΄ όπου έχουμε:

$$\prod_{i=1}^{k}(1 + p_i + \cdots + p_i^{a_i}) = 2\prod_{i=1}^{k} p_i^{a_i}.$$

Ο n είναι περιττός και επομένως $p_i \neq 2$ $(i = 1, \ldots)$. Η μοναδικότητα της γραφής ενός θετικού ακεραίου σε γινόμενο πρώτων συνεπάγεται ότι υπάρχει δείκτης i έτσι ώστε ο ακέραιος $1 + p_i + \cdots + p_i^{a_i}$ να διαιρείται ακριβώς από τον 2 και οι $1 + p_j + \cdots + p_j^{a_j}$ $(j = 1, \ldots, k,\ j \neq i)$ είναι όλοι περιττοί.

Ένα άθροισμα της μορφής $1 + p_i + \cdots + p_i^m$ είναι άρτιος ακέραιος αν και μόνον αν ο εκθέτης m είναι περιττός. Έτσι, έχουμε $a_i = 2b + 1$, όπου $b \in \mathbb{Z}^+$, και όλοι οι a_j $(j = 1, \ldots, k,\ j \neq i)$ είναι άρτιοι.

Ένας πρώτος $p > 2$ είναι της μορφής $4k + 1$ ή $4k - 1$. Ας υποθέσουμε ότι έχουμε $p_i = 4k - 1$. Αν t είναι θετικός ακέραιος, τότε έχουμε $p_i^t = 4A_t + e_t$, όπου $A_t \in \mathbb{Z}^+$, $e_t = 1$ αν t είναι άρτιος και $e_t = -1$, διαφορετικά. Οπότε, παίρνουμε:

$$1 + p_i + \cdots + p_i^{a_i} = 1 + 4A_1 - 1 + 4A_2 + 1 \cdots + 4A_{a_i} - 1 = 4(A_1 + A_2 + \cdots + A_{a_i})$$

που είναι άτοπο, γιατί ο $1 + p_i + \cdots + p_i^{a_i}$ διαιρείται ακριβώς με τον 2. Άρα, έχουμε $p_i = 4A + 1$, με $A \in \mathbb{Z}^+$.

Τέλος, θα δείξουμε ότι ο a_i είναι της μορφής $4k + 1$. Πρώτα παρατηρούμε ότι αν t είναι θετικός ακέραιος, τότε έχουμε $p_i^t = 4B_t + 1$, με $B_t \in \mathbb{Z}^+$. Θέτουμε $B = B_1 + \cdots + B_{a_i}$ και θεωρούμε το άθροισμα:

$$1 + p_i + \cdots + p_i^{a_i} = 4B + a_i + 1 = 4B + 2b + 2.$$

Αν $b = 2c + 1$, με $c \in \mathbb{Z}^+$, τότε ισχύει

$$1 + p_i + \cdots + p_i^{a_i} = 4B + 4c + 4$$

που είναι άτοπο. Άρα, έχουμε $b = 2c$ και επομένως $a_i = 4b + 1$. □

Σύμφωνα με την παραπάνω άσκηση, αν n είναι περιττός τέλειος αριθμός, τότε $n = p^r a^2$, όπου p πρώτος, $r, a \in \mathbb{Z}^+$ με $(p, a) = 1$ και $p \equiv r \equiv 1 \pmod 4$. Ο παράγοντας p^r αναφέρεται συχνά στην βιβλιογραφία ως *παράγοντας του Euler του* n.

Άσκηση 3.29. *Να δειχθεί ότι αν n είναι περιττός τέλειος αριθμός, τότε ο n έχει τουλάχιστον τρεις πρώτους διαφορετικούς διαιρέτες.*

Απόδειξη. Αρκεί να δείξουμε ότι δεν υπάρχουν περιττοί τέλειοι αριθμοί με ένα ή δύο πρώτους διαιρέτες.

Ας είναι n της μορφής p^r όπου p περιττός πρώτος και $r \in \mathbb{Z}^+$. Ισχύει ότι

$$\sigma(n) = \sigma(p^r) = \frac{p^{r+1} - 1}{p - 1} < \frac{p^{r+1}}{p - 1} = \frac{np}{p - 1} = \frac{n}{1 - \frac{1}{p}}.$$

Καθώς $p \geq 3$ έχουμε ότι

$$1 - \frac{1}{p} \geq \frac{2}{3}.$$

Οπότε,

$$\sigma(n) < \frac{n}{\frac{2}{3}} = \frac{3n}{2} < 2n,$$

το οποίο είναι αδύνατο, καθώς ο n ως τέλειος ικανοποιεί την ισότητα $\sigma(n) = 2n$.

Ας είναι n της μορφής $p^r q^s$ όπου p, q διαφορετικοί περιττοί πρώτοι και $r, s \in \mathbb{Z}^+$. Ισχύει:

$$\sigma(n) = \sigma(p^r q^s) = \frac{p^{r+1}-1}{p-1}\frac{q^{s+1}-1}{q-1} < \frac{p^{r+1}q^{s+1}}{(p-1)(q-1)} = \frac{npq}{(p-1)(q-1)}.$$

Έτσι, έχουμε:

$$\sigma(n) < \frac{n}{\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)}.$$

Καθώς οι p και q είναι διαφορετικοί περιττοί πρώτοι, ο ένας θα είναι μεγαλύτερος ή ισος με 3 και ο άλλος θα είναι μεγαλύτερος ή ισος με 5. Οπότε, ισχύει:

$$\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) \geq \frac{2}{3}\cdot\frac{4}{5}.$$

Τότε, παίρνουμε:

$$\sigma(n) < \frac{n}{\frac{2}{3}\cdot\frac{4}{5}} = \frac{15n}{8} < 2n,$$

το οποίο, όπως και στην προηγούμενη περίπτωση, είναι αδύνατο. □

3.6 Συνδυαστικές Ασκήσεις

Οι πρώτες δύο ασκήσεις συνδυάζουν βασικές πολλαπλασιαστικές συναρτήσεις και εξάγουν ενδιαφέροντα αποτελέσματα.

Άσκηση 3.30. *Ας είναι n θετικός ακέραιος ≥ 2 και $n = p_1^{a_1}\cdots p_r^{a_r}$ η πρωτογενής μορφή του. Να δειχθεί ότι ισχύουν οι εξής σχέσεις:*

$$\sum_{d|n}\frac{\mu^2(d)}{\tau(d)} = \frac{3^r}{2^r} \quad \text{και} \quad \sum_{d|n}\frac{\mu^2(d)}{\sigma(d)} = \prod_{i=1}^{r}\frac{p_i+2}{p_i+1}.$$

Απόδειξη. Η συνάρτηση $f = \mu/\tau$ είναι πολλαπλασιαστική, ως πηλίκο πολλαπλασιαστικών συναρτήσεων. Έτσι, η Πρόταση 3.7 δίνει:

$$\sum_{d|n}\frac{\mu^2(d)}{\tau(d)} = \sum_{d|n}\mu(d)f(d) = \prod_{i=1}^{r}(1-f(p_i)).$$

Επιπλέον, έχουμε:

$$1-f(p_i) = 1-\frac{\mu(p_i)}{\tau(p_i)} = 1-\frac{-1}{2} = \frac{3}{2}.$$

Συνδυάζοντας, τις δύο προηγούμενες ισότητες, παίρνουμε:

$$\sum_{d|n}\frac{\mu^2(d)}{\tau(d)} = \frac{3^r}{2^r}.$$

Η συνάρτηση $g = \mu/\sigma$ είναι επίσης πολλαπλασιαστική, ως πηλίκο πολλαπλασιαστικών συναρτήσεων. Επομένως, από την Πρόταση 3.7 έχουμε:

$$\sum_{d|n} \frac{\mu^2(d)}{\sigma(d)} = \sum_{d|n} \mu(d)g(d) = \prod_{i=1}^{r}(1 - g(p_i)).$$

Επίσης, ισχύει:

$$1 - g(p_i) = 1 - \frac{\mu(p_i)}{\sigma(p_i)} = 1 - \frac{-1}{1+p_i} = \frac{p_i+2}{1+p_i}.$$

Συνδυάζοντας τις παραπάνω δύο ισότητες, προκύπτει:

$$\sum_{d|n} \frac{\mu^2(d)}{\sigma(d)} = \prod_{i=1}^{r} \frac{p_i+2}{p_i+1}.$$

□

΄Ασκηση 3.31. *Ας είναι n ακέραιος ≥ 2 ελεύθερος τετραγώνου. Να δειχθεί ότι για κάθε ακέραιο $k \geq 2$ ισχύει:*

$$\sum_{d|n} \sigma(d^{k-1})\phi(d) = n^k.$$

Απόδειξη. Θεωρούμε την αριθμητική συνάρτηση f, με $f(n) = \sigma(n^{k-1})$, $\forall\ n \in \mathbb{Z}^+$. ΄Εχουμε $f(1) = \sigma(1) = 1 \neq 0$. Επιπλέον, για κάθε ζεύγος θετικών ακεραίων m, n με $(m,n) = 1$, παίρνουμε:

$$f(mn) = \sigma((mn)^{k-1}) = \sigma(m^{k-1})\sigma(n^{k-1}) = f(m)f(n)$$

γιατί η συνάρτηση σ είναι πολλαπλασιαστική και $(m^{k-1}, n^{k-1}) = 1$. ΄Αρα, η συνάρτηση f είναι πολλαπλασιαστική. Οπότε, σύμφωνα με την Πρόταση 3.3, η συνάρτηση $f\phi$ είναι πολλαπλασιαστική. ΄Ετσι, από το Πόρισμα 3.5 έπεται ότι η συνάρτηση F, με

$$F(n) = \sum_{d|n} \sigma(d^{k-1})\phi(d), \quad \forall\ n \in \mathbb{Z}^+,$$

είναι πολλαπλασιαστική.

Ας υποθέσουμε ότι ο ακέραιος $n \geq 2$ είναι ελεύθερος τετραγώνου. Τότε, $n = p_1 \cdots p_r$, όπου $p_1, \ldots, p_r$ είναι διαφορετικοί πρώτοι. Τότε, έχουμε:

$$F(p_i) = \sum_{d|p_i} \sigma(d^{k-1})\phi(d) = 1 + \sigma(p_i^{k-1})\phi(p_i) = 1 + (1 + p_i + \cdots + p_i^{k-1})(p_i - 1) = p_i^k.$$

΄Ετσι, παίρνουμε:

$$F(n) = F(p_1)\cdots F(p_r) = (p_1 \cdots p_r)^k = n^k.$$

□

Στη συνέχεια, θα αντιμετωπίσουμε κάποιες ασκήσεις στις οποίες ζητείται να αποδειχθεί η ισότητα δύο συναρτήσεων που προκύπτουν από βασικές πολλαπλασιαστικές συναρτήσεις. Σ΄ αυτές τις ασκήσεις αποδεικνύουμε συνήθως ότι οι δύο παραστάσεις είναι πολλαπλασιαστικές συναρτήσεις, κατόπιν αποδεικνύουμε ότι οι τιμές των δύο συναρτήσεων ταυτίζονται στις δυνάμεις των πρώτων και στη συνέχεια το Πόρισμα 3.2 δίνει το αποτέλεσμα. Οι παρακάτω δύο ασκήσεις είναι τέτοιου τύπου.

΄Ασκηση 3.32. *Να δειχθεί ότι για κάθε $n \in \mathbb{Z}^+$ ισχύει:*

$$\sum_{d|n} \frac{\mu(d)^2}{\phi(d)} = \frac{n}{\phi(n)}.$$

Απόδειξη. Οι συναρτήσεις μ και ϕ είναι πολλαπλασιαστικές. Από την Πρόταση 3.3 έπεται ότι η συνάρτηση μ^2 είναι πολλαπλασιαστική και κατόπιν η συνάρτηση $f = \mu^2/\phi$ είναι πολλαπλασιαστική. Στη συνέχεια, από το Πόρισμα 3.4 έχουμε ότι η συνάρτηση F που ορίζεται από την σχέση

$$F(n) = \sum_{d|n} f(d), \quad \forall\, n \in \mathbb{Z}^+,$$

είναι πολλαπλασιαστική. Από την άλλη πλευρά, σύμφωνα με την Πρόταση 3.3, η συνάρτηση G με $G(n) = n/\phi(n)$, $\forall\, n \in \mathbb{Z}^+$, είναι πολλαπλασιαστική ως πηλίκο της ταυτοτικής συνάρτησης και της ϕ.

Ας είναι p πρώτος και $a \in \mathbb{Z}^+$. Τότε, έχουμε:

$$F(p^a) = \sum_{d|p^a} \frac{\mu(d)^2}{\phi(d)} = 1 + \frac{1}{p-1} = \frac{p}{p-1}$$

και

$$G(p^a) = \frac{p^a}{p^{a-1}(p-1)} = \frac{p}{p-1}.$$

΄Αρα, ισχύει $F(p^a) = G(p^a)$ για κάθε πρώτο p και $a \in \mathbb{Z}^+$. ΄Ετσι, από το Πόρισμα 3.2 παίρνουμε το αποτέλεσμα. □

΄Ασκηση 3.33. *Να δειχθεί ότι για κάθε $n \in \mathbb{Z}^+$ ισχύει:*

$$\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d}\tau(d) \quad \text{και} \quad \sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d).$$

Απόδειξη. Θέτουμε:

$$F(n) = \sum_{d|n} \sigma(d) \quad \text{και} \quad G(n) = \sum_{d|n} \frac{n}{d}\tau(d).$$

Θα δείξουμε ότι $F(n) = G(n)$. Η συναρτηση σ είναι πολλαπλασιαστική και επομένως, σύμφωνα με το Πόρισμα 3.5, έχουμε ότι η F είναι επίσης πολλαπλασιαστική. Από την άλλη πλευρά, έχουμε $G(n) = i * \tau$. Καθώς η G είναι το ενελικτικό γινόμενο των

πολλαπλασιαστικών συναρτήσεων i και τ, από την Πρόταση 3.4, έχουμε ότι η G είναι πολλαπλασιαστική συνάρτηση. Ας είναι p πρώτος και a θετικός ακέραιος. Τότε, έχουμε:

$$\begin{aligned} F(p^a) &= \sum_{d|p^a} \sigma(d) \\ &= \sigma(1) + \sigma(p) + \sigma(p^2) + \cdots + \sigma(p^a) \\ &= 1 + (1+p) + (1+p+p^2) + \cdots + (1+p+\cdots+p^a) \\ &= (a+1) + ap + (a-1)p^2 + \cdots + p^a \end{aligned}$$

και

$$G(p^a) = \sum_{d|p^a} \frac{p^a}{d}\tau(d) = p^a + 2p^{a-1} + \cdots + ap + (a+1).$$

Άρα, για κάθε πρώτο p και $a \in \mathbb{Z}^+$, ισχύει $F(p^a) = G(p^a)$. Έτσι, το Πόρισμα 3.2 δίνει $F(n) = G(n)$.

Θέτουμε:

$$F(n) = \sum_{d|n} \frac{n}{d}\sigma(d) \quad \text{και} \quad G(n) = \sum_{d|n} d\tau(d).$$

Έχουμε $F = i * \sigma$ και επομένως η F είναι πολλαπλασιαστική συνάρτηση ως ενελικτικό γινόμενο των i και σ. Επιπλέον, η συνάρτηση $i\tau$ είναι πολλαπλασιαστική, ως (συνηθισμένο) γινόμενο των πολλαπλασιαστικών συναρτήσεων i και τ, και επομένως η G είναι πολλαπλασιαστική συνάρτηση. Ας είναι p πρώτος και a θετικός ακέραιος. Τότε, έχουμε:

$$\begin{aligned} F(p^a) &= \sum_{d|p^a} \frac{p^a}{d}\sigma(d) \\ &= p^a\sigma(1) + p^{a-1}\sigma(p) + p^{a-2}\sigma(p^2) + \cdots + \sigma(p^a) \\ &= p^a + p^{a-1}(1+p) + p^{a-2}(1+p+p^2) + \cdots + (1+p+\cdots+p^a) \\ &= (a+1)p^a + ap^{a-1} + (a-1)p^{a-2} + \cdots + 1 \end{aligned}$$

και

$$G(p^a) = \sum_{d|p^a} d\tau(d) = 1 + 2p + \cdots + p^{a-1}a + p^a(a+1).$$

Άρα, για κάθε πρώτο p και $a \in \mathbb{Z}^+$, έχουμε $F(p^a) = G(p^a)$. Επομένως, το Πόρισμα 3.2 δίνει $F(n) = G(n)$. □

Άσκηση 3.34 (American Mathematical Monthly, E3101 [4])**.** *Ας είναι n ακέραιος > 1. Να δειχθεί ότι το πλήθος των λύσεων x της εξίσωσης $\tau(nx) = n$ είναι 1 αν $n = 4$, $t!$ αν ο n είναι γινόμενο t διακεκριμμένων πρώτων και άπειρο σε οποιαδήποτε άλλη περίπτωση.*

Απόδειξη. Ας είναι $n = p_1^{s_1} \cdots p_t^{s_t}$ η πρωτογενής ανάλυση του n. Γράφουμε:

$$x = p_1^{r_1} \cdots p_t^{r_t} q_1^{u_1} \cdots q_k^{u_k},$$

όπου $q_1, \ldots, q_k$ διακεκριμμένοι πρώτοι διαφορετιοί από τους $p_1, \ldots, p_t$ και $r_i \geq 0$ $(i = 1, \ldots, t)$, $u_i \geq 0$ $(i = 1, \ldots, k)$. Τότε, έχουμε:

$$\tau(nx) = \prod_{i=1}^{t}(r_i + s_i + 1) \prod_{i=1}^{k}(u_i + 1).$$

Διακρίνουμε τρεις περιπτώσεις. Η πρώτη είναι $s_1 = \cdots s_t = 1$. Τότε, έχουμε:

$$\tau(nx) = n \iff p_1 \cdots p_t = \prod_{i=1}^{t}(r_i + 2) \prod_{i=1}^{k}(u_i + 1).$$

Καθώς το πλήθος των φυσικών r_i είναι t και $r_i + 2 \geq 2$, για κάθε δείκτη i υπάρχει δείκτης j έτσι, ώστε $r_i + 2 = p_j$ και $u_i = 0$ $(i = 1, \ldots, k)$. Τπάρχουν $t!$ τρόποι για να διαλέξουμε τους φυσικούς r_i και επομένως το πλήθος των λύσεων της εξίσωσης $\tau(nx) = n$ είναι $t!$.

Η δεύτερη περίπτωση είναι $n = 4$, δηλαδή $t = 1$, $p_1 = 2$, $s_1 = 2$. Τότε, έχουμε:

$$\tau(4x) = 4 \iff (3 + r_1) \prod_{i=1}^{k}(u_i + 1) = 4 \iff r_1 = 1,\ u_i = 0\,(i = 1, \ldots, k).$$

΄Αρα, η μοναδική λύση είναι $x = 2$.

Η τρίτη περίπτωση είναι $n > 4$ και υπάρχει πρώτος p με $p^2 \mid n$. Ας είναι $p = p_1$. Διαλέγουμε για q_1 έναν οποιοδήποτε πρώτο διαφορετικό από τους $p_1, \ldots, p_t$. Αν $n = 4p_2 \cdots p_t$ με $t \geq 2$, τότε παίρνουμε $r_1 = p_2 - 3$, $r_2 = 0$, $r_i = p_i - 2$ $(i = 3, \ldots, t)$ και $u_1 = 1$. Τέλος, αν έχουμε $p_1 \geq 3$ και $s_1 \geq 2$ ή $p_1 = 2$ και $s_1 \geq 3$, τότε παίρνουμε $r_1 = p_1^{s_1 - 1} - s_1 - 1$, $r_i = p_i^{s_i} - s_i - 1$ $(i = 2, \ldots, t)$ και $u_1 = p_1 - 1$. □

΄Ασκηση 3.35 (American Mathematical Monthly, E3398 [10]). *Να βρεθούν όλα τα ζεύγη θετικών ακεραίων m και n τα οποία είναι τέτοια, ώστε να ισχύουν οι σχέσεις $\phi(m) \mid n$ και $\phi(n) \mid m$.*

Απόδειξη. Θα καλούμε ένα ζεύγος θετικών ακεραίων m, n πρωτογενές, αν ο μέγιστος κοινός διαιρέτης τους d είναι ελεύθερος τετραγώνου. Κατ΄ αρχάς θα δείξουμε ότι υπάρχουν ακριβώς 11 πρωτογενή ζεύγη ακεραίων τα οποία έχουν την ιδιότητα της εκφώνησης, τα εξής:

$$(1,1), (1,2), (2,2), (2,3), (2,4), (2,6), (4,6), (4,10), (6,6), (6,14), (6,18).$$

Ας είναι m, n ένα πρωτογενές ζεύγος με την παραπάνω ιδιότητα. Αν $m = 2^r$, τότε ο ακέραιος $\phi(m) = 2^{r-1}$ διαιρεί τον n. Επειδή ο d είναι ελεύθερος τετραγώνου, έχουμε $4 \nmid d$ και επομένως $r \leq 2$. ΄Ετσι, από την σχέση $\phi(n) \mid 2^r$, $r = 1, 2$, έχουμε ότι οι m, n αποτελούν ένα από τα οκτώ πρώτα ζεύγη της παραπάνω λίστας.

Ας θεωρήσουμε στη συνέχεια ότι αμφότεροι οι αριθμοί m και n έχουν περιττούς πρώτους διαιρέτες. Τότε, οι ακέραιοι $\phi(m)$ και $\phi(n)$ είναι άρτιοι, και καθώς έχουμε $\phi(m) \mid n$ και $\phi(n) \mid m$, έπεται ότι οι m και n είναι άρτιοι. Αν $4 \mid m$, τότε, καθώς ο m έχει ένα περιττό πρώτο διαιρέτη, έχουμε $4 \mid \phi(m)$ και επομένως $4 \mid n$. ΄Αρα, $4 \mid d$ που είναι άτοπο. Συνεπώς, ισχύει $4 \nmid m$. ΄Ομοια έχουμε $4 \nmid n$. Αν ο m έχει δύο διαφορετικούς

περιττούς πρώτους διαιρέτες p και q, τότε $4 \mid \phi(m)$ και επομένως $4 \mid n$ που είναι άτοπο. Άρα, ο m δεν έχει δύο διαφορετικούς περιττούς πρώτους παράγοντες. Το ίδιο ισχύει και για τον n. Επομένως, έχουμε $m = 2p^r$ και $n = 2q^s$, όπου p και q περιττοί πρώτοι και $r \geq 1$, $s \geq 1$.

Μπορούμε να υποθέσουμε ότι $p \leq q$. Τότε, από τις σχέσεις $\phi(m) \mid n$ και $\phi(m) = p^{r-1}(p-1)$, έχουμε $p^{r-1}(p-1) \mid 2q^s$. Καθώς $p - 1 < q$, έχουμε $p - 1 \nmid q$ και επομένως $p - 1 \mid 2$, απ' όπου $p = 3$. Αν $q = 3$, τότε, επειδή ο d είναι ελεύθερος τετραγώνου, έχουμε $r = 1$ ή $s = 1$. Ας είναι $r = 1$. Τότε $s = 1$ ή 2. Έτσι, παίρνουμε τα ζεύγη $(6, 6)$ και $(6, 18)$ της παραπάνω λίστας. Στη συνέχεια, υποθέτουμε ότι $q > 3$. Τότε, έχουμε τις σχέσεις $3^{r-1}2 \mid 2q^s$ και $q^{s-1}(q-1) \mid 2 \cdot 3^r$. Αν $r > 1$, τότε από την πρώτη σχέση έπεται $q = 3$ που είναι άτοπο. Άρα $r = 1$. Όμοια, αν $s > 1$, τότε από την δεύτερη σχέση έπεται $q = 3$ που είναι άτοπο. Οπότε $s = 1$ και έχουμε $q - 1 \mid 6$ με $q > 3$. Άρα, $q = 7$ και έτσι προκύπτει το ζεύγος $(6, 14)$ της παραπάνω λίστας.

Τέλος, θα δείξουμε ότι τα ζεύγη με την επιθυμητή ιδιότητα προκύπτουν από τα 11 ζεύγη της παραπάνω λίστας. Παρατηρούμε ότι αν p είναι πρώτος διαιρέτης του θετικού ακεραίου n, τότε ισχύει $\phi(pn) = p\phi(n)$. Έτσι, ένα ζεύγος θετικών ακεραίων m, n το οποίο έχει ένα κοινό πρώτο διαιρέτη p, έχει την επιθυμητή ιδιότητα, αν και μόνον αν, το ζεύγος pm, pn την έχει. Συνεπώς, τα ζεύγη της λίστας

$$(2, 2), (2, 4), (2, 6), (4, 6), (4, 10), (6, 6), (6, 14), (6, 18).$$

παράγουν τις οικογένειες ζευγών

$$(2^{r+1}, 2^{r+1}), (2^{r+1}, 2^{r+2}), (2^{r+1}, 2^{r+1}3), (2^{r+2}, 2^{r+1}3), (2^{r+2}, 2^{r+1}5),$$

$$(2^{r+1}3^{s+1}, 2^{r+1}3^{s+1}), (2^{r+1}3, 2^{r+1}7), (2^{r+1}3^{s+1}, 2^{r+1}3^{s+2}),$$

όπου r και s είναι φυσικοί. □

Άσκηση 3.36 (American Mathematical Monthly, E3211 [11])**.** *Ας είναι k θετικός ακέραιος. Συμβολίζουμε με $\omega(k)$ το πλήθος των διαφορετικών πρώτων που διαιρούν τον k. Να εκφραστεί το άθροισμα*

$$\alpha(n) = \sum_{i=1}^{n} 2^{\omega((i,n))}$$

(όπου (i, n) είναι ο μέγιστος κοινός διαιρέτης των i και n) με όρους της πρωτογενούς ανάλυσης του n.

Απόδειξη. Θέτουμε $f(n) = 2^{\omega(n)}$. Η συνάρτηση f είναι πολλαπλασιαστική. Πράγματι, ας είναι a, b ακέραιοι πρώτοι μεταξύ τους και $a = p_1^{a_1} \cdots p_m^{a_m}$, $b = q_1^{b_1} \cdots q_n^{b_n}$ οι πρωτογενείς τους αναλύσεις. Τότε, έχουμε

$$ab = p_1^{a_1} \cdots p_m^{a_m} q_1^{b_1} \cdots q_n^{b_n}$$

και, επειδή $(a, b) = 1$, οι πρώτοι $p_1, \ldots, p_m, q_1, \ldots, q_n$ είναι διαφορετικοί. Άρα, έχουμε $\omega(ab) = \omega(a) + \omega(b)$ και κατά συνέπεια $f(ab) = f(a)f(b)$. Άρα, η συνάρτηση f είναι πολλαπλασιαστική.

Έχουμε:

$$\begin{aligned}\alpha(n) &= \sum_{i=1}^{n} f((i,n)) \\ &= \sum_{d|n}\Big(\sum_{\substack{1\le i\le n\\(i,n)=d}} 1\Big) f(d) \\ &= \sum_{d|n} f(d)\Big(\sum_{\substack{1\le k\le n/d\\(k,n/d)=1}} 1\Big) \\ &= \sum_{d|n} f(d)\phi(n/d) \\ &= (f*\phi)(n).\end{aligned}$$

Καθώς οι συναρτήσεις f και ϕ είναι πολλαπλασιαστικές, έπεται ότι και η $\alpha(n)$ είναι επίσης πολλαπλασιαστική. Έτσι, αν n είναι θετικός ακέραιος με πρωτογενή ανάλυση $a = p_1^{a_1}\cdots p_m^{a_m}$, τότε έχουμε:

$$\alpha(n) = \prod_{i=1}^{m} \alpha(p_i^{a_i}).$$

Επίσης, για $n = p^c$, όπου p πρώτος και c θετικός ακέραιος, ισχύει:

$$\alpha(p^c) = (f*\phi)(p^c) = \sum_{d|p^c} f(d)\phi(n/d) = 2^0\phi(p^c) + 2\phi(p^{c-1}) + \cdots + 2\phi(p) + 2.$$

Από το Θεώρημα 3.2, παίρνουμε:

$$\phi(p^{c-1}) + \cdots + \phi(p) + 1 = p^{c-1}.$$

Από τις δύο παραπάνω ισότητες προκύπτει:

$$\alpha(p^c) = \phi(p^c) + 2p^{c-1} = p^c - p^{c-1} + 2p^{c-1} = p^c + p^{c-1} = p^c\left(1 + \frac{1}{p}\right).$$

Επομένως, έχουμε:

$$\alpha(n) = \prod_{i=1}^{m} p_i^{a_i}\left(1 + \frac{1}{p_i}\right) = n\prod_{i=1}^{m}\left(1 + \frac{1}{p_i}\right).$$

□

Άσκηση 3.37 (American Mathematical Monthly, E2985 [5])**.** *Να δειχθεί ότι αν $x \in \mathbb{R}$ με $0 < x < 1$, τότε ισχύει:*

$$\prod_{l=0}^{\infty}\left(\frac{1+x^{2l+1}}{1-x^{2l+1}}\right)^{\phi(2l+1)/(2l+1)} = \exp\left(\frac{2x}{1-x^2}\right).$$

Απόδειξη. Θέτουμε:

$$F(x) = \prod_{l=0}^{\infty} \left(\frac{1+x^{2l+1}}{1-x^{2l+1}} \right)^{\phi(2l+1)/(2l+1)}.$$

Τότε, έχουμε:

$$\log F(x) = \sum_{l=0}^{\infty} \frac{\phi(2l+1)}{2l+1} \log \frac{1+x^{2l+1}}{1-x^{2l+1}}.$$

Καθώς ισχύει

$$\log(1 \pm x^(2l+1)) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(\pm x^{2l+1})^n}{n},$$

παίρνουμε:

$$\begin{aligned}
\log F(x) &= \sum_{l=0}^{\infty} \frac{\phi(2l+1)}{2l+1} \left(\sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^{(2l+1)n}}{n} - \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(-x^{(2l+1)})^n}{n} \right) \\
&= 2 \sum_{l=0}^{\infty} \frac{\phi(2l+1)}{2l+1} \sum_{m=0}^{\infty} \frac{x^{(2l+1)(2m+1)}}{2m+1} \\
&= 2 \sum_{l=0}^{\infty} \sum_{m=0}^{\infty} \phi(2l+1) \frac{x^{(2l+1)(2m+1)}}{(2l+1)(2m+1)} \\
&= 2 \sum_{l=0}^{\infty} \left(\sum_{d|2l+1} \phi(d) \right) \frac{x^{2l+1}}{2l+1}.
\end{aligned}$$

Από το Θεώρημα 3.2, έπεται:

$$\sum_{d|2l+1} \phi(d) = 2l+1.$$

Έτσι, προκύπτει:

$$\log F(x) = 2 \sum_{l=0}^{\infty} x^{2l+1}.$$

Από την άλλη πλευρά, έχουμε:

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} x^{2l+1} + \sum_{m=0}^{\infty} x^{2m} = \sum_{n=0}^{\infty} x^{2l+1} + \frac{1}{1-x^2}.$$

Επομένως, ισχύει:

$$\sum_{n=0}^{\infty} x^{2l+1} = \frac{1}{1-x} - \frac{1}{1-x^2} = \frac{x}{1-x^2}.$$

Συνεπώς, παίρνουμε:

$$\log F(x) = \frac{2x}{1-x^2},$$

απ΄ όπου έπεται το ζητούμενο. □

΄Ασκηση 3.38 (American Mathematical Monthly, E3246 [7])**.** *Ας είναι ψ η συνάρτηση που ορίζεται από την σχέση:*

$$\psi(n) = n\phi(n), \quad \forall\, n \in \mathbb{Z}^+.$$

Να δειχθούν τα εξής:

α) Η συνάρτηση ψ είναι ένεση.

β) Δεν υπάρχει ακέραιος $n > 1$ με $\psi(n) = a^2$, όπου $a \in \mathbb{Z}^+$.

γ) Για κάθε $m \in \mathbb{Z}^+$ υπάρχει $n \in \mathbb{Z}^+$ με $m \mid n$ και $\psi(n) = a^3$, όπου $a \in \mathbb{Z}^+$.

Απόδειξη. α) Ας είναι m και n θετικοί ακέραιοι > 1 με πρωτογενείς αναλύσεις

$$m = p_1^{a_1} \cdots p_k^{a_k} \quad \text{και} \quad n = q_1^{b_1} \cdots q_l^{a_l}.$$

Μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι $p_1 < \ldots < p_k$. Ας είναι $\psi(m) = \psi(n)$. Θα δείξουμε ότι $m = n$.

Τότε, έχουμε:

$$p_1^{2a_1-1} \cdots p_k^{2a_k-1}(p_1 - 1) \cdots (p_k - 1) = q_1^{2b_1-1} \cdots q_l^{2b_l-1}(q_1 - 1) \cdots (q_l - 1). \tag{3.3}$$

Ας υποθέσουμε ότι $p_k \neq q_j$ $(j = 1, \ldots, l)$. Τότε, υπάρχει δείκτης s με $p_k | q_s - 1$. Αν $q_s = p_r$, για κάποιο δείκτη r, τότε $r < k$ (γιατί αν $r = k$, τότε $p_k | 1$ που είναι άτοπο) και $p_k | p_r - 1$, απ΄ όπου $p_k < p_r$ που είναι άτοπο. Τότε, έχουμε $q_s \neq p_i$ $(i = 1, \ldots, k)$, και επομένως υπάρχει δείκτης t με $q_s | p_t - 1$. Οπότε, έχουμε $p_k < q_s < p_t$ που είναι άτοπο. ΄Αρα, υπάρχει δείκτης c με $p_k = q_c$.

Αν $a_k > b_c$, τότε $p_k | q_u$, για κάποιο δείκτη u. Καθώς $q_u = p_v$ ή $q_u = p_v - 1$, για κάποιο δείκτη u, καταλήγουμε, όπως και παραπάνω, σε άτοπο. Αν $a_k < b_c$, τότε $q_c | p_w - 1$, για κάποιο δείκτη $w < k$, και καθώς $p_k = q_c$, έχουμε $p_k < p_w$ που είναι άτοπο. Συνεπώς, ισχύει $a_k = b_c$. Διαιρώντας και τα δύο μέλη της (3.3) με $p_k^{a_k}(p_k - 1)$, επαναλαμβάνουμε την προηγουμένη διαδικασία και τέλος παίρνουμε $m = n$.

β) Ας είναι n ακέραιος > 1 με $\psi(n) = a^2$, όπου $a \in \mathbb{Z}^+$, και $n = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής του ανάλυση. Ας υποθέσουμε ότι $p_1 < \ldots < p_k$. ΄Εχουμε:

$$p_1^{2a_1-1} \cdots p_k^{2a_k-1}(p_1 - 1) \cdots (p_k - 1) = a^2.$$

Αν $k = 1$, τότε ο $p_1^{2a_1-1}(p_1 - 1)$ είναι τετράγωνο ακεραίου και επομένως $p_1 | p_1 - 1$ που είναι άτοπο. ΄Αρα $k \geq 2$. Οπότε, υπάρχει δείκτης $s < k$ με $p_k | p_s - 1$ και επομένως $p_k < p_s$ που είναι άτοπο. Συνεπώς, δεν υπάρχει ακέραιος $n > 1$ τέτοιος, ώστε ο $\psi(n)$ να είναι τέλειο τετράγωνο.

γ) Ας είναι m ακέραιος > 1 με πρωτογενή ανάλυση $m = p_1^{a_1} \cdots p_k^{a_k}$. Τότε,

$$\psi(m) = p_1^{2a_1-1} \cdots p_k^{2a_k-1}(p_1 - 1) \cdots (p_k - 1).$$

Ας υποθέσουμε ότι ο αριθμός $\psi(m)$ δεν είναι κυβική δύναμη ακεραίου. Επιλέγουμε θετικούς περιττούς ακεραίους $w_1, \ldots, w_k$ έτσι, ώστε να ισχύει:

$$x_i = (3w_i + 1)/2 \geq a_i \quad (i = 1, \ldots, k)$$

Θεωρούμε τον ακέραιο

$$n_1 = p_1^{x_1} \cdots p_k^{x_k}.$$

Έχουμε $m \mid n_1$ και

$$\psi(n_1) = p_1^{2x_1-1} \cdots p_k^{2x_k-1}(p_1-1)\cdots(p_k-1) = \left(p_1^{w_1}\cdots p_k^{w_k}\right)^3 (p_1-1)\cdots(p_k-1).$$

Ας υποθέσουμε ότι ο ακέραιος $(p_1-1)\cdots(p_k-1)$ δεν είναι τέλειος κύβος. Η πρωτογενής ανάλυση του $(p_1-1)\cdots(p_k-1)$ είναι:

$$(p_1-1)\cdots(p_k-1) = p_1^{b_1}\cdots p_k^{b_k} q_1^{c_1}\cdots q_l^{c_l}$$

όπου $b_1 \ldots, b_k$ είναι ακέραιοι ≥ 0, $q_1, \ldots, q_l$ είναι οι πρώτοι διαφορετικοί από τους $p_1, \ldots, p_k$ οι οποίοι διαιρούν τον $(p_1-1)\cdots(p_k-1)$ και $c_1, \ldots, c_l$ είναι θετικοί ακέραιοι. Επιλέγουμε ακέραιους $v_i \geq 0$ έτσι, ώστε οι αριθμοί $z_i = (3v_i - b_i)/2$ $(i = 1, \ldots, k)$ να είναι ακέραιοι ≥ 0. Επιπλέον, επιλέγουμε θετικούς ακεραίους $t_1, \ldots, t_l$ έτσι, ώστε οι αριθμοί $r_i = (3t_i + 1 - c_i)/2$ $(i = 1, \ldots, l)$ να είναι θετικοί ακέραιοι (επιλέγουμε t_i περιττό αν ο c_i είναι άρτιος και t_i άρτιο, διαφορετικά). Θεωρούμε τον ακέραιο

$$n_2 = p_1^{x_1+z_1}\cdots p_k^{x_k+z_k} q_1^{r_1}\cdots q_l^{r_l}.$$

Τότε, έχουμε $m \mid n_2$ και

$$\begin{aligned}\psi(n_2) &= \prod_{i=1}^{k} p_i^{2(x_i+z_i)-1+b_i} \prod_{i=1}^{l} q_i^{2r_i-1+c_i}(q_i-1),\\ &= \left(p_1^{w_1+v_1}\cdots p_k^{w_k+v_k} q_1^{t_1}\cdots q_l^{t_l}\right)^3 (q_1-1)\cdots(q_l-1).\end{aligned}$$

Επιπλέον, ισχύει:

$$(q_1-1)\cdots(q_l-1) < (p_1-1)\cdots(p_k-1).$$

Αν ο αριθμός $(q_1-1)\cdots(q_l-1)$ δεν είναι τέλειος κύβος, τότε ακολουθώντας την προηγουμένη διαδικασία προσδιορίζουμε θετικό ακέραιο n_3 με $m \mid n_3$ και

$$\psi(n_3) = A^3(e_1-1)\cdots(e_h-1),$$

όπου A θετικός ακέραιος και $e_1 \ldots e_h$ διαφορετικοί πρώτοι με

$$(e_1-1)\cdots(e_h-1) < (q_1-1)\cdots(q_l-1) < (p_1-1)\cdots(p_k-1).$$

Βλέπουμε λοιπόν ότι κατά την εκτέλεση αυτής της διαδικασίας παράγεται μία φθίνουσα ακολουθία θετικών ακεραίων. Συνεπώς, μετά από πεπερασμένο πλήθος βημάτων η διαδικασία αυτή σταματά και μας δίνει έναν θετικό ακέραιο με τις επιθυμητές ιδιότητες. □

3.7 Θεωρία Αριθμών με Maple

Για τον υπολογισμό των τιμών των βασικών αριθμητικών συναρτήσεων τ, σ, μ και ϕ το Maple έχει εντολές υπολογισμού.

Άσκηση 3.39. *Να υπολογιστουν οι τιμές $\tau(n)$, $\sigma(n)$, $\mu(n)$ και $\phi(n)$ για*

α) $n = 32453543$,
β) $n = 4237531$,
γ) $n = -10$.

Απόδειξη. Οι εντολές υπολογισμού των αριτμητικών συναρτήσεων $\tau(n)$, $\sigma(n)$, $\mu(n)$ και $\phi(n)$ γίνονται με τις ομώνυμες εντολές:

```
with(NumberTheory);
n := 32453543;
tau(n);
sigma(n);
mu(n);
phi(n);
                          n := 32453543
                                 4
                              33065928
                                 1
                              31841160
n := 4237531;
tau(n);
sigma(n);
mu(n);
phi(n);
                           n := 4237531
                                 2
                              4237532
                                 -1
                              4237530
n := -10;
tau(n);
sigma(n);
mu(n);
phi(n);
                              n := -10
                                 4
                                 18
Error, invalid input: NumberTheory:-mu expects its 1st argument, n,
to be of type {posint, And(algebraic, Not({boolean, `in`,
complexcons, extended_numeric}))}, but received -10
Error, invalid input: NumberTheory:-phi expects its 1st argument, n,
to be of type {posint, And(algebraic, Not({boolean, `in`,
complexcons, extended_numeric}))}, but received -10
```

□

Βιβλιογραφία

[1] Apostol, T. (1986) Εισαγωγή στην Αναλυτική Θεωρία Αριθμών, Gunteberg.

[2] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[3] Edwards, H. (2001). Derivation of von Mangoldt's Formula for $\psi(x)$. New York: Dover.

[4] Eynden, C., Barger, S. (1987). E3101. The American Mathematical Monthly, 94(6), 552-553. doi:10.2307/2322854

[5] Forrester, P., Glasser, M., Abbott, H. (1986). E2985. The American Mathematical Monthly, 93(7), 570-570. doi:10.2307/2323045

[6] Great Internet Mersenne Prime Search (2020). Retrieved from http://www.mersenne.org/primes

[7] Golomb, S. (1989). E3246. The American Mathematical Monthly, 96(10), 935-936. doi:10.2307/2324595

[8] Hardy, G.H. (1999). Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work, 3rd ed. New York: Chelsea.

[9] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[10] Stein, A., Honold, T., Keichle, H. (1992). E3398. The American Mathematical Monthly, 99(1), 71-72. doi:10.2307/2324563

[11] Toth, L., Georghiou, C. (1988). E3211. The American Mathematical Monthly, 95(10), 962-963. doi:10.2307/2322405

[12] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[13] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 4

Ισοτιμίες

Οι ισοτιμίες είναι ένα βασικό εργαλείο της θεωρίας αριθμών και εισήχθησαν για πρώτη φορά από τον Gauss στο βιβλίο του Disquisitiones Arithmeticae [5]. Σε αυτό το κεφάλαιο θα δούμε ασκήσεις που αφορούν στις ιδιότητές των ισοτιμιών και τα συστήματα αντιπροσώπων $\bmod n$. Το Θεώρημα Wilson και το Μικρό Θεώρημα του Fermat αποτελούν ορόσημα αυτού του κεφαλαίου ενώ το Θεώρημα Euler-Fermat αποτελεί την κορωνίδα του. Το όνομα του Wilson αποδόθηκε στο θεώρημα που αναφέρεται στην τρίτη ενότητα όχι επειδή το απέδειξε αλλά επειδή, όπως αναφέρει ο Waring [11], ανακάλυψε αυτην την ιδιότητα των πρώτων. Απόδειξη του θεωρήματος δημοσίευσε πρώτος ο Lagrange [7] αν και υπάρχουν ενδείξεις ότι την ιδιότητα αυτήν την γνώριζε και ο Leibniz. Το Μικρό Θεώρημα του Fermat, το οποίο ονομάστηκε έτσι από αυτόν που το διατύπωσε, αποδείχθηκε από τον Euler [3], οποίος στην συνέχεια απέδειξε και το Θεώρημα Euler-Fermat [2]. Την σημαντικότητα των προαναφερόμενων θεωρημάτων καταμαρτυρούν οι αμέτρητες εφαρμογές τους στην θεωρία αριθμών αλλά και στην κρυπτογραφία.

4.1 Σχέσεις Ισοτιμίας

Ας είναι n θετικός ακέραιος.

Ορισμός 4.1. Ο ακέραιος a καλείται *ισότιμος* με τον ακέραιο b *κατά μέτρο* n ή modulo n και γράφουμε $a \equiv b \pmod{n}$, αν και μόνο αν ο n διαιρεί το $a - b$. Δηλαδή, έχουμε:

$$a \equiv b \pmod{n} \iff n \mid a - b.$$

Στην αντίθετη περίπτωση, ο ακέραιος a καλείται ανισότιμος με τον b κατά μέτρο n ή modulo n και γράφουμε $a \not\equiv b \pmod{n}$. Δηλαδή, ισχύει:

$$a \not\equiv b \pmod{n} \iff n \nmid a - b.$$

Στη βιβλιογραφία οι ισοτιμίες συναντώνται συχνά και ως ισοϋπόλοιπα ή ισοδυναμίες $\pmod{n}$.

Πρόταση 4.1. *Η σχέση ισοτιμίας* $(\mathrm{mod}\ n)$ *είναι μια σχέση ισοδυναμίας στο* $\mathbb{Z}$*. Δηλαδή, ισχύουν οι εξής ιδιότητες:*

α) *Για κάθε* $a \in \mathbb{Z}$ *ισχύει* $a \equiv a\,(\mathrm{mod}\ n)$.
β) *Αν* $a \equiv b\,(\mathrm{mod}\ n)$*, τότε* $b \equiv a\,(\mathrm{mod}\ n)$.
γ) *Αν* $a \equiv b\,(\mathrm{mod}\ n)$ *και* $b \equiv c\,(\mathrm{mod}\ n)$*, τότε* $a \equiv c\,(\mathrm{mod}\ n)$.

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πρόταση 1.2]. □

Οι προτάσεις που ακολουθούν περιέχουν τις βασικότερες ιδιότητες των ισοτιμιών, απαραίτητες για την επίλυση ασκήσεων και την απόδειξη σχέσεων και ιδιοτήτων.

Πρόταση 4.2. *Ας είναι* $a, b, c, d \in \mathbb{Z}$*. Αν* $a \equiv b\,(\mathrm{mod}\ n)$ *και* $c \equiv d\,(\mathrm{mod}\ n)$*, τότε ισχύουν τα εξής:*

α) $a + c \equiv b + d\,(\mathrm{mod}\ n)$,
β) $ac \equiv bd\,(\mathrm{mod}\ n)$,
γ) $a^k \equiv b^k\,(\mathrm{mod}\ n)$*, για κάθε* $k \in \mathbb{N}$,
δ) $f(a) \equiv f(b)\,(\mathrm{mod}\ n)$*, για κάθε* $f(x) \in \mathbb{Z}[x]$.

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πρόταση 1.4] ή [12, Πρόταση 4.1.2, Πόρισμα 4.1.3, εδώ]. □

Πρόταση 4.3. *Ας είναι* $a, b, k, n \in \mathbb{Z}$ *με* $k \neq 0$*,* $n > 0$ *και* $\delta = (k, n)$*. Τότε, έχουμε:*

$$ka \equiv kb\,(\mathrm{mod}\ n) \iff a \equiv b\,(\mathrm{mod}\ n/\delta).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πρόταση 1.5] ή [12, Πρόταση 4.1.4, Πόρισμα 4.1.5, εδώ]. □

Ασκήσεις

Για να αποδείξουμε ισότητες κατά μέτρο n συχνά χρησιμοποιούμε ιδιότητες διαιρετότητας.

΄Ασκηση 4.1. *Ας είναι* $a, b, m, n \in \mathbb{Z}$ *με* $m, n > 0$*. Να δειχθεί ότι ισχύει:*

$$a \equiv b\,(\mathrm{mod}\ m),\ \ a \equiv b\,(\mathrm{mod}\ n) \iff a \equiv b\,(\mathrm{mod}\ [n, m]).$$

Απόδειξη. Ας υποθέσουμε ότι $a \equiv b\,(\mathrm{mod}\ m)$ και $a \equiv b\,(\mathrm{mod}\ n)$. Τότε, έχουμε $m \mid a - b$ και $n \mid a - b$, απ΄ όπου παίρνουμε $[m, n] \mid a - b$. Επομένως, ισχύει $a \equiv b\,(\mathrm{mod}\ [n, m])$. Αντιστρόφως, ας υποθέσουμε ότι $a \equiv b\,(\mathrm{mod}\ [n, m])$. Οπότε, έχουμε $[m, n] \mid a - b$ και κατά συνέπεια $m \mid a - b$ και $n \mid a - b$. Επομένως, ισχύει $a \equiv b\,(\mathrm{mod}\, m)$ και $a \equiv b\,(\mathrm{mod}\ n)$. □

΄Ασκηση 4.2. *Να δειχθεί ότι για κάθε* $n \in \mathbb{Z}$ *ισχύει ότι*

$$2n^3 + 3n^2 + n \equiv 0\,(\mathrm{mod}\ 6).$$

Απόδειξη. Αρκεί να δείξουμε ότι το 6 διαιρεί τον $2n^3 + 3n^2 + n$. Καθώς $6 = 2 \cdot 3$ αρκεί να δείξουμε ότι και το 2 διαιρεί τον $2n^3 + 3n^2 + n$ και το 3 διαιρεί τον $2n^3 + 3n^2 + n$. Ισχύει ότι

$$2n^3 + 3n^2 + n = n(n+1)(2n+1).$$

1ος τρόπος: Αν ο n άρτιος, τότε $2 \mid n$, ενώ αν ο n περιττός τότε $2 \mid n+1$. Οπότε, σε κάθε περίπτωση $2 \mid n(n+1)(2n+1)$. Αν $n = 3k$, τότε $3 \mid n$, αν $n = 3k+1$ τότε ο 3 διαιρεί τον $2n+1 = 6k+3$, και αν $n = 3k+2$ τότε ο 3 διαιρεί τον $n+1 = 3k+3$. Έτσι, σε κάθε περίπτωση και ο 3 διαιρεί τον $n(n+1)(2n+1)$.

2ος τρόπος: Το γινόμενο $n(n+1)(2n+1)$ περιέχει το γινόμενο δύο διαδοχικών αριθμων $n(n+1)$ και επομένως διαιρείται από το 2. Επιπλέον έχουμε ότι

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

Ο 3 διαιρεί και τον $n(n+1)(n-1)$ αλλά και τον $n(n+1)(n+2)$ ως γινόμενο τριών διαδοχικών. Οπότε, ο 3 διαιρεί τον $n(n+1)(2n+1)$. □

Άσκηση 4.3. *Ας είναι n σύνθετος ακέραιος > 4. Να δειχθεί ότι ισχύουν τα εξής:*

α) $(n-1)! \equiv 0 \pmod{n}$.

β) Ο ακέραιος $(n-1)! + 1$ δεν είναι δύναμη του n.

Απόδειξη. α) Ο ακέραιος n είναι σύνθετος και κατά συνέπεια υπάρχουν ακέραιοι s, t με $n = st$ και $2 \leq s \leq t \leq n-1$. Αν $s \neq t$, τότε οι s, t είναι διαφορετικοί παράγοντες του $(n-1)!$ και έτσι $st \mid (n-1)!$. Αν $s = t$, τότε $n = s^2$ και επομένως $n - 1 = (s-1)(s+1)$. Καθώς $n > 4$, έπεται $s > 2$ και επομένως $s - 1 \geq 2$. Έτσι, έχουμε $n - 1 \geq 2(s+1) > 2s$. Συνεπώς, οι ακέραιοι s και $2s$ είναι διαφορετικοί παράγοντες του $(n-1)!$ και επομένως $s^2 \mid (n-1)!$. Άρα, σε κάθε περίπτωση ισχύει $n \mid (n-1)!$.

β) Ας υποθέσουμε ότι υπάρχει θετικός ακέραιος k τέτοιος, ώστε $(n-1)! + 1 = n^k$. Τότε, ισχύει $n \mid (n-1)! + 1$ και επομένως $(n-1)! + 1 \equiv 0 \pmod{n}$. Από την (α) έχουμε $(n-1)! \equiv 0 \pmod{n}$. Έτσι,προκύπτει $1 \equiv 0 \pmod{n}$ που είναι άτοπο. Άρα, ο $(n-1)! + 1$ δεν είναι δύναμη του n. □

Στη συνέχεια θα χρησιμοποιήσουμε τις ισοτιμίες για να αντιμετωπίσουμε ασκήσεις διαιρετότητας.

Άσκηση 4.4. *Να βρεθεί το υπόλοιπο της διαίρεσης του 251^{143} με το 7.*

Απόδειξη. Παρατηρούμε ότι ισχύει:

$$251 \equiv -1 \pmod{7}.$$

Από τις ιδιότητες των ισοτιμιών έχουμε:

$$251^{143} \equiv (-1)^{143} \equiv -1 \equiv 6 \pmod{7}.$$

Άρα, υπάρχει ακέραιος z έτσι, ώστε να ισχύει $251^{143} = 7z + 6$ και κατά συνέπεια το υπόλοιπο της διαίρεσης του 251^{143} με το 7 είναι το 6. □

Άσκηση 4.5. *Ας είναι $n \in \mathbb{Z}^+$ με $3 \nmid n$. Να δειχθεί ότι ισχύει:*

$$13 \mid 3^{2n} + 3^n + 1.$$

Απόδειξη. Θα δείξουμε ότι $3^{2n} + 3^n + 1 \equiv 0 \pmod{13}$ που είναι ισοδύναμο με το ζητούμενο. Καθώς $3 \nmid n$, έπεται ότι ο n είναι της μορφής $3k+1$ ή $3k+2$ με $k \in \mathbb{N}$. Ας υποθέσουμε ότι $n = 3k+1$. Αρκεί να δείξουμε ότι

$$3^{6k+2} + 3^{3k+1} + 1 \equiv 0 \pmod{13}$$

Παρατηρούμε ότι ισχύει:

$$3^3 \equiv 27 \equiv 1 \pmod{13}.$$

Έτσι, έχουμε:

$$3^{3k+1} \equiv (3^3)^k 3 \equiv 3 \pmod{13}.$$

Υψώνοντας και τα δύο μέλη της ισοτιμίας στο τετράγωνο, παίρνουμε:

$$3^{2(3k+1)} \equiv 9 \pmod{13}.$$

Επομένως, έχουμε:

$$3^{2n} + 3^n + 1 \equiv 3^{6k+2} + 3^{3k+1} + 1 \equiv 9 + 3 + 1 \equiv 13 \equiv 0 \pmod{13}.$$

Ας υποθέσουμε τώρα ότι $n = 3k+2$. Έχουμε:

$$3^{3k+2} \equiv (3^3)^k 9 \equiv 9 \pmod{13}.$$

Υψώνοντας και τα δύο μέλη της ισοτιμίας στο τετράγωνο, προκύπτει:

$$3^{2(3k+2)} \equiv 9^2 \equiv (-4)^2 \equiv 16 \equiv 3 \pmod{13}.$$

Άρα, έχουμε:

$$3^{2n} + 3^n + 1 \equiv 3^{2(3k+2)} + 3^{3k+2} + 1 \equiv 3 + 9 + 1 \equiv 13 \equiv 0 \pmod{13}.$$

Συνεπώς, σε κάθε περίπτωση ισχύει ότι $3^{2n} + 3^n + 1 \equiv 0 \pmod{13}$. □

Άσκηση 4.6. *Να βρεθεί το υπόλοιπο της διαίρεσης του αριθμού*

$$A = 11^{11} + 11^{11^2} + \cdots + 11^{11^{11}}$$

με το 7.

Απόδειξη. Κατ' αρχάς παρατηρούμε ότι ισχύει $11 \equiv 4 \pmod{7}$, απ' όπου έχουμε:

$$11^2 \equiv 4^2 \equiv 16 \equiv 2 \pmod{7}$$

και

$$11^3 \equiv 11^2 \cdot 11 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}.$$

Επίσης, για κάθε $k \in \mathbb{Z}^+$ έχουμε

$$11^{2k} \equiv 2^{2k} \equiv 4^k \equiv 1 \pmod{3}$$

και

$$11^{2k+1} \equiv 11^{2k} \dot{1}1 \equiv 11 \equiv 2 \pmod{3}.$$

Συνδυάζοντας τα παραπάνω, παίρνουμε:

$$A \equiv 4^2 + 4 + 4^2 + 4 + 4^2 + 4 + 4^2 + 4 + 4^2 + 4 + 4^2 \equiv 6 \cdot 4^2 + 5 \cdot 4 \equiv -16 + 20 \equiv 4 \pmod{7}.$$

Επομένως, υπάρχει $b \in \mathbb{Z}^+$ έτσι, ώστε να ισχύει $A = 7b + 4$. Συνεπώς, το υπόλοιπο της διαίρεσης του A με τον 7 είναι ο 4. □

΄Ασκηση 4.7. *Να προσδιοριστούν οι αριθμοί $n \in \mathbb{N}$ για τους οποίους ισχύει $y+1 \mid y^n+1$, για κάθε $y \in \mathbb{N}$.*

Απόδειξη. Ισχύει ότι

$$y + 1 \equiv 0 \pmod{y+1} \Rightarrow y \equiv -1 \pmod{y+1}.$$

Επομένως για κάθε $n \in \mathbb{N}$ ισχύει ότι

$$y^n + 1 \equiv (-1)^n + 1 \pmod{y+1}.$$

΄Ετσι, για κάθε $y \in \mathbb{N}$ έχουμε:

$$y + 1 \mid y^n + 1 \iff y + 1 \mid (-1)^n + 1 \iff n = 2k + 1, \text{ με } k \in \mathbb{N}.$$

Συνεπώς, οι ζητούμενοι ακέραιοι είναι όλοι οι περιττοί φυσικοί αριθμοί. □

΄Ασκηση 4.8. *Να εξεταστεί αν υπάρχει ακέραιος k τέτοιος, ώστε να ισχύει:*

$$k^2 = 1989^{1988} + 6.$$

Απόδειξη. Υπολογίζουμε το τελευταίο ψηφίο του αριθμού $1989^{1988} + 6$. Ισχύει:

$$1989 \equiv -1 \pmod{10} \Rightarrow 1989^{1988} \equiv 1 \pmod{10} \Rightarrow 1989^{1988} + 6 \equiv 7 \pmod{10}.$$

Θέτουμε $k = 10k_1 + k_0$, με $k_0 \in \{0, \ldots, 9\}$ και $k_1 \in \mathbb{Z}$. Αν ισχύει $k^2 = 1989^{1988} + 6$, τότε, χρησιμοποιώντας την προηγούμενη ισοτιμία, έχουμε

$$(10k_1 + k_0)^2 \equiv 7 \pmod{10},$$

απ΄ όπου

$$k_0^2 \equiv 7 \pmod{10}.$$

Από την άλλη πλευρά, τα τετράγωνα κατά μέτρο 10 είναι τα εξής:

$$0^2 \equiv 0 \pmod{10}, \quad (\pm 1)^2 \equiv 1 \pmod{10}, \quad (\pm 2)^2 \equiv 4 \pmod{10},$$

$$(\pm 3)^2 \equiv 9 \pmod{10}, \quad (\pm 4)^2 \equiv 6 \pmod{10}, \quad 5^2 \equiv 5 \pmod{10}.$$

Καθώς ο 7 δεν είναι τετράγωνο κατά μέτρο 10, δεν υπάρχει τέτοιο k. □

΄Ασκηση 4.9. *Ας είναι $A = 3^{2n+2} + 2^{6n+1}$ και $B = 2^{2n-1}3^{n+2} + 1$. Να δειχθεί ότι το γινόμενο AB είναι πολλαπλάσιο του 121.*

Απόδειξη. Ισχύει $121 = 11^2$. ΄Εχουμε:

$$A \equiv 3^{2n+2} + 2^{6n+1} \equiv 9^n \cdot 9 + 9^n \cdot 2 \equiv 9^n \cdot 11 \equiv 0 \pmod{11}.$$

Επομένως $11 \mid A$. Για τον αριθμό $2B = 2^{2n}3^{n+2} + 2$ έχουμε:

$$2B \equiv 12^n \cdot 9 + 2 \equiv 9 + 2 \equiv 11 \equiv 0 \pmod{11}.$$

΄Αρα $11 \mid 2B$, και καθώς $(11, 2) = 1$, παίρνουμε $11 \mid B$. Συνεπώς $121 \mid AB$. □

΄Ασκηση 4.10. *Να δειχθεί ότι για κάθε περιττό ακέραιο a ισχύει $a^2 \equiv 1 \pmod 8$. Κατόπιν, να δειχθεί ότι κανένας ακέραιος της μορφής $8k+3$ ή $8k+5$, όπου $k \in \mathbb{Z}$, δεν είναι της μορφής $x^2 - 2y^2$, όπου $x, y \in \mathbb{Z}$.*

Απόδειξη. Ας είναι a περιττός ακέραιος. Τότε, έχουμε $a = 4q+1$ ή $4q+3$, όπου q ακέραιος. Έτσι, παίρνουμε:

$$a^2 \equiv (4q+1)^2 \equiv 16q^2 + 8q + 1 \equiv 1 \pmod 8$$

και

$$a^2 \equiv (4q+3)^2 \equiv 16q^2 + 24q + 9 \equiv 1 \pmod 8.$$

Ας είναι τώρα z ακέραιος της μορφής $8k+3$ ή $8k+5$ και $z = x^2 - 2y^2$. Καθώς $z = 8k+3$ ή $8k+5$, ο ακέραιος z είναι περιττός και επομένως ο x είναι περιττός. Αν ο y είναι άρτιος, τότε ισχύει:

$$z \equiv x^2 - 2y^2 \equiv 1 \pmod 8,$$

ενώ, αν ο y είναι περιττός, έχουμε:

$$z \equiv x^2 - 2y^2 \equiv 1 - 2 \equiv -1 \equiv 7 \pmod 8.$$

Καθώς όμως $z \equiv 3$ ή $5 \pmod 8$, καταλήγουμε σε άτοπο. □

΄Ασκηση 4.11. *Να βρεθούν όλοι οι φυσικοί m και n που ικανοποιούν την εξίσωση*

$$3^n - 2^m = 1.$$

Απόδειξη. Ας είναι $n = 2k+1$, όπου k φυσικός. Έχουμε:

$$3^{2k+1} \equiv 9^k \, 3 \equiv 3 \pmod 4.$$

Τότε, παίρνουμε:

$$2^m \equiv 3^n - 1 \equiv 3^{2k+1} - 1 \equiv 3 - 1 \equiv 2 \pmod 4.$$

΄Αρα $4 \mid 2^m - 2$ και επομένως $2 \mid 2^m - 1$. Αν $m > 1$, τότε $2 \mid 1$ που είναι άτοπο. Συνεπώς $m = 1$. Έτσι, έχουμε $3^n = 1 + 2 = 3$ και επομένως $n = 1$.

Ας είναι τώρα $n = 2k$, όπου k φυσικός. Τότε, έχουμε:

$$2^m = 3^{2k} - 1 = (3^k - 1)(3^k + 1).$$

Οπότε, από την μοναδικότητα της πρωτογενούς ανάλυσης ενός φυσικού αριθμού, παίρνουμε:

$$3^k - 1 = 2^a \quad \text{και} \quad 3^k + 1 = 2^b,$$

όπου a, b φυσικοί αριθμοί με $a < b$. Από τις δύο παραπάνω ισότητες προκύπτει:

$$2^a + 2 = 2^b.$$

Αν $a > 1$, τότε έχουμε $2^{a-1} + 1 = 2^{b-1}$ και επομένως $2 \mid 1$ που είναι άτοπο. ΄Αρα $a = 1$ και κατά συνέπεια έχουμε $3^k = 3$, απ΄ όπου $k = 1$. Έτσι, παίρνουμε:

$$2^m = 3^2 - 1 = 8,$$

απ΄ όπου έπεται $m = 3$. Συνεπώς, οι λύσεις της εξίσωσης είναι $(n, m) = (1, 1), (2, 3)$. □

΄Ασκηση 4.12. *Ας είναι $a_n = 2^{2n+1} - 2^{n+1} + 1$ και $b_n = 2^{2n+1} + 2^{n+1} + 1$, όπου $n \in \mathbb{N}$. Να βρεθεί ποιός από τους αριθμούς a_n και b_n είναι διαιρετός από το 5 και ποιός όχι.*

Απόδειξη. Διακρίνουμε τις παρακάτω περιπτώσεις.

(α) $n = 4k$, όπου $k \in \mathbb{N}$. Τότε, έχουμε:

$$a_n \equiv 2^{8k+1} - 2^{4k+1} + 1 \equiv 16^{2k}\, 2 - 16^k\, 2 + 1 \equiv 2 - 2 + 1 \equiv 1 \pmod 5,$$

$$b_n \equiv 2^{8k+1} + 2^{4k+1} + 1 \equiv 16^{2k}\, 2 + 16^k\, 2 + 1 \equiv 2 + 2 + 1 \equiv 5 \equiv 0 \pmod 5.$$

(β) $n = 4k + 1$, όπου $k \in \mathbb{N}$. Τότε, παίρνουμε:

$$a_n \equiv 2^{8k+3} - 2^{4k+2} + 1 \equiv 16^{2k}\, 8 - 16^k\, 4 + 1 \equiv 8 - 4 + 1 \equiv 5 \equiv 0 \pmod 5,$$

$$b_n \equiv 2^{8k+3} + 2^{4k+2} + 1 \equiv 16^{2k}\, 8 + 16^k\, 4 + 1 \equiv 8 + 4 + 1 \equiv 13 \equiv 3 \pmod 5.$$

(γ) $n = 4k + 2$, όπου $k \in \mathbb{N}$. Τότε, έχουμε:

$$a_n \equiv 2^{8k+5} - 2^{4k+3} + 1 \equiv 16^{2k}\, 32 - 16^k\, 8 + 1 \equiv 32 - 8 + 1 \equiv 25 \equiv 0 \pmod 5,$$

$$b_n \equiv 2^{8k+5} + 2^{4k+3} + 1 \equiv 16^{2k}\, 32 + 16^k\, 8 + 1 \equiv 32 + 8 + 1 \equiv 41 \equiv 1 \pmod 5.$$

(δ) $n = 4k + 3$, όπου $k \in \mathbb{N}$. Τότε, προκύπτει:

$$a_n \equiv 2^{8k+7} - 2^{4k+4} + 1 \equiv 16^{2k}\, 128 - 16^k\, 16 + 1 \equiv 8 - 6 + 1 \equiv 3 \pmod 5,$$

$$b_n \equiv 2^{8k+7} + 2^{4k+4} + 1 \equiv 16^{2k}\, 128 + 16^k\, 16 + 1 \equiv 8 + 6 + 1 \equiv 15 \equiv 0 \pmod 5.$$

΄Ετσι, για $n \equiv 1, 2 \pmod 4$, ισχύει $5 \mid a_n$ και $5 \nmid b_n$, ενώ για $n \equiv 0, 3 \pmod 4$, ισχύει $5 \nmid a_n$ και $5 \mid b_n$. □

΄Ασκηση 4.13. *Ας είναι p πρώτος > 2 και k ακέραιος με $1 \leq k \leq p - 1$. Να δειχθεί ότι ισχύει:*

$$\binom{p-1}{k} \equiv (-1)^k \pmod p.$$

Απόδειξη. ΄Εχουμε:

$$\binom{p-1}{k} - (-1)^k = \frac{(p-1)\cdots(p-k)}{k!} - (-1)^k = \frac{(p-1)\cdots(p-k) - (-1)^k k!}{k!}.$$

΄Ετσι, ισχύει:

$$k!\left(\binom{p-1}{k} - (-1)^k\right) = (p-1)\cdots(p-k) - (-1)^k k! = Ap + (-1)^k k! - (-1)^k k! = Ap,$$

όπου A ακέραιος. Ετσι, παίρνουμε:

$$p \,\Big|\, k!\left(\binom{p-1}{k} - (-1)^k\right).$$

Από την Πρόταση 2.10 έχουμε:

$$(k!, p) = (1, p)(2, p)\cdots(p-1, p) = 1.$$

Οπότε, η Πρόταση 2.3 μας δίνει:

$$p \left| \left(\binom{p-1}{k} - (-1)^k \right). \right.$$

Συνεπώς, ισχύει:

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

□

΄Ασκηση 4.14. *Να δειχθεί ότι η εξίσωση*

$$x^2 - 4x - 19^{96} - 96^{19} - 1992 = 0$$

δεν έχει ακέραια λύση.

Απόδειξη. Η εξίσωση γράφεται:

$$(x-2)^2 = 19^{96} + 96^{19} + 1996.$$

΄Εχουμε:

$$\begin{aligned} 1996 &\equiv 6 \pmod{10}, \\ 19^{96} &\equiv 9^{2\cdot 48} \equiv 81^{48} \equiv 1 \pmod{10}, \\ 96^{19} &\equiv 6^{19} \equiv (6^2)^9 6 \equiv 6^9 6 \equiv 6^{10} \equiv (6^2)^5 \equiv 6^5 \equiv (6^2)^2 6 \equiv 6^2 6 \equiv 6 \pmod{10}. \end{aligned}$$

΄Ετσι, παίρνουμε:

$$19^{96} + 96^{19} + 1996 \equiv 3 \pmod{10}.$$

Επίσης, για ακέραιο n ισχύει $n^2 \equiv 0, 1, 4, 5, 6, 9 \pmod{10}$. ΄Αρα, αν υπάρχει ακέραιος x που επαληθεύει την εξίσωση θα έχουμε $(x-2)^2 \equiv 3 \pmod{6}$ και $(x-2)^2 \not\equiv 3 \pmod{6}$ που είναι άτοπο. □

4.2 Ο δακτύλιος $\mathbb{Z}_n$

Η κλάση ισοδυναμίας ενός ακεραίου a ως προς την ισοδυναμία (mod n) είναι το σύνολο

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\},$$

δηλαδή, είναι το σύνολο όλων των ακεραίων της μορφής $x = a + kn$, όπου $k \in \mathbb{Z}$. Συχνά, όταν θέλουμε να δηλώσουμε το μέτρο της ισοτιμίας, γράφουμε $[a]_n$.

Ορισμός 4.2. Το σύνολο $\overline{a}$ καλείται κλάση ισοτιμίας ή κλάση υπολοίπων κατά μέτρο n ή modulo n. Κάθε ακέραιος ο οποίος ανήκει στην κλάση $\overline{a}$ καλείται *αντιπρόσωπος* της $\overline{a}$.

Το σύνολο των κλάσεων υπολοίπων κατά μέτρο n συμβολίζεται με $\mathbb{Z}_n$.

Πρόταση 4.4. *Το σύνολο $\mathbb{Z}_n$ είναι αντιμεταθετικός δακτύλιος και ισχύει:*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Απόδειξη. Βλέπε[13, Κεφάλαιο 4, Πρόταση 1.3 και 2.1]. □

Ορισμός 4.3. Μία κλάση του $\mathbb{Z}_n$ καλείται *πρωτογενής*, αν είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$.

Το σύνολο των πρωτογενών κλάσεων του $\mathbb{Z}_n$ συμβολίζεται με U_n και αποτελεί ομάδα.

Πρόταση 4.5. *Μία κλάση $\bar{a}$ του $\mathbb{Z}_n \setminus \{\bar{0}\}$ είναι πρωτογενής αν και μόνον αν $(a, n) = 1$. Ειδικότερα, ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα, αν και μόνον αν, ο ακέραιος n είναι πρώτος.*

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πρόταση 2.2 και Πόρισμα 2.1]. □

Ορισμός 4.4. Ένα σύνολο n ακεραίων καλείται *πλήρες σύστημα υπολοίπων κατά μέτρο* ή $\bmod n$, αν περιέχει έναν ακέραιο από κάθε κλάση ισοτιμίας $\bmod n$. Ένα σύνολο $\phi(n)$ ακεραίων καλείται *περιορισμένο σύστημα υπολοίπων κατά μέτρο n* ή $\bmod n$, αν περιέχει έναν ακέραιο από κάθε πρωτογενή κλάση ισοτιμίας $\bmod n$.

Πρόταση 4.6. *Ας είναι $a, b \in \mathbb{Z}$ με $(a, n) = 1$.*

α) Αν $\{x_0, \ldots, x_{n-1}\}$ ένα πλήρες σύστημα υπολοίπων $\bmod n$, τότε το σύνολο $\{ax_0 + b, \ldots, ax_{n-1} + b\}$ είναι ένα πλήρες σύστημα υπολοίπων $\bmod n$.

β) Αν $\{x_1, \ldots, x_{\phi(n)}\}$ ένα περιορισμένο σύστημα υπολοίπων $\bmod n$, τότε το σύνολο $\{ax_1, \ldots, ax_{\phi(n)}\}$ είναι ένα περιορισμένο σύστημα υπολοίπων $\bmod n$.

Απόδειξη. α) Βλέπε [13, Κεφάλαιο 4, Πρόταση 3.1].
β) Βλέπε [13, Κεφάλαιο 4, Πρόταση 3.2] ή [12, Πρόταση 4.2.4, εδώ]. □

Ασκήσεις

Άσκηση 4.15. *Να εξεταστεί αν η κλάση $\overline{17}$ του $\mathbb{Z}_{65}$ είναι πρωτογενής, και αν είναι, τότε να βρεθεί ο αντιπρόσωπος a της αντίστροφης κλάσης της με $0 \leq a \leq 64$.*

Απόδειξη. Παρατηρούμε ότι ισχύει $(65, 17) = 1$. Επομένως, σύμφωνα με την Πρόταση 4.5, η κλάση $\overline{17}$ του $\mathbb{Z}_{65}$ είναι πρωτογενής. Για να προσδιορίσουμε την αντίστροφη κλάση της θα χρειαστούμε τον Ευκλείδειο αλγόριθμο. Έχουμε:

$$\begin{aligned} 65 &= 3 \cdot 17 + 14, \\ 17 &= 1 \cdot 14 + 3, \\ 14 &= 4 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Στη συνέχεια υπολογίζουμε:

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (14 - 4 \cdot 3) = -1 \cdot 14 + 5 \cdot 3 = -1 \cdot 14 + 5 \cdot (17 - 1 \cdot 14) = 5 \cdot 17 - 6 \cdot 14 = 5 \cdot 17 - 6(65 - 3 \cdot 17) = -6 \cdot 65 + 23 \cdot 17.$$

Έτσι, παίρνουμε $23 \cdot 17 \equiv 1 \,(\mathrm{mod}\, 65)$, απ΄ όπου έπεται ότι ο 23 αντιπροσωπεύει την αντίστροφη κλάση της $\overline{17}$. □

΄Ασκηση 4.16. *Ας είναι περιττός ακέραιος $k \geq 2$ και $\{x_1, \ldots, x_k\}$ ένα πλήρες σύστημα υπολοίπων* mod k. *Να δειχθεί ότι ισχύει*

$$x_1 + \cdots + x_k \equiv 0 \,(\mathrm{mod}\, k).$$

Απόδειξη. Ας είναι $\{x_1, \ldots, x_k\}$ ένα πλήρες σύστημα υπολοίπων mod k. Τότε, έχουμε:

$$\{\overline{x}_1, \ldots, \overline{x}_k\} = \mathbb{Z}_k = \{\overline{0}, \ldots, \overline{k-1}\}.$$

Επομένως, ισχύει:

$$\overline{x_1 + \cdots + x_k} = \overline{x}_1 + \cdots + \overline{x}_k = \overline{0} + \cdots + \overline{k-1} = \overline{1 + \cdots + (k-1)} = \overline{\frac{k(k-1)}{2}}.$$

Καθώς ο ακέραιος k είναι περιττός, ο αριθμός $(k-1)/2$ είναι ακέραιος. ΄Ετσι, η παραπάνω ισότητα δίνει:

$$\overline{x_1 + \cdots + x_k} = \overline{k}\ \overline{\frac{k-1}{2}} = \overline{0},$$

απ΄ όπου προκύπτει:

$$x_1 + \cdots + x_k \equiv 0 \,(\mathrm{mod}\, k).$$

□

΄Ασκηση 4.17. *Ας είναι ακέραιοι $m, n \geq 2$ με $(m, n) = 1$. Αν $\{x_0, \ldots, x_{m-1}\}$ είναι ένα πλήρες σύστημα υπολοίπων* mod m *και $\{y_0, \ldots, y_{n-1}\}$ ένα πλήρες σύστημα υπολοίπων* mod n *τότε το σύνολο*

$$\{nx_i + my_j \mid i = 0, \ldots, m-1,\ j = 0, \ldots, n-1\}$$

αποτελεί ένα πλήρες σύστημα υπολοίπων mod mn.

Απόδειξη. Εφόσον τα $nx_i + my_j$ είναι mn το πλήθος, αρκεί να δείξουμε ότι είναι ανισότιμα ανά δύο (mod mn). Ας υποθέσουμε ότι υπάρχουν δείκτες i, j, k, l με $(i, j) \neq (k, l)$ τέτοιοι, ώστε να ισχύει:

$$nx_i + my_j \equiv nx_k + my_l \,(\mathrm{mod}\, mn).$$

Τότε, έχουμε:

$$nx_i \equiv nx_k \,(\mathrm{mod}\, m) \quad \text{και} \quad my_j \equiv my_l \,(\mathrm{mod}\, n),$$

απ΄ όπου παίρνουμε:

$$m \mid n(x_i - x_k) \quad \text{και} \quad n \mid m(y_j - y_l).$$

Από την σχέση $(m, n) = 1$, έπεται $m \mid x_i - x_k$, $n \mid y_j - y_l$ και επομένως $x_i \equiv x_k \,(\mathrm{mod}\, m)$, $y_j \equiv y_l \,(\mathrm{mod}\, n)$. Καθώς $(i, j) \neq (k, l)$, αυτό είναι άτοπο. ΄Αρα, οι mn ακέραιοι $nx_i + my_j$ $(i = 1, \ldots, m,\ j = 1, \ldots, n)$ είναι ανισότιμοι ανά δύο κατά μέτρο mn και κατά συνέπεια αποτελούν ένα πλήρες σύστημα υπολοίπων mod mn. □

΄Ασκηση 4.18. *Ας είναι ακέραιοι $m, n \geq 2$ με $(m, n) = 1$. Αν $\{x_1, \ldots, x_{\phi(m)}\}$ είναι ένα περιορισμένο σύστημα υπολοίπων* mod m *και $\{y_1, \ldots, y_{\phi(n)}\}$ ένα περιορισμένο σύστημα υπολοίπων* mod n *τότε το σύνολο*

$$\{nx_i + my_j \mid i = 1, \ldots, \phi(m),\ j = 1, \ldots, \phi(n)\} \tag{4.1}$$

αποτελεί ένα περιορισμένο σύστημα υπολοίπων mod mn.

Απόδειξη. Αποδεικνύεται, όπως και στη προηγούμενη άσκηση, ότι οι ακέραιοι $nx_i + my_j$ $(i = 1, \ldots, \phi(m),\ j = 1, \ldots, \phi(n))$ είναι ανισότιμοι ανά δύο κατά μέτρο mn. Καθώς το πλήθος τους είναι $\phi(m)\phi(n) = \phi(mn)$, αρκεί να δείξουμε ότι $(nx_i + my_j, mn) = 1$ $(i = 1, \ldots, \phi(m),\ j = 1, \ldots, \phi(n))$.

Ας υποθέσουμε ότι p είναι πρώτος τέτοιος, ώστε $p \mid nx_i + my_j$ και $p \mid mn$. Τότε, έχουμε $p \mid m$ ή $p \mid n$. Αν $p \mid m$, τότε ισχύει $p \mid nx_i$ και επομένως $p \mid n$ ή $p \mid x_i$. Καθώς $\{x_1, \ldots, x_{\phi(m)}\}$ είναι ένα περιορισμένο σύστημα υπολοίπων mod m, έχουμε $(x_i, m) = 1$. Από την άλλη πλευρά, ισχύει $(m, n) = 1$. Συνεπώς, $p \nmid n$ και $p \nmid x_i$ που είναι άτοπο. ΄Αρα, έχουμε $p \nmid m$. Ομοίως παίρνουμε $p \nmid n$. Επομένως, ισχύει $(nx_i + my_j, mn) = 1$. □

΄Ασκηση 4.19. *Να βρεθούν οι θετικοί ακέραιοι x και y οι οποίοι ικανοποιούν την ισότητα*

$$1! + 2! + 3! + \cdots + x! = y^2.$$

Απόδειξη. Ας είναι x και y θετικοί ακέραιοι τέτοιοι, ώστε να ισχύει η ισότητα

$$1! + 2! + 3! + \cdots + x! = y^2.$$

Ας υποθέσουμε ότι $x \geq 5$. Τότε, για κάθε ακέραιο z με $5 \leq z \leq x$, έχουμε $10 \mid z!$. Επομένως, ισχύει:

$$y^2 \equiv 1! + 2! + 3! + 4! \equiv 33 \equiv 3 \,(\mathrm{mod}\ 10).$$

Στη συνέχεια, θεωρούμε το πλήρες σύστημα υπολοίπων κατά μέτρο 10:

$$\{0, \pm 1, \pm 2, \pm 3, \pm 4, 5\}.$$

Παρατηρούμε τα εξής:

$$0^2 \equiv 0 \,(\mathrm{mod}\ 10), \quad (\pm 1)^2 \equiv 1 \,(\mathrm{mod}\ 10), \quad (\pm 2)^2 \equiv 4 \,(\mathrm{mod}\ 10),$$

$$(\pm 3)^2 \equiv 9 \,(\mathrm{mod}\ 10), \quad (\pm 4)^2 \equiv 6 \,(\mathrm{mod}\ 10), \quad 5^2 \equiv 5 \,(\mathrm{mod}\ 10).$$

΄Ετσι, βλέπουμε ότι για κάθε ακέραιο y ισχύει $y^2 \not\equiv 3 \,(\mathrm{mod}\ 10)$ και επομένως η παραπάνω ισότητα δεν ισχύει. Για $x = 1, 2, 3, 4$ παίρνουμε αντίστοιχα $y^2 = 1, 3, 9, 33$. ΄Αρα, έχουμε $(x, y) = (1, 1), (3, 3)$. □

΄Ασκηση 4.20. *Ας είναι p ένας περιττός πρώτος και m θετικός ακέραιος με $2^m \not\equiv 1 \,(\mathrm{mod}\ p)$. Να δειχθεί ότι ισχύει:*

$$1^m + 2^m + \cdots + (p-1)^m \equiv 0 \,(\mathrm{mod}\ p).$$

Απόδειξη. Το σύνολο $\{1, \ldots, p-1\}$ είναι ένα περιορισμένο σύστημα υπολοίπων mod p. Έχουμε $p > 2$ και επομένως $(2, p) = 1$. Οπότε, η Πρόταση 4.6 συνεπάγεται ότι το σύνολο $\{2 \cdot 1, 2 \cdot 2, \ldots, 2(p-1)\}$ είναι επίσης ένα περιορισμένο σύστημα υπολοίπων mod p. Έτσι, έχουμε:

$$\{\overline{2 \cdot 1}, \overline{2 \cdot 2}, \ldots, \overline{2(p-1)}\} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

Επομένως, έχουμε:

$$\overline{2 \cdot 1}^m + \overline{2 \cdot 2}^m + \cdots + \overline{2(p-1)}^m = \overline{1}^m + \overline{2}^m + \cdots + \overline{p-1}^m,$$

ή ισοδύναμα:

$$(2 \cdot 1)^m + (2 \cdot 2)^m + \cdots + (2(p-1))^m \equiv 1^m + 2^m + \cdots + (p-1)^m \pmod{p},$$

απ' όπου προκύπτει:

$$(2^m - 1)(1^m + 2^m + \cdots + (p-1)^m) \equiv 0 \pmod{p}.$$

Καθώς $2^m \not\equiv 1 \pmod{p}$, έχουμε $p \nmid 2^m - 1$ και κατά συνέπεια $(p, 2^m - 1) = 1$. Έτσι, χρησιμοποιώντας την Πρόταση 4.3, παίρνουμε:

$$1^m + 2^m + \cdots + (p-1)^m \equiv 0 \pmod{p}.$$

□

4.3 Το Θεώρημα του Wilson

Το παρακάτω θεώρημα δίνει μία ικανή και αναγκαία συνθήκη για να είναι ένας ακέραιος πρώτος.

Θεώρημα 4.1. (*Θεώρημα του Wilson*) *Ένας ακέραιος $p > 1$ είναι πρώτος, αν και μόνον αν, ισχύει:*

$$(p-1)! \equiv -1 \pmod{p}.$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Θεώρημα 4.1] ή [12, Πρόταση 4.7.7, εδώ]. □

Ασκήσεις

Άσκηση 4.21. *Ας είναι ακέραιος $n > 2$. Να δειχθεί ότι ο n είναι πρώτος, αν και μόνον αν, ισχύει:*

$$(n-2)! \equiv 1 \pmod{n}.$$

Απόδειξη. Ας υποθέσουμε ότι ο ακέραιος n είναι πρώτος. Τότε, από το Θεώρημα του Wilson παίρνουμε $(n-1)! \equiv -1 \pmod{n}$ και επομένως ισχύει $n \mid (n-1)! + 1$. Από την άλλη πλευρά, έχουμε

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

Συνδυάζοντας τις δύο προηγούμενες σχέσεις, παίρνουμε $n \mid (n-2)! - 1$ και επομένως $(n-2)! \equiv 1 \pmod{n}$.

Αντιστρόφως, ας υποθέσουμε ότι ισχύει $(n-2)! \equiv 1 \pmod{n}$. Αν ο n είναι σύνθετος, τότε $n = ab$, όπου a, b ακέραιοι με $1 < a \leq b < n$. Έτσι, έχουμε $a \mid n$ και $n \mid (n-1)! + 1$, απ' όπου έπεται $a \mid (n-1)! + 1$. Καθώς $a \leq n-1$, έχουμε $a \mid (n-1)!$ και επομένως $a \mid 1$ που είναι ατοπο. Άρα, ο n είναι πρώτος. □

Άσκηση 4.22. *Αν p είναι περιττός πρώτος, τότε να δειχθεί ότι ισχύει:*

$$\prod_{k=1}^{(p-1)/2} (2k-1)^2 \equiv (-1)^{(p+1)/2} \equiv \prod_{k=1}^{(p-1)/2} (2k)^2 \pmod{p}.$$

Απόδειξη. Επειδή ο p είναι περιττός, ο αριθμός $(p-1)/2$ είναι θετικός ακέραιος. Παρατηρούμε ότι ισχύει:

$$-2 \equiv p-2 \pmod{p}, \quad -4 \equiv p-4 \pmod{p}, \ldots, -(p-1) \equiv 1 \pmod{p}.$$

Πολλαπλασιάζοντας τις παραπάνω ισότητες κατά μέλη, παίρνουμε:

$$(-1)^{(p-1)/2}\, 2 \cdot 4 \cdots (p-1) \equiv 1 \cdot 3 \cdot 5 \cdots (p-2) \pmod{p}. \tag{4.2}$$

Πολλαπλασιάζοντας και τα δύο μέλη της 4.2 με $1 \cdot 3 \cdot 5 \cdots (p-2)$ παίρνουμε:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p-1)/2}\, 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \pmod{p}.$$

Οπότε, χρησιμοποιώντας το Θεώρημα του Wilson, παίρνουμε:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p-1)/2}\, (p-1)! \equiv (-1)^{(p-1)/2}\, (-1) \pmod{p}.$$

Επομένως, ισχύει:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p},$$

από όπου προκύπτει το ζητούμενο.

Επίσης, πολλαπλασιάζοντας και τα δύο μέλη της 4.2 με $2 \cdot 4 \cdots (p-1)$

$$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{(p-1)/2}\, 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \pmod{p}.$$

Οπότε, από το Θεώρημα του Wilson προκύπτει:

$$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{(p-1)/2}\, (p-1)! \equiv (-1)^{(p-1)/2}\, (-1) \pmod{p}.$$

Επομένως, έχουμε:

$$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p},$$

από όπου προκύπτει το ζητούμενο. □

4.4 Το Θεώρημα των Fermat-Euler

Ένα από τα βασικότερα θεωρήματα της Θεωρίας Αριθμών είναι το παρακάτω.

Θεώρημα 4.2. (*Θεώρημα των Fermat – Euler*) *Ας είναι n ακέραιος > 1 και a ακέραιος με $(a, n) = 1$. Τότε, ισχύει:*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Θεώρημα 5.1]. □

Πόρισμα 4.1. (*Μικρό Θεώρημα του Fermat*) *Ας είναι p πρώτος και a ακέραιος με $p \nmid a$. Τότε, ισχύει:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πόρισμα] ή [12, Πρόταση 4.2.1, εδώ]. □

Πόρισμα 4.2. *Ας είναι p πρώτος και a ακέραιος. Τότε, ισχύει:*

$$a^{p} \equiv a \pmod{p}.$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πόρισμα] ή [12, Πρόταση 4.2.2, εδώ]. □

Ασκήσεις

Στις επόμενες ασκήσεις διαιρετότητας γίνεται χρήση του θεωρήματος των Fermat-Euler ή των πορισμάτων του.

΄Ασκηση 4.23. *Ας είναι ακέραιοι $m, n \geq 2$ με $(m, n) = 1$. Να δειχθεί ότι ισχύει:*

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

Απόδειξη. Απο το Θεώρημα των Fermat-Euler έχουμε:

$$m^{\phi(n)} \equiv 1 \pmod{n} \quad \text{και} \quad n^{\phi(m)} \equiv 1 \pmod{m}$$

ή ισοδύναμα:

$$n \mid m^{\phi(n)} - 1 \quad \text{και} \quad m \mid n^{\phi(m)} - 1.$$

Πολλαπλασιάζοντας τις δύο σχέσεις παίρνουμε:

$$nm \mid (m^{\phi(n)} - 1)(n^{\phi(m)} - 1),$$

απ΄ όπου προκύπτει:

$$nm \mid m^{\phi(n)} n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1.$$

Καθώς $mn \mid m^{\phi(n)} n^{\phi(m)}$, έχουμε:

$$nm \mid m^{\phi(n)} + n^{\phi(m)} - 1$$

το οποίο δίνει το ζητούμενο. □

΄Ασκηση 4.24. *Ας είναι p πρώτος και $a, b \in \mathbb{Z}$. Να δειχθεί ότι αν $a^p \equiv b^p \pmod p$, τότε έχουμε:*

$$a^p \equiv b^p \pmod{p^2}.$$

Απόδειξη. Το Μικρό Θεώρημα του Fermat δίνει:

$$a \equiv a^p \pmod p \quad \text{και} \quad b \equiv b^p \pmod p.$$

΄Αρα, έχουμε $a \equiv b \pmod p$, απ΄ όπου έχουμε $a = b + sp$, για κάποιο $s \in \mathbb{Z}$. Από το διώνυμο του Newton παίρνουμε:

$$a^p = (b + sp)^p = b^p + b^{p-1}sp^2 + \sum_{k=2}^{p} \binom{p}{k} b^{p-k} (sp)^k.$$

Οπότε, προκύπτει $a^p \equiv b^p \pmod{p^2}$. □

΄Ασκηση 4.25. *Ας είναι p και q διαφορετικοί πρώτοι τέτοιοι, ώστε για κάθε ακέραιο a να έχουμε:*

$$a^p \equiv a \pmod q, \quad a^q \equiv a \pmod p.$$

Να δειχθεί ότι για κάθε ακέραιο a ισχύει:

$$a^{pq} \equiv a \pmod{pq}.$$

Απόδειξη. Από το Πόρισμα 4.2 έχουμε $a^p \equiv a \pmod p$, απ΄ όπου παίρνουμε $a^{pq} \equiv a^q \pmod p$. Καθώς $a^q \equiv a \pmod p$, προκύπτει $a^{pq} \equiv a \pmod p$. ΄Ετσι, έχουμε $p \mid a^{pq} - a$. Ομοίως παίρνουμε $q \mid a^{pq} - a$. ΄Εχουμε $(p, q) = 1$ και επομένως $pq \mid a^{pq} - a$, απ΄ όπου συνάγεται το ζητούμενο. □

΄Ασκηση 4.26. *Ας είναι a και b ακέραιοι τέτοιοι, ώστε $3 \nmid a$ και $3 \nmid b$. Να δειχθεί ότι ο ακέραιος $a^2 + b^2$ δεν είναι τέλειο τετράγωνο ακεραίου.*

Απόδειξη. Ας υποθέσουμε ότι υπάρχει ακέραιος c τέτοιος, ώστε $a^2 + b^2 = c^2$. Από την άλλη πλευρά, καθώς $3 \nmid a$ και $3 \nmid b$, το Μικρό Θεώρημα του Fermat μας δίνει $a^2 \equiv b^2 \equiv 1 \pmod 3$. Οπότε, έχουμε $c^2 \equiv 2 \pmod 3$. Αν $3 \mid c$, τότε $0 \equiv 2 \pmod 3$ που είναι άτοπο. Αν $3 \nmid c$, τότε από το Μικρό Θεώρημα του Fermat έχουμε ότι $c^2 \equiv 1 \pmod 3$ και επομένως έχουμε $1 \equiv 2 \pmod 3$ που είναι επίσης άτοπο. ΄Αρα, ο ακέραιος $a^2 + b^2$ δεν είναι τέλειο τετράγωνο ακεραίου. □

΄Ασκηση 4.27. *Να δειχθεί ότι ισχύει:*

$$561 \mid 128^{561} - 128.$$

Απόδειξη. Η πρωτογενής ανάλυση του 561 είναι: $561 = 3 \cdot 11 \cdot 17$. ΄Ετσι, σύμφωνα με το Πόρισμα 2.6, αρκεί να δείξουμε ότι ο καθένας από τους πρώτους 3, 11 και 17 διαιρεί τον ακέραιο $128^{561} - 128$. Καθώς $128 = 2^7$, οι ακέραιοι 3, 7 και 11 δεν διαιρούν τον 128 και επομένως από το Μικρό θεώρημα του Fermat έχουμε τα εξής:

$$128^2 \equiv 1 \pmod 3, \quad 128^{10} \equiv 1 \pmod{11}, \quad 128^{16} \equiv 1 \pmod{17}.$$

Ο 560 διαιρείται από τους 2, 10, 16, και έτσι, έχουμε:

$$128^{560} \equiv 1 \pmod 3, \quad 128^{560} \equiv 1 \pmod{11}, \quad 128^{560} \equiv 1 \pmod{17},$$

ή ισοδύναμα:

$$3 \mid 128^{560} - 1, \quad 11 \mid 128^{560} - 1, \quad 17 \mid 128^{560} - 1,$$

απ΄ όπου προκύπτει το αποτέλεσμα. □

΄Ασκηση 4.28. *Να δειχθεί ότι ισχύει:*

$$20801 \mid 20^{15} - 1.$$

Απόδειξη. Η πρωτογενής ανάλυση του 20801 είναι: $20801 = 11 \cdot 31 \cdot 61$. Οπότε, αρκεί να δείξουμε ότι οι πρώτοι 11, 31 και 61 διαιρούν τον ακέραιο $20^{15} - 1$.

Καθώς $11 \nmid 20$, από το Μικρό Θεώρημα του Fermat έχουμε $20^{10} \equiv 1 \pmod{11}$. Χρησιμοποιώντας αυτή την σχέση, παίρνουμε:

$$20^{15} \equiv 20^{10}\, 20^5 \equiv 9^5 \equiv (-2)^5 \equiv -32 \equiv 1 \pmod{11}$$

και κατά συνέπεια έχουμε $11 \mid 20^{15} - 1$.

Για την απόδειξη της δεύτερης σχέσης διαιρετότητας, έχουμε:

$$20^{15} \equiv 4^{15}\, 5^{15} \equiv 2^{30}\, 125^5 \pmod{31}.$$

Από το Μικρό Θεώρημα του Fermat παίρνουμε $2^{30} \equiv 1 \pmod{31}$. Επίσης, έχουμε $125 \equiv 1 \pmod{31}$. Από όλα τα παραπάνω προκύπτει $20^{15} \equiv 1 \pmod{31}$ και επομένως ισχύει $31 \mid 20^{15} - 1$.

Για την τελευταία σχέση διαιρετότητας, έχουμε:

$$20^{15} \equiv 4^{15}\, 5^{15} \equiv (2^6)^5\, (5^3)^5 \equiv 64^5\, 125^5 \equiv 3^5\, 3^5 \equiv 243^2 \equiv (-1)^2 \equiv 1 \pmod{61}.$$

Επομένως, ισχύει $61 \mid 20^{15} - 1$. □

΄Ασκηση 4.29. *Να δειχθεί ότι ισχύει:*

$$7 \mid 2222^{5555} + 5555^{2222}.$$

Απόδειξη. ΄Εχουμε $2222 = 22 \cdot 100 + 22 = 22 \cdot 101$ και $5555 = 55 \cdot 100 + 55 = 55 \cdot 101$. Οπότε, ισχύουν τα εξής:

$$2222 \equiv 22 \cdot 101 \equiv 3 \pmod 7 \quad \text{και} \quad 5555 \equiv 55 \cdot 101 \equiv -3 \pmod 7.$$

Από την άλλη πλευρά, το Μικρό Θεώρημα του Fermat δίνει:

$$3^6 \equiv 1 \pmod 7.$$

Επίσης, έχουμε:

$$2222 \equiv 22 \cdot 101 \equiv 4 \cdot 5 \equiv 20 \equiv 2 \pmod 6$$

και

$$5555 \equiv 55 \cdot 101 \equiv 1 \cdot 5 \equiv 5 \pmod 6.$$

Επομένως, υπάρχουν θετικοί ακέραιοι a και b έτσι, ώστε να ισχύει $2222 = 6a + 2$ και $5555 = 6b + 5$. Συνδυάζοντας τα παραπάνω, παίρνουμε:

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 3^{2222} \equiv 3^{6a+2} + 3^{6b+5} \equiv 3^2(1 + 3^3) \equiv 9 \cdot 28 \equiv 0 \pmod 7.$$

Συνεπώς, ισχύει $7 \mid 2222^{5555} + 5555^{2222}$. □

΄Ασκηση 4.30. *Να βρεθούν οι θετικοί ακέραιοι n που ικανοποιούν την εξής σχέση:*

$$7 \mid 5^{6n} - 5^n + 2.$$

Απόδειξη. Αρκεί να βρούμε τους θετικούς ακέραιους n για τα οποίους ισχύει:

$$5^{6n} - 5^n + 2 \equiv 0 \pmod 7.$$

Καθώς $(5, 7) = 1$, από το Μικρό Θεώρημα του Fermat έχουμε ότι $5^6 \equiv 1 \pmod 7$. Οπότε, η αρχική σχέση γίνεται:

$$1^n - 5^n + 2 \equiv 0 \pmod 7$$

απ΄ όπου παίρνουμε:

$$5^n \equiv 3 \pmod 7.$$

Ας είναι $n = 6k + v$, όπου $v = 0, 1, 2, 3, 4, 5$. Τότε, έχουμε:

$$5^n \equiv 5^{6k}\, 5^v \equiv 5^v \pmod 7.$$

Επιπλέον, ισχύουν τα εξής:

$$5^0 \equiv 1 \pmod 7, \quad 5^1 \equiv 5 \pmod 7, \quad 5^2 \equiv 4 \pmod 7,$$

$$5^3 \equiv 6 \pmod 7, \quad 5^4 \equiv 2 \pmod 7, \quad 5^5 \equiv 3 \pmod 7.$$

Συνδυάζοντας τα παραπάνω, έπεται ότι οι θετικοί ακέραιοι που ικανοποιούν την δοθείσα σχέση είναι οι ακέραιοι της μορφής $n = 5 + 6k$, όπου $k \in \mathbb{Z}^+$. □

Οι ισοτιμίες τύπου $5^n \equiv 3 \pmod 7$ καλούνται εκθετικές ισοτιμίες και στο επόμενο κεφάλαιο θα δούμε και άλλες μεθόδους επίλυσής τους.

΄Ασκηση 4.31. *Να δειχθεί ότι για κάθε $n \in \mathbb{Z}$ ο αριθμός*

$$A = \frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$$

είναι ακέραιος.

Απόδειξη. Καθώς

$$A = \frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n = \frac{3n^5 + 5n^3 + 7n}{15}$$

αρκεί να δείξουμε ότι

$$15 \mid 3n^5 + 5n^3 + 7n$$

και, καθώς $(3,5)=1$, αρκεί να δείξουμε ότι

$$3 \mid 3n^5+5n^3+7n \quad \text{και} \quad 5 \mid 3n^5+5n^3+7n.$$

Χρησιμοποιώντας το Πόρισμα 4.2, παίρνουμε:

$$3n^5+5n^3+7n \equiv 2n+7n \equiv 9n \equiv 0 \pmod 3$$

και

$$3n^5+5n^3+7n \equiv 3n+7n \equiv 10n \equiv 0 \pmod 5,$$

ή ισοδύναμα

$$3 \mid 3n^5+5n^3+7n \ \text{ και } \ 5 \mid 3n^5+5n^3+7n.$$

□

΄Ασκηση 4.32. *Να δειχθεί ότι για κάθε $n \in \mathbb{Z}$ ισχύει:*

$$42 \mid n^7-n.$$

Απόδειξη. Καθώς $42 = 2\cdot 3\cdot 7$ και οι 2, 3 και 7 είναι πρώτοι μεταξύ τους ανά δύο, αρκεί να δείξουμε ότι $2 \mid n^7-n$, $3 \mid n^7-n$ και $7 \mid n^7-n$.

Έχουμε:

$$n^7-n = n(n^6-1) = n(n^2-1)(n^4+n^2+1) = n(n-1)(n+1)(n^4+n^2+1).$$

Καθώς ένας από τους $n-1$ και n είναι άρτιος, έπεται ότι $2 \mid (n-1)n$ και επομένως $2 \mid n^7-n$. Επίσης, ο ακέραιος $n(n-1)(n+1)$ είναι γινόμενο τριών διαδοχικών ακεραίων και επομένως διαιρείται με το 3. Συνεπώς, $3 \mid n^7-n$. Τέλος, από το Πόρισμα 4.2, έχουμε $n^7 \equiv n \pmod 7$, απ΄ όπου $7 \mid n^7-n$. □

΄Ασκηση 4.33. *Να βρεθούν όλοι οι πρώτοι p με την ιδιότητα ο p^4-6 να είναι επίσης πρώτος.*

Απόδειξη. Για $p=2$ και $p=3$ προκύπτει ότι ο p^4-6 είναι ίσος με 10 και 75 αντίστοιχα που δεν είναι πρώτοι. Για $p=5$ έχουμε $p^4-6 = 625-6 = 619$ που είναι πρώτος. Υποθέτουμε στη συνέχεια ότι $p>5$. Τότε, με την χρήση του Μικρού Θεωρήματος του Fermat έχουμε:

$$p^4-6 \equiv 1-6 \equiv -5 \equiv 0 \pmod 5.$$

Επομένως, ο p^4-6 δεν είναι πρώτος. Συνεπώς, ο μοναδικός πρώτος με την παραπάνω ιδιότητα είναι ο 5. □

΄Ασκηση 4.34. *Αν ο p είναι πρώτος, να εξεταστεί αν ο ακέραιος*

$$N = p^{1997} + 1997^p + 1998^{1997+p}$$

είναι πρώτος.

Απόδειξη. Αν $p \geq 3$, τότε ο p είναι περιττός και επομένως ο N άρτιος. Ας υποθέσουμε ότι $p = 2$. Τότε, παίρνουμε:

$$N = 2^{1997} + 1997^2 + 1998^{1999}.$$

Έχουμε:

$$2^{1997} \equiv 4^{998} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \,(\mathrm{mod}\, 3).$$

Καθώς $3 \nmid 1997$, το Μικρό Θεώρημα του Fermat δίνει:

$$1997^2 \equiv 1 \,(\mathrm{mod}\, 3).$$

Επίσης, $3 \mid 1998$. Επομένως, έχουμε:

$$N \equiv 2 + 1 + 0 \equiv 3 \equiv 0 \,(\mathrm{mod}\, 3).$$

Οπότε, $3 \mid N$ και κατά συνέπεια ο N είναι σύνθετος. □

Άσκηση 4.35. *Ας είναι m φυσικός και $5^m = a_k 10^k + \cdots + a_1 10 + a_0$, όπου $a_0, \ldots, a_k \in \{0, \ldots, 9\}$ και $a_k \neq 0$, η δεκαδική παράσταση του 5^m. Αν $n = m + 2^k$, δείξτε ότι η δεκαδική παράσταση του 5^n είναι της μορφής*

$$5^n = b_{k+\ell} 10^{k+\ell} + \cdots + b_{k+1} 10^{k+1} + a_k 10^k + \cdots + a_1 10 + a_0,$$

όπου $b_{k+\ell}, \ldots, b_{k+1} \in \{0, \ldots, 9\}$ και $b_{k+\ell} \neq 0$.

Απόδειξη. Αρκεί να δείξουμε ότι $10^{k+1} \mid 5^n - 5^m$. Έχουμε:

$$5^n - 5^m = 5^m(5^{n-m} - 1) = 5^m(5^{2^k} - 1).$$

Καθώς $10^k \leq 5^m$, έχουμε $k + 1 \leq m$ και επομένως, από την παραπάνω ισότητα, προκυπτει ότι $5^{k+1} \mid 5^n - 5^m$. Από την άλλη πλευρά, το Θεώρημα των Fermat-Euler δίνει:

$$5^{\phi(2^{k+1})} \equiv 1 \,(\mathrm{mod}\, 2^{k+1})$$

Έχουμε $\phi(2^{k+1}) = 2^k$ και επομένως έπεται:

$$5^{2^k} \equiv 1 \,(\mathrm{mod}\, 2^{k+1}).$$

Οπότε, ισχύει $2^{k+1} \mid 5^{2^k} - 1$. Καθώς $(2, 5) = 1$, προκύπτει $10^{k+1} \mid 5^n - 5^m$ που είναι το ζητούμενο. □

Άσκηση 4.36. *Ας είναι p ένας πρώτος. Να δειχθεί ότι για κάθε ακέραιο a ισχύουν τα εξής:*

$$p \mid a^p + (p-1)!a, \quad p \mid a^p(p-1)! + a.$$

Απόδειξη. Από το Θεώρημα του Wilson έχουμε $(p-1)! \equiv -1 \,(\mathrm{mod}\ p)$. Πολλαπλασιάζοντας και τα δύο μέλη με a, παίρνουμε $(p-1)!a \equiv -a \,(\mathrm{mod}\ p)$. Το Πόρισμα 4.2 δίνει $a^p \equiv a \,(\mathrm{mod}\ p)$. Έτσι, προκύπτει $(p-1)!a \equiv -a^p \,(\mathrm{mod}\ p)$ και επομένως $p \mid a^p + (p-1)!a$.

Ομοίως, για την απόδειξη της δεύτερης σχέσης, πολλαπλασιάζουμε και τα δύο μέλη της $(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$ με a^p και παίρνουμε $(p-1)!a^p \equiv -a^p \,(\mathrm{mod}\, p)$. Στη συνεχεια, η σχέση $a^p \equiv a \,(\mathrm{mod}\, p)$ δίνει $(p-1)!a^p \equiv -a \,(\mathrm{mod}\, p)$, απ' όπου έχουμε $p \mid a^p(p-1)! + a$. □

4.5 Τάξη Ακεραίων

Ορισμός 4.5. Ας είναι n φυσικός αριθμός μεγαλύτερος του 1 και a ακέραιος τέτοιος ώστε $(a,n)=1$. Ο μικρότερος θετικός ακέραιος r για τον οποίο ισχύει $a^r \equiv 1 \pmod{n}$ καλείται *τάξη* του a κατά μέτρο n ή mod n, και συμβολίζεται με $\mathrm{ord}_n(a)$.

Οι βασικότερες ιδιότητες της τάξης ενός ακεραίου δίνονται στην παρακάτω πρόταση.

Πρόταση 4.7. *Ας είναι $a,s,t,n \in \mathbb{Z}$ με $n>1$, $(a,n)=1$ και $r=\mathrm{ord}_n(a)$.*
α) $a^s \equiv a^t \pmod{n} \Leftrightarrow s \equiv t \pmod{r}$.
β) $a^s \equiv 1 \pmod{n} \Leftrightarrow r \mid s$.
γ) $r \mid \phi(n)$.
δ) οι ακέραιοι $1, a, \ldots, a^{r-1}$ *είναι ανά δύο ανισότιμοι* mod n.
ε) $b \equiv a \pmod{n} \Rightarrow \mathrm{ord}_n(b) = r$.

Απόδειξη. Βλέπε [13, Κεφάλαιο 4, Πρόταση 6.1] ή [12, Πρόταση 5.4.3, Πρόταση 5.4.5, εδώ]. □

Πρόταση 4.8. *Ας είναι $a,n \in \mathbb{Z}$ με $n>1$ και $(a,n)=1$. Αν $r=\mathrm{ord}_n(a)$ και k φυσικός ≥ 1, τότε ισχύει:*

$$\mathrm{ord}_n(a^k) = r/(r,k).$$

Απόδειξη. Βλέπε [13, Κεφάλαιο 5, Λήμμα 4.1] □

Ασκήσεις

΄Ασκηση 4.37. *Να βρεθούν οι τάξεις των ακεραίων* mod 28.

Απόδειξη. Η τάξη ενός ακεραίου a έχει νόημα μόνον αν $(a,28)=1$. Επιπλέον, κάθε τέτοιος ακέραιος a ανήκει σε κάποια κλάση ενός περιορισμένου συστήματος υπολοίπων. Εφόσον οι ακέραιοι της ίδιας κλάσης έχουν την ίδια τάξη αρκεί να βρούμε την τάξη των ακεραίων που αποτελούν ένα περιορισμένο σύστημα υπολοίπων.

΄Ενα περιορισμένο σύστημα υπολοίπων mod 28 είναι το σύνολο

$$\{\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13\}.$$

Η τάξη mod 28 των παραπάνω ακεραίων είναι κάποιος διαιρέτης του

$$\phi(28) = \phi(2^2)\phi(7) = 2 \cdot 6 = 12.$$

Εύκολα υπολογίζουμε:

$$\mathrm{ord}_{28}(1) = 1, \qquad \mathrm{ord}_{28}(-1) = \mathrm{ord}_{28}(\pm 13) = 2,$$
$$\mathrm{ord}_{28}(-3) = \mathrm{ord}_{28}(9) = 3, \quad \mathrm{ord}_{28}(3) = \mathrm{ord}_{28}(\pm 5) = \mathrm{ord}_{28}(\pm 11) = \mathrm{ord}_{28}(-9) = 6.$$

΄Αρα, οι τάξεις των ακεραίων mod 28 είναι: 1, 2, 3 και 6. □

Οι δύο ασκήσεις που ακολουθούν αφορούν σε ιδιότητες της τάξης των ακεραίων.

΄Ασκηση 4.38. *Ας είναι $a,b \in \mathbb{Z}$ με $ab \equiv 1 \pmod{n}$. Τότε* $\mathrm{ord}_n(a) = \mathrm{ord}_n(b)$.

Απόδειξη. Ας είναι $\mathrm{ord}_n(a) = s$ και $\mathrm{ord}_n(b) = t$. Αν $s < t$, τότε, από την σχέση $ab \equiv 1 \pmod n$, έχουμε $a^s b^s \equiv 1 \pmod n$. Καθώς $\mathrm{ord}_n(a) = s$, έπεται $b^s \equiv 1 \pmod n$. Αυτό όμως είναι άτοπο γιατί ο t είναι ο μικρότερος θετικός για τον οποίο ισχύει $b^t \equiv 1 \pmod n$. Ομοίως, αν υποθέσουμε ότι $t < s$ καταλήγουμε σε άτοπο. Άρα, $s = t$. □

Άσκηση 4.39. *Ας είναι $n, a, b \in \mathbb{Z}$ με $n \geq 2$ και $(a, n) = (b, n) = 1$. Αν $(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1$, τότε να δειχθεί ότι ισχύει*

$$\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\ \mathrm{ord}_n(b).$$

Απόδειξη. Ας είναι $b \equiv 1 \pmod n$. Τότε, ισχύει $ab \equiv a \pmod n$. Έτσι, από την Πρόταση 4.7 έχουμε $\mathrm{ord}_n(b) = \mathrm{ord}_n(1) = 1$ και $\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)$. Άρα ισχύει:

$$\mathrm{ord}_n(ab) = \mathrm{ord}_n(a) = \mathrm{ord}_n(a)\ \mathrm{ord}_n(b).$$

Επομένως, η προς απόδειξη σχέση ισχύει. Αν $a \equiv 1 \pmod n$, τότε ομοίως προκύπτει το αποτέλεσμα.

Ας υποθέσουμε τώρα ότι $a \not\equiv 1 \pmod n$ και $b \not\equiv 1 \pmod n$. Θέτουμε $\mathrm{ord}_n(a) = s$ και $\mathrm{ord}_n(b) = t$. Έχουμε:

$$(ab)^{st} = a^{st} b^{st} = (a^s)^t (b^t)^s \equiv 1 \pmod n. \tag{4.3}$$

Ας είναι m θετικός ακέραιος έτσι, ώστε να ισχύει $(ab)^m \equiv 1 \pmod n$. Υψώνουμε και τα δύο μέλη της ισοτιμίας στη δύναμη s και παίρνουμε $a^{sm} b^{sm} \equiv 1 \pmod n$, απ' όπου προκύπτει $b^{sm} \equiv 1 \pmod n$. Οπότε, από την Πρόταση 4.7(β) έχουμε $t \mid sm$. Καθώς $(s, t) = 1$, έπεται $t \mid m$. Ομοίως παίρνουμε $s \mid m$. Καθώς $(s, t) = 1$, συνεπάγεται $st \mid m$. Άρα ο st είναι ο μικρότερος ακέραιος για τον οποίο ισχύει η (4.3). Συνεπώς, έχουμε $\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\ \mathrm{ord}_n(b)$. □

4.6 Συνδυαστικές Ασκήσεις

Άσκηση 4.40 (American Mathematical Monthly, E3014 [4])**.** *Ας είναι n ακέραιος ≥ 3. Να δειχθεί ότι η ισοτιμία*

$$3^x \equiv y \pmod{2^n}$$

επαληθεύεται από φυσικούς x και y αν και μόνον αν $y \equiv 1, 3 \pmod 8$.

Απόδειξη. Κατ' αρχάς θα υπολογίσουμε την τάξη του 3 $\pmod{2^n}$, για $n \geq 3$. Πιο συγκεκριμένα, θα δείξουμε ότι ο ακέραιος 2^{n+2} διαιρεί ακριβώς τον $3^{2^n} - 1$. Θα εφαρμόσουμε την μέθοδο της επαγωγής. Για $n = 1$, αυτό είναι προφανές, καθώς έχουμε $2^{n+2} = 8$ και $3^{2^n} - 1 = 8$. Ας υποθέσουμε ότι ισχύει για $n = k$, δηλαδή ο 2^{k+2} διαιρεί ακριβώς τον $3^{2^k} - 1$. Έχουμε:

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

Από την υπόθεση της επαγωγής, έχουμε $3^{2^k} - 1 = 2^{k+2} A$, όπου A περιττός ακέραιος. Έτσι, παίρνουμε:

$$3^{2^{k+1}} - 1 = 2^{k+3} A(2^{k+1} A + 1),$$

απ΄ όπου έχουμε ότι ο ακέραιος 2^{k+3} διαιρεί ακριβώς τον $3^{2^{k+1}}-1$.

Ας είναι $m=\mathrm{ord}_{2^n}(3)$. Τότε $m=2^b$, με $b\le n-2$. Αν $b<n-2$, τότε έχουμε $2^n \mid 3^{2^b}-1$ που είναι άτοπο, γιατί σύμφωνα με τα προηγούμενα, ο 2^{b+2} διαιρεί ακριβώς τον $3^{2^b}-1$ και $b+2<n$. ΄Αρα, ισχύει $\mathrm{ord}_{2^n}(3)=2^{n-2}$. Συνεπώς, οι ακέραιοι 3^x $(x=0,\dots,2^{n-2}-1)$ είναι ανισότιμοι ανά δύο κατά μέτρο 2^n.

Από την άλλη πλευρά, για κάθε άρτιο φυσικό m έχουμε $3^m\equiv 1\,(\mathrm{mod}\,8)$, ενώ για κάθε περιττό φυσικό m ισχύει $3^m\equiv 3\,(\mathrm{mod}\,8)$. ΄Ετσι, αν $-1\equiv 3^x\,(\mathrm{mod}\,2^n)$ για κάποιο $x\in\{0,\dots,2^{n-3}\}$, τότε έχουμε $-1\equiv 1$ ή $3\,(\mathrm{mod}\,8)$ που είναι άτοπο. ΄Αρα, η κλάση του -1 δεν ανήκει στην ομάδα που παράγεται από την κλάση του 3 μέσα στην ομάδα U_{2^n}. Επομένως, οι 2^{n-1} ακέραιοι $(-1)^k 3^x$ $(k=0,1,\ x=0,\dots,2^{n-2}-1)$ είναι ανισότιμοι ανά δύο $(\mathrm{mod}\,2^n)$ και, καθώς $|U_{2^n}|=\phi(2^n)=2^{n-1}$, αποτελούν ένα περιορισμένο σύστημα υπολοίπων $(\mathrm{mod}\,2^n)$.

Ας είναι $y\equiv 1$ ή $3\,(\mathrm{mod}\,8)$. Τότε, ο y είναι περιττός και επομένως υπάρχουν $k\in\{0,1\}$ και $x\in\{0,\dots,2^{k-3}\}$ έτσι, ώστε $y\equiv(-1)^k 3^x\,(\mathrm{mod}\,2^n)$. Αν $k=1$, τότε $y\equiv -3^x\ (\mathrm{mod}\ 2^n)$ και επομένως $y\equiv -1$ ή $-3\ (\mathrm{mod}\ 2^n)$ που είναι άτοπο. ΄Αρα, έχουμε $y\equiv 3^x\,(\mathrm{mod}\,2^n)$. Αντιστρόφως, αν $y\equiv 3^x\,(\mathrm{mod}\,2^n)$, όπου $n\ge 3$, τότε, όπως είδαμε πιο πάνω, ισχύει $y\equiv 1$ ή $3\,(\mathrm{mod}\,8)$. □

΄Ασκηση 4.41 (American Mathematical Monthly, E3452 [9])**.** *Ας είναι n περιττός ακέραιος >3. Να δειχθεί ότι υπάρχει πρώτος p τέτοιος, ώστε $2^{\phi(n)}\equiv 1\,(\mathrm{mod}\,p)$ και $p\nmid n$.*

Απόδειξη. Ας είναι $n=p_1^{a_1}\cdots p_k^{a_k}$ η πρωτογενής ανάλυση του n. Τότε, έχουμε:

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

Επομένως, ισχύει $2^k\mid\phi(n)$. Οπότε, έχουμε $2^{\phi(n)}-1=Y^{2^k}-1$, όπου Y άρτιος ακέραιος >3 (γιατί $\phi(n)\ge 4$). Γράφουμε:

$$Y^{2^k}-1=(Y-1)\prod_{i=0}^{k-1}(Y^{2^i}+1).$$

Αν q είναι πρώτος με $q\mid Y^{2^i}+1$ και $q\mid Y-1$, τότε $Y^{2^i}+1\equiv 0\,(\mathrm{mod}\,q)$ και $Y\equiv 1\,(\mathrm{mod}\,q)$, απ΄ όπου $2\equiv 0\,(\mathrm{mod}\,q)$, και επομένως $q=2$. Καθώς όμως ο ακέραιος Y είναι άρτιος, ο πρώτος q είναι περιττός. ΄Ετσι, καταλήγουμε σε άτοπο και κατά συνέπεια έχουμε $(Y^{2^i}+1,Y-1)=1$.

Αν q είναι πρώτος με $q\mid Y^{2^i}+1$ και $q\mid Y^{2^j}+1$ με $j>i$. Τότε, έχουμε $q\mid Y^{2^j}-Y^{2^i}$. Καθώς $q\nmid Y$, ισχύει $q\mid Y^{2^{j-i}}-1$. Οπότε, έχουμε $Y^{2^{j-i}}\equiv 1\,(\mathrm{mod}\,q)$, απ΄ όπου έπεται $Y^{2^j}\equiv 1\,(\mathrm{mod}\,q)$. Καθώς, ισχύει $Y^{2^j}\equiv -1\,(\mathrm{mod}\,q)$, παίρνουμε $2\equiv 0\,(\mathrm{mod}\,q)$, και καταλήγουμε όπως προηγουμένως σε άτοπο.

΄Αρα, έχουμε $(Y^{2^i}+1,Y^{2^j}+1)=1$. Συνεπώς, ο ακέραιος $Y^{2^k}-1$ είναι ένα γινόμενο από $k+1$ πρώτους ανά δύο παράγοντες >1. Επειδή, ο ακέραιος n έχει ακριβώς k παράγοντες, συνεπάγεται ότι υπάρχει πρώτος p με $p\nmid n$ και $p\mid Y^{2^k}-1$. □

΄Ασκηση 4.42 (American Mathematical Monthly, E3089 [6])**.** *Να βρεθούν όλοι οι άρτιοι ακέραιοι $n\ge 4$ που έχουν την εξής ιδιότητα: αν b ακέραιος με $1<b<n$ και $(b,n)=1$,*

τότε η γραμμική ισοτιμία

$$(b-1)x \equiv \frac{n}{2} \pmod{n}$$

έχει λύση.

Απόδειξη. Ας είναι $n = 2m$ και b ακέραιος με $1 < b < n$ και $(b, n) = 1$. Θέτουμε $d = (b-1, n)$. Τότε, η γραμμική ισοτιμία $(b-1)x \equiv m \pmod{n}$ έχει λύση, αν και μόνον αν, ισχύει $d \mid m$.

Αν $n = 2^k$, τότε, καθώς $1 < b < n$, έχουμε $d = 2^j$ για κάποιο j με $1 \leq j < k$. Οπότε $d \mid m$ και κατά συνέπεια η παραπάνω γραμμική ισοτιμία έχει λύση.

Ας υποθέσουμε στη συνέχεια ότι $n = 2^k c$, όπου c περιττός ακέραιος > 1. Επειδή ισχύει $(2^k, c) = 1$, υπάρχει ακέραιος t με $1 \leq t < c$ έτσι, ώστε $2^k t \equiv 1 \pmod{c}$. Παίρνουμε $b = 2^k t + 1$. Αν p είναι ένας περιττός πρώτος με $p \mid n$ και $p \mid b$, έχουμε $p \mid c$ και $p \mid b$. Έτσι, καθώς $b \equiv 2^k t + 1 \equiv 2 \pmod{c}$, παίρνουμε $p \mid 2$ που είναι άτοπο. Από την άλλη πλευρά, επειδή ο n είναι άρτιος και ο b περιττός, ο μέγιστος κοινός τους διαιρέτης, δεν είναι άρτιος. Άρα, ισχύει $(n, b) = 1$. Επίσης, έχουμε $1 < b < n$, $2^k \nmid m$ και $2^k \mid d$. Άρα, $d \nmid m$ και επομένως η γραμμική ισοτιμία $(b-1)x \equiv m \pmod{n}$ δεν έχει λύση. Συνεπώς, ο ακέραιος n δεν έχει την ιδιότητα της εκφώνησης. Έτσι, συμπεραίνουμε ότι οι μόνοι ακέραιοι που έχουν την παραπάνω ιδιότητα είναι οι 2^k, όπου k ακέραιος ≥ 2. □

Άσκηση 4.43 (American Mathematical Monthly, E3210 [10])**.** *Να βρεθούν όλα τα ζεύγη ακεραίων m, n που είναι τέτοια, ώστε $1 \leq m < n$, $m^2 \equiv -1 \pmod{n}$ και $n^2 \equiv -1 \pmod{m}$.*

Απόδειξη. Συμβολίζουμε με $\mathcal{T}$ το σύνολο των ζευγών $(a, b) \in \mathbb{N}^2$ που είναι τέτοια, ώστε:

$$1 \leq a < b, \quad a^2 \equiv -1 \pmod{b}, \quad b^2 \equiv -1 \pmod{a}.$$

Καθώς $a^2 \equiv -1 \pmod{b}$, ο αριθμός $c = (a^2+1)/b$ είναι φυσικός. Έχουμε:

$$c^2 \equiv \frac{(a^2+1)^2}{b^2} \equiv -(a^2+1)^2 \equiv -1 \pmod{a}$$

και

$$a^2 \equiv bc - 1 \equiv -1 \pmod{c}.$$

Επίσης, ισχύει:

$$1 \leq c = \frac{a^2+1}{b} < \frac{a^2+1}{a} = a + \frac{1}{a}.$$

Οπότε, επειδή ο αριθμός c είναι φυσικός, έχουμε $1 \leq c \leq a$. Αν $a = c$, τότε $-1 \equiv a^2 \equiv 0 \pmod{a}$ και επομένως $a \mid 1$, απ' όπου έπεται $a = c = 1$.

Θεωρούμε την απεικόνιση:

$$T : \mathcal{T} \longrightarrow \mathbb{N}^2, \ (a, b) \longmapsto (c, a).$$

Εύκολα διαπιστώνουμε ότι η απεικόνιση T είναι ένεση. Η αντίστροφός της απεικόνιση είναι:

$$T^{-1} : T(\mathcal{T}) \longrightarrow \mathcal{T}, \ (m, n) \longmapsto (n, (n^2+1)/m).$$

Για κάθε φυσικό μ γράφουμε $T^{\mu}(a,b) = (c_{\mu}, a_{\mu})$ και έτσι προκύπτει μία φθίνουσα ακολουθία φυσικών αριθμών: $a \geq c_1 \geq c_2 \geq \ldots$. Ας είναι $c_0 = \min_{\nu \in \mathbb{N}}\{c_{\nu}\}$. Αν $c_0 \neq a_0$, τότε $T(c_0, a_0) = (c', c_0)$ και $c' \leq c_0$. Οπότε, έχουμε $c' = c_0$ και επομένως, όπως είδαμε παραπάνω, ισχύει $T(c_0, a_0) = (1,1)$. Δηλαδή, υπάρχει φυσικός k τέτοιος, ώστε $T^k(a,b) = (1,1)$. Άρα, $(a,b) = T^{-k}(1,1)$.

Από την άλλη πλευρά, θεωρούμε την ακολουθία των αριθμών του Fibonacci, $(F_n)_{n\geq 1}$ που ορίζεται ως εξής:

$$F_1 = F_2 = 1, \quad F_{n+1} = F_n + F_{n-1}.$$

Θα δείξουμε ότι για κάθε $n \geq 3$ ισχύει:

$$F_n^2 - F_{n-2}F_{n+2} = (-1)^n.$$

Για $n = 3$ έχουμε:

$$F_3^2 - F_1F_5 = 4 - 5 = -1 = (-1)^3.$$

Υποθέτουμε ότι η παραπάνω ισότητα ισχύει για $n = m-1$, δηλαδή έχουμε $F_{m-1}^2 - F_{m-3}F_{m+1} = (-1)^{m-1}$. Ας είναι $n = m$. Τότε:

$$\begin{aligned} F_m^2 - F_{m-2}F_{m+2} &= F_m(F_{m-1} + F_{m-2}) - F_{m-2}(F_m + F_{m+1}) \\ &= F_mF_{m-1} - F_{m-2}F_{m+1} \\ &= F_m(F_{m-2} + F_{m-3}) - F_{m-2}(F_m + F_{m-1}) \\ &= F_mF_{m-3} - F_{m-2}F_{m-1} \\ &= F_mF_{m-3} + F_{m-1}F_{m-3} - F_{m-1}F_{m-3} - F_{m-2}F_{m-1} \\ &= F_{m+1}F_{m-3} - F_{m-1}^2 \\ &= (-1)^m. \end{aligned}$$

Συνεπώς, η προς απόδειξη ισότητα αληθεύει. Οπότε, για κάθε $m \geq 1$, έχουμε:

$$F_{2m-1} < F_{2m+1} \quad F_{2m+1}^2 \equiv -1 \,(\mathrm{mod}\, F_{2m-1}), \quad F_{2m-1}^2 \equiv -1 \,(\mathrm{mod}\, F_{2m+1}).$$

Τέλος, θα δείξουμε ότι για κάθε $k \geq 1$ ισχύει:

$$T^{-k}(1,1) = (F_{2k-1}, F_{2k+1}).$$

Για $k = 1$, έχουμε $T^{-1}(1,1) = (1,2) = (F_1, F_3)$. Υποθέτουμε ότι η ισότητα ισχύει για $k = m$, δηλαδή $T^{-m}(1,1) = (F_{2m-1}, F_{2m+1})$. Ας είναι $k = m+1$. Τότε, έχουμε:

$$T^{-(m+1)}(1,1) = T^{-1}(F_{2m-1}, F_{2m+1}) = \left(F_{2m+1}, \frac{F_{2m+1}^2 + 1}{F_{2m-1}}\right).$$

Καθώς όμως $F_{2m+1}^2 - (-1)^{2m+1} = F_{2m-1}F_{2m+3}$, παίρνουμε:

$$T^{-(m+1)}(1,1) = (F_{2m+1}, F_{2m+3}).$$

Συνεπώς, τα ζεύγη (F_{2k-1}, F_{2k+1}) $(k = 1, 2, \ldots)$ συνιστούν το σύνολο των ζευγών που επαληθεύουν την δοσμένη συνθήκη. □

4.7 Θεωρία Αριθμών με Maple

Οι αλγόριθμοι που υλοποιούν την επίλυση ισοτιμιών ποικίλουν ανάλογα με το αν οι ισοτιμίες είναι γραμμικές, πολυωνυμικές ή εκθετικές. Η ταχύτητα που χρειάζεται ο κάθε αλγόριθμος για την επίλυση μιας ισοτιμίας διαφέρει και για αυτό το λόγο η προσπάθεια εξεύρεσης αλγορίθμων που να υλοποιούν ταχύτερα την διαδικασία αποτελεί έναν από τους ποιο ταχύτατα αναπτυσσόμενους τομείς των εφαρμοσμένων μαθηματικών.

Οι εντολή για να υπολογίσουμε την τάξη ενός ακεραίου $a \pmod n$ είναι η order(a,n). Αν οι a και n δεν είναι πρώτοι μεταξύ τους το πρόγραμμα μας επιστρέφει FAIL. Στην επόμενη άσκηση εκτός από την εντολή order χρησιμοποιούμε και τις if και for για να υπολογίσουμε την τάξη όλων των ακεραίων a με $(a, n) = 1$ και $1 \leq a \leq n$.

΄Ασκηση 4.44. *Να βρεθούν οι τάξεις των ακεραίων* $\bmod 28$.

Απόδειξη. Με κώδικα Maple:

```
for i to 28 do if gcd(i,28)=1 then
print(ord_28(i)=order(i,28)) end if end do;
                        ord_28(1) = 1
                        ord_28(3) = 6
                        ord_28(5) = 6
                        ord_28(9) = 3
                        ord_28(11) = 6
                        ord_28(13) = 2
                        ord_28(15) = 2
                        ord_28(17) = 6
                        ord_28(19) = 6
                        ord_28(23) = 6
                        ord_28(25) = 3
                        ord_28(27) = 2
```

□

Για να λυθεί η γραμμική ισοτιμία $ax \equiv b \pmod n$ η εντολή που εισάγουμε είναι η msolve(ax=b,n). Οι λύσεις που επιστρέφει η εντολή είναι $\bmod n$. Σε περίπτωση που δεν υπάρχουν λύσεις η εντολή δεν επιστρέφει τίποτα.

΄Ασκηση 4.45. *Να λυθούν οι γραμμικές ισοτιμίες*
α) $45x - 2 \equiv 0 \pmod 7$,
β) $-660x \equiv 121 \pmod{143}$,
γ) $255x \equiv 221 \pmod{374}$.

Απόδειξη. Με κώδικα Maple:

```
msolve(45*x-2, 7);
                              {x = 3}
msolve(-660*x = 121, 143);
   {x = 10}, {x = 23}, {x = 140}, {x = 36}, {x = 49}, {x = 62},
   {x = 75}, {x = 88}, {x = 101}, {x = 127}, {x = 114}
```

```
msolve(255*x = 221, 374);
 {x = 149}, {x = 303}, {x = 17}, {x = 39}, {x = 259}, {x = 61},
 {x = 281}, {x = 171}, {x = 215}, {x = 83}, {x = 193}, {x = 369},
 {x = 105}, {x = 325}, {x = 127}, {x = 237}, {x = 347}
```

□

Βιβλιογραφία

[1] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[2] Euler, L. (1763). Theoremata arithmetica nova methodo demonstrata, Novi Commentarii academiae scientiarum Petropolitanae, 8, p. 74–104.

[3] Euler, L. (1741). Theorematum quorundam ad numeros primos spectantium demonstratio Commentarii academiae scientiarum Petropolitanae, 8, p. 141–146.

[4] Foster, L., & Lossers, O. (1987). E3014. The American Mathematical Monthly, 94(1), 74-74. doi:10.2307/2323511

[5] Gauss, F. (1801). Disquisitiones Arithmeticae. Leipzig: Gerh. Fleischer

[6] Jacobson, E., & Klein, E. (1987). E3089. The American Mathematical Monthly, 94(4), 385-386. doi:10.2307/2323111

[7] Lagrange, J.L. (1771). Démonstration d'un théorème nouveau concernant les nombres premiers, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres (Berlin), p. 125–137.

[8] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[9] Nicol, C., Selfridge, J., Callan, D., & Rogers, K. (1993). E3452. The American Mathematical Monthly, 100(4), 404-404. doi:10.2307/2324978

[10] Smith, P., & Students in the 1987 Mathematical Olympiad Program. (1988). E3210. The American Mathematical Monthly, 95(9), 879-880. doi:10.2307/2322918

[11] Waring, E. (1770). Meditationes Algebraicae, England: Cambridge

[12] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[13] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 5

Γραμμικές Ισοτιμίες και Συστήματα

Το πέμπτο κεφάλαιο εστιάζει στην επίλυση γραμμικών ισοτιμιών και στην επίλυση συστημάτων γραμμικών ισοτιμιών. Γίνεται η κατάλληλη ανάπτυξη μεθοδολογίας για τον υπολογισμό των λύσεων και στην τρίτη ενότητα παρουσιάζεται ο τρόπος επίλυσης τους με το υπολογιστικό πρόγραμμα maple. Το κεφάλαιο περιλαμβάνει και την επίλυση γρίφων με την χρήση συστημάτων γραμμικών ισοτιμιών.

5.1 Επίλυση Γραμμικών Ισοτιμιών

Ορισμός 5.1. Ας είναι $a, b, n \in \mathbb{Z}$ με $n > 1$. Μια ισοτιμία της μορφής

$$ax \equiv b \pmod{n},$$

όπου x ένας προσδιοριστέος ακέραιος, καλείται *γραμμική ισοτιμία*. Καλούμε *λύση* της παραπάνω ισοτιμίας κάθε κλάση ισοτιμίας $\overline{x}_0$ (ή $x_0 \pmod{n}$) η οποία περιέχει έναν ακέραιο ο οποίος την επαληθεύει (δηλαδή, υπάρχει $y \in \overline{x}_0$ με $ay \equiv b \pmod{n}$).

Η επίλυση γραμμικών ισοτιμιών βασίζεται στο θεώρημα που ακολουθεί.

Θεώρημα 5.1. *Η γραμμική ισοτιμία $ax \equiv b \pmod{n}$ έχει λύση αν και μόνον αν $\delta \mid b$, όπου $\delta = (a, n)$. Αν ο ακέραιος x_0 επαληθεύει την παραπάνω ισοτιμία, τότε οι λύσεις της είναι οι εξής:*

$$x \equiv x_0, x_0 + \frac{n}{\delta}, x_0 + 2\frac{n}{\delta}, \ldots, x_0 + (\delta - 1)\frac{n}{\delta} \pmod{n}.$$

Απόδειξη. Βλέπε [4, Κεφάλαιο 4, Θεώρημα 7.1] ή [3, Πρόταση 4.3.1, εδώ]. □

Συνεπώς, για λυθεί μια γραμμική ισοτιμία $\bmod n$ αρκεί να βρεθεί ένας ακέραιος x_0 που να την επαληθεύει. Στη συνέχεια θα δούμε τρεις τρόπους με τους οποίους μπορούμε να προσδιορίσουμε τον ακέραιο x_0. Ο πρώτος τρόπος εύρεσης λύσεων μιας γραμμικής ισοτιμίας $\bmod n$ είναι δοκιμάζοντας έναν αντιπρόσωπο από κάθε

κλάση $\bmod n$. Ο δεύτερος τρόπος είναι με την χρήση του Ευκλείδειου αλγόριθμου και ο τρίτος είναι με την χρήση του Θεωρήματος των Fermat-Euler ή της τάξης ενός ακεραίου.

Ας υποθέσουμε λοιπόν ότι έχουμε την γραμμική ισοτιμία

$$ax \equiv b \pmod{n}. \tag{5.1}$$

Αρχικά, για να ευκολυνθούμε στους υπολογισμούς, βρίσκουμε ακεραίους a', b' με $a' \equiv a \pmod{n}$, $b' \equiv b \pmod{n}$ και $a', b' \in \{0, \ldots, n-1\}$ ή $|a'| \leq n/2$, $|b'| \leq n/2$ και τους αντικαθιστούμε στην 5.1. Κατόπιν, υπολογίζουμε τον μέγιστο κοινό διαιρέτη $\delta = (a', n)$. Αν $\delta \nmid b'$, τότε η γραμμική ισοτιμία δεν έχει λύση. Αν $\delta \mid b'$, τότε η γραμμική ισοτιμία

$$\frac{a}{\delta} x \equiv \frac{b}{\delta} \left(\bmod \frac{n}{\delta} \right)$$

έχει μοναδική λύση $x \equiv x_0 \pmod{n/\delta}$. Ο ακέραιος x_0 επαληθεύει την 5.1 και επομένως, με την βοήθεια του Θεωρήματος 5.1, προσδιορίζουμε και τις υπόλοιπες της λύσεις $\bmod n$.

Στη συνέχεια θα θεωρήσουμε ότι οι γραμμικές ισοτιμίες είναι της μορφής

$$ax \equiv b \pmod{n}, \quad \text{με} \quad 0 \leq a, b < n \quad \text{και} \quad (a, n) = 1$$

και θα περιγράψουμε τις τρεις μεθόδους για την εύρεση της μοναδική τους λύσης.

Επίλυση Γραμμικής Ισοτιμίας - 1η Μέθοδος. Για την εύρεση της λύσης της παραπάνω γραμμικής ισοτιμίας, αν ο n είναι άρτιος αντικαθιστούμε διαδοχικά στο x τις τιμές

$$0, 1, 2, \ldots, \frac{n-2}{2}, \frac{n}{2}, -\frac{n-2}{2}, \ldots, -2, -1,$$

ενώ αν ο n είναι περιττός τις τιμές

$$0, 1, 2, \ldots, \frac{n-1}{2}, -\frac{n-1}{2}, \ldots, -2, -1,$$

μέχρι να βρούμε την τιμή x_0 που την επαληθεύει. Οπότε η μοναδική λύση σε αυτήν την περίπτωση είναι η $x \equiv x_0 \pmod{n}$.

Επίλυση Γραμμικής Ισοτιμίας - 2η Μέθοδος. Αρχικά εφαρμόζουμε τον Ευκλείδειο Αλγόριθμο για την διαίρεση του n από το a. Καθώς $(a, n) = 1$, έχουμε:

$$\begin{aligned} n &= \pi_1 \cdot a + u_1, \\ a &= \pi_2 \cdot u_1 + u_2, \\ \vdots &= \quad \vdots \\ u_{s-2} &= \pi_s \cdot u_{s-1} + 1. \end{aligned}$$

Στη συνέχεια, ξεκινώντας από την σχέση

$$1 = u_{s-1} - \pi_s \cdot u_{s-1}$$

και αντικαθιστώντας διαδοχικά τα $u_{s-1}, \ldots, u_1$ από τις σχέσεις που προκύπτουν από τα βήματα του Ευκλείδειου αλγορίθμου βρίσκουμε c και d έτσι, ώστε να ισχύει:

$$1 = ca + dn.$$

Οπότε, έχουμε $ca \equiv 1 \pmod{n}$ και επομένως έχουμε $bca \equiv b \pmod{n}$. Συνεπώς, η ζητούμενη λύση είναι $x \equiv bc \pmod{n}$.

Επίλυση Γραμμικής Ισοτιμίας - 3η Μέθοδος. Καθώς $(a, n) = 1$, υπάρχει θετικός ακέραιος r τέτοιος, ώστε να ισχύει $a^r \equiv 1 \pmod{n}$. Για παράδειγμα, ένας τέτοιος ακέραιος είναι η τάξη του a κατά μέτρο n ή ο $\phi(n)$. Πολλαπλασιάζοντας τα δύο μέλη της $ax \equiv b \pmod{n}$ με a^{r-1} παίρνουμε την λύση της γραμμικής ισοτιμίας, $x \equiv a^{r-1}b \pmod{n}$.

Παρατήρηση. Το βασικό ερώτημα που τίθεται είναι ποια από τις τρεις μεθόδους είναι η καταλληλότερη για να γίνουν υπολογισμοί με το χέρι. Η πρώτη μέθοδος που αφορά την αντικατάσταση του x με n ακεραίους είναι ιδανική για μικρό n. Πόσο μικρό; Όσο αντέχει κάποιος να κάνει υπολογισμούς με το χέρι... 10; 20; Η μέθοδος με την χρήση του Ευκλείδειου αλγόριθμου είναι σίγουρα ιδανικότερη για μεγάλα n. Η περίπτωση της επίλυσης γραμμικής ισοτιμίας με την χρήση της συνάρτησης Euler ή της χρήσης των ιδιοτήτων της τάξης ενός ακεραίου είναι λίγο ποιο δυσδιάκριτη. Η μεθοδος αυτή είναι μάλλον ιδανικότερη όταν το $\phi(n)$ είναι μικρό ή η τάξη του a είναι μικρή.

Ασκήσεις

Στη συνέχεια θα δούμε την επίλυση γραμμικών ισοτιμιών χρησιμοποιώντας τις μεθόδους που προαναφέρθηκαν.

Άσκηση 5.1. *Να λυθούν οι εξής γραμμικές ισοτιμίες:*

α) $45x - 2 \equiv 0 \pmod{7}$,

β) $-660x \equiv 121 \pmod{143}$,

γ) $255x \equiv 221 \pmod{374}$.

Απόδειξη. α) Αρχικά φέρνουμε την γραμμική ισοτιμία στην επιθυμητή μορφή. Έχουμε:

$$45x - 2 \equiv 0 \pmod{7} \iff 45x \equiv 2 \pmod{7} \iff 3x \equiv 2 \pmod{7}.$$

Εφόσον $(3, 7) = 1$, η γραμμική ισοτιμία έχει μοναδική λύση. Για να την βρούμε, δοκιμάζουμε διαδοχικά $x = 0, 1, 2, 3, -3, -2, -1$ και βρίσκουμε ότι επαληθεύεται για $x_0 = 3$. Άρα, η μοναδική της λύση είναι η $x \equiv 3 \pmod{7}$.

β) Καθώς $-660 \equiv 55 \pmod{143}$, έχουμε:

$$55x \equiv 121 \pmod{143}.$$

Επιπλέον, έχουμε ότι

$$(143, 55) = (13 \cdot 11, 5 \cdot 11) = 11.$$

Καθώς $11 \mid 121$ συνεπάγεται ότι η γραμμική ισοτιμία έχει 11 λύσεις. Διαιρώντας τους όρους της γραμμικής ισοτιμίας με 11, προκύπτει η γραμμική ισοτιμία

$$5x \equiv 11 \,(\mathrm{mod}\, 13),$$

η οποία έχει μοναδική λύση την οποία θα βρούμε κάνοντας χρήση του Ευκλείδειου αλγορίθμου. Έτσι, έχουμε:

$$\begin{aligned} 13 &= 2 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Στη συνέχεια, παίρνουμε:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3), \\ &= -1 \cdot 5 + 2 \cdot 3 = -1 \cdot 5 + 2 \cdot (13 - 2 \cdot 5), \\ &= 2 \cdot 13 - 5 \cdot 5. \end{aligned}$$

Άρα, ένας ακέραιος που επαληθεύει την $5x \equiv 11 \bmod 13$ και κατα επέκταση την $-660x \equiv 121 \bmod 143$ είναι ο $-5 \cdot 11 = -55$ ο οποίος είναι είναι ισότιμος (mod 13) με το 10. Συνεπώς, για να βρούμε τις λύσεις τις αρχικής μας γραμμικής ισοτιμίας υπολογίζουμε τους ακέραιους

$$x_0, x_0 + \frac{n}{\delta}, x_0 + 2\frac{n}{\delta}, \ldots, x_0 + (\delta - 1)\frac{n}{\delta}$$

για $x_0 = 10$, $n = 143$ και $\delta = 11$. Δηλαδή, οι λύσεις είναι:

$$x \equiv 10, 23, 36, 49, 62, 75, 88, 101, 114, 127, 140 \,(\mathrm{mod}\, 143).$$

γ) Η γραμμική ισοτιμία είναι στην επιθυμητή μορφή και στη συνέχεια υπολογίζουμε την πρωτογενή ανάλυση του 374 και του 255 για να βρούμε τον μέγιστο κοινό διαιρέτη. Έχουμε:

$$374 = 2 \cdot 11 \cdot 17, \quad 255 = 3 \cdot 5 \cdot 17.$$

Άρα, $(374, 255) = 17$ και εφόσον $17 \mid 221$ συνεπάγεται ότι υπάρχουν ακριβώς 17 λύσεις.

Διαιρώντας με 17 τους όρους της αρχικής ισοτιμίας προκύπτει η ισοδύναμη γραμμική ισοτιμία

$$15x \equiv 13 \,(\mathrm{mod}\, 22).$$

Καθώς $(15, 22) = 1$, από το Θεώρημα των Fermat-Euler προκύπτει:

$$15^{\phi(22)} \equiv 1 \,(\mathrm{mod}\, 22).$$

Έχουμε $\phi(22) = 10$ και επομένως έχουμε:

$$15^{10} \equiv 1 \,(\mathrm{mod}\, 22).$$

Επιπλέον, $\mathrm{ord}_{22}(15) \mid \phi(22)$ που συνεπάγεται ότι $\mathrm{ord}_{22}(15) \in \{1, 2, 5, 10\}$. Στη συνέχεια, υπολογίζουμε:

$$15^2 \equiv (-7)^2 \equiv 5 \,(\mathrm{mod}\, 22),$$
$$15^5 \equiv 15^4 \cdot 15 \equiv 5^2 \cdot (-7) \equiv 3 \cdot (-7) \equiv -21 \equiv 1 \,(\mathrm{mod}\, 22).$$

΄Αρα $\mathrm{ord}_{22}(15) = 5$, και επομένως η λύση της γραμμικής ισοτιμίας είναι:

$$x_0 \equiv 13 \cdot 15^4 \equiv (-9) \cdot (-7)^4 \equiv (-9) \cdot 5^2 \equiv -27 \equiv 17 \,(\mathrm{mod}\, 22).$$

Συνεπώς, οι λύσεις της αρχικής γραμμικής ισοτιμίας είναι:

$$x \equiv 17 + 22k \,(\mathrm{mod}\, 374), \quad (k = 0, \ldots, 16).$$

□

΄Ασκηση 5.2. *΄Ενας πλασιέ επισκέπτεται μία πόλη κάθε 5 μήνες. Είναι δυνατόν η επίσκεψή του να πραγματοποιηθεί τον μήνα Μάρτιο;*

Απόδειξη. Συμβολίζουμε τους μήνες Ιανουάριο,..., Δεκέμβριο με τους αριθμούς $0, \ldots,$ αντίστοιχα. Ας υποθέσουμε ότι η πρώτη επίσκεψη του πλασιέ πραγματοποιήθηκε τον μήνα x_0. Οπότε, σ΄ αυτή την πόλη ξαναβρίσκεται μετά από $5y$ μήνες $y = 1, 2, \ldots$. ΄Ετσι, για να είναι Μάρτιος ο μήνας της επίσκεψής του, θα πρέπει να έχουμε $x_0 + 5y \equiv 2 \,(\mathrm{mod}\, 12)$. Δηλαδή, θα πρέπει η γραμμική ισοτιμία $5y \equiv 2 - x_0 \,(\mathrm{mod}\, 12)$ να έχει λύση. Καθώς όμως έχουμε $(5, 12) = 1$, η γραμμική ισοτιμία έχει λύση και κατά συνέπεια μία επίσκεψή του θα πραγματοποιηθεί τον μήνα Μάρτιο. □

5.2 Επίλυση Συστημάτων Γραμμικών Ισοτιμιών

Ορισμός 5.2. Ας είναι

$$\begin{aligned} a_1 x &\equiv c_1 \,(\mathrm{mod}\, m_1) \\ &\vdots \\ a_k x &\equiv c_k \,(\mathrm{mod}\, m_k) \end{aligned} \tag{5.2}$$

ένα σύστημα γραμμικών ισοτιμιών. Κάθε ακέραιος που επαληθεύει κάθε μία από τις γραμμικές ισοτιμίες καλείται *λύση* του συστήματος. Δύο συστήματα γραμμικών ισοτιμιών καλούνται *ισοδύναμα* όταν έχουν ακριβώς τις ίδιες λύσεις.

Θα λέμε ότι το παραπάνω σύστημα έχει λύση την $x \equiv \alpha \,(\mathrm{mod}\, \omega)$, αν όλα τα στοιχεία της κλάσης του α κατά μέτρο ω είναι λύσεις του.

Για να έχει το σύστημα (5.2) λύση, θα πρέπει κάθε γραμμική ισοτιμία του συστήματος να έχει λύση. Δηλαδή, θα πρέπει να ισχύει $\delta_i = (a_i, m_i) \mid c_i$ $(i = 1, \ldots, k)$. Στην περίπτωση όπου όλες οι ισοτιμίες έχουν λύση, για κάθε $i = 1, \ldots, k$ διαιρούμε την i-οστή ισοτιμία με δ_i και θέτουμε $\alpha_i = a_i/\delta_i$, $\gamma_i = c_i/\delta_i$, $n_i = m_i/\delta_i$. ΄Ετσι, προκύπτει το παρακάτω σύστημα που είναι ισοδύναμο με το αρχικό:

$$\begin{aligned} \alpha_1 x &\equiv \gamma_1 \,(\mathrm{mod}\, n_1), \\ &\vdots \\ \alpha_k x &\equiv \gamma_k \,(\mathrm{mod}\, n_k). \end{aligned} \tag{5.3}$$

Αν κάποιος από τους ακεραίους α_i, γ_i δεν ανήκει στο σύνολο $\{0, \ldots, n_i - 1\}$ μπορούμε να τον αντικαταστήσουμε με τον ισότιμό του μέσα σ΄ αυτό, ώστε οι πράξεις που θα κάνουμε κατόπιν να είναι ευκολότερες. Καθώς $(\alpha_i, n_i) = 1$, η γραμμική ισοτιμία $\alpha_i x \equiv \gamma_i \pmod{n_i}$ έχει μοναδική λύση $x \equiv b_i \pmod{n_i}$ $(i = 1, \ldots, k)$. Επομένως, το προηγούμενο σύστημα είναι ισοδύναμο με το εξής:

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv b_k \pmod{n_k}. \end{aligned} \tag{5.4}$$

Έτσι, βλέπουμε ότι η επίλυση ενός συστήματος γραμμικών ισοτιμιών ανάγεται στην επίλυση ενός συστήματος της μορφής (5.4).

Στην περίπτωση όπου τα μέτρα των ισοτιμιών είναι πρώτα μεταξύ τους ανά δύο, έχουμε το παρακάτω θεώρημα που είναι γνωστό ως Κινέζικο Θεώρημα Υπολοίπων.

Θεώρημα 5.2. *Ας είναι $b_1, \ldots, b_k$ ακέραιοι και $n_1, \ldots, n_k$ ακέραιοι > 1, πρώτοι μεταξύ τους ανά δύο. Τότε, το σύστημα γραμμικών ισοτιμιών (5.4) έχει μοναδική λύση* $\bmod (n_1 \cdots n_k)$.

Απόδειξη. Βλέπε [4, Κεφάλαιο 4, Πρόταση 8.1] ή [3, Πρόταση 4.3.5, εδώ]. □

Από την απόδειξη του παραπάνω θεωρήματος προκύπτει η εξής μέθοδος εύρεσης μίας λύσης του συστήματος (5.4) και κατά συνέπεια όλων των λύσεών του.

Επίλυση Συστήματος με το Κινέζικο Θεώρημα Υπολοίπων.

1) Υπολογίζουμε τις τιμές $N_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$ $(i = 1, \ldots, k)$.
2) Υπολογίζουμε έναν ακέραιο M_i που επαληθεύει την γραμμική ισοτιμία $N_i x \equiv 1 \pmod{n_i}$ $(i = 1, \ldots, k)$.
3) Υπολογίζουμε την τιμή $x_0 = \sum_{i=1}^{k} b_i N_i M_i$.
4) Οι λύσεις του συστήματος είναι οι ακέραιοι της κλάσης $x_0 \pmod{n_1 \cdots n_k}$.

Για την γενική περίπτωση έχουμε το παρακάτω θεώρημα.

Θεώρημα 5.3. *Το σύστημα γραμμικών ισοτιμιών (5.4) έχει λύση, αν και μόνον αν, για κάθε ζεύγος δεικτών i, j ισχύει $(n_i, n_j) \mid b_i - b_j$. Αν x_0 είναι μια λύση του συστήματος, τότε το σύνολο των λύσεών του είναι η κλάση του* $x_0 \pmod{[n_1, \ldots, n_k]}$.

Απόδειξη. Βλέπε [4, Κεφάλαιο 4, Θεώρημα 8.1] ή [3, Πρόταση 4.3.7, εδώ]. □

Στην περίπτωση όπου το σύστημα έχει λύση, με την μέθοδο που ακολουθεί μπορούμε να υπολογίσουμε την λύση του συστήματος.

Επίλυση Συστήματος με Αντικατάσταση. Για την επίλυση του συστήματος της μορφής (5.4) ακολουθούμε την εξής διαδικασία:

Πρώτα ελέγχουμε για κάθε ζεύγος δεικτών $i, j = 1, \ldots, k$, με $i \neq j$, αν ισχύει η σχέση $(n_i, n_j) \mid b_i - b_j$. Αν για κάποιο ζεύγος δεν ισχύει, τότε το σύστημα δεν έχει λύση. Διαφορετικά, συνεχίζουμε την διαδικασία επίλυση του συστήματος, επιλύοντας διαδοχικά τις ισοτιμίες ανά δύο. Δηλαδή, χωρίς περιορισμό της γενικότητας επιλύουμε

το σύστημα των δύο πρώτων ισοτιμιών και την λύση τους την κάνουμε σύστημα δύο γραμμικών ισοτιμιών με την τρίτη γραμμική ισοτιμία και την λύση τους την κάνουμε σύστημα δύο γραμμικών ισοτιμιών με την τέταρτη γραμμική ισοτιμία κ.ο.κ. Έτσι, η επίλυση ενός συστήματος k γραμμικών ισοτιμιών με την μέθοδο της αντικατάστασης ανάγεται στην επίλυση $k-1$ συστημάτων δύο γραμμικών ισοτιμιών.

Στη συνέχεια παρατίθεται η διαδικασία επίλυσης συστήματος δύο γραμμικών ισοτιμιών

$$x \equiv b_1 \pmod{n_1}, \quad x \equiv b_2 \pmod{n_2}.$$

1) Η πρώτη ισοτιμία ικανοποιείται από όλους τους ακεραίους της μορφής $kn_1 + b_1$, όπου $k \in \mathbb{Z}$. Επομένως, θέτουμε $x = n_1k + b_1$ στη δεύτερη ισοτιμία και έτσι προκύπτει η γραμμική ισοτιμία $n_1k \equiv b_2 - b_1 \pmod{n_2}$ (με προσδιοριστέα ποσότητα το k).
2) Βρίσκουμε έναν ακέραιο k_0 ο οποίος επαληθεύει την προηγούμενη γραμμική ισοτιμία.
3) Υπολογίζουμε $x_0 = k_0n_1 + b_1$.
4) Η λύση του συστήματος είναι η $x \equiv x_0 \pmod{[n_1, n_2]}$.

Ασκήσεις

Άσκηση 5.3. *Να λυθούν τα συστήματα γραμμικών ισοτιμιών:*

α) $x \equiv 1 \pmod 6$, $x \equiv 3 \pmod 4$,
β) $x \equiv 4 \pmod 5$, $x \equiv -27 \pmod{22}$, $x \equiv -31 \pmod{39}$,
γ) $5x \equiv 3 \pmod 8$, $22x \equiv 10 \pmod{14}$, $15x \equiv 25 \pmod{20}$.

Απόδειξη. α) Οι γραμμικές ισοτιμίες του συστήματος είναι στην επιθυμητή μορφή. Έχουμε $(6,4) = 2$ και $2 \mid 3 - 1$. Οπότε, σύμφωνα με το Θεώρημα 5.3, το σύστημα έχει λύση. Από την πρώτη ισοτιμία έχουμε ότι $x = 6k + 1$. Αντικαθιστώντας το x στη δεύτερη ισοτιμία, έχουμε:

$$6k + 1 \equiv 3 \pmod 4.$$

Έτσι, παίρνουμε την ισοτιμία $2k \equiv 2 \pmod 4$ η οποία επαληθεύεται για $k = 1$. Οπότε, μία λύση του συστήματος είναι η $x_0 = 6 \cdot 1 + 1 = 7$. Επομένως, από το Θεώρημα 5.3 έχουμε ότι η λύση του συστήματος είναι $x \equiv 7 \pmod{[4,6]}$ ή $x \equiv 7 \pmod{12}$.

β) Κάνοντας χρήση των ιδιοτήτων των ισοτιμιών το αρχικό σύστημα γράφεται ισοδύναμα:

$$x \equiv 4 \pmod 5 \quad x \equiv 17 \pmod{22}, \quad x \equiv 8 \pmod{39}.$$

Καθώς το 5, το 22 και το 39 είναι πρώτοι μεταξύ τους ανά δύο, μπορούμε να χρησιμοποιήσουμε την μέθοδο του Κινέζικου Θεωρήματος Υπολοίπων. Θέτουμε $n_1 = 5$, $n_2 = 22$, $n_3 = 39$ και $b_1 = 4$, $b_2 = 17$, $b_3 = 8$. Κατόπιν, υπολογίζουμε:

$$N_1 = n_2n_3 = 858, \quad N_2 = n_1n_3 = 195, \quad N_3 = n_1n_2 = 110.$$

Στη συνέχεια, λύνουμε τις ισοτιμίες $N_ix \equiv 1 \pmod{n_i}$ $(i = 1, 2, 3)$, δηλαδή τις ισοτιμίες

$$858x \equiv 1 \pmod 5, \quad 195x \equiv 1 \pmod{22}, \quad 110x \equiv 1 \pmod{39}$$

που είναι ισοδύναμες με τις εξής:

$$3x \equiv 1 \pmod 5, \quad 19x \equiv 1 \pmod{22}, \quad 32x \equiv 1 \pmod{39}.$$

Έυκολα βρίσκουμε ότι τα $M_1 = 2$, $M_2 = 7$, $M_3 = 11$ επαληθεύουν, αντίστοιχα, τις παραπάνω ισοτιμίες. Έτσι, υπολογίζουμε την ποσότητα

$$x_0 = b_1N_1M_1 + b_2N_2M_2 + b_3N_3M_3 = 6864 + 23205 + 9680 = 39749.$$

Οπότε, η λύση του συστήματος είναι:

$$x \equiv 39749 \equiv 1139 \,(\mathrm{mod}\, 4290).$$

γ) Κατ΄ αρχάς θα εξετάσουμε αν κάθε μία από τις γραμμικές ισοτιμίες του συστήματος έχει λύση. Για την πρώτη έχουμε $(5, 8) = 1 \mid 3$ και επομένως έχει λύση. Για την δεύτερη ισχύει $(22, 14) = 2 \mid 10$ και κατά συνέπεια έχει λύση. Τέλος, $(15, 20) = 5 \mid 25$ και επομένως και αυτή έχει λύση. Απλοποιώντας το σύστημα όπως δείξαμε παραπάνω προκύπτει το εξής σύστημα που είναι ισοδύναμο με το αρχικό:

$$5x \equiv 3 \,(\mathrm{mod}\, 8), \quad 4x \equiv 5 \,(\mathrm{mod}\, 7), \quad 3x \equiv 1 \,(\mathrm{mod}\, 4).$$

Λύνουμε κάθε μία από τις γραμμικές ισοτιμίες του συστήματος και έτσι προκύπτει το εξής ισοδύναμο σύστημα.

$$x \equiv 7 \,(\mathrm{mod}\, 8), \quad x \equiv 3 \,(\mathrm{mod}\, 7), \quad x \equiv 3 \,(\mathrm{mod}\, 4).$$

Το σύστημα έχει λύση, καθώς ισχύει:

$$(8, 7) \mid 7 - 3, \quad (8, 4) \mid 7 - 3, \quad (7, 4) \mid 3 - 3.$$

Θα το επιλύσουμε το παραπάνω σύστημα με την μέθοδο της αντικατάστασης. Αρχίζοντας από την πρώτη ισοτιμία θέτουμε $x = 7 + 8k$ και αντικαθιστώντας στη δεύτερη ισοτιμία παίρνουμε $k \equiv 3 \,(\mathrm{mod}\, 7)$. Οπότε, για $k_0 = 3$ έχουμε $x_0 = 7 + 8 \cdot 3 = 31$. Επίσης, ισχύει $[8, 7] = 56$. Έτσι, η λύση του συστήματος των δύο πρώτων ισοτιμιών είναι:

$$x \equiv 31 \,(\mathrm{mod}\, 56).$$

Στη συνέχεια, θέτουμε $x = 31 + 56\ell$ και μετά από αντικατάσταση στη τρίτη ισοτιμία προκύπτει:

$$56\ell \equiv -28 \,(\mathrm{mod}\, 4).$$

Καθώς $56 \equiv -28 \equiv 0 \,(\mathrm{mod}\, 4)$, έπεται $0\ell \equiv 0 \,(\mathrm{mod}\, 4)$ και επομένως η ισοτιμία αυτή επαληθεύεται για κάθε ακέραιο ℓ. Άρα, η λύση του συστήματός μας είναι:

$$x \equiv 31 \,(\mathrm{mod}\, 56).$$

□

5.3 Συνδυαστικές Ασκήσεις

Άσκηση 5.4. (*Πρόβλημα του Brahmagupta, 7ος αιώνας*) *Όταν παίρνουμε αυγά από ένα καλάθι ανά: 2, 3, 4, 5, 6 κάθε φορά, τότε μένουν, αντίστοιχα: 1, 2, 3, 4, 5 αυγά στο καλάθι. Όταν όμως παίρνουμε ανά 7 δεν μένει κανένα. Να υπολογιστεί ο ελάχιστος αριθμός αυγών που θα πρέπει να περιέχει το καλάθι.*

Απόδειξη. Ας είναι x ο αριθμός των αυγών που περιέχει το καλάθι. Από την πρώτη φορά κατά την οποία παίρνουμε τα αυγά ανά δύο, έχουμε $x = 2k_1 + 1$, όπου $k_1 \in \mathbb{Z}$. Από την δεύτερη φορά, προκύπτει $x = 3k_2 + 2$, όπου $k_2 \in \mathbb{Z}$. Από την τρίτη, $x = 4k_3 + 3$, όπου $k_3 \in \mathbb{Z}$, και από τις υπόλοιπες τρεις φορές, παίρνουμε $x = 5k_4 + 4$, $x = 6k_5 + 5$, $x = 7k_6$, όπου $k_4, k_5, k_6 \in \mathbb{Z}$, αντίστοιχα. Έτσι, έχουμε το σύστημα γραμμικών ισοτιμιών:

$$\begin{aligned} x &\equiv 1 \,(\mathrm{mod}\, 2) \\ x &\equiv 2 \,(\mathrm{mod}\, 3) \\ x &\equiv 3 \,(\mathrm{mod}\, 4) \\ x &\equiv 4 \,(\mathrm{mod}\, 5) \\ x &\equiv 5 \,(\mathrm{mod}\, 6) \\ x &\equiv 0 \,(\mathrm{mod}\, 7). \end{aligned}$$

Ο ζητούμενος ελάχιστος αριθμός αυγών είναι η μικρότερη θετική λύση αυτού του συστήματος. Κατ΄ αρχάς θα εξετάσουμε αν αυτό έχει λύση. Έχουμε:

$$\begin{gathered} (2,3) = 1,\ (2,4) = 2 \mid 3-1,\ (2,5) = 1,\ (2,6) = 2 \mid 5-1,\ (2,7) = 1, \\ (3,4) = (3,5) = 1,\ (3,6) = 3 \mid 5-2,\ (3,7) = 1,\ (4,5) = 1, \\ (4,6) = 2 \mid 5-3,\ (4,7) = 1,\ (5,6) = (5,7) = (6,7) = 1. \end{gathered}$$

Συνεπώς, το σύστημα έχει λύση. Παρατηρούμε ότι η λύση του συστήματος των δύο πρώτων ισοτιμιών είναι $x \equiv 5 \,(\mathrm{mod}\, 6)$. Καθώς αυτή η ισοτιμία υπάρχει στο αρχικό μας σύστημα, αυτό είναι ισοδύναμο με το παρακάτω:

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\, 4) \\ x &\equiv 4 \,(\mathrm{mod}\, 5) \\ x &\equiv 5 \,(\mathrm{mod}\, 6) \\ x &\equiv 0 \,(\mathrm{mod}\, 7). \end{aligned}$$

Από την τελευταία ισοτιμία έχουμε $x = 7k$, όπου $k \in \mathbb{Z}$. Αντικαθιστούμε την τιμή του x στην προτελευταία ισοτιμία και παίρνουμε $k \equiv 5 (\mathrm{mod}\, 6)$. Οπότε, για $x = 35$ επαληθεύεται το σύστημα το δύο τελευταίων ισοτιμιών και κατά συνέπεια η λύση του είναι $x \equiv 35 \,(\mathrm{mod}\, 42)$. Άρα, το σύστημά μας είναι ισοδύναμο με το εξής:

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\, 4) \\ x &\equiv 4 \,(\mathrm{mod}\, 5) \\ x &\equiv 35 \,(\mathrm{mod}\, 42). \end{aligned}$$

Από την τελευταία ισοτιμία έχουμε $x = 42k + 35$, όπου $k \in \mathbb{Z}$, και αντικαθιστώντας την τιμή του x στη δεύτερη ισοτιμία προκύπτει $2k \equiv 4 \,(\mathrm{mod}\, 5)$. Για $k = 2$, η ισοτιμία αυτή επαληθεύεται. Επομένως, η τιμή $x_0 = 42 \cdot 2 + 35 = 119$ είναι μία λύση του συστήματος των δύο τελευταίων ισοτιμιών, και κατά συνέπεια η λύση του είναι $x \equiv 119 \,(\mathrm{mod}\, 210)$. Άρα, το αρχικό σύστημα είναι ισοδύναμο με το παρακάτω:

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\, 4) \\ x &\equiv 119 \,(\mathrm{mod}\, 210). \end{aligned}$$

Από την δεύτερη ισοτιμία έχουμε $x = 210k + 119$. Αντικαθιστώντας την τιμή αυτή στη πρώτη ισοτιμία, παίρνουμε $2k \equiv 0 \pmod 4$. Για $k = 0$, η ισοτιμία επαληθεύεται και επομένως μία λύση του συστήματος είναι η $x_0 = 119$. Συνεπώς, η λύση του αρχικού συστήματος είναι $x \equiv 119 \pmod{840}$. Έτσι, συμπεραίνουμε ότι ο ελάχιστος αριθμός αυγών που περιέχει το καλάθι είναι 119. □

΄Ασκηση 5.5. (*Το πρόβλημα του κινέζου μάγειρα*). *Σ΄ ένα πλιάτσικο 17 πειρατές αρπάζουν ένα μπαούλο γεμάτο χρυσές λίρες (ίσης αξίας). Αποφασίζουν να τις μοιράσουν σε ίσα μέρη και να δώσουν το υπόλοιπο στον κινέζο μάγειρα του καραβιού τους. Σ΄ αυτόν αντιστοιχούν 3 λίρες. Σε μία ναυμαχία σκοτώνονται 6 από αυτούς. Στον μάγειρα αντιστοιχούν τότε 4 λίρες. Κατόπιν, σ΄ ένα ναυάγιο σώζονται μόνο 6 από αυτούς, το μπαούλο και ο μάγειρας. Στον μάγειρα αντιστοιχούν τότε 5 λίρες. Κατόπιν, ο μάγειρας δηλητηριάζει τους πειρατές και παίρνει το μπαούλο. Πόσες λίρες τουλάχιστον περιέχει το μπαούλο;*

Απόδειξη. Ας είναι x το πλήθος των λιρών που περιέχει το μπαούλο. Από την πρώτη μοιρασιά έχουμε $x = 17m_1 + 3$, όπου $m_1 \in \mathbb{Z}$. Στη δεύτερη μοιρασιά έχουν μείνει 11 πειρατές και έτσι έχουμε $x = 11m_2 + 4$, όπου $m_2 \in \mathbb{Z}$. Η τρίτη μοιρασιά δίνει $x = 6m_3 + 5$, όπου $m_3 \in \mathbb{Z}$. Έτσι,για να βρούμε το ελάχιστο πλήθος λιρών που περιέχει το μπαούλο, αρκεί να λύσουμε το εξής σύστημα γραμμικών ισοτιμιών:

$$x \equiv 3 \pmod{17}$$
$$x \equiv 4 \pmod{11}$$
$$x \equiv 5 \pmod 6.$$

Παρατηρούμε ότι τα μέτρα των ισοτιμιών, 17, 11, 6 είναι πρώτα μεταξύ τους ανά δύο και κατά συνέπεια το σύστημα έχει λύση. Από την πρώτη ισοτιμία έχουμε $x = 17k + 3$, $k \in \mathbb{Z}$. Αντικαθιστούμε την τιμή του x στη δεύτερη ισοτιμία και παίρνουμε την γραμμική ισοτιμία

$$6k \equiv 1 \pmod{11}.$$

Η ισοτιμία αυτή επαληθεύεται για $k = 2$. Οπότε, το σύστημα των δύο πρώτων ισοτιμιών επαληθεύεται για $x = 37$ και επομένως η λύση του είναι $x \equiv 37 \pmod{187}$. Έτσι, το αρχικό μας σύστημα είναι ισοδύναμο με το παρακάτω:

$$x \equiv 37 \pmod{187}$$
$$x \equiv 5 \pmod 6.$$

Θέτουμε $x = 187l + 37$ στη δεύτερη ισοτιμία και παίρνουμε:

$$l \equiv 4 \pmod 6.$$

Άρα, το σύστημα επαληθεύεται για $x = 785$ και επομένως η λύση του είναι $x \equiv 785 \pmod{1122}$. Συνεπώς, το μπαούλο περιέχει τουλάχιστον 785 λίρες. □

5.4 Θεωρία Αριθμών με Maple

Ας είναι

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

ένα σύστημα $k \geq 2$ γραμμικών ισοτιμιών. Αν το σύστημα έχει λύσεις για να προσδιορίσουμε τις λύσεις του αρκεί να βρούμε ένα ακέραιο a που να επαληθεύει όλες τις γραμμικές ισοτιμίες. Τότε, οι λύσεις του συστήματος είναι οι ακέραιοι της κλάσης $a \pmod{(n_1, \ldots, n_k)}$. Στην περίπτωση που $k = 2$, η εντολή με την οποία υπολογίζουμε τον ακέραιο a είναι η mcombine(n_1, b_1, n_2, b_2). Στην περίπτωση όπου έχουμε $k \geq 2$ γραμμικές ισοτιμίες, όπου ισχύουν οι προϋποθέσεις του Θεωρήματος του Κινέζου, η εντολή με την οποία υπολογίζουμε τον ακέραιο a είναι η chrem$([b_1, \ldots mb_k], [n_1, \ldots, n_k])$. Όταν το σύστημα δεν έχει λύση οι εντολές επιστρέφουν FAIL.

Άσκηση 5.6. *Να λυθούν τα συστήματα γραμμικών ισοτιμιών*

α) $x \equiv 1 \pmod 6$, $x \equiv 3 \pmod 4$.

β) $x \equiv 4 \pmod 5$, $x \equiv -27 \pmod{22}$, $x \equiv -31 \pmod{39}$.

γ) $5x \equiv 3 \pmod 8$, $22x \equiv 10 \pmod{14}$, $15x \equiv 25 \pmod{20}$.

Απόδειξη. Με κώδικα Maple:

```
mcombine(6, 1, 4, 3);
                                7
chrem([4, -27, -31], [5, 22, 39]);
                               1139
```

□

Βιβλιογραφία

[1] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[2] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[3] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[4] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 6

Πολυωνυμικές Ισοτιμίες - Αρχικές Ρίζες

Το κεφάλαιο αυτό αφορά στην επίλυση ισοτιμιών γενικότερα. Η πρώτη ενότητα αφορά την επίλυση πολυωνυμικών ισοτιμιών ενώ στη συνέχεια εισάγονται οι έννοιες των αρχικών ριζών και των δεικτών. Στη τρίτη ενότητα περιγράφεται ο τρόπος επίλυσης εκθετικών, πολυωνυμικών αλλά και γραμμικών ισοτιμιών με τη χρήση δεικτών.

6.1 Επίλυση Πολυωνυμικών Ισοτιμιών

Ορισμός 6.1. Μια ισοτιμία της μορφής

$$f(x) \equiv 0 \,(\mathrm{mod}\, n), \tag{6.1}$$

όπου $f(x) \in \mathbb{Z}[x]$, καλείται *πολυωνυμική ισοτιμία*. Αν $f(x_0) \equiv 0 \pmod{n}$ για κάποιο $x_0 \in \mathbb{Z}$, τότε λέμε ότι ο ακέραιος x_0 *επαληθεύει* την (6.1). Η κλάση του $x_0 \bmod n$ καλείται *λύση* της (6.1). Δύο πολυωνυμικές ισοτιμίες καλούνται *ισοδύναμες* αν έχουν ακριβώς τις ίδιες λύσεις. Ο βαθμός μια πολυωνυμικής ισοτιμίας είναι ίσος με το βαθμός του μεγιστοβάθμιου όρου της $f(x) = a_k x^k + \cdots + a_1 x + a_0$ με $a_i \not\equiv 0 \pmod{n}$.

Πρόταση 6.1. *Ας είναι $f(x) \equiv 0 \pmod{p}$, όπου $\deg f(x) \geq p$ και p πρώτος. Υπάρχει ισοδύναμη ισοτιμία $g(x) \equiv 0 \pmod{p}$, όπου $\deg g(x) < p$.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 5, Πρόταση 2.1] ή [5, Πρόταση 4.7.3, εδώ]. □

Θεώρημα 6.1. (*Θεώρημα του Lagrange*) *Έστω p πρώτος και*

$$f(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_k$$

ένα πολυώνυμο βαθμού $k \geq 1$, με ακέραιους συντελεστές και $a_0 \not\equiv 0 \pmod{p}$. Τότε, η πολυωνυμική ισοτιμία

$$f(x) \equiv 0 \pmod{p}$$

έχει το πολύ k λύσεις.

Απόδειξη. Βλέπε [6, Κεφάλαιο 5, Πόρισμα 2.1] ή [5, Πρόταση 4.7.4, εδώ]. □

Στη συνέχεια παραθέτουμε μία μέθοδο επίλυση της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod{n}$, η οποία διακρίνεται σε τρία στάδια:

- την επίλυση πολυωνυμικής ισοτιμίας mod p, όπου p πρώτος,
- την επίλυση πολυωνυμικής ισοτιμίας mod p^r, όπου $r \in \mathbb{Z}^+$ και
- την επίλυση πολυωνυμικής ισοτιμίας mod n για κάθε $n > 1$.

Στη συνέχεια, παρουσιάζεται ο τρόπος επίλυσης της πολυωνυμικής ισοτιμίας

$$a_s x^s + \cdots + a_1 x + a_0 \equiv 0 \pmod{n}, \tag{6.2}$$

όπου $a_0, \ldots, a_s \in \mathbb{Z}$, σε κάθε ένα από τα παραπάνω στάδια.

Επίλυση Πολυωνυμικής Ισοτιμίας για $n = p$. Το πρώτο βήμα που γίνεται για την επίλυση της (6.2) είναι η μετατροπή της σε μια ισοδύναμη πολυωνυμική ισοτιμία της μορφής

$$a_k x^k + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \tag{6.3}$$

όπου $0 \leq a_i, k < p$. Ο περιορισμός των συντελεστών a_i ανάμεσα στο 0 και το p επιτυγχάνεται με απλή εφαρμογή των ιδιοτήτων των ισοτιμιών, ενώ η μείωση του βαθμού του πολυωνύμου με την χρήση του Πορίσματος 4.2, δηλαδή την σχέση $x^p \equiv x \pmod{p}$. Στην συνέχεια αντικαθιστούμε στο x αντιπροσώπους από όλες τις κλάσεις mod p. Οι κλάσεις των αντιπροσώπων που επαληθεύουν την πολυωνυμική ισοτιμία είναι οι λύσεις της. Σύμφωνα με το Θεώρημα του Lagrange (6.1) το πλήθος των λύσεων της (6.3) είναι το πολύ k.

Επίλυση Πολυωνυμικής Ισοτιμίας για $n = p^r$. Για την επίλυση μιας πολυωνυμικής ισοτιμίας mod p^r παρατηρούμε ότι αν ο ακέραιος x_0 επαληθεύει την ισοτιμία $f(x) \equiv 0 \pmod{p^r}$, τότε επαληθεύει και την ισοτιμία $f(x) \equiv 0 \pmod{p^k}$ για κάθε $k < r$. Το αντίστροφο δεν ισχύει. Οπότε, από τις λύσεις της ισοτιμίας $f(x) \equiv 0 \pmod{p}$, μπορούμε να συνάγουμε τις λύσεις της $f(x) \equiv 0 \pmod{p^r}$. Αυτό μπορούμε να το επιτύχουμε με τον εξής τρόπο. Κατ΄ αρχάς προσδιορίζουμε τις λύσεις της $f(x) \equiv 0 \pmod{p}$, $x \equiv x_1, \ldots, x_r \pmod{p}$. Στη συνέχεια, θέτουμε $x = x_i + pt$, $i = 1, \ldots, r$, $t \in \mathbb{Z}$ και αντικαθιστούμε το x στη $f(x) \equiv 0 \pmod{p^2}$ την οποία επιλύουμε με την σειρά της (ως προς t). Η διαδικασία αυτή επαναλαμβάνεται μέχρι την ισοτιμία $f(x) \equiv 0 \pmod{p^r}$. Η μέθοδος αυτή είναι δυνατόν να επιταχυνθεί, με την χρήση του θεωρήματος που ακολουθεί. Για τον σκοπό αυτό θα χρειαστεί να υπενθυμίσουμε τον ορισμό της τυπικής παραγώγου ενός πολυωνύμου. Ας είναι $f(x) = a_n x^n + \cdots + a_1 x + a_0$ ένα πολυώνυμο με ακέραιους συντελεστές. Η *τυπική παράγωγος* του $f(x)$ είναι το πολυώνυμο $f'(x) = n a_n x^{n-1} + \cdots + a_1$.

Θεώρημα 6.2. *Ας είναι*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p^{r-1}}$$

μία πολυωνυμική ισοτιμία, όπου p πρώτος, $r \geq 2$ και $x \equiv b_0 \pmod{p^{r-1}}$ μία λύση της. Έχουμε τις εξής περιπτώσεις:

(α) *Αν* $p \mid f'(b_0)$ *και* $p^r \nmid f(b_0)$, *τότε η* $f(x) \equiv 0 \pmod{p^r}$ *δεν έχει λύσεις.*
(β) *Αν* $p \mid f'(b_0)$ *και* $p^r \mid f(b_0)$, *τότε η* $f(x) \equiv 0 \pmod{p^r}$ *έχει ακριβώς* p *λύσεις που είναι οι* $x_t \equiv tp^{r-1} + b_0 \pmod{p^r}$, *όπου* $t = 0, 1, \ldots, p-1$.
(γ) *Αν* $p \nmid f'(b_0)$, *τότε υπάρχει μοναδική λύση της* $f(x) \equiv 0 \pmod{p^r}$ *που είναι η* $x_0 \equiv tp^{r-1} + b_0 \pmod{p^r}$, *όπου* t *ένας ακέραιος που επαληθεύει την γραμμική ισοτιμία* $f'(b_0)t \equiv (-f(b_0)/p^{r-1}) \pmod{p}$.

Απόδειξη. Βλέπε [6, Κεφάλαιο 5, Θεώρημα 3.1] ή [5, Πρόταση 4.7.2, εδώ]. □

Τα βήματα επίλυσης της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod{p^r}$ βάσει του Θεωρήματος 6.2 έχουν ως εξής:

1) Βρίσκουμε όλες τις λύσεις της $f(x) \equiv 0 \pmod{p}$. Ας είναι $x_1, \ldots, x_s$ οι αντιπρόσωποι όλων των διαφορετικών λύσεών της.
2) Για κάθε x_i, βρίσκουμε τις λύσεις της $f(x) \equiv 0 \pmod{p^2}$ που προκύπτουν από τα x_i, σύμφωνα με το Θεώρημα 6.2. Ας είναι $x'_1, \ldots, x'_{s'}$ οι αντιπρόσωποι όλων των διαφορετικών λύσεών της.
3) Για κάθε x'_i, βρίσκουμε τις λύσεις της $f(x) \equiv 0 \pmod{p^3}$ που προκύπτουν από τα x'_i, σύμφωνα με το Θεώρημα 6.2.
4) Επαναλαμβάνουμε την ίδια διαδικασία σε κάθε βήμα μέχρι να προσδιορίσουμε τις λύσεις της $f(x) \equiv 0 \pmod{p^r}$.

Για την επίλυση μιας πολυωνυμικής ισοτιμίας (mod n) για για κάθε $n > 1$, χρειαζόμαστε την παρακάτω πρόταση.

Πρόταση 6.2. *Έστω* $f(x)$ *πολυώνυμο με ακέραιους συντελεστές και* n *ακέραιος* > 1 *με πρωτογενή ανάλυση* $p_1^{a_1} \cdots p_s^{a^s}$. *Η πολυωνυμική ισοτιμία*

$$f(x) \equiv 0 \pmod{n}$$

έχει λύση αν και μόνο αν κάθε μία από τις ισοτιμίες

$$f(x) \equiv 0 \pmod{p_i^{a_i}},\ i = 1, \ldots, s$$

εχει λύση. Έστω N *το πλήθος των λύσεων της* $f(x) \equiv 0 \pmod{n}$ *και* N_i *είναι το πλήθος των λύσεων* $f(x) \equiv 0 \pmod{p_i^{a_i}}$, *όπου* $i = 1, \ldots, s$. *Οι λύσεις της* $f(x) \equiv 0 \pmod{n}$ *είναι οι λύσεις των* $N_1 \cdots N_s$ *συστημάτων*

$$\begin{aligned} x &\equiv x_{1j} \pmod{p_1^{a_1}} \\ &\vdots \\ x &\equiv x_{sj} \pmod{p_s^{a_s}} \end{aligned}$$

όπου $x_{ij} \pmod{p_i^{a_i}}$, $j = 1, \ldots, N_i$ *οι λύσεις των ισοτιμιών* $f(x) \equiv 0 \pmod{p_i^{a_i}}$. *Επομένως ισχύει ότι*

$$N = N_1 \cdots N_s.$$

Επίλυση Πολυωνυμικής Ισοτιμίας για $n > 1$. Αν $n = p_1^{a_1} \cdots p_k^{a_k}$ είναι η πρωτογενής ανάλυση του n, τότε η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod{n}$ έχει λύση, αν και μόνο αν, κάθε μια από τις ισοτιμίες $f(x) \equiv 0 \pmod{p_i^{a_i}}$ έχει λύση [6, Κεφάλαιο 5, Πρόταση 3.1]. Οι λύσεις της $f(x) \equiv 0 \pmod{n}$ προκύπτουν επιλύοντας όλα τα συστήματα k γραμμικών ισοτιμιών που προκύπτουν παίρνοντας μία λύση από κάθε πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod{p_i^{a_i}}$.

Ασκήσεις

Στη συνέχεια θα δούμε την επίλυση μερικών πολυωνυμικών ισοτιμιών χρησιμοποιώντας τις μεθόδους που προαναφέρθηκαν. Στο Παράρτημα, υπάρχουν και οι λύσεις τους με την χρήση υπολογιστικών πακέτων.

΄Ασκηση 6.1. *Να βρεθούν οι λύσεις των παρακάτω πολυωνυμικών ισοτιμιών:*

α) $9x^{15} - 6x^{11} + x^2 + 23 \equiv 0 \pmod{7}$,
β) $x^6 \equiv 1 \pmod{49}$,
γ) $x^3 + 10x^2 + x + 3 \equiv 0 \pmod{27}$,
δ) $x^3 + x^2 - 4 \equiv 0 \pmod{686}$,
ε) $6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod{30}$.

Απόδειξη. α) Θέτουμε $f(x) = 9x^{15} - 6x^{11} + x^2 + 23$. Από το μικρό θεώρημα του Fermat έχουμε ότι $a^7 \equiv a \pmod{7}$, για κάθε $a \in \mathbb{Z}$. Επομένως, για κάθε $a \in \mathbb{Z}$, ισχύει:

$$a^{11} \equiv a^7 a^4 \equiv a^5 \pmod{7}, \quad a^{15} \equiv (a^7)^2 a \pmod{7} \equiv a^3 \pmod{7}.$$

΄Ετσι, έχουμε:

$$f(a) \equiv a^5 + 2a^3 + a^2 + 2 \pmod{7}.$$

Οπότε, η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod{7}$ είναι ισοδύναμη με την

$$x^5 + 2x^3 + x^2 + 2 \equiv 0 \pmod{7}.$$

Στη συνέχεια, θεωρούμε το πλήρες σύστημα αντιπροσώπων των κλάσεων $\bmod 7$, $\{0, \pm1, \pm2, \pm3\}$, και αντικαθιστώντας το x στη παραπάνω ισοτιμία με καθένα από τα στοιχεία του, διαπιστώνουμε ότι αυτή επαληθεύεται για $x = 3, -2, -1$. Συνεπώς, οι λύσεις της $f(x) \equiv 0 \pmod{7}$ είναι: $x \equiv 3, -2, -1 \pmod{7}$.

β) Πρώτα, θα λύσουμε την ισοτιμία $x^6 \equiv 1 \pmod{7}$. Εύκολα διαπιστώνουμε ότι εφόσον $\phi(7) = 6$, η σχέση $x^6 \equiv 1 \pmod{7}$ ταυτίζεται με το Μικρό Θεώρημα του Fermat, και επομένως ισχύει για κάθε ακέραιο x με $(x, 7) = 1$. ΄Αρα, οι λύσεις της $x^6 \equiv 1 \pmod{7}$ είναι οι $x \equiv 1, 2, 3, 4, 5, 6 \pmod{7}$. Στη συνέχεια, θέτουμε $x = a + 7k$, όπου $a \in \{1, 2, 3, 4, 5, 6\}$, και θεωρούμε την ισοτιμία

$$(a + 7k)^6 \equiv 1 \pmod{49}.$$

Οπότε, έχουμε:

$$a^6 + 42a^5 k \equiv 1 \pmod{49},$$

καθώς όλοι οι υπόλοιποι όροι του διωνύμου $(a + 7k)^6$ είναι πολλαπλάσια του 49. Θέτοντας $a = 1, 2, 3, 4, 5, 6$, παίρνουμε αντίστοιχα $k \equiv 0, 4, 4, 2, 2, 6 \pmod{49}$ και έτσι προκύπτουν οι λύσεις της ισοτιμίας,

$$x \equiv 1, 18, 19, 30, 31, 48 \pmod{49}.$$

γ) Θέτουμε $f(x) = x^3 + 10x^2 + x + 3$. Θα επιλύσουμε την πολυωνυμική ισοτιμία

$$f(x) \equiv 0 \pmod{3^3},$$

χρησιμοποιώντας το Θεώρημα 6.2. Πρώτα επιλύουμε την ισοτιμία $f(x) \equiv 0 \pmod 3$. Ένα πλήρες σύστημα υπολοίπων mod 3 δίνεται από το σύνολο $\{-1, 0, 1\}$. Δοκιμάζουμε τις τιμές $x = 0, \pm 1$ στη ισοτιμία $f(x) \equiv 0 \pmod 3$ και βλέπουμε ότι αυτή επαληθεύεται για $x = 0, 1$.

Το επόμενο βήμα είναι να βρούμε τις λύσεις της ισοτιμίας

$$f(x) \equiv 0 \pmod{3^2}.$$

Η παράγωγος του $f(x)$ είναι $f'(x) = 3x^2 + 20x + 1$. Έχουμε να εξετάσουμε τις περιπτώσεις όπου $x = 0$ και $x = 1$

Έστω $x = 0$. Έχουμε $f'(0) = 1$ και $f(0) = 3$. Καθώς $3 \nmid f'(0)$, η παραπάνω ισοτιμία έχει την λύση $x \equiv 3t \pmod{3^2}$, όπου t ακέραιος τέτοιος, ώστε $f'(0)t \equiv (-f(0)/3) \pmod 3$. Οπότε, $t \equiv -1 \pmod 3$ και επομένως $x \equiv 6 \pmod{3^2}$ είναι λύση της ισοτιμίας μας.

Έστω $x = 1$. Έχουμε $3 \mid f'(1) = 24$, $3^2 \nmid f(1) = 15$, και επομένως δεν προκύπτει λύση. Άρα, η ισοτιμία $f(x) \equiv 0 \pmod{3^2}$ έχει την μοναδική λύση $x \equiv 6 \pmod{3^2}$.

Τέλος, βρίσκουμε τις λύσεις της ισοτιμίας

$$f(x) \equiv 0 \pmod{3^3}$$

οι οποίες προέρχονται από την μοναδική λύση $x \equiv 6 \pmod{3^2}$ της ισοτιμίας $f(x) \equiv 0 \pmod{3^2}$. Έχουμε $f'(6) = 229$ και $3 \nmid 229$. Έτσι, η $f(x) \equiv 0 \pmod{3^3}$ έχει λύση την

$$x \equiv t \cdot 3^2 + 6 \pmod{3^3},$$

όπου t ακέραιος ο οποίος επαληθεύει την ισοτιμία $f'(6)t \equiv (-f(6)/3^2) \pmod 3$ η οποία είναι $229t \equiv -65 \pmod 3$, απ΄ όπου έχουμε $t \equiv 1 \pmod 3$. Άρα, η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod{27}$ έχει την μοναδική λύση

$$x \equiv 1 \cdot 3^2 + 6 \equiv 15 \pmod{27}.$$

δ) Έχουμε ότι $686 = 2 \cdot 7^3$. Οι λύσεις της πολυωνυμικής ισοτιμίας θα προκύψουν από τις λύσεις των συστημάτων γραμμικών ισοτιμιών που θα πάρουμε από τις λύσεις των ισοτιμιών

$$x^3 + x^2 - 4 \equiv 0 \pmod{7^3} \quad \text{και} \quad x^3 + x^2 - 4 \equiv 0 \pmod 2.$$

Για την επίλυση της πρώτης ισοτιμίας θεωρούμε την $x^3 + x^2 - 4 \equiv 0 \pmod 7$. Το σύνολο $\{-3, -2, -1, 0, 1, 2, 3\}$ είναι ένα πλήρες σύστημα υπολοίπων mod 7. Αντικαθιστώντας διαδοχικά το x με τους ακεραίους του παραπάνω συνόλου, βλέπουμε ότι κανένας από αυτούς δεν επαληθεύει την $x^3 + x^2 - 4 \equiv 0 \pmod 7$. Επομένως, η αυτή η ισοτιμία δεν έχει λύση και κατά συνέπεια ούτε η ισοτιμία $x^3 + x^2 - 4 \equiv 0 \pmod{686}$ έχει λύση.

ε) Καθώς $30 = 2 \cdot 3 \cdot 5$, θεωρούμε τις ισοτιμίες:

$$6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod 2,$$
$$6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod 3,$$
$$6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod 5.$$

Εύκολα διαπιστώνουμε ότι οι λύσεις της πρώτης είναι $x \equiv 0, 1 \pmod 2$, της δεύτερης $x \equiv 2 \pmod 3$ και της τρίτης $x \equiv 0, 1, 2 \pmod 5$. Συνεπώς, το σύνολο των λύσεων της $6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod{30}$ προκύπτει από τα $2 \cdot 1 \cdot 3 = 6$ διαφορετικά γραμμικά συστήματα τα οποία θα δημιουργηθούν από τις παραπάνω λύσεις. Στη συνέχεια θα λύσουμε τα συστήματα που δημιουργούνται. Καθώς οι ακέραιοι 2, 3 και 5 είναι πρώτοι μεταξύ τους ανά δύο, από το Θεώρημα 5.2 έπεται ότι όλα αυτά τα συστήματα έχουν λύση. Το πρώτο σύστημα είναι:

$$\begin{aligned} x &\equiv 0 \pmod 2, \\ x &\equiv 2 \pmod 3, \\ x &\equiv 0 \pmod 5. \end{aligned}$$

Πρώτα λύνουμε το σύστημα των δύο πρώτων ισοτιμιών. Θέτουμε $x = 2 + 3k$ στην πρώτη ισοτιμία και έχουμε $2 + 3k \equiv 0 \pmod 2$. Η ισοτιμία αυτή επαληθεύεται για $k = 0$. Άρα, η λύση του συστήματος είναι $x \equiv 2 \pmod 6$. Επομένως, το αρχικό σύστημα είναι ισοδύναμο με το εξής:

$$x \equiv 2 \pmod 6, \quad x \equiv 0 \pmod 5.$$

Θέτουμε $x = 2 + 6k$ στη δεύτερη ισοτιμία και έχουμε $2 + 6k \equiv 0 \pmod 5$, απ' όπου $k \equiv 3 \pmod 5$. Επομένως, το σύστημα επαληθεύεται για $x = 20$. Άρα, η λύση του αρχικού συστήματος είναι

$$x \equiv 20 \pmod{30}.$$

Το δεύτερο σύστημα είναι:

$$\begin{aligned} x &\equiv 0 \pmod 2, \\ x &\equiv 2 \pmod 3, \\ x &\equiv 1 \pmod 5. \end{aligned}$$

Παρατηρούμε αμέσως ότι για $x = 2$ οι δύο πρώτες ισοτιμίες του συστήματος επαληθεύονται. Επομένως, η λύση του συστήματος των δύο πρώτων ισοτιμιών είναι $x \equiv 2 \pmod 6$. Άρα, το αρχικό σύστημα είναι ισοδύναμο με το σύστημα:

$$x \equiv 2 \pmod 6, \quad x \equiv 1 \pmod 5.$$

Θέτουμε $x = 6k + 2$ στη δεύτερη ισοτιμία και παίρνουμε $6k + 2 \equiv 1 \pmod 5$, απ' όπου $k \equiv -1 \pmod 5$. Οπότε, η ισοτιμία αυτή επαληθεύεται για $k = 4$. Συνεπώς, η λύση του συστήματος είναι $x \equiv 26 \pmod{30}$.

Το τρίτο σύστημα είναι:

$$\begin{aligned} x &\equiv 0 \pmod 2, \\ x &\equiv 2 \pmod 3, \\ x &\equiv 2 \pmod 5. \end{aligned}$$

Η λύση του συστήματος των δύο πρώτων ισοτιμιών, όπως είδαμε παραπάνω, είναι $x \equiv 2 \pmod 6$. Άρα, το σύστημά μας είναι ισοδύναμο με το εξής:

$$x \equiv 2 \pmod 6, \quad x \equiv 2 \pmod 5.$$

Για $x = 2$, επαληθεύονται και οι δύο ισοτιμίες. Συνεπώς, η λύση του συστήματος των δύο ισοτιμιών και κατά συνέπεια και του αρχικού συστήματος είναι $x \equiv 2 \pmod{30}$.

Στη συνέχεια, έχουμε να λύσουμε το σύστημα:

$$x \equiv 1 \pmod 2,$$
$$x \equiv 2 \pmod 3,$$
$$x \equiv 1 \pmod 5).$$

Παρατηρούμε ότι για $x = 5$, οι δύο πρώτες ισοτιμίες επαληθεύονται. Άρα, η λύση του συστήματος των δύο πρώτων ισοτιμιών είναι $x \equiv 5 \pmod 6$. Συνεπώς, το σύστημα είναι ισοδύναμο με το εξής:

$$x \equiv 5 \pmod 6), \quad x \equiv 1 \pmod 5).$$

Θέτουμε $x = 6k+5$ στη δεύτερη ισοτιμία και παίρνουμε την ισοτιμία $6k+5 \equiv 1 \pmod 5$ η οποία επαληθεύεται για $k = 1$. Άρα, η λύση του αρχικού μας συστήματος είναι $x \equiv 11 \pmod{30}$.

Το επόμενο σύστημα είναι:

$$x \equiv 1 \pmod 2),$$
$$x \equiv 2 \pmod 3),$$
$$x \equiv 2 \pmod 5).$$

Παρατηρούμε ότι οι δύο τελευταίες ισοτιμίες επαληθεύονται για $x = 2$. Οπότε, η λύση του συστήματος των δύο τελευταίων ισοτιμιών είναι $x \equiv 2 \pmod{15}$. Άρα, το αρχικό σύστημα είναι ισοδύναμο με το σύστημα:

$$x \equiv 1 \pmod 2), \quad x \equiv 2 \pmod{15}).$$

Θέτουμε $x = 2+15k$ στη πρώτη ισοτιμία και έχουμε $k \equiv 1 \pmod 2$. Παίρνοντας $k = 1$, βλέπουμε ότι η τιμή $x = 17$ επαληθεύει το παραπάνω σύστημα και κατά συνέπεια η λύση του αρχικού συστήματος είναι $x \equiv 17 \pmod{30}$.

Τέλος, έχουμε να λύσουμε το σύστημα:

$$x \equiv 1 \pmod 2),$$
$$x \equiv 2 \pmod 3),$$
$$x \equiv 0 \pmod 5).$$

Παρατηρούμε αμέσως ότι η τιμή $x = 5$ επαληθεύει το σύστημα. Συνεπώς, η λύση του είναι $x \equiv 5 \pmod{30}$.

Οπότε, οι λύσεις της ισοτιμίας $6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod{30}$ είναι:

$$x \equiv 2, 5, 11, 17, 20, 26 \pmod{30}.$$

□

6.2 Αρχικές Ρίζες

Από την Πρόταση 4.7 έχουμε ότι $\text{ord}_n(a) \mid \phi(n)$. Σ΄ αυτή την ενότητα θα μελετήσουμε την περίπτωση όπου $\text{ord}_n(a) = \phi(n)$.

Ορισμός 6.2. Ας είναι $n \in \mathbb{N}$, $n > 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Αν $\text{ord}_n(a) = \phi(n)$, τότε ο ακέραιος a καλείται *αρχική ρίζα* $(\text{mod } n)$.

Το θεώρημα που ακολουθεί προσδιορίζει πότε υπάρχουν αρχικές ρίζες $\text{mod} n$, όπως επίσης και το πλήθος τους.

Θεώρημα 6.3. *Ας είναι $n \in \mathbb{Z}$. Υπάρχουν αρχικές ρίζες $(\text{mod } n)$ αν και μόνον αν $n = 2, 4, p^r, 2p^r$, όπου p περιττός πρώτος και $r \in \mathbb{Z}^+$. Σε αυτήν την περίπτωση υπάρχουν ακριβώς $\phi(\phi(n))$ ανά δύο ανισότιμες αρχικές ρίζες $(\text{mod } n)$. Αν g είναι μια αρχική ρίζα $(\text{mod } n)$, ένα σύνολο ανισότιμων ανά δύο αρχικών ριζών $(\text{mod } n)$ είναι το σύνολο των ακεραίων g^k με $1 \leq k \leq \phi(n)$ και $(k, \phi(n)) = 1$.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 5, Θεώρημα 4.1] ή [5, Θεώρημα 5.4.23, εδώ]. □

Μία συστηματική μέθοδος για την εύρεση των αρχικών ριζών δίνεται παρακάτω.

Εύρεση των αρχικών ριζών (mod n)

1) Εξετάζουμε αν ο n είναι της μορφής $2, 4, p^r, 2p^r$. Αν δεν είναι, τότε δεν υπάρχουν αρχικές ρίζες $(\text{mod } n)$, διαφορετικά συνεχίζουμε στο δεύτερο βήμα.
2) Υπολογίζουμε τον ακέραιο $\phi(n)$.
3) Επιλέγουμε έναν ακέραιο a με $1 < a < n$ και $(a, n) = 1$. Έστω D το σύνολο των φυσικών διαιρετών d του $\phi(n)$ με $d < \phi(n)$. Υπολογίζουμε τις τιμές a^d για κάθε $d \in D$. Αν $a^d \not\equiv 1 (\text{mod } n)$ για κάθε $d \in D$, τότε ο a είναι μια αρχική ρίζα $(\text{mod } n)$. Αν $a^d \equiv 1 (\text{mod } n)$ για κάποιο $d \in D$, τότε ο a δεν είναι αρχική ρίζα $(\text{mod } n)$. Στη συνέχεια, επαναλαμβάνουμε την διαδικασία για κάποιο άλλο a μέχρι να βρούμε μια αρχική ρίζα.
4) Έστω g αρχική ρίζα που υπολογίστηκε στο προηγούμενο βήμα. Ένα σύνολο ανισότιμων ανά δύο αρχικών ριζών $(\text{mod } n)$ είναι το εξής:

$$\left\{ g^k / \; k = 1, \ldots, \phi(n) - 1, \; (k, \phi(n)) = 1 \right\}.$$

Το πλήθος των ανισότιμων ανά δύο αρχικών ριζών $(\text{mod } n)$ είναι ίσο με $\phi(\phi(n))$. Ο υπολογισμός του πλήθους των ανισότιμων ριζών ανά δύο δεν είναι απαραίτητος για τον προσδιορισμό τους, αλλά είναι χρήσιμος για να επαληθευτεί το πλήθος των αρχικών ριζών που προκύπτει από το τελευταίο βήμα.

Ασκήσεις

΄Ασκηση 6.2. *Ας είναι $a, n \in \mathbb{Z}$ με $n \geq 2$ και $(a, n) = 1$. Ο a είναι αρχική ρίζα $(\text{mod } n)$ αν και μόνον αν για κάθε πρώτο διαιρέτη p του $\phi(n)$ ισχύει:*

$$a^{\phi(n)/p} \not\equiv 1 (\text{mod } n).$$

Απόδειξη. Αν ο a είναι αρχική ρίζα (mod n), τότε ο μικρότερος φυσικός m με την ιδιότητα $a^m \equiv 1 \pmod{n}$ είναι ο $\phi(n)$. Συνεπώς, για κάθε πρώτο διαιρέτη p του $\phi(n)$, έχουμε:

$$a^{\phi(n)/p} \not\equiv 1 \pmod{n}.$$

Αντίστροφα, ας υποθέσουμε ότι ο a δεν είναι αρχική ρίζα (mod n). Τότε, $\mathrm{ord}_n(a) = d$ με $d \neq \phi(n)$. Από την Πρόταση 4.7 έχουμε $d \mid \phi(n)$. Οπότε, υπάρχει πρώτος p τέτοιος, ώστε $p \mid \phi(n)/d$, απ΄ όπου προκύπτει ότι $d \mid \phi(n)/p$. Επομένως, ισχύει:

$$a^{\phi(n)/p} \equiv 1 \pmod{n}.$$

□

Παρατήρηση. Η παραπάνω άσκηση αποτελεί έναν τρόπο υπολογισμού αρχικών ριζών (mod n). Δηλαδή, αντί στο 3ο βήμα στο «Εύρεση των αρχικών ριζών (mod n)» να υπολογιστούν όλοι οι ακέραιοι a^d, όπου d διαιρέτης του $\phi(n)$, αρκεί να υπολογιστούν οι ακέραιοι a^d, όπου $d = \phi(n)/p$, για κάθε πρώτο διαιρέτη p του $\phi(n)$.

΄Ασκηση 6.3. *Ας είναι $n = 4, p^r, 2p^r$, όπου p περιττός πρώτος και r θετικός ακέραιος. Αν g είναι μία αρχική ρίζα* (mod n)*, τότε ισχύει:*

$$g^{\phi(n)/2} \equiv -1 \pmod{n}.$$

Απόδειξη. Καθώς ο ακέραιος n είναι της μορφής $4, p^r, 2p^r$, συνεπάγεται ότι υπάρχουν αρχικές ρίζες (mod n). Ας είναι g μια αρχική ρίζα (mod n). Καθώς ισχύει $(-1, n) = 1$, υπάρχει ακέραιος k με $1 \leq k \leq \phi(n) - 1$ τέτοιος, ώστε να ισχύει:

$$g^k \equiv -1 \pmod{n}.$$

Οπότε, έχουμε:

$$g^{2k} \equiv 1 \pmod{n}.$$

΄Αρα, ισχύει $\phi(n) \mid 2k$ και επομένως υπάρχει ακέραιος l με $2k = \phi(n)l$. Καθώς $k < \phi(n)$, παίρνουμε $\phi(n)l < 2\phi(n)$ και επομένως $l = 1$. ΄Ετσι, έχουμε $k = \phi(n)/2$. □

΄Ασκηση 6.4. *Να βρεθούν οι αρχικές ρίζες* (mod 91) *και* (mod 54).

Απόδειξη. Αρχικά υπολογίζουμε την πρωτογενή ανάλυση του 91 και του 54:

$$91 = 7 \cdot 13 \quad \text{και} \quad 54 = 2 \cdot 3^3.$$

΄Αρα, δεν υπάρχουν αρχικές ρίζες (mod 91) αλλά υπάρχουν αρχικές ρίζες (mod 54). Ισχύει:

$$\phi(\phi(54)) = \phi(\phi(2 \cdot 3^3)) = \phi(18) = \phi(2 \cdot 3^2) = 6.$$

Επομένως, υπάρχουν 6 ανισότιμες ανά δύο αρχικές ρίζες (mod 54). Επιπλέον, οι πρώτοι διαιρέτες του $\phi(54) = 18$ είναι οι 2 και 3.

Στη συνέχεια επιλέγουμε έναν ακέραιο a με $1 < a < n$ και $(a, n) = 1$. Ας είναι $a = 5$ ο μικρότερος με αυτές τις ιδιότητες. Σύμφωνα με την παρατήρηση αρκεί να υπολογίσω τα 5^6 και 5^9. ΄Εχουμε ότι

$$5^6 \equiv (125)^2 \equiv 17^2 \equiv 289 \equiv 19 \pmod{54}$$

και

$$5^9 \equiv 19 \cdot 17 \equiv 323 \equiv -1 \pmod{54}.$$

Άρα το 5 είναι μια αρχική ρίζα (mod 54).

Έτσι, ένα σύνολο ανισότιμων ανά δύο αρχικών ριζών (mod 54) αποτελείται από τους αριθμούς $5, 5^5, 5^7, 5^{11}, 5^{13}, 5^{17}$. Καθώς έχουμε $5^5 \equiv 47 \pmod{54}$, $5^7 \equiv 41 \pmod{54}$, $5^{11} \equiv 29 \pmod{54}$, $5^{13} \equiv 23 \pmod{54}$ και $5^{17} \equiv 11 \pmod{54}$, ένα σύνολο ανισότιμων ανά δύο αρχικών ριζών (mod 54) δίνεται επίσης και από τους ακεραίους $5, 11, 23, 29, 41, 47$. □

Άσκηση 6.5. *Ας είναι ακέραιος $n \geq 2$. Να δειχθεί ότι αν ο $F_n = 2^{2^n} + 1$ είναι πρώτος, τότε το 2 δεν είναι αρχική ρίζα* (mod F_n).

Απόδειξη. Για να δείξουμε ότι ο 2 δεν είναι αρχική ρίζα (mod F_n) αρκεί να βρούμε έναν ακέραιο m μικρότερο του $\phi(F_n) = F_n - 1 = 2^{2^n}$ με $2^m \equiv 1 \pmod{F_n}$. Ισχύει:

$$2^{2^n} + 1 \equiv 0 \pmod{F_n},$$

απ΄ όπου παίρνουμε:

$$(2^{2^n})^2 \equiv (-1)^2 \equiv 1 \pmod{F_n}.$$

Έτσι, έχουμε:

$$2^{2^{n+1}} \equiv 1 \pmod{F_n}.$$

Επίσης, για κάθε $n \geq 2$ ισχύει $n + 1 < 2^n$ (Άσκηση 1.4) και επομένως έχουμε $2^{n+1} < \phi(F_n)$. Άρα, το 2 δεν είναι αρχική ρίζα (mod F_n). □

Άσκηση 6.6. *Ας είναι n ακέραιος της μορφής $2, 4, p^r, 2p^r$, όπου p πρώτος ≥ 3 και $r \in \mathbb{Z}^+$. Αν $x_1, \ldots, x_{\phi(n)}$ είναι ένα περιορισμένο σύστημα υπολοίπων* (mod n)*, τότε ισχύει:*

$$x_1 \cdots x_{\phi(n)} \equiv -1 \pmod{n}.$$

Απόδειξη. Αν $n = 2$, τότε το περιορισμένο σύστημα υπολοίπων (mod n) είναι το $\{1\}$ και επομένως ισχύει $1 \equiv -1 \pmod{2}$. Ας είναι n ακέραιος της μορφής $4, p^r, 2p^r$. Τότε, υπάρχει αρχική ρίζα $g \pmod{n}$ και επομένως το σύνολο $\{1, g, \ldots, g^{\phi(n)-1}\}$ αποτελεί ένα περιορισμένο σύστημα υπολοίπων (mod n). Έτσι, αν $\{x_1, \ldots, x_{\phi(n)}\}$ είναι ένα περιορισμένο σύστημα υπολοίπων (mod n), τότε παίρνουμε:

$$x_1 \cdots x_{\phi(n)} \equiv 1 \cdot g \cdot g^2 \cdots g^{\phi(n)-1} \pmod{n}.$$

Από την άλλη πλευρά, έχουμε:

$$1 \cdot g \cdot g^2 \cdots g^{\phi(n)-1} = g^{1+2+\cdots+(\phi(n)-1)} = g^{\phi(n)(\phi(n)-1)/2}.$$

Σύμφωνα με την Άσκηση 6.3, ισχύει $g^{\frac{\phi(n)}{2}} \equiv -1 \pmod{n}$. Επίσης, από το Πόρισμα 3.6 έχουμε ότι για $n > 2$ ο ακέραιος $\phi(n)$ είναι άρτιος. Έτσι, παίρνουμε:

$$g^{\phi(n)(\phi(n)-1)/2} \equiv (-1)^{\phi(n)-1} \equiv -1 \pmod{n}.$$

Συνδυάζοντας τις παραπάνω σχέσεις, προκύπτει:

$$x_1 \cdots x_{\phi(n)} \equiv -1 \pmod{n}.$$

□

΄Ασκηση 6.7. *Ας είναι p πρώτος, $k \in \mathbb{Z}^+$ και $S_k = \sum_{a=1}^{p-1} a^k$. Να δειχθεί ότι αν $p-1 \mid k$ τότε $S_k \equiv -1 \pmod p$ και αν $p-1 \nmid k$, τότε $S_k \equiv 0 \pmod p$.*

Απόδειξη. Ας είναι $p-1 \mid k$. Καθώς $1 \le a \le p-1$, έχουμε $(a,p)=1$, και επομένως το μικρό θεώρημα του Fermat δίνει:

$$a^{p-1} \equiv 1 \pmod p.$$

΄Ετσι, για κάθε ακέραιο a με $1 \le a \le p-1$, ισχύει:

$$a^k \equiv 1 \pmod p.$$

Οπότε, έχουμε:

$$S_k = \sum_{a=1}^{p-1} a^k \equiv p-1 \equiv -1 \pmod p.$$

Ας είναι τώρα $p-1 \nmid k$ και g μία αρχική ρίζα $\pmod p$. Τότε $g^k \not\equiv 1 \pmod p$. Καθώς οι αριθμοί $g, 2g, \ldots, (p-1)g$ είναι ανισότιμοι ανα δύο $\pmod p$, καθένας από τους $g, 2g, \ldots, (p-1)g$ είναι ισότιμοι ($\mod p$) με έναν ακριβώς από τους $1, 2, \ldots, (p-1)$. ΄Ετσι, έχουμε:

$$\sum_{a=1}^{p-1} (ag)^k \equiv \sum_{a=1}^{p-1} a^k \pmod p,$$

απ΄ όπου, έπεται:

$$(g^k - 1) \sum_{a=1}^{p-1} a^k \equiv 0 \pmod p.$$

Τέλος, καθώς $g^k \not\equiv 1 \pmod p$, παίρνουμε ότι $S_k \equiv 0 \pmod p$. □

΄Ασκηση 6.8. *Ας είναι p περιττός πρώτος και g ακέραιος. Αν $p \equiv 1 \pmod 4$, τότε ο g είναι αρχική ρίζα $\pmod p$ αν και μόνον αν ο $-g$ είναι αρχική ρίζα $\pmod p$. Αν $p \equiv 3 \pmod 4$, τότε ο g είναι αρχική ρίζα $\pmod p$ αν και μόνον αν ισχύει $\operatorname{ord}_p(-g) = (p-1)/2$.*

Απόδειξη. Ας είναι $p \equiv 1 \pmod 4$. Τότε, έχουμε $\phi(p) = p-1 = 4k$, όπου k θετικός ακέραιος. ΄Ετσι, για κάθε πρώτο διαιρέτη q του $\phi(p)$ ο ακέραιος $\phi(p)/q$ είναι άρτιος και επομένως για κάθε ακέραιο g ισχύει $g^{\phi(p)/q} \not\equiv 1 \pmod p$ αν και μόνον αν $(-g)^{\phi(p)/q} \not\equiv 1 \pmod p$. Επομένως, σύμφωνα με την ΄Ασκηση 6.2, ο ακέραιος g είναι αρχική ρίζα $\pmod p$ αν και μόνον αν ο $-g$ είναι αρχική ρίζα $\pmod p$.

Ας είναι τώρα $p \equiv 3 \pmod 4$. Τότε, ισχύει $\phi(p) = p-1 = 2(2k+1)$. Αν g είναι μία αρχική ρίζα $\pmod p$, τότε, σύμφωνα με την ΄Ασκηση 6.3, ισχύει $g^{\phi(p)/2} \equiv -1 \pmod p$. ΄Ετσι, καθώς ο ακέραιος $\phi(p)/2$ είναι περιττός, ισχύει $(-g)^{\phi(p)/2} \equiv 1 \pmod p$. Επίσης, από την ΄Ασκηση 6.2, έχουμε ότι για κάθε πρώτο διαιρέτη q του $2k+1$, ισχύει:

$$(-g)^{2(2k+1)/q} \equiv g^{2(2k+1)/q} \not\equiv 1 \pmod p.$$

΄Αρα, έχουμε:

$$(-g)^{(2k+1)/q} \not\equiv 1 \pmod p,$$

απ΄ όπου, παίρνουμε:

$$(-g)^{(p-1)/2q} \not\equiv 1 \pmod{p}$$

Επομένως, έχουμε $\mathrm{ord}_p(-g) = (p-1)/2$.

Αντιστρόφως, ας υποθέσουμε ότι ισχύει $\mathrm{ord}_p(-g) = (p-1)/2$. Τότε, για κάθε πρώτο διαιρέτη q του $(p-1)/2$, ισχύει:

$$(-g)^{(p-1)/2q} \not\equiv 1 \pmod{p}.$$

Καθώς $(p-1)/2 = 2k+1$, ο πρώτος q είναι περιττός. Από την Πρόταση 4.8 έπεται $\mathrm{ord}_p(-g)^{(p-1)/2q} = q$ και επομένως $(-g)^{(p-1)/q} \not\equiv 1 \pmod{p}$. Έτσι, έχουμε:

$$g^{(p-1)/q} \equiv (-g)^{(p-1)/q} \not\equiv 1 \pmod{p}.$$

Άρα, σύμφωνα με την Άσκηση 6.2, ο g είναι αρχική ρίζα $\pmod{p}$. □

Άσκηση 6.9. *Ας υποθέσουμε ότι n είναι φυσικός > 6 και ότι υπάρχουν αρχικές ρίζες $\pmod{n}$. Αν $g_1, \ldots, g_s$, όπου $s = \phi(\phi(n))$, είναι αρχικές ρίζες ανισότιμες ανά δύο $\pmod{n}$, τότε ισχύει:*

$$g_1 \cdots g_s \equiv 1 \pmod{n}.$$

Απόδειξη. Καθώς οι αρχικές ρίζες $g_1, \ldots, g_s$ είναι ανισότιμες ανά δύο $\pmod{n}$ και το πλήθος τους ισούται με $\phi(\phi(n))$, συνεπάγεται ότι κάθε άλλη αρχική ρίζα $\pmod{n}$ είναι ισότιμη $\pmod{n}$ με μία από αυτές. Ας είναι g μία αρχική ρίζα $\pmod{n}$. Τότε, κάθε στοιχείο του συνόλου

$$A = \left\{ g^k / \ 1 \le k < \phi(n) \ \text{ και } \ (k, \phi(n)) = 1 \right\}$$

είναι μία αρχική ρίζα $\pmod{n}$ και κατά συνέπεια είναι ισότιμο με έναν ακριβώς από τους $g_1, \ldots, g_s$. Έτσι, έχουμε:

$$g_1 \cdots g_s \equiv \prod_{\substack{k=1 \\ (k,n)=1}}^{\phi(n)-1} g^k \pmod{n}.$$

Επομένως, αρκεί να δείξουμε ότι ισχύει:

$$\prod_{\substack{k=1 \\ (k,n)=1}}^{\phi(n)-1} g^k \equiv 1 \pmod{n}.$$

Για κάθε $k \in \{1, \ldots, \phi(n)\}$ με $(k, \phi(n)) = 1$, έχουμε $\phi(n) - k \in \{1, \ldots, \phi(n)\}$ με $(\phi(n) - k, \phi(n)) = 1$. Έτσι, $g^{\phi(n)-k} \in A$. Επίσης, αν $\phi(n) = 2k$, τότε $(\phi(n)/2, \phi(n)) = (k, \phi(n)) = 1$, απ΄ όπου παίρνουμε $\phi(n) = 2$. Έχουμε $n = p^r$ ή $n = 2p^r$, όπου p πρώτος ≥ 3 και r θετικός ακέραιος. Επομένως, ισχύει $\phi(n) = p^{r-1}(p-1)$. Έτσι, αν $r > 1$, τότε έχουμε $p \mid 2$ που είναι άτοπο. Οπότε, $r = 1$ και $p = 3$, απ΄ όπου $n = 3$ που είναι άτοπο. Συνεπώς, ισχύει $k \neq \phi(n)/2$. Άρα, για κάθε $k \in \{1, \ldots, \phi(n)/2\}$ με $(k, \phi(n)) = 1$, έχουμε $g^k \not\equiv g^{\phi(n)-k} \pmod{n}$ και $g^k g^{\phi(n)-k} \equiv 1 \pmod{n}$, απ΄ όπου προκύπτει το αποτέλεσμα. □

6.3 Δείκτες

Οι δείκτες εμφανίζονται στην βιβλιογραφία (κυρίως στην κρυπτογραφία) και ως διακριτός λογάριθμος, ενώ ο υπολογισμός του διακριτού λογαρίθμου, δηλαδή ο υπολογισμός κάποιου δείκτη, είναι από τα πιο ενδιαφέροντα θέματα της σύγχρονης κρυπτανάλυσης.

Ορισμός 6.3. Ας είναι n ακέραιος > 1, g μία αρχική ρίζα $(\mathrm{mod}\, n)$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Καλούμε *δείκτης του a* ως προς τη βάση g $(\mathrm{mod}\, n)$ τον μοναδικό φυσικό $k < \phi(n)$ για τον οποίον ισχύει $a \equiv g^k \,(\mathrm{mod}\, n)$. Ο δείκτης του a ως προς τη βάση g $(\mathrm{mod}\, n)$ συμβολίζεται με $\mathrm{ind}_g\, a$.

Παρατήρηση. Ας είναι g μια αρχική ρίζα $(\mathrm{mod}\, n)$. Αν $(a, n) = (b, n) = 1$, τότε ισχύει:

$$a \equiv b \,(\mathrm{mod}\, n) \iff \mathrm{ind}_g\, a \equiv \mathrm{ind}_g\, b \,(\mathrm{mod}\, \phi(n)).$$

Οι ιδιότητες των δεικτών είναι παρόμοιες με αυτές των λογαρίθμων.

Πρόταση 6.3. *Ας είναι g μια αρχική ρίζα $(\mathrm{mod}\, n)$. Ισχύουν τα εξής:*

(α) *Αν $a_1, \ldots, a_s \in \mathbb{Z}$, με $(a_i, n) = 1$, τότε:*

$$\mathrm{ind}_g(a_1 \cdots a_s) = \mathrm{ind}_g\, a_1 + \cdots + \mathrm{ind}_g\, a_s \,(\mathrm{mod}\, \phi(n)).$$

(β) *Για κάθε $a \in \mathbb{Z}$, με $(a, n) = 1$, και για κάθε $s \in \mathbb{Z}^+$, έχουμε:*

$$\mathrm{ind}_g\, a^s = s \,\mathrm{ind}_g\, a \,(\mathrm{mod}\, \phi(n)).$$

(γ) $\mathrm{ind}_g\, 1 = 0$ *και* $\mathrm{ind}_g\, g = 1$.

(δ) *Αν h είναι μια άλλη αρχική ρίζα $(\mathrm{mod}\, n)$, τότε για κάθε $a \in \mathbb{Z}$, με $(a, n) = 1$, τότε:*

$$\mathrm{ind}_g\, a = \mathrm{ind}_h\, a \cdot \mathrm{ind}_g\, h \,(\mathrm{mod}\, \phi(n)).$$

(ε) $\mathrm{ind}_g(-1) = \phi(n)/2$, *για $n > 2$.*

Απόδειξη. Βλέπε [6, Κεφάλαιο 5, Πρόταση 5.1]. □

Στη συνέχεια, υποθέτουμε ότι $n = 2, 4, p^r, 2p^r$, όπου p πρώτος ≥ 3 και $r \in \mathbb{Z}^+$. Θα δώσουμε παρακάτω μεθόδους επίλυσης διάφορων μορφών ισοτιμιών με την χρήση δεικτών.

Επίλυση Γραμμικής Ισοτιμίας με την Χρήση Δεικτών. Για την επίλυση της γραμμικής ισοτιμίας $ax \equiv b \,(\mathrm{mod}\, n)$ με $(a, n) = (b, n) = 1$ ακολουθούμε τα εξής βήματα:

1) Υπολογίζουμε μια αρχική ρίζα g $(\mathrm{mod}\, n)$.
2) Υπολογίζουμε τους δείκτες $\mathrm{ind}_g\, a$ και $\mathrm{ind}_g\, b$.
3) Η λύση της γραμμικής ισοτιμίας είναι $x \equiv g^{\mathrm{ind}_g\, b - \mathrm{ind}_g\, a} \,(\mathrm{mod}\, n)$.

Προφανώς, αυτή η μέθοδος υπερτερεί των υπολοίπων που είδαμε στο προηγούμενο κεφάλαιο μόνο στην περίπτωση που οι δείκτες μπορούν να υπολογιστούν άμεσα ή τους γνωρίζουμε ήδη.

Ας είναι a, k και n ακέραιοι με $n > 1$. Μία πολυωνυμική ισοτιμία της μορφής

$$x^k \equiv b \pmod{n}$$

καλείται *διωνυμική*. Στην περίπτωση όπου υπάρχουν αρχικές ρίζες $\pmod{n}$, μπορούμε να βρούμε τις λύσεις της διωνυμικής ισοτιμίας χρησιμοποιώντας δείκτες, με την παρακάτω μέθοδο.

Επίλυση Διωνυμικής Ισοτιμίας με την Χρήση Δεικτών. Ας είναι $n = p^m$ ή $n = 2p^m$. Για να επιλύσουμε την διωνυμική ισοτιμία $x^k \equiv b \pmod{n}$ ακολουθούμε τα εξής βήματα:

1) Υπολογίζουμε μια αρχική ρίζα $g \pmod{n}$.
2) Υπολογίζουμε τον δείκτη $\operatorname{ind}_g b$.
3) Επιλύουμε την γραμμική ισοτιμία $k \cdot \operatorname{ind}_g x \equiv \operatorname{ind}_g b \pmod{\phi(n)}$ ως προς $\operatorname{ind}_g x$.
4) Αν η γραμμική ισοτιμία δεν έχει λύσεις, τότε ούτε και η αρχική έχει. Αν $\operatorname{ind}_g x \equiv y_i \pmod{\phi(n)}$ $(i = 1, \ldots, s)$ είναι οι λύσεις της γραμμικής ισοτιμίας, τότε οι λύσεις της διωνυμικής ισοτιμίας είναι: $x \equiv g^{y_i} \pmod{n}$ $(i = 1, \ldots, s)$.

Η διωνυμική ισοτιμία είναι μια πολυωνυμική ισοτιμία. Επομένως τίθεται το ερώτημα πότε επιλέγουμε να λύσουμε την διωνυμική ισοτιμία με τους τρόπους που είδαμε στην πρώτη ενότητα και πότε με την μέθοδο της χρήσης δεικτών. Αν γνωρίζουμε μία αρχική ρίζα $g \pmod{n}$ και ο δείκτης $\operatorname{ind}_g b$ μπορεί να υπολογιστεί εύκολα, τότε αυτός ο τρόπος είναι ο καλύτερος, καθώς μεταθέτει την επίλυση της πολυωνυμικής ισοτιμίας σε μία γραμμική ισοτιμία.

Ας είναι a, b και n ακέραιοι με $n > 1$. Μία ισοτιμία της μορφής

$$a^x \equiv b \pmod{n},$$

όπου x προσδιοριστέος ακέραιος, καλείται *εκθετική*. Καλούμε *λύση* της εκθετικής ισοτιμίας κάθε ακέραιο ο οποίος την επαληθεύει. Παρακάτω δίνουμε μία μέθοδο επίλυσης της εκθετικής ισοτιμίας.

Επίλυση Εκθετικής Ισοτιμίας με την Χρήση Δεικτών. Για την επίλυση της εκθετικής ισοτιμίας $a^x \equiv b \pmod{n}$, με $(a, n) = (b, n) = 1$, ακολουθούμε τα εξής βήματα:

1) Βρίσκουμε μια αρχική ρίζα $g \pmod{n}$.
2) Υπολογίζουμε τους δείκτες $\operatorname{ind}_g a$ και $\operatorname{ind}_g b$.
3) Λύνουμε την γραμμική ισοτιμία $x \cdot \operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{\phi(n)}$.
4) Αν $x \equiv x_1, \ldots, x_k \pmod{\phi(n)}$ είναι όλες οι διαφορετικές λύσεις της παραπάνω γραμμικής ισοτιμίας, τότε οι λύσεις της εκθετικής ισοτιμίας είναι όλοι οι ακέραιοι οι οποίοι ανήκουν στις αντίστοιχες κλάσεις.

Ασκήσεις

Ο υπολογισμός ενός δείκτη είναι μία επίπονη διαδικασία καθώς δεν υπάρχει κάποια αλγοριθμική διαδικασία υπολογισμού κάθε δείκτη.

΄Ασκηση 6.10. *Να δειχθεί ότι ο 3 είναι αρχική ρίζα* (mod 17) *και να βρεθούν όλοι οι δείκτες των ακεραίων* a*, με* $(a, 17) = 1$*, ως προς τη βάση* 3 (mod 17).

Απόδειξη. Σύμφωνα με την ΄Ασκηση 6.2, για να είναι ο 3 αρχική ρίζα (mod 17), αρκεί για κάθε p πρώτο διαιρέτη του $\phi(17)$ να ισχύει:

$$3^{\phi(17)/p} \not\equiv 1 \pmod{17}.$$

Καθώς $\phi(17) = 16 = 2^4$, έχουμε:

$$3^{16/2} \equiv 3^8 \equiv 9^4 \equiv 81^2 \equiv 13^2 \equiv 169 \equiv -1 \pmod{17}.$$

Επομένως, ο 3 είναι αρχική ρίζα (mod 17).

Εφόσον ο 17 είναι πρώτος θα ορίζεται ο δείκτης του a με βάση το 3 για κάθε $1 \leq a \leq 16$.

Σχέση Ισοτιμίας	**Δείκτης**
$3^0 \equiv 1 \pmod{17}$	$\text{ind}_3\, 1 = 0$
$3^1 \equiv 3 \pmod{17}$	$\text{ind}_3\, 3 = 1$
$3^2 \equiv 9 \pmod{17}$	$\text{ind}_3\, 9 = 2$
$3^3 \equiv 10 \pmod{17}$	$\text{ind}_3\, 10 = 3$
$3^4 \equiv 13 \pmod{17}$	$\text{ind}_3\, 13 = 4$
$3^5 \equiv 5 \pmod{17}$	$\text{ind}_3\, 5 = 5$
$3^6 \equiv 15 \pmod{17}$	$\text{ind}_3\, 15 = 6$
$3^7 \equiv 11 \pmod{17}$	$\text{ind}_3\, 11 = 7$
$3^8 \equiv 16 \pmod{17}$	$\text{ind}_3\, 16 = 8$
$3^9 \equiv 14 \pmod{17}$	$\text{ind}_3\, 14 = 9$
$3^{10} \equiv 8 \pmod{17}$	$\text{ind}_3\, 8 = 10$
$3^{11} \equiv 7 \pmod{17}$	$\text{ind}_3\, 7 = 11$
$3^{12} \equiv 4 \pmod{17}$	$\text{ind}_3\, 4 = 12$
$3^{13} \equiv 12 \pmod{17}$	$\text{ind}_3\, 12 = 13$
$3^{14} \equiv 2 \pmod{17}$	$\text{ind}_3\, 2 = 14$
$3^{15} \equiv 6 \pmod{17}$	$\text{ind}_3\, 6 = 15$

□

Οι επόμενες τρεις ασκήσεις είναι εφαρμογές της μεθοδολογίας επίλυσης ισοτιμιών με την χρήση δεικτών.

΄Ασκηση 6.11. *Να λυθεί η γραμμική ισοτιμία*

$$7x \equiv 9 \pmod{50}.$$

Απόδειξη. Πρώτα παρατηρούμε ότι $(7, 50) = 1$ και επομένως η παραπάνω γραμμική ισοτιμία έχει λύση. Στη συνέχεια θα δείξουμε ότι ο ακέραιος 3 είναι αρχική ρίζα (mod 50). Ισχύει $\phi(50) = \phi(2)\phi(25) = 20$ και επομένως θα πρέπει να δείξουμε ότι $\text{ord}(3) = 20$. ΄Εχουμε $\text{ord}(3) \mid 20$ και κατά συνέπεια $\text{ord}(3) \in \{1, 2, 4, 5, 10, 20\}$. Επιπλέον, ισχύει

$$3^2 = 9, \quad 3^4 \equiv 31 \pmod{50}, \quad 3^5 \equiv 43 \pmod{50}, \quad 3^{10} \equiv -1 \pmod{50}.$$

΄Αρα $\operatorname{ord}(3) = 20$ και επομένως ο ακέραιος 3 είναι αρχική ρίζα (mod 50).

Καθώς

$$\operatorname{ind}_3 9 = \operatorname{ind}_3 3^2 = 2 \operatorname{ind}_3 3 = 2,$$

η λύση της γραμμικής ισοτιμίας είναι:

$$x \equiv 3^{\operatorname{ind}_3 9 - \operatorname{ind}_3 7} \equiv 3^{-13} \pmod{50}.$$

Επίσης, έχουμε $-13 \equiv 7 \pmod{20}$. ΄Αρα, λύση της ισοτιμίας είναι:

$$x \equiv 3^7 \equiv 37 \pmod{50}.$$

□

΄Ασκηση 6.12. *Να βρεθούν, με την χρήση δεικτών, οι ακέραιοι που επαληθεύουν τις παρακάτω πολυωνυμικές ισοτιμίες:*

α) $x^{15} \equiv 11 \pmod{26}$.

β) $2x^3 \equiv 5 \pmod{49}$.

Απόδειξη. α) Αρχικά υπολογίζουμε μία αρχική ρίζα (mod 26). Καθώς

$$\phi(26) = \phi(2)\,\phi(13) = 12 = 2^2 \cdot 3,$$

για να δείξουμε ότι το a, με $(a, 26) = 1$, είναι αρχική ρίζα αρκεί να δείξουμε ότι $a^{\phi(26)/d} \not\equiv 1 \pmod{26}$, για $d = 2, 3$. Για $a = 7$ έχουμε:

$$7^{\phi(26)/3} \equiv 7^4 \equiv 49^2 \equiv (-3)^2 \equiv 9 \pmod{26},$$
$$7^{\phi(26)/2} \equiv 7^6 \equiv 49^3 \equiv (-3)^3 \equiv -1 \pmod{26}.$$

΄Αρα, ο ακέραιος 7 είναι μια αρχική ρίζα (mod 26).

Στη συνέχεια, υπολογίζοντας τις δυνάμεις του 7, βρίσκουμε ότι ισχύει $7^5 \equiv 11 \pmod{26}$ και επομένως $\operatorname{ind}_7 11 = 5$. Οπότε, έχουμε τη γραμμική ισοτιμία:

$$15 \cdot \operatorname{ind}_7 x \equiv 5 \pmod{12}.$$

Καθώς όμως ισχύει $(12, 15) = 3 \nmid 5$, η παραπάνω γραμμική ισοτιμία δεν έχει λύση. Επομένως, η ισοτιμία $x^{15} \equiv 11 \pmod{26}$ δεν έχει επίσης λύση.

β) Πολλαπλασιάζουμε την ισοτιμία επί 25 ώστε να την φέρουμε στην επιθυμητή μορφή. ΄Ετσι η ισοτιμία γίνεται

$$x^3 \equiv 27 \pmod{49}.$$

Ισχύει:

$$\phi(49) = \phi(7^2) = 7 \cdot 6 = 42 = 2 \cdot 3 \cdot 7$$

και

$$3^{\phi(49)/7} \equiv 3^6 \equiv 27^2 \equiv (-22)^2 \equiv -6 \pmod{49},$$
$$3^{\phi(49)/3} \equiv 3^{14} \equiv (-6)^2 \cdot 9 \equiv -19 \pmod{49},$$
$$3^{\phi(49)/2} \equiv 3^{21} \equiv (-19) \cdot (-6) \cdot 3 \equiv -1 \pmod{49}.$$

΄Αρα, το 3 είναι μια αρχική ρίζα (mod 49).

Στη συνέχεια, κάνοντας χρήση των ιδιοτήτων των δεικτών, παίρνουμε:

$$\operatorname{ind}_3 27 = \operatorname{ind}_3 3^3 = 3 \operatorname{ind}_3 3 = 3.$$

΄Ετσι, η γραμμική ισοτιμία γίνεται:

$$3 \cdot \operatorname{ind}_3 x \equiv 3 \pmod{42}.$$

Προφανώς, για $\operatorname{ind}_3 x = 1$ η ισοτιμία επαληθεύεται. Επομένως, εφαρμόζοντας της διαδικασία επίλυσης γραμμικών ισοτιμιών προκύπτει ότι οι λύσεις της ισοτιμίας ως προς $\operatorname{ind}_3 x$ είναι $1, 15, 29 \pmod{42}$.

Τέλος, υπολογίζουμε τις λύσεις της διωνυμικής ισοτιμίες:

$$\begin{aligned} x &\equiv 3^1 \equiv 3 \pmod{49}, \\ x &\equiv 3^{15} \equiv (3^{14}) \cdot 3 \equiv -19 \cdot 3 \equiv -57 \equiv 41 \pmod{49}, \\ x &\equiv 3^{29} \equiv 3^{21} \cdot 3^6 \cdot 3^2 \equiv -1 \cdot (-6) \cdot 9 \equiv 5 \pmod{49}. \end{aligned}$$

΄Αρα, οι λύσεις της αρχικής ισοτιμίας είναι οι $x \equiv 3, 5, 41 \pmod{49}$. □

΄Ασκηση 6.13. *Να βρεθούν, με την χρήση δεικτών, οι ακέραιοι που επαληθεύουν τις παρακάτω εκθετικές ισοτιμίες:*

α) $11^x \equiv 7 \pmod{13}$,

β) $3^x \equiv 7 \pmod{22}$.

Απόδειξη. α) ΄Εχουμε $\phi(13) = 12 = 2^2 \cdot 3$ και ισχύει:

$$2^{\phi(13)/2} \equiv 2^6 \equiv -1 \pmod{13}, \quad 2^{\phi(13)/3} \equiv 2^4 \equiv 16 \pmod{13}.$$

΄Αρα, ο 2 είναι μια αρχική ρίζα (mod 13). ΄Αλλες αρχικές ρίζες (mod 13) είναι οι 6, 7 και 11. Κατόπιν, βρίσκουμε ότι $\operatorname{ind}_2 11 = 7$ και $\operatorname{ind}_2 7 = 11$. ΄Ετσι, έχουμε την γραμμική ισοτιμία

$$7x \equiv 11 \pmod{12}.$$

Εύκολα διαπιστώνουμε ότι η μοναδική λύση της γραμμικής ισοτιμίας είναι η $x \equiv 5 \pmod{12}$. ΄Αρα, οι λύσεις της εκθετικής ισοτιμίας είναι όλοι οι ακέραιοι της κλάσης $5 \pmod{12}$.

β) ΄Εχουμε $\phi(22) = \phi(2) \cdot \phi(11) = 10 = 2 \cdot 5$. Επίσης, ισχύει:

$$7^{\phi(22)/5} = 7^2 \equiv 5 \pmod{22}, \quad 7^{\phi(22)/2} = 7^5 \equiv -1 \pmod{22},$$

΄Αρα, ο 7 είναι μια αρχική ρίζα. ΄Αλλες αρχικές ρίζες (mod 22) είναι οι 13, 17 και 19. ΄Εχουμε $\operatorname{ind}_7 7 = 1$ και υπολογίζοντας τις δυνάμεις του 7 βρίσκουμε ότι $7^4 \equiv 3 \pmod{22}$, απ΄ όπου έπεται ότι $\operatorname{ind}_7 3 = 4$. ΄Ετσι, προκύπτει η γραμμική ισοτιμία

$$4x \equiv 1 \pmod{10}.$$

Καθώς $(4, 10) = 2 \nmid 1$ συνεπάγεται ότι η γραμμική ισοτιμία δεν έχει λύση και επομένως η εκθετική ισοτιμία $3^x \equiv 7 \pmod{22}$ δεν έχει λύση. □

΄Ασκηση 6.14. *Να βρεθούν οι ακέραιοι που επαληθεύουν την ισοτιμία*

$$25^x \equiv 17 \pmod{47},$$

αν γνωρίζουμε ότι $2^6 \equiv 17 \pmod{47}$ *και* $2^{18} \equiv 25 \pmod{47}$.

Απόδειξη. ΄Εχουμε $(2, 47) = 1$ και $\phi(47) = 46 = 23 \cdot 2$. Ισχύει:

$$2^{\phi(47)/23} = 2^2 \equiv 4 \pmod{47},$$
$$2^{\phi(47)/2} = 2^{23} \equiv 1 \pmod{47}.$$

΄Αρα, $\mathrm{ord}_{47}\, 2 = 23$.

Αντικαθιστώντας στην αρχική ισοτιμία τους ακέραιους 25 και 17 από τους ισότιμούς τους, παίρνουμε:

$$2^{18x} \equiv 2^6 \pmod{47} :$$

Οπότε, η Πρόταση 4.7(α) δίνει:

$$18x \equiv 6 \pmod{23}.$$

Απλοποιώντας με 6, παίρνουμε:

$$3x \equiv 1 \pmod{23}.$$

Τότε $x \equiv 8 \pmod{23}$ και κατά συνέπεια οι λύσεις της εκθετικής ισοτιμίας είναι όλοι οι ακέραιοι της κλάσης $8 \pmod{23}$. □

΄Οπως και στην περίπτωση των διωνυμικών ισοτιμιών, έτσι και στην επίλυση των εκθετικών ισοτιμιών η ταχύτητα υπολογισμού των λύσεων εξαρτάται από την ταχύτητα υπολογισμού των δεικτών $\mathrm{ind}_g\, a$ και $\mathrm{ind}_g\, b$. Για παράδειγμα στην προηγούμενη άσκηση αν γνωρίζαμε εξ αρχής ότι το 5 είναι αρχική ρίζα $(\mathrm{mod}\, 47)$ θα είχαμε υπολογίσει άμεσα τον δείκτη $\mathrm{ind}_5\, 25$ και θα χρειαζόταν να υπολογίσουμε μόνο το $\mathrm{ind}_5\, 17$.

6.4 Συνδυαστικές Ασκήσεις

΄Ασκηση 6.15. *Ας είναι* n *θετικός ακέραιος. Να δειχθούν τα εξής:*
α) Ο ακέραιος 2 είναι αρχική ρίζα $(\mathrm{mod}\, 3^n)$.
β) Το πρόβλημα της εύρεσης του $\mathrm{ind}_2\, a \pmod{3^n}$*, όπου* a *ακέραιος με* $(a, 3) = 1$*, είναι ισοδύναμο με την επίλυση της εκθετικής ισοτιμίας* $4^x c \equiv 1 \pmod{3^n}$*, όπου* c *ακέραιος με* $c \equiv 1 \pmod 3$.

Απόδειξη. α) Καθώς $\phi(3^n) = 2 \cdot 3^{n-1}$, για να είναι ο 2 αρχική ρίζα $(\mathrm{mod}\, 3^n)$, θα πρέπει να δείξουμε ότι για $k = 0, 1, \ldots, n-2$ ισχύει:

$$2^{2\cdot 3^k} \not\equiv 1 \pmod{3^n}.$$

Για $n = 2$ έχουμε $k = 2$ και επομένως έχουμε $2^{2\cdot 3^0} = 4$ και $4 \not\equiv 1 \pmod 9$. Ας υποθέσουμε ότι η προς απόδειξη σχέση ισχύει για $n = a$. Θα δείξουμε ότι ισχύει και για $n = a + 1$. Αν k είναι ακέραιος με $0 \le k \le a - 2$ και

$$2^{2\cdot 3^k} \equiv 1 \pmod{3^{a+1}},$$

τότε έχουμε

$$2^{2\cdot 3^k} \equiv 1 \pmod{3^a},$$

το οποίο, σύμφωνα με την υπόθεση επαγωγής, είναι άτοπο. Άρα, για κάθε $k = 0, \ldots, a-2$ ισχύει

$$2^{2\cdot 3^k} \not\equiv 1 \pmod{3^{a+1}}.$$

Ας υποθέσουμε ότι $2^{2\cdot 3^{a-1}} \equiv 1 \pmod{3^{a+1}}$. Τότε έχουμε:

$$(2^{3^{a-1}}+1)(2^{3^{a-1}}-1) \equiv 0 \pmod{3^{a+1}}$$

ή

$$3^{a+1} \mid (2^{3^{a-1}}+1)(2^{3^{a-1}}-1).$$

Αν $3^{a+1} \mid 2^{3^{a-1}}-1$, τότε $2^{3^{a-1}} \equiv 1 \pmod 3$. Από την άλλη πλευρά όμως, έχουμε

$$2^{3^{a-1}} \equiv (2^3)^{3^{a-2}} \equiv 2^{3^{a-2}} \equiv \cdots \equiv 2 \pmod 3$$

που είναι άτοπο. Άρα, $3^{a+1} \nmid 2^{3^{a-1}}-1$ και επομένως έχουμε $3^{a+1} \mid 2^{3^{a-1}}+1$. Ισχύει ότι

$$2^{3^{a-1}}+1 = 3(2^{3^{a-2}2}-2^{3^{a-2}}+1)$$

οπότε

$$3^{a+1} \mid 3(2^{3^{a-2}2}-2^{3^{a-2}}+1)$$

που συνεπάγεται ότι

$$9 \mid 2^{3^{a-2}2}-2^{3^{a-2}}+1.$$

Έτσι, για $x = 2^{3^{a-2}}$ επαληθεύεται η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod 9$ με $f(x) = x^2-x+1$. Από την άλλη πλευρά, θεωρούμε το πλήρες σύστημα υπολοίπων $\pmod 9$ $\{0, \pm 1, \pm 2, \pm 3, \pm 4\}$. Τότε, ισχύει: $f(0) = f(1) = 1$, $f(-1) = f(2) = 3$, $f(-2) = 7$, $f(3) = -2$, $f(-3) = 4$, $f(4) = 13$ και $f(-4) = 21$. Καμία από αυτές τις τιμές δεν επαληθεύει την πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod 9$. Συνεπώς, ισχύει:

$$2^{2\cdot 3^{a-1}} \not\equiv 1 \pmod{3^{a+1}}.$$

Άρα, δείξαμε ότι για $k = 0, 1, \ldots, n-2$ ισχύει $2^{2\cdot 3^k} \not\equiv 1 \pmod{3^n}$ και κατά συνέπεια ο ακέραιος 2 είναι αρχική ρίζα $\pmod{3^n}$.

β) Πρώτα παρατηρούμε ότι ένας ακέραιος b με $0 \le b < \phi(3^n)$ είναι λύση της $2^x \equiv a \pmod{3^n}$ αν και μόνον αν ο $\phi(3^n)-b$ είναι λύση της $2^x a \equiv 1 \pmod{3^n}$. Επίσης, ένας ακέραιος b με $0 \le b < \phi(3^n)$ είναι λύση της $2^x a \equiv 1 \pmod{3^n}$ αν και μόνον αν ο $b-1$ είναι λύση της $2^x(2a) \equiv 1 \pmod{3^n}$. Άρα, η εύρεση του $\operatorname{ind}_2 a \pmod{3^n}$ είναι ισοδύναμη με την επίλυση της $2^x c \equiv 1 \pmod{3^n}$, όπου c ακέραιος με $c \equiv 1 \pmod 3$. Καθώς $c \equiv 1 \pmod 3$, έχουμε $2^x \equiv 1 \pmod 3$. Έτσι, αν ο x είναι περιττός, τότε $2^x \equiv 2 \not\equiv 1 \pmod 3$ που είναι άτοπο. Άρα, ο x είναι άρτιος. Έτσι, λοιπόν ο ακέραιος y είναι λύση της $2^x c \equiv 1 \pmod{3^n}$ έχει λύση αν και μόνον αν ο $y/2$ είναι λύση της $4^x c \equiv 1 \pmod{3^n}$. Συνεπώς, η εύρεση του δείκτη $\operatorname{ind}_2 a \pmod{3^n}$, όπου a ακέραιος με $(a,3)=1$, είναι ισοδύναμη με την επίλυση της $4^x c \equiv 1 \pmod{3^n}$, όπου c ακέραιος με $c \equiv 1 \pmod 3$. □

Στη συνέχεια θα δούμε μια ισοτιμία με δύο αγνώστους. Αν και δεν έχουμε προαναφέρει κάποια συγκεκριμένη μέθοδο επίλυσης τέτοιων ισοτιμιών, παρόλα αυτά μπορούμε να προσεγγίσουμε με τις υπάρχουσες γνώσεις αρκετούς τρόπους υπολογισμού των ζευγών των λύσεων. Εμείς θα τις προσεγγίσουμε ως διωνυμική ισοτιμία.

΄Ασκηση 6.16. *Να βρεθούν όλες οι αρχικές ρίζες* $(\mathrm{mod}\ 7)$ *και να προσδιοριστούν όλα τα ζεύγη ακεραίων* (x, y) *που επαληθεύουν την ισοτιμία*

$$y^2 - 2x^3 \equiv 0\,(\mathrm{mod}\ 7).$$

Απόδειξη. Καθώς ο 7 είναι πρώτος, υπάρχουν αρχικές ρίζες $(\mathrm{mod}\,7)$. ΄Εχουμε ότι $\phi(7) = 6 = 2 \cdot 3$ και $\phi(\phi(7))) = 2$. ΄Αρα υπάρχουν μόνο δύο ανισότιμες αρχικές ρίζες $(\mathrm{mod}\ 7)$. ΄Εχουμε:

$$3^{\phi(7)/3} \equiv 9 \equiv 2\,(\mathrm{mod}\ 7),\quad 3^{\phi(7)/2} \equiv 27 \equiv 6\,(\mathrm{mod}\ 7),$$
$$5^{\phi(7)/3} \equiv 25 \equiv 4\,(\mathrm{mod}\ 7),\quad 5^{\phi(7)/2} \equiv 125 \equiv 6\,(\mathrm{mod}\ 7).$$

Επομένως, οι ακέραιοι 3 και 5 είναι δύο ανισότιμες αρχικές ρίζες $(\mathrm{mod}\ 7)$.

Αν $7 \mid x$, δηλαδή $x \equiv 0\,(\mathrm{mod}\,7)$, έχουμε ότι $y^2 \equiv 0\,(\mathrm{mod}\,7)$ που ισοδυναμεί με $y \equiv 0\,(\mathrm{mod}\,7)$. Αν $7 \nmid x$, τότε $(7, x) = 1$ και επομένως $(7, y) = 1$. Καθώς το 5 είναι αρχική ρίζα $(\mathrm{mod}\ 7)$, η ισοτιμία $y^2 \equiv 2x^3\,(\mathrm{mod}\ 7)$ είναι ισοδύναμη με την ισοτιμία

$$2\,\mathrm{ind}_5\, y \equiv \mathrm{ind}_5\, 2 + 3\,\mathrm{ind}_5\, x\,(\mathrm{mod}\ 6).$$

Ισχύει $5^4 \equiv 2\,(\mathrm{mod}\ 7)$. Συνεπώς, αρκεί να λύσουμε την γραμμική ισοτιμία

$$2z - 3w \equiv 4\,(\mathrm{mod}\ 6),$$

όπου $z = \mathrm{ind}_5\, y$ και $w = \mathrm{ind}_5\, x$. Πολλαπλασιάζοντας την παραπάνω ισοτιμία με 2, παίρνουμε $4z \equiv 2\,(\mathrm{mod}\ 6)$, απ΄ όπου $z \equiv 2, 5\,(\mathrm{mod}\ 6)$. Για $z \equiv 2, 5 \bmod 6$ προκύπτει ότι $w \equiv 1, 3, 5\,(\mathrm{mod}\ 6)$. ΄Ετσι, έχουμε:

$$\begin{aligned}
&\mathrm{ind}_5\, y \equiv 2\,(\mathrm{mod}\ 6) \iff y \equiv 5^2\,(\mathrm{mod}\ 7) \iff y \equiv 4\,(\mathrm{mod}\ 7),\\
&\mathrm{ind}_5\, y \equiv 5\,(\mathrm{mod}\ 6) \iff y \equiv 5^5\,(\mathrm{mod}\ 7) \iff y \equiv 3\,(\mathrm{mod}\ 7),\\
&\mathrm{ind}_5\, x \equiv 1\,(\mathrm{mod}\ 6) \iff x \equiv 5^1\,(\mathrm{mod}\ 7) \iff x \equiv 5\,(\mathrm{mod}\ 7),\\
&\mathrm{ind}_5\, x \equiv 3\,(\mathrm{mod}\ 6) \iff x \equiv 5^3\,(\mathrm{mod}\ 7) \iff x \equiv 6\,(\mathrm{mod}\ 7),\\
&\mathrm{ind}_5\, x \equiv 5\,(\mathrm{mod}\ 6) \iff x \equiv 5^5\,(\mathrm{mod}\ 7) \iff x \equiv 3\,(\mathrm{mod}\ 7).
\end{aligned}$$

Επομένως, οι λύσεις της ισοτιμίας είναι τα εξής ζεύγη:

$$(x, y) = (0,0), (3,3), (3,4), (5,3), (5,4), (6,3), (6,4)\,(\mathrm{mod}\ 7).$$

□

Η επόμενη άσκηση είναι από εθνικό διαγωνισμό της Ρουμανίας [1].

΄Ασκηση 6.17. *Να βρεθούν όλα τα ζεύγη* $(m, n) \in \mathbb{Z}$ *με* $m, n \geq 2$ *τέτοια ώστε* $m \mid a^n - 1$ *για κάθε* $a \in \{1, \ldots, n\}$.

Απόδειξη. Ας υποθέσουμε ότι (m,n) είναι ένα ζεύγος με τις ζητούμενες ιδιότητες. Ας είναι p πρώτος με $p \mid m$. Αν $p \leq n$ τότε για $a = p$ θα είχαμε $p \mid p^n - 1$, απ΄ όπου έπεται $p \mid 1$, το οποίοι είναι αδύνατο. ΄Αρα $p > n$ και καθώς $n \geq 2$ συνεπάγεται ότι $p \geq 3$. Επομένως, το m έχει μόνο περιττούς πρώτους διαιρέτες.

Ας είναι τώρα $p \geq n+2$. Αν n περιττός, τότε έχουμε $n+1$ άρτιος και $p > n+1$. Αν n άρτιος, τότε $n+2$ άρτιος και επομένως $p > n+2$, καθώς ο p είναι περιττός. ΄Ετσι, σε κάθε περίπτωση υπάρχει άρτιος k με $n < k < p$ και $k/2 \leq n$. Επομένως, έχουμε

$$k^n = 2^n \left(\frac{k}{2}\right)^n \equiv 1 \pmod{m},$$

και, καθώς $p \mid m$ παίρνουμε $k^n \equiv 1 \pmod{p}$. Οι ακέραιοι $1, \ldots, n, k$ αποτελούν $n+1$ διαφορετικές λύσεις $(\mathrm{mod}\ p)$ της πολυωνυμικής ισοτιμίας $x^n - 1 \equiv 0 \pmod{p}$. Αυτό όμως, σύμφωνα με το Θεώρημα του Lagrange (6.1), είναι αδύνατο. ΄Αρα $p < n+2$ και σε συνδυασμό με το ότι $p > n$ έχουμε ότι το m έχει μοναδικό πρώτο διαιρέτη τον p με $p = n+1$. Δηλαδή, ο m είναι της μορφής p^s και n της μορφής $p-1$.

Ας είναι $(m,n) = (p^s, p-1)$ με $s \geq 2$. Ισχύει:

$$\begin{aligned}(p-1)^{p-1} - 1 &= \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^{p-1-i} p^i - 1 \\ &\equiv \binom{p-1}{0}(-1)^{p-1} + \binom{p-1}{1}(-1)^{p-2} p - 1 \pmod{p^2} \\ &\equiv 1 - (p-1)p - 1 \pmod{p^2} \\ &\equiv p \pmod{p^2}.\end{aligned}$$

Δηλαδή, $p^2 \nmid (p-1)^{p-1} - 1$ που συνεπάγεται ότι $p^s \nmid (p-1)^{p-1} - 1$ για κάθε $s \geq 2$. Από την άλλη πλευρά όμως για $a = p-1$ έχουμε $p^s \mid (p-1)^{p-1} - 1$. ΄Ετσι, καταλήγουμε σε άτοπο και επομένως $s = 1$. ΄Αρα, τα ζεύγη (m,n) είναι της μορφής $(p, p-1)$.

Τέλος, για κάθε $a \in \{1, \ldots, n\}$ από το Μικρό Θεώρημα του Fermat έχουμε ότι $a^{p-1} \equiv 1 \pmod{p}$, δηλαδή, $p \mid a^{p-1} - 1$. ΄Αρα, όλα τα ζεύγη της μορφής $(p, p-1)$, όπου p περιττός πρώτος, έχουν την ιδιότητα της άσκησης. □

΄Ασκηση 6.18 (American Mathematical Monthly, 11254 [3])**.** *Ας είναι p πρώτος ≥ 5 και g αρχική ρίζα* $(\mathrm{mod}\ p)$*. Θεωρούμε το σύνολο*

$$S_p = \left\{ a \in \mathbb{Z}^+ \mid a < \frac{p-1}{2},\ (a, p-1) = 1 \right\}.$$

Να βρεθούν οι πρώτοι p για τους οποίους ο ακέραιος g^s, όπου $s = \sum_{a \in S_p} a$, είναι αρχική ρίζα $(\mathrm{mod}\ p)$*.*

Απόδειξη. Ο ακέραιος g^s είναι αρχική ρίζα $(\mathrm{mod}\ p)$ αν και μόνον αν $(s, p-1) = 1$. Συνεπώς, αρκεί να προσδιορίσουμε τους πρώτους p με $(s, p-1) = 1$.

Ας είναι $p \equiv 1 \pmod{4}$. Αν $p = 5$, τότε $S_p = \{1\}$ και επομένως $s = 1$. ΄Ετσι, ο ακέραιος g^s είναι αρχική ρίζα. Ας υποθέσουμε ότι $p \neq 5$. Προφανώς, $a \in S_p$ αν και μόνον αν $(p-1)/2 - a \in S_p$. Αν $(p-1)/2 - a = a$, τότε $a = (p-1)/4$ και καθώς $p > 5$

έχουμε ότι $((p-1)/4, p-1) = (p-1)/4 \neq 1$. Άρα $(p-1)/2 - a \neq a$ για κάθε $a \in S_p$ και επομένως το πλήθος των στοιχείων του S_p είναι άρτιο. Όμως, κάθε στοιχείο του S_p είναι περιττός, οπότε s άρτιος και επομένως $(s, p-1) \neq 1$.

Ας υποθέσουμε τώρα ότι $p \equiv 3 \pmod 4$ με $(s, p-1) = 1$. Το πλήθος των θετικών ακεραίων $a < p-1$ που είναι πρώτοι με τον $p-1$ είναι $\phi(p-1)$. Παρατηρούμε ότι $a \in S_p$ αν και μόνον αν $p-1-a \notin S_p$ και $(p-1-a, p-1) = 1$. Έτσι, καθώς $a \neq (p-1)/2$, παίρνουμε:

$$|S_p| = \frac{1}{2}\,\phi(p-1).$$

Τα στοιχεία του S_p είναι περιττοί ακέραιοι. Οπότε, αν το πλήθος των στοιχείων του S_p είναι άρτιο (αντίστοιχα περιττό), τότε και το s που είναι άθροισμα περιττών ακεραίων είναι άρτιο (αντίστοιχα περιττό). Έτσι, έχουμε $|S_p| \equiv s \pmod 2$. Καθώς ισχύει $(s, p-1) = 1$, έπεται ότι ο $|S_p|$ είναι περιττός και επομένως $\phi(p-1) \equiv 2 \pmod 4$

Ας είναι $p_1^{a_1} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση του θετικού ακεραίου $p-1$. Ισχύει:

$$\phi(p-1) = p_1^{a_1-1} \cdots p_s^{a_s-1}(p_1-1)\cdots(p_s-1).$$

Καθώς όμως $\phi(p-1) = 2m$, όπου $m \in \mathbb{Z}^+$ είναι περιττός, ο $p-1$ δεν μπορεί να περιέχει παραπάνω από ένα πρώτο διαιρέτη. Έτσι, έχουμε $p-1 = 2q^k$, όπου q περιττός πρώτος και $k \in \mathbb{Z}^+$. Αν $q \equiv 1 \pmod 4$, τότε $4 \mid \phi(p-1)$ που είναι άτοπο. Άρα, έχουμε $q \equiv 3 \pmod 4$.

Τέλος, θα υπολογίσουμε το s. Το s ισούται με το άθροισμα των περιττών ακεραίων που είναι μικρότεροι του $(p-1)/2$ και δεν διαιρούνται από τον q. Καθώς $q \mid (p-1)/2$, υπολογίζουμε το άθροισμα των περιττών ακεραίων από το 1 έως και το $(p-1)/2$, και αφαιρούμε q φορές το άθροισμα των περιττών ακεραίων από το 1 έως και το $(p-1)/2q$. Σύμφωνα με την Άσκηση 1.2β, έχουμε:

$$1+3+\cdots+\frac{p-1}{2} = \left(\frac{p+1}{4}\right)^2 \quad \text{και} \quad 1+3+\cdots+\frac{p-1}{2q} = \left(\frac{p+1+2q}{4q}\right)^2.$$

Έτσι, παίρνουμε:

$$\begin{aligned} s &= \left(\frac{p+1}{4}\right)^2 - q\left(\frac{p-1+2q}{4q}\right)^2 = \frac{1}{4}(q^m+1)^2 - \frac{q}{4}(q^{m-1}+1)^2 \\ &= \frac{1}{4}(q-1)(q^{2m-1}-1). \end{aligned}$$

Επίσης, εύκολα διαπιστώνουμε ότι $(s, 2q^m) = 1$.

Συνεπώς οι προϋποθέσεις της εκφώνησης ικανοποιούνται για $p = 5$ και για p της μορφής $1 + 2q^k$, όπου q περιττός πρώτος της μορφής $q \equiv 3 \pmod 4$ και $k \in \mathbb{Z}^+$. □

6.5 Θεωρία Αριθμών με Maple

Για να λυθεί η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod n$ εντολή που εισάγουμε είναι η msolve(f(x)=0,n). Οι λύσεις που επιστρέφει η εντολή είναι $a \pmod n$ με $0 \leq a < n$. Σε περίπτωση που δεν υπάρχουν λύσεις η εντολή δεν επιστρέφει τίποτα.

΄Ασκηση 6.19. *Να βρεθούν οι λύσεις των παρακάτω πολυωνυμικών ισοτιμιών:*
α) $9x^{15} - 6x^{11} + x^2 + 23 \equiv 0 \pmod 7$,
β) $x^6 \equiv 1 \pmod{49}$,
γ) $x^3 + 10x^2 + x + 3 \equiv 0 \pmod{27}$,
δ) $x^3 + x^2 - 4 \equiv 0 \pmod{686}$,
ε) $6x^3 - 3x^2 + 17x - 10 \equiv 0 \pmod{30}$.

Απόδειξη. Με κώδικα Maple:

```
msolve(9*x^15-6*x^11+x^2+23 = 0, 7);
                  {x = 3}, {x = 5}, {x = 6}
msolve(x^6-1 = 0, 49);
{x = 1}, {x = 18}, {x = 19}, {x = 31}, {x = 30}, {x = 48}
msolve(x^3+10*x^2+x+3 = 0, 27);
                              {x = 15}
msolve(x^3+x^2-4 = 0, 686);

msolve(6*x^3-3*x^2+17*x-10 = 0, 30);
   {x = 2}, {x = 5}, {x = 11}, {x = 17}, {x = 20}, {x = 26}
```

□

΄Ασκηση 6.20. *Να βρεθούν οι ακέραιοι που επαληθεύουν τις παρακάτω πολυωνυμικές ισοτιμίες:*
α) $x^{15} \equiv 11 \pmod{26}$.
β) $2x^3 \equiv 5 \pmod{49}$.

Απόδειξη. Με κώδικα Maple:

```
msolve(x^15 = 11, 26);
msolve(2*x^3 = 5, 49);
                  {x = 3}, {x = 5}, {x = 41}
```

□

Με την εντολή msolve υπολογίζουμε και για τις λύσεις μιας εκθετικής ισοτιμίας. Το αποτέλεσμα της μορφής $a + b\_Z1$ ερμηνεύεται ως το $a \pmod b$.

΄Ασκηση 6.21. *Να βρεθούν οι ακέραιοι που επαληθεύουν τις παρακάτω εκθετικές ισοτιμίες:*
α) $25^x \equiv 17 \pmod{47}$,
β) $11^x \equiv 7 \pmod{13}$,
γ) $3^x \equiv 7 \pmod{22}$.

Απόδειξη. Με κώδικα Maple:

```
with(numtheory);
msolve(25^x = 17, 47);
                        {x = 8 + 23 _Z1}
msolve(11^x = 7, 13);
                        {x = 5 + 12 _Z1}
msolve(3^x = 7, 22);
```

□

Για τον υπολογισμό των αρχικών ριζών σύμφωνα αρκεί να βρούμε μία αρχική ρίζα. Η εντολή που εισάγουμε για να βρούμε μια αρχική ρίζα mod$n$ είναι η primroot(n) αφού πρώτα φορτώσουμε το πακέτο numtheory. Σε περίπτωση που για κάποιο n δεν υπάρχουν αρχικές ρίζες η εντολή επιστρέφει FAIL.

΄Ασκηση 6.22. *Να βρεθούν οι αρχικές ρίζες* mod91 *και* mod54.

Απόδειξη. Με κώδικα Maple:

```
with(numtheory);
primroot(54);
                                5
primroot(91);
                              FAIL
```

□

Έστω g μια αρχική ρίζα (mod n). Η εντολή που εισάγουμε για να υπολογίσουμε τον δείκτη $\text{ind}_g a$ είναι η mlog(a,g,n) αφού πρώτα φορτώσουμε το πακέτο numtheory. Φυσικά για έχει νόημα ο δείκτης $\text{ind}_g a$ θα πρέπει $(a, n) = 1$, διαφορετικά η εντολή επιστρέφει FAIL.

΄Ασκηση 6.23. *Να δειχθεί ότι ο 3 είναι αρχική ρίζα* mod17 *και να βρεθούν όλοι οι δείκτες των ακεραίων a με $(a, 17) = 1$ ως προς τη βάση* 3 mod 17.

Απόδειξη. Με κώδικα Maple:

```
with(numtheory);
 for i to 17 do if gcd(i,17)=1 then
 print(ind_3(i)=mlog(i,3,17)) end if end do
                          ind_3(1) = 0
                          ind_3(2) = 14
                          ind_3(3) = 1
                          ind_3(4) = 12
                          ind_3(5) = 5
                          ind_3(6) = 15
                          ind_3(7) = 11
                          ind_3(8) = 10
                          ind_3(9) = 2
                          ind_3(10) = 3
                          ind_3(11) = 7
                          ind_3(12) = 13
                          ind_3(13) = 4
                          ind_3(14) = 9
                          ind_3(15) = 6
                          ind_3(16) = 8
```

□

Για την επίλυση πολυωνυμικών ισοτιμιών με δύο αγνώστους χρησιμοποιούμε πάλι την εντολή msolve.

΄Ασκηση 6.24. *Να προσδιοριστούν όλα τα ζεύγη ακεραίων* (x, y) *που επαληθεύουν την ισοτιμία*

$$y^2 \equiv 5x^3 \pmod 7.$$

Απόδειξη. Με κώδικα Maple:

```
msolve(5*x^3 = y^2, 7);
{x = 0, y = 0}, {x = 3, y = 3}, {x = 3, y = 4}, {x = 5, y = 3},
  {x = 5, y = 4}, {x = 6, y = 3}, {x = 6, y = 4}
```

□

Βιβλιογραφία

[1] Andreescu, T., Feng, Z. and Lee, G.Jr. (2003). Mathematical Olympiads: Problems and Solutions from Around the World. American Mathematical Society.

[2] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[3] Jones, L., & Ernvall, T. (2008). Primes with Special Primitive Roots: 11254. The American Mathematical Monthly, 115(9), 861-861.

[4] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[5] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[6] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 7

Τετραγωνικά Υπόλοιπα

Το κεφάλαιο αυτό ξεκινά με την εισαγωγική ενότητα στα υπόλοιπα δυνάμεων και στη συνέχεια εστιάζει στα τετραγωνικά υπόλοιπα. Γίνεται αναλυτική παρουσίαση των συμβόλων Legendre και Jacobi, παρατίθεται μεθοδολογία υπολογισμού των συμβόλων αυτών και περιέχει ασκήσεις με την χρήση θεωρημάτων ορόσημα όπως το κριτήριο του Euler και οι νόμοι της τετραγωνικής αντίστροφης.

Ο Gauss αποκαλούσε το θεώρημα της τετραγωνικής αντιστροφής ως aureum theorema (χρυσό θεώρημα). Ο Euler το 1783 διατύπωσε το θεώρημα χωρίς όμως να το αποδείξει. Ο Legendre ήταν ο πρώτος που δημοσίευσε μια απόδειξη, αλλά ήταν λάθος. Το 1796, ο Gauss έγινε ο πρώτος που δημοσίευσε μια σωστή απόδειξη. Το θεώρημα της τετραγωνικής αντιστροφής ήταν το αγαπημένο θεώρημα του Gauss από τη θεωρία αριθμών και επινόησε οχτώ διαφορετικές αποδείξεις αυτού κατά τη διάρκεια της ζωής του ([6]).

Η προσπάθεια γενίκευσης του θεωρήματος τετραγωνικής αντιστροφής για δυνάμεις υψηλότερες από τη δεύτερη ήταν ένας από τους κύριους στόχους που οδήγησαν τους μαθηματικούς του 19ου αιώνα, όπως οι Gauss, Dirichlet, Jacobi, Dedekind, Kummer και Hilbert στη μελέτη των αλγεβρικών σωμάτων αριθμών και των δακτυλίων ακέραιων τους. Η μελέτη της γενίκευσης του θεωρήματος τετραγωνικής αντιστροφής θεωρείται από κάποιους πιο σημαντική από την μελέτη του τελευταίου θεωρήματος του Fermat ([4], [3]). Ο Hilbert συμπεριέλαβε την γενίκευση του θεωρήματος τετραγωνικής αντιστροφής στην περίφημη λίστα του με τα 23 προβλήματα που θεωρούσε ότι θα απασχολήσουν τους μαθηματικούς τον 20ο αιώνα. Το 9ο πρόβλημα του Hilbert, όπως είναι επίσης γνωστό το θεώρημα τετραγωνικής αντιστροφής, δεν έχει αποδειχθεί για όλα τα αλγεβρικά σώματα αριθμών. Για το λόγο παραμένει ένα από τα πιο ενδιαφέροντα πεδία έρευνας της θεωρίας αριθμών.

7.1 Υπόλοιπα Δυνάμεων

Ορισμός 7.1. Ας είναι $a, n, m \in \mathbb{Z}$ με $m \geq 1$, $n \geq 2$, $(a, n) = 1$. Ο ακέραιος a καλείται υπόλοιπο m-οστής δύναμης $(\mathrm{mod}\ n)$ αν η ισοτιμία $x^m \equiv a\ (\mathrm{mod}\ n)$ έχει λύση.

Το θεώρημα που ακολουθεί μας παρέχει την δυνατότητα να υπολογίζουμε υπό-

λοιπα m-οστής δύναμης $(\mathrm{mod}\ n)$ για συγκεκριμένα n.

Θεώρημα 7.1. *Ας είναι $m \in \mathbb{Z}^+$ και $n = 2, 4, p^r, 2p^r$, όπου p περιττός πρώτος και $r \in \mathbb{Z}^+$. Αν $a \in \mathbb{Z}$ με $(a, n) = 1$ και $d = (m, \phi(n))$, τότε ο a είναι υπόλοιπο m-οστής δύναμης $(\mathrm{mod}\ n)$, αν και μόνο αν, ισχύει:*

$$a^{\frac{\phi(n)}{d}} \equiv 1 \,(\mathrm{mod}\ n).$$

Το πλήθος των ανά δύο ανισότιμων υπολοίπων m-οστής δύναμης $(\mathrm{mod}\, n)$ είναι $\phi(n)/d$ και καθένα από αυτά είναι η m-οστή δύναμη ακριβώς d ακεραίων $(\mathrm{mod}\ n)$.

Απόδειξη. Βλέπε [9, Κεφάλαιο 5, Θεώρημα 6.1] □

Στην περίπτωση που το n δεν είναι της μορφής $2, 4, p^r, 2p^r$ τότε για να υπολογίσουμε τα υπόλοιπα m-οστής δύναμης $(\mathrm{mod}\, n)$ θα πρέπει να υπολογίσουμε το υπόλοιπο $(\mathrm{mod}\ n)$ για κάθε κλάση $(\mathrm{mod}\ n)$.

Ασκήσεις

΄Ασκηση 7.1. *Να βρεθούν όλα τα υπόλοιπα 35ης δύναμης $(\mathrm{mod}\ 49)$ και να λυθεί η ισοτιμία*

$$x^{35} \equiv a \,(\mathrm{mod}\ 49), \tag{7.1}$$

όπου a είναι ένα υπόλοιπο 35ης δύναμης $(\mathrm{mod}\ 49)$.

Απόδειξη. Εφόσον $49 = 7^2$, για να βρούμε όλα τα υπόλοιπα 35ης δύναμης $(\mathrm{mod}\ 49)$ αρκεί να προσδιορίσουμε τους ακεραίους a για τα οποίους ισχύει

$$a^{\frac{\phi(49)}{d}} \equiv 1 \,(\mathrm{mod}\ 49),$$

όπου $\phi(49) = \phi(7^2) = 7(7-1) = 42$ και $d = (\phi(49), 35) = (42, 35) = 7$. ΄Αρα, αρκεί να λύσουμε την πολυωνυμική ισοτιμία

$$a^6 \equiv 1 \,(\mathrm{mod}\ 49).$$

Η παραπάνω ισοτιμία έχει λυθεί στην ΄Ασκηση 6.1. Οι λύσεις της είναι:

$$a \equiv 1, 18, 19, 30, 31, 48 \,(\mathrm{mod}\ 49).$$

΄Αρα, τα υπόλοιπα 35ης δύναμης $(\mathrm{mod}\ 49)$ είναι οι ακέραιοι 1, 18, 19, 30, 31 και 48.

Σύμφωνα με το Θεώρημα 7.1, κάθε υπόλοιπο m-οστής δύναμης είναι η m-οστή δύναμη $d = (m, \phi(n))$ ακεραίων $(\mathrm{mod}\ n)$. Συνεπώς, η εξίσωση (7.1) έχει $d = 7$ λύσεις $(\mathrm{mod}\ 49)$ για κάθε $a \in \{1, 18, 19, 30, 31, 48\}$.

Θα λύσουμε την πολυωνυμική ισοτιμία

$$x^{35} \equiv 1 \,(\mathrm{mod}\ 49).$$

Κατά την λύση της ΄Ασκησης 6.12(β) δείξαμε ότι ο 3 είναι μια αρχική ρίζα $(\mathrm{mod}\ 49)$. Οπότε, η παραπάνω ισοτιμία είναι ισοδύναμη με την

$$35 \,\mathrm{ind}_3\, x \equiv 0 \,(\mathrm{mod}\ 42)$$

όπου προφανώς το 0 είναι ένας ακέραιος που την επαληθεύει. Συνεπώς έχουμε ότι οι λύσεις της εξίσωσης είναι οι $\text{ind}_3 x \equiv z \pmod{42}$, όπου $z \in \{0, 6, 12, 18, 24, 30, 36\}$. Άρα, οι ζητούμενες λύσεις είναι: $x \equiv 3^z \pmod{49}$ ($z = 0, 6, 12, 18, 24, 30, 36$), δηλαδή, οι $x \equiv 1, 43, 36, 29, 22, 15, 8 \pmod{49}$, αντίστοιχα.

Η επίλυση των υπολοίπων διωνυμικών ισοτιμιών αφήνεται στον αναγνώστη. □

Άσκηση 7.2. *Ας είναι p πρώτος. Ισχύουν τα εξής:*

α) *Αν $p = 3k + 2$, τότε κάθε ακέραιος a με $(a, p) = 1$ είναι υπόλοιπο τρίτης δύναμης $\pmod{p}$.*

β) *Αν $p = 3k + 1$, τότε υπάρχουν ακριβώς k ακέραιοι ανά δύο ανισότιμοι που είναι υπόλοιπα τρίτης δύναμης $\pmod{p}$.*

Απόδειξη. α) Ο a είναι υπόλοιπο τρίτης δύναμης $\pmod{p}$ αν και μόνον αν η ισοτιμία $x^3 \equiv a \pmod{p}$ έχει λύση. Επιπλέον, η ισοτιμία $x^3 \equiv a \pmod{p}$ έχει λύση αν και μόνον αν ισχύει $a^{\phi(p)/d} \equiv 1 \pmod{p}$, όπου $\phi(p) = p - 1$ και $d = (p - 1, 3)$. Αν $p = 3k + 2$, τότε $d = (3k + 1, 3) = 1$. Οπότε, ο a είναι υπόλοιπο τρίτης δύναμης $\pmod{p}$ αν και μόνον αν $a^{p-1} \equiv 1 \pmod{p}$ το οποίο αληθεύει (βλέπε Πόρισμα 4.1).

β) Από το Θεώρημα 7.1 προκύπτει ότι το πλήθος των ανά δύο ανισότιμων υπολοίπων τρίτης δύναμης $\pmod{p}$ είναι $\phi(p)/d$. Έχουμε $\phi(p) = p - 1 = 3k$ και $d = (p - 1, 3) = (3k, 3) = 3$. Άρα, ισχύει $\phi(p)/d = k$. □

7.2 Τετραγωνικά Υπόλοιπα

Ορισμός 7.2. Τα υπόλοιπα δεύτερης δύναμης $\pmod{n}$ καλούνται τετραγωνικά υπόλοιπα.

Θεώρημα 7.2. *Ας είναι $a, n \in \mathbb{Z}$, $n > 1$, $(a, n) = 1$ και $p_1, \ldots, p_s$ οι διαφορετικοί περιττοί πρώτοι παράγοντες του n. Η ισοτιμία $x^2 \equiv a \pmod{n}$ έχει λύση αν και μόνον αν ισχύουν τα εξής:*

α) *$n = p_1^{r_1} \cdots p_s^{r_s}$ ή $2p_1^{r_1} \cdots p_s^{r_s}$ και όλες οι ισοτιμίες $x^2 \equiv a \pmod{p_i}$ έχουν λύση.*

β) *$n = 4p_1^{r_1} \cdots p_s^{r_s}$, όλες οι ισοτιμίες $x^2 \equiv a \pmod{p_i}$ έχουν λύση και $a \equiv 1 \pmod{4}$.*

γ) *$n = 2^t p_1^{r_1} \cdots p_s^{r_s}$, $t \geq 3$, όλες οι ισοτιμίες $x^2 \equiv a \pmod{p_i}$ έχουν λύση και $a \equiv 1 \pmod{8}$.*

Αν η $x^2 \equiv a \pmod{n}$ έχει λύση, τότε το πλήθος των λύσεων της $\pmod{n}$ είναι 2^{s+u}, όπου $u = 0, 1, 2$ για τις περιπτώσεις (α), (β) και (γ), αντίστοιχα.

Απόδειξη. Βλέπε [9, Κεφάλαιο 6, Θεώρημα 1.1] ή [8, Πρόταση 5.3.4, εδώ]. □

Πόρισμα 7.1. *Ας είναι $a, n \in \mathbb{Z}$, $n > 1$, $(a, n) = 1$ και $p_1, \ldots, p_s$ οι διαφορετικοί περιττοί πρώτοι παράγοντες του n. Το a είναι τετραγωνικό υπόλοιπο $\pmod{n}$ αν και μόνον αν ισχύουν τα εξής:*

α) *$n = p_1^{r_1} \cdots p_s^{r_s}$ ή $2p_1^{r_1} \cdots p_s^{r_s}$ και a τετραγωνικό υπόλοιπο $\pmod{p_i}$.*

β) *$n = 4p_1^{r_1} \cdots p_s^{r_s}$, a τετραγωνικό υπόλοιπο $\pmod{p_i}$ και $a \equiv 1 \pmod{4}$.*

γ) *$n = 2^t p_1^{r_1} \cdots p_s^{r_s}$, $t \geq 3$, a τετραγωνικό υπόλοιπο $\pmod{p_i}$ και $a \equiv 1 \pmod{8}$.*

Απόδειξη. Βλέπε [9, Κεφάλαιο 6, Πόρισμα XXX]. □

Ασκήσεις

΄Ασκηση 7.3. *Να εξετάσετε αν το a είναι τετραγωνικό υπόλοιπο* (mod n)*, και στην περίπτωση που είναι, να υπολογιστεί το πλήθος των λύσεων της ισοτιμίας* $x^2 \equiv a \pmod{n}$*, όπου*

$\alpha)$ $a = 37$, $n = 2772$.

$\beta)$ $a = 89$, $n = 400$.

$\gamma)$ $a = 7$, $n = 99464$.

Απόδειξη. Πρώτα παρατηρούμε ότι σε όλες τις περιπτώσεις έχουμε $(a, n) = 1$.

α) Το 37 είναι τετραγωνικό υπόλοιπο (mod 2772) αν η εξίσωση

$$x^2 \equiv 37 \pmod{2772}$$

έχει λύση. Η πρωτογενής ανάλυση του 2772 είναι $2772 = 2^2 \cdot 3^2 \cdot 7 \cdot 11$. ΄Ετσι, η παραπάνω ισοτιμία έχει λύση, αν και μόνον αν, έχουν λύση οι ισοτιμίες

$$x^2 \equiv 37 \equiv 1 \pmod{3},$$
$$x^2 \equiv 37 \equiv 2 \pmod{7},$$
$$x^2 \equiv 37 \equiv 4 \pmod{11}$$

και $37 \equiv 1 \pmod{4}$. Πράγματι, η τελευταία ισοτιμία ισχύει, ενώ οι παραπάνω ισοτιμίες έχουν λύση $x \equiv 1, 2 \pmod{3}$ η πρώτη, $x \equiv 3, 4 \pmod{7}$ η δεύτερη και $x = 2, 9 \pmod{11}$, η τρίτη. Επομένως, η αρχική ισοτιμία έχει λύση και το πλήθος των λύσεων της είναι $2^{3+1} = 16$.

β) ΄Εχουμε $400 = 2^4 5^2$ και $89 \equiv 1 \pmod{8}$ και η ισοτιμία

$$x^2 \equiv 89 \equiv 4 \pmod{5}$$

έχει τις λύσεις $x \equiv 2, 3 \pmod{5}$. Επομένως, η αρχική ισοτιμία έχει λύση και το πλήθος των λύσεων της είναι 2^{s+u} όπου $s = 1$ και $u = 2$, δηλαδή 8.

γ) Παρατηρούμε ότι $2^3 \mid 99464$. Συνεπώς, αν η $x^2 \equiv 7 \pmod{99464}$ έχει λύση, τότε $7 \equiv 1 \pmod{8}$ το οποίο δεν συμβαίνει. ΄Αρα, η ισοτιμία δεν έχει λύση. □

7.3 Το Σύμβολο του Legendre

Ορισμός 7.3. Ας είναι $a \in \mathbb{Z}$ και p περιττός πρώτος. Το σύμβολο Legendre (a/p) ορίζεται ως εξής:

$$(a/p) = \begin{cases} 0, & \text{αν } p \mid a, \\ 1, & \text{αν ο } a \text{ είναι τετραγωνικό υπόλοιπο } (\mathrm{mod}\ p), \\ -1, & \text{αν ο } a \text{ δεν είναι τετραγωνικό υπόλοιπο } (\mathrm{mod}\ p). \end{cases}$$

Η πρόταση και το θεώρημα που ακολουθούν περιγράφουν τις βασικότερες ιδιότητες του συμβόλου Legendre.

Πρόταση 7.1. *Ας είναι p πρώτος περιττός και $a, b \in \mathbb{Z}$. Ισχύουν τα εξής:*

$\alpha)$ *Αν $a \equiv b \pmod{p}$, τότε $(a/p) = (b/p)$.*

β) $(a/p) \equiv a^{(p-1)/2} \pmod p$ (*Κριτήριο Euler*).
γ) $(ab/p) = (a/p)(b/p)$.
δ) *Αν* $p \nmid b$, *τότε* $(ab^2/p) = (a/p)$.

Απόδειξη. Βλέπε [9, Κεφάλαιο 6, Πρόταση 2.1] ή [5, Πρόταση 5.2.1, εδώ]. □

Θεώρημα 7.3. *Ας είναι* p, q *περιττοί πρώτοι διαφορετικοί μεταξύ τους. Τότε*
α) $(p/q) = (-1)^{(p-1)(q-1)/4}(q/p)$ (*νόμος τετραγωνικής αντιστροφής*),
β) $(-1/p) = (-1)^{(p-1)/2}$ (*πρώτος συμπληρωματικός νόμος της τετραγωνικής αντιστροφής*),
γ) $(2/p) = (-1)^{(p^2-1)/8}$ (*δεύτερος συμπληρωματικός νόμος της τετραγωνικής αντιστροφής*).

Απόδειξη. α) Βλέπε [9, Κεφάλαιο 6, Θεώρημα 2.2] ή [8, Θεώρημα 5.2.12, εδώ].
β) Βλέπε [9, Κεφάλαιο 6, Παράδειγμα 2.1] ή [8, Πόρισμα 5.2.2, εδώ].
γ) Βλέπε [9, Κεφάλαιο 6, Πόρισμα 2.1] ή [8, Πόρισμα 5.2.10, εδώ]. □

Πόρισμα 7.2. *Ας είναι* p *πρώτος. Τότε, έχουμε τα εξής:*
α) *Ο ακέραιος* -1 *είναι τετραγωνικό υπόλοιπο* $(\mathrm{mod}\, p)$ *αν και μόνον αν ισχύει* $p \equiv 1 \pmod 4$.
β) *Ο ακέραιος* 2 *είναι τετραγωνικό υπόλοιπο* $(\mathrm{mod}\, p)$ *αν και μόνον αν ισχύει* $p \equiv \pm 1 \pmod 8$.

Η ονομασία πρώτος και δεύτερος συμπληρωματικός νόμος τετραγωνικής αντιστροφής δεν είναι τυχαία αλλά αποδόθηκε διότι μαζί με τον τετραγωνικό νόμο της αντιστροφής επαρκούν για τον υπολογισμό οποιουδήποτε συμβόλου Legendre.

Υπολογισμός Συμβόλου Legendre. Τα βήματα υπολογισμού ενος συμβόλου Legendre (a/p), όπου p περιττός πρώτος και $p \nmid a$, είναι ως εξής:

1) Υπολογίζουμε a' τέτοιος ώστε $a \equiv a' \pmod p$ με $0 < a' < p$, Οπότε έχουμε:

$$(a/p) = (a'/p).$$

2) Αν μπορούμε να υπολογίσουμε εύκολα το (a'/p), τότε εξάγουμε το αποτέλεσμα. Αν όχι, τότε υπολογίζουμε την πρωτογενή ανάλυση του a'. Ας είναι $p_1, \ldots, p_n$ οι πρώτοι παράγοντες του a' που βρίσκονται σε περιττή δύναμη στην πρωτογενή του ανάλυση. Έτσι, έχουμε:

$$(a'/p) = (p_1/p) \cdots (p_n/p).$$

3) Αν μπορούμε να υπολογίσουμε εύκολα όλα τα (p_i/p), τότε εξάγουμε το αποτέλεσμα. Διαφορετικά, ας είναι s το αποτέλεσμα για τα (p_i/p) τα οποία μπορούμε να υπολογίσουμε εύκολα. Ας είναι (p_i'/p) $(i = 1, \ldots, m)$ αυτά τα οποία δεν υπολογίζονται εύκολα. Εφαρμόζοντας τον νόμο τετραγωνικής αντιστροφής, παίρνουμε:

$$(a'/p) = s(-1)^{(p-1)(p_1'-1)/4}(p/p_1') \cdots (-1)^{(p-1)(p_n'-1)/4}(p/p_m').$$

Στη συνέχεια, επαναλαμβάνουμε την ίδια διαδικασία από το βήμα 1 για κάθε σύμβολο Legendre (p/p_i').

Η παραπάνω διαδικασία υπολογισμού του συμβόλου Legendre δεν είναι απόλυτη. Χρησιμοποιώντας καταλλήλως τις ιδιότητες του συμβόλου πιθανόν να μπορούμε να φτάσουμε στο αποτέλεσμα ταχύτερα.

Ασκήσεις

΄Ασκηση 7.4. *Να υπολογιστεί το σύμβολο του Legendre* $(53/31)$.

Απόδειξη. Θα υπολογίσουμε το σύμβολο Legendre με δύο τρόπους. Στον πρώτο ακολουθούμε τα βήματα της διαδικασίας υπολογισμού του συμβόλου Legendre που περιγράφηκε ενώ στον δεύτερο υπολογίζουμε το σύμβολο κάνοντας «βολικές» αντικαταστάσεις. Καταρχάς, επιβεβαιώνουμε ότι το 31 δεν διαιρεί το 53.

1ος τρόπος. ΄Εχουμε:

$$\begin{aligned}(53/31) &\overset{\text{βήμα 1}}{=} (22/31)\\ &\overset{\text{βήμα 2}}{=} (2/31)\cdot(11/31)\\ &\overset{\text{βήμα 3}}{=} (-1)^{\frac{31^2-1}{8}}\cdot(-1)^{(31-1)(11-1)/4}(31/11) = -(31/11)\\ &\overset{\text{βήμα 1}}{=} -(9/11) = -1.\end{aligned}$$

2ος τρόπος. Καθώς $53 \equiv -9 \pmod{31}$ έχουμε:

$$(53/31) = (-9/31) = (-1/31)\cdot(9/31) = (-1)^{\frac{31-1}{2}}\cdot 1 = -1.$$

□

΄Ασκηση 7.5. *Να εξεταστεί αν το* 131 *και το* -999 *είναι τετραγωνικά υπόλοιπα* (mod 1999).

Απόδειξη. Καθώς ο αριθμός 1999 είναι πρώτος, μπορούμε να χρησιμοποιήσουμε το σύμβολο Legendre. Είναι προφανές ότι το 1999 δεν διαιρεί ούτε το 131 ούτε το 999, οπότε έχουμε:

$$\begin{aligned}(131/1999) &= (-1)^{(131-1)(1999-1)/4}(1999/131) = -(1999/131) = -(34/131)\\ &= -(2/131)(17/131) = -(-1)^{(131^2-1)/8}(-1)^{(131-1)(17-1)/4}(131/17)\\ &= (131/17) = (12/17) = (2^2 3/17) = (3/17)\\ &= (-1)^{(3-1)(17-1)/4}(17/3) = (17/3) = (2/3) = -1.\end{aligned}$$

΄Αρα, παίρνουμε $(131/1999) = -1$ και επομένως ο ακέραιος 131 δεν είναι τετραγωνικό υπόλοιπο (mod 1999).

Ομοίως, υπολογίζουμε:

$$\begin{aligned}(-999/1999) &= (1000/1999) = (2^3\cdot 5^3/1999) = (2\cdot 5/1999)\\ &= (2/1999)(5/1999) = (-1)^{1999^2-1/8}\,(-1)^{(5-1)(1999-1)/4}\,(1999/5)\\ &= (4/5) = (2^2/5) = 1.\end{aligned}$$

΄Αρα, ο ακέραιος -999 είναι τετραγωνικό υπόλοιπο (mod 1999). □

΄Ασκηση 7.6. *Να εξεταστεί αν οι ακόλουθες πολυωνυμικές ισοτιμίες έχουν λύση:*
α) $x^2 \equiv -1 \pmod{365}$,
β) $x^2 \equiv 2 \pmod{118}$,
γ) $x^2 \equiv 2 \pmod{7^3}$,
δ) $1709x^2 \equiv 2455 \pmod{4993}$.

Απόδειξη. α) Καθώς $365 = 5 \cdot 73$ και $(-1, 365) = 1$ σύμφωνα με το Θεώρημα 7.2 αρκεί να διερευνήσουμε αν οι ισοτιμίες $x^2 \equiv -1 \pmod 5$ και $x^2 \equiv -1 \pmod{73}$ έχουν λύση. Οπότε αρκεί να υπολογίσουμε τα παρακάτω σύμβολα Legendre:

$$(-1/5) = (-1)^{(5-1)/2} = 1,$$
$$(-1/73) = (-1)^{(73-1)/2} = 1.$$

Επομένως, η ισοτιμία $x^2 \equiv -1 \pmod{365}$ έχει λύση.

β) Καθώς $(2, 118) \neq 1$ δεν μπορούμε να επικαλεστούμε το Θεώρημα 7.2 αλλά την Πρόταση 6.2. ΄Εχουμε ότι $118 = 2 \cdot 59$ οπότε αρκεί να εξετάσουμε αν η ισοτιμίες $x^2 \equiv 2 \pmod 2$ και $x^2 \equiv 2 \pmod{59}$ έχουν λύση. Προφανώς η $x^2 \equiv 2 \pmod 2$ έχει λύση ενώ για να διερευνήσουμε αν η $x^2 \equiv 2 \pmod{59}$ έχει λύση αρκεί να δούμε αν το 2 είναι τετραγωνικό υπόλοιπο (mod 59) ή όχι. Ισχύει ότι:

$$(2/59) = (-1)^{(59^2-1)/8} = -1.$$

΄Αρα, η ισοτιμία $x^2 \equiv 2 \pmod{118}$ δεν έχει λύση.

γ) Αρκεί να διερευνήσουμε αν η ισοτιμία $x^2 \equiv 2 \pmod 7$ έχει λύση. Ισχύει:

$$(2/7) = (-1)^{(7^2-1)/8} = 1.$$

΄Αρα, η ισοτιμία $x^2 \equiv 2 \pmod{7^3}$ έχει λύση.

δ) Το 4993 είναι πρώτος οπότε $(4993, 1709) = 1$. Συνεπώς θα βρούμε τον αντίστροφο (mod 4993) του 1709 για να φέρουμε την ισοτιμία στην κατάλληλη μορφή. ΄Οπως έχουμε δει και σε προηγούμενες ενότητες, ο αντίστροφος μπορεί να υπολογιστεί με αρκετούς τρόπους. Στη συγκεκριμένη περίπτωση, λόγω του μεγέθους των αριθμών, επιλέγουμε να το κάνουμε χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο. Συνεπώς, έχουμε:

$$\begin{aligned}
4993 &= 2 \cdot 1709 + 1575 \\
1709 &= 1 \cdot 1575 + 134 \\
1575 &= 11 \cdot 134 + 101 \\
134 &= 1 \cdot 101 + 33 \\
101 &= 3 \cdot 33 + 2 \\
33 &= 16 \cdot 2 + 1
\end{aligned}$$

Στη συνέχεια, υπολογίζουμε:

$$\begin{aligned}
1 &= 33 - 16 \cdot 2 = 33 - 16 \cdot (101 - 3 \cdot 33) = -16 \cdot 101 + 49 \cdot 33 \\
&= -16 \cdot 101 + 49 \cdot (134 - 1 \cdot 101) = 49 \cdot 134 - 65 \cdot 101 \\
&= 49 \cdot 134 - 65 \cdot (1575 - 11 \cdot 134) = -65 \cdot 1575 + 764 \cdot 134 \\
&= -65 \cdot 1575 + 764 \cdot (1709 - 1 \cdot 1575) = 764 \cdot 1709 - 829 \cdot 1575 \\
&= 764 \cdot 1709 - 829 \cdot (4993 - 2 \cdot 1709) = -829 \cdot 4993 + 2422 \cdot 1709
\end{aligned}$$

Πολλαπλασιάζοντας την αρχική ισοτιμία με 2422 προκύπτει:

$$x^2 \equiv 2455 \cdot 2422 \pmod{4993} \equiv 4340 \pmod{4993}.$$

Καθώς ο 4993 είναι πρώτος, αρκεί να υπολογίσουμε το (4340/4993). Έτσι, έχουμε:

$$\begin{aligned}
&(4340/4993) = \\
&= (2^2 \cdot 5 \cdot 7 \cdot 31/4993) = (5/4993)(7/4993)(31/4993), \\
&= (-1)^{(5-1)(4993-1)/4+(7-1)(4993-1)/4+(31-1)(4993-1)/4}(4993/5)(4993/7)(4993/31), \\
&= (4993/5)(4993/7)(4993/31) = (3/5)(2/7)(2/31), \\
&= (-1)^{(5-1)(3-1)/4}(5/3)(-1)^{(7^2-1)/8}(-1)^{(31^2-1)/8}, \\
&= (2/3) = (-1)^{(3^2-1)/8} = -1.
\end{aligned}$$

Συνεπώς, η ισοτιμία $1709x^2 \equiv 2455 \pmod{4993}$ δεν έχει λύση. □

Άσκηση 7.7. *Να εξεταστεί αν οι ακόλουθες πολυωνυμικές ισοτιμίες έχουν λύση:*
α) $x^2 + 6x - 154 \equiv 0 \pmod{339}$,
β) $5x^2 + 7x + 1 \equiv 0 \pmod{775}$.

Απόδειξη. α) Ισχύει:

$$x^2 + 6x - 154 \equiv 0 \pmod{339} \iff (x+3)^2 \equiv 163 \pmod{339}.$$

Καθώς $339 = 3 \cdot 113$ και $(163, 339) = 1$ θα εξετάσουμε αν το 163 είναι τετραγωνικό υπόλοιπο (mod 3) και (mod 113). Έχουμε:

$$\begin{aligned}
&(163/3) = (1/3) = 1, \\
&(163/113) = (50/113) = (2/113)(5^2/113) = (-1)^{(113^2-1)/8} = 1.
\end{aligned}$$

Άρα, υπάρχει ακέραιος y τέτοιος, ώστε $y^2 \equiv 163 \pmod{339}$ και επομένως για $x = y-3$ η ισοτιμία έχει λύση.

β) Καθώς $775 = 5^2 \cdot 31$, για να έχει λύση η ισοτιμία θα πρέπει να έχουν λύση οι ισοτιμίες $5x^2 + 7x + 1 \equiv 0 \pmod{5}$ και $5x^2 + 7x + 1 \equiv 0 \pmod{31}$. Επειδή $(6, 31) = 1$, έχουμε:

$$\begin{aligned}
5x^2 + 7x + 1 \equiv 0 \pmod{31} &\iff -30x^2 - 42x - 6 \equiv 0 \pmod{31} \\
&\iff x^2 + 20x + 25 \equiv 0 \pmod{31} \\
&\iff (x+10)^2 \equiv 13 \pmod{31}.
\end{aligned}$$

Οπότε υπολογίζουμε το σύμβολο του Legendre

$$\begin{aligned}
(13/31) &= (-18/31) = (-1/31)(2/31)(9/31) \\
&= (-1)^{(31-1)/2}(-1)^{(31^2-1)/8} = -1.
\end{aligned}$$

Άρα η ισοτιμία δεν έχει λύση. □

Στη συνέχεια θα δούμε περισσότερο θεωρητικές ασκήσεις που σχετίζονται με τα σύμβολα Legendre και Jacobi.

΄Ασκηση 7.8. *Ας είναι περιττός πρώτος $p \neq 5$. Να δειχθεί:*

$$(5/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{10}, \\ -1, & p \equiv \pm 3 \pmod{10}. \end{cases}$$

Απόδειξη. Από τον νόμο της τετραγωνικής αντιστροφής έχουμε:

$$(5/p) = (p/5)(-1)^{(p-1)(5-1)/4} = (p/5).$$

Ο πρώτος p είναι τετραγωνικό υπόλοιπο (mod 5) αν και μόνον αν η ισοτιμία $x^2 \equiv p \pmod 5$ έχει λύση. Για $p \equiv 2, 3 \pmod 5$ διαπιστώνουμε ότι η παραπάνω ισοτιμία δεν έχει λύση, ενώ για $p \equiv 1, 4 \pmod 5$ έχει τις λύσεις $x \equiv \pm 1 \pmod 5$ και $x \equiv \pm 2 \pmod 5$, αντίστοιχα. Επιπλέον, έχουμε ότι $p \equiv 1 \pmod 2$. Οπότε, λύνοντας τα συστήματα

$$p \equiv \pm 1 \pmod 5, \quad p \equiv 1 \pmod 2$$

και

$$p \equiv \pm 2 \pmod 5, \quad p \equiv 1 \pmod 2$$

προκύπτουν οι ζητούμενες σχέσεις. □

΄Ασκηση 7.9. *Ας είναι περιττός πρώτος $p \neq 3$. Να δειχθεί:*

$$(-3/p) = \begin{cases} 1, & \text{αν } p \equiv 1 \pmod 6, \\ -1, & \text{αν } p \equiv -1 \pmod 6. \end{cases}$$

Απόδειξη. Από τις ιδιότητες του συμβόλου του Legendre και τον νόμο της τετραγωνικής αντιστροφής έχουμε:

$$(-3/p) = (-1/p)(3/p) = (-1)^{(p-1)/2}(p/3)(-1)^{(p-1)(3-1)/4} = (p/3)(-1)^{p-1} = (p/3).$$

Ο πρώτος p είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, 3)$ αν και μόνον αν η ισοτιμία $x^2 \equiv p \pmod 3$ έχει λύση. Αυτό όμως συμβαίνει, αν και μόνον αν, ισχύει $p \equiv 1 (\mathrm{mod}\ 3)$. Επιπλέον, έχουμε $p \equiv 1 \pmod 2$. Επομένως $(-3/p) = 1$ αν και μόνον αν $p \equiv 1 \pmod 3$ και $p \equiv 1 \pmod 2$ το οποίο ισοδυναμεί με $p \equiv 1 \pmod 6$.

Καθώς ο p είναι περιττός πρώτος, έχουμε $p \equiv 1, 5 \pmod 6$. Συνεπώς, ισχύει $(-3/p) = -1$ αν και μόνον αν ισχύει $p \equiv 5 \equiv -1 \pmod 6$. □

΄Ασκηση 7.10. *Να βρεθούν όλοι οι πρώτοι p για τους οποίους η πολυωνυμική ισοτιμία*

$$x^2 \equiv 13 \pmod p$$

έχει λύση.

Απόδειξη. Αν $p = 2$, τότε έχουμε την ισοτιμία $x^2 \equiv 1 \pmod 2$ η οποία έχει την λύση $x \equiv 1 \pmod 2$. Επίσης, αν $p = 13$, τότε η ισοτιμία $x^2 \equiv 0 \pmod{13}$ έχει προφανώς λύση. Ας υποθέσουμε ότι $p \geq 3$, $p \neq 13$. Από το νόμο της τετραγωνικής αντιστροφής έχουμε:

$$(13/p) = (p/13)(-1)^{(p-1)(13-1)/4} = (p/13)(-1)^{3(p-1)} = (p/13).$$

Από την άλλη πλευρά, τα μη-μηδενικά τετράγωνα (mod 13) είναι:

$$(\pm 1)^2 = 1 \,(\mathrm{mod}\ 13),\ \ (\pm 2)^2 = 4 \,(\mathrm{mod}\ 13),\ \ (\pm 3)^2 = 9 \,(\mathrm{mod}\ 13),$$

$$(\pm 4)^2 \equiv 3 \,(\mathrm{mod}\ 13),\ \ (\pm 5)^2 \equiv 12 \,(\mathrm{mod}\ 13),\ \ (\pm 6)^2 \equiv 10 \,(\mathrm{mod}\ 13).$$

Άρα, η ισοτιμία $x^2 \equiv 13 \pmod p$ έχει λύση, αν και μόνον αν, $p = 2, 13$ ή p της μορφής $1, 3, 4, 9, 10, 12 \pmod{13}$. □

Άσκηση 7.11. *Ας είναι p περιττός πρώτος. Να δειχθεί:*

$$\sum_{a=1}^{p-1} (a/p) = 0.$$

Απόδειξη. Ας είναι g αρχική ρίζα (mod p). Οι ακέραιοι $g, g^2, \ldots, g^{p-1}$ αποτελούν ένα περιορισμένο σύστημα υπολοίπων (mod p). Οι ακέραιοι $1, 2, \ldots, p-1$ αποτελούν επίσης ένα περιορισμένο σύστημα υπολοίπων (mod p). Άρα, κάθε στοιχείο του συνόλου $A = \{1, 2, \ldots, p-1\}$ θα είναι ισότιμο (mod p) με ένα ακριβώς στοιχείο του συνόλου $B = \{g, g^2, \ldots, g^{p-1}\}$. Δηλαδή, τα μισά στοιχεία του A είναι ισότιμα (mod p) με στοιχεία g^k του B, όπου k άρτιος, και τα άλλα μισα με στοιχεία g^k, όπου k περιττός.

Ας είναι $a_1, \ldots, a_{(p-1)/2}$ τα στοιχεία του συνόλου $\{1, 2, \ldots, p-1\}$ τα οποία είναι ισότιμα (mod p) με στοιχεία της μορφής $g^{2\ell_i}$ ($\ell_i = 1, \ldots, (p-1)/2$). Τότε, οι ακέραιοι a_i είναι τετραγωνικά υπόλοιπα (mod p), καθώς ισχύει:

$$\left(g^{\ell_i}\right)^2 \equiv a_i \,(\mathrm{mod}\ p).$$

Ας είναι $b_1, \ldots, b_{(p-1)/2}$ τα στοιχεία του συνόλου $\{1, 2, \ldots, p-1\}$ τα οποία είναι ισότιμα (mod p) με στοιχεία της μορφής $g^{2\ell_j+1}$, ($\ell_j = 0, \ldots, (p-3)/2$). Αν κάποιο από τα b_j είναι τετραγωνικό υπόλοιπο (mod p), τότε και το ισότιμό το, ας είναι το $g^{2\ell_s+1}$, είναι τετραγωνικό υπόλοιπο (mod p). Επομένως υπάρχει ακέραιος x_0 με $x_0^2 \equiv g^{2\ell_s+1} \pmod p$, απ΄ όπου προκύπτει

$$(g^{-\ell_s} x_0)^2 \equiv g \,(\mathrm{mod}\ p)$$

και κατά συνέπεια ο ακέραιος g είναι τετραγωνικό υπόλοιπο (mod p). Υψώνοντας και τα δύο μέλη της παραπάνω ισοτιμίας στη δύναμη $\phi(p)/2$, παίρνουμε:

$$g^{\phi(p)/2} \equiv (g^{-\ell_s} x_0)^{\phi(p)} \equiv 1 \,(\mathrm{mod}\ p).$$

Αυτό όμως είναι άτοπο και κατά συνέπεια οι ακέραιοι b_j δεν είναι τετραγωνικά υπόλοιπα (mod p).

Έτσι, για τα μισά στοιχεία του συνόλου $\{1, 2, \ldots, p-1\}$ τα οποία είναι τετραγωνικά υπόλοιπα (mod p) ισχύει $(a/p) = 1$, ενώ για τα άλλα μισά τα οποία δεν είναι τετραγωνικά υπόλοιπα (mod p) ισχύει $(a/p) = -1$. Συνεπώς, το άθροισμα όλων αυτών μας δίνει μηδέν. □

Άσκηση 7.12. *Ας είναι p πρώτος της μορφής $p \equiv 3 \pmod 4$. Αν $a, b \in \mathbb{Z}$ και $a^2 + b^2 \equiv 0 \pmod p$, τότε να δειχθεί ότι $a \equiv b \equiv 0 \pmod p$.*

Απόδειξη. Ας είναι $a \not\equiv 0 \pmod p$. Τότε, έχουμε $p \nmid a$, και καθώς ο p είναι πρώτος, παίρνουμε $(p, a) = 1$. Άρα, ο a έχει αντίστροφο (mod p) το οποίο συμβολίζουμε με a'. Έτσι, έχουμε:

$$a^2 + b^2 \equiv 0 \pmod p \Rightarrow 1 + b^2a'^2 \equiv 0 \pmod p \Rightarrow (ba')^2 \equiv -1 \pmod p.$$

Δηλαδή, το -1 είναι τετραγωνικό υπόλοιπο (mod p) και επομένως ισχύει $(-1/p) = 1$. Από τον πρώτο συμπληρωματικό νόμο της τετραγωνικής αντιστροφής, έχουμε:

$$(-1/p) = 1 \Rightarrow (-1)^{(p-1)/2} = 1 \Rightarrow (-1)^{(3+4k-1)/2} = 1 \Rightarrow (-1)^{2k+1} = 1.$$

Αυτό όμως είναι άτοπο και κατά συνέπεια ισχύει $a \equiv 0 \pmod p$. Έτσι έχουμε $b^2 \equiv 0 \pmod p$, απ΄ όπου έπεται $b \equiv 0 \pmod p$. □

7.4 Το Σύμβολο του Jacobi

Σ΄ αυτή την ενότητα θ΄ ασχοληθούμε με το σύμβολο Jacobi το οποίο είναι γενίκευση του συμβόλου Legendre.

Ορισμός 7.4. Ας είναι n θετικός περιττός ακέραιος > 1 και $n = p_1^{n_1} \cdots p_t^{n_t}$ η πρωτογενής ανάλυση του n. Τότε για κάθε $a \in \mathbb{Z}$, το σύμβολο Jacobi (a/n) ορίζεται ως εξής:

$$(a/n) = (a/p_1)^{n_1} \cdots (a/p_t)^{n_t},$$

όπου (a/p_i) τα σύμβολα Legendre.

Οι ιδιότητες και οι νόμοι της τετραγωνικής αντιστροφής του συμβόλου Jacobi είναι ανάλογοι του συμβόλου Legendre ([9, Κεφάλαιο 6, Πρόταση 3.1, Πρόταση 3.2, Θεώρημα 3.1]). Για αυτό και η διαδικασία υπολογισμού του συμβόλου Jacobi είναι ανάλογη της διαδικασίας υπολογισμού του συμβόλου Legendre. Να επισημανθεί η ιδιότητα:

$$(a/nm) = (a/n)(a/m), \quad \forall a \in \mathbb{Z},$$

η οποία δεν υφίσταται για το σύμβολο Legendre.

Παρατήρηση. Έστω (a/n) το σύμβολο Jacobi. Αν $(a/n) = -1$, τότε υπάρχει $i \in \{1, \ldots, n\}$ με $(a/p_i) = -1$ και επομένως, σύμφωνα με το Θεώρημα 7.2, το a δεν είναι τετραγωνικό υπόλοιπο (mod n). Αν όμως $(a/n) = 1$, σε αντίθεση με το σύμβολο Legendre, δεν σημαίνει ότι το a είναι τετραγωνικό υπόλοιπο (mod n). Επιπλέον, $(a/n) = 0$ αν και μόνον αν $(a, n) \neq 1$, δηλαδή ο a και ο n δεν είναι πρώτοι μεταξύ τους. Ο υπολογισμός δηλαδή του συμβόλου Jacobi είναι μία μέθοδος επαλήθευσης αν δύο ακέραιοι είναι πρώτοι μεταξύ τους.

Ασκήσεις

Άσκηση 7.13. *Να υπολογιστούν τα σύμβολα Jacobi (a/n) και να εξεταστεί αν το a είναι τετραγωνικό υπόλοιπο* (mod n) *στις παρακάτω περιπτώσεις:*

α) $a = 5683$, $n = 3425$,

β) $a = 3717$, $n = 7373$,

γ) $a = 676$, $n = 1337$.

Απόδειξη. Διαπιστώνουμε εύκολα ότι σε κάθε περίπτωση ισχύει $(a, n) = 1$.

α) Ακολουθώντας ανάλογη διαδικασία με τον υπολογισμό του συμβόλου Legendre έχουμε

$$\begin{aligned}(5683/3425) &= (5683/5^2)(5683/137) = (5683/137) = (66/137)\\ &= (2/137)(3/137)(11/137)\\ &= (-1)^{137^2-1/8}(-1)^{(3-1)(137-1)/4}(137/3)(-1)^{(11-1)(137-1)/4}(137/11)\\ &= 1\cdot 1\cdot (1/3)\cdot(-1)\cdot(5/11) = -(5/11)\\ &= -(-1)^{(11-1)(5-1)/4}(11/5) = -(11/5) = -(1/5) = -1.\end{aligned}$$

΄Αρα το 5683 δεν είναι τετραγωνικό υπόλοιπο (mod 3425).

β) ΄Εχουμε ότι

$$\begin{aligned}(3717/7373) &= (3^2\cdot 7\cdot 59/73\cdot 101) = (7\cdot 59/73\cdot 101)\\ &= (7/73)(7/101)(59/73)(59/101)\\ &= (-1)^{(7-1)(73-1)/4}(73/7)(-1)^{(7-1)(101-1)/4}(101/7)\\ &\quad\cdot(-1)^{(59-1)(73-1)/4}(73/59)(-1)^{(59-1)(101-1)/4}(101/59)\\ &= (73/7)(101/7)(73/59)(101/59) = (3/7)(3/7)(14/59)(42/59)\\ &= (14/59)(42/59) = (14/59)(14/59)(3/59) = (3/59)\\ &= (-1)^{(59-1)(3-1)/4}(59/3) = -(2/3) = 1.\end{aligned}$$

Εφόσον $7373 = 73\cdot 101$, ισχύει:

$$1 = (3717/7373) = (3717/73)(3717/101).$$

Οπότε, αν $(3717/73) = 1$, τότε $(3717/101) = 1$ και επομένως ο ακέραιος 3717 είναι τετραγωνικό υπόλοιπο (mod 7373). ΄Εχουμε:

$$\begin{aligned}(3717/73) &= (-6/73) = (-1/73)(2/73)(3/73)\\ &= (-1)^{(73-1)/2}(-1)^{(73^2-1)/8}(-1)^{(73-1)(3-1)/4}(73/3)\\ &= (1/3) = 1.\end{aligned}$$

΄Αρα $(3717/73) = (3717/101) = 1$ και κατά συνέπεια ο ακέραιος 3717 είναι τετραγωνικό υπόλοιπο (mod 7373).

γ) Εύκολα διαπιστώνουμε ότι

$$(676/1337) = (26^2/1337) = 1$$

Προφανώς, η ισοτιμία $x^2 \equiv 676 \pmod{1337}$ έχει λύση για $x = 26$. ΄Αρα το 676 είναι τετραγωνικό υπόλοιπο (mod 1337). □

7.5 Συνδυαστικές Ασκήσεις

΄Ασκηση 7.14 (American Mathematical Monthly, E3012 [7])**.** *Ας είναι a και b φυσικοί > 1 οι οποίοι είναι και οι δύο άρτιοι ή περιττοί. Τότε να δειχθεί ότι ισχύει:*

$$2^a - 1 \nmid 3^b - 1.$$

Απόδειξη. Ας υποθέσουμε ότι ο a είναι άρτιος. Τότε $2^a \equiv 1 \pmod 3$ και επομένως έχουμε $3 \mid 2^a - 1$. Έτσι, αν $2^a - 1 \mid 3^b - 1$, τότε $3 \mid 3^b - 1$, που είναι άτοπο για κάθε b.

Ας υποθέσουμε τώρα ότι ο a είναι περιττός. Θέτουμε $A = 2^a - 1$. Τότε, έχουμε $A \equiv 1 \pmod 3$ και επομένως $(A/3) = 1$. Οι ακέραιοι A και 3 είναι περιττοί και πρώτοι μεταξύ τους. Από τον νόμο της τετραγωνικής αμοιβαιότητας για το σύμβολο του Jacobi έχουμε:

$$(3/A) = (A/3)(-1)^{(A-1)/2} = (-1)^{2^{a-1}-1} = -1.$$

Άρα, ο ακέραιος 3 δεν είναι τετραγωνικό υπόλοιπο $\pmod A$.

Ας είναι $A \mid 3^b - 1$ με $b = 2n - 1$, όπου n φυσικός. Τότε, ισχύει $A \mid 3^{2n} - 3$ και επομένως $(3^n)^2 \equiv 3 \pmod A$ που είναι άτοπο. Άρα, αν οι φυσικοί a και b είναι περιττοί, τότε έχουμε $2^a - 1 \nmid 3^b - 1$. □

Άσκηση 7.15 (American Mathematical Monthly, E4790 [2])**.** *Έστω p περιττός πρώτος και έστω*

$$N_r(a) = \sum_{x_1,\dots,x_r=1}^{p-1} (x_1 \cdots x_r(a - x_1 - \cdots - x_r)/p),$$

όπου $a \in \mathbb{Z}$. Να δειχθεί ότι ισχύει:

$$N_{2m}(a) = (-1/p)^m (a/p) p^m, \quad N_{2m-1}(a) = \begin{cases} -(-1/p)^m p^{m-1}, & p \nmid a \\ (p-1)(-1/p)^m p^{m-1}, & p \mid a. \end{cases}$$

Απόδειξη. Αρχικά θα δείξουμε ότι ισχύει για $r = 2m - 1 = 1$. Ισχύει:

$$N_1(0) = \sum_{x=1}^{p-1} (-x^2/p) = \sum_{x=1}^{p-1} (-1/p) = (p-1)(-1/p). \tag{7.2}$$

Επιπλέον,

$$N_1(a) = \sum_{x=1}^{p-1} (x(a-x)/p) = \sum_{x=1}^{p-1} (x/p)(a - x/p)$$

και επομένως

$$\sum_{a=0}^{p-1} N_1(a) = \sum_{x=1}^{p-1} (x/p) \sum_{a=0}^{p-1} (a - x/p).$$

Για κάθε $x \in \{1, \dots, p-1\}$, καθώς το a διατρέχει τις τιμές από το 0 έως το $p-1$, η ποσότητα $a - x \pmod p$ παίρνει τις τιμές $0, 1, \dots, p-1$. Οπότε, σύμφωνα με την Άσκηση 7.11, έχουμε:

$$\sum_{a=0}^{p-1} (a - x/p) = (0/p) + \sum_{i=1}^{p-1} (i/p) = 0.$$

Συνδυάζοντας τις δύο προηγούμενες ισότητες, έχουμε

$$\sum_{a=0}^{p-1} N_1(a) = 0,$$

απ΄ όπου προκύπτει

$$\sum_{a=1}^{p-1} N_1(a) = -(p-1)(-1/p). \tag{7.3}$$

Επιπλέον, αν $a, b \in \mathbb{Z}$ με $p \nmid a$, $p \nmid b$ και $b \not\equiv a \pmod{p}$, τότε υπάρχει $s \neq 0, 1$ τέτοιο, ώστε $b \equiv sa \pmod{p}$. Έτσι, καθώς το γινόμενο $sx \pmod{p}$ διατρέχει όλες τις τιμές από 1 έως $p-1$, προκύπτει:

$$N_1(a) = \sum_{x=1}^{p-1}(s^2x(a-x)/p) = \sum_{x=1}^{p-1}(sx(sa-sx)/p) = \sum_{y=1}^{p-1}(y(b-y)/p) = N_1(b). \tag{7.4}$$

Έτσι, συνδυάζοντας τις ισότητα (7.3) και (7.4), έχουμε ότι για κάθε a με $p \nmid a$ ισχύει:

$$N_1(a) = -(-1/p).$$

Άρα, η προς απόδειξη σχέση ισχύει για $r = 1$.

Ας υποθέσουμε ότι ισχύει για κάθε $r < 2m$. Παρατηρούμε ότι

$$N_r(a) = \sum_{x_r=1}^{p-1}(x_r/p)N_{r-1}(a-x_r).$$

Έτσι, έχουμε

$$N_{2m}(a) = \sum_{x_{2m}=1}^{p-1}(x_{2m}/p)N_{2m-1}(a-x_{2m})$$

και από την υπόθεση της επαγωγής προκύπτει

$$N_{2m}(a) = (a/p)(-1/p)^m p^{m-1}(p-1) - \sum_{x_{2m}=1, p\nmid x_{2m}-a}^{p-1}(x_{2m}/p)(-1/p)^m(-p^{m-1}).$$

Σύμφωνα πάλι με την Άσκηση (7.11) έχουμε ότι

$$\sum_{x_{2m}=1, x_{2m}\not\equiv a \pmod{p}}^{p-1}(x_{2m}/p) = \sum_{x_{2m}=1}^{p-1}(x_{2m}/p) - (a/p) = -(a/p),$$

Οπότε, από τις παραπάνω δύο ισότητες, προκύπτει:

$$N_{2m}(a) = (a/p)(-1/p)^m p^m.$$

Τέλος, έχουμε:

$$\begin{aligned} N_{2m+1}(a) &= \sum_{x_{2m+1}=1}^{p-1} (x_{2m+1}/p) N_{2m}(a - x_{2m+1}) \\ &= \sum_{x_{2m+1}=1}^{p-1} (x_{2m+1}/p)(-1/p)^m ((a - x_{2m+1})/p) p^m \\ &= (-1/p)^m p^m \sum_{x_{2m+1}=1}^{p-1} (x_{2m+1}(a - x_{2m+1})/p) \\ &= (-1/p)^m p^m N_1(a). \end{aligned}$$

Άρα, ισχύει:

$$N_{2m+1}(a) = \begin{cases} (-1/p)^{m+1} p^m (-1), & p \nmid a \\ (-1/p)^{m+1} p^m (p-1), & p \mid a. \end{cases}$$

□

7.6 Θεωρία Αριθμών με Maple

Καθώς τα τετραγωνικά υπόλοιπα (mod n) συνδέονται άμεσα με την επίλυση μιας δευτέρου βαθμού εκθετική ισοτιμία, η εντολή msolve μπορεί να μας φανεί χρήσιμη στην διερεύνυση αν ένας ακέραιος είναι τετραγωνικό υπόλοιπο (mod n) όταν το n δεν είναι περιττός.

Άσκηση 7.16. *Να εξετάσετε αν το a είναι τετραγωνικό υπόλοιπο* (mod n) *και στην περίπτωση που είναι να υπολογιστεί το πλήθος των λύσεων της ισοτιμίας* $x^2 \equiv a \pmod{n}$*, όπου*

α) $a = 37$, $n = 2772$.
β) $a = 89$, $n = 400$.
γ) $a = 10$, $n = 99464$.

Απόδειξη. Με κώδικα Maple:

```
msolve(x^2 = 37, 2772);
  {x = 2341}, {x = 1025}, {x = 1747}, {x = 2033}, {x = 1333},
  {x = 431}, {x = 1439}, {x = 53}, {x = 739}, {x = 2125},
  {x = 361}, {x = 2411}, {x = 2719}, {x = 955}, {x = 647},
  {x = 1817}
msolve(x^2 = 89, 400);
  {x = 133}, {x = 317}, {x = 267}, {x = 283}, {x = 67},
  {x = 83}, {x = 333}, {x = 117}
msolve(x^2 = 10, 99464);
```

□

Άσκηση 7.17. *Να εξεταστεί αν οι παρακάτω πολυωνυμικές ισοτιμίες έχουν λύση:*

α) $x^2 \equiv -1 \pmod{365}$,
β) $x^2 \equiv 2 \pmod{118}$,
γ) $x^2 \equiv 2 \pmod{7^3}$,
δ) $1709x^2 \equiv 2455 \pmod{4993}$,
ε) $x^2 + 6x - 154 \equiv 0 \pmod{339}$,
$\sigma\tau$) $5x^2 + 7x + 1 \equiv 0 \pmod{775}$.

Απόδειξη. Με κώδικα Maple:

```
msolve(x^2 = -1, 365);
           {x = 27}, {x = 173}, {x = 192}, {x = 338}
msolve(x^2 = 2, 118);
                        {x = 36}, {x = 82}
msolve(x^2 = 2, 7^3);
                      {x = 108}, {x = 235}
msolve(1709*x^2 = 2455, 4993);
msolve(x^2+6*x-154 = 0, 399);
{x = 308}, {x = 28}, {x = 161}, {x = 175}, {x = 365}, {x = 218},
  {x = 85}, {x = 232}
msolve(5*x^2+7*x+1 = 0, 775);
```

□

Η εντολή που εισάγουμε για το υπολογισμό του συμβόλου Legendre (a/p) είναι η legendre(a,p) αφού πρώτα φορτώσουμε το πακέτο numtheory.

΄Ασκηση 7.18. *Να υπολογιστούν τα εξής σύμβολα του Legendre:*
α) (53/31),
β) (131/1999),
γ) (−999/1999).

Απόδειξη. Με κώδικα Maple:

```
with(numtheory);
legendre(131, 1999);
                                -1
legendre(131, 1999);
                                -1
legendre(-999, 1999);
                                1
```

□

Η εντολή που εισάγουμε για το υπολογισμό του συμβόλου Jacobi (a/n) είναι η Jacobi(a,n) αφού πρώτα φορτώσουμε το πακέτο numtheory.

΄Ασκηση 7.19. *Να υπολογιστούν τα εξής σύμβολα του Jacobi:*
α) (5683/3425),
β) (3717/7373),
γ) (676/1337).

Απόδειξη. Με κώδικα Maple:

```
with(numtheory);
jacobi(5683, 3425);
                                -1
jacobi(3717, 7373);
                                1
jacobi(676, 1337);
                                1
```

□

Για την εύρεση ακεραίων λύσεων σε εξισώσεις χρησιμοποιούμε την εντολή isolve.

΄Ασκηση 7.20. *Να βρεθούν οι ακέραιοι x, y που επαληθεύουν τις εξισώσεις:*
α) $5x^2 + 14xy + 11y^2 = 35$,
β) $5x^2 + 14xy + 11y^2 = 46$,
γ) $x^2 + xy + 5y^2 = 11$.

Απόδειξη. Με κώδικα Maple:

```
isolve(5*x^2+14*x*y+11*y^2 = 35);
       {x = -8, y = 5}, {x = -6, y = 5}, {x = -4, y = 1},
       {x = -2, y = 3}, {x = 2, y = -3}, {x = 4, y = -1},
       {x = 6, y = -5}, {x = 8, y = -5}
isolve(5*x^2+14*x*y+11*y^2 = 49);
isolve(x^2+x*y+5*y^2 = 11);
       {x = -3, y = 1}, {x = -2, y = -1},
       {x = 2, y = 1}, {x = 3, y = -1}
```

□

Βιβλιογραφία

[1] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[2] Carlitz, L. (1959). 4790. The American Mathematical Monthly, 66(3), 239-240. doi:10.2307/2309532

[3] Edwards, H. (1977). Fermat's Last Theorem. New York: Springer.

[4] Lemmermeyer, F. (2000). Reciprocity Laws, Springer Monographs in Mathematics, Berlin: Springer-Verlag.

[5] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[6] Nagell, T. (1951). The Quadratic Reciprocity Law. In Introduction to Number Theory (41). New York: Wiley.

[7] Selfridge, J., & Breusch, R. (1987). E3012. The American Mathematical Monthly, 94(1), 73-74. doi:10.2307/2323510

[8] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[9] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 8

Παράσταση Ακεραίων από Τετραγωνικές Μορφές

Το όγδοο κεφάλαιο είναι αφιερωμένο στις τετραγωνικές μορφές. Οι πρώτες δύο ενότητες αφορούν ιδιότητες των τετραγωνικών μορφών ενώ η τρίτη την παράσταση ακεραίων από δυαδικές μορφές.

Η τετραγωνικές μορφές συναντόνται σε πολλούς τομείς τομείς πέραν της θεωρία αριθμών, όπως η γραμμική άλγεβρα, η θεωρία ομάδων, η διαφορική γεωμετρία κ.α. Μελέτη τετραγωνικών μορφών ενός ακεραίου είχε γίνει στην αρχαιότητα (πυθαγόρειες τριάδες, Brahmagupta) ενώ ο Gauss στο βιβλίο του [3] ασχολείται εκτενώς με την τετραγωνική μορφή $ax^2+bxy+cy^2$, γεγονός που καταδεικνύει και την συμαντικότητάς τους.

8.1 Ακέραιοι και Τετραγωνικές Μορφές

Ορισμός 8.1. Ένα πολυώνυμο της μορφής

$$f(x_1,\dots,x_m)=\sum_{i,j=1}^{m} c_{ij}x_ix_j,$$

με $c_{ij}\in\mathbb{Z}$ καλείται *ακέραια τετραγωνική μορφή*. Ένας ακέραιος n καλείται *παραστάσιμος* από την ακέραια τετραγωνική μορφή $f(x_1,\dots,x_m)$ αν υπάρχει $(a_1,\dots,a_m)\in\mathbb{Z}^m$ τέτοιο ώστε $n=f(a_1,\dots,a_m)$, ενώ η m-άδα $(a_1,\dots,a_m)$ καλείται *παράσταση* του n. Αν $m=2$, τότε η τετραγωνική μορφή $f(x_1,x_2)$ καλείται *δυαδική*.

Στη συνέχεια θ΄ ασχοληθούμε με τις ακέραιες δυαδικές τετραγωνικές μορφές.

Ορισμός 8.2. Ας είναι $f(x,y)=ax^2+bxy+cy^2$ μία ακέραια δυαδική τετραγωνική μορφή. Ο ακέραιος $d=b^2-4ac$ καλείται *διακρίνουσα* της μορφής $f(x,y)$. Αν $d<0$, τότε η μορφή $f(x,y)$ καλείται *θετικά ορισμένη* ενώ αν $d>0$, τότε η $f(x,y)$ καλείται αρνητικά ορισμένη. Ο μκδ των a,b,c καλείται *διαιρέτης* της μορφής $f(x,y)$, ενώ αν $(a,b,c)=1$ τότε η $f(x,y)$ καλείται *αρχική δυαδική τετραγωνική μορφή*. Ας είναι n

ακέραιος παραστάσιμος από την $f(x,y)$ και (x_0,y_0) μια παράστασή του. Ο μκδ των x_0, y_0 καλείται *διαιρέτης της παράστασης* (x_0,y_0) ενώ αν $(x_0,y_0)=1$, τότε η παράσταση καλείται *αρχική*.

Ας είναι $f(x,y)$ μια θετικά ορισμένη αναγμένη μορφή. Καθώς $d<0$, παίρνουμε $ac\neq 0$. Πολλαπλασιάζοντας την $f(x,y)$ με $4a$ προκύπτει η χρήσιμη ταυτότητα

$$4af(x,y)=(2ax+by)^2+(4ac-b^2)y^2=(2ax+by)^2-dy^2. \tag{8.1}$$

Επιπλέον, έχουμε

$$d=b^2-4ac\leq a^2-4a^2,$$

απ΄ όπου προκύπτει

$$a\leq\sqrt{\frac{-d}{3}},$$

δηλαδή η ποσότητα a είναι φραγμένη από την διακρίνουσα d.

Πρόταση 8.1. *Ας είναι $f(x,y)=ax^2+bxy+cy^2$, μία ακέραια δυαδική μορφή, θετικά ορισμένη. Τότε, το πλήθος των παραστάσεων (x,y) ενός ακεραίου n από την $f(x,y)$ είναι πεπερασμένο και ισχύει*

$$|y|\leq 2\sqrt{\frac{an}{4ac-b^2}}.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 7, Πρόταση 1.1]. □

Ασκήσεις

΄Ασκηση 8.1. *Να βρεθεί ο μικρότερος θετικός ακέραιος που είναι παραστάσιμος από τις παρακάτω ακέραιες δυαδικές μορφές*

α) $f(x,y)=7x^2+25xy+23y^2$,
β) $f(x,y)=5x^2+6xy+7y^2$,
γ) $f(x,y)=11x^2+7xy+9y^2$.

Απόδειξη. (α) Ισχύει

$$d=25^2-4\cdot 7\cdot 23=-19$$

και επομένως η μορφή $f(x,y)$ είναι θετικά ορισμένη. Παρατηρούμε ότι $f(1,-1)=5$. Οπότε, από την ταυτότητα 8.1, έχουμε

$$(14x+25y)^2+19y^2\leq 140.$$

Επιπλέον, ισχύει:

$$|y|\leq 2\sqrt{7\cdot 5/(4\cdot 7\cdot 23-25^2)}\leq 2.$$

Για $y=1$, έχουμε:

$$(14x+25)^2+19\leq 140,$$

απ΄ όπου $|14x+25|\leq 11$ και επομένως $x\in\{-1,-2\}$. Για $y=-1$, έχουμε:

$$(14x-25)^2+19\leq 140$$

απ΄ όπου $|14x - 25| \leq 11$ και κατά συνέπεια $x \in \{1, 2\}$. Για $y = 2$, έχουμε:

$$(14x + 50)^2 + 76 \leq 140.$$

΄Ετσι, παίρνουμε $|14x + 50| \leq 8$, απ΄ όπου έχουμε $x \in \{-3, -4\}$. Για $y = -2$, έχουμε:

$$(14x - 50)^2 + 76 \leq 140$$

και επομένως $|14x + 50| \leq 8$, απ΄ όπου έπεται $x \in \{3, 4\}$. Τέλος, για $y = 0$ έχουμε: $(14x)^2 \leq 140$ και επομένως $x = 0$. Στη συνέχεια υπολογίζουμε:

$$f(0,0) = 0, \quad f(1,-1) = 5, \quad f(1,-2) = 49, \quad f(-1,1) = 5, \quad f(-1,2) = 49$$
$$f(2,-3) = 85, \quad f(2,-4) = 196, \quad f(-2,3) = 85, \quad f(-2,4) = 196.$$

΄Αρα, ο μικρότερος θετικός ακέραιος που είναι παραστάσιμος από την $f(x, y)$ είναι ο 5.

Με τον ίδιο τρόπο εργαζόμαστε και στις περιπτώσεις (β), (γ) και βρίσκουμε ότι ο μικρότερος ακέραιοι που είναι παραστάσιμοι από τις μορφές $f(x, y)$ είναι οι αριθμοί 5 και 9, αντίστοιχα. □

΄Ασκηση 8.2. *Να βρεθούν οι ακέραιοι x, y που επαληθεύουν τις εξισώσεις:*

α) $5x^2 + 14xy + 11y^2 = 35$,

β) $5x^2 + 14xy + 11y^2 = 46$,

γ) $x^2 + xy + 5y^2 = 11$.

Απόδειξη. Θα επιλύσουμε την πρώτη περίπτωση και θα παραθέσουμε τις λύσεις των άλλων δύο.

α) Η διακρίνουσα της μορφής $f(x, y) = 5x^2 + 14xy + 11y^2$ είναι -24 και επομένως η $f(x, y)$ είναι θετικά ορισμένη. Οπότε, για $f(x, y) = 35$ έχουμε

$$|y| \leq 2\sqrt{\frac{35 \cdot 5}{4 \cdot 5 \cdot 11 - 14^2)}} \leq 5.$$

Επιλύοντας την εξίσωση

$$5x^2 + 14xy + 11y^2 - 35 = 0$$

για $y = \{-5, -4, \ldots, 4, 5\}$, παίρνουμε τις λύσεις $(\pm 6, \mp 5)$, $(\pm 8, \mp 5)$, $(\pm 2, \mp 3)$, $(\pm 4, \mp 1)$.

β) Η εξίσωση δεν έχει ακέραιες λύσεις.

γ) Οι ακέραιες λύσεις της εξίσωσης είναι οι $(\pm 2, \pm 1)$, $(\pm 3, \mp 1)$. □

΄Ασκηση 8.3. *Το 0 έχει μία αρχική παράσταση από μια ακέραια δυαδική μορφή $f(x, y)$ αν και μόνον αν η διακρίνουσα του $f(x, y)$ ισούται με το τετράγωνο ακεραίου.*

Απόδειξη. Ας είναι $f(x, y) = ax^2 + bxy + cy^2$ μία ακέραια δυαδική μορφή και d η διακρίνουσά της. Αν $(x_0, y_0) \in \mathbb{Z}^* \times \mathbb{Z}^*$ με $f(x_0, y_0) = 0$, τότε έχουμε:

$$(2ax_0 + by_0)^2 - dy_0^2 = 0,$$

απ΄ όπου

$$d = \left(\frac{2ax_0 + by_0}{y_0}\right)^2,$$

δηλαδή, το d είναι τέλειο τετράγωνο.

Αντιστρόφως, ας είναι $d = k^2$. Τότε, ισχύει:

$$4af(x,y) = (2ax+by)^2 - (ky)^2 = (2ax+(b-k)y)(2ax+(b+k)y).$$

Θέτουμε $y_0 = -2a$, $x_0 = b+k$ και έχουμε $4af(x_0,y_0) = 0$. Άρα, το ζεύγος (x_0,y_0) είναι μια αρχική παράσταση του 0. □

Άσκηση 8.4. *Να δειχθεί ότι κανένας ακέραιος n με $n \equiv 3$ ή $5 \pmod 8$ δεν είναι παραστάσιμος από την μορφή $x^2 - 2y^2$.*

Απόδειξη. Παρατηρούμε ότι για έναν ακέραιο z ισχύει $z^2 \equiv 0,1,4 \pmod 8$. Έτσι, αν n είναι ακέραιος για τον οποίον υπάρχουν ακέραιοι x, y έτσι, ώστε $n = x^2 - 2y^2$, τότε $n \equiv 0,1,2,4,6,7 \pmod 8$. Συνεπώς, αν $n \equiv 3$ ή $5 \pmod 8$, τότε ο n δεν είναι παραστάσιμος από την μορφή $x^2 - 2y^2$. □

Άσκηση 8.5. *Να προσδιοριστούν όλοι οι θετικοί ακέραιοι που είναι παραστάσιμοι από την μορφή $x^2 - y^2$.*

Απόδειξη. Ας είναι n θετικός ακέραιος. Αν $n = 2m+1$, όπου m φυσικός, τότε θέτουμε $x = m+1$, $y = m$ και έχουμε:

$$x^2 - y^2 = (x+y)(x-y) = 2m+1 = n.$$

Άρα, αν ο n είναι περιττός, τότε είναι παραστάσιμος από την $x^2 - y^2$. Ας υποθέσουμε ότι $n \equiv 2 \pmod 4$. Αν υπάρχουν ακέραιοι x, y με $n = x^2 - y^2$, τότε έχουμε $x^2 - y^2 \equiv 2 \pmod 4$. Από την άλλη πλευρά, καθώς $x^2, y^2 \equiv 0,1 \pmod 4$, συνεπάγεται ότι $x^2 - y^2 \not\equiv 2 \pmod 4$ που είναι άτοπο. Τέλος, ας υποθέσουμε ότι $n = 4m$. Τότε, θέτουμε $x = m+1$, $y = m-1$ και έχουμε:

$$x^2 - y^2 = (x+y)(x-y) = 4m = n.$$

Συνεπώς, οι μόνοι θετικοί ακέραιοι που είναι παραστάσιμοι από την μορφή $x^2 - y^2$ είναι οι θετικοί ακέραιοι $n \not\equiv 2 \pmod 4$. □

8.2 Ισοδυναμία Τετραγωνικών Μορφών

Ας είναι $M_2(\mathbb{Z})$ το σύνολο των 2×2-πινάκων με στοιχεία ακέραιους αριθμούς. Αν $A \in M_2(\mathbb{Z})$, τότε θεωρούμε την απεικόνιση

$$\mu_A : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2,\ v \longmapsto vA.$$

Ορισμός 8.3. Η απεικόνιση μ_A καλείται *ακέραιος μετασχηματισμός* που αντιστοιχεί στον πίνακα A.

Συμβολίζουμε με G το σύνολο των ακεραίων μετασχηματισμών μ_A, όπου η ορίζουσα του A ισούται με ± 1.

Πρόταση 8.2. *Το σύνολο G εφοδιασμένο με την σύνθεση απεικονίσεων αποτελεί ομάδα.*

Απόδειξη. Βλέπε [7, Κεφάλαιο 7, Πρόταση 2.4]. □

Ας είναι $f(x,y) = ax^2 + bxy + cy^2$ και $g(x,y) = a'x^2 + b'xy + c'y^2$ δύο ακέραιες τετραγωνικές μορφές.

Ορισμός 8.4. Λέμε ότι η $f(x,y)$ είναι *ισοδύναμη* με την $g(x,y)$ και θα γράφουμε $f(x,y) \sim g(x,y)$, αν υπάρχει μετασχηματισμός $\mu_A \in G$ έτσι, ώστε $f(\mu_A(x,y)) = g(x,y)$.

Η $\sim$ είναι μία σχέση ισοδυναμίας στο σύνολο των ακεραίων τετραγωνικών μορφών (βλέπε [7, Κεφάλαιο 7, Πρόταση 2.5]).

Πρόταση 8.3. *Ας είναι $f(x,y)$ και $g(x,y)$ δύο ισοδύναμες ακέραιες τετραγωνικές μορφές και $\mu_A \in G$ με $g_A(x,y) = f(\mu_A(x,y))$. Τότε, ισχύουν τα εξής:*

α) Οι μορφές $f(x,y)$ και $g(x,y)$ έχουν τον ίδιο διαιρέτη και την ίδια διακρίνουσα.

β) Οι μορφές $f(x,y)$ και $g(x,y)$ παριστάνουν τους ίδιους ακεραίους.

γ) Οι παραστάσεις (x,y) και $\mu_A(x,y)$ ενός ακεραίου n από τις μορφές $g(x,y)$ και $f(x,y)$, αντίστοιχα, έχουν τον ίδιο διαιρέτη.

Απόδειξη. Βλέπε [7, Κεφάλαιο 7, Πρόταση 2.6] ή [6, Πρόταση 9.2.4, εδώ]. □

Ορισμός 8.5. Μια θετικά ορισμένη μορφή $f(x,y)$ καλείται αναγμένη αν $-a < b \leq a < c$ ή $0 < b \leq a = c$.

Το πλήθος των αναγμένων μορφών με διακρίνουσα $d < 0$ είναι πεπερασμένο [7, Κεφάλαιο 7, Πρόταση 3.1]. Σύμφωνα με το Θεώρημα 3.1 του [7, Κεφάλαιο 7], κάθε θετικά ορισμένη ακέραια τετραγωνική μορφή είναι ισοδύναμη με μία ακριβώς αναγμένη μορφή. Έτσι, παίρνουμε ότι το πλήθος των κλάσεων ισοδυναμίας θετικά ορισμένων τετραγωνικών μορφών με διακρίνουσα $d < 0$ είναι πεπερασμένο.

Έτσι, δοθείσης μίας θετικά ορισμένη ακέραια τετραγωνική μορφή $f(x,y)$ μπορεί να βρεθεί μία αναγμένη μορφή $h(x,y)$ η οποία είναι ισοδύναμη με την $f(x,y)$. Μία μέθοδος με την οποία είναι δυνατόν να γίνει αυτό, περιγράφεται κατά την απόδειξη του Θεώρημα 3.1 του [7, Κεφάλαιο 7], και την οποία δίνουμε παρακάτω.

Υπολογισμός ισοδύναμης αναγμένης μορφής. Ας είναι $f(x,y)$ μία θετικά ορισμένη ακέραια τετραγωνική μορφή. Θα υπολογίσουμε μία αναγμένη μορφή $g(x,y)$ ακολουθώντας τα εξής βήματα:

1) Υπολογίζουμε τον μικρότερο θετικός ακέραιο a που παριστάνεται από την $f(x,y)$ και ακέραιοι u, v πρώτοι μεταξύ τους έτσιι, ώστε $a = f(u,v)$.

2) Υπολογίζουμε ακέραιους z, w με $uz - vw = 1$.

3) Θεωρούμε τον πίνακα

$$T = \begin{pmatrix} u & v \\ w & z \end{pmatrix}$$

ο οποίος έχει ορίζουσα 1 και υπολογίζουμε την ακεραία μορφή

$$h(x,y) = f(\mu_T(x,y)) = ax^2 + kxy + my^2.$$

4) Υπολογίζουμε ένα ακέραιο j_0 τέτοιον ώστε να ισχύει $|k - 2aj_0| \leq a$.

5) Θεωρούμε τον πίνακα

$$T_{j_0} = \begin{pmatrix} 1 & 0 \\ -j_0 & 1 \end{pmatrix}$$

και υπολογίζουμε την ακεραία μορφή

$$g(x,y) = Ax^2 + Bxy + Cy^2,$$

όπου $A = a$, $B = k - 2aj_0$, $C = aj_0^2 - kj_0 + m$.

6) Αν $B > 0$, τότε η μορφή $g(x,y)$ είναι αναγμένη και ισοδύναμη με την $f(x,y)$. Αν $B < 0$, τότε θεωρούμε τον μετασχηματισμό $\mu(x,y) = (-x,y)$ και παίρνουμε την μορφή $g'(x,y) = g(\mu(x,y)) = Ax^2 - Bxy + Cy^2$ η οποία είναι αναγμένη και ισοδύναμη με την $f(x,y)$.

Απόδειξη της ορθότητας της μεθόδου. Από την κατασκεύη της $g(x,y)$ έχουμε ότι η $g(x,y)$ είναι ισοδύναμη με την $f(x,y)$. Σύμφωνα με την Πρόταση 8.3 ο ακέραιος a είναι ο μικρότερος ακέραιος που παριστάνεται από την $g(x,y)$. Καθώς $g(0,1) = C$, έχουμε $a \leq C$ και επομένως ισχύει $0 \leq B \leq A \leq C$. Οπότε, η $g(x,y)$ είναι αναγμένη. Αν $B < 0$, τότε η $g'(x,y)$ είναι αναγμένη.

Ασκήσεις

΄Ασκηση 8.6. *Να βρεθούν όλες οι αναγμένες μορφές με διακρίνουσα*

$$d \in \{-19, -20, -23, -24, -27, -28\}.$$

Ποιές από αυτές είναι αρχικές;

Απόδειξη. Ας είναι $f(x,y) = ax^2 + bxy + cy^2$ μία αναγμένη δυαδική μορφή με διακρίνουσα d. Αν $d = -20$, τότε έχουμε

$$a \leq \sqrt{\frac{-d}{3}} = \sqrt{\frac{20}{3}},$$

απ΄ όπου έπεται ότι $a \in \{1,2\}$. Αν $a = 1$, τότε έχουμε ότι $b \in \{0,1\}$. Για $b = 0$, από την σχέση $d = b^2 - 4ac$, παίρνουμε $c = 5$, ενώ για $b = 1$ προκύπτει ότι $c \notin \mathbb{Z}$. Αν $a = 2$, τότε έχουμε ότι $b \in \{-1,0,1,2\}$. Για $b = 2$ από την σχέση $d = b^2 - 4ac$ προκύπτει ότι $c = 3$, ενώ για $b \in \{-1,0,1\}$ παίρνουμε ότι $c \notin \mathbb{Z}$. ΄Αρα, για $d = -20$ οι αναγμένες μορφές είναι οι εξής:

$$x^2 + 5y^2, \quad 2x^2 + 2xy + 3y^2.$$

Καθώς $(1,5) = 1$ και $(2,2,3) = 1$ συνεπάγεται ότι και οι δύο αναγμένες μορφές είναι αρχικές.

Στον επόμενο πίνακα συνοψίζουμε τα αποτελέσματα για τα υπόλοιπα d.

Διακρίνουσα d	Αναγμένες Μορφές	Αναγμένες Αρχικές Μορφές
-19	x^2+5y^2	x^2+5y^2
-20	x^2+5y^2, $2x^2+2xy+3y^2$	x^2+5y^2, $2x^2+2xy+3y^2$
-23	$x^2+xy+6y^2$, $2x^2+xy+3y^2$	$x^2+xy+6y^2$, $2x^2+xy+3y^2$
-24	x^2+6y^2, $2x^2+3y^2$	x^2+6y^2, $2x^2+3y^2$
-27	$x^2+xy+7y^2$, $3x^2+3xy+3y^2$	$x^2+xy+7y^2$
-28	x^2+7y^2, $2x^2+2xy+4y^2$	x^2+7y^2

□

΄Ασκηση 8.7. *Να βρεθούν οι αναγμένες μορφές που είναι ισοδύναμες με τις μορφές:*
α) $2x^2-5xy+4y^2$,
β) $3x^2-7xy+11y^2$,
γ) $3x^2+xy+y^2$.
Επίσης, να βρεθεί ο πίνακας μετασχηματισμού σε κάθε περίπτωση.

Απόδειξη. Θα εφαρμόσουμε την μέθοδο υπολογισμού που περιγράψαμε παραπάνω διατηρώντας τους ίδιους συμβολισμούς.

α) Θέτουμε $f(x,y)=2x^2-5xy+4y^2$. Παρατηρούμε ότι ο μικρότερος θετικός ακέραιος που παριστάνεται από την $f(x,y)$ είναι ο 1 και ισχύει $1=f(1,1)$. Έτσι, έχουμε $u=v=1$. Οπότε, επιλέγουμε $z=2$, $w=1$ και θεωρούμε τον πίνακα

$$T=\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}.$$

Υπολογίζουμε:

$$h(x,y)=f(\mu_T(x,y))=f(x+y,x+2y)=x^2+5xy+8y^2.$$

΄Ετσι, έχουμε $a=1$, $k=5$ και $m=8$. Ο ακέραιος για τον οποίο ισχύει $|k-2aj_0|\le a$, δηλαδή $|5-2j_0|=1$, είναι $j_0=2$. Θεωρούμε τον πίνακα

$$T(2)=\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix}$$

και υπολογίζουμε:

$$g(x,y)=h(\mu_{T(2)}(x,y)=h(x-2y,y)=x^2+xy+2y^2.$$

Η μορφή $g(x,y)$ είναι αναγμένη και ο πίνακας του μετασχηματισμού από την $f(x,y)$ στη $g(x,y)$ είναι ο εξής:

$$A=\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}=\begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}.$$

β) Θέτουμε $f(x,y) = 3x^2 - 7xy + 11y^2$. Η διακρίνουσα της $f(x,y)$ είναι $d = -83$. Από την σχέση 8.1 έχουμε:

$$12f(x,y) = (6x - 7y)^2 + 83y^2.$$

Έτσι, αν $f(x,y) = 1$ ή 2, τότε καταλήγουμε σε άτοπο. Άρα, ο μικρότερος θετικός ακέραιος που παριστάνεται από την $f(x,y)$ είναι ο 3 και ισχύει $3 = f(1,0)$. Οπότε, έχουμε $u = 1$, $v = 0$ και επομένως παίρνουμε $z = 1$ και $w = 0$. Συνεπώς, ο πίνακας T είναι ο μοναδιαίος και έτσι $h(x,y) = f(x,y)$. Έχουμε λοιπόν $a = 3$, $k = -7$ και $m = 11$. Για $j_0 = -1$ ισχύει $|k - 2aj_0| \leq 3$ και επομένως θεωρούμε τον πίνακα

$$T(-1) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Υπολογίζουμε:

$$g(x,y) = h(\mu_{T(-1)}(x,y) = h(x+y,y) = 3x^2 - xy + 7y^2.$$

Η μορφή $g(x,y)$ είναι αναγμένη και ο πίνακας του μετασχηματισμού από την $f(x,y)$ στη $g(x,y)$ είναι ο $T(-1)$.

γ) Θέτουμε $f(x,y) = 3x^2 + xy + y^2$. Παρατηρούμε ότι η μορφή $g(x,y) = x^2 + xy + 3y^2$ είναι αναγμένη και ότι

$$g(x,y) = f(y,x) = f(\mu_A(x,y)),$$

όπου

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

□

8.3 Παράσταση Ακεραίων από Δυαδικές Μορφές

Θεώρημα 8.1. *Ένας ακέραιος $n \neq 0$ είναι παραστάσιμος κατά αρχικό τρόπο από μία τουλάχιστον μορφή με διακρίνουσα d αν και μόνον αν η πολυωνυμική ισοτιμία $x^2 \equiv d \pmod{4|n|}$ έχει λύση.*

Απόδειξη. Βλέπε [7, Κεφάλαιο 7, Θεώρημα 4.1] ή [6, Πρόταση 9.3.7, εδώ]. □

Θεώρημα 8.2. *Ένας ακέραιος n μπορεί να παρασταθεί ως άθροισμα δύο τετραγώνων αν και μόνον αν κάθε πρώτος παράγοντας του p με $p \equiv 3 \pmod 4$ βρίσκεται σε άρτια δύναμη στην πρωτογενή του ανάλυση.*

Απόδειξη. Βλέπε [7, Κεφάλαιο 7, Θεώρημα 4.2] ή [6, Πρόταση 9.3.9, εδώ]. □

Ασκήσεις

Άσκηση 8.8. *Να δειχθεί ότι ένας θετικός ακέραιος n είναι παραστάσιμος από την μορφή $x^2 + 2y^2$ αν και μόνον αν κάθε πρώτος διαιρέτης p του n με $p \equiv 5$ ή $7 \pmod 8$ εμφανίζεται με άρτια δύναμη στη πρωτογενή ανάλυση του n.*

Απόδειξη. Ας υποθέσουμε ότι υπάρχουν $x, y \in \mathbb{Z}$ με $n = x^2 + 2y^2$. Αν $\delta = (x, y)$, τότε $x = \delta x'$, $y = \delta y'$ και $(x', y') = 1$. Τότε $n = \delta^2 n'$, όπου $n' = (x'^2 + 2y'^2)$. Αντιστρόφως, αν $n = \delta^2(x'^2 + 2y'^2)$ με $(x', y') = 1$, τότε $n = \delta x'^2 + 2(\delta y')^2$. Δηλαδή, ο n παριστάνεται από την μορφή $x^2 + 2y^2$ αν και μόνον αν γράφεται ως $n = \delta^2 n'$ και ο n' έχει αρχική παράσταση από την μορφή x^2+2y^2. Σ΄ αυτή την περίπτωση έχουμε $4 \nmid n'$. Πράγματι, αν $4 \mid n'$, τότε $2 \mid x'$, απ΄ όπου έπεται ότι $2 \mid y'$. Καθώς όμως $(x', y') = 1$, αυτό είναι άτοπο.

Παρατηρούμε ότι η μορφή $x^2 + 2y^2$ είναι αναγμένη και ότι η διακρίνουσα της ισούται με -8. Θα δείξουμε ότι αυτή είναι η μοναδική αναγμένη μορφή με διακρίνουσα -8. Πράγματι, αν $f(x, y) = ax^2 + bxy + cy^2$ είναι μία αναγμένη μορφή με διακρίνουσα -8, τότε $0 \le b \le a \le c$ και επομένως $8 = 4ac - b^2 \ge 3ac$. ΄Αρα, έχουμε $c = 1$ ή 2. Αν $c = 1$, τότε $b = a = 1$ και επόμενως $8 \le 4$ που είναι άτοπο. Οπότε, έχουμε $c = 2$, $a = 1$ και $b = 0$. Συνεπώς, η $x^2 + 2y^2$ είναι η μοναδική αναγμένη μορφή με διακρίνουσα -8.

Ας υποθέσουμε ότι

$$m = 2^{\nu} p_1^{n_1} \cdots p_k^{n_k},$$

όπου $\nu = 0, 1, p_1, \ldots, p_k$ περιττοί διακεκριμμένοι πρώτοι και $n_1, \ldots, n_k$ θετικοί ακέραιοι. Σύμφωνα με τα παραπάνω, την Πρόταση 8.3 και το Θεώρημα 8.1, έπεται ότι ο ακέραιος m έχει μία αρχική παράσταση από την μορφή $x^2 + 2y^2$ αν και μόνον αν η πολυωνυμική ισοτιμία $x^2 \equiv -8 \pmod{4m}$ έχει λύση. Παρατηρούμε ότι η ισοτιμία αυτή έχει λύση αν και μόνον αν η ισοτιμία $x^2 \equiv -2 \pmod{m}$ έχει λύση. Αυτό συμβαίνει αν και μόνον αν όλες οι ισοτιμίες $x^2 \equiv -2 \pmod{p_i}$ έχουν λύση που ισοδυναμεί με $(-2/p_i) = 1$ $(i = 1, \ldots, k)$. Ισχύει

$$(-2/p_i) = (-1/p_i)(2/p_i).$$

Σύμφωνα με το Πόρισμα 7.2 έχουμε $(-1/p_i) = 1$ αν και μόνον αν $p_i \equiv 1 \pmod 4$ και $(2/p_i) = 1$ αν και μόνον αν $p_i \equiv \pm 1 \pmod 8$. ΄Ετσι, έχουμε $(-2/p_i) = 1$ αν και μόνον αν $p_i \equiv 1, 3 \pmod 8$. Επομένως, ο ακέραιος n είναι παραστάσιμος από την μορφή $x^2 + 2y^2$ αν και μόνον αν κάθε πρώτος διαιρέτης p του n με $p \equiv 5$ ή $7 \pmod 8$ εμφανίζεται με άρτια δύναμη στη πρωτογενή ανάλυση του n. □

΄Ασκηση 8.9. *Να δειχθεί ότι κανένας ακέραιος της μορφής $4^h(8k + 7)$, όπου $k, h \in \mathbb{N}$, δεν γράφεται ως άθροισμα τριών τετραγώνων.*

Απόδειξη. Ας είναι $x_1, x_2, x_3 \in \mathbb{N}$ έτσι, ώστε

$$x_1^2 + x_2^2 + x_3^2 = 4^h(8k + 7),$$

όπου $k, h \in \mathbb{N}$. Ας υποθέσουμε ότι $h = 0$. Τότε, έχουμε:

$$x_1^2 + x_2^2 + x_3^2 \equiv 7 \pmod 8.$$

Καθώς όμως ισχύει $x_i^2 \equiv 0, 1, 4 \pmod 8$, το παραπάνω άθροισμα δεν ισούται ποτέ με $7 \pmod 8$. ΄Ατοπο. Ας υποθέσουμε στη συνέχεια ότι $h \neq 0$. Τότε, έχουμε:

$$x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod 4.$$

Καθώς $x_i \equiv 0, 1 \pmod 4$, η παραπάνω ισοτιμία δίνει $x_i \equiv 0 \pmod 4$ $(i = 1, 2, 3)$. ΄Ετσι, παίρνουμε:

$$\left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2 = 4^{h-1}(8k + 7).$$

Συνεχίζοντας έτσι, μετά από h βήματα, καταλήγουμε στην ισότητα:

$$\left(\frac{x_1}{2^h}\right)^2 + \left(\frac{x_2}{2^h}\right)^2 + \left(\frac{x_3}{2^h}\right)^2 = 8k + 7,$$

όπου οι αριθμοί $x_i/2^h$ $(i = 1, 2, 3)$ είναι ακέραιοι. Αυτό όμως είναι άτοπο, όπως είδαμε παραπάνω. □

8.4 Συνδυαστικές Ασκήσεις

΄Ασκηση 8.10 (American Mathematical Monthly, 11950 [2])**.** *Ας είναι a και b θετικοί ακέραιοι. Να δείξετε ότι υπάρχουν άπειροι θετικοί ακέραιοι n τέτοιοι, ώστε οι ακέραιοι n, $n + a$, $n + b$ οι οποίοι μπορούν να παρασταθούν ως άθροισμα δύο τέλειων τετραγώνων.*

Απόδειξη. Για την απόδειξη της άσκησης θα διακρίνουμε την περίπτωση όπου $a, b \equiv 2 \pmod 4$ και a ή $b \not\equiv 2 \pmod 4$.

Ας είναι $a \equiv 2 \pmod 4$ και $b \equiv 2 \pmod 4$. Θέτοντας $n = m - a$, $c = b - a$ και $d = -a$ αρκεί να βρούμε άπειρους ακεραίους $m > a$ τέτοιους, ώστε οι ακέραιοι της μορφής m, $m + c$, $m + d$ να μπορούν να παρασταθούν ως άθροισμα δύο τέλειων τετραγώνων. Παρατηρούμε ότι σε αυτήν την περίπτωση $c \equiv 0 \pmod 4$.

Έστω $a \not\equiv 2 \pmod 4$ ή $b \not\equiv 2 \pmod 4$. Θέτοντας $n = m$, $c = a$ και $d = b$ αρκεί να βρούμε άπειρους ακεραίους $m > 0$ τέτοιους ώστε οι ακέραιοι της μορφής m, $m + c$, $m + d$ να μπορούν να παρασταθούν ως άθροισμα δύο τέλειων τετραγώνων. Παρατηρούμε ότι σε αυτήν την περίπτωση $c \not\equiv 2 \pmod 4$.

Καθώς και στις δύο περιπτώσεις $c \not\equiv 2 \pmod 4$ διακρίνουμε τις περιπτώσεις όπου $c \equiv 0 \pmod 4$ και $c \equiv 1$ ή $3 \pmod 4$. Αν $c \equiv 0 \pmod 4$, τότε θέτοντας $x = c/4 - 1$ και $y = c/4 + 1$, παίρνουμε $y^2 - x^2 = c$. Αν $c \equiv 1$ ή $3 \pmod 4$, τότε θέτοντας $x = (c - 1)/2$ και $y = (c + 1)/2$ έχουμε πάλι $y^2 - x^2 = c$.

Ας είναι z ακέραιος με $z \not\equiv x^2 + d \pmod 2$. Θέτουμε $r = (z^2 - x^2 - d + 1)/2$ και $s = r - 1$. Θεωρούμε τον ακέραιο $m = r^2 + x^2$. Τότε έχουμε:

$$m + c = r^2 + x^2 + y^2 - x^2 = r^2 + y^2$$

και

$$\begin{aligned} m + d = r^2 + x^2 + d = \\ s^2 + 2r - 1 + x^2 + d = s^2 + x^2 + d - 1 + z^2 - x^2 - d + 1 = s^2 + z^2. \end{aligned}$$

Καθώς υπάρχουν άπειρα z τέτοια ώστε $z \not\equiv x^2 + d \pmod 2$ συνεπάγεται και ότι υπάρχουν άπειρα m της μορφής $r^2 + x^2$. ΄Αρα υπάρχουν άπειρα m τέτοια ώστε m, $m + c$, $m + d$ να μπορούν να παρασταθούν ως άθροισμα δύο τέλειων τετραγώνων. □

΄Ασκηση 8.11 (American Mathematical Monthly, 11894 [4])**.** *Ας είναι a, b, c, d, x, y, z ακέραιοι τέτοιοι, ώστε $a^2 + b^2 + c^2 = d^2$, $d \neq 0$ και $ax + by + cz = 0$. Να δειχθεί ότι ο ακέραιος $x^2 + y^2 + z^2$ μπορεί να γραφεί ως άθροισμα δύο τέλειων τετραγώνων.*

Απόδειξη. Καθώς $d \neq 0$ συνεπάγεται ότι ένας τουλάχιστον ακέραιος από τους a, b, c είναι μη μηδενικός. Υποθέτουμε, χωρίς περιορισμό της γενικότητας, ότι $c \neq 0$. Ισχύει:

$$\begin{aligned}(a^2+c^2)c^2(x^2+y^2+z^2) &= (a^2+c^2)(c^2x^2+c^2y^2+(-ax-by)^2)\\ &= ((a^2+c^2)x+aby)^2+(a^2+b^2+c^2)c^2y^2\\ &= ((a^2+c^2)x+aby)^2+(dcy)^2.\end{aligned}$$

Οι ακέραιοι a^2+c^2, $((a^2+c^2)x+aby)^2+(dcy)^2$ είναι αθροίσματα τετραγώνων και επομένως όλοι οι πρώτοι παράγοντές τους της μορφής $3 \pmod 4$ βρίσκονται σε άρτια δύναμη στην πρωτογενή τους ανάλυση. Επιπλέον, κάθε πρώτος παράγοντας της μορφής $3 \pmod 4$ του c^2 βρίσκεται σε άρτια δύναμη στην πρωτογενή του ανάλυση. Συνεπώς, από την παραπάνω ισότητα συνεπάγεται ότι οι πρώτοι παράγοντες της μορφής $3 \pmod 4$ του ακεραίου $x^2+y^2+z^2$ βρίσκονται σε άρτια δύναμη στην πρωτογενή του ανάλυση. Άρα, ο ακέραιος $x^2+y^2+z^2$ μπορεί να γραφεί ως άθροισμα δύο τετραγώνων. □

8.5 Θεωρία Αριθμών με Maple

Οι τετραγωνικές εξισώσεις που ακολουθούν επιλύονται με την εντολή του Maple, isolve. Αν δεν υπάρχουν ακέραιες λύσεις το Maple δεν επιστρέφει τίποτα (NULL).

Άσκηση 8.12. *Να βρεθούν οι ακέραιοι x, y που επαληθεύουν τις εξισώσεις:*
$\alpha)$ $5x^2+14xy+11y^2=35$,
$\beta)$ $5x^2+14xy+11y^2=46$,
$\gamma)$ $x^2+xy+5y^2=11$.

Απόδειξη. Με κώδικα Maple:

```
{isolve}(5*x^2 + 14*x*y + 11*y^2 = 35);
     {{x = -8, y = 5}, {x = -6, y = 5}, {x = -4, y = 1},
      {x = -2, y = 3}, {x = 2, y = -3}, {x = 4, y = -1},
      {x = 6, y = -5}, {x = 8, y = -5}}
{isolve}(5*x^2 + 14*x*y + 11*y^2 = 46);
NULL;
{isolve}(x^2 + x*y + 5*y^2 = 11);
      {{x = -3, y = 1}, {x = -2, y = -1}, {x = 2, y = 1},
       {x = 3, y = -1}}
```

□

Για τις υπόλοιπες υπολογιστικές ασκήσεις, π.χ. τις αναγμένες μορφές, παραστάσιμους αριθμού κτλ, δεν υπάρχουν εντολές στο Maple. Υπάρχει όμως η δυνατότητα φτιάχνοντας ένα μικρό προγραμματάκι να υπολογίσουμε αυτό που θέλουμε, όπως κάνουμε και στην επόμενη άσκηση.

Άσκηση 8.13. *Να βρεθεί ο μικρότερος θετικός ακέραιος που είναι παραστάσιμος από τις παρακάτω ακέραιες δυαδικές μορφές*
$\alpha)$ $f(x,y)=7x^2+25xy+23y^2$,

$\beta)$ $f(x,y) = 5x^2 + 6xy + 7y^2$,
$\gamma)$ $f(x,y) = 11x^2 + 7xy + 9y^2$.

Απόδειξη. Με κώδικα Maple:

```
a := 7; b := 25; c := 23;
xx := 1; yy := -1;
n := a*xx^2 + b*xx*yy + c*yy^2 - 1;
k := floor(sqrt(4*a*n/(4*a*c - b^2)));
for i from -k while i <= k do
  print(y = i, isolve((2*a*x + b*i)^2 - (-4*a*c + b^2)*i^2 <= 4*a*n));
end do;
                    y = -2, {x = 3}, {x = 4}
                    y = -1, {x = 1}, {x = 2}
                         y = 0, {x = 0}
                   y = 1, {x = -2}, {x = -1}
                   y = 2, {x = -4}, {x = -3}
```

Έτσι, υπολογίζοντας τις τιμές των $f(x,y)$ για τις παραπάνω τιμές των x και y έχουμε το ζητούμενο

```
F(x, y):= a*x^2 + b*x*y + c*y^2;
F(-2, 3), F(-2, 4), F(-1, 1), F(-1, 2), F(0, 0),
F(1, -2), F(1, -1), F(2, -4), F(2, -3);
            F := (x, y) arrow  a*x^2+b*x*y+c*y^2
            85, 196, 5, 49, 0, 49, 5, 196, 85
```

Ομοίως για $\beta)$

```
a := 5; b := 6; c := 7;
xx := 1; yy := -1;
n := a*xx^2 + b*xx*yy + c*yy^2;
k := floor(sqrt(4*a*n/(4*a*c - b^2)));
for i from -k while i <= k do
    print(y = i, isolve((2*a*x + b*i)^2 - (-4*a*c + b^2)*i^2 <= 4*a*n));
end do;
                        y = -1, {x = 1}
               y = 0, {x = -1}, {x = 0}, {x = 1}
                        y = 1, {x = -1}
F := (x, y) -> a*x^2 + b*x*y + c*y^2;
F(1, -1), F(-1, 0), F(0, 0), F(1, 0), F(-1, 1);
         F := (x, y) arrow  a*x^2+b*x*y+c*y^2
         6, 5, 0, 5, 6
```

Ομοίως για $\gamma)$.

```
a := 11; b := 7; c := 9;
xx := 1; yy := -1;
n := a*xx^2 + b*xx*yy + c*yy^2;
k := floor(sqrt(4*a*n/(4*a*c - b^2)));
```

```
for i from -k while i <= k do
    print(y = i, isolve((2*a*x + b*i)^2 - (-4*a*c + b^2)*i^2 <= 4*a*n));
end do;
                    y = -1, {x = 0}, {x = 1}
                y = 0, {x = -1}, {x = 0}, {x = 1}
                    y = 1, {x = -1}, {x = 0}
F := (x, y) -> a*x^2 + b*x*y + c*y^2;
F(1, -1), F(0, -1), F(-1, 0), F(0, 0), F(1, 0), F(-1, 1), F(0, 1)
         F := (x, y) arrow  a*x^2+b*x*y+c*y^2
         13, 9, 11, 0, 11, 13, 9
```

□

Τέλος, χρησιμοποιώντας την εντολή του Maple QuadraticResidue(a, n) μπορούμε σύμφωνα με το Θεώρημα 8.1 να αποφανθούμε αν ένας ακέραιος n είναι παραστάσιμος. Η εντολή QuadraticResidue(a, n) μας επιστρέφει 1 αν το a είναι τετραγωνικό υπόλοιπο $\bmod n$ και -1 αν δεν είναι.

΄Ασκηση 8.14. *Να εξετάσετε αν οι ακέραιοι* $7, 2346, 232112357$ *είναι παραστάσιμοι από την τετραγωνική μορφή* $5x^2 + 6xy + 9y^2$.

Απόδειξη. Με κώδικα Maple:

```
d := 6^2 - 9*4*5;
n1 := 23;
n2 := -2348;
n3 := 3^10 + 4;
QuadraticResidue(d, 4*abs(n1));
QuadraticResidue(d, 4*abs(n2));
QuadraticResidue(d, 4*abs(n3));
                          d := -144
                               -1
                               -1
                               1
```

□

Βιβλιογραφία

[1] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[2] Gerald A. Edgar, Daniel H. Ullman & Douglas B. West (2018) Problems and Solutions, The American Mathematical Monthly, 125:9, 851-859.

[3] Gauss, F. (1801). Disquisitiones Arithmeticae. Leipzig: Gerh. Fleischer

[4] Eugen J. Ionascu (2018) Problems and Solutions, The American Mathematical Monthly, 125:2,179-187

[5] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[6] Αντωνιάδης, Ι., Κοντογεώργης, Α. (2015). Θεωρία Αριθμών και Εφαρμογές. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/107

[7] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Κεφάλαιο 9

Διοφαντικές Εξισώσεις

Οι Διοφαντικές Εξισώσεις που μελετώνται σε αυτό το κεφάλαιο πήραν το όνομά τους από τον Έλληνα Μαθηματικό Διόφαντο. Ο Διόφαντος είναι γνωστός για την δουλειά του «Αριθμητικά», που περιέχει 13 βιβλία εκ των οποίων μόνο 6 έχουν διασωθεί. Οι καινοτομίες που εισήγαγε στον χώρο των Μαθηματικών είχαν διαχρονικά αποτελέσματα και μεγάλα οφέλη για την μελέτη της Άλγεβρας και της Θεωρίας των Αριθμών. Ήταν ο πρώτος που ασχολήθηκε με τις λύσεις πολυωνυμικών εξισώσεων από το σύνολο των ακεραίων και για αυτό οι εξισώσεις όπου μόνο ακέραιες λύσεις γίνονται αποδεκτές ονομάστηκαν Διοφαντικές. Ο κλάδος των Μαθηματικών ο οποίος μελετά τέτοιες εξισώσεις είναι γνωστός σήμερα ως Διοφαντική Γεωμετρία.

9.1 Στοιχειώδεις Μέθοδοι

Ορισμός 9.1. Μία εξίσωση της μορφής

$$f(x_1, \ldots, x_n) = 0, \tag{9.1}$$

όπου $f(x_1, \ldots, x_n)$ πολυώνυμο n μεταβλητών με ακέραιους συντελεστές καλείται *Διοφαντική*. Καλούμε *βαθμό* μιας Διοφαντικής εξίσωσης τον βαθμό του πολυωνύμου $f(x_1, \ldots, x_n)$. Μία διατεταγμένη n-άδα $(t_1, \ldots, t_n) \in \mathbb{Q}^n$ τέτοια ώστε $f(t_1, \ldots, t_n) = 0$ καλείται *ρητή λύση* της (9.1). Αντίστοιχα, μία διατεταγμένη n-άδα $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ τέτοια ώστε $f(t_1, \ldots, t_n) = 0$ καλείται *ακέραια λύση* της (9.1).

Αν $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ είναι μία λύση της (9.1) τότε η n-άδα $(t_1, \ldots, t_n)$ επαληθεύει την ισοτιμία

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{n}, \tag{9.2}$$

για κάθε $n \in \mathbb{Z}^+$. Το αντίστροφο δεν ισχύει. Επομένως μία μέθοδος για να αποδείξουμε ότι μια Διοφαντική εξίσωση δεν έχει ακέραια λύση είναι να επιλέξουμε κατάλληλο n και να δείξουμε ότι η ισοτιμία (9.2) δεν έχει λύση.

Μία άλλη τεχνική για να αποδείξουμε ότι μια Διοφαντική εξίσωση δεν έχει λύση είναι να υποθέσουμε ότι η εξίσωση έχει μια ελάχιστη λύση, δηλαδή, μία λύση n-άδα

$(x_1, \ldots, x_n)$ όπου κάποια από τις συντεταγμένες x_i παίρνει την ελάχιστη θετική τιμή, και να αποδείξουμε ότι υπάρχει μία ακόμη μικρότερη, απ΄ όπου καταλήγουμε σε άτοπο.

Παρακάτω δίνουμε παραδείγματα εφαρμογής αυτών των μεθόδων.

Ασκήσεις

Στις ασκήσεις της ενότητας αυτής θα δούμε την επίλυση Διοφαντικών εξισώσεων τόσο κάνοντας χρήση των μεθόδων που αναφέρθηκαν παραπάνω αλλά και με τεχνικές που επιλέγονται κατά περίπτωση.

΄Ασκηση 9.1. *Να δειχθεί ότι η εξίσωση $x^2 + y^2 + z^2 = 8t + 7$ δεν έχει λύση.*

Απόδειξη. Εύκολα διαπιστώνουμε ότι το υπόλοιπο (mod 8) ενός ακεραίου στο τετράγωνο είναι 0, 1 ή 4. Οπότε

$$x^2 + y^2 + z^2 = 8t + 7 \Rightarrow x^2 + y^2 + z^2 \equiv 7 \pmod 8 \Rightarrow a + b + c \equiv 7 \pmod 8,$$

με $a, b, c \in \{0, 1, 4\}$, όπου a, b, c τα υπόλοιπα (mod 8) των x^2, y^2, z^2, αντίστοιχα. Εύκολα βλέπουμε ότι $a + b + c \not\equiv 7 \pmod 8$, για κάθε $a, b, c \in \{0, 1, 4\}$. Συνεπώς, η εξίσωση $x^2 + y^2 + z^2 = 8t + 7$ δεν έχει λύση. □

΄Ασκηση 9.2. *Να δειχθεί ότι η εξίσωση $y^2 = x^3 + 7$ δεν έχει λύση.*

Απόδειξη. Αν x άρτιος τότε υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $x = 2k$. Οπότε η ισότητα $y^2 = (2k)^3 + 7$ δίνει $y^2 \equiv 7 \pmod 8$. Αυτό όμως είναι αδύνατο, καθώς το υπόλοιπο mod 8 ενός ακεραίου στο τετράγωνο είναι 0, 1 ή 4.

΄Ας είναι x περιττός. Τότε, ο y είναι άρτιος και επομένως έχουμε $x^3 + 7 \equiv 0 \pmod 4$, απ΄ όπου $x^3 \equiv 1 \pmod 4$. Αν $x \equiv 3 \pmod 4$, τότε έχουμε $3 \equiv 1 \pmod 4$ το οποίο είναι αδύνατο. ΄Αρα, ισχύει $x \equiv 1 \pmod 4$.

Από την άλλη πλευρά, η ισότητα $y^2 = x^3 + 7$ δίνει:

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4).$$

΄Εχουμε $x + 2 \equiv 3 \pmod 4$. Αν όλοι οι πρώτοι παράγοντες του $x + 2$ ισούνται με $1 \pmod 4$, τότε θα είχαμε $1 \equiv 3 \pmod 4$ το οποίο είναι άτοπο. Συνεπώς, υπάρχει τουλάχιστον ένας πρώτος παράγοντας p του $x + 2$ με $p \equiv 3 \pmod 4$. ΄Ετσι, έχουμε ότι $p \mid y^2 + 1$ και επομένως $y^2 \equiv -1 \pmod p$, απ΄ όπου έπεται $(-1/p) = 1$ το οποίο, σύμφωνα με το Πόρισμα 7.2, δεν ισχύει. □

΄Ασκηση 9.3. *Να δειχθεί ότι η μόνη λύση της εξίσωσης $x^2 + y^2 = 3z^2$ είναι η $x = y = z = 0$.*

Απόδειξη. Ας είναι (x_0, y_0, z_0) μία λύση της εξίσωσης. Ας υποθέσουμε ότι $x_0 = 0$. Αν $(y_0, z_0) \neq (0, 0)$, τότε $y_0^2 = 3z_0^2$ και επομένως $3 \mid y_0$. ΄Ετσι, όμως ο εκθέτης του 3 στο αριστερό σκέλος της ισότητας είναι άρτιος, ενώ στο δεξί περιττός, το οποίο είναι αδύνατο. ΄Αρα $(y_0, z_0) = (0, 0)$ και επομένως $(x_0, y_0, z_0) = (0, 0, 0)$.

Αν $x_0 \neq 0$, τότε η τριάδα $(-x_0, y_0, z_0)$ θα είναι επίσης λύση της εξίσωσης. ΄Ετσι, αν η εξίσωση έχει μη μηδενική λύση, τότε θα έχει τουλάχιστον μία λύση της μορφής (x_0, y_0, z_0) με $x_0 > 0$. Ας είναι (x_0, y_0, z_0) η λύση της εξίσωσης με τον μικρότερο θετικό

ακέραιο x_0. Τότε, έχουμε $x_0^2 + y_0^2 \equiv 0 \pmod 3$. Καθώς για κάθε ακέραιο w έχουμε $w^2 \equiv 0$ ή $1 \pmod 3$, προκύπτει ότι

$$x_0^2 + y_0^2 \equiv 0 \pmod 3 \Rightarrow x_0 \equiv y_0 \equiv 0 \pmod 3 \Rightarrow 3 \mid x_0,\ 3 \mid y_0.$$

Οπότε, $x_0 = 3k$ και $y_0 = 3l$, όπου $k, l \in \mathbb{Z}$. Έτσι, έχουμε:

$$9k^2 + 9l^2 = 3z_0^2 \Rightarrow 3k^2 + 3l^2 = z_0^2 \Rightarrow z_0^2 \equiv 0 \pmod 3.$$

Άρα $3 \mid z_0$ και επομένως $z_0 = 3m$, όπου m ακέραιος. Συνεπώς, η παραπάνω σχέση γίνεται

$$9k^2 + 9l^2 = 3z_0^2 \Rightarrow 9k^2 + 9l^2 = 27m^2 \Rightarrow k^2 + l^2 = 3m^2,$$

δηλαδή, η τριάδα $(k, l, m) = (x_0/3, y_0/3, z_0/3)$ είναι λύση της εξίσωσης με $x_0/3 < x_0$ που είναι άτοπο. Άρα, η μόνη λύση της εξίσωσης είναι η $x = y = z = 0$. □

Μία επίσης πολύ κλασσική τεχνική επίλυσης διοφαντικών εξισώσεων είναι το φράξιμο των πιθανών λύσεων. Αρχικά με διάφορες τεχνικές προσπαθούμε να προσδιορίσουμε τις πιθανές τιμές των λύσεων και στην συνέχεια να ανιχνεύσουμε ποιες από αυτές επαληθεύουν την εξίσωση. Το φράξιμο μπορεί να γίνει με οποιοδήποτε τρόπο π.χ. με ανισοτικές σχέσεις, με σχέσεις διαιρετότητας κ.α..

Άσκηση 9.4. *Να βρεθούν όλες οι ακέραιες λύσεις της εξίσωσης*

$$2x - xy^3 - 2 = 0$$

Απόδειξη. Ας είναι (x, y) μία ακέραια λύση της παραπάνω εξίσωσης. Τότε, έχουμε

$$x(2 - y^3) = 2$$

και επομένως $x \mid 2$, απ' όπου παίρνουμε $x \in \{\pm 1, \pm 2\}$. Διαπιστώνουμε αμέσως ότι η εξίσωση έχει ακέραια λύση μόνο για $x = 1, 2$. Άρα, οι λύσεις είναι οι $(x, y) = (2, 1), (1, 0)$. □

Άσκηση 9.5. *Να βρεθούν όλες οι ακέραιες λύσεις της εξίσωσης*

$$19x + 20y = 1909$$

με $x, y > 0$.

Απόδειξη. Καθώς $x, y > 0$, ισχύει $0 < 20y, 1909$ και $0 < 19x < 1909$. Οπότε, έχουμε

$$0 < y < \frac{1909}{20} \quad 0 < x < \frac{1909}{19},$$

και επομένως $y \in \{1, \ldots, 95\}$ και $x \in \{1, \ldots, 100\}$. Παρατηρούμε ότι για $x = 100$, η εξίσωση δεν έχει λύση. Θέτουμε $x = 10x_1 + x_2$, όπου x_1, x_2 τα ψηφία του αριθμού x τα οποία δεν μπορούν να είναι ταυτόχρονα ίσα με 0. Έχουμε

$$20y = 1909 - 19(10x_1 + x_2) \Rightarrow 20y = 10(190 - 19x_1 - x_2) + (9 - 9x_2),$$

και επομένως

$$10 \mid 9 - 9x_2 \Rightarrow 10 \mid -1 + x_2.$$

Καθώς $x_2 \in \{0, \ldots, 9\}$, παίρνουμε $x_2 = 1$. Άρα $x = 10x_1 + 1$ και επομένως έχουμε

$$20y = 10(189 - 19x_1)$$

και επομένως $2y = 189 - 19x_1$, απ' όπου προκύπτει ότι ο x_1 είναι περιττός. Έτσι, για $x_1 = 1, 3, 5, 7, 9$ παίρνουμε ότι $x \in \{11, 31, 51, 71, 91\}$. Αντικαθιστώντας τις πιθανές τιμές του x προκύπτουν οι παρακάτω λύσεις:

$$(x, y) = (91, 9), (71, 28), (51, 37), (31, 56), (11, 75).$$

□

Άσκηση 9.6. *Να δειχθεί ότι η εξίσωση*

$$15x^2 - 7y^2 = 9$$

δεν έχει ακεραία λύση.

Απόδειξη. Ας είναι (u, v) μία ακεραία λύση της εξίσωσης. Τότε $15u^2 - 7v^2 = 9$ και επομένως έχουμε $3 \mid 7v^2$. Άρα $3 \mid v$ και κατά συνέπεια $v = 3v'$, όπου v' ακέραιος. Οπότε, έχουμε $15u^2 - 7 \cdot 9(v')^2 = 9$, απ' όπου $3 \mid u$ και επομένως $u = 3u'$, όπου u' ακέραιος. Αντικαθιστώντας στην εξίσωση, παίρνουμε

$$15(u')^2 - 7(v')^2 = 1.$$

Οπότε, έχουμε $(v')^2 \equiv -1 \pmod 3$. Από την άλλη πλευρά, ισχύει $(v')^2 \equiv 0$ ή $1 \pmod 3$. Έτσι, καταλήγουμε σε άτοπο και κατά συνέπεια η παραπάνω εξίσωση δεν έχει ακεραία λύση. □

Άσκηση 9.7. *Να βρεθούν όλοι οι ακέραιοι n για τους οποίους η εξίσωση*

$$\frac{1}{x} + \frac{1}{y} = \frac{n}{x + y}$$

έχει ακέραια λύση (x, y) με $xy \neq 0$ και $x \neq -y$.

Απόδειξη. Η παραπάνω εξίσωση μετασχηματίζεται στην εξίσωση

$$(x + y)^2 = nxy,$$

όπου $x \neq -y$ και επομένως $xy \neq 0$. Διαιρώντας την παραπάνω εξίσωση με y^2 έχουμε ισοδύναμα ότι

$$\left(\frac{x}{y}\right)^2 - (n - 2)\frac{x}{y} + 1 = 0.$$

Για να είναι ο αριθμός x/y ρητός πρέπει και αρκεί η διακρίνουσα αυτής της εξίσωσης $\Delta = (n - 2)^2 - 4$ να είναι τέλειο τετράγωνο, δηλαδή να υπάρχει ακέραιος k τέτοιος, ώστε να ισχύει

$$(n - 2)^2 - 4 = k^2.$$

Ισοδύναμα, έχουμε:

$$(n-2-k)(n-2+k)=4.$$

Έτσι, προκύπτει $n-2-k=\pm1,\pm2,\pm4$. Αν $n-2-k=\pm1$, τότε $n-2+k=\pm4$, οπότε προσθέτοντας τις δύο τελευταίες εξισώσεις προκύπτει ότι

$$2(n-2)=\pm5\Rightarrow 2\mid 5,$$

που είναι άτοπο. Ομοίως, αν $n-2-k=\pm4$, τότε $n-2+k=\pm1$ και επομένως $2(n-2)=\pm5$ που οδηγεί επίσης σε άτοπο. Αν $n-2-k=\pm2$, τότε $n-2+k=\pm2$, απ΄ όπου προκύπτει ότι $k=-k$ που συνεπάγεται $k=0$. Άρα $n-2=\pm2$ και έτσι έχουμε $n\in\{0,4\}$. Για $n=0$, παίρνουμε $(x/y+1)^2=0$ και επομένως $x/y=-1$, απ΄ όπου $x=-y$ που είναι άτοπο. Για $n=4$, ισχύει $(x/y-1)^2=0$ και κατά συνέπεια ισχύει $x/y=1$, απ΄ όπου $x=y$. Συνεπως, μόνο για $n=4$ υπάρχουν ακέραιες λύσεις x,y με $x\neq -y$. □

Άσκηση 9.8. *Να δειχθεί ότι η εξίσωση*

$$y^2=x^5-4$$

δεν έχει λύση σε ακέραιους x,y.

Απόδειξη. Παρατηρούμε ότι η εξίσωση δεν έχει λύση με $x=0$ ή $y=0$. Αν οι ακέραιοι x,y είναι ο ένας άρτιος και ο άλλος περιττός, τότε ο ακέραιος x^5-y^2 είναι περιττός που είναι άτοπο καθώς ισούται με 4.

Ας υποθέσουμε ότι οι ακέραιοι x,y είναι και οι δύο άρτιοι. Τότε, έχουμε:

$$\left(\frac{y}{2}\right)^2+1\equiv 8\left(\frac{x}{2}\right)^5.$$

Επομένως, ισχύει $(y/2)^2\equiv -1\pmod 4$ που είναι άτοπο.

Στη συνέχεια, ας υποθέσουμε ότι οι ακέραιοι x,y είναι και οι δύο περιττοί. Τότε, έχουμε:

$$y^2+36=x^5+32=(x+2)(x^4-2x^3+4x^2-8x+16).$$

Θέτουμε $P(x)=x^4-2x^3+4x^2-8x+16$. Καθώς ο x είναι περιττός, παίρνουμε:

$$P(x)\equiv x^4-2x^3\equiv 3\pmod 4.$$

Άρα, ο ακέραιος $P(x)$ έχει ένα πρώτο διαιρέτη p με $p\equiv 3\pmod 4$. Επομένως, έχουμε $y^2+6^2\equiv 0\pmod p$. Αν $p>3$, τότε, καθώς $(6,p)=1$ υπάρχει ακέραιος a τέτοιος, ώστε $6a\equiv 1\pmod p$ και επομένως $(ya)^2\equiv -1\pmod p$. Επομένως, παίρνουμε $p\equiv 1\pmod 4$ που είναι άτοπο σύμφωνα με το Πόρισμα 7.2. Άρα $p=3$ και έτσι έχουμε $P(x)\equiv 0\pmod 3$. Από την άλλη πλευρά, αν $x=3k$ για κάποιο $k\in\mathbb{Z}$ προκύπτει ότι:

$$P(x)=x^4-2x^3+4x^2-8x+16\equiv 1\pmod 3,$$

αν $x=3k+1$ τότε

$$P(x)=x^4-2x^3+4x^2-8x+16\equiv -1\pmod 3$$

και αν $x = 3k - 1$ τότε

$$P(x) = x^4 - 2x^3 + 4x^2 - 8x + 16 \equiv 1 \pmod 3.$$

Έτσι, καταλήγουμε πάλι σε άτοπο. Συνεπώς, η παραπάνω Διοφαντική εξίσωση δεν έχει ακέραια λύση. □

Άσκηση 9.9. *Να βρεθούν όλες οι θετικές ακέραιες λύσεις της εξίσωσης*

$$\frac{13}{x^2} + \frac{1996}{y^2} = \frac{z}{1997}.$$

Απόδειξη. Ας είναι (x, y, z) μία τριάδα θετικών ακεραίων η οποία επαληθεύει την εξίσωση. Τότε, έχουμε:

$$1997(13y^2 + 1996x^2) = zx^2y^2. \tag{9.3}$$

Ο ακέραιος 1997 είναι πρώτος και ισχύει $1997 \mid zx^2y^2$. Διακρίνουμε τις περιπτώσεις όπου $1997 \mid z$ και όπου $1997 \nmid z$.

Έστω $1997 \mid z$. Τότε, $z = 1997z_1$, όπου z_1 ακέραιος, και έτσι από την ισότητα 9.3 παίρνουμε:

$$13y^2 + 1996x^2 = z_1x^2y^2. \tag{9.4}$$

Οπότε, $x^2 \mid 13y^2$. Αν $x = 13$, τότε $13 \mid y$ και επομένως $y = 13y'$, όπου y' ακέραιος. Έτσι, αντικαθιστώντας στην ισότητα 9.4, παίρνουμε:

$$13(y')^2 + 1996 = z_1 13^2 (y')^2.$$

Επομένως, έχουμε $13 \mid 1996$ που είναι άτοπο. Άρα, $(x, 13) = 1$ και κατά συνέπεια $x \mid y$. Έτσι, έχουμε $y = xx'$, όπου x' ακέραιος. Από την άλλη πλευρά, η ισότητα 9.4 μας δίνει $y^2 \mid 1996x^2$, απ' όπου έπεται $(x')^2 \mid 499 \cdot 4$. Καθώς 499 πρώτος, έχουμε ότι $x' \mid 2$. Αν $x' = 1$, τότε $y = x$ και επομένως από την ισότητα 9.4 έχουμε $2009 = z_1x^2$ ή $z_1x^2 = 7^2 41$, απ' όπου παίρνουμε τα ζεύγη $(x, z_1) = (1, 2009), (7, 41)$. Αν $x' = 2$, τότε $y = 2x$ και επομένως η 9.4 δίνει $512 = z_1x^2$ ή $z_1x^2 = 2^9$, απ' όπου προκύπτουν τα ζεύγη $(x, z_1) = (1, 2^9), (2, 2^7), (2^2, 2^5), (2^3, 2^3), (2^4, 2)$.

Έστω $1997 \nmid z$. Τότε $1997 \mid x^2y^2$, απ' όπου έπεται ότι $1997 \mid x$ ή $1997 \mid y$. Αν $1997 \mid x$, τότε, από την ισότητα 9.3 έχουμε $1997 \mid 13y^2 + 1996x^2$ και επομένως $1997 \mid y$. Ομοίως, αν $1997 \mid y$, τότε έχουμε ότι $1997 \mid x$. Άρα, ισχύει $x = 1997x'$ και $y = 1997y'$, όπου x' και y' είναι ακέραιοι. Έτσι, παίρνουμε:

$$13(y')^2 + 1996(x')^2 = z1997(x')^2(y')^2. \tag{9.5}$$

Αν $x' > 1$ και $y' > 1$, τότε έχουμε:

$$13(y')^2 + 1996(x')^2 \le 2009 \max\{x', y'\}^2 < z4 \cdot 1997 \max\{x', y'\}^2 \le z1997(x')^2(y')^2.$$

Από την ισότητα 9.5 έχουμε ότι η παραπάνω ανισότητα είναι αδύνατη. Αν $x' = y' = 1$, τότε έχουμε $2009 = z1997$ που είναι άτοπο. Αν $x' = 1$ και $y' > 1$, τότε παίρνουμε:

$$1996 = (z1997 - 13)(y')^2.$$

Από την άλλη πλευρά, έχουμε

$$(z1997 - 13)(y')^2 \geq 1984 \cdot 4 > 1996$$

που είναι άτοπο. Τέλος, αν $x' > 1$ και $y' = 1$, τότε παίρνουμε

$$13 + 1996(x')^2 = z1997(x')^2,$$

απ΄ όπου έπεται ότι $(x')^2 \mid 13$ το οποίο είναι αδύνατο. Επομένως, η εξίσωση δεν έχει λύση με $1997 \nmid z$.

Συνεπώς, όλες οι λύσεις της δίνονται από τις παρακάτω τριάδες:

$$(x, y, z) = (1, 1, 2009 \cdot 1997), (7, 7, 41 \cdot 1997), (1, 2, 2^9 \cdot 1997), (2, 4, 2^7 \cdot 1997),$$

$$(2^2, 2^3, 2^5 \cdot 1997), (2^3, 2^4, 2^3 \cdot 1997), (2^4, 2^5, 2 \cdot 1997).$$

□

9.2 Γραμμικές Διοφαντικές Εξισώσεις

Ορισμός 9.2. Μία Διοφαντική εξίσωση πρώτου βαθμού καλείται *γραμμική Διοφαντική εξίσωση*.

Οι επόμενες δύο προτάσεις μας παρέχουν εργαλεία για να διερευνήσουμε αν μια γραμμική Διοφαντική έχει λύση και σε περίπτωση που έχει να τις προσδιορίσουμε.

Πρόταση 9.1. *Ας είναι $a_1, \ldots, a_n, b \in \mathbb{Z}$ και $n \geq 2$. Αν $\delta = (a_1, \ldots, a_n)$, τότε η εξίσωση*

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

έχει ακέραια λύση αν και μόνο αν, $\delta \mid b$.

Απόδειξη. Βλέπε [10, Κεφάλαιο 8, Πρόταση 2.1]. □

Πρόταση 9.2. *Ας είναι $a, b, c \in \mathbb{Z}$, με $a, b \neq 0$ και $\delta = (a, b)$. Ας υποθέσουμε ότι το ζεύγος (x_0, y_0) είναι μια ακέραια λύση της εξίσωσης*

$$ax + by = c.$$

Τότε, όλες οι ακέραιες λύσεις της είναι τα ζεύγη (x, y), όπου

$$x = x_0 + \frac{b}{\delta}k, \quad y = y_0 - \frac{a}{\delta}k, \quad \forall k \in \mathbb{Z}.$$

Απόδειξη. Βλέπε [10, Κεφάλαιο 8, Πρόταση 2.2]. □

Το ζεύγος

$$\left(x_0 + \frac{b}{\delta}t, y_0 - \frac{a}{\delta}t\right)$$

που προκύπτει από την παραπάνω πρόταση συχνά αναφέρεται στην βιβλιογραφία ως η *γενική λύση* της Διοφαντικής εξίσωσης. Προφανώς, η γενική λύση δεν είναι μοναδική.

Επίλυση Γραμμικών Διοφαντικών Εξισώσεων με Δύο Μεταβλητές. Θεωρούμε την γραμμική Διοφαντική εξίσωση

$$ax + by = c.$$

Τα βήματα υπολογισμού των λύσεων της παραπάνω εξίσωσης έχουν ως εξής:

1) Υπολογίζουμε τον μέγιστο κοινό διαιρέτη $\delta = (a, b)$. Αν $\delta \nmid c$, τότε η εξίσωση δεν έχει λύση. Διαφορετικά συνεχίζουμε στο επόμενο βήμα.
2) Υπολογίζουμε τους ακεραίους $a' = a/\delta$, $b' = b/\delta$ και $c' = c/\delta$.
3) Υπολογίζουμε $s, t \in \mathbb{Z}$ τέτοια, ώστε $sa' + tb' = 1$.
4) Οι λύσεις της γραμμικής εξίσωσης είναι τα ζεύγη

$$(x, y) = (c's + b'k, c't - a'k), \quad k \in \mathbb{Z}.$$

Το βήμα 3 μπορεί να υλοποιηθεί με τον εκτεταμένο Ευκλείδειο αλγόριθμο. Φυσικά, τόσο στην περίπτωση των γραμμικών εξισώσεων με δύο μεταβλητές όσο και στην περίπτωση των γραμμικών εξισώσεων με τρεις μεταβλητές που ακολουθεί αν υπάρχει προφανής λύση μπορούμε να παραλείψουμε όλα τα ενδιάμεσα βήματα και να εξάγουμε κατευθείαν τις λύσεις.

Επίλυση Γραμμικών Διοφαντικών Εξισώσεων με Τρεις Μεταβλητές. Θεωρούμε την γραμμική Διοφαντική εξίσωση

$$ax + by + cz = d.$$

Τα βήματα υπολογισμού των λύσεων της παραπάνω εξίσωσης έχουν ως εξής:

1) Υπολογίζουμε τον μέγιστο κοινό διαιρέτη $\delta = (a, b, c)$. Αν $\delta \nmid d$ τότε η εξίσωση δεν έχει λύση. Διαφορετικά συνεχίζουμε στο επόμενο βήμα.
2) Υπολογίζουμε τους ακεραίους $\delta' = (a, b)$, $a' = a/\delta'$ και $b' = b/\delta'$.
3) Υπολογίζουμε την γενική λύση $(w_1 + w_2\ell, z_1 + z_2\ell)$, $\ell \in \mathbb{Z}$, της εξίσωσης $\delta' w + cz = d$.
4) Υπολογίζουμε μία λύση (x_0, y_0) της γραμμικής εξίσωσης $a'x + b'y = 1$.
5) Οι λύσεις της γραμμικής εξίσωσης είναι οι

$$(x, y, z) = (x_0w_1 + x_0w_2\ell + b'k, y_0w_1 + y_0w_2\ell - a'k, z_1 + z_2\ell)$$

για κάθε $k, \ell \in \mathbb{Z}$.

Ας δούμε καλύτερα τι κάνει ο αλγόριθμος επίλυσης γραμμικής Διοφαντικής εξίσωσης με τρεις μεταβλητές για καταλάβουμε καλύτερα πως προκύπτει ο επόμενος αλγόριθμος που αποτελεί την γενίκευσή του. Θεωρούμε την Διοφαντική εξίσωση

$$ax + by + cz = d$$

και θέτουμε $\delta' = (a, b)$. Έτσι, έχουμε:

$$\delta'(a'x + b'y) + cz = d.$$

Οπότε, λύνοντας την Διοφαντική εξίσωση $\delta' w + cz = d$, παίρνουμε:

$$(a'x + b'y, z) = (w_1 + w_2\ell, z_1 + z_2\ell).$$

Συνεπώς, χρειάζεται να λύσουμε την εξίσωση

$$a'x + b'y = w_1 + w_2\ell.$$

Βρίσκοντας μια λύση (x_0, y_0) της Διοφαντικής εξίσωσης $a'x + b'y = 1$ έχουμε βρει και μια λύση της προηγούμενης εξίσωσης η οποία είναι η $(x_0(w_1 + w_2\ell), y_0(w_1 + w_2\ell))$. Από τον τύπο υπολογισμού της γενικής λύσης μιας Διοφαντικής εξίσωσης με δύο μεταβλητές προκύπτουν οι τιμές των x και y.

Επίλυση Γραμμικών Διοφαντικών Εξισώσεων με *n* Μεταβλητές. Ας είναι η γραμμική Διοφαντική εξίσωση

$$a_1x_1 + \cdots + a_nx_n = b.$$

Τα βήματα υπολογισμού των λύσεων της παραπάνω εξίσωσης έχουν ως εξής:

1) Υπολογίζουμε το $\delta = (a_1, \ldots, a_n)$. Αν $\delta \nmid b$ τότε η γραμμική εξίσωση δεν έχει λύσεις. Διαφορετικά συνεχίζουμε στο επόμενο βήμα.
2) Υπολογίζουμε τα $a'_1 = a_1/\delta$, $a'_2 = a_2/\delta$, …, $a'_n = a_n/\delta$, $b' = b/\delta$.
3) Υπολογίζουμε τις γραμμικές εξίσωσης:

$$\begin{aligned} a'_1x_1 + a'_2x_2 &= (a'_1, a'_2) \\ a'_3x_3 + (a'_1, a'_2)w_3 &= (a'_1, a'_2, a'_3) \\ &\vdots \\ a'_nx_n + (a'_1, a'_2, \ldots, a'_{n-1})w_n &= b'. \end{aligned}$$

4) Υπολογίζουμε την γενική λύση της τελευταίας εξίσωσης και όπως στην περίπτωση των τριών μεταβλητών βρίσκουμε την γενική λύση της προτελευταίας εξίσωσης κ.ο.κ. μέχρι να βρούμε την γενική λύση της πρώτης εξίσωσης. Η γενική λύση θα είναι συναρτήσει $n-1$ παραμέτρων $k_2, \ldots, k_n$.

Ασκήσεις

Η πρώτη άσκηση είναι μια εφαρμογή των αλγορίθμων επίλυσης γραμμικών Διοφαντικών εξισώσεων με δύο και τρεις μεταβλητές.

΄Ασκηση 9.10. *Να λυθούν οι παρακάτω Διοφαντικές εξισώσεις:*

α) $12x + 501y = 273$,
β) $41x + 73y = 3$,
γ) $2072x + 1813y = 2849$,
δ) $-24x - 10y + 14z = 6$,
ε) $7x - 11y + 20z = 59$.

Απόδειξη. α) Θα ακολουθήσουμε την μέθοδο επίλυσης που παρουσιάσαμε προηγουμένως. ΄Εχουμε $a = 12$, $b = 501$, $c = 273$. Πρώτα υπολογίζουμε τον μέγιστο κοινό διαιρέτη $\delta = (a, b) = (12, 501) = 3$. Καθώς ο ακέραιος c διαιρεί το 273, η εξίσωση έχει λύση. ΄Εχουμε $a' = 4$, $b' = 167$, $c' = 91$. Ο Ευκλείδειος αλγόριθμος δίνει:

$$\begin{aligned} 167 &= 41 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1. \end{aligned}$$

Στη συνέχεια παίρνουμε:

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (167 - 41 \cdot 4) = -1 \cdot 167 + 42 \cdot 4.$$

΄Αρα, έχουμε $s = 42$, $t = -1$ και επομένως οι λύσεις της εξίσωσης είναι:

$$(x, y) = (3822 + 167k, -91 - 4k), \quad k \in \mathbb{Z}.$$

β) Η διαδικασία επίλυσης της εξίσωσης είναι όπως στην περίπτωση (α) για αυτό και παραθέτουμε μόνο τις λύσεις της:

$$(x, y) = (-48 + 73k, 27 - 41k), \quad k \in \mathbb{Z}.$$

γ) Ομοίως, οι λύσεις της εξίσωσης είναι:

$$(x, y) = (11 + 7k, -11 - 8k), \quad k \in \mathbb{Z}.$$

δ) Καθώς $\delta = (24, 10, 14) = 2 \mid 6$, η εξίσωση έχει λύση. Ισχύει ότι $\delta' = (24, 10) = 2$, $a' = -12$, $b' = -5$. Η γενική λύση της εξίσωσης $2w + 14z = 6$ είναι η $(w, z) = (3 + 7\ell, -\ell)$. Μία λύση της εξίσωσης $-12x - 5y = 1$ είναι η $(x_0, y_0) = (2, -5)$. Συνεπώς, οι λύσεις της εξίσωσης είναι οι

$$(x, y, z) = (6 + 14\ell - 5k, -15 - 35\ell + 12k, -\ell),$$

για κάθε $k, \ell \in \mathbb{Z}$.

ε) Η διαδικασία επίλυσης της εξίσωσης είναι όπως στην περίπτωση (δ) για αυτό και παραθέτουμε μόνο τις λύσεις της εξίσωσης.

$$(x, y, z) = (-177 - 60\ell - 11k, -118 - 40\ell - 7k, -\ell),$$

για κάθε $k, \ell \in \mathbb{Z}$. □

΄Ασκηση 9.11. *Να δείξετε ότι δεν υπάρχει ακέραιος n τέτοιος ώστε οι αριθμοί $(7n-1)/4$ και $(5n + 3)/12$ να είναι και οι δύο ακέραιοι.*

Απόδειξη. Ας υποθέσουμε ότι οι αριθμοί $(7n - 1)/4$ και $(5n + 3)/12$ είναι ακέραιοι, δηλαδή, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε

$$\frac{7n - 1}{4} = x, \quad \frac{5n + 3}{12} = y,$$

απ΄ όπου έχουμε

$$7n - 1 = 4x, \quad 5n + 3 = 12y.$$

Απαλοίφοντας τον n, προκύπτει η γραμμική εξίσωση

$$20x - 84y = -26.$$

Καθώς $(20, 84) = 4 \nmid 26$, η παραπάνω εξίσωση δεν έχει λύσεις και επομένως δεν υπάρχει ακέραιος n τέτοιος, ώστε οι αριθμοί $(7n - 1)/4$ και $(5n + 3)/12$ να είναι ακέραιοι. □

Την άσκηση που ακολουθεί την λύσαμε στην πρώτη ενότητα φράζοντας τις πιθανές λύσεις με ανισοτικές σχέσεις και σχέσεις διαιρετότητας. Παραθέτουμε τώρα μία άλλη λύση εφαρμόζοντας τον αλγορίθμο επίλυσης γραμμικών εξισώσεων.

΄Ασκηση 9.12. *Να βρεθούν όλες οι ακέραιες λύσεις της εξίσωσης*

$$19x + 20y = 1909,$$

με $x, y > 0$.

Απόδειξη. Οι λύσεις της εξίσωσης που προκύπτουν εφαρμόζοντας τον αλγόριθμο επίλυσης γραμμικών εξισώσεων είναι οι εξής:

$$(x, y) = (-1909 + 20k, 1909 - 19k), \ \forall k \in \mathbb{Z}.$$

Επιπλέον, έχουμε:

$$-1909 + 20k > 0 \quad \text{και} \quad 1909 - 19k > 0,$$

απ΄ όπου παίρνουμε

$$100 \geq k \geq 96.$$

΄Ετσι, για $k = 96, 97, 98, 99, 100$ οι λύσεις που προκύπτουν είναι οι εξής:

$$(x, y) = (91, 9), (71, 28), (51, 37), (31, 56), (11, 75).$$

□

9.3 Πυθαγόρειες Τριάδες

Ορισμός 9.3. Κάθε τριάδα θετικών ακεραίων (x, y, z) που είναι λύση της εξίσωσης

$$x^2 + y^2 = z^2$$

καλείται *Πυθαγόρεια τριάδα*. Αν επιπλέον ισχύει $(x, y, z) = 1$, τότε η Πυθαγόρεια τριάδα καλείται *αρχική*.

Το παρακάτω θεώρημα προσδιορίζει όλες τις Πυθαγόρειες τριάδες.

Θεώρημα 9.1. *Οι αρχικές Πυθαγόρειες τριάδες δίνονται από τις σχέσεις:*

$$(x, y, z) = (2uv, u^2 - v^2, u^2 + v^2),$$
$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2),$$

όπου $u, v \in \mathbb{Z}$, $u \not\equiv v \pmod 2$, $u > v > 0$ *και* $(u, v) = 1$.

Απόδειξη. Βλέπε [10, Κεφάλαιο 8, Θεώρημα 3.1]. □

Ασκήσεις

΄Ασκηση 9.13. *Να βρεθούν όλα τα ορθογώνια τρίγωνα με ακέραιες πλευρές, πρώτες μεταξύ τους, των οποίων το εμβαδόν ισούται με την περίμετρό τους.*

Απόδειξη. Ας είναι x, y οι κάθετες πλευρές ενός ορθογωνίου τριγώνου και z η υποτείνουσά του. Από την υπόθεση έχουμε το εμβαδόν αυτού του τριγώνου ισούται με την περίμετρό του, δηλαδή, ισχύει:

$$\frac{1}{2}xy = x + y + z.$$

΄Οποια μορφή και αν έχει η Πυθαγόρεια τριάδα (x, y, z) σύμφωνα με το Θεώρημα 9.1 η παραπάνω σχέση γίνεται

$$\frac{1}{2}(2uv(u^2 - v^2)) = 2uv + (u^2 - v^2) + (u^2 + v^2).$$

απ΄ όπου έχουμε

$$uv(u^2 - v^2) = 2uv + 2u^2$$

και επομένως ισχύει

$$v(u - v)(u + v) = 2v + 2u.$$

΄Αρα, παίρνουμε $v(u - v) = 2$ και κατά συνέπεια $v \mid 2$, απ΄ όπου έχουμε $v \in \{1, 2\}$. Καθώς $u \not\equiv v \pmod 2$, $u > v > 0$ και $(u, v) = 1$ συνεπάγεται ότι $v = 2$ και $u = 3$. ΄Αρα, αν η Πυθαγόρεια τριάδα είναι της μορφής $(2uv, u^2 - v^2, u^2 + v^2)$ η Πυθαγόρεια τριάδα είναι η $(12, 5, 13)$, ενώ αν είναι της μορφής $(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$ η Πυθαγόρεια τριάδα είναι η $(5, 12, 13)$. ΄Αρα, το μοναδικό τρίγωνο για το οποίο ισχύει η αρχική σχέση είναι αυτό με κάθετες πλευρές 5 και 12 και υποτείνουσα 13. □

΄Ασκηση 9.14. *Να δειχθεί ότι η εξίσωση*
α) $x^4 - y^4 = z^2$ *δεν έχει λύση με* $yz \neq 0$,
β) $x^4 + 4y^4 = z^2$ *δεν έχει λύση με* $yx \neq 0$.

Απόδειξη. α) Αν $x = 0$, τότε $z^2 + y^4 = 0$, δηλαδή, $y = z = 0$. Ας είναι $x \neq 0$. Αν (x_0, y_0, z_0) είναι μία λύση της εξίσωσης, τότε και η $(-x_0, y_0, z_0)$ είναι λύση. Δηλαδή, αν η εξίσωση έχει λύση με $x_0 \neq 0$, τότε θα έχει μία λύση (x_0, y_0, z_0) με $x_0 > 0$. ΄Ετσι, θεωρούμε την λύση (x_0, y_0, z_0) με τον μικρότερο ακέραιο $x_0 > 0$. Καθώς έχουμε

$$x_0^4 = y_0^4 + z_0^2,$$

η τριάδα (x_0^2, y_0^2, z_0) είναι μια Πυθαγόρεια τριάδα.

Ας είναι p πρώτος με $p \mid (x_0^2, y_0^2)$. Τότε, έχουμε $p \mid x_0^2$ και $p \mid y_0^2$, απ΄ όπου έπεται $p \mid x_0$ και $p \mid y_0$. ΄Αρα, έχουμε $p^4 \mid x_0^4 - y_0^4$ και επομένως $p^4 \mid z_0^2$. Συνεπώς, ισχύει $p^2 \mid z_0$. ΄Αρα, η τριάδα $(x_0/p, y_0/p, z_0/p^2)$ είναι λύση της εξίσωσης. Αυτό όμως είναι άτοπο γιατί η τριάδα (x_0, y_0, z_0) είναι η λύση της εξίσωσης με τον μικρότερο θετικό ακέραιο x_0. ΄Αρα, οι ακέραιοι x_0^2 και y_0^2 είναι πρώτοι μεταξύ τους και επομένως $(x_0^2, y_0^2, z_0) = 1$, δηλαδή, η Πυθαγόρεια τριάδα (x_0^2, y_0^2, z_0) είναι αρχική.

Σύμφωνα με το Θεώρημα 9.1, υπάρχουν δύο περιπτώσεις, ο y_0^2 να είναι άρτιος και ο z_0 περιττός, και αντίστροφα. Ας είναι y_0^2 άρτιος. Τότε, υπάρχουν $m, n \in \mathbb{Z}^+$ με $m > n$, $(m, n) = 1$ και $m \not\equiv n \pmod 2$ έτσι, ώστε

$$z_0 = m^2 - n^2, \quad y_0^2 = 2mn, \quad x_0^2 = m^2 + n^2.$$

Καθώς έχουμε $x_0^2 = m^2 + n^2$ και $(m, n) = 1$, η τριάδα (m, n, x_0) είναι μία αρχική Πυθαγόρεια τριάδα. Οπότε υπάρχουν $s, t \in \mathbb{Z}^+$ με $t > s$, $(s, t) = 1$ έτσι, ώστε να έχουμε:

$$m = t^2 - s^2, \quad n = 2st, \quad x_0 = s^2 + t^2$$

ή

$$n = t^2 - s^2, \quad m = 2st, \quad x_0 = s^2 + t^2.$$

Σε κάθε περίπτωση έχουμε $y_0^2 = 2mn$, απ΄ όπου $y_0^2 = 4st(t^2 - s^2)$ και επομένως ισχύει:

$$\left(\frac{y_0}{2}\right)^2 = st(t^2 - s^2).$$

Καθώς ισχύει $(s, t) = (t, t^2 - s^2) = (s, t^2 - s^2) = 1$, υπάρχουν $u, v, w \in \mathbb{Z}^+$ έτσι, ώστε να έχουμε:

$$s = u^2, \quad t = v^2, \quad t^2 - s^2 = w^2.$$

Τότε, ισχύει $v^4 - u^4 = w^2$, δηλαδή, η τριάδα (v, u, w) είναι λύση της εξίσωσης. ΄Ομως,

$$v < v^4 = t^2 < t^2 + s^2 = x_0.$$

΄Ατοπο, καθώς ο x_0 είναι ο μικρότερος θετικός ακέραιος με αυτήν την ιδιότητα.

Ας υποθέσουμε στη συνέχεια ότι ο y_0^2 είναι περιττός. Τότε, υπάρχουν $m, n \in \mathbb{Z}^+$ με $m > n$, $(m, n) = 1$ και $m \not\equiv n \pmod 2$ έτσι ώστε να ισχύει:

$$y_0 = m^2 - n^2, \quad z_0^2 = 2mn, \quad x_0^2 = m^2 + n^2.$$

΄Εχουμε $m^4 - n^4 = (x_0 y_0)^2$ και επομένως η τριάδα $(m, n, x_0 y_0)$ είναι μία λύση της εξίσωσης με $m^2 < m^2 + n^2 = x_0^2$, απ΄ όπου $m < x_0$. Αυτό όμως είναι άτοπο λόγω της επιλογής του x_0.

β) Αν $z = 0$, τότε $x^4 + 4y^4 = 0$ και επομένως $x = y = 0$. Ας υποθέσουμε ότι (x_0, y_0, z_0) είναι μία λύση της εξίσωσης με $x_0 y_0 z_0 \neq 0$. Τότε, υψώνοντας στο τετράγωνο τα δύο μέλη της $x_0^4 + 4y_0^4 = z_0^2$ και αφαιρώντας την ποσότητα $16x_0^4 y_0^4$ από κάθε μέλος προκύπτει:

$$(x_0^4 - 4y_0^4)^2 = z_0^4 - (2x_0 y_0)^4.$$

Δηλαδή, η εξίσωση $x^4 - y^4 = z^2$ έχει την λύση $(z_0, 2x_0 y_0, x_0 4 - 4y_0^4)$ με $x_0 y_0 z_0 \neq 0$. Αυτό, όμως είναι άτοπο λόγω της (α). Συνεπώς, η δοθείσα εξίσωση δεν έχει λύση. □

9.4 Η Εξίσωση $ax^2 + by^2 + cz^2 = 0$

Σ΄ αυτή την ενότητα θα ασχοληθούμε με την εξίσωση

$$ax^2 + by^2 + cz^2 = 0 \tag{9.6}$$

η οποία είναι γνωστή ως *εξίσωση του Legendre*.

Θεώρημα 9.2. *Ας είναι $a, b, c \in \mathbb{Z}^*$, πρώτοι μεταξύ τους ανά δύο και ελεύθεροι τετραγώνου. Τότε, η εξίσωση (9.6) έχει ακέραια λύση $(x, y, z) \neq (0, 0, 0)$ αν και μόνο αν ισχύουν τα εξής:*

α) οι ακέραιοι a, b, c δεν έχουν το ίδιο πρόσημο.

β) οι ακέραιοι $-ab, -bc, -ac$ είναι αντίστοιχα τετραγωνικά υπόλοιπα $\bmod |c|$, $\bmod |a|$, $\bmod |b|$ (όταν αντίστοιχα $|c| \neq 1, |a| \neq 1, |b| \neq 1$).

Απόδειξη. Βλέπε [10, Κεφάλαιο 8, Θεώρημα 5.1]. □

Εφαρμόζοντας το παραπάνω θεώρημα μπορούμε να προσδιορίσουμε αν μια εξίσωση της μορφής (9.6) έχει λύση. Στην περίπτωση που η εξίσωση (9.6) έχει ακέραια λύση, η πρόταση που ακολουθεί μας παρέχει ένα φράγμα μέσα στο οποίο μπορούμε να ανιχνεύσουμε μία.

Πρόταση 9.3. *Αν η εξίσωση*

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

έχει μη μηδενική ακέραια λύση, τότε υπάρχει ακέραια λύση (x_0, y_0, z_0) της εξίσωσης τέτοια ώστε $x_0, y_0, z_0 \in \mathbb{N}$ και

$$\max\{x_0, y_0, z_0\} < 2 \max\{a^2, b^2, c^2\}.$$

Απόδειξη. Βλέπε [10, Κεφάλαιο 8, Πόρισμα 5.1]. □

Ορίζουμε την *συνάρτηση πρόσημο*, $sgn : \mathbb{Z} \to \{-1, 0, 1\}$, ως εξής:

$$sgn(z) = \begin{cases} 1, & \text{αν } z > 0, \\ 0, & \text{αν } z = 0, \\ -1, & \text{αν } z < 0. \end{cases}$$

Ανίχνευση Λύσεων Εξισώσεων Legendre. Θεωρούμε την εξίσωση (9.6). Τα βήματα προσδιορισμού ύπαρξης ακέραιας λύσης έχουν ως εξής:

1) Ελέγχουμε τα πρόσημα των a, b, c. Αν $\operatorname{sgn}(a) = \operatorname{sgn}(b) = \operatorname{sgn}(c)$ τότε η εξίσωση δεν έχει λύση. Διαφορετικά, συνεχίζουμε στο επόμενο βήμα
2) Απλοποιούμε την εξίσωση. Διαιρούμε την εξίσωση με το $d = (a, b, c)$ οπότε η εξίσωση γίνεται
$$a'x^2 + b'y^2 + c'z^2 = 0,$$
όπου $a' = a/d$, $b' = b/d$, $c' = c/d$.
3) Ελέγχουμε αν οι ακέραιοι a', b', c' είναι ελεύθεροι τετραγώνου. Υπολογίζουμε:
$$\begin{aligned} a' &= \operatorname{sgn}(a) a''^2 p_1 \cdots p_m r_1 \cdots r_s p'_1 \cdots p'_{m'}, \\ b' &= \operatorname{sgn}(b) b''^2 p_1 \cdots p_m q_1 \cdots q_n q'_1 \cdots q'_{n'}, \\ c' &= \operatorname{sgn}(c) c''^2 r_1 \cdots r_s q_1 \cdots q_n r'_1 \cdots r'_{s'} \end{aligned}$$
όπου $p_i, p'_i, q_i, q'_i, r_i, r'_i$ είναι πρώτοι διαφορετικοί μεταξύ τους ανά δύο.

4) Πολλαπλασιάζουμε την εξίσωση με

$$p_1 \cdots p_m q_1 \cdots q_n r_1 \cdots r_s.$$

5) Θέτουμε

$$A = q_1 \cdots q_n p_1' \cdots p_{m'}', \quad B = r_1 \cdots r_s q_1' \cdots q_{n'}', \quad C = p_1 \cdots p_m r_1' \cdots r_{s'}'$$

και

$$X = a'' p_1 \cdots p_m r_1 \cdots r_s x, \quad Y = b'' p_1 \cdots p_m q_1 \cdots q_n y, \quad Z = c'' r_1 \cdots r_s q_1 \cdots q_n z.$$

Έτσι, προκύπτει η εξίσωση

$$\operatorname{sgn}(a) A x^2 + \operatorname{sgn}(b) B y^2 + \operatorname{sgn}(c) C z^2 = 0,$$

η οποία πληροί τις υποθέσεις του Θεωρήματος 9.2.

6) Υπολογίζουμε τα σύμβολα του Legendre

$$(-AB/r_i'), \quad (-AB/p_i), \quad (-BC/p_i'), \quad (-BC/q_i), \quad (-AC/q_i'), \quad (-AC/r_i),$$

για κάθε $r_i', p_i, p_i', q_i, q_i', r_i \neq 2$. Αν όλα αυτά τα σύμβολα ισούνται με 1, τότε η αρχική εξίσωση έχει ακέραια λύση, διαφορετικά δεν έχει.

Ρητά Σημεία Κωνικής Θεωρούμε την κωνική που ορίζεται από την εξίσωση

$$f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{9.7}$$

όπου $a, b, c, d, e, f \in \mathbb{Q}$ με a, b και c όχι όλα μηδέν. Θα δείξουμε πως είναι δυνατόν να προσδιορίσουμε όλα τα σημεία της με ρητές συντεταγμένες, δηλαδή όλες τις ρητές λύσεις της παραπάνω εξίσωσης. Θα δούμε ότι ο υπολογισμός τους ανάγεται στον υπολογισμό μία λύσης για την εξίσωση του Legendre.

Πρώτα θα ασχοληθούμε με την περίπτωση όπου $b = 0$ και $ac \neq 0$. Όπως θα δούμε απαραίτητη προϋπόθεση για των υπολογισμό των ρητών λύσεων είναι η δυνατότητα υπολογισμού μία ρητής λύσης. Παρακάτω δίνουμε έναν αλγόριθμο για την εύρεση των ρητών λύσεων σε αυτή την περίπτωση. Πρώτα όμως ας παρατηρήσουμε ότι η ύπαρξη ρητής λύσης της εξίσωσης $ax^2 + by^2 + c = 0$ ισοδυναμεί με την ύπαρξη ακεραίας λύσης της εξίσωσης $ax^2 + by^2 + cz^2 = 0$.

Αλγόριθμος Εύρεσης των Ρητών Λύσεων της Εξίσωσης

$$ax^2 + cy^2 + dx + ey + f = 0, \quad ac \neq 0.$$

Τα βήματα που ακολουθούμε είναι τα εξής:

1) Θέτουμε $x = x' - d/2a$ και $y = y' - e/2c$ και φέρουμε την εξίσωση στην μορφή

$$Ax'^2 + By'^2 + C = 0.$$

2) Πολλαπλασιάζουμε με το ελάχιστο κοινό πολλαπλάσιο των παρανομαστών των A, B, C και απλοποιώντας με τον μέγιστο κοινό διαιρέτη των αριθμητών προκύπτει μία εξίσωση της μορφής

$$A'X^2 + B'Y^2 + C' = 0,$$

όπου A', B', C' είναι ακέραιοι ελεύθεροι τετραγώνου και πρώτοι μεταξύ τους ανά δύο.
3) Ελέγχουμε αν η εξίσωση του Legendre

$$A'u^2 + B'v^2 + C'w^2 = 0,$$

έχει μη μηδενική ακεραία λύση. Αν δεν έχει, τότε η εξίσωση $A'X^2 + B'Y^2 + C' = 0$ δεν έχει ρητές λύσεις και κατά συνέπεια η αρχική εξίσωση δεν έχει ρητές λύσεις. Διαφορετικά συνεχίζουμε στο επόμενο βήμα.
4) Υπολογίζουμε μία ακέραια λύση της $A'u^2 + B'v^2 + C'w^2 = 0$ και κατόπιν την αντίστοιχη ρητή λύση (x_0, y_0) της $A'X^2 + B'Y^2 + C' = 0$.
5) Θέτουμε $Y = m(X - x_0) + y_0$ στην εξίσωση $A'X^2 + B'Y^2 + C' = 0$ και υπολογίζουμε τις τιμές των X και Y συναρτήσει του m. Έτσι, προκύπτουν όλες οι ρητές λύσεις της εξίσωσης $A'X^2 + B'Y^2 + C' = 0$.
6) Υπολογίζουμε τις τιμές των x, y οι οποίες αντιστοιχούν στις τιμές των X και Y οι οποίες υπολογίστηκαν στο Βήμα 6.
7) Οι ρητές λύσεις της εξίσωσης είναι οι (x, y), για κάθε $m \in \mathbb{Q}$.

Στη συνέχεια, περιγράφουμε τις ρητές λύσεις της εξίσωσης (9.7) στη γενική περίπτωση.

Ρητές λύσεις της (9.7) Διακρίνουμε τις εξής περιπτώσεις:

1) Αν $a = b = 0$, τότε οι ρητές λύσεις είναι:

$$(x, y) = \left(\frac{-cm^2 - em - f}{d}, m\right), \quad m \in \mathbb{Q}.$$

2) Αν $c = b = 0$, τότε οι ρητές λύσεις είναι:

$$(x, y) = \left(m, \frac{-am^2 - dm - f}{e}\right), \quad m \in \mathbb{Q}.$$

3) Αν $b = 0$ και $ac \neq 0$ τότε βρίσκουμε τις ρητές λύσεις με τον «Αργόριθμο Εύρεσης Ρητών Λύσεων».
4) Αν $b \neq 0$ και $a = c = 0$, τότε θέτουμε $x = x' - y'$ και $y = x' + y'$ και στη συνέχεια βρίσκουμε τις ρητές λύσεις με τον «Αλγόριθμο Εύρεσης Ρητών Λύσεων».
5) Αν $b \neq 0$ και $a \neq 0$, τότε θέτουμε $x = x' - by'/2a$, $y = y'$ και στη συνέχεια βρίσκουμε τις ρητές λύσεις με τον «Αλγόριθμο Εύρεσης Ρητών Λύσεων».
6) Αν $b \neq 0$ και $c \neq 0$, τότε εργαζόμαστε ανάλογα με την προηγουμένη περίπτωση.

Ασκήσεις

΄Ασκηση 9.15. *Να εξετασθεί αν οι παρακάτω εξισώσεις έχουν ακέραια μη μηδενική λύση:*

α) $18x^2 + 28y^2 - 7z^2 = 0$,
β) $75x^2 + 27y^2 - 30z^2 = 0$,
γ) $6x^2 + 10y^2 - 125z^2 = 0$.

Απόδειξη. α) Ακολουθώντας τα βήματα του αλγορίθμου παρατηρούμε ότι οι συντελεστές δεν έχουν όλοι το ίδιο πρόσημο και ότι $(18, 28, 7) = 1$. ΄Αρα η εξίσωση δεν απλοποιείται άλλο. Σύμφωνα με το βήμα 3, έχουμε:

$$18 = 3^2 2 = a''^2 p_1', \;\; 28 = 2^2 7 = b''^2 q_1, \;\; -7 = -q_1$$

Οπότε, θέτουμε:

$$A = 7 \cdot 2 = 14, \;\; B = 1, \;\; C = 1,$$

και

$$X = 3x, \;\; Y = 2 \cdot 7y = 14y, \;\; Z = 7z.$$

΄Ετσι, προκύπτει η εξίσωση:

$$14X^2 + Y^2 - Z^2 = 0.$$

Τέλος, υπολογίζουμε το σύμβολο του Legendre:

$$(-BC/q_1) = (1/7) = 1.$$

΄Αρα, η εξίσωση έχει ακέραια μη μηδενική λύση.

β) Αρχικά παρατηρούμε ότι ο μέγιστος κοινός διαιρέτης των συντελεστών της εξίσωσης είναι ο 3. Διαιρώντας όλους τους συντελεστές με 3, η εξίσωση γίνεται:

$$25x^2 + 9y^2 - 10z^2 = 0.$$

Στην συνέχεια, τους συντελεστές που δεν είναι ελεύθεροι τετραγώνου τους απλοποιούμε με κατάλληλη αλλαγή συντεταγμένων. Οπότε, θέτουμε $5x = X$, $3y =$, $z = Z$ και η εξίσωση γίνεται:

$$X^2 + Y^2 - 10Z^2 = 0.$$

Εύκολα παρατηρούμε ότι όλοι οι συντελεστές είναι πρώτοι μεταξύ τους ανά δύο οπότε πληρούνται οι προϋποθέσεις του Θεωρήματος 9.2. Καθώς ο μόνος συντελεστής που δεν 1 είναι ο $c = -10$, αρκεί να βρούμε αν το $-ab = -1$ είναι τετραγωνικό υπόλοιπο $\bmod 10$. Καθώς $10 = 2 \cdot 5$ αρκεί να βρούμε αν το -1 είναι τετραγωνικό υπόλοιπο $\bmod 5$. Καθώς

$$(-1/5) = (-1)^{(5-1)/2} = 1,$$

η εξίσωση έχει ακέραια μη μηδενική λύση.

γ) Αρχικά παρατηρούμε ότι οι συντελεστές της εξίσωσης είναι πρώτοι μεταξύ τους. Στη συνέχεια, θέτουμε $x = x'$, $y = y'$, $5z = z'$. ΄Ετσι, έχουμε:

$$6x'^2 + 10y'^2 - 5z'^2 = 0.$$

Πολλαπλασιάζουμε την εξίσωση με 10 και προκύπτει η εξίσωση

$$60x'^2 + 100y'^2 - 50z'^2 = 0.$$

Θέτοντας $2x' = X$, $10y' = Y$, $5z' = Z$, παίρνουμε:

$$15X^2 + Y^2 - 2Z^2 = 0.$$

Ελέγχουμε αν το 2 είναι τετραγωνικό υπόλοιπο 15. Καθώς

$$(2/3) = (-1)^{(3^2-1)/8} = -1,$$

η εξίσωση δεν έχει ακέραια μη μηδενική λύση. □

΄Ασκηση 9.16. *Να υπολογιστούν οι ρητές λύσεις των παρακάτω εξισώσεων:*
α) $x^2 + y^2 - 53 = 0$,
β) $x^2 + x + 2y - 1 = 0$,
γ) $x^2 + xy + y - 37 = 0$,
δ) $x^2 + xy + y^2 + 4x - 15y - 19 = 0$.

Απόδειξη. α) Καθώς $b = 0$ και $ac \neq 0$ βρισκόμαστε στην τρίτη περίπτωση της εύρεσης ρητών λύσεων. Ακολουθώντας τον Αργόριθμο Εύρεσης Ρητών Λύσεων προσπερνάμε τα βήματα 1 και 2 και σύμφωνα με το βήμα 3 διερευνούμε αν η εξίσωση $u^2+v^2-53w^2 = 0$ έχει ακέραιες λύσεις. Καθώς

$$(-1/53) = (-1)^{(53-1)/2} = 1,$$

από το Θεώρημα 9.2 συνεπάγεται ότι η $u^2 + v^2 - 53w^2 = 0$ έχει ακέραιες λύσεις.

Εύκολα διαπιστώμουμε ότι η $(x_0, y_0) = (2, 7)$ αποτελεί ρητή λύση της $x^2+y^2-53 = 0$. ΄Ετσι, αντικαθιστούμε το y με $m(x - 2) - 7$, όπου $m \in \mathbb{Q}$ και προκύπτει ότι

$$x^2 + m^2(x - 2)^2 + 49 + 14m(x - 2) - 53 = 0.$$

Από την παραπάνω σχέση έχουμε ότι

$$(x^2 - 4) + m^2(x - 2)^2 + 14m(x - 2) = 0$$

και απλοποιώντας με το $x - 2$ προκύπτει ότι

$$x = \frac{2m^2 - 14m - 2}{m^2 + 1}.$$

Αντικαθιστώντας τέλος το x στην σχέση $m(x - 2) + 7$ προκύπτει το y. ΄Ετσι, έχουμε ότι

$$(x, y) = \left(\frac{2m^2 - 14m - 2}{m^2 + 1}, \frac{-7m^2 - 4m + 7}{m^2 + 1}\right), \quad m \in \mathbb{Q}$$

είναι όλες οι ρητές λύσεις της αρχικής εξίσωσης.

β) Καθώς $b = c = 0$ βρισκόμαστε στην δεύτερη περίπτωση της εύρεσης ρητών λύσεων η οποία μας παραθέτει άμεσα τις ρητές λύσεις της εξίσωσης που είναι οι

$$(x, y) = \left(m, \frac{-m^2 - m + 1}{2}\right), \quad m \in \mathbb{Q}.$$

γ) Καθώς $b \neq 0$ και $a \neq 0$ βρισκόμαστε στην πέμπτη περίπτωση της εύρεσης ρητών λύσεων. Θέτοντας $x = x' - y'/2$ και $y = y'$, προκύπτει:

$$(x')^2 - \frac{(y')^2}{4} + y' - 37 = 0.$$

Ακολουθώντας τον Αργόριθμο Εύρεσης Ρητών Λύσεων, θέτουμε $x' = x''$ και $y' = y''+2$. Έτσι, παίρνουμε:

$$(x'')^2 - \frac{(y'')^2}{4} - 36 = 0.$$

Στη συνέχεια, θέτουμε $x'' = 6X$, $y'' = 12Y$ και έτσι έχουμε την εξίσωση

$$X^2 - Y^2 - 1 = 0.$$

Αμέσως διαπιστώμουμε ότι το ζεύγος $(x_0, y_0) = (1, 0)$ αποτελεί ρητή λύση της $X^2 - Y^2 - 1 = 0$. Έτσι, θέτουμε $Y = m(X - 1)$, όπου $m \in \mathbb{Q}$, και παίρνουμε:

$$X^2 - m^2(X - 1)^2 - 1 = 0.$$

Απλοποιώντας με το $X - 1$, προκύπτει:

$$X = \frac{m^2 + 1}{m^2 - 1}, \quad m \in \mathbb{Q} \setminus \{\pm 1\}.$$

Αντικαθιστώντας τέλος το X στην σχέση $U = m(X - 1)$ προκύπτει το Y. Έτσι, παίρνουμε:

$$(X, Y) = \left(\frac{m^2 + 1}{m^2 - 1}, \frac{2m}{m^2 - 1}\right).$$

Από τις αντικαταστάσεις που κάναμε, έχουμε ότι $x = 6X + 6Y + 1$ και $y = 12Y + 2$. Επομένως, τα ζεύγη

$$(x, y) = \left(\frac{5m^2 - 12m + 7}{m^2 - 1}, \frac{2m^2 + 24m - 2}{m^2 - 1}\right), \quad m \in \mathbb{Q} \setminus \{\pm 1\}$$

είναι όλες οι ρητές λύσεις της αρχικής εξίσωσης.

δ) Καθώς $b \neq 0$ και $ac \neq 0$ η εξίσωση ανήκει και στην πέμπτη και στην έκτη περίπτωση της εύρεσης ρητών λύσεων. Επιλέγουμε την τυχαία την έκτη και έτσι θέτουμε $x = x'$ και $y = y' - x'/2$. Έτσι, προκύπτει η εξίσωση

$$\frac{3}{4}(x')^2 + (y')^2 - \frac{7}{2}x' + 15y' - 19 = 0.$$

Συνεχίζοντας με τον Αργόριθμο Εύρεσης Ρητών Λύσεων θέτουμε $x' = x'' + 7/3$, $y' = y'' - 15/2$, και έχουμε:

$$\frac{9}{4}(x'')^2 + 3(y'')^2 - 238 = 0.$$

Στη συνέχεια αντικαθιστούμε $x'' = 2/3X$, $y'' = Y$ και καταλήγουμε στην εξίσωση

$$X^2 + 3Y^2 - 238 = 0.$$

Καθώς $238 = 2 \cdot 7 \cdot 17$, το Θεώρημα 9.2 συνεπάγεται ότι η εξίσωση $u^2 + 3v^2 - 258w^2 = 0$ έχει ακέραιες λύσεις, αν το -3 είναι τετραγωνικό υπόλοιπο (mod 258), δηλαδή, αν τα σύμβολα του Legendre $(-3/7)$ και $(-3/17)$ είναι ίσα με 1. Εύκολα διαπιστώνουμε ότι $(-3/17) = -1$ και κατά συνέπεια η εξίσωση δεν έχει ρητές λύσεις. □

9.5 Η Εξίσωση $x^2 - dy^2 = 1$

Μία από τις πλέον γνωστές Διοφαντικές εξισώσεις είναι και η εξίσωση

$$x^2 - dy^2 = 1, \tag{9.8}$$

όπου d είναι ακέραιος > 1 ο οποίος δεν είναι τέλειο τετράγωνο. Πολύ συχνά αναφέρεται στη βιβλιογραφία ως *εξίσωση των Pell – Fermat*.

Θεώρημα 9.3. *Η εξίσωση (9.8) έχει άπειρο πλήθος ακεραίων λύσεων. Ας είναι (x_1, y_1) μία ακέραια λύση με $x_1 > 1$, $y_1 > 0$ έτσι, ώστε για κάθε άλλη ακέραια λύση (x, y) με $x > 1$, $y > 0$ να ισχύει $x > x_1$. Τότε, όλες οι ακέραιες λύσεις (x, y) της 9.8 δίνονται από την σχέση*

$$x + y\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{Z}.$$

Έτσι, ο υπολογισμός των λύσεων της (9.8), ανάγεται στην εύρεση της λύσης (x_1, y_1) η οποία καλείται *βασική*. Για μικρές τιμές του d είναι εύκολο να βρεθεί, ενώ για μεγάλες είναι δυνατόν με την χρήση της μεθόδου των συνεχών κλασμάτων που θα συναντήσουμε στο επόμενο κεφάλαιο.

Ασκήσεις

Στη παρακάτω άσκηση η βασική λύση των προτεινομένων εξισώσεων υπολογίζεται εύκολα κάνοντας διαδοχικές αντικαταστάσεις στο x ξεκινώντας από το 2 και λύνοντας ως προς y για y θετικό.

΄Ασκηση 9.17. *Να βρεθούν οι ακέραιες λύσεις των εξισώσεων*
α) $x^2 - 2y^2 = 1$,
β) $x^2 - 11y^2 = 1$,
γ) $x^2 - 15y^2 = 1$.

Απόδειξη. α) Παρατηρούμε αμέσως για $x = 2$ η εξίσωση δεν έχει λύση, ενώ για $x = 3$ προκύπτει ότι $y = 2$. Συνεπώς, η βασική λύση της $x^2 - 2y^2 = 1$ είναι το ζεύγος $(3, 2)$. Επομένως, οι ακέραιες λύσεις (x, y) της εξίσωσης δίνονται από την σχέση:

$$x + y\sqrt{2} = \pm(3 + 2\sqrt{2})^n, \quad n \in \mathbb{Z}.$$

β) Παρατηρούμε όπως και παραπάνω ότι το ζεύγος $(10, 3)$ είναι η βασική λύση της εξίσωσης $x^2 - 11y^2 = 1$. ΄Αρα, οι ακέραιες λύσεις (x, y) της εξίσωσης δίνονται από την σχέση:

$$x + y\sqrt{11} = \pm(10 + 3\sqrt{11})^n, \quad n \in \mathbb{Z}.$$

γ) Παρατηρούμε ότι το ζεύγος $(4, 1)$ είναι η βασική λύση της $x^2 - 15y^2 = 1$. ΄Αρα, οι ακέραιες λύσεις της εξίσωσης δίνονται από την σχέση:

$$x + y\sqrt{15} = \pm(4 + \sqrt{15})^n, \quad n \in \mathbb{Z}.$$

□

΄Ασκηση 9.18. *Ας είναι p πρώτος. Να δείξετε ότι η εξίσωση*

$$x^2 - py^2 = -1 \tag{9.9}$$

έχει ακέραιες λύσεις αν και μόνον αν $p = 2$ ή $p \equiv 1 \pmod 4$.

Απόδειξη. Ας είναι $(x_0, y_0) \in \mathbb{Z}^2$ μία λύση της (9.9) με $y_0 > 0$. Τότε, έχουμε $py_0^2 = x_0^2 + 1$. Αν $x_0 = 2k$, με $k \in \mathbb{Z}$, τότε $py_0^2 = 4k^2 + 1$ και κατά συνέπεια οι ακέραιοι p και y_0 είναι περιττοί. Καθώς $y_0^2 \equiv 1 \pmod 4$, έχουμε $p \equiv 1 \pmod 4$. Αν $x_0 = 2k + 1$, με $k \in \mathbb{Z}$, τότε $py_0^2 = 2(2k^2 + 2k + 1)$. Αν ο y_0 άρτιος, τότε $4 \mid 2(2k^2 + 2k + 1)$ που είναι άτοπο. ΄Αρα, παίρνουμε ότι ο ακέραιος y_0 είναι περιττός και $p = 2$.

Αντίστροφα, ας είναι $p = 2$. Τότε, έχουμε την εξίσωση

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

Μία προφανής λύση της εξίσωσης είναι η $(1, 1)$. Στη συνέχεια, ας υποθέσουμε ότι $p \equiv 1 \pmod 4$. Θεωρούμε την εξίσωση

$$x^2 - py^2 = 1. \tag{9.10}$$

Συμβολίζουμε με (x_0, y_0) την βασική της λύση. Αν ο ακέραιος x_0 είναι άρτιος, τότε έχουμε $py_0^2 \equiv 3 \pmod 4$, απ΄ όπου προκύπτει $y_0^2 \equiv 3 \pmod 4$, το οποίο είναι αδύνατο. ΄Αρα, ο ακέραιος x_0 είναι περιττός. ΄Ετσι, έχουμε:

$$py_0^2 = (x_0 - 1)(x_0 + 1)$$

και $(x_0 - 1, x_0 + 1) = 2$. Επομένως, υπάρχουν ακέραιοι m, n τέτοιοι, ώστε ισχύει $x_0 - 1 = 2m^2$ και $x_0 + 1 = 2pn^2$ ή το αντίστροφο. Αν $x_0 - 1 = 2pn^2$ και $x_0 + 1 = 2m^2$, τότε αφαιρώντας τις δύο σχέσεις παίρνουμε $m^2 - pn^2 = 1$, δηλαδή, η (m, n) είναι λύση της (9.10) με $m < x_0$ το οποίο είναι άτοπο. ΄Αρα $x_0 - 1 = 2m^2$ και $x_0 + 1 = 2pn^2$, που συνεπάγεται ότι $m^2 - pn^2 = -1$, δηλαδή, η (m, n) είναι μία λύση τις εξίσωσης $x^2 - py^2 = -1$. □

΄Ασκηση 9.19. *Ας είναι d ένας ακέραιος > 1 ο οποίος δεν είναι τέλειο τετράγωνο ακεραίου και διαιρείται από ένα πρώτο p με $p \equiv 3 \pmod 4$. Τότε, η εξίσωση*

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

δεν έχει ακέραια λύση.

Απόδειξη. Ας είναι x_0, y_0 ακέραιοι τέτοιοι, ώστε $x_0^2 - dy_0^2 = -1$. Καθώς $p \mid d$, έχουμε $x_0^2 \equiv -1 \pmod p$. Τότε, από το Πόρισμα 7.2, έχουμε $p \equiv 1 \pmod 4$ που είναι άτοπο. ΄Αρα, η εξίσωση δεν έχει ακέραια λύση. □

΄Ασκηση 9.20. *Ας είναι d ένας ακέραιος > 1 ο οποίος δεν είναι τέλειο τετράγωνο ακεραίου. Τότε, η εξίσωση*

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

έχει ένα άπειρο πλήθος ακεραίων λύσεων (x, y) με $y \equiv 0 \pmod d$.

Απόδειξη. Καθώς η παραπάνω εξίσωση έχει άπειρο πλήθος ακεραίων λύσεων, υπάρχει $(a,b) \in \{0,\dots,d-1\}^2$ έτσι, ώστε υπάρχει πλήθος ακεραίων λύσεων (u,v) με $u \equiv a \pmod d$ και $v \equiv b \pmod d$. Συμβολίζουμε με S το σύνολο αυτών των λύσεων. Αν $(u_1,v_1) \in S$, τότε για κάθε $(u,v) \in S$ έχουμε $u \equiv u_1 \pmod d$ και $v \equiv v_1 \pmod d$. Τότε, παίρνουμε τις σχέσεις

$$1 = (u^2 - dv^2)(u_1^2 - dv_1^2) = (uu_1 - dvv_1)^2 - d(uv_1 - u_1v)^2$$

οι οποίες δίνουν τις λύσεις $(uu_1 - dvv_1, uv_1 - u_1v)$, με $(u,v) \in S$. Ισχύει $uv_1 - u_1v \equiv ab - ab \equiv 0 \pmod d$. Έτσι, καθώς το σύνολο S είναι άπειρο, υπάρχει ένα άπειρο πλήθος ακεραίων λύσεων (x,y) της παραπάνω εξίσωσης με $y \equiv 0 \pmod d$. □

9.6 Συνδυαστικές Ασκήσεις

Ορισμός 9.4. Ένα ορθογώνιο τρίγωνο του οποίου τα μήκη των πλευρών του είναι ακέραιοι αριθμοί καλείται *Πυθαγόρειο τρίγωνο*. Επιπλέον, αν τα μήκη των πλευρών του Πυθαγορείου τριγώνου είναι ακέραιοι πρώτοι μεταξύ τους, τότε το Πυθαγόρειο τρίγωνο καλείται *αρχικό*.

Άσκηση 9.21 (American Mathematical Monthly, 11122 [8])**.** *Να δείχθούν τα εξής:*

α) Οι κάθετες πλευρές ενός Πυθαγορείου τριγώνου δεν είναι τέλειοι αριθμοί.

β) Η υποτείνουσα ενός Πυθαγορείου τριγώνου δεν είναι τέλειος άρτιος.

Απόδειξη. α) Ας είναι (a,b,c) μία Πυθαγόρεια τριάδα, όπου a, b είναι οι κάθετες πλευρές και c η υποτείνουσα. Τότε, οι a, b δεν είναι και οι δύο περιττοί Ας υποθέσουμε ότι οι ακέραιοι a, b είναι άρτιοι τέλειοι αριθμοί. Έτσι, έχουμε $a = 2^{p-1}(2^p - 1)$ και $b = 2^{q-1}(2^q - 1)$, όπου p, q, 2^{p-1}, 2^{q-1} είναι πρώτοι. Καθώς $a \neq b$ (διαφορετικά η υποτείνουσα δε θα ήταν ακέραιος αριθμός), έχουμε ότι $p \neq q$. Χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι $p < q$. Τότε, ισχύει $(a,b) = 2^{p-1}$ και η τριάδα (a',b',c'), όπου $a' = 2^p - 1$, $b' = 2^{q-p}(2^q - 1)$, $c' = c/2^{p-1}$, είναι μια αρχική Πυθαγόρεια τριάδα. Τότε, χωρίς περιορισμό της γενικότητας, μπορούμε να γράψουμε ότι

$$a' = u^2 - v^2 = (u-v)(u+v) \quad \text{και} \quad b = 2uv,$$

όπου $u,v \in \mathbb{Z}^+$, $u > v$, $u \not\equiv v \pmod 2$ και $(u,v) = 1$. Καθώς ο ακέραιος a' έναι πρώτος, έχουμε

$$u - v = 1 \quad \text{και} \quad u + v = 2^p - 1,$$

από όπου προκύπτει

$$u = 2^{p-1} \quad \text{και} \quad v = 2^{p-1} - 1.$$

Οπότε, από την σχέση $b = 2uv$ έχουμε ότι

$$2^{q-p}(2^q - 1) = 2^p(2^{p-1} - 1)$$

από όπου προκύπτει ότι

$$2^{q-p} = 2^p \quad \text{και} \quad 2^q - 1 = 2^{p-1} - 1.$$

Έτσι, παίρνουμε $q = 2p$ και $q = p - 1$, απ' όπου έπεται $p = -1$ που είναι άτοπο.

Ας υποθέσουμε τώρα ότι ο a είναι περιττός και ο b άρτιος. Καθώς a περιττός τέλειος, $4 \nmid \sigma(a)$ και, σύμφωνα με την Άσκηση 3.28, ισχύει $a \equiv 1 \pmod 4$. Επίσης, έχουμε $b = 2^{q-1}(2^q - 1)$, όπου q και $2^q - 1$ είναι πρώτοι. Στη συνέχεια θα διακρίνουμε δύο περιπτώσεις. Αν το $2^q - 1 \mid a$ και αν όχι.

Ας είναι $2^q - 1 \mid a$. Τότε (a', b', c') είναι μια Πυθαγόρεια τριάδα με $a' = a/(2^q - 1)$, $b' = 2^{q-1}$ και $(a', b') = 1$. Συνεπώς, υπάρχουν $u, v \in \mathbb{Z}^+$ με $u > v$, $u \not\equiv v \pmod 2$ και $(u, v) = 1$ τέτοια ώστε

$$a' = u^2 - v^2 = (u - v)(u + v) \quad \text{και} \quad b' = 2uv.$$

Από τις σχέσεις $(u, v) = 1$ και $b' = 2^{q-1}$ έχουμε $u = 2^{q-2}$, $v = 1$ και, καθώς $u > v$, παίρνουμε $q \geq 3$. Έτσι, έχουμε:

$$a = (u^2 - v^2)(2^q - 1) = (2^{2q-4} - 1)(2^q - 1).$$

Ισχύει ότι $2^q - 1 \nmid 2^{2q-4} - 1$. Πράγματι, αν $q = 3$, τότε $2^3 - 1 = 7$, $2^2 - 1 = 3$ και $7 \nmid 3$. Για $q > 3$, έχουμε:

$$2^{2q-4} - 1 = (2^q - 1)2^{q-4} + (2^{q-4} - 1).$$

Αν $2^q - 1 \mid 2^{2q-4} - 1$, τότε από την παραπάνω ισότητα έπεται ότι $2^q - 1 \mid 2^{q-4} - 1$ που είναι άτοπο. Άρα, ισχύει $2^q - 1 \nmid 2^{2q-4} - 1$ και επομένως $(2^{2q-4} - 1, 2^q - 1) = 1$. Επομένως, ισχύει:

$$\sigma(a) = \sigma(2^{2q-4} - 1)\sigma(2^q - 1) = \sigma(2^{2q-4} - 1)2^q.$$

Καθώς $q \geq 3$, έχουμε ότι $\sigma(a) \equiv 0 \pmod 4$ το οποίο δεν συμβαίνει.

Στη συνέχεια, υποθέτουμε ότι $2^q - 1 \nmid a$. Έχουμε:

$$a = u^2 - v^2 = (u - v)(u + v) \quad \text{και} \quad b = 2uv,$$

όπου $u, v \in \mathbb{Z}^+$, $u > v$, $u \not\equiv v \pmod 2$ και $(u, v) = 1$. Καθώς οι μοναδικοί περιττοί θετικοί ακέραιοι διαιρέτες του b είναι οι 1 και $2^q - 1$, παίρνουμε:

$$u = 2^{q-2}(2^q - 1),\ v = 1 \quad \text{ή} \quad u = 2^q - 1, \quad v = 2^{q-2}.$$

Έτσι, έχουμε:

$$a = 2^{2q-4}(2^q - 1)^2 - 1 \quad \text{ή} \quad a = (2^q - 1)^2 - 2^{2q-4}.$$

Αν $q = 2$, τότε και στις τις δύο περιπτώσεις έχουμε $a = 8$ που είναι άτοπο. Άρα, $q \geq 3$. Αν $a = 2^{2q-4}(2^q - 1)^2 - 1$, τότε $a \equiv 3 \pmod 4$ που είναι άτοπο. Ας υποθέσουμε ότι $a = (2^q - 1)^2 - 2^{2q-4}$. Τότε, έχουμε:

$$a = (2^q - 2^{q-2} - 1)(2^q + 2^{q-2} - 1).$$

Ας είναι $s = (2^q - 2^{q-2} - 1, 2^q + 2^{q-2} - 1)$. Τότε, ο s διαιρεί την διαφορά των δύο ακεραίων και επομένως $s \mid 2^{q-1}$. Άρα $s = 1$ ή $s = 2^m$ με $m \leq q - 1$. Καθώς οι ακέραιοι $2^q - 2^{q-2} - 1$ και $2^q + 2^{q-2} - 1$ είναι περιττοί, ο s είναι επίσης περιττός. Άρα $s = 1$. Αν $q = 3$, τότε $a = 45$ που δεν είναι τέλειος. Ας είναι $q \geq 5$. Τότε $2^q - 2^{q-2} - 1 \equiv 3 \pmod 4$. Από τα παραπάνω έπεται ότι η πρωτογενής ανάλυση του a περιέχει περιττή δύναμη πρώτου που είναι ισότιμος με $3 \pmod 4$. Αυτό όμως είναι αδύνατο, σύμφωνα με την

΄Ασκηση 3.28. ΄Αρα, οι κάθετες πλευρές ενός Πυθαγορείου τριγώνου δεν είναι τέλειοι αριθμοί.

β) Αν x είναι άρτιος τέλειος, τότε $x = 2^{p-1}(2^p - 1)$, όπου p και $2^p - 1$ πρώτοι. Επομένως, οι πρώτοι παράγοντες του x είναι ο 2 και ο $2^p - 1$. Κανένας από αυτούς δεν είναι ισότιμος με 1 (mod 4).

Ας είναι (A, B, C) μια Πυθαγόρεια τριάδα με C υποτείνουσα η οποία είναι άρτιος τέλειος αριθμός. Αν (a, b, c) είναι η αντίστοιχη αρχική Πυθαγόρεια τριάδα, δηλαδή,

$$A = ad, \quad B = bd, \quad C = cd,$$

όπου $d = (A, B, C)$. Υποθέτουμε, χωρίς περιορισμό της γενικότητας, ότι έχουμε

$$a = u^2 - v^2 = (u - v)(u + v) \quad \text{και} \quad b = 2uv,$$

όπου $u, v \in \mathbb{Z}^+$, $u > v$, $u \not\equiv v \pmod 2$ και $(u, v) = 1$. Το τετράγωνο ενός περιττού είναι 1 (mod 4) ενώ το τετράγωνο ενός άρτιου είναι 0 (mod 4). Επομένως, $c \equiv 1 \pmod 4$. Καθώς το c είναι παράγοντας ενός άρτιου τέλειου αυτό είναι αδύνατο. ΄Αρα δεν υπάρχει υποτείνουσα ίση με έναν άρτιο τέλειο αριθμό. □

Η επόμενη άσκηση αναφέρεται σε ένα αρχαίο πρόβλημα, στη κατασκευή τριών διαδοχικών όρων μίας αριθμητικής προόδου οι οποίοι να είναι τέλεια τετράγωνα ακεραίων.

΄Ασκηση 9.22. *Ας είναι x, y θετικοί ακέραιοι πρώτοι μεταξύ τους. Τότε, έχουμε $y^2 - x = A^2$ και $y^2 + x = B^2$, όπου A, B θετικοί ακέραιοι, αν και μόνον αν ο ακέραιος y είναι το μήκος της υποτείνουσας ενός αρχικού Πυθαγορείου τριγώνου και ο x το τετραπλάσιο του εμβαδού του. Επιπλέον, υπάρχουν θετικοί ακέραιοι $b > a$, πρώτοι μεταξύ τους, ώστε να ισχύει:*

$$A = |(a + b)^2 - 2b^2|, \quad y = a^2 + b^2, \quad B = (a + b)^2 - 2a^2.$$

Απόδειξη. Ας υποθέσουμε ότι $y^2 - x = A^2$ και $y^2 + x = B^2$, όπου A, B θετικοί ακέραιοι. Παρατηρούμε ότι οι A και B είναι και οι δύο άρτιοι ή και οι δύο περιττοί. Θέτουμε $p = (A + B)/2$ και $q = (B - A)/2$. ΄Ετσι, έχουμε:

$$y^2 - x = (p - q)^2 \quad \text{και} \quad y^2 + x = (p + q)^2.$$

Προσθέτοντας και αφαιρώντας κατά μέλη της δύο ισότητες, προκύπτει:

$$y^2 = p^2 + q^2 \quad \text{και} \quad x = 2pq.$$

΄Αρα, ο ακέραιος y είναι το μήκος της υποτείνουσας ενός Πυθαγορείου τριγώνου με μήκη κάθετων πλευρών p και q, του οποίου το τετραπλάσιο του εμβαδού του ισούται με x. Καθώς οι ακέραιοι x και y είναι πρώτοι μεταξύ τους, συνεπάγεται ότι η Πυθαγόρεια τριάδα (p, q, y) είναι αρχική.

Αντίστροφα, αν ο ακέραιος y είναι το μήκος της υποτείνουσας ενός αρχικού Πυθαγορείου τριγώνου και ο x το τετραπλάσιο του εμβαδού του, τότε υπάρχουν ακέραιοι p και q με $y^2 = p^2 + q^2$ και $x = 2pq$. ΄Ετσι, προκύπτει $y^2 - x = (p - q)^2$ και $y^2 + x = (p + q)^2$, δηλαδή οι ακέραιοι $y^2 - x$ και $y^2 + x$ είναι τέλεια τετράγωνα ακεραίων.

Επιπλέον, από το Θεώρημα 9.1 έπεται ότι υπάρχουν ακέραιοι a, b με $a \not\equiv b \pmod 2$, $b > a > 0$ και $(a,b) = 1$ τέτοιοι, ώστε να έχουμε:

$$y = a^2 + b^2, \quad p = b^2 - a^2, \quad q = 2ab,$$

ή

$$y = a^2 + b^2, \quad p = 2ab, \quad q = b^2 - a^2.$$

΄Ετσι, παίρνουμε:

$$B = p + q = (a+b)^2 - 2a^2 \quad \text{και} \quad A = p - q = |(a+b)^2 - 2b^2|.$$

□

Στην επόμενη άσκηση εφαρμόζεται η ΄Ασκηση 9.22 και η απόδειξή της βασίζεται στην αρχή της άπειρης καθόδου.

΄Ασκηση 9.23. *Να δειχθεί ότι δεν είναι δυνατόν τέσσερεις διαδοχικοί όροι μίας αριθμητικής προόδου να είναι τετράγωνα ακεραίων.*

Απόδειξη. Ας είναι A_1^2, A_2^2, A_3^2, A_4^2, όπου A_1, A_2, A_3, A_4 θετικοί ακέραιοι, τέσσερεις διαδοχικοί όροι μίας αριθμητικής προόδου με διαφορά x. Θέτουμε $d = (A_1, A_2, A_3, A_4)$. Υποθέτουμε ότι $d > 1$. Καθώς $A_i^2 + x = A_{i+1}^2$ $(i = 1,2,3)$, έχουμε $d^2 \mid x$. Οπότε, οι ακέραιοι $(A_1/d)^2$, $(A_2/d)^2$, $(A_3/d)^2$, $(A_4/d)^2$ είναι πρώτοι μεταξύ τους και είναι διαδοχικοί όροι μίας αριθμητικής προόδου με διαφορά x/d^2. Συνεπώς, μπορούμε να υποθέσουμε από την αρχή ότι $(A_1, A_2, A_3, A_4) = 1$.

Σύμφωνα με την ΄Ασκηση 9.22 υπάρχουν θετικοί ακέραιοι a, b, u, v με $b > a$, $v > u$ $(a,b) = 1$, $(u,v) = 1$, ώστε να ισχύουν τα εξής:

$$A_1 = |(a+b)^2 - 2b^2|, \quad A_2 = a^2 + b^2, \quad A_3 = (a+b)^2 - 2a^2$$

και

$$A_2 = |(u+v)^2 - 2v^2|, \quad A_3 = u^2 + v^2, \quad A_4 = (u+v)^2 - 2u^2.$$

΄Ετσι, έχουμε:

$$\begin{aligned} a^2 + b^2 &= |(u+v)^2 - 2v^2|, \\ (a+b)^2 - 2a^2 &= u^2 + v^2. \end{aligned}$$

Διακρίνουμε τις εξής δύο περιπτώσεις:

(α) $(u+v)^2 > 2v^2$. Τότε, έχουμε το σύστημα:

$$a^2 + b^2 = (u+v)^2 - 2v^2, \quad (a+b)^2 - 2a^2 = u^2 + v^2.$$

Προσθέτοντας και αφαιρώντας κατά μέλη τις δύο ισότητες, παίρνουμε:

$$b(a+b) = u(u+v), \quad a(b-a) = v(v-u).$$

Θέτουμε στις δύο ισότητες $b = ux$, όπου x ρητός. Από την πρώτη ισότητα, προκύπτει

$$a = \frac{u+v}{x} - ux.$$

Αντικαθιστώντας στη δεύτερη ισότητα, παίρνουμε:

$$(1-x^2)(2x^2-1)\left(\frac{u}{v}\right)^2+2(2x^2-1)\frac{u}{v}-(1+x^2)=0.$$

΄Αρα, η εξίσωση

$$(1-x^2)(2x^2-1)T^2+2(2x^2-1)T-(1+x^2)=0$$

έχει ρητή ρίζα και κατά συνέπεια η διακρίνουσά της

$$D=4(2x^2-1)^2+4(2x^2-1)(1-x^4)=4(2x^2-1)(2-x^2)x^2$$

είναι τέλειο τετράγωνο. Ισοδύναμα, η ποσότητα

$$(2x^2-1)(2-x^2)$$

είναι τέλειο τετράγωνο. Θέτουμε $x=c/d$, όπου c, d είναι θετικοί ακέραιοι, πρώτοι μεταξύ τους. Τότε, η ποσότητα

$$(2c^2-d^2)(2d^2-c^2)$$

είναι τετράγωνο ακεραίου. Ας είναι $\delta=(2c^2-d^2,2d^2-c^2)$. Αν $2\mid\delta$, τότε συνεπάγεται ότι οι ακέραιοι c και d είναι άρτιοι το οποίο είναι άτοπο. ΄Αρα, ο δ είναι περιττός. Αν $3\mid\delta$, τότε $2c^2\equiv d^2\pmod 3$, απ΄ όπου παίρνουμε $c\equiv d\equiv 0\pmod 3$ που είναι άτοπο. ΄Αρα, $(3,\delta)=1$. Στη συνέχεια, καθώς ο δ διαιρεί το άθροισμα και την διαφορά των $2c^2-d^2$ και $2d^2-c^2$, παίρνουμε $\delta\mid c^2+d^2$ και $\delta\mid 3(c^2-d^2)$, απ΄ όπου $\delta\mid c^2-d^2$. ΄Ετσι, προκύπτει ότι $\delta\mid 2c^2$ και $\delta\mid 2d^2$. Καθώς ο δ είναι περιττός, έχουμε $\delta\mid c^2$ και $\delta\mid d^2$, απ΄ όπου έχουμε $\delta=1$. Επομένως, υπάρχουν θετικοί ακέραιοι α, β, πρώτοι μεταξύ τους, ώστε να έχουμε:

$$2c^2-d^2=\alpha^2,\quad 2d^2-c^2=\beta^2.$$

΄Ετσι, οι ακέραιοι α^2, c^2, d^2, β^2 είναι διαδοχικοί όροι αριθμητικής προόδου με διαφορά d^2-c^2. Καθώς $x=c/d=b/u$ και $(c,d)=1$, έχουμε $c\le b$ και $d\le u$, απ΄ όπου έπεται ότι $c^2<a^2+b^2$ και $d^2<u^2+v^2$. Συνεχίζοντας με αυτό τον τρόπο μπορούμε να κατασκευάσουμε μία φθίνουσα ακολουθία θετικών ακεραίων οι οποίοι είναι μικρότεροι του a^2+b^2 με περισσότερο από a^2+b^2 στοιχεία που είναι αδύνατο.

(β) $(u+v)^2<2v^2$. Τότε, έχουμε το σύστημα:

$$a^2+b^2=2v^2-(u+v)^2,\quad (a+b)^2-2a^2=u^2+v^2,$$

απ΄ όπου παίρνουμε:

$$b(a+b)=v(v-u),\quad a(b-a)=u(u+v).$$

Θέτοντας $a=ux$, όπου x ρητός και απαλοίφοντας τον b, προκύπτει, όπως στη προηγουμένη περίπτωση ο ρητός u/v είναι λύση της εξίσωσης

$$(1+x^2)(1+2x^2)T^2+2(1+2x^2)T+(1-x^2)=0$$

και επομένως η διακρίνουσά της είναι τέλειο τετράγωνο. Έτσι, προκύπτει ότι η ποσότητα $(1+2x^2)(2+x^2)$ είναι τέλειο τετράγωνο. Θέτοντας $x = c/d$, όπου c, d είναι θετικοί ακέραιοι, πρώτοι μεταξύ τους, παίρνουμε ότι η ποσότητα

$$(2c^2 + d^2)(2d^2 + c^2)$$

είναι τετράγωνο ακεραίου. Ας είναι $\delta = (2c^2 + d^2, 2d^2 + c^2)$. Αν $2 \mid \delta$, τότε συνεπάγεται ότι οι ακέραιοι c και d είναι άρτιοι το οποίο είναι άτοπο. Άρα, ο δ είναι περιττός. Έχουμε $\delta \mid 2c^2 + d^2$ και $\delta \mid 2d^2 + c^2$, απ΄ όπου παίρνουμε $\delta \mid 3(c^2 + d^2)$, $\delta \mid c^2 - d^2$, και έτσι προκύπτει ότι $\delta \mid 6c^2$ και $\delta \mid 6d^2$. Καθώς ο δ είναι περιττός και $(c, d) = 1$, έπεται ότι $\delta \mid 3$. Καθώς $(c, d) = 1$, οι c, d δεν διαιρούνται και οι δύο με τον 3. Ας υποθέσουμε ότι ένας ακριβώς από τους c, d διαιρείται από τον 3. Τότε έχουμε $\delta = 1$. Οπότε, υπάρχουν θετικοί ακέραιοι α, β, πρώτοι μεταξύ τους, ώστε να ισχύει:

$$2c^2 + d^2 = \alpha^2, \quad 2d^2 + c^2 = \beta^2.$$

Ας είναι $3 \mid c$ και $3 \nmid d$. Τότε, έχουμε $\beta^2 \equiv 2 \pmod 3$ που είναι άτοπο. Στο ίδιο συμπερασμα καταλήγουμε αν $3 \mid d$ και $3 \nmid c$. Στη συνέχεια, ας υποθέσουμε ότι $3 \nmid c$ και $3 \nmid d$. Τότε $c^2 + 2d^2 \equiv d^2 + 2c^2 \equiv 0 \pmod 3$ και επομένως $\delta = 3$. Οπότε, υπάρχουν θετικοί ακέραιοι α, β, πρώτοι μεταξύ τους, ώστε να ισχύει:

$$2c^2 + d^2 = 3\alpha^2, \quad 2d^2 + c^2 = 3\beta^2.$$

Προσθέτοντας κατά μέλη παίρνουμε $c^2 + d^2 = \alpha^2 + \beta^2$. Έτσι, εύκολα διαπιστώνουμε ότι οι ακέραιοι $d^2, \beta^2, \alpha^2, c^2$ είναι διαδοχικοί όροι αριθμητικής προόδου με διαφορά $c^2 - \alpha^2$. Καθώς $x = c/d = a/u$ και $(c, d) = 1$, έχουμε $c \le b$ και $d \le u$, απ΄ όπου έπεται ότι $c^2 < a^2 + b^2$ και $d^2 < u^2 + v^2$. Έτσι, όπως και στη προηγουμένη περίπτωση καταλήγουμε σε άτοπο. □

9.7 Θεωρία Αριθμών με Maple

Το maple μέχρι σήμερα δεν έχει την δυνατότητα να επιλύει πολλές κατηγορίες Διοφαντικών εξισώσεων για αυτό και όταν κάποιος χρησιμοποιεί την εντολή isolve θα πρέπει να είναι πολύ προσεκτικός. Για παράδειγμα,

```
isolve(13/x^2 + 1996/y^2 = z/1997);
                {x = -1, y = -1, z = 4011973}
```

δηλαδή, το maple βρίσκει μία λύση για την διοφαντική εξίσωση

$$\frac{13}{x^2} + \frac{1996}{y^2} = \frac{z}{1997},$$

ενώ στην (9.9) είδαμε ότι υπάρχουν πολύ περισσότερες. Παρόλα αυτά οι γραμμικές Διοφαντικές εξισώσεις επιλύονται με μεγάλη ευκολία.

΄Ασκηση 9.24. *Να λυθούν οι παρακάτω Διοφαντικές εξισώσεις:*

α) $12x + 501y = 273$,

β) $41x + 73y = 3$,

γ) $2072x + 1813y = 2849$,
δ) $-24x - 10y + 14z = 6$,
ε) $7x - 11y + 20z = 59$.

Απόδειξη. Με κώδικα Maple:

```
isolve(12*x + 501*y = 273, k);
                 {x = -19 - 167 k, y = 1 + 4 k}
isolve(41*x + 73*y = 3, k);
               {x = -48 - 73 k, y = 27 + 41 k}
isolve(2072*x + 1813*y = 2849, k);
                  {x = 4 + 7 k, y = -3 - 8 k}
isolve(-24*x - 10*y + 14*z = 6, {k, l});
           {x = k, y = 5 - k + 7 l, z = 4 + k + 5 l}
isolve(7*x - 11*y + 20*z = 59, {k, l});
        {x = -3 - 7 k - 20 l, y = k, z = 4 + 3 k + 7 l}
```

□

Όπως παρατηρούμε οι γενικές λύσεις που δίνει το Maple διαφέρουν από αυτές που βρήκαμε στο (9.10) ακολουθώντας την αλγοριθμική διαδικασία που περιγράψαμε. Εύκολα διαπιστώνουμε ότι αν και με την πρώτη ματιά διαφέρουν εν τούτοις παράγουν ακριβώς τις ίδιες λύσεις.

Η επίλυση εξισώσεων Pell-Fermat είναι κατά κάποιο τρόπο εφικτή. Για παράδειγμα για την επίλυση της $x^2 - 2y^2 = 1$ το Maple δίνει ένα σύνολο τεσσάρων λύσεων οι οποίες είναι ίσες κατά απόλυτη τιμή και και από τις οποίες μπορεί να εκμαιεύσουμε την βασική λύση.

Άσκηση 9.25. *Να βρεθούν οι ακέραιες λύσεις των εξισώσεων*
α) $x^2 - 2y^2 = 1$,
β) $x^2 - 11y^2 = 1$,
γ) $x^2 - 15y^2 = 1$.

Απόδειξη. α) Εδώ βλέπουμε ότι ο αριθμός $3 + 2 * sqrt(2)$ μας προσδιορίζει και την βασική λύση που είναι η $(3, 2)$.

```
isolve(x^2 - 2*y^2 - 1, k)
       {(x = -(3 + 2*sqrt(2))^k/2 - (3 - 2*sqrt(2))^k/2,
       y = -sqrt(2)*((3 + 2*sqrt(2))^k - (3 - 2*sqrt(2))^k)/4),
       (x = -(3 + 2*sqrt(2))^k/2 - (3 - 2*sqrt(2))^k/2,
       y = sqrt(2)*((3 + 2*sqrt(2))^k + (3 - 2*sqrt(2))^k)/4)
       (x = (3 + 2*sqrt(2))^k/2 + (3 - 2*sqrt(2))^k/2,
       y = -sqrt(2)*((3 + 2*sqrt(2))^k - (3 - 2*sqrt(2))^k)/4)
       (x = (3 + 2*sqrt(2))^k/2 + (3 - 2*sqrt(2))^k/2,
       y = sqrt(2)*((3 + 2*sqrt(2))^k + (3 - 2*sqrt(2))^k)/4)}
```

β) Εδώ βλέπουμε ότι βασική λύση είναι η $(10, 3)$.

```
isolve(x^2 - 11*y^2 - 1, k);
{x = -(10 + 3*sqrt(11))^k/2 - (10 - 3*sqrt(11))^k/2,
 y = -sqrt(11)*((10 + 3*sqrt(11))^k - (10 - 3*sqrt(11))^k)/22},
{x = -(10 + 3*sqrt(11))^k/2 - (10 - 3*sqrt(11))^k/2,
 y = sqrt(11)*((10 + 3*sqrt(11))^k - (10 - 3*sqrt(11))^k)/22},
{x = (10 + 3*sqrt(11))^k/2 + (10 - 3*sqrt(11))^k/2,
 y = -sqrt(11)*((10 + 3*sqrt(11))^k - (10 - 3*sqrt(11))^k)/22},
{x = (10 + 3*sqrt(11))^k/2 + (10 - 3*sqrt(11))^k/2,
 y = sqrt(11)*((10 + 3*sqrt(11))^k - (10 - 3*sqrt(11))^k)/22}
```

γ) Εδώ βλέπουμε ότι βασική λύση είναι η $(4, 1)$.

```
isolve(x^2 - 15*y^2 - 1, k);
{x = -(4 + sqrt(15))^k/2 - (4 - sqrt(15))^k/2,
 y = -sqrt(15)*((4 + sqrt(15))^k - (4 - sqrt(15))^k)/30},
{x = -(4 + sqrt(15))^k/2 - (4 - sqrt(15))^k/2,
 y = sqrt(15)*((4 + sqrt(15))^k - (4 - sqrt(15))^k)/30},
{x = (4 + sqrt(15))^k/2 + (4 - sqrt(15))^k/2,
 y = -sqrt(15)*((4 + sqrt(15))^k - (4 - sqrt(15))^k)/30},
{x = (4 + sqrt(15))^k/2 + (4 - sqrt(15))^k/2,
 y = sqrt(15)*((4 + sqrt(15))^k - (4 - sqrt(15))^k)/30}
```

□

Για τον υπολογισμό ρητών λύσεων εξισώσεων δευτέρου βαθμού με δύο αγνώστους $f(x, y) = 0$ θα παραμετρικοποιήσουμε την $f(x, y)$ χρησιμοποιώντας την εντολή parametrization(f, x, y, t). Απαραίτητη προϋπόθεση είναι η $f(x, y)$ να είναι ανάγωγη και να έχουμε φορτώσει το πακέτο with(algcurves).

΄Ασκηση 9.26. *Να υπολογιστούν οι ρητές λύσεις των παρακάτω εξισώσεων:*
$\alpha)$ $x^2 + y^2 - 53 = 0$,
$\beta)$ $x^2 + x + 2y - 1 = 0$,
$\gamma)$ $x^2 + xy + y - 37 = 0$.

Απόδειξη. α) Για $f(x, y) = x^2 + y^2 - 53$ έχουμε

```
f := x^2 + y^2 - 53;
parametrization(f, x, y, t);
                              2    2
                        f := x  + y  - 53
                [    2                2           ]
                [-7 t  - 4 t + 7  -2 t  + 14 t + 2]
                [---------------, ----------------]
                [     2                 2         ]
                [    t  + 1            t  + 1     ]
```

β) Για $f(x, y) = x^2 + x + 2y - 1$ έχουμε

```
f := x^2 + x + 2*y - 1;
parametrization(f, x, y, t);
                          2
                    f := x  + x + 2 y - 1
                    [     1  2   1     1]
                    [t, - - t  - - t + -]
                    [     2      2     2]
```

γ) Για $f(x, y) = x^2 + xy + y - 37$ έχουμε

```
f := x^2 + xy + y - 37;
parametrization(f, x, y, t);
                          2
                    f := x  + xy + y - 37
                      [     2          ]
                      [t, -t  - xy + 37]
```

□

Βιβλιογραφία

[1] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[2] Gauss, F. (1801). Disquisitiones Arithmeticae. Leipzig: Gerh. Fleischer

[3] Heath, T.L. (1910). Diophantus of Alexandria: A Study in the History of Greek Algebra. Cambridge: University Press.

[4] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[5] Matijasevich, Yu.V. (1993). Hilbert's Tenth Problem. Cambridge, MA: MIT Press.

[6] Matijasevich, Yu.V. (1970). The Diophantineness of Enumerable Sets. Dokl. Akad. Nauk SSSR 191, p. 279–282. English translation: Soviet Math. Dokl 11, p. 354-358.

[7] Mordell, L. J. (1969). Diophantine Equations, Academic Press.

[8] Pambuccian, V. (2004). 11122. The American Mathematical Monthly, 111(10), 916-916.

[9] Ribenboim P. (1999). Fermat'As Last Theorem for Amateurs, Springer.

[10] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.

[11] Φερεντίνου-Νικολακοπούλου, Ι. (1984). Το Τελευταίο Θεώρημα του Fermat, Μέρος Πρώτο, Οργανισμός Εκδόσεων Διδακτικών Βιβλίων.

Κεφάλαιο 10

Συνεχή Κλάσματα

Η ιστορία των συνεχών κλασμάτων ξεκινάει με την ανακάλυψη των άρρητων αριθμών και την ανάγκη προσέγγισης τους με κάποιο κλάσμα. Ο όρος που χρησιμοποιήθηκε στην αρχή για την διαδικασία προσέγγισης ενός πραγματικού αριθμού είναι η «ανθυπαφαίρεση». Ο Fowler στο [3] αναφέρει ότι η ανθυπαφαίρεση παρείχε το πλαίσιο για την αρχική ανακάλυψη των μη-μετρήσιμων μεγεθών και το συνδέει με το πεντάγωνο των Πυθαγορείων. Η διαδικασία της ανθυπαφαίρεσης αναφέρεται ακόμα και στους Πλατωνικούς διαλόγους Θεαίτητο, Σοφιστή και Πολιτικό. Ειδικότερα ο Νεγρεπόντης στο [5] στοιχειοθετεί την άποψή του με τη βοήθεια των Πλατωνικών Διαλόγων και του 10ου βιβλίου των Στοιχείων του Ευκλείδη ότι ο Θεαίτητος γνώριζε την απόδειξη για το Θεώρημα της Παλινδρομικότητας της ανθυπαφαίρεσης άρρητων αριθμών, ένα από τα σημαντικότερα αποτελέσματα αυτού του κεφαλαίου. Ο πρώτος που χρησιμοποίησε τον όρο «συνεχές κλάσμα» ήταν ο Wallis [4].

Την σημαντικότητα των συνεχών κλασμάτων καταδεικνύουν οι αμέτρητες εργασίες μέσα στις οποίες εμφανίζονται αλλά και τα πολυάριθμα βιβλία που έχουν γραφτεί αποκλειστικά για αυτά. Το συνεχές κλάσμα εκτός από μία διαδικασία προσέγγισης ενός πραγματικού αριθμού είναι ένα πολύ καλό εργαλείο για την επίλυση προβλημάτων που σχετίζονται τόσο με θεωρητικά ζητήματα (π.χ. θεωρίας αριθμών, μιγαδικής ανάλυσης, δυναμικών συστημάτων κ.α.) όσο και με πιο πρακτικά θέματα (π.χ. ημερολόγια, μουσική, κ.α.). Στο [6] γίνεται αναφορά σε αρκετές εφαρμογών των συνεχών κλασμάτων.

10.1 Ανάπτυγμα Πραγματικού Αριθμού σε Συνεχές Κλάσμα

Ας είναι ρ ένας ρητός αριθμός. Τότε, υπάρχουν ακέραιοι a_0, a_1 με $a_1 > 0$ και $(a_0, a_1) = 1$ έτσι, ώστε να έχουμε $\rho = a_0/a_1$. Εφαρμόζοντας τον Ευκλείδειο αλγόριθμο στους ακεραίους a_0, a_1 προκύπτουν ζεύγη ακεραίων (q_i, a_{i+1}) $(i = 1, \ldots, n)$ τέτοια, ώστε να έχουμε:

$$a_{i-1} = a_i q_i + a_{i+1}, \quad 0 \leq a_{i+1} < a_i$$

και $a_n = 1$, $a_{n+1} = 0$. Έτσι, έχουμε τις σχέσεις:

$$\begin{aligned}
\frac{a_0}{a_1} &= q_1 + \frac{1}{a_1/a_2},\\
\frac{a_1}{a_2} &= q_2 + \frac{1}{a_2/a_3},\\
\cdots &\quad \cdots\\
\frac{a_{n-3}}{a_{n-2}} &= q_{n-2} + \frac{1}{a_{n-2}/a_{n-1}},\\
\frac{a_{n-2}}{a_{n-1}} &= q_{n-1} + \frac{1}{a_{n-1}},\\
a_{n-1} &= q_n.
\end{aligned}$$

Απαλοίφοντας τους ακέραιους $a_1, \ldots, a_{n-1}$, παίρνουμε:

$$\rho = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots \cfrac{}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Για συντομία, θα γράφουμε $\rho =< q_1, \ldots, q_n >$.

Ορισμός 10.1. Η παράσταση $\rho =< q_1, \ldots, q_n >$ καλείται *ανάπτυγμα του ρητού αριθμού ρ σε συνεχές κλάσμα*.

Παρατηρούμε ότι αν ο ρητός ρ δεν είναι ακέραιος, τότε $q_n = a_{n-1} \geq 2$. Θεωρούμε το σύνολο

$$S = \mathbb{Z} \cup \{(q_1, \ldots, q_n) \in \mathbb{Z}^n / \ n \geq 2,\ q_i > 0\ (i = 2, \ldots, n-1),\ q_n \geq 2\}.$$

Θεώρημα 10.1. *Η απεικόνιση*

$$\Theta : \mathbb{Q} \longrightarrow S,\ < q_1, \ldots, q_n > \longmapsto (q_1, \ldots, q_n)$$

είναι αμφίεση.

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Θεώρημα 1.1]. □

Στη συνέχεια υπενθυμίζουμε ότι αν a είναι ένας πραγματικός αριθμός, τότε συμβολίζουμε με $\lfloor a \rfloor$ τον μεγαλύτερο ακέραιο $\leq a$. Ας είναι τώρα θ ένας πραγματικός αριθμός. Θέτουμε $a_0 = \lfloor \theta \rfloor$. Αν $a_0 \neq \theta$, τότε γράφουμε $\theta = a_0 + 1/\theta_1$, όπου $\theta_1 > 1$. Θέτουμε $a_1 = \lfloor \theta_1 \rfloor$. Αν $a_1 \neq \theta_1$, τότε γράφουμε $\theta_1 = a_1 + 1/\theta_2$, όπου $\theta_2 > 1$. Η διαδικασία αυτή είναι δυνατόν να συνεχιστεί επ΄ άπειρο, εκτός και αν υπάρχει δείκτης n με $a_n = \lfloor \theta_n \rfloor$. Σ΄ αυτή την περίπτωση είναι προφανές ότι ο αριθμός θ είναι ρητός. Αντιστρόφως, αν ο αριθμός θ είναι ρητός, τότε η παραπάνω διαδικασία είναι η ανάπτυξη του θ σε συνεχές κλάσμα. Συνεπώς, ο αριθμός θ είναι άρρητος αν και μόνον αν για κάθε δείκτη n ισχύει $a_n \neq \lfloor \theta_n \rfloor$. Σ΄ αυτή την περίπτωση, η ακολουθία των ακεραίων $a_0, a_1, a_2, \ldots$ είναι άπειρη και γράφουμε $\theta =< a_0, a_1, a_2, \ldots >$.

Ορισμός 10.2. Η παράσταση $\theta =< a_0, a_1, a_2, \dots >$ καλείται *ανάπτυγμα του* θ *σε συνεχές κλάσμα*. Οι αριθμοί a_n και θ_n καλούνται *n-οστό μερικό πηλίκο* και *n-οστό πλήρες πηλίκο*, αντίστοιχα, του θ.

Από τα παραπάνω, για κάθε $n \geq 1$, ισχύει:

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{}{a_{n-1} + \cfrac{1}{\theta_n}}}}.$$

Ορισμός 10.3. Ο ρητός αριθμός $< a_0, a_1, \dots, a_n >$ καλείται *n-οστός συγκλίνων ρητός στο* θ.

Γράφουμε:

$$\frac{p_n}{q_n} =< a_0, a_1, \dots, a_n >,$$

όπου p_n, q_n είναι ακέραιοι πρώτοι μεταξύ τους και $q_n > 0$.

Πρόταση 10.1. *Ισχύουν τα εξής:*

α) $p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}, \quad n \geq 2,$
$p_1 = a_0 a_1 + 1, \quad q_1 = a_1, \quad p_0 = a_0, \quad q_0 = 1.$

β) $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}, \quad p_n q_{n+2} - p_{n+2} q_n = a_{n+2}$, *για κάθε* $n \in \mathbb{N}$.

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 1.1 και Πρόταση 1.2]. □

Πρόταση 10.2. *Για κάθε ακέραιο* $n \geq 1$ *ισχύει:*

$$\theta = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 1.3]. □

Πρόταση 10.3. *Ισχύει:*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \frac{p_{2k}}{q_{2k}} < \theta < \frac{p_{2k+1}}{q_{2k+1}} < \dots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

και

$$\left| \theta - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2}.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 1.4]. □

Πόρισμα 10.1. *Ας είναι* $\theta \in \mathbb{R} \setminus \mathbb{Q}$. *Τότε, ισχύει:*

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \theta.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πόρισμα 1.2]. □

Ας είναι A το σύνολο των ακολουθιών ακεραίων αριθμών $(a_n)_{n\in\mathbb{N}}$ με $a_n > 0$ για $n \geq 1$. Καθώς η ανάπτυξη ενός πραγματικού άρρητου αριθμού σε συνεχές κλάσμα δίνει ένα στοιχείο του A έχουμε την απεικόνιση

$$\Phi : \mathbb{R} \setminus \mathbb{Q} \longrightarrow A,\ \theta =< a_0, a_1, \ldots > \longmapsto (a_n)_{n\in\mathbb{N}}.$$

Θεώρημα 10.2. *Η απεικόνιση Φ είναι αμφίεση.*

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Θεώρημα 1.2]. □

Ασκήσεις

΄Ασκηση 10.1. *Να υπολογιστούν τα αναπτύγματα σε συνεχή κλάσματα των ρητών* $53/15$, $25/113$, $-157/16$ *και* $1145/233$.

Απόδειξη. Πρώτα παρατηρούμε ότι όλα τα παραπάνω κλάσματα είναι ανάγωγα. Θα υπολογίσουμε, με την χρήση του Ευκλείδειου αλγόριθμου, το ανάπτυγμα μόνο ενός ρητού (του αρνητικού) καθώς όλες οι άλλες περιπτώσεις είναι παρόμοιες. ΄Εχουμε:

$$\begin{aligned} -157 &= -10 \cdot 16 + 3, \\ 16 &= 5 \cdot 3 + 1, \\ 3 &= 3 \cdot 1. \end{aligned}$$

΄Ετσι, παίρνουμε:

$$\frac{-157}{16} =< -10, 5, 3 > .$$

Ομοίως, βρίσκουμε:

$$\frac{53}{15} =< 3, 1, 1, 7 >,\ \ \frac{25}{113} =< 0, 4, 1, 1, 12 >,\ \ \frac{1145}{223} =< 5, 7, 2, 3, 4 > .$$

□

΄Ασκηση 10.2. *Να υπολογιστούν τα έντεκα πρώτα μερικά πηλίκα των αριθμών* $\sqrt{2}$ *και* $\ln 5$.

Απόδειξη. Για τον αριθμό $\sqrt{2}$ έχουμε:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{1/(\sqrt{2} - 1)} = 1 + \frac{1}{\sqrt{2} + 1}$$

και

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

Από τα παραπάνω συνεπάγεται ότι τα μερικά πηλίκα του $\sqrt{2}$ είναι τα $1, 2, 2, 2, \ldots$ και κατά συνέπεια έχουμε $\sqrt{2} =< 1, 2, 2, 2 \ldots >$.

Θεωρούμε στη συνέχεια τον αριθμό $\ln 5$. Έχουμε:

$$\ln 5 = 1 + (\ln 5 - 1) = 1 + \frac{1}{1/(\ln 5 - 1)},$$

$$\frac{1}{\ln 5 - 1} = 1,64085623752 = 1 + \frac{1}{1/0,64085623752},$$

$$\frac{1}{0,64085623752} = 1,56041236935 = 1 + \frac{1}{1/0,56041236935},$$

$$\frac{1}{0,56041236935} = 1,78440030001 = 1 + \frac{1}{1/0,78440030001},$$

$$\frac{1}{0,78440030001} = 1,27485927783 = 1 + \frac{1}{1/0,27485927783},$$

$$\frac{1}{0,27485927783} = 3.63822537807 = 1 + \frac{1}{1/0,63822537807}.$$

Συνεχίζοντας με αυτόν τον τρόπο, βρίσκουμε ότι τα έντεκα πρώτα μερικά πηλίκα του $\ln 5$ είναι τα εξής: 1, 1, 1, 1, 1, 3, 1, 1, 1, 3, 4. Έτσι, προκύπτει $\ln 5 =< 1,1,1,1,1,3,1,1,1,3,4,\ldots >$. □

Άσκηση 10.3. *Να χρησιμοποιηθούν οι συγκλίνοντες ρητοί ώστε να υπολογιστεί ένας ρητός p/q τέτοιος, ώστε να ισχύει:*

$$\left| a - \frac{p}{q} \right| < 10^{-6},$$

όπου $a = \sqrt{2}, \ln 5$.

Απόδειξη. Ας είναι $a = \sqrt{2}$. Θα προσδιορίσουμε τους συγκλίνοντες ρητούς του $\sqrt{2} = 1,41421356237...$ μέχρι να βρούμε την επιθυμητή προσέγγιση. Από την Άσκηση 10.17 έχουμε ότι το συνεχές κλάσμα του $\sqrt{2}$ είναι:

$$\sqrt{2} =< 1,2,2,2,2,2,2,2,\ldots > .$$

Χρησιμοποιώντας στη συνέχεια την Πρόταση 10.1 παίρνουμε:

$$p_0 = 1, \quad p_1 = 1 \cdot 2 + 1 = 3, \quad p_2 = 2 \cdot 3 + 1 = 7, \quad p_3 = 2 \cdot 7 + 3 = 17,$$

$$p_4 = 2 \cdot 17 + 7 = 41, \quad p_5 = 2 \cdot 41 + 17 = 99, \quad p_6 = 2 \cdot 99 + 41 = 239,$$

$$p_7 = 2 \cdot 239 + 99 = 577, \quad p_8 = 2 \cdot 577 + 239 = 1393$$

και

$$q_0 = 1, \quad q_1 = 2, \quad q_2 = 2 \cdot 2 + 1 = 5, \quad q_3 = 2 \cdot 5 + 2 = 12,$$

$$q_4 = 2 \cdot 12 + 5 = 29, \quad q_5 = 2 \cdot 29 + 12 = 70, \quad q_6 = 2 \cdot 70 + 29 = 169,$$

$$q_7 = 2 \cdot 169 + 70 = 408, \quad q_8 = 2 \cdot 408 + 169 = 985.$$

Έτσι, βρίσκουμε τους παρακάτω συγκλίνοντες ρητούς του $\sqrt{2}$:

$$\frac{p_0}{q_0} = 1, \quad \frac{p_1}{q_1} = \frac{3}{2}, \quad \frac{p_2}{q_2} = \frac{7}{5}, \quad \frac{p_3}{q_3} = \frac{17}{12}, \quad \frac{p_4}{q_4} = \frac{41}{29},$$

$$\frac{p_5}{q_5} = \frac{99}{70}, \quad \frac{p_6}{q_6} = \frac{239}{169}, \quad \frac{p_7}{q_7} = \frac{577}{408}, \quad \frac{p_8}{q_8} = \frac{1393}{985}, \ldots$$

Υπολογίζοντας διαδοχικά τις τιμές $\sqrt{2} - p_i/q_i$ $(i = 0, \ldots, 8)$ βλέπουμε ότι ο ζητούμενος ρητός είναι ο $p_8/q_8 = 1393/985 = 1,41421319797$.

Ας είναι $a = \ln 5$. Όπως και στη προηγουμένη περίπτωση, θα προσδιορίσουμε τους συγκλίνοντες ρητούς στο $\ln 5 = 1,60943791243$. Σύμφωνα με την Άσκηση 10.17, το συνεχές κλάσμα του $\ln 5$ είναι:

$$\ln 5 =< 1, 1, 1, 1, 1, 3, 1, 1, 1, 3, 4, \ldots > .$$

Στη συνέχεια, υπολογίζουμε:

$$p_0 = 1, \quad p_1 = 1 \cdot 1 + 1 = 2, \quad p_2 = 1 \cdot 2 + 1 = 3, \quad p_3 = 1 \cdot 3 + 2 = 5,$$

$$p_4 = 1 \cdot 5 + 3 = 8, \quad p_5 = 3 \cdot 8 + 5 = 29, \quad p_6 = 1 \cdot 29 + 8 = 37,$$

$$p_7 = 1 \cdot 37 + 29 = 66, \quad p_8 = 1 \cdot 66 + 37 = 103,$$

$$p_9 = 3 \cdot 103 + 66 = 375, \quad p_{10} = 4 \cdot 375 + 103 = 1603$$

και

$$q_0 = 1, \quad q_1 = 1, \quad q_2 = 1 \cdot 1 + 1 = 2, \quad q_3 = 1 \cdot 2 + 1 = 3,$$

$$q_4 = 1 \cdot 3 + 2 = 5, \quad q_5 = 3 \cdot 5 + 3 = 18, \quad q_6 = 1 \cdot 18 + 5 = 23,$$

$$q_7 = 1 \cdot 23 + 18 = 41, \quad q_8 = 1 \cdot 41 + 23 = 64,$$

$$q_9 = 3 \cdot 64 + 41 = 233, \quad q_{10} = 4 \cdot 233 + 64 = 996.$$

Οπότε, έχουμε τους εξής συγκλίνοντες ρητούς στο $\ln 5$:

$$\frac{p_0}{q_0} = 1, \quad \frac{p_1}{q_1} = \frac{2}{1} = 2, \quad \frac{p_2}{q_2} = \frac{3}{2}, \quad \frac{p_3}{q_3} = \frac{5}{3}, \quad \frac{p_4}{q_4} = \frac{8}{5}, \quad \frac{p_5}{q_5} = \frac{29}{18},$$

$$\frac{p_6}{q_6} = \frac{37}{23}, \quad \frac{p_7}{q_7} = \frac{66}{41}, \quad \frac{p_8}{q_8} = \frac{103}{64}, \quad \frac{p_9}{q_9} = \frac{375}{233}, \quad \frac{p_{10}}{q_{10}} = \frac{1603}{996}.$$

Υπολογίζουμε διαδοχικά τις τιμές $\ln 5 - p_i/q_i$ $(i = 0, \ldots, 10)$ βλέπουμε ότι ο ζητούμενος ρητός είναι ο $p_{10}/q_{10} = 1603/996 = 1,609437751$. □

Άσκηση 10.4. *Ας υποθέσουμε ότι $\pi = 3,1415926\ldots$. Να υπολογιστεί ο μικρότερος δείκτης i τέτοιος, ώστε ο συγκλίνων ρητός p_i/q_i να ικανοποιεί την ανισότητα:*

$$\left|\pi - \frac{p_i}{q_i}\right| < 10^{-6}.$$

Απόδειξη. Έχουμε:

$$\pi = 3 + \frac{1}{1/0,1415926},$$

$$\frac{1}{0,1415926} = 7,0625159 = 7 + \frac{1}{1/0,0625159},$$

$$\frac{1}{0,0625159} = 15,9959306 = 15 + \frac{1}{1/0,9959306},$$

$$\frac{1}{0,9959306} = 1.0040860 = 1 + \frac{1}{1/0,0040860}.$$

Έτσι, παίρνουμε:

$$\pi =< 3, 7, 15, 1, \dots > .$$

Οπότε, οι τέσσερεις πρώτοι συγκλίνοντες ρητοί είναι:

$$\frac{p_0}{q_0} = 3, \quad \frac{p_1}{q_1} = \frac{3 \cdot 7 + 1}{7} = \frac{22}{7}, \quad \frac{p_2}{q_2} = \frac{15 \cdot 22 + 3}{15 \cdot 7 + 1} = \frac{333}{106}, \quad \frac{p_3}{q_3} = \frac{333 + 22}{106 + 7} = \frac{355}{113}.$$

Καθώς έχουμε

$$\frac{22}{7} = 3,14285714286, \quad \frac{333}{106} = 3,14150943396, \quad \frac{355}{113} = 3,14159292035,$$

βλέπουμε ότι μόνον για τον συγκλίνοντα ρητό $p_3/q_3 = 3,14159292035$ ισχύει:

$$\left|\pi - \frac{p_3}{q_3}\right| < 10^{-6}.$$

□

10.2 Προσέγγιση αρρήτου από τους συγκλίνοντες ρητούς

Ας είναι θ ένας άρρητος πραγματικός αριθμός και $(p_n/q_n)_{n\in\mathbb{N}}$ η ακολουθία των συγκλινόντων ρητών στο θ.

Πρόταση 10.4. *Για κάθε $n \in \mathbb{N}$, ένας τουλάχιστον από τους συγκλίνοντες ρητούς p_n/q_n και p_{n+1}/q_{n+1} ικανοποιεί την ανισότητα*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Επομένως, υπάρχει άπειρο πλήθος ρητών p/q, όπου p, q ακέραιοι πρώτοι μεταξύ τους έτσι, ώστε

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 2.1]. □

Πρόταση 10.5. *Για κάθε $n \in \mathbb{N}$, ένας τουλάχιστον από τους συγκλίνοντες ρητούς p_n/q_n, p_{n+1}/q_{n+1} και p_{n+2}/q_{n+2} ικανοποιεί την ανισότητα*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Επομένως, υπάρχει άπειρο πλήθος ρητών p/q, όπου p, q ακέραιοι πρώτοι μεταξύ τους έτσι, ώστε

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 2.2]. □

Πρόταση 10.6. *Για κάθε $n \geq 1$, ισχύει*

$$|q_n\theta - p_n| < |q_{n-1}\theta - p_{n-1}|.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 2.3]. □

Η παρακάτω πρόταση δείχνει ότι οι συγκλίνοντες ρητοί προσεγγίζουν τον θ καλύτερα από οποιονδήποτε άλλο ρητό.

Πρόταση 10.7. *Ας είναι p, q ακέραιοι με $0 < q < q_{n+1}$. Τότε, ισχύει:*

$$|q\theta - p| > |q_n\theta - p_n|.$$

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πρόταση 2.4]. □

Πόρισμα 10.2. *Ας είναι p/q ρητός τέτοιος, ώστε*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Τότε, υπάρχει φυσικός n έτσι, ώστε $p/q = p_n/q_n$.

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Πόρισμα 2.3]. □

Ασκήσεις

΄Ασκηση 10.5. *Ας είναι $A = (\sqrt{5}-1)/2$, $(P_n/Q_n)_{n\in\mathbb{N}}$ η ακολουθία συγκλινόντων ρητών στο A και m ακέραιος ≥ 1. Θέτουμε:*

$$C_m = \frac{\sqrt{5}+1}{2} + \frac{P_{2m-1}}{Q_{2m-1}}.$$

Επίσης, ας είναι $\alpha =< a_0, a_1, \ldots >$ ένας πραγματικός άρρητος αριθμός και $(p_n/q_n)_{n\in\mathbb{N}}$ η ακολουθία συγκλινόντων ρητών στο α. Για $n \geq 1$, ορίζουμε τον πραγματικό θετικό αριθμό λ_n από την ισότητα

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{\lambda_n q_n^2}.$$

α) *Να δειχθεί ότι* $\lambda_n =< a_{n+1}, a_{n+2}, \ldots > + < 0, a_n, \ldots, a_1 >$.
β) *Ισχύει η ανισότητα*

$$\sqrt{5} < C_m \leq \frac{\sqrt{5}+3}{2} < \frac{8}{3}.$$

γ) *Αν* p/q *ρητός με*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{C_m q^2},$$

τότε υπάρχει φυσικός n *τέτοιος, ώστε* $p/q = p_n/q_n$. *Επιπλέον, ο ρητός* p_n/q_n *επαληθεύει την προηγουμένη ανισότητα αν και μόνον αν ισχύει* $\lambda_n \geq C_m$.

δ) *Να δειχθεί ότι υπάρχουν ακριβώς* m *ρητοί* p/q (*όπου* p, q *ακέραιοι πρώτοι μεταξύ τους και* $q > 0$) *με*

$$\left|A - \frac{p}{q}\right| \leq \frac{1}{C_m q^2}.$$

Επιπλέον, αν $C > C_m$, *τότε να δειχθεί ότι υπάρχουν λιγότεροι από* m *ρητοί* p/q (*όπου* p, q *ακέραιοι πρώτοι μεταξύ τους και* $q > 0$) *με*

$$\left|A - \frac{p}{q}\right| \leq \frac{1}{Cq^2}.$$

ε) *Ας είναι* $\alpha \neq A$ *και* $0 < C \leq 3$. *Αν υπάρχει άπειρο πλήθος φυσικών* n *με* $a_n \geq 3$, *τότε υπάρχει άπειρο πλήθος ρητών* p/q (*όπου* p, q *ακέραιοι πρώτοι μεταξύ τους και* $q > 0$) *με*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Cq^2}.$$

στ) *Ας είναι* $\alpha \neq A$ *και* $0 < C \leq 8/3$. *Αν υπάρχει φυσικός* k *έτσι, ώστε για κάθε* $n \geq k$ *να ισχύει* $a_n \leq 2$ *και* $a_n = 2$ *για άπειρο πλήθος* n, *τότε υπάρχει άπειρο πλήθος ρητών* p/q (*όπου* p, q *ακέραιοι πρώτοι μεταξύ τους και* $q > 0$) *με*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Cq^2}.$$

ζ) *Ας υποθέσουμε ότι υπάρχει ακέραιος* $r \geq 2$ *έτσι, ώστε* $a_r > 1$ *και για κάθε* $n \geq r$ *να ισχύει* $a_n = 1$. *Να δειχθεί ότι αν*

$$\frac{p}{q} \in \left\{\frac{p_{r-1}}{q_{r-1}}, \frac{p_{r+1}}{q_{r+1}}, \ldots, \frac{p_{r+2m-3}}{q_{r+2m-3}}\right\},$$

τότε

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{C_m q^2}.$$

Απόδειξη. Θα συμβολίζουμε με α_n το n-οστό πλήρες πηλίκο του α. α) Χρησιμοποιώντας τις Προτάσεις 10.1(β) και 10.2 παίρνουμε:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(q_n\alpha_{n+1} + q_{n-1})}\right| = \frac{1}{q_n(q_n\alpha_{n+1} + q_{n-1})}.$$

Έτσι, προκύπτει:

$$\lambda_n = \alpha_{n+1} + \frac{q_{n-1}}{q_n}.$$

Χρησιμοποιώντας την Πρόταση 10.1(α) παίρνουμε:

$$\frac{q_{n-1}}{q_n} = 0 + \cfrac{1}{a_n + \cfrac{1}{a_{n-1} + \ddots + \cfrac{1}{a_2 + \cfrac{1}{a_1}}}}.$$

Επομένως, ισχύει:

$$\lambda_n = < a_{n+1}, a_{n+2}, \ldots > + < 0, a_n, \ldots, a_1 > .$$

β) Από την Πρόταση 10.3 έχουμε:

$$\frac{\sqrt{5}-1}{2} < \frac{P_{2m-1}}{Q_{2m-1}} < \ldots < \frac{P_1}{Q_1} = 1.$$

Επομένως, παίρνουμε:

$$\sqrt{5} = \frac{\sqrt{5}+1}{2} + \frac{\sqrt{5}-1}{2} < \frac{\sqrt{5}+1}{2} + \frac{P_{2m-1}}{Q_{2m-1}} = C_m \leq \frac{\sqrt{5}+1}{2} + \frac{P_1}{Q_1} = \frac{\sqrt{5}+3}{2} < \frac{8}{3}.$$

γ) Ας είναι p/q ρητός τέτοιος, ώστε

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{C_m q^2}.$$

Καθώς $C_m > 2$, από το Πόρισμα 10.2 έπεται ότι υπάρχει φυσικός n έτσι, ώστε $p/q = p_n/q_n$. Από τον ορισμό του λ_n συνεπάγεται αμέσως ο ρητός p_n/q_n επαληθεύει την παραπάνω ανισότητα αν και μόνον αν $\lambda_n \geq C_m$.

δ) Θα υπολογίσουμε πρώτα τα μερικά πηλίκα του A. Έχουμε:

$$\frac{\sqrt{5}-1}{2} = \frac{1}{2/(\sqrt{5}-1)} = \frac{1}{(\sqrt{5}+1)/2} = \frac{1}{1+(\sqrt{5}-1)/2}.$$

Έτσι, παίρνουμε:

$$\frac{\sqrt{5}-1}{2} = < 0, 1, 1, 1, \ldots > .$$

Επομένως, η ακολουθία των μερικών πηλίκων του A είναι: $0, 1, 1, 1, \ldots$. Έτσι, για $n \geq 1$, έχουμε:

$$\lambda_n = < 1, 1, \ldots > + < 0, \underbrace{1, \ldots, 1}_{n \text{ φορές}} > = \frac{\sqrt{5}+1}{2} + \frac{P_n}{Q_n}.$$

Επομένως, η ανισότητα $\lambda_n \geq C_m$ είναι ισοδύναμη με την

$$\frac{P_n}{Q_n} \geq \frac{P_{2m-1}}{Q_{2m-1}}.$$

Η ανισότητα αυτή ισχύει αν και μόνον αν $n \in \{1, 3, \ldots, 2k-1, \ldots, 2m-1\}$. Άρα, υπάρχουν ακριβώς m ρητοί αριθμοί p/q με

$$\left|A - \frac{p}{q}\right| \leq \frac{1}{C_m q^2}.$$

Επίσης, αν $C > C_m$, τότε υπάρχουν λιγότεροι από m ρητοί p/q

$$\left|A - \frac{p}{q}\right| \leq \frac{1}{Cq^2}.$$

ε) Αν $a_{n+1} \geq 3$, τότε από την (α) έχουμε ότι $\lambda_n > 3$. Έτσι, αν για άπειρο πλήθος φυσικών n ισχύει $a_{n+1} \geq 3$, τότε ισχύει $\lambda_n > 3$, για άπειρο πλήθος n, και επομένως ισχύει

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{Cq_n^2},$$

για άπειρο πλήθος n.

στ) Από το (α), για $n \geq 1$, έχουμε:

$$\lambda_n = a_{n+1} + \frac{1}{\alpha_{n+2}} + \frac{1}{< a_n, a_{n-1}, \ldots, a_1 >} > a_{n+1} + \frac{1}{a_{n+2}+1} + \frac{1}{\alpha_n + 1}.$$

Αν $a_n \leq 2$, $a_{n+1} = 2$, $a_{n+2} \leq 2$, τότε $\lambda_n > 8/3$. Καθώς υπάρχει άπειρο πλήθος n με την παραπάνω ιδιότητα, ισχύει

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{Cq_n^2},$$

για άπειρο πλήθος n.

ζ) Στην απόδειξη του (δ) δείξαμε ότι

$$\frac{\sqrt{5}-1}{2} =< 0, 1, 1, 1, \ldots > .$$

Έτσι, συνδυάζοντας αυτό το αποτέλεσμα με το (α), έχουμε:

$$\lambda_{r-1} >< a_r, 1, 1, \ldots >= a_r + \frac{1}{< 1, 1 \ldots >} = a_r + \frac{\sqrt{5}-1}{2} \geq \frac{\sqrt{5}+3}{2} \geq C_m.$$

Έτσι, από το (γ) προκύπτει:

$$\left|\alpha - \frac{p_{r-1}}{q_{r-1}}\right| \leq \frac{1}{C_m q^2}.$$

Καθώς $a_r \geq 2$ έχουμε:

$$< a_r, \ldots, a_1 > \geq a_r \geq 2 > < \underbrace{1, 1, \ldots, 1, 1}_{2m-n+r-1 \text{ φορές}} > .$$

Έτσι, αν ο ακέραιος $n-r$ είναι περιττός και $2m-3 \geq n-r$, τότε

$$< \underbrace{1,\ldots,1}_{n-r-\text{φορές}}, a_r, \ldots, a_1 > \leq < \underbrace{1,\ldots,1}_{2m-1-\text{φορές}} >,$$

απ΄ όπου

$$\lambda_n = < 1,1,\ldots > + < 0, \underbrace{1,\ldots,1}_{n-r-\text{φορές}}, a_r, \ldots, a_1 > \geq \frac{\sqrt{5}+1}{2} + < 0, \underbrace{1,\ldots,1}_{2m-1-\text{φορές}} >= C_m.$$

Επομένως, έχουμε:

$$\left|\alpha - \frac{p_{r-1+j}}{q_{r-1+j}}\right| \leq \frac{1}{C_m q^2} \ (j = 0,\ldots,m-1).$$

□

10.3 Τετραγωνικοί Άρρητοι

Ας είναι A το σύνολο που ορίσαμε στην Ενότητα 10.1.

Ορισμός 10.4. Μία ακολουθία $(a_n)_{n\in\mathbb{N}}$ του A καλείται *περιοδική*, αν υπάρχουν φυσικοί k και $m \geq 1$ τέτοιοι, ώστε να ισχύει $a_{m+n} = a_n$, για κάθε $n \geq k$. Αν οι φυσικοί k και m είναι οι μικρότεροι που έχουν αυτή την ιδιότητα, τότε ο φυσικός m καλείται *περίοδος* της ακολουθίας. Αν $k = 0$, τότε η ακολουθία $(a_n)_{n\in\mathbb{N}}$ καλείται *γνησίως περιοδική*.

Αν λοιπόν η ακολουθία $(a_n)_{n\in\mathbb{N}}$ είναι περιοδική με περίοδο m, τότε έχει την μορφή:

$$a_0,\ldots,a_{k-1},a_k,\ldots,a_{k+m-1},a_k,\ldots,a_{k+m-1},a_k,\ldots.$$

Ας είναι θ ο άρρητος πραγματικός αριθμός που αντιστοιχεί στην ακολουθία $(a_n)_{n\in\mathbb{N}}$. Τότε, γράφουμε:

$$\theta = < a_0,\ldots,a_{k-1},\overline{a_k,\ldots,a_{k+m-1}} > .$$

Ορισμός 10.5. Ένας πραγματικός άρρητος αριθμός ο οποίος είναι ρίζα μίας δευτεροβάθμιας εξίσωσης με ακέραιους συντελεστές καλείται *τετραγωνικός*.

Θεώρημα 10.3. *Ας είναι θ ένας πραγματικός άρρητος και $\theta = < a_0, a_1, \ldots >$ το ανάπτυγμά του σε συνεχές κλάσμα. Ο αριθμός θ είναι τετραγωνικός, αν και μόνον αν, η ακολουθία $(a_n)_{n\in\mathbb{N}}$ είναι περιοδική.*

Απόδειξη. Βλέπε [7, Κεφάλαιο 9, Θεώρημα 3.1]. □

Ας είναι θ ένας τετραγωνικός άρρητος. Τότε, ο θ είναι ρίζα μίας δευτεροβάθμιας εξίσωσης με ακέραιους συντελεστές. Η εξίσωση αυτή έχει και μία δεύτερη ρίζα διαφορετική από την θ που την συμβολίζουμε με $\bar{\theta}$.

Ορισμός 10.6. Ο άρρητος αριθμός $\bar{\theta}$ καλείται *συζυγής* του θ.

Πρόταση 10.8. *Ας είναι θ ένας τετραγωνικός άρρητος, $\theta =< a_0, a_1, \ldots >$ το ανάπτυγμά του σε συνεχές κλάσμα και $\bar{\theta}$ ο συζυγής του. Η ακολουθία $(a_n)_{n\in\mathbb{N}}$ είναι γνησίως περιοδική, αν και μόνον αν, ισχύει $\theta > 1$ και $-1 < \bar{\theta} < 0$.*

Πόρισμα 10.3. *Ας είναι d θετικός ακέραιος ο οποίος δεν είναι τέλειος τετράγωνο ακεραίου. Αν $\sqrt{d} + \lfloor \sqrt{d} \rfloor =< b_0, b_1, \ldots >$ και $1/(\sqrt{d} - \lfloor \sqrt{d} \rfloor) =< c_0, c_1, \ldots >$, τότε οι ακολουθίες $(b_n)_{n\in\mathbb{N}}$ και $(c_n)_{n\in\mathbb{N}}$ είναι γνησίως περιοδικές.*

Στη συνέχεια, θα δούμε τον αλγόριθμο μετατροπής ενός τετραγωνικού άρρητου σε συνεχές κλάσμα και το αντίστροφο.

Υπολογισμός Συνεχούς Κλάσματος Τετραγωνικού Άρρητου. Ας είναι $\theta > 0$ ένας τετραγωνικός άρρητος. Τα βήματα υπολογισμού του συνεχούς του κλάσματος έχουν ως εξής:

1) Υπολογίζουμε διαδοχικά τα

$$\begin{aligned}
\theta &= \lfloor \theta \rfloor + \theta_1, \\
\frac{1}{\theta_1} &= \left\lfloor \frac{1}{\theta_1} \right\rfloor + \theta_2, \\
\frac{1}{\theta_2} &= \left\lfloor \frac{1}{\theta_2} \right\rfloor + \theta_3, \\
&\vdots \qquad\quad \vdots \\
\frac{1}{\theta_{k-1}} &= \left\lfloor \frac{1}{\theta_{k-1}} \right\rfloor + \theta_k, \\
&\vdots \qquad\quad \vdots \\
\frac{1}{\theta_{n-1}} &= \left\lfloor \frac{1}{\theta_{n-1}} \right\rfloor + \theta_n,
\end{aligned}$$

μέχρι $\theta_k = \theta_n$.

2) Το συνεχές κλάσμα του θ είναι το

$$\theta =< \lfloor \theta \rfloor, \left\lfloor \frac{1}{\theta_1} \right\rfloor, \ldots, \left\lfloor \frac{1}{\theta_{k-1}} \right\rfloor, \overline{\left\lfloor \frac{1}{\theta_k} \right\rfloor, \ldots, \left\lfloor \frac{1}{\theta_{n-1}} \right\rfloor} > .$$

Μετατροπή Συνεχούς Κλάσματος σε Τετραγωνικό Άρρητο. Δίνεται το συνεχές κλάσμα $< a_0, \ldots, a_k, \overline{a_{k+1}, \ldots, a_n} >$ ενός τετραγωνικού άρρητου θ. Τα βήματα υπολογισμού του θ έχουν ως εξής:

1) Θέτουμε $y = < \overline{a_{k+1}, \ldots, a_n} >$.

2) Επιλύουμε την εξίσωση

$$y =< a_{k+1}, \ldots, a_n, y > .$$

3) Υπολογίζουμε το κλάσμα

$$< a_0, \ldots, a_k, y_1 >,$$

όπου y_1 είναι η μοναδική θετική ρίζα της εξίσωσης που βρέθηκε στο βήμα 2. Το αποτέλεσμα του υπολογισμού είναι ο ζητούμενος αριθμός θ.

Ας σημειωθεί ότι το συνεχές κλάσμα του y είναι πλήρως περιοδικό και επομένως από την Πρόταση 10.8 έχουμε ότι η εξίσωση στο βήμα 2 θα έχει ακριβώς μία θετική ρίζα. Στις ασκήσεις που ακολουθούν θα εφαρμόσουμε τους παραπάνω αλγόριθμους.

Ασκήσεις

΄Ασκηση 10.6. *Να υπολογιστούν τα αναπτύγματα σε συνεχή κλάσματα των αρρήτων* $\sqrt{3}$, $(1+\sqrt{3})/3$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{10}$, $(1+\sqrt{5})/3$ *και* $\sqrt{43}$.

Απόδειξη. ΄Εχουμε:

$$\sqrt{3} = 1 + (\sqrt{3} - 1),$$
$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = 1 + \left(\frac{\sqrt{3}+1}{2} - 1\right) = 1 + \frac{\sqrt{3}-1}{2},$$
$$\frac{2}{\sqrt{3}-1} = \sqrt{3}+1 = 2 + (\sqrt{3}-1).$$

΄Αρα, παίρνουμε:

$$\sqrt{3} =< 1, \overline{1,2} > .$$

Ομοίως, υπολογίζουμε:

$$\frac{\sqrt{3}+1}{3} = 0 + \frac{\sqrt{3}+1}{3},$$
$$\frac{3}{\sqrt{3}+1} = \frac{3(\sqrt{3}-1)}{2} = 1 + \left(\frac{3(\sqrt{3}-1)}{2} - 1\right) = 1 + \frac{3\sqrt{3}-5}{2},$$
$$\frac{2}{3\sqrt{3}-5} = 3\sqrt{3}+5 = 10 + (3\sqrt{3}-5),$$
$$\frac{1}{3\sqrt{3}-5} = \frac{3\sqrt{3}+5}{2} = 5 + \left(\frac{3\sqrt{3}+5}{2} - 5\right) = 5 + \frac{3\sqrt{3}-5}{2}.$$

΄Αρα, ισχύει:

$$\frac{\sqrt{3}+1}{3} =< 0, 1, \overline{10,5} > .$$

Επίσης, έχουμε:

$$\sqrt{43} = 6 + (\sqrt{43} - 6),$$
$$\frac{1}{\sqrt{43}-6} = \frac{\sqrt{43}+6}{7} = 1 + \frac{\sqrt{43}-1}{7},$$
$$\frac{7}{\sqrt{43}-1} = \frac{\sqrt{43}+1}{6} = 1 + \frac{\sqrt{43}-5}{6},$$
$$\frac{6}{\sqrt{43}-5} = \frac{\sqrt{43}+5}{3} = 3 + \frac{\sqrt{43}-4}{3},$$

$$\frac{3}{\sqrt{43}-4} = \frac{\sqrt{43}+4}{9} = 1 + \frac{\sqrt{43}-5}{9},$$
$$\frac{9}{\sqrt{43}-5} = \frac{\sqrt{43}+5}{2} = 5 + \frac{\sqrt{43}-5}{2}, \ldots$$

Συνεχίζοντας έτσι παίρνουμε:

$$\sqrt{43} =< 6, \overline{1,1,3,1,5,1,3,1,1,12} > .$$

Ομοίως παίρνουμε:

$$\sqrt{5} =< 2, \overline{4} >, \quad \sqrt{6} =< 2, \overline{2,4} >, \quad \sqrt{7} =< 2, \overline{1,1,1,4} >,$$
$$\sqrt{8} =< 2, \overline{1,4} >, \quad \sqrt{10} =< 3, \overline{6} >, \quad \frac{1+\sqrt{5}}{3} =< 1, \overline{12,1,2,2,2,1} > .$$

□

Άσκηση 10.7. *Να υπολογιστούν οι αριθμοί* $\theta =< \overline{1} >$ *και* $\eta =< 1,2,3,\overline{1,4} >$.

Απόδειξη. Ας είναι $\theta =< \overline{1} >$. Τότε, έχουμε:

$$\theta = 1 + \frac{1}{\theta}.$$

Άρα, ο θ είναι λύση της εξίσωσης

$$\theta^2 - \theta - 1 = 0.$$

Έτσι, καθώς $\theta > 0$, παίρνουμε:

$$\theta = \frac{1+\sqrt{5}}{2}.$$

Δηλαδή, ο αριθμός $< \overline{1} >$ είναι η «χρυσή τομή φ».

Για τον υπολογισμό του η θα ακολουθήσουμε τα βήματα αλγόριθμου μετατροπής συνεχούς κλάσματος σε τετραγωνικού άρρητου. Ας είναι $y =< \overline{1,4} >$. Θα λύσουμε την εξίσωση $y =< 1,4,y >$. Έχουμε

$$y = 1 + \frac{1}{4 + \frac{1}{y}},$$

απ' όπου προκύπτει την εξίσωση

$$4y^2 - 4y - 1 = 0.$$

Καθώς, $y > 0$ παίρνουμε:

$$y = \frac{1+\sqrt{2}}{2}.$$

Άρα, ο ζητούμενος αριθμός είναι:

$$\eta =< 1,2,3, \frac{1+\sqrt{2}}{2} >= \frac{36-\sqrt{8}}{23}.$$

□

΄Ασκηση 10.8. *΄Εστω $n \in \mathbb{Z}^+$. Να δειχθούν οι ισότητες:*

$$\sqrt{n^2+1} =< n, \overline{2n} >, \quad \sqrt{n^2-1} =< n-1, \overline{1, 2n-2} > .$$

Απόδειξη. Θέτουμε:

$$x = n + \cfrac{1}{2n + \cfrac{1}{2n + \cdots}}.$$

Προσθέτοντας τον ακέραιο n σε κάθε μέλος προκύπτει:

$$x + n = 2n + \cfrac{1}{2n + \cfrac{1}{2n + \cdots}}.$$

Οπότε, αντικαθιστώντας το κομμάτι που επαναλαμβάνεται έχουμε:

$$x + n = 2n + \frac{1}{x+n}.$$

΄Ετσι, προκύπτει η εξίσωση:

$$x^2 - n^2 - 1 = 0.$$

Οπότε, καθώς $x > 0$, παίρνουμε:

$$x = \sqrt{n^2+1}.$$

Ομοίως θέτουμε:

$$x = n - 1 + \cfrac{1}{1 + \cfrac{1}{2n - 2 + \cfrac{1}{1 + \cdots}}}.$$

Προσθέτοντας τον ακέραιο $n-1$ σε κάθε μέλος, προκύπτει:

$$x + n - 1 = 2n - 2 + \cfrac{1}{1 + \cfrac{1}{2n - 2 + \cfrac{1}{1 + \cdots}}}.$$

Αντικαθιστώντας το κομμάτι που επαναλαμβάνεται, έχουμε:

$$x + n - 1 = 2n - 2 + \cfrac{1}{1 + \cfrac{1}{x + n - 1}}.$$

΄Ετσι, παίρνουμε την εξίσωση:

$$x^2 - n^2 + 1 = 0.$$

Επομένως, καθώς $x > 0$, ο ζητούμενος αριθμός είναι:

$$x = \sqrt{n^2 - 1}.$$

□

Άσκηση 10.9. *Ας είναι α ένας τετραγωνικός ακέραιος του οποίου το ανάπτυγμα σε συνεχές κλάσμα έχει περίοδο s. Ας είναι p_n/q_n $(n = 0, 1, \ldots)$ η ακολουθία των συγκλινόντων ρητών στο α. Θέτουμε $V_n = (p_n, q_n)$ $(n = 0, 1, \ldots)$. Να δειχθεί ότι υπάρχουν ακέραιος n_0 και πίνακας $A \in M_2(\mathbb{Z})$ με $\det A = (-1)^s$, ώστε ο ακέραιος μετασχηματισμός μ_A να ικανοποιεί τις σχέσεις:*

$$V_{n+s} = \mu_A(V_n), \quad \text{για } n \geq n_0.$$

Απόδειξη. Ας υποθέσουμε ότι $\alpha =< a_0, \ldots, a_{n_0-1}, \overline{a_{n_0}, \ldots, a_{n_0+s-1}} >$. Θεωρούμε τα γραμμικά συστήματα:

$$p_{n_0+s} = ap_{n_0} + bq_{n_0}, \quad p_{n_0+s+1} = ap_{n_0+1} + bq_{n_0+1}$$

και

$$q_{n_0+s} = cp_{n_0} + dq_{n_0}, \quad p_{n_0+s+1} = cp_{n_0+1} + dq_{n_0+1},$$

με αγνώστους τους a, b και c, d, αντίστοιχα. Από την Πρόταση 10.1(β) έχουμε ότι η ορίζουσα καθενός από τα δύο συστήματα είναι:

$$p_{n_0}q_{n_0+1} - p_{n_0+1}q_{n_0} = (-1)^{n_0+1}.$$

Επομένως, τα δύο συστήματα έχουν ακέραιες λύσεις (a, b) και (c, d), αντίστοιχα.

Συμβολίζουμε με A τον πίνακα με πρώτη και δεύτερη γραμμή τα ζεύγη (a, b) και (c, d), αντίστοιχα. Έτσι, προκύπτει ο ακέραιος μετασχηματισμός μ_A, για τον οποίον θα δείξουμε, χρησιμοποιώντας επαγωγή επί του n, ότι ισχύει:

$$V_{n+s} = \mu_A(V_n), \quad \forall n \geq n_0.$$

Για $n = n_0, n_0 + 1$, από τον ορισμό των a, b, c, d, έχουμε:

$$V_{n_0+s} = \mu_A(V_{n_0}) \quad \text{και} \quad V_{n_0+s+1} = \mu_A(V_{n_0+1}).$$

Ας υποθέσουμε ότι η προς απόδειξη ισότητα ισχύει για $n = n_0 + 2, \ldots, k$. Έχουμε:

$$\mu_A(V_{k+1}) = \mu_A(a_{k+1}V_k + V_{k-1}) = a_{k+1}\mu_A(V_k) + \mu_A(V_{k-1}).$$

Χρησιμοποιώντας την υπόθεση επαγωγής και την περιοδικότητα της ακολουθίας (a_n), παίρνουμε:

$$\mu_A(V_{k+1}) = a_{k+1+s}V_{k+s} + V_{k-1+s} = V_{k+1+s}.$$

Άρα, η προς απόδειξη σχέση ισχύει.

Ας είναι $n \geq n_0$. Από τις ισότητες $V_{n+1+s} = \mu_A(V_{n+1})$ και $V_{n+s} = \mu_A(V_n)$ έχουμε:

$$\begin{pmatrix} p_{n+1+s} & q_{n+1+s} \\ p_{n+s} & q_{n+s} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_{n+1} & q_{n+1} \\ p_n & q_n \end{pmatrix}.$$

Παίρνοντας τις ορίζουσες και των δύο μερών της ισότητας, προκύπτει:

$$p_{n+1+s}q_{n+s} - p_{n+s}q_{n+1+s} = \det A\,(p_{n+1}q_n - p_nq_{n+1}).$$

Τέλος, από την Πρόταση 10.1(β), έχουμε:

$$p_{n+1+s}q_{n+s} - p_{n+s}q_{n+1+s} = (-1)^{s+n} \quad \text{και} \quad p_{n+1}q_n - p_nq_{n+1} = (-1)^n.$$

Συνδυάζοντας τις παραπάνω ισότητες, προκύπτει:

$$\det A = (-1)^s.$$

□

΄Ασκηση 10.10. *Ας είναι n ένας θετικός ακέραιος ο οποίος δεν είναι τετράγωνο ακεραίου και P_k/Q_k $(k = 0, 1, \ldots)$ οι συγκλίνοντες ρητοί στο $\sqrt{n}$. Να δειχθεί ότι ισχύει:*

$$|P_k^2 - nQ_k^2| < 2\sqrt{n}.$$

Απόδειξη. Χρησιμοποιώντας την Πρόταση 10.3 παίρνουμε:

$$\begin{aligned} |P_k^2 - nQ_k^2| &= Q_k^2\left|\sqrt{n} - \frac{P_k}{Q_k}\right|\left|\sqrt{n} + \frac{P_k}{Q_k}\right|, \\ &\le Q_k^2\left|\sqrt{n} - \frac{P_k}{Q_k}\right|\left(2\sqrt{n} + \left|\sqrt{n} - \frac{P_k}{Q_k}\right|\right), \\ &< Q_k^2\left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right|\left(2\sqrt{n} + \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right|\right). \end{aligned}$$

Στη συνέχεια, από την Πρόταση 10.1(β) έχουμε

$$P_kQ_{k+1} - P_{k+1}Q_k = (-1)^{k+1}.$$

Οπότε, παίρνουμε:

$$|P_k^2 - nQ_k^2| < \frac{Q_k}{Q_{k+1}}\left(2\sqrt{n} + \frac{1}{Q_kQ_{k+1}}\right).$$

Επομένως, έχουμε:

$$\begin{aligned} |P_k^2 - nQ_k^2| - 2\sqrt{n} &< 2\sqrt{n}\left(-1 + \frac{Q_k}{Q_{k+1}} + \frac{1}{2\sqrt{n}\,Q_{k+1}^2}\right), \\ &< 2\sqrt{n}\left(-1 + \frac{Q_k}{Q_{k+1}} + \frac{1}{Q_{k+1}}\right), \\ &< 2\sqrt{n}\left(-1 + \frac{Q_{k+1}}{Q_{k+1}}\right) = 0. \end{aligned}$$

Συνεπώς, ισχύει $|P_k^2 - nQ_k^2| < 2\sqrt{n}$. □

10.4 Εφαρμογή στην εξίσωση $x^2 - dy^2 = 1$

Ας είναι d ένας ακέραιος > 1 ο οποίος δεν είναι τέλειο τετράγωνο. Σ΄ αυτή την ενότητα θα δείξουμε πως βρίσκεται η βασική λύση της εξίσωσης

$$x^2 - dy^2 = 1 \tag{10.1}$$

με την χρήση των συνεχών κλασμάτων. Σύμφωνα με το Πόρισμα 10.3, έχουμε $\sqrt{d} =< a_0, \overline{a_1, \ldots, a_m} >$. Ας είναι p_n/q_n $(n = 0, 1, \ldots)$ (όπου p_n, q_n ακέραιοι πρώτοι μεταξύ τους και $q_n > 0$) οι συγκλίνοντες ρητοί στο $\sqrt{d}$ και Λ το σύνολο των λύσεων (x, y) της (10.1) με $x > 0$, $y > 0$.

Θεώρημα 10.4. *Αν m είναι άρτιος, τότε $\Lambda = \{(p_{lm-1}, q_{lm-1})/\ l = 1, 2, 3, \ldots\}$ και αν ο m είναι περιττός, τότε $\Lambda = \{(p_{lm-1}, q_{lm-1})/\ l = 2, 4, 6, \ldots\}$.*

Απόδειξη. Βλέπε [7, Θεώρημα 4.1]. □

Πόρισμα 10.4. *Η βασική λύση της (10.1) είναι το ζεύγος (p_{m-1}, q_{m-1}), αν ο m είναι άρτιος και (p_{2m-1}, q_{2m-1}), αν ο m είναι περιττός.*

Υπολογισμός Λύσεων της εξίσωσης (10.1). Τα βήματα υπολογισμού των λύσεων της εξίσωσης (10.1) έχουν ως εξής:

1) Υπολογίζουμε το συνεχές κλάσμα του $\sqrt{d}$,
$$\sqrt{d} =< a_0, \overline{a_1, \ldots, a_m} > .$$
2) Αν ο m είναι περιττός τότε η βασική λύση της εξίσωσης είναι το ζεύγος (p_{2m-1}, q_{2m-1}), ενώ αν m άρτιος, τότε η βασική λύση της εξίσωσης είναι το ζεύγος (p_{m-1}, q_{m-1}).
3) Αν (x_0, y_0) η βασική λύση, τότε το σύνολο τον λύσεων της εξίσωσης (10.1) δίνεται από την σχέση:
$$x + y\sqrt{d} = \pm(x_0 \pm y_0\sqrt{d})^n,$$
όπου $n \in \mathbb{Z}$.

Ασκήσεις

΄Ασκηση 10.11. *Να επιλυθούν οι παρακάτω εξισώσεις:*

$$x^2 - 29y^2 = 1, \quad x^2 - 59y^2 = 1, \quad x^2 - 97y^2 = 1.$$

Απόδειξη. Θα εφαρμόσουμε την παραπάνω διαδικασία. Συμβολίζουμε με p_n/q_n $(n = 0, 1, \ldots)$ τους συγκλίνοντες ρητούς στο $\sqrt{d}$. Υπολογίζουμε το συνεχές κλάσμα του $\sqrt{29}$. Έχουμε:

$$\sqrt{29} =< 5, \overline{2, 1, 1, 2, 10} > .$$

Η περίοδος του συνεχούς κλάσματος είναι 5. Τότε, η βασική λύση της εξίσωσης $x^2 - 29y^2 = 1$ είναι το ζεύγος (p_9, q_9). Υπολογίζουμε τους συγκλίνοντες ρητούς στο

$\sqrt{29}$ και βρίσκουμε $p_9/q_9 = 9801/1820$. Άρα, η ζητούμενη βασική λύση είναι το ζεύγος $(9801, 1820)$ και επομένως οι λύσεις της εξίσωσης δίνονται από την σχέση

$$\pm(9801 + 1820\sqrt{29})^n, \quad n \in \mathbb{Z}.$$

Στη συνέχεια, υπολογίζουμε το συνεχές κλάσμα του $\sqrt{59}$. Έχουμε:

$$\sqrt{59} =< 7, \overline{1, 2, 7, 2, 1, 14} > .$$

Η περίοδος του συνεχούς κλάσματος είναι 6 και επομένως η βασική λύση της εξίσωσης $x^2 - 59y^2 = 1$ είναι το ζεύγος (p_5, q_5). Υπολογίζουμε τους συγκλίνοντες ρητούς στο $\sqrt{59}$ και βρίσκουμε $p_5/q_5 = 530/69$. Άρα, η ζητούμενη βασική λύση είναι το ζεύγος $(530, 69)$ και επομένως οι λύσεις της εξίσωσης δίνονται από την σχέση

$$\pm(530 + 69\sqrt{59})^n, \quad n \in \mathbb{Z}.$$

Τέλος, το συνεχές κλάσμα του $\sqrt{97}$ είναι:

$$\sqrt{97} =< 9, \overline{1, 5, 1, 1, 1, 1, 1, 5, 1, 18} > .$$

Η περίοδος του συνεχούς κλάσματος είναι 11 και επομένως η βασική λύση της εξίσωσης $x^2 - 97y^2 = 1$ είναι το ζεύγος (p_{21}, q_{21}). Υπολογίζουμε τους συγκλίνοντες ρητούς στο $\sqrt{97}$ και βρίσκουμε $p_{21}/q_{21} = 62809633/6377352$. Επομένως, η βασική λύση της εξίσωσης είναι το ζεύγος $(62809633, 6377352)$ και επομένως οι λύσεις της εξίσωσης δίνονται από την σχέση

$$\pm(62809633 + 6377352\sqrt{97})^n, \quad n \in \mathbb{Z}.$$

□

Άσκηση 10.12. *Να δείξετε ότι αν ο αριθμός $s = 2 + 2\sqrt{1 + 28t^2}$ είναι ακέραιος για κάποιο $t \in \mathbb{N}$, τότε ο s είναι τέλειο τετράγωνο.*

Απόδειξη. Ας υποθέσουμε ότι ο αριθμός s είναι ακέραιος. Τότε, υπάρχει θετικός ακέραιος u τέτοιος, ώστε $u^2 = 1 + 28t^2$. Έτσι, $s = 2 + 2u$ και επομένως ο ακέραιος s είναι άρτιος. Έχουμε:

$$\frac{s}{2} - 1 = \sqrt{1 + 28t^2}.$$

Οπότε, ισχύει:

$$\left(\frac{s}{2} - 1\right)^2 - 28t^2 = 1.$$

Άρα, το ζεύγος $(s/2 - 1, t)$ είναι μία ακέραια λύση της εξίσωσης

$$x^2 - 28y^2 = 1.$$

Θα υπολογίσουμε τις λύσης αυτής της εξίσωσης. Το συνεχές κλάσμα του $\sqrt{28}$ είναι:

$$\sqrt{28} =< 5, \overline{3, 2, 3, 10} > .$$

Έχουμε $m = 4$ και επομένως η βασική λύση της εξίσωσης, σύμφωνα με το Πόρισμα 10.4, δίνεται από τον συγκλίνοντα ρητό $p_3/q_3 = 127/24$. Επομένως, η βασική λύση της εξίσωσης είναι το ζεύγος $(127, 24)$ και κατά συνέπεια όλες οι λύσεις της εξίσωσης δίνονται από την σχέση:

$$x + y\sqrt{28} = \pm(127 + 24\sqrt{28})^n, \quad \forall n \in \mathbb{Z}.$$

Επομένως, υπάρχει $k > 0$ έτσι, ώστε να ισχύει:

$$\frac{s}{2} - 1 + t\sqrt{28} = (127 + 24\sqrt{28})^k.$$

Έτσι, έχουμε:

$$\frac{s}{2} - 1 = \frac{(127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k}{2},$$

απ΄ όπου προκύπτει:

$$s = 2 + (127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k.$$

Τέλος, παρατηρούμε ότι ισχύει:

$$((8 + 3\sqrt{7})^k + (8 - 3\sqrt{7})^k)^2 = 2 + (127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k.$$

Συνεπώς, ο ακέραιος s είναι τέλειο τετράγωνο. □

10.5 Συνδυαστικές Ασκήσεις

΄Ασκηση 10.13. *Ας είναι d θετικός ακέραιος ο οποίος δεν είναι τέλειο τετράγωνο και N ακέραιος με $|N| < \sqrt{d}$. Αν u, v είναι θετικοί ακέραιοι με $u^2 - dv^2 = N$, τότε να δειχθεί ότι το κλάσμα u/v είναι ένας συγκλίνων ρητός στο $\sqrt{d}$.*

Απόδειξη. Ας υποθέσουμε πρώτα ότι $N > 0$. Τότε, έχουμε:

$$0 < u - v\sqrt{d} = \frac{N}{u + v\sqrt{d}} < \frac{\sqrt{d}}{u + v\sqrt{d}} = \frac{1}{u/\sqrt{d} + v} = \frac{1}{v((u/v\sqrt{d}) + 1)}.$$

Καθώς $u/v > \sqrt{d}$, παίρνουμε:

$$\left|\sqrt{d} - \frac{u}{v}\right| < \frac{1}{2v^2}.$$

Έτσι, από το Πόρισμα 10.2, συμπεραίνουμε ότι ο ρητός u/v είναι ένας συγκλίνων ρητός στο $\sqrt{d}$.

Στη συνέχεια, ας υποθέσουμε ότι $N < 0$. Τότε, έχουμε

$$v^2 - \frac{u^2}{d} = \frac{-N}{d},$$

απ΄ όπου παίρνουμε:

$$0 < v - \frac{u}{\sqrt{d}} = \frac{-N/d}{v + (u/\sqrt{d})} < \frac{1}{v\sqrt{d} + u} = \frac{1}{u(1 + (v\sqrt{d}/u))}.$$

Καθώς έχουμε $1 < v\sqrt{d}/u$, προκύπτει:

$$\left| \frac{1}{\sqrt{d}} - \frac{v}{u} \right| < \frac{1}{2u^2}.$$

Σύμφωνα με το Πόρισμα 10.2, έχουμε ότι το κλάσμα v/u είναι ένας συγκλίνων ρητός στο $1/\sqrt{d}$.

Ας είναι $\sqrt{d} =< a_0, a_1, \ldots >$ και p_n/q_n $(n = 0, 1, \ldots)$ είναι οι συγκλίνοντες ρητοί στο $\sqrt{d}$. Τότε, έχουμε $1/\sqrt{d} =< 0, a_0, a_1, \ldots >$ και επομένως οι συγκλίνοντες ρητοί στο $1/\sqrt{d}$ δίνονται από την ακολουθία $0, q_0/p_0, q_1/p_1, \ldots$, δηλαδή είναι το 0 και οι αντίστροφοι των συγκλινόντων ρητών στο $\sqrt{d}$. ΄Αρα, το κλάσμα u/v είναι ένας συγκλίνων ρητός στο $\sqrt{d}$. □

΄Ασκηση 10.14. *Να προσδιοριστούν οι τιμές του n για τις οποίες το άθροισμα*

$$\sum_{k=1}^{n} k^5$$

είναι ένα τέλειο τετράγωνο.

Απόδειξη. Από την ΄Ασκηση έχουμε:

$$\sum_{k=1}^{n} k^5 = \frac{1}{12} n^2 (n+1)^2 (2n^2 + 2n - 1).$$

΄Ενας από τους ακέραιους n, $n+1$ είναι άρτιος και επομένως $4 \mid n(n+1)$. ΄Ετσι, το παραπάνω άθροισμα είναι τέλειο τετράγωνο αν και μόνον αν υπάρχει ακέραιος m ώστε να ισχύει

$$3m^2 = 2n^2 + 2n - 1.$$

Πολλαπλασιάζοντας τα δύο μέλη με 2, παίρνουμε:

$$(2n+1)^2 - 6m^2 = 3.$$

Οπότε, $3 \mid 2n+1$ και επομένως υπάρχει ακέραιος N με $2n + 1 = 3N$. ΄Αρα, έχουμε:

$$3N^2 - 2m^2 = 1,$$

απ΄ όπου, πολλαπλασιάζοντας και τα δύο μέλη με 2, προκύπτει:

$$(2m)^2 - 6N^2 = -2.$$

Στη συνέχεια θα επιλύσουμε την εξίσωση

$$x^2 - 6y^2 = -2.$$

Αν (u, v) είναι μία ακέραια λύση αυτής της εξίσωσης με $u > 0$, $v > 0$, τότε, από την Άσκηση 10.13, έπεται ότι το κλάσμα u/v είναι ένας συγκλίνων ρητός στο $\sqrt{6}$. Στην Άσκηση 10.16 δείξαμε ότι ισχύει $\sqrt{6} =< 2, \overline{2,4} >$. Συμβολίζουμε με θ_n το n-οστό πλήρες πηλίκο και p_n/q_n τον n-οστό συγκλίνοντα ρητό στο $\sqrt{6}$. Τότε έχουμε

$$\sqrt{6} = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_n + q_{n-1}},$$

απ΄ όπου παίρνουμε

$$\begin{aligned}
\theta_{n+1} &= \frac{q_{n-1}\sqrt{6} - p_{n-1}}{p_n - q_n\sqrt{6}} \\
&= \frac{(q_{n-1}\sqrt{6} - p_{n-1})(p_n + q_n\sqrt{6})}{p_n^2 - \sqrt{6}q_n^2} \\
&= \frac{(p_nq_{n-1} - q_np_{n-1})\sqrt{6} + q_nq_{n-1} - p_{n-1}p_n}{p_n^2 - \sqrt{6}\,q_n^2} \\
&= \frac{\sqrt{6} + (-1)^{n+1}(q_nq_{n-1}d - p_np_{n-1})}{(-1)^{n+1}(p_n^2 - \sqrt{6}\,q_n^2)}.
\end{aligned}$$

Η ακολουθία των πλήρων πηλίκων θ_n είναι γνησίως περιοδική με περίοδο 2 και επομένως η ακολουθία $p_n^2 - \sqrt{6}\,q_n^2$ $(n = 0, 1, \ldots)$ είναι επίσης περιοδική. Έχουμε $p_0/q_0 = 2$, $p_1/q_1 = 5/2$ και παίρνουμε $p_0^2 - 6q_0^2 = -2$, $p_1^2 - 6q_1^2 = 1$. Το ζεύγος $(2, 1)$ είναι λύση της εξίσωσης και επομένως όλες οι λύσεις της εξίσωσωσης δίνονται από τους συγκλίνοντες ρητούς p_{2k}/q_{2k} $(k = 0, 1, \ldots)$. Συνεπώς, έχουμε:

$$n = \frac{3N - 1}{2} = \frac{3q_{2k} - 1}{2} \quad (k = 0, 1, \ldots).$$

□

10.6 Θεωρία Αριθμών με Maple

Το Maple διαθέτει αρκετά εργαλεία για τον υπολογισμό συνεχών κλασμάτων. Παρακάτω παραθέτουμε υπολογιστικές ασκήσεις του κεφαλαίου που επιλύονται άμεσα με εντολές του Maple. Φυσικά, όπως στις περισσότερες περιπτώσεις που έχουμε δει θα χρειαστεί πρώτα η φόρτωση του πακέτου with(NumberTheory).

Με την εντολή ContinuedFraction το Maple μας επιστρέφει το ανάπτυγμα του πραγματικού αριθμού σε σύνθετο κλάσμα ενώ με την εντολή Term μας επιστρέφει τον πραγματικό αριθμό στην μορφή είδαμε στον Ορισμό 10.1.

Άσκηση 10.15. *Να υπολογιστούν τα αναπτύγματα σε συνεχή κλάσματα των ρητών* $53/15$, $25/113$, $-157/16$ *και* $1145/233$.

Απόδειξη. Με κώδικα Maple:

```
ContinuedFraction(53/15);
                                  1
                        3 + -------------
                                    1
                             1 + ---------
                                      1
                                  1 + -----
                                      7 + 0
Term(ContinuedFraction(53/15), all);
                            [3, 1, 1, 7]
```

Ομοίως και οι υπόλοιποι ρητοί.

```
Term(ContinuedFraction(25/113), all);
                          [0, 4, 1, 1, 12]
Term(ContinuedFraction(-157/16), all);
                            [-10, 5, 3]
Term(ContinuedFraction(1145/233), all);
                       [4, 1, 10, 1, 1, 1, 6]
```

□

Η εντολή Term(ContinuedFraction(x), all) την χρησιμοποιούμε όταν το συνεχές κλάσμα είναι περπερασμένο ενώ όταν είναι περιοδικό χρησιμοποιούμε το Term(ContinuedFraction(x), periodic) όπου το Maple μας επιστρέφει δύο λίστες. Η πρώτη αφορά το μέρος του συνεχούς κλάσματος που δεν επαναλαμβάνεται ενώ το η δεύτερη λίστα είναι το περιοδικό μέρος του συνεχούς κλάσματος. Στην περίπτωση των περιοδικών κλασμάτων η εντολή ContinuedFraction μας δίνει από προεπιλογή τους δέκα πρώτους όρους του συνεχούς κλάσματος.

΄Ασκηση 10.16. *Να υπολογιστούν τα αναπτύγματα σε συνεχή κλάσματα των αρρήτων* $\sqrt{3}$*,* $(1+\sqrt{3})/3$*,* $\sqrt{5}$*,* $\sqrt{6}$*,* $\sqrt{7}$*,* $\sqrt{8}$*,* $\sqrt{10}$*,* $(1+\sqrt{5})/3$ *και* $\sqrt{43}$*.*

Απόδειξη. Με κώδικα Maple:

```
ContinuedFraction(sqrt(3));
                                    1
          1 + ---------------------------------------
                                  1
              1 + -----------------------------------
                                1
                  2 + -------------------------------
                              1
                      1 + ---------------------------
                                  1
                          2 + -----------------------
                                    1
                              1 + -------------------
                                        1
                                  1 + ---------------
                                            1
                                      1 + -----------
                                                1
```

```
                                  2 + --------------------
                                                  1
                                      1 + ----------------
                                                    1
                                          2 + ------------
                                                  1 + ...
Term(ContinuedFraction(sqrt(3)), periodic);
                          [[1], [1, 2]]
```

Ομοίως και οι υπόλοιποι άρρητοι.

```
Term(ContinuedFraction((1 + sqrt(3))/3), periodic);
                        [[0, 1], [10, 5]]
Term(ContinuedFraction(sqrt(5)), periodic);
                           [[2], [4]]
Term(ContinuedFraction(sqrt(6)), periodic);
                           [[2], [2, 4]]
Term(ContinuedFraction(sqrt(7)), periodic);
                        [[2], [1, 1, 1, 4]]
Term(ContinuedFraction(sqrt(8)), periodic);
                           [[2], [1, 4]]
Term(ContinuedFraction(sqrt(10)), periodic);
                             [[3], [6]]
Term(ContinuedFraction((1 + sqrt(5))/3), periodic);
                     [[], [1, 12, 1, 2, 2, 2]]
Term(ContinuedFraction(sqrt(43)), periodic);
              [[6], [1, 1, 3, 1, 5, 1, 3, 1, 1, 12]]
```

□

Η εντολή Term(ContinuedFraction(sqrt(2)), n) μας δίνει το n-οστό μερικό πηλίκο ενώ υπάρχει και η δυνατότητα να μας επιστραφεί τα μερικά πηλίκα από x εώς y.

΄Ασκηση 10.17. *Να υπολογιστούν τα έντεκα πρώτα μερικά πηλίκα των αριθμών* $\sqrt{2}$ *και* $\ln 5$.

Απόδειξη. Με κώδικα Maple:

```
Term(ContinuedFraction(sqrt(2)), 0 .. 10);
               [1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2]
Term(ContinuedFraction(ln(5)), 0 .. 10);
               [1, 1, 1, 1, 1, 3, 1, 1, 1, 3, 4, 6]
```

□

Επίσης, μπορούμε να υπολογίσουμε τους συγκλίνοντες αριθμούς ενός συνεχούς κλάσματος και έτσι μπορούμε να λύσουμε ασκήσεις όπως την επόμενη.

΄Ασκηση 10.18. *Να χρησιμοποιηθούν οι συγκλίνοντες ρητοί ώστε να υπολογιστεί ένας ρητός p/q τέτοιος, ώστε να ισχύει:*

$$\left| a - \frac{p}{q} \right| < 10^{-6},$$

όπου ο $a = \sqrt{2}, \ln 5$.

Απόδειξη. Με κώδικα Maple:

```
Convergent(ContinuedFraction(sqrt(2)), 0 .. 11);
    [   3  7  17  41  99  239  577  1393  3363  8119  19601]
    [1, -, -, --, --, --, ---, ---, ----, ----, ----, -----]
    [   2  5  12  29  70  169  408  985   2378  5741  13860]
Convergent(ContinuedFraction(ln(5)), 0 .. 11);
       [      3  5  8  29  37  66  103  375  1603  9993]
       [1, 2, -, -, -, --, --, --, ---, ---, ----, ----]
       [      2  3  5  18  23  41  64   233  996   6209]
```

Από όπου μπορούμε να εκμαιεύσουμε το αποτέλεσμα. □

Βιβλιογραφία

[1] Baker, A. (1984) A Concise Introduction to the Theory of Numbers, Cambridge University Press.

[2] Leveque, W. J. (1977). Fundamentals of Number Theory, Addison-Wesley Publishing Compagny.

[3] Fowler, D.H. (1979). Ratio in early Greek mathematics. Bull. Amer. Math. Soc. 1(6), p. 807–846

[4] Havil, J. (2003). Gamma: Exploring Euler's Constant. Princeton, NJ: Princeton University Press.

[5] Sialaros, M. (2018). Revolutions and Continuity in Greek Mathematics. Science, Technology, and Medicine in Ancient Cultures Series 8. Berlin: De Gruyter.

[6] Waldschmidt, M. (2017). Continued Fractions: Introduction and Applications. PROCEEDINGS OF THE ROMAN NUMBER THEORY ASSOCIATION Vol. 2(1), p. 61–8.

[7] Πουλάκης, Δ. (1997). Θεωρία Αριθμών. Θεσσαλονίκη: Εκδόσεις Ζήτη.