Υπολογιστική Θεωρία Αριθμών

Δημήτριος Πουλάκης

Καθηγητής Τμήματος Μαθηματικών
Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης

Υπολογιστική Θεωρία Αριθμών

Υπολογιστική Θεωρία Αριθμών

Συγγραφή

Δημήτριος Πουλάκης

Κριτικός αναγνώστης

Νικόλαος Τζανάκης

Συντελεστές έκδοσης

Τεχνική Επεξεργασία: Αναστάσιος Καρακώστας

ISBN: 978-960-603-127-4

ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ

Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφουwww.kallipos.gr

Στην πολυαγαπημένη μου σύζυγο

Πετρούλα

Περιεχόμενα

Πρόλογος

Την τελευταία τριακονταετία η Θεωρία Αριθμών έχει χρησιμοποιηθεί ως βασικό εργαλείο για την ανάπτυξη σημαντικών εφαρμογών σε πολλούς επιστομονικούς τομείς όπως η Κρυπτογραφία, η Θεωρία Κωδίκων, οι Ψηφιακές Επικοινωνίες, η Φυσική κλπ. Σκοπός του παρόντος συγγράμματος είναι να δώσει μία εισαγωγή στη Θεωρία Αριθμών με έμφαση στους αλγόριθμους, η οποία να παρέχει τις απαραίτητες βασικές γνώσεις για την κατανόηση των σύγχρονων εφαρμογών της. Οι γνώσεις που απαιτούνται για την μελέτη του είναι αυτές της δευτεροβάθμιας εκπαίδευσης. Έτσι, το κείμενο αυτό είναι προσιτό όχι μόνο από φοιτητές μαθηματικών τμημάτων, αλλά και τμημάτων Πληροφορικής και Πολυτεχνειών Σχολών, καθώς και από οποιονδήποτε ενδιαφέρεται για την Θεωρία Αριθμών και ιδιαίτερα τον υπολογιστικό της χαρακτήρα.

Το βιβλίο αυτό περιλαμβάνει οκτώ κεφάλαια. Στο πρώτο κεφάλαιο μελετάται η διαιρετότητα των ακεραίων, δίνεται μία στοιχειώδη εισαγωγή στους αλγόριθμους ακεραίων και αναλύεται ο εκτεταμένος Ευκλείδειος αλγόριθμος. Το δεύτερο κεφάλαιο είναι αφιερωμένο στο ανάπτυγμα των πραγματικών αριθμών σε συνεχές κλάσμα και στις βασικές του ιδιότητες. Στο τρίτο κεφάλαιο εισάγονται οι πρώτοι αριθμοί. Αποδεικνύεται το θεμελειώδες θεώρημα της αριθμητικής, δίνονται εφαρμογές του, μελετώνται κλασσικά θεωρήματα επί της κατανομής των πρώτων αριθμών και εξετάζονται ειδικές κατηγορίες πρώτων. Μία παρουσίαση των βασικών αλγεβρικών δομών του μονοειδούς, της ομάδας, του δακτυλίου και σώματος, καθώς επίσης και των βασικών ιδιοτήτων των πολυωνύμων δίνεται στο τέταρτο κεφάλαιο. Το πέμπτο κεφάλαιο είναι αφιερωμένο στη σχέση ισοτιμίας των ακεραίων αριθμών. Δίνονται οι βασικές ιδιότητες των ισοτιμίων, μελετάται η επίλυση των γραμμικών ισοτιμιών και των συστημάτων τους. Αποδεικνύεται σε ποιες περιπτώσεις υπάρχουν πρωτογενείς ρίζες κατά μέτρο n, εισάγονται τα σύμβολα των Legendre και Jacobi και μελετάται η επίλυση των τετραγωνικών

ισοτιμιών. Τέλος, δίνεται η κατασκευή των πεπερασμένων σωμάτων και οι βασικές τους ιδιότητες. Στο έκτο κεφάλαιο δίνονται μερικοί κλασσικοί μέθοδοι που χρησιμοποιούνται για να διαπιστωθεί εάν ένας ακέραιος είναι πρώτος, καθώς και ο μοναδικός αιτιοκρατικός αλγόριθμος πολυωνυμικού χρόνου AKS. Το έβδομο κεφάλαιο διαπραγματεύεται το θέμα της παραγοντοποίησης ακεραίων και περιγράφονται αλγόριθμοι για την αντιμετώπισή του. Τέλος, το όγδοο κεφάλαιο είναι αφιερωμένο στο πρόβλημα του διακριτού λογαρίθμου και δίνονται μερικοί αλγόριθμοι για την επίλυσή του.

Θα χρησιμοποιούμε τα συνήθη σύμβολα της Θεωρίας Συνολων: $\in$, $\subseteq$, $\subset$, $\emptyset$, $\cap$ 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. Αν X είναι ένα πεπερασμένο σύνολο που έχει πεπερασμένο πλήθος στοιχείων, τότε θα συμβολίζουμε με $|X|$ το πλήθος των στοιχείων του. Τέλος, με $\mathbb{N}$ θα συμβολίζεται το σύνολο των φυσικών αριθμών $\{0, 1, 2, \ldots\}$, με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών $\{\ldots, -1, 0, 1, \ldots\}$ και με $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ τα σύνολα των ρητών, πραγματικών αριθμών και μιγαδικών αριθμών, αντίστοιχα.

Θα ήθελα να ευχαριστήσω θερμά τον συναδελφο και φίλο καθηγητή του Τμήματος Μαθηματικών του Πανεπιστημίου Κρήτης, Νικόλαο Τζανάκη, ο οποίος, ως κριτικός αναγνώστης αυτού του βιβλίου, έκανε εύστοχες παρατηρήσεις οι οποίες βοήθησαν στη βελτίωσή του.

Θεσσαλονίκη 2015 Δημήτριος Πουλάκης

Κεφάλαιο 1

Ακέραιοι Αριθμοί

Σύνοψη
Σ′ αυτό το κεφάλαιο θα εξετάσουμε τις βασικές έννοιες της αριθμητικής των ακεραίων αριθμών, καθώς και τον χρόνον εκτέλεσης των στοιχειωδών πράξεών τους, τον μέγιστο κοινό διαιρέτη, το ελάχιστο κοινό πολλαπλάσιο, τον εκτεταμένο Ευκλείδειο αλγόριθμο και τις γραμμικές Διοφαντικές εξισώσεις. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να ανατρέξει στις εξής πηγές: [1, 2, 3, 4, 9, 10, 11].

Προαπαιτούμενη γνώση
Μαθηματικά Λυκείου

1.1 Ευκλείδεια Διαίρεση

Ας είναι $a, b \in \mathbb{Z}$. Λέμε ότι ο a *διαιρεί* τον b και γράφουμε $a|b$ αν υπάρχει $c \in \mathbb{Z}$ έτσι, ώστε $b = ac$. Σ′ αυτή την περίπτωση ο a καλείται *διαιρέτης* του b και ο b *πολλαπλάσιο* του a. Αν ο a δεν διαιρεί τον b, τότε γράφουμε $a \nmid b$. Για παράδειγμα, $4|20$, $7|21$, $3 \nmid 10$. Παρατηρούμε αμέσως ότι αν $0|b$, τότε $b = 0$ και για κάθε $a \in \mathbb{Z}$ ισχύει $a|a$ και $a|0$. Επίσης, για κάθε $a, b \in \mathbb{Z}$ ισχύουν τα εξης:

$$a|b \iff -a|b \iff a|-b \iff -a|-b.$$

Έτσι, για να εξετάσουμε αν $a|b$ αρκεί να το κάνουμε για τις απόλυτες τιμές τους. Μερικές βασικές ιδιότητες δίνονται στην παρακάτω πρόταση:

Πρόταση 1.1 *Ας είναι $a, b, c \in \mathbb{Z}$. Τότε ισχύουν τα εξής:*
(α) Αν $a|b$ και $b|c$, τότε $a|c$.
(β) Αν $a|b$ και $c|d$, τότε $ac|bd$.
(γ) Αν $a|b$ και $a|c$, τότε $a|bx + cy$, για κάθε $x, y \in \mathbb{Z}$.
(δ) Αν $a|b$ και $b \neq 0$, τότε $|a| \leq |b|$.
(ε) Αν $a|b$ και $b|a$, τότε $|a| = |b|$.

Απόδειξη. (α) Καθώς $a|b$ και $b|c$, υπάρχουν ακέραιοι k και l τέτοιοι, ώστε $b = ak$ και $c = bl$. Επομένως $c = akl$ και κατά συνέπεια $a|c$.

(β) Από τις σχέσεις $a|b$ και $b|d$ έπεται ότι υπάρχουν ακέραιοι k και l τέτοιοι, ώστε $b = ka$ και $d = cl$. Οπότε, έχουμε $bd = ackl$ και επομένως $ac|bd$.

Η απόδειξη των υπολοίπων ιδιοτήτων αφήνεται ως άσκηση. □

Παράδειγμα 1.1 Θα προσδιορίσουμε όλους τους ακέραιους a με την ιδιότητα $a + 1|a^2 + 1$. Ας είναι a ένας τέτοιος ακέραιος. Αν $a = -1$, τότε $a^2 + 1 = 0$ που είναι άτοπο. Άρα $a \neq -1$. Η σχέση $a + 1|a^2 + 1$ γράφεται $a + 1|(a + 1)^2 - 2a$, απ΄ όπου έπεται $a + 1|2a$. Έτσι, έχουμε $a + 1|2(a + 1) - 2a$ και, επομένως $a + 1|2$. Άρα, $a \in \{0, 1, -2, -3\}$. Από την άλλη πλευρά, όλοι οι ακέραιοι $0, 1, -2, -3$ έχουν την επιθυμητή ιδιότητα και κατά συνέπεια είναι οι ζητούμενοι ακέραιοι.

Παράδειγμα 1.2 Θα δείξουμε ότι για κάθε ζεύγος θετικών ακεραίων a και b ισχύει $a!b!|(a + b)!$. Για $a = 1$ ή $b = 1$ προφανώς ισχύει. Υποθέτουμε ότι για $a + b = n$ ισχύει. Ας είναι $a + b = n + 1$ με $a > 1$ και $b > 1$. Καθώς $(a - 1) + b = n$ και $a + (b - 1) = n$, έχουμε:

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

αντίστοιχα. Οπότε, ο $a!b!$ 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 $a!b!|(a + b)!$.

Από την παραπάνω σχέση έπεται ότι $b!|(a + 1) \cdots (a + b)$, δηλαδή, το γινόμενο b διαδοχικών θετικών ακεραίων διαιρείται από το $b!$.

Αν $x \in \mathbb{R}$, τότε θα συμβολίζουμε με $\lfloor x \rfloor$ τον μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος του x. Άρα $x = \lfloor x \rfloor + \epsilon$, όπου $\epsilon \in \mathbb{R}$ με $0 \leq \epsilon < 1$. Ο ακέραιος $\lfloor x \rfloor$ καλείται *κάτω ακέραιο μέρος* του x. Ένα από τα πλέον σημαντικά θεωρήματα της Θεωρίας Αριθμών είναι το παρακάτω:

Θεώρημα 1.1 *Αν είναι $a, b \in \mathbb{Z}$ με $b \neq 0$. Τότε υπάρχει μοναδικό ζεύγος $(q, r) \in \mathbb{Z}^2$ τέτοιο, ώστε:*

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

Απόδειξη. Ας υποθέσουμε πρώτα ότι $b > 0$. Αν $q = \lfloor a/b \rfloor$, τότε $0 \leq a/b - q < 1$ και επομένως ο ακέραιος $r = a - bq$ ικανοποιεί την ανισότητα $0 \leq r < b$. Άρα, το ζεύγος (q, r) έχει τις επιθυμητές ιδιότητες. Αν τώρα οι ακέραιοι u, v είναι τέτοιοι, ώστε να έχουμε

$$a = bu + v \quad \text{και} \quad 0 \leq v < b,$$

τότε $0 \leq v/b < 1$ και επομένως $u = \lfloor a/b \rfloor = q$. Οπότε, ισχύει:

$$r = aq - b = au - b = v.$$

Συνεπώς, το ζεύγος (q, r) είναι μοναδικό. Τέλος, αν $b < 0$, τότε εφαρμόζοντας τα παραπάνω για τους ακέραιους a και $|b|$, παίρνουμε το αποτέλεσμα. □

Ο ακέραιος q καλείται *πηλίκο* της διαίρεσης του a δια b και ο r *υπόλοιπο*. Οι σχέσεις του Θεωρήματος 1.1 καλούνται *Ευκλείδεια διαίρεση*.

Σύμφωνα με το Θεώρημα 1.1, για κάθε ακέραιο a υπάρχει μοναδικό ζεύγος ακεραίων (q, r) έτσι, ώστε $a = 2q + r$ και $r = 0$ ή 1. Αν $r = 0$, τότε $a = 2q$ και ο ακέραιος a καλείται *άρτιος*. Αν $r = 1$, τότε $a = 2q+1$ και ο a καλείται *περιττός*.

Παράδειγμα 1.3 Θα προσδιορίσουμε όλους τους θετικούς ακέραιους x οι οποίοι διαιρούμενοι με τον 157 δίνουν πηλίκο a και υπόλοιπο a^3. Τότε, έχουμε:

$$x = 157a + a^3 \quad \text{και} \quad 0 \leq a^3 < 157.$$

Έτσι, προκύπτει $a = 0, 1, 2, 3, 4, 5$ και επομένως παίρνουμε, αντίστοιχα, $x = 0, 158, 322, 498, 692, 910$.

Μία σημαντική εφαρμογή της Ευκλείδειας διαίρεσης είναι το εξής θεώρημα:

Θεώρημα 1.2 *Ας είναι g ένας ακέραιος > 1. Για κάθε φυσικό αριθμό a υπάρχει μοναδικός θετικός ακέραιος k και μοναδικά ορισμένοι ακέραιοι $a_1, \ldots, a_k \in \{0, \ldots, g-1\}$ με $a_1 \neq 0$ έτσι, ώστε να ισχύει:*

$$a = a_1 g^{k-1} + \cdots + a_k.$$

Επίσης, έχουμε $k = \lfloor \log_g a \rfloor + 1$ και

$$a_i = \lfloor (a - \sum_{j=1}^{i-1} a_j g^{k-j}) / g^{k-i} \rfloor \quad (i = 1, \ldots, k).$$

Απόδειξη. Πρώτα θ′ αποδείξουμε την ύπαρξη της k-άδας $(a_1, \ldots, a_k)$ εφαρμόζοντας τη μέθοδο της επαγωγής επί του a. Για $a = 0$ είναι τετριμμένο. Ας υποθέσουμε ότι η προς απόδειξη πρόταση ισχύει για κάθε θετικό ακέραιο $c < a$. Αν $a \leq g-1$, τότε $k = 1$ και $a = a_1$. Επίσης, αν $a = g$, τότε $k = 2$, $a_1 = 1$ και $a_2 = 0$. Ας είναι λοιπόν $a > g$. Τότε υπάρχουν ακέραιοι q, r, με $a = qg + r$ και $0 \leq r < g$. Από την υπόθεση της επαγωγής έπεται ότι υπάρχουν ακέραιοι $c_1, \ldots, c_l$ με $0 \leq c_i \leq g-1$ έτσι, ώστε $q = c_1 g^{l-1} + \cdots + c_l$. Οπότε, έχουμε:

$$a = c_1 g^l + \cdots + c_l g + r.$$

Ας υποθέσουμε τώρα ότι $a = a_1 g^{k-1} + \cdots + a_k$. Τότε:

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

Επομένως $k - 1 \leq \log_g a < k$, απ′ όπου $k = \lfloor \log_g a \rfloor + 1$.

Στη συνέχεια, εφαρμόζοντας επαγωγή επί του k θ′ αποδείξουμε την μοναδικότητα της k-άδας $(a_1, \ldots, a_k)$. Για $k = 1$ έχουμε $a = a_1$ και επομένως δεν υπάρχει άλλη επιλογή για τον a_1. Ας υποθέσουμε ότι η προς απόδειξη πρόταση ισχύει για κάθε θετικό ακέραιο $< k$ και ας είναι $a = a_1 g^{k-1} + \cdots + a_k$. Τότε:

$$0 \leq a - a_1 g^{k-1} \leq (g-1)(g^{k-2} + \cdots + 1) < g^{k-1}.$$

Ο ακέραιος a_1 είναι το πηλίκο της διαίρεσης του a με τον g^{k-1} και συνεπώς είναι μονοσήμαντα ορισμένος. Έτσι, εφαρμόζοντας την υπόθεση της επαγωγής, στη σχέση

$$a - a_1 g^{k-1} = a_2 g^{k-2} + \cdots + a_k$$

έπεται ότι οι ακέραιοι $a_2, \ldots, a_k$ είναι μονοσήμαντα ορισμένοι.

Τέλος, για $i = 1, \ldots, k$, έχουμε:

$$\left(a - \sum_{j=1}^{i-1} a_j g^{k-j} \right) \Big/ g^{k-i} = a_i + \sum_{j=i+1}^{k} a_j / g^{j-i}.$$

Καθώς ισχύει

$$\sum_{j=i+1}^{k} a_j / g^{j-i} \leq (g-1) \sum_{j=i+1}^{k} 1/g^{j-i} \leq (g^{k-i} - 1)/g^{k-i} < 1,$$

παίρνουμε:

$$a_i = \lfloor (a - \sum_{j=1}^{i-1} a_j g^{k-j})/g^{k-i} \rfloor \quad (i = 1, \ldots, k). \quad \square$$

Η γραφή του φυσικού a,

$$a = a_1 g^{k-1} + \cdots + a_k,$$

με $0 \leq a_i \leq g-1$ $(i = 1, \ldots, k)$, καλείται *παράσταση του a στην κλίμακα του g* ή *g-αδική παράσταση του a*. Συμβολίζεται συνήθως, με $a = (a_1 \ldots a_k)_g$. Ο ακέραιος g καλείται *βάση* της κλίμακας. Οι ακέραιοι $a_1, \ldots, a_k$ καλούνται *g-αδικά ψηφία* του a. Αν δεν υπάρχει αμφιβολία σχετικά με ποια βάση χρησιμοποιείται, τότε συμβολίζουμε πιο απλά με $a_1 \ldots a_k$ την παράσταση του a στην κλίμακα του g. Γενικότερα, μπορούμε να παραστήσουμε στην κλίμακα του g έναν ακέραιο a γράφοντας $a = (e, a_1 \ldots a_k)_g$, όπου e είναι ένα δυαδικό ψηφίο που δηλώνει το πρόσημο του a και $a_1, \ldots, a_k$ τα ψηφία του $|a|$ στην κλίμακα του g.

Η συνηθισμένη γραφή των ακεραίων χρησιμοποιεί την παράστασή τους στην κλίμακα του 10. Για παράδειγμα, $381 = 3 \cdot 10^2 + 8 \cdot 10 + 1$. Αν $g > 10$, τότε συνήθως χρησιμοποιούνται γράμματα για να εκφράσουν τα ψηφία που είναι > 9. Για παράδειγμα στη 16-αδική παράσταση των ακεραίων αντί των ψηφίων 10, 11, 12, 13, 14, 15 χρησιμοποιούνται τα γράμματα A, B, Γ, Δ, E, Z. Έτσι, A1E είναι η 16-αδική παράσταση του $2590 = 10 \cdot 16^2 + 16 + 14$. Τέλος, ας σημειωθεί ότι οι Υλεκτρονικοί Υπολογιστές χρησιμοποιούν τη δυαδική γραφή των αριθμών για την αναπαράσταση αριθμητικών δεδομένων, καθώς τα ψηφία 0 και 1

αντιστοιχούν σε τάσεις του ρεύματος μικρότερες ή μεγαλύτερες μίας συγκεκριμένης τιμής.

Το προηγούμενο θεώρημα δίνει μία διαδικασία για τον υπολογισμό της g-αδικής παράστασης ενός ακεραίου. Αυτή εφαρμόζεται στο παρακάτω παράδειγμα:

Παράδειγμα 1.4 Θα υπολογίσουμε τη δυαδική παράσταση του 173. Έχουμε $2^7 < 173 < 2^8$. Τα δυαδικά ψηφία του 173 είναι:

$$\begin{aligned}
a_1 &= \lfloor 173/2^7 \rfloor = 1, \\
a_2 &= \lfloor (173 - 2^7)/2^6 \rfloor = 0, \\
a_3 &= \lfloor (173 - 2^7)/2^5 \rfloor = 1, \\
a_4 &= \lfloor (173 - 2^7 - 2^5)/2^4 \rfloor = 0, \\
a_5 &= \lfloor (173 - 2^7 - 2^5)/2^3 \rfloor = 1, \\
a_6 &= \lfloor (173 - 2^7 - 2^5 - 2^3)/2^2 \rfloor = 1, \\
a_7 &= \lfloor (173 - 2^7 - 2^5 - 2^3 - 2^2)/2 \rfloor = 0, \\
a_8 &= 173 - 2^7 - 2^5 - 2^3 - 2^2 = 1.
\end{aligned}$$

Επομένως $173 = (10101101)_2$.

Ας είναι $a = (a_1 \dots a_k)_2$ και $b = (b_1 \dots b_l)_2$ δύο θετικοί ακέραιοι. Θα χρησιμοποιήσουμε τη δυαδική τους παράσταση για να τους συγκρίνουμε. Ας είναι $k \neq l$. Τότε αν $k > l$ έχουμε αμέσως $a > b$, ενώ διαφορετικά $a < b$. Αν $k = l$, τότε $a_1 = b_1 = 1$. Σ′ αυτή την περίπτωση ακολουθούμε την παρακάτω διαδικασία:

Για $i = 2, \dots, k$ κάνουμε τα εξής:

1. Αν $a_i = 1$ και $b_i = 0$, τότε συμπεραίνουμε $a > b$.
2. Αν $a_i = 0$ και $b_i = 1$, τότε συμπεραίνουμε $a < b$.
3. Αν $a_i = b_i$, τότε κοιτάμε τα ψηφία a_{i+1} και b_{i+1}.

Αν για κάθε $i = 2, \dots, k$ έχουμε $a_i = b_i$, τότε προφανώς $a = b$.

Η αιτιολόγηση της ορθότητας της διαδικασίας είναι απλή. Ας υποθέσουμε ότι έχουμε $a_j = b_j$ $(j = 1, \dots, m-1)$ $a_m = 1$ και $b_m = 0$. Τότε έχουμε:

$$2^{k-1} + a_2 2^{k-2} + \cdots + a_{m-1} 2^{k-m+1} = 2^{k-1} + b_2 2^{k-2} + \cdots + b_{m-1} 2^{k-m+1}$$

και

$$2^{k-m} + a_{m+1}2^{k-m-1} + \cdots + a_k \geq 2^{k-m} > \\ 2^{k-m} - 1 = 2^{k-m-1} + \cdots + 1 \geq b_{m+1}2^{k-m-1} + \cdots + b_k,$$

απ΄ όπου έπεται $a > b$. Όμοια, και στην άλλη περίπτωση.

Καλούμε *μήκος* ενός φυσικού αριθμού a και το συμβολίζουμε με $\ell(a)$ το πλήθος των ψηφίων της δυαδικής παράστασης του. Δηλαδή, έχουμε:

$$\ell(a) = 1 + \lfloor \log_2 a \rfloor = 1 + \lfloor \log a / \log 2 \rfloor.$$

Εύκολα διαπιστώνουμε ότι:

$$\ell(a) = k \quad \text{αν και μόνον αν} \quad 2^{k-1} \leq a < 2^k.$$

Ας είναι a και b δύο φυσικοί αριθμοί μήκους k και l αντίστοιχα. Αν $a \leq b$, τότε αμέσως παίρνουμε $k \leq l$. Ας σημειωθεί ότι είναι δυνατόν να έχουμε $a < b$ και $k = l$. Για παράδειγμα, αν $a = 2^k+1$ και $b = 2^k+2+1$, με $k \geq 2$, τότε έχουμε $b > a$ και $\ell(a) = k = \ell(b)$. Επίσης, από τις ανισότητες $2^{k-1} \leq a < 2^k$ και $2^{l-1} \leq b < 2^l$, παίρνουμε

$$2^{k+l-2} \leq ab < 2^{k+l} \quad \text{και} \quad 2^{\max\{k,l\}-1} \leq a + b < 2^{\max\{k,l\}+1},$$

απ΄ όπου προκύπτει $\ell(ab) = k + l$ ή $k + l - 1$ και $\ell(a + b) = \max\{k, l\}$ ή $\max\{k, l\} + 1$. Πιο γενικά ισχύει η παρακάτω πρόταση.

Πρόταση 1.2 *Ας είναι $a_1, \ldots, a_s$ φυσικοί μήκους $\leq k$. Τότε, έχουμε:*

$$\ell(a_1 \cdots a_s) \leq sk \quad \textit{και} \quad \ell(a_1 + \cdots + a_s) \leq k + \ell(s).$$

Απόδειξη. Καθώς $\ell(a_i) \leq k$, έχουμε $a_i < 2^k$ $(i = 1, \ldots, s)$. Οπότε, ισχύει $a_1 \cdots a_s < 2^{sk}$, απ΄ όπου $\ell(a_1 \cdots a_s) \leq sk$.

Επίσης, έχουμε $a_1 + \cdots + a_s < s2^k$ και επομένως παίρνουμε:

$$\ell(a_1 + \cdots + a_s) \leq \ell(s2^k) = 1 + \lfloor \log_2 s \rfloor + k = \ell(s) + k. \quad \square$$

Πόρισμα 1.1 *Για κάθε φυσικό αριθμό m ισχύει:*

$$\ell(m!) \leq m\ell(m).$$

Ένα άνω φράγμα του μήκους του πηλίκου στην Ευκλείδεια διαίρεση δίνεται στην παρακάτω πρόταση.

Πρόταση 1.3 *Ας είναι a, b θετικοί ακέραιοι και q το πηλίκο της διαίρεσης του a διά b. Τότε, έχουμε:*

$$\ell(q) \leq \ell(a) - \ell(b) + 1.$$

Απόδειξη. Έχουμε $a = bq + r$ και $0 \leq r < b$. Έτσι, $\ell(r) \leq \ell(b)$ και επομένως παίρνουμε:

$$\ell(a) = \ell(bq) + \epsilon, \quad \ell(bq) = \ell(b) + \ell(q) - \zeta$$

με $\epsilon, \zeta \in \{0, 1\}$. Συνδυάζοντας τις παραπάνω σχέσεις, προκύπτει:

$$\ell(q) \leq \ell(a) - \ell(b) + 1. \quad \square$$

1.2 Δυαδικές Ψηφιακές Πράξεις

Σ′ αυτή την ενότητα θα εξετάσουμε τον χρόνο εκτέλεσης των πράξεων της πρόσθεσης, αφαίρεσης, πολλαπλασιασμού ακεραίων, καθώς και της Ευκλείδειας διαίρεσης. Θα ακολουθήσουμε την σχολική διαδικασία εκτέλεσης αυτών των πράξεων προσαρμοσμένη στο δυαδικό σύστημα και θα την αναλύσουμε σε απλούστερες πράξεις.

Ας είναι $a = (a_1 \cdots a_k)_2$ και $b = (b_1 \cdots b_l)_2$ δύο θετικοί ακέραιοι. Για να προσθέσουμε τους a και b, γράφουμε τον b κάτω από τον a θέτοντας το b_l κάτω από το a_k, το b_{l-1} κάτω από το a_{k-1}, κοκ. Σε μία γραμμή πάνω από τα ψηφία του a σημειώνουμε τα ''κρατούμενα''. Έτσι, δημιουργούνται τρεις γραμμές. Αρχίζουμε από τα δεξιά και εργαζόμαστε σε κάθε στήλη, ώστε να δημιουργήσουμε μία τέταρτη γραμμή κάτω από το b με το αποτέλεσμα της πράξης, με τον εξής τρόπο:

1. Αν και στις τρεις πρώτες γραμμές υπάρχει το 0, τότε θέτουμε το 0 στην τελευταία γραμμή.

2. Αν σε μία από τις τρεις πρώτες γραμμές υπάρχει το 1 και στις άλλες δύο το 0, τότε θέτουμε στην τελευταία γραμμή το 1.

3. Αν σε μία από τις τρεις πρώτες γραμμές υπάρχει το 0 και στις άλλες δύο το 1, τότε θέτουμε το 0 στην τελευταία γραμμή και μεταφέρουμε το 1 στο πάνω μέρος της επόμενης στήλης.

4. Αν και στις τρεις πρώτες γραμμές υπάρχει το 1, τότε θέτουμε το 1 στην τελευταία γραμμή και μεταφέρουμε το 1 στο πάνω μέρος της επόμενης στήλης.

Κάθε μία από τις παραπάνω διαδικασίες καλείται *δυαδική ψηφιακή πράξη*. Αν στην τελευταία στήλη αριστερά έχουμε μόνο το κρατούμενο, τότε το κατέβασμά του στην τελευταία γραμμή δεν θεωρείται ως δυαδική ψηφιακή πράξη. Συνεπώς, η πρόσθεση των ακεραίων a και b μήκους k και l, αντίστοιχα, απαιτεί $\max\{k, l\}$ δυαδικές ψηφιακές πράξεις.

Παράδειγμα 1.5 Θα υπολογίσουμε το άθροίσμα των 1101000 και 111010. Έχουμε:

$$\begin{array}{cccccccc} 1 & 1 & 1 & 1 & & & & \\ & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ & & 1 & 1 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}$$

Η διαδικασία της αφαίρεσης στο δυαδικό σύστημα είναι παρόμοια μ΄ αυτή της πρόσθεσης. Ας υποθέσουμε ότι $a \geq b$. Για να αφαιρέσουμε τον b από τον a, γράφουμε τον b κάτω από τον a θέτοντας το b_l κάτω από το a_k, το b_{l-1} κάτω από το a_{k-1}, κοκ. Σε μία τρίτη γραμμή κάτω από τα ψηφία του b σημειώνουμε τα ''κρατούμενα''. Έτσι, δημιουργούνται τρεις γραμμές. Αρχίζουμε από τα δεξιά και εργαζόμαστε σε κάθε στήλη, ώστε να δημιουργήσουμε μία τέταρτη γραμμή κάτω από τα κρατούμενα με το αποτέλεσμα της πράξης, με τον εξής τρόπο:

1. Αν και στις τρεις πρώτες γραμμές υπάρχει το 0, τότε θέτουμε το 0 στην τελευταία γραμμή.

2. Αν στην πρώτη γραμμή υπάρχει το 1 και στις άλλες δύο το 0, τότε θέτουμε στην τελευταία γραμμή το 1.

3. Αν στην πρώτη γραμμή υπάρχει το 1 και στις άλλες δύο το 1 και το 0 (με οποιαδήποτε σειρά), τότε θέτουμε το 0 στην τελευταία γραμμή.

4. Αν και στις τρεις πρώτες γραμμές υπάρχει το 1, τότε θέτουμε το 1 στην τελευταία γραμμή και μεταφέρουμε το 1 στη γραμμή των κρατουμένων της επόμενης στήλης.

5. Αν στην πρώτη γραμμή υπάρχει το 0 και στις άλλες δύο το 1 και το 0 (με οποιαδήποτε σειρά), τότε θέτουμε το 1 στην τελευταία γραμμή και μεταφέρουμε το 1 στη γραμμή των κρατουμένων της επόμενης στήλης.

6. Αν στην πρώτη γραμμή υπάρχει το 0 και στις άλλες δύο το 1, τότε θέτουμε το 0 στην τελευταία γραμμή και μεταφέρουμε το 1 στη γραμμή των κρατουμένων της επόμενης στήλης.

Κάθε μία από τις παραπάνω διαδικασίες καλείται επίσης *δυαδική ψηφιακή πράξη*. Έτσι, η αφαίρεση του b από τον a απαιτεί το πολύ k δυαδικές ψηφιακές πράξεις.

Παράδειγμα 1.6 Θα αφαιρέσουμε τον ακεραίο 10101 από τον 111010. Έχουμε:

$$\begin{array}{cccccc} 1 & 1 & 1 & 0 & 1 & 0 \\ & 1 & 0 & 1 & 0 & 1 \\ & & 1 & & 1 & \\ \hline 1 & 0 & 0 & 1 & 0 & 1 \end{array}$$

Η *συνάρτηση προσήμου* $sign : \mathbb{Z} \to \{0, \pm 1\}$ ορίζεται ως εξής:

$$sign(x) = \begin{cases} 1 & \text{αν} \quad x > 0, \\ 0 & \text{αν} \quad x = 0, \\ -1 & \text{αν} \quad x < 0. \end{cases}$$

Ας υποθέσουμε τώρα ότι θέλουμε να υπολογίσουμε το άθροισμα δύο οποιωνδήποτε ακεραίων a και b. Αν $sign(a) = sign(b)$, τότε υπολογίζουμε το άθροισμα $|a| + |b|$ καί έχουμε:

$$a + b = sign(a)(|a| + |b|).$$

Ας είναι $sign(a) \neq sign(b)$. Τότε συγκρίνουμε τους $|a|$ και $|b|$. Αν $|a| > |b|$, τότε υπολογίζουμε τη διαφορά $|a| - |b|$ και έχουμε:

$$a + b = sign(a)(|a| - |b|).$$

Διαφορετικά, υπολογίζουμε τη διαφορά $|b| - |a|$ και έχουμε:

$$a + b = sign(b)(|b| - |a|).$$

Σε κάθε περίπτωση ο υπολογισμός χρειάζεται το πολύ $\max\{k, l\}$ δυαδικές ψηφιακές πράξεις.

Στον υπολογισμό του αθροίσματος δεν λάβαμε υπόψιν μας την σύγκριση δύο θετικών αριθμών, η οποία, όπως είδαμε παραπάνω, γίνεται με έναν απλό έλεγχο των δυαδικών τους ψηφίων. Στη συνέχεια, δεν θα υπολογίζουμε τη σύγκριση δύο θετικών ακεραίων ως δυαδική ψηφιακή πράξη.

Στη συνέχεια θ΄ ασχοληθούμε με τον πολλαπλασιασμό των ακεραίων στο δυαδικό σύστημα. Θεωρούμε πάλι θετικούς ακεραίους $a = a_1 \cdots a_k$ και $b = b_1 \cdots b_l$ γραμμένους στο δυαδικό σύστημα. Όπως και στην πρόσθεση γράφουμε τον b κάτω από τον a. Αρχίζουμε από το πρώτο δεξί μη μηδενικό ψηφίο του b και γράφουμε στην παρακάτω γραμμή τον a. Στην επόμενη γραμμή γράφουμε πάλι τον a μετατοπισμένο τόσες θέσεις όσα είναι τα επόμενα προς τα αριστερά μηδενικά ψηφία του b συν ένα. Συνεχίζουμε με τον ίδιο τρόπο μέχρι να εξαντλήσουμε όλα τα μη μηδενικά ψηφία του b. Κατόπιν, εκτελούμε την πρόσθεση των δύο πρώτων γραμμών, μετά προσθέτουμε το αποτέλεσμα στην τρίτη γραμμή κ.ο.κ. Σε κάθε τέτοια πρόσθεση, καθώς τα πρώτα δεξιά ψηφία του δεύτερου ακεραίου είναι μηδενικά, αντιγράφουμε στο αποτέλεσμα τα ψηφία του πρώτου ακεραίου που βρίσκονται πάνω από αυτά. Αυτή η διαδικασία δεν υπολογίζεται ως ψηφιακή πράξη και επομένως έχουμε να υπολογίσουμε το πλήθος των πράξεων για την πρόσθεση δύο ακεραίων μήκους $\leq k$. Καθώς έχουμε να εκτελέσουμε το πολύ $l-1$ προσθέσεις, το πλήθος των δυαδικών ψηφιακών πράξεων για τον πολλαπλασιασμό του a με τον b είναι το πολύ $(l-1)k$.

Στην περίπτωση όπου $b = 2^{l-1}$ έχουμε $ab = a_1 \cdots a_k 0 \cdots 0$ (το 0 υπάρχει στις τελευταίες $l-1$ θέσεις). Άρα ο υπολογισμός του ab γίνεται με μετατόπιση των ψηφίων του a κατά $l-1$ θέσεις αριστερά στη δυαδική γραφή του και θέτοντας το 0 στις τελευταίες $l-1$ θέσεις. Τέλος, αν οι a και b είναι οποιοιδήποτε ακέραιοι, τότε ο υπολογισμός του γινομένου ab γίνεται υπολογίζοντας το γινόμενο $|a||b|$ και θέτοντας $ab = sign(a)sign(b)|a||b|$.

Παράδειγμα 1.7 Θα πολλαπλασιάσουμε τους ακέραιους 11101 και 10101. Έχουμε:

					1	1	1	0	1
					1	0	1	0	1
					1	1	1	0	1
			1	1	1	0	1		
	1	1	1	0	1				
1	0	0	1	1	0	0	0	0	1

Η διαδικασία της διαίρεσης μπορεί ν΄ αναλυθεί με τον ίδιο τρόπο, όπως και ο πολλαπλασιασμός. Ας υποθέσουμε ότι η διαίρεση του a με b δίνει πηλίκο q μήκους m. Για την εκτέλεση αυτής της διαίρεσης απαιτείται η εκτέλεση m αφαιρέσεων ακεραίων μήκους $\leq l$ και επομένως χρειάζονται το πολύ lm δυαδικές ψηφιακές πράξεις. Καθώς η Πρόταση 1.3 δίνει $m \leq k-l+1$, έχουμε το πολύ $l(k-l+1)$ δυαδικές ψηφιακές πράξεις.

Στην περίπτωση όπου $a = 2^{l-1}a'$, όπου a' είναι ακέραιος μήκους $k-l+1$, έχουμε $a = a_1 \cdots a_{k-l+1}0 \cdots 0$ (το 0 υπάρχει στις τελευταίες $l-1$ θέσεις). Άρα το πηλίκο της διαίρεσης του a με τον $b = 2^{l-1}$ είναι ο ακέραιος $a' = a_1 \cdots a_{k-l+1}$ του οποίου ο υπολογισμός γίνεται με μετατόπιση των πρώτων $k-l+1$ ψηφίων του a κατά $l-1$ θέσεις δεξιά στη δυαδική γραφή του.

Παράδειγμα 1.8 Θα διαιρέσουμε τον ακέραιο 110101 με τον 1001. Έχουμε:

1	1	0	1	0	1	1	0	0	1
1	0	0	1			1	0	1	
	1	0	0	0	1				
		1	0	0	1				
		1	0	0	0				

Άρα το πηλίκο είναι 1001 και το υπόλοιπο 1000.

1.3 Αλγόριθμοι

Σ΄ αυτή την ενότητα θα παρουσιάσουμε μερικά στοιχεία από την Θεωρία Αλγορίθμων. Θα περιοριστούμε μόνο στις απολύτως απαραίτητες έννοιες που θα μας χρειαστούν και σε αλγόριθμους που δέχονται ως είσοδο φυσικούς αριθμούς. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να ανατρέξει σε εξιδικευμένα συγγράμματα όπως τα [5, 7].

1.3.1 Ασυμπτωτικοί Συμβολισμοί.

Καταρχήν θα εισαγάγουμε μερικούς συμβολισμούς οι οποίοι είναι χρήσιμοι για την περιγραφή της απόδοσης ενός αλγορίθμου και άλλων συναφών θεμάτων. Ας είναι m ένας θετικός ακέραιος, A, B υποσύνολα του $\mathbb{N}^m$, $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$ συναρτήσεις και η g παίρνει θετικές τιμές. Θα γράφουμε $f = O(g)$ και $f = \Omega(g)$, αν υπάρχουν θετικοί

πραγματικοί αριθμοί C και D, ώστε για κάθε $(x_1, \ldots, x_m) \in A \cap B$ με $x_i > C$ $(i = 1, \ldots, m)$ να ισχύει:

$$|f(x_1, \ldots, x_m)| \leq Dg(x_1, \ldots, x_m)$$

και

$$f(x_1, \ldots, x_m) \geq Dg(x_1, \ldots, x_m),$$

αντίστοιχα. Στην περίπτωση όπου g είναι μία σταθερά, θα γράφουμε $f = O(1)$ και $f = \Omega(1)$, αντίστοιχα. Αν ισχύει ταυτόχρονα $f = O(g)$ και $f = \Omega(g)$, τότε θα γράφουμε $f = \Theta(g)$.

Παράδειγμα 1.9 Ας είναι $f : \mathbb{N} \to \mathbb{Z}$ η συνάρτηση που ορίζεται από την σχέση:

$$f(x) = a_0 x^d + \cdots + a_d,$$

όπου $a_0, \ldots, a_d \in \mathbb{Z}$ με $a_0 > 0$. Τότε υπάρχει θετικός ακέραιος n_0 έτσι, ώστε για κάθε ακέραιο $n \geq n_0$ να ισχύει $f(n) > 0$. Αν $M = \max\{a_0, |a_1|, \ldots, |a_d|\}$, τότε για κάθε θετικό ακέραιο $n \geq n_0$ έχουμε:

$$f(n) \leq (d+1)Mn^d.$$

Έτσι, ισχύει $f = O(x^d)$.

Παράδειγμα 1.10 Ας είναι f και g συναρτήσεις που είναι ορισμένες για κάθε θετικό ακέραιο $n \geq n_0$, όπου n_0 ακέραιος ≥ 0, και παίρνουν θετικές πραγματικές τιμές. Ας υποθέσουμε ότι έχουμε:

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = c,$$

όπου c πραγματικός αριθμός. Τότε υπάρχει φυσικός m τέτοιος, ώστε για κάθε $n \geq m$ να ισχύει:

$$\left| \frac{f(n)}{g(n)} - c \right| < 1.$$

Επομένως, έχουμε $f(n) < (1 + c)g(n)$, απ' όπου έπεται $f = O(g)$.

Ειδικότερα, για κάθε $\epsilon > 0$ ισχύει:

$$\lim_{n\to\infty} \frac{\log n}{n^\epsilon} = 0$$

και, επομένως έχουμε $\log n = O(n^\epsilon)$. Ας σημειωθεί ότι οι σταθερές που δηλώνονται δια μέσου αυτής της γραφής είναι συναρτήσεις του ϵ.

Παράδειγμα 1.11 Ας είναι a ακέραιος > 0 και $f : [a, \infty) \to [0, \infty)$ μία αύξουσα συνεχής συνάρτηση. Θεωρούμε έναν ακέραιο $n > a$ και το άθροισμα

$$S_f(n) = \sum_{k=a}^{n} f(k).$$

Θα δώσουμε μία εκτίμηση του $S_f(n)$ με την βοήθεια του ολοκληρώματος της f. Ερμηνεύοντας το ολοκλήρωμα της f με άκρα τα k και $k+1$ ως το εμβαδόν του χωρίου που ορίζεται σε ένα ορθοκανονικό σύστημα $0xy$ από τον άξονα $0x$, τις ευθείες $x = k$, $x = k+1$ και την γραφική παράσταση της f, παίρνουμε:

$$f(k) \leq \int_k^{k+1} f(x)\,dx \leq f(k+1) \quad (k = a, a+1, \ldots).$$

Επομένως, έχουμε:

$$S_f(n) \leq \int_a^n f(x)\,dx + f(n)$$

και

$$f(a) + \int_a^n f(x)\,dx \leq S_f(n),$$

απ΄ όπου:

$$0 \leq f(a) \leq S_f(n) - \int_a^n f(x)\,dx \leq f(n).$$

Ετσι, προκύπτει:

$$S_f(n) = \int_a^n f(x)\,dx + O(f(n)).$$

Ειδικότερα, για $f(x) = \log x$, έχουμε:

$$\int \log x\,dx = x \log x - x + C$$

και κατα συνέπεια ισχύει:

$$\sum_{k=1}^{n} \log k = n \log n - n + O(\log n).$$

1.3.2 Είδη Αλγορίθμων

Μία συγκεκριμένη βήμα προς βήμα πεπερασμένη διαδικασία για τον υπολογισμό μίας ποσότητας καλείται *αλγόριθμος*.

Συχνά υπάρχουν περισσότεροι του ενός αλγόριθμοι για τον υπολογισμό μίας ποσότητας. Η επιλογή ενός από αυτούς εξαρτάται από το ενδιαφέρον του χρήστη, ο οποίος μπορεί να επιλέξει τον απλούστερο, ή τον ταχύτερο ή κάποιο συνδυασμό και των δύο.

Ας είναι $\mathcal{A}$ ένας αλγόριθμος που δέχεται ως είσοδο φυσικούς αριθμούς. Ο χρόνος που χρειάζεται ένας υπόλογιστής για να φέρει εις πέρας τον αλγόριθμο $\mathcal{A}$ είναι ουσιαστικά ανάλογος του πλήθους των δυαδικών ψηφιακών πράξεων που απαιτείται για την εκτέλεση του.

Καλούμε *χρόνο εκτέλεσης του αλγορίθμου* $\mathcal{A}$ και το συμβολίζουμε με $T(\mathcal{A})$ το πλήθος των δυαδικών ψηφιακών πράξεων που απαιτούνται για την εκτέλεση του. Έτσι, για τις πράξεις της πρόσθεσης, αφαίρεσης, πολλαπλασιασμού και Ευκλείδειας διαίρεσης, σύμφωνα με την ανάλυση που κάναμε στην προηγούμενη ενότητα, έχουμε:

1. $T(a+b) = \max\{\ell(|a|), \ell(|b|)\}$, για κάθε $a, b \in \mathbb{Z}$.
2. $T(a \times b) \leq (\ell(|b|) - 1)\ell(|a|)$, για κάθε $a, b \in \mathbb{Z}$.
3. $T(a : b) \leq \ell(b)(\ell(a) - \ell(b) + 1)$, για κάθε $a, b \in \mathbb{Z}$ με $a > b > 0$.

Συχνά δεν μας ενδιαφέρει το ακριβές πλήθος των απαιτούμενων δυαδικών ψηφιακών πράξεων αλλά μόνο ο ρυθμός αύξησής τους. Γι΄ αυτό τον λόγο θα χρησιμοποιούμε τους συμβολισμούς που εισάγαμε παραπάνω. Παρατηρούμε ότι για κάθε θετικό ακέραιο a έχουμε $\ell(a) = \Theta(\log a)$ και επομένως παίρνουμε:

1. $T(a \pm b) = O(\max\{\log |a|, \log |b|\})$, για κάθε $a, b \in \mathbb{Z}$.
2. $T(a \times b) = O((\log |a|)(\log |b|))$, για κάθε $a, b \in \mathbb{Z}$.
3. $T(a : b) = O((\log b)(\log a - \log b))$, για κάθε $a, b \in \mathbb{Z}$ με $a > b > 0$.

Ο $\mathcal{A}$ καλείται *αλγόριθμος πολυωνυμικού χρόνου* αν υπάρχει ένας ακέραιος $d > 0$, ώστε ο χρόνος που απαιτείται για την εκτέλεση της εργασίας του, κάθε φορά που έχει ως είσοδο φυσικούς συνολικού μήκους $\leq k$, να είναι $O(k^d)$ δυαδικές ψηφιακές πράξεις. Παραδείγματα

αλγορίθμων πολυωνυμικού χρόνου είναι οι αλγόριθμοι των συνήθων αριθμητικών πράξεων πρόσθεσης, πολλαπλασιασμού, αφαίρεσης και διαίρεσης.

Παράδειγμα 1.12 Ας είναι $m_1, \ldots, m_k$ ακέραιοι ≥ 2. Θα υπολογίσουμε το γινόμενο $m = m_1 \cdots m_k$ πολλαπλασιάζοντας πρώτα τον m_1 με τον m_2, κατόπιν το γινόμενο $m_1 m_2$ με τον m_3 κ.ο.κ. Ο πολλαπλασιασμός του $m_1 \cdots m_i$ με τον m_{i+1} απαιτεί χρόνο $O(\ell(m_1 \cdots m_i)\ell(m_{i+1}))$. Έτσι, ο χρόνος που απαιτείται για όλους τους πολλαπλασιασμούς είναι:

$$O(\ell(m_1)\ell(m_2) + \ell(m_1 m_2)\ell(m_3) + \cdots + \ell(m_1 \cdots m_{k-1})\ell(m_k)) =$$

$$O(\ell(m)(k + \log m_2 + \cdots + \log m_k)).$$

Από την ανισότητα $m \geq 2^k$ έπεται $\log m \geq k \log 2$ και επομένως $k = O(\log m) = O(\ell(m))$. Έτσι, ο ζητούμενος χρόνος είναι $O(\ell(m)^2)$. Καθώς $\ell(m) = O(\ell(m_1) + \cdots + \ell(m_k))$, ο αλγόριθμος που χρησιμοποιήθηκε γι΄ αυτόν τον υπολογισμό είναι πολυωνυμικού χρόνου.

Παράδειγμα 1.13 Ας είναι n και k ακέραιοι ≥ 2. Θα δώσουμε έναν αλγόριθμο για τον υπολογισμό του $m = \lfloor \sqrt[k]{n} \rfloor$. Πρώτα παρατηρούμε ότι ισχύει:

$$2^{\lfloor (\log_2 n)/k \rfloor} \leq m < 2^{\lfloor (\log_2 n)/k \rfloor + 1}.$$

Έτσι, το μήκος του m ισούται με

$$l = \left\lfloor \frac{\log_2 n}{k} \right\rfloor + 1$$

και επομένως έχουμε:

$$m = 2^l + a_1 2^{l-1} + \cdots + a_l.$$

Ο προσδιορισμός του m μπορεί να γίνει με τον εξής αλγόριθμο:

Αλγόριθμος 1.1 Υπολογισμός k-οστής ρίζας ακεραίου.
Είσοδος: Ακέραιοι $n, k \geq 2$.
Έξοδος: $m = \lfloor \sqrt[k]{n} \rfloor$.
Θέτουμε $m_0 = 0$. Για $i = 0, 1, \ldots, l$ κάνουμε τα εξής:

1. Υπολογίζουμε $M_i = m_i + 2^{l-i}$.
2. Υπολογίζουμε τον ακέραιο M_i^k και κάνουμε τα εξής:

(α′) Αν $M_i^k < n$, τότε θέτουμε $m_{i+1} = M_i$.

(β′) Αν $M_i^k > n$, τότε θέτουμε $m_{i+1} = m_i$.

(γ′) Αν $M_i^k = n$, τότε εξάγουμε την τιμή $m = M_i$ και σταματάμε.

3. Αν $M_i^k \neq n$, για κάθε $i = 0, \ldots, l$, τότε εξάγουμε την τιμή $m = m_l$.

Ο ακέραιος m που δίνει ο αλγόριθμος είναι ο μεγαλύτερος ακέραιος με $m^k < n$ και κατά συνέπεια είναι ο ζητούμενος ακέραιος. Θα υπολογίσουμε στη συνέχεια τον χρόνο που χρειάζεται για την εκτέλεσή του.

Από την ισότητα $m^k \leq n$, έπεται $k = O(\log n)$. Καθώς $M_i^k < 2^k n$, από το Παράδειγμα 1.12 έχουμε ότι ο απαιτούμενος χρόνος για τον υπολογισμό του M_i^k είναι:

$$O((\log(2^k n))^2) = O((k \log 2 + \log n)^2) = O((\log n)^2).$$

Έτσι, ο χρόνος που απαιτείται για τον υπολογισμό όλων των M_i^k ισούται με $O(l(\log n)^2)$. Επίσης, χρειάζεται κάθε πρόσθεση $m_i + 2^{l-i}$ χρειάζεται χρόνο $O(\log n)$. Οπότε, ο συνολικός χρόνος για την εκτέλεση αυτών των προσθέσεων είναι $O(l \log n)$. Συνεπώς, ο χρόνος υπολογισμού του $\lfloor \sqrt[k]{n} \rfloor$ είναι $O((\log n)^3)$ δυαδικές ψηφιακές πράξεις.

Στη συνέχεια θα δούμε πώς εξετάζουμε αν ο θετικος ακέραιος $n > 1$ είναι τέλεια δύναμη ακεραίου, δηλαδή αν υπάρχουν ακέραιοι $m, k > 1$ τέτοιοι, ώστε $n = m^k$. Παρατηρούμε ότι $k \leq \lfloor \log_2 n \rfloor$. Συνεπώς, αρκεί για κάθε $k = 2, \ldots, \lfloor \log_2 n \rfloor$ να υπολογίσουμε τον ακέραιο $\lfloor \sqrt[k]{n} \rfloor$ και κατόπιν να τον υψώσουμε στην δύναμη k για να δούμε αν μας δίνει τον n. Από τον παραπάνω αλγόριθμο και το Παράδειγμα 1.12 έπεται ότι ο χρόνος που απαιτείται για αυτή την διαδικασία είναι $O((\log n)^4)$ δυαδικές ψηφιακές πράξεις.

Παράδειγμα 1.14 Το Θεώρημα 1.2 μας δίνει τον παρακατω αλγόριθμο για τον υπολογισμό της παράστασης ενός θετικού ακεραίου a στην κλίμακα του g:

Αλγόριθμος 1.2 Εύρεση g-αδικής παράστασης ακεραίου.
Είσοδος: Θετικός ακέραιος a.
Έξοδος: Τα ψηφία της g-αδικής παράστασης του a.

1. Υπολογίζουμε $k = 1 + \lfloor \log_g a \rfloor$ και θέτουμε $A_1 = a$.
2. Για $i = 1, \ldots, k$ κάνουμε τα εξής:
   (α′) Διαιρούμε τον A_i με τον g^{k-i}. Συμβολίζουμε με a_i το πηλίκο αυτής της διαίρεσης.
   (β′) Υπολογίζουμε τον ακέραιο $A_{i+1} = A_i - a_i g^{k-i}$.
3. Εξάγουμε τους ακεραίους $a_1, \ldots, a_k$.

Θα υπολογίσουμε τον χρόνο εκτέλεσης του αλγορίθμου. Ο χρόνος υπολογισμού του πηλίκου της διαίρεσης του A_i με τον g^{k-i} είναι: $O(\ell(g^{k-i})(\ell(A_i) - \ell(g^{k-i})))$. Από την άλλη πλευρά έχουμε:

$$A_i \leq (g-1)(g^{k-i} + \cdots + g + 1) = g^{k-i+1} - 1 < g^{k-i+1}.$$

Ο χρόνος υπολογισμού όλων των διαιρέσεων είναι:

$$O\left(\sum_{i=1}^{k} \ell(g^{k-i})(\ell(A_i) - \ell(g^{k-i}))\right) =$$
$$O\left(\sum_{i=1}^{k} \ell(g^{k-i})(\ell(g^{k-i+1}) - \ell(g^{k-i}))\right) = O(\ell(g^{k-1})\ell(g^k)).$$

Καθώς όμως ισχύει $\ell(g^k) \leq 2\ell(g^{k-1}) \leq 2\ell(a)$, ο χρόνος υπολογισμού όλων των διαιρέσεων είναι $O(\ell(a)^2)$ δυαδικές ψηφιακές πράξεις.

Ο χρόνος υπολογισμού κάθε A_{i+1} $(i = 1, \ldots, k-1)$ είναι ο χρόνος εκτέλεσης της αφαίρεσης $A_i - a_i g^{k-i}$ ο οποίος είναι $O(\ell(A_i)) = O(\ell(g^{k-i+1}))$. Έτσι, ο χρόνος υπολογισμού των $A_2, \ldots, A_k$ είναι:

$$O\left(\sum_{i=1}^{k-1} \ell(g^{k-i+1})\right).$$

Χρησιμοποιώντας τις ανισότητες $\ell(g^i) \leq \ell(a)$ $(i = 1, \ldots, k-1)$ και $\ell(g^k) \leq 2\ell(a)$, συμπεραίνουμε ότι ο παραπάνω χρόνος είναι $O(\ell(a)^2)$ δυαδικές ψηφιακές πράξεις. Συνεπώς, ο χρόνος που απαιτείται για την εύρεση της παράστασης ενός θετικού ακεραίου a στην κλίμακα του g είναι $O(\ell(a)^2)$ δυαδικές ψηφιακές πράξεις. Παρατηρούμε ότι αυτός ο χρόνος δεν εξαρτάται από τον g.

Ο $\mathcal{A}$ καλείται *αλγόριθμος εκθετικού χρόνου*, αν υπάρχει θετικός πραγματικός αριθμός c, ώστε ο χρόνος που απαιτείται για την εκτέλεση της εργασίας του, κάθε φορά που έχει ως είσοδο φυσικούς συνολικού μήκους $\leq k$, να είναι $O(e^{ck})$ δυαδικές ψηφιακές πράξεις. Ένα παράδείγμα αλγορίθμου εκθετικού χρόνου δίνεται παρακάτω.

Παράδειγμα 1.15 Ας είναι n ένας θετικός ακέραιος. Θα εκτιμήσουμε τον χρόνο που απαιτείται για τον υπολογισμό του $n!$. Χρησιμοποιούμε τον εξής αλγόριθμο: Πρώτα πολλαπλασιάζουμε τον 2 με τον 3, το αποτέλεσμα με τον 4 κ.ο.κ. Στο $(j-1)$-οστό βήμα πολλαπλασιάζουμε τον $j!$ με τον $j+1$. Έτσι, έχουμε $n-2$ πολλαπλασιασμούς. Από το Πόρισμα 1.1 έχουμε $\ell(n!) = O(n \log n)$ και επομένως ο κάθε πολλαπλασιασμός απαιτεί $O(n(\log n)^2)$ δυαδικές ψηφιακές πράξεις. Άρα, ο υπολογισμός του $n!$ απαιτεί $O((n \log n)^2)$ πράξεις. Έτσι, παίρνουμε:

$$T(\text{υπολογισμός του } n!) = O((n \log n)^2).$$

Επομένως, ο παραπάνω αλγόριθμος είναι εκθετικού χρόνου.

Ας είναι n θετικός ακέραιος, $\gamma \in [0,1]$ και c θετικός πραγματικός αριθμός. Θέτουμε:

$$L_n(\gamma; c) = O(e^{c(\log n)^{\gamma}(\log\log n)^{1-\gamma}}).$$

Ειδικότερα, έχουμε $L_n(1;c) = O(n^c)$ και $L_n(0;c) = O((\log n)^c)$. Καλούμε *$L(\gamma)$-αλγόριθμο* έναν αλγόριθμο ο οποίος δέχεται ως είσοδο θετικούς ακεραίους και κάθε φορά που εφαρμόζεται σ΄ έναν ακέραιο n ο χρόνος που χρειάζεται για να τελειώσει την εργασία του είναι της μορφής $L_n(\gamma; c)$. Ειδικότερα, ένας αλγόριθμος πολυωνυμικού χρόνου είναι ένας $L(0)$-αλγόριθμος και ένας αλγόριθμος εκθετικού χρόνου είναι ένας $L(1)$-αλγόριθμος. Καλούμε *αλγόριθμο υποεκθετικού χρόνου* κάθε $L(\gamma)$-αλγόριθμο με $\gamma < 1$.

Ένας αλγόριθμος καλείται *αιτιοκρατικός*, αν όσες φορες τροφοδοτηθεί με μία συγκεκριμένη είσοδο ακολουθεί τα ίδια βήματα με την ίδια σειρά και δίνει πάντα το ίδιο αποτέλεσμα. Τέτοιοι αλγόριθμοι είναι οι αλγόριθμοι των συνήθων αριθμητικών πράξεων πρόσθεσης, πολλαπλασιασμού, αφαίρεσης και διαίρεσης, καθώς και αυτοί των Παραδειγμάτων 1.12 και 1.15. Από την άλλη πλευρά, συχνά στην πράξη είναι χρήσιμοι αλγόριθμοι οι οποίοι κατά την εκτέλεσή τους χρησιμοποιούν τυχαία επιλεγμένους αριθμούς. Αυτοί οι αριθμοί προσδιορίζουν τα βήματά τους

και είναι δυνατόν να επηρεάσουν τον χρόνο εκτέλεσής τους. Τέτοιοι αλγόριθμοι καλούνται *πιθανοτικοί ή τυχαιοκρατικοί.*

Ένας πιθανοτικός $Monte\ Carlo$ αλγόριθμος πολυωνυμικού χρόνου είναι ένας πιθανοτικός αλγόριθμος με πολυωνυμικό χρόνος εκτέλεσης ο οποίος δίνει σωστό αποτέλεσμα με κάποια πιθανότητα. Δηλαδή, για κάποιες επιλογές των τυχαίων αριθμών το αποτέλεσμα είναι λάθος ή δεν υπάρχει αποτέλεσμα.

Ένας πιθανοτικός $Las\ Vegas$ αλγόριθμος είναι ένας πιθανοτικός αλγόριθμος ο οποίος δίνει πάντα σωστό αποτέλεσμα. Ένας τέτοιος αλγόριθμος, ενδέχεται για κάποιες εισόδους να μην παράγει έξοδο. Ο χρόνος εκτέλεσής του για κάθε είσοδο μήκους k είναι μία τυχαία μεταβλητή επί όλων των επιλογών των τυχαίων αριθμών που χρησιμοποιεί. Ο *αναμενόμενος χρόνος* εκτέλεσής του για κάθε είσοδο μήκους k είναι η μέση τιμή αυτής της τυχαίας μεταβλητής η οποία είναι της μορφής $O(k^d)$, όπου d σταθερός ακέραιος > 0. Ας σημειωθεί ότι ο χρόνος εκτέλεσης ενός τέτοιου αλγόριθμου για κάποιες επιλογές των τυχαίων αριθμών είναι δυνατόν να είναι εκθετικός.

1.4 Ταχύτερος Πολλαπλασιασμός

Ας είναι $x \in \mathbb{R}$. Τότε θα συμβολίζουμε με $\lceil x \rceil$ τον μικρότερο ακέραιο που είναι μεγαλύτερος ή ίσος του x. Άρα $\lceil x \rceil = x + \epsilon$, όπου $\epsilon \in \mathbb{R}$ με $0 \leq \epsilon < 1$. Ο ακέραιος $\lceil x \rceil$ καλείται *άνω ακέραιο μέρος* του x.

Σ′ αυτή την ενότητα θα δώσουμε μία ταχύτερη μέθοδο για τον πολλαπλασιασμό δύο ακεραίων. Ας είναι x, y θετικοί ακέραιοι και $n = \max\{\ell(x), \ell(y)\}$. Τότε έχουμε:

$$x = a2^{\lceil n/2 \rceil} + b, \quad y = c2^{\lceil n/2 \rceil} + d,$$

όπου a, b, c, d φυσικοί μήκους $\leq \lceil n/2 \rceil$. Έτσι, παίρνουμε:

$$\begin{aligned} xy &= ac2^n + (ad + bc)2^{\lceil n/2 \rceil} + bd, \\ &= ac2^n + ((a + b)(c + d) - ac - bd)2^{\lceil n/2 \rceil} + bd. \end{aligned}$$

Ο υπολογισμός του xy, σύμφωνα με την πρώτη γραμμή, απαιτεί την εκτέλεση των πολλαπλασιασμών ab, ad, bc και bd ενώ, σύμφωνα με την δεύτερη γραμμή, την εκτέλεση των πολλαπλασιασμών ab, ad και $(a + b)(c + d)$. Επίσης, όπως είδαμε στην Ενότητα 1.2, ο πολλαπλασιασμός ενός φυσικού m με τον 2^l, δεν είναι παρά μία μετατόπιση των δυαδικών

ψηφίων του m κατά l θέσεις αριστερά στην δυαδική γραφή του και συμπλήρωση των τελευταίων l δυαδικών ψηφίων με το 0.

Αν $a = (a_1, \ldots, a_l)_2$ και μ φυσικός με $1 \leq \mu < l$, τότε γράφουμε:

$$A(\mu, a) = (a_1, \ldots, a_\mu)_2, \quad T(\mu, a) = (a_{\mu+1}, \ldots, a_l)_2.$$

Στα 1962 ο A. A. Karatsuba έδωσε τον εξής αλγόριθμο για τον πολλαπλασιασμό δύο ακεραίων ο οποίος βασίζεται στην παραπάνω παρατήρηση:

Αλγόριθμος 1.3 Πολλαπλασιασμός του Karatsuba (ΠΟΛΚ).
Είσοδος: Θετικοί ακέραιοι x, y.
Έξοδος: Το γινόμενο $z = xy$.

1. Θέτουμε $n = \max\{\ell(x), \ell(y)\}$. Αν $n = 1$, τότε $z = xy$.

2. Υπολογίζουμε

$$(a, b) = (A(\lfloor n/2 \rfloor, x), T(\lfloor n/2 \rfloor, x)),$$

$$(c, d) = (A(\lfloor n/2 \rfloor, y), T(\lfloor n/2 \rfloor, y)).$$

3. Υπολογίζουμε

$$\begin{aligned} u &= \text{ΠΟΛΚ}(a + b, c + d), \\ v &= \text{ΠΟΛΚ}(a, c), \\ w &= \text{ΠΟΛΚ}(b, d). \end{aligned}$$

4. Υπολογίζουμε

$$z = v2^n + (u - v - w)2^{\lceil n/2 \rceil} + w.$$

5. Εξάγουμε τον ακέραιο z.

Πρόταση 1.4 *Ο αλγόριθμος* ΠΟΛΚ *υπολογίζει το γινόμενο δύο φυσικών αριθμών x και y μήκους $\leq n$ σε χρόνο $O(n^{\log_2 3})$ δυαδικών ψηφιακών πράξεων.*

Απόδειξη. Ας είναι $M(n)$ το πλήθος των δυαδικών ψηφιακών πράξεων που απαιτείται για να υπολογιστεί το γινόμενο δύο φυσικών με μήκος $\leq n$. Καταρχήν ας υποθέσουμε ότι $n = 2^k$. Σύμφωνα με τον αλγόριθμο

ΠΟΛΚ, ο υπολογισμός του z απαιτεί την εκτέλεση των πολλαπλασιασμών ac, bd, $(a+b)(c+d)$. Οι ακέραιοι a, c, b και d έχουν μήκος $\leq n/2$, ενώ οι $a+b$ και $c+d$ έχουν μήκος $\leq n/2+1$. Γράφουμε:

$$a+b=\alpha_1 2^{n/2}+\alpha_2, \quad c+d=\beta_1 2^{n/2}+\beta_2,$$

όπου $\alpha_1, \beta_1 \in \{0,1\}$ και $0 \leq \alpha_2 < 2^{n/2}$, $0 \leq \beta_2 < 2^{n/2}$. Τότε, έχουμε:

$$(a+b)(c+d)=\alpha_1\beta_1 2^n+(\alpha_1\beta_2+\alpha_2\beta_1)2^{n/2}+\alpha_2\beta_2.$$

Τα γινόμενα $\alpha_1\beta_1$, $\alpha_1\beta_2$, $\alpha_2\beta_1$ προέρχονται από πολλαπλασιασμούς όπου ένας από τους όρους είναι ένα δυαδικό ψηφίο. Από την άλλη πλευρά οι παράγοντες του γινομένου $\alpha_2\beta_2$ έχουν μήκος $\leq n/2$. Τέλος, ο πολλαπλασιασμός ενός φυσικου με μία δύναμη του 2 πραγματοποιείται με μία μετατόπιση. Συνεπώς, ο υπολογισμός του z απαιτεί 3 πολλαπλασιασμούς φυσικών μήκους $\leq n/2$, τεσσάρων προσθέσεων φυσικών μήκους $\leq n+1$ και δύο μετατοπίσεων. Από τα παραπάνω έχουμε:

$$M(n) \leq 3M(n/2)+Cn,$$

όπου C μία σταθερά ≥ 1.

Θα δείξουμε στην συνεχεια ότι για κάθε ακέραιο $k \geq 0$ έχουμε:

$$M(2^k) \leq C(3^{k+1}-2^{k+1}).$$

Για $k=0$, ισχύει $M(1)=1 \leq C$. Ας υποθέσουμε ότι η ανισότητα ισχύει για $k=m$. Έχουμε:

$$\begin{aligned} M(2^{m+1}) &\leq 3M(2^m)+C2^{m+1} \leq \\ &3C(3^{m+1}-2^{m+1})+C2^{m+1}=C(3^{m+2}-2^{m+2}). \end{aligned}$$

Άρα, η ανισότητα ισχύει για $k=m+1$ και κατά συνέπεια ισχύει για κάθε ακέραιο $k \geq 0$. Έτσι, παίρνουμε:

$$M(n) \leq C(3n^{\log_2 3}-2n).$$

Τέλος, ας υποθέσουμε ότι ο ακέραιος n δεν είναι δύναμη του 2. Τότε, υπάρχει ακέραιος $\mu \geq 0$ με $2^{\mu-1} < n < 2^\mu$. Οπότε $2^\mu < 2n$ και επομένως έχουμε:

$$M(n) \leq M(2^\mu) \leq C(3(2^\mu)^{\log_2 3}-2(2^\mu)) < C(3(2n)^{\log_2 3}).$$

Συνεπώς, σε κάθε περίπτωση ισχύει $M(n) = O(n^{\log_2 3})$. $\square$

Η μέθοδος του Karatsuba βελτιώθηκε από τους Toom και Cook [6]. Στα 1971, οι Schönhage και Strassen, χρησιμοποιώντας τον διακριτό μετασχηματισμό του Fourier, ανέπτυξαν μία μέθοδο για τον πολλαπλασιασμό δύο ακεραίων μήκους $\leq k$ η οποία απαιτεί χρόνο ίσο με $O(k(\log k)(\log\log k))$. Στην πράξη όμως, για $k \leq 10^4$, η μέθοδος αυτή είναι λιγότερο αποτελεσματική. Πρόσφατα ο M. Fürer βελτίωσε την παραπάνω μέθοδο [8]. Στη συνέχεια θα περιοριστούμε στη χρήση της ασθενέστερης εκτίμησης που δώσαμε στην Ενότητα 1.2.

1.5 Μέγιστος Κοινός Διαιρέτης

Ας είναι $a_1, \ldots, a_n$ $(n \geq 2)$ διακεκριμμένοι ακέραιοι οι οποίοι δεν είναι όλοι μηδέν. Καλούμε *κοινό διαιρέτη* των $a_1, \ldots, a_n$ κάθε ακέραιο b με $b|a_1, \ldots, b|a_n$. Αν b είναι ένας κοινός διαιρέτης των $a_1, \ldots, a_n$ και $a_1 \neq 0$, τότε $b|a_1$ και επομένως $|b| \leq |a_1|$. Συνεπώς, το σύνολο των κοινών διαιρετών των $a_1, \ldots, a_n$ είναι πεπερασμένο. Ο μεγαλύτερος θετικός κοινός διαιρέτης των $a_1, \ldots, a_n$ καλείται *μέγιστος κοινός διαιρέτης* ($\mu\kappa\delta$) των $a_1, \ldots, a_n$ και συμβολίζεται με $\mu\kappa\delta(a_1, \ldots, a_n)$.

Παράδειγμα 1.16 Οι κοινοί διαιρέτες των 12, 16 και 20 είναι οι ακέραιοι ± 1, ± 2 και ± 4. Έτσι, έχουμε $\mu\kappa\delta(12, 16, 20) = 4$.

Κάθε ακέραιος a έχει το ίδιο σύνολο θετικών διαιρετών με τον $-a$ και επομένως $\mu\kappa\delta(a_1, \ldots, a_n) = \mu\kappa\delta(|a_1|, \ldots, |a_n|)$. Το μηδέν διαιρείται από κάθε ακέραιο. Οπότε $\mu\kappa\delta(0, a_1, \ldots, a_n) = \mu\kappa\delta(a_1, \ldots, a_n)$.

Οι ακέραιοι $a_1, \ldots, a_n$ καλούνται *πρώτοι μεταξύ τους* αν ισχύει $\mu\kappa\delta(a_1, \ldots, a_n) = 1$ και *πρώτοι μεταξύ τους ανά δύο* αν για κάθε ζεύγος δεικτών i, j με $i \neq j$ έχουμε $\mu\kappa\delta(a_i, a_j) = 1$. Αν οι ακέραιοι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε είναι και πρώτοι μεταξύ τους. Το αντίστροφο όμως δεν ισχύει πάντα. Για παράδειγμα, έχουμε $\mu\kappa\delta(30, 25, 9) = 1$ και από την άλλη πλευρά $\mu\kappa\delta(30, 25) = 5$, $\mu\kappa\delta(30, 9) = 3$ και $\mu\kappa\delta(25, 9) = 1$.

Θεώρημα 1.3 *Ας είναι $a_1, \ldots, a_n \in \mathbb{Z}\backslash\{0\}$ και $d = \mu\kappa\delta(a_1, \ldots, a_n)$. Τότε υπάρχουν ακέραιοι $k_1, \ldots, k_n$ έτσι, ώστε να ισχύει:*

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

Απόδειξη. Θεωρούμε το σύνολο:

$$\Sigma = \{z_1a_1 + \cdots + z_na_n / \ z_1, \ldots, z_n \in \mathbb{Z}\}.$$

Παρατηρούμε ότι $\pm a_1, \ldots, \pm a_n \in \Sigma$. Συνεπώς, το Σ περιέχει θετικούς ακεραίους. Ας είναι $d = k_1a_1 + \cdots + k_na_n$, όπου $k_1, \ldots, k_n \in \mathbb{Z}$, ο μικρότερος θετικός του Σ. Θα δείξουμε ότι $d = \mu\kappa\delta(\mathrm{a_1}, \ldots, \mathrm{a_n})$.

Ας είναι $z = z_1a_1 + \cdots + z_na_n$ ένα στοιχείο του Σ. Τότε υπάρχουν ακέραιοι q, r έτσι, ώστε $z = dq + r$ με $0 \leq r < d$. Από την άλλη πλευρά, έχουμε:

$$r = z - dq = (z_1 - k_1q)a_1 + \cdots + (z_n - k_nq)a_n$$

και επομένως $r \in \Sigma$. Ας είναι $r > 0$. Τότε, καθώς ο d είναι ο μικρότερος θετικός του Σ, έπεται $r \geq d$ που είναι άτοπο. Άρα $r = 0$ και επομένως $d|z$. Ειδικότερα, $d|a_1, \ldots, d|a_n$. Αν δ είναι ένας θετικός ακέραιος με $\delta|a_1, \ldots, \delta|a_n$, τότε $\delta|k_1a_1, \ldots, \delta|k_na_n$ και επομένως $\delta|d$. Άρα $\delta \leq d$ και επομένως $d = \mu\kappa\delta(a_1, \ldots, a_n)$. □

Πόρισμα 1.2 *Ας είναι d ένας θετικός διαιρέτης των $a_1, \ldots, a_n$. Τότε $d = \mu\kappa\delta(a_1, \ldots, a_n)$, αν και μόνον αν για κάθε θετικό ακέραιο δ με $\delta|a_1, \ldots, \delta|a_n$ έχουμε $\delta|d$.*

Απόδειξη. Ας υποθέσουμε ότι $d = \mu\kappa\delta(a_1, \ldots, a_n)$. Τότε, σύμφωνα με το Θεώρημα 1.3, υπάρχουν ακέραιοι $k_1, \ldots, k_n$ έτσι, ώστε $d = k_1a_1 + \cdots + k_na_n$. Αν δ είναι θετικός ακέραιος με $\delta|a_1, \ldots, \delta|a_n$, τότε $\delta|k_1a_1, \ldots, \ \delta|k_na_n$ και επομένως $\delta|d$. Αντίστροφα, αν για κάθε θετικό ακέραιο δ με $\delta|a_1, \ldots, \delta|a_n$ ισχύει $\delta|d$, τότε $\delta \leq d$ και επομένως $d = \mu\kappa\delta(a_1, \ldots, a_n)$. □

Πρόταση 1.5 *Ας είναι a, b, c μη μηδενικοί ακέραιοι. Αν $a|bc$ και $\mu\kappa\delta(a, b) = 1$, τότε $a|c$.*

Απόδειξη. Καθώς $\mu\kappa\delta(a, b) = 1$, το Θεώρημα 1.3 έπεται ότι υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $1 = ax + by$. Επομένως $c = cax + cby$ και από τη σχέση $a|bc$ παίρνουμε $a|c$. □

Μερικές βασικές ιδιότητες του $\mu\kappa\delta$ δίνονται στην παρακάτω πρόταση.

Πρόταση 1.6 *Αν $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ με $\mu\kappa\delta(a_1, \ldots, a_n) = d$, τότε ισχύουν τα εξής:*
(α) $\mu\kappa\delta(la_1, \ldots, la_n) = |l|d$, όπου $l \in \mathbb{Z} \setminus \{0\}$.
(β) $\mu\kappa\delta(a_1/d, \ldots, a_n/d) = 1$.
(γ) $d = \mu\kappa\delta(a_1 + l_2a_2 + \cdots + l_na_n, a_2 \ldots, a_n)$, όπου $l_2, \ldots, l_n \in \mathbb{Z}$.

Απόδειξη. (α) Καταρχήν παρατηρούμε ότι ο θετικός ακέραιος $d|l|$ διαιρεί τους $la_1, \ldots, la_n$. Σύμφωνα με το Θεώρημα 1.3, υπάρχουν ακέραιοι $k_1, \ldots, k_n$ έτσι, ώστε $d = k_1a_1 + \cdots + k_na_n$. Τότε, ισχύει:

$$|l|d = (ek_1)la_1 + \cdots + (ek_n)la_n,$$

όπου $e = 1$ αν $l > 0$ και $e = -1$ αν $l < 0$. Αν δ είναι ένας θετικός διαιρέτης των $a_1, \ldots, a_n$, τότε $\delta|la_1, \ldots, \delta|la_n$ και κατά συνέπεια $\delta|d|l|$. Έτσι, από το Πόρισμα 1.2, έχουμε $\mu\kappa\delta(la_1, \ldots, la_n) = |l|d$.

(β) Από την (α) έχουμε:

$$d = \mu\kappa\delta(d(a_1/d), \ldots, d(a_n/d)) = d\ \mu\kappa\delta(a_1/d, \ldots, a_n/d))$$

και επομένως $\mu\kappa\delta(a_1/d, \ldots, a_n/d) = 1$.

(γ) Ας είναι $\delta = \mu\kappa\delta(a_1 + l_2a_2 + \cdots + l_na_n, a_2, \ldots, a_n)$. Καθώς $d|a_1, \ldots, d|a_n$ έπεται $d|l_2a_2, \ldots, d|l_na_n$, απ΄ όπου $d|a_1+l_2a_2+\cdots+l_na_n$. Άρα $d|\delta$. Αντίστροφα, έχουμε $\delta|a_1 + l_2a_2 + \cdots + l_na_n$, $\delta|a_2, \ldots, \delta|a_n$. Οπότε $\delta|l_2a_2, \ldots, \delta|l_na_n$ και επομένως $\delta|a_1$. Συνεπώς $\delta|d$. Καθώς $d|\delta$, $\delta|d$ και οι ακέραιοι d και δ ειναι θετικοί, έχουμε $d = \delta$. □

Παράδειγμα 1.17 Ας είναι a και b δύο ακέραιοι πρώτοι μεταξύ τους. Θα δείξουμε ότι $\mu\kappa\delta(a+b, a-b) = 1$ ή 2. Ας είναι $d = \mu\kappa\delta(a+b, a-b)$. Τότε $d|a + b$ και $d|a - b$ και επομένως $d|(a + b) \pm (a - b)$. Άρα $d|2a$ και $d|2b$, απ΄ όπου $d|(2a, 2b)$. Από την Πρόταση 1.3 έχουμε $(2a, 2b) = 2(a, b) = 2$. Έτσι, παίρνουμε $d|2$ και επομένως $d = 1$ ή 2.

Ας είναι $a_1, \ldots, a_n$ $(n \geq 2)$ διακεκριμμένοι ακέραιοι. Καλούμε *κοινό πολλαπλάσιο* των $a_1, \ldots, a_n$ κάθε ακέραιο b με $a_1|b, \ldots, a_n|b$. Αν κάποιος από τους $a_1, \ldots, a_n$ είναι το μηδέν, τότε το μοναδικό κοινό τους πολλαπλάσιο είναι το μηδέν. Έτσι, υποθέτουμε όλοι οι ακέραιοι $a_1, \ldots, a_n$ είναι $\neq 0$. Ο αριθμός $|a_1 \cdots a_n|$ είναι ένα θετικό κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Οπότε, το σύνολο των θετικών κοινών πολλαπλασίων των $a_1, \ldots, a_n$ είναι μη κενό και κατά συνέπεια έχει ελάχιστο στοιχείο. Το μικρότερο θετικό κοινό πολλαπλάσιο των $a_1, \ldots, a_n$

καλείται *ελάχιστο κοινό πολλαπλάσιο* ($\epsilon\kappa\pi$) των $a_1, \ldots, a_n$ και συμβολίζεται με $\epsilon\kappa\pi(a_1, \ldots, a_n)$. Παρατηρούμε ότι το σύνολο των θετικών κοινών πολλαπλασίων των $a_1, \ldots, a_n$ συμπίπτει μ΄ αυτό των $|a_1|, \ldots, |a_n|$ και επομένως $\epsilon\kappa\pi(a_1, \ldots, a_n) = \epsilon\kappa\pi(|a_1|, \ldots, |a_n|)$.

Παράδειγμα 1.18 Θα υπολογίσουμε το $\epsilon\kappa\pi(6, 15, 10)$. Τα θετικά πολλαπλάσια του 6 είναι οι ακέραιοι $6, 12, 18, 24, 30, 36, \ldots$, του 10 οι ακέραιοι $10, 20, 30, 40, \ldots$ και του 15 οι $15, 30, 45, \ldots$. Άρα έχουμε $\epsilon\kappa\pi(6, 15, 10) = 30$.

Πρόταση 1.7 *Ας είναι m θετικό κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Τότε $m = \epsilon\kappa\pi(a_1, \ldots, a_n)$, αν και μόνον αν για κάθε θετικό ακέραιο μ με $a_1|\mu, \ldots, a_n|\mu$ ισχύει $m|\mu$.*

Απόδειξη. Ας υποθέσουμε ότι $m = \epsilon\kappa\pi(a_1, \ldots, a_n)$. Ας είναι μ θετικός ακέραιος μ με $a_1|\mu, \ldots, a_n|\mu$. Τότε υπάρχουν ακέραιοι q, r έτσι, ώστε $\mu = mq + r$ και $0 \leq r < m$. Από τις σχέσεις $a_i|m$ και $a_i|\mu$ $(i = 1, \ldots, n)$, έπεται $a_i|r$ $(i = 1, \ldots, n)$. Έτσι, αν $r \neq 0$, τότε $r \geq m$ που είναι άτοπο. Άρα $r = 0$ και επομένως $m|\mu$. Αντίστροφα, ας υποθέσουμε ότι για κάθε θετικό ακέραιο πολλαπλάσιο μ των $a_1, \ldots, a_n$ ισχύει $m|\mu$. Άρα $m \leq \mu$. Επομένως, ο m είναι το μικρότερο από όλα τα θετικά κοινά πολλαπλάσια των $a_1, \ldots, a_n$ και κατά συνέπεια $m = \epsilon\kappa\pi(a_1, \ldots, a_n)$. □

Η παρακάτω πρόταση συνδέει τον $\mu\kappa\delta$ και το $\epsilon\kappa\pi$ δύο ακεραίων.

Πρόταση 1.8 *Ας είναι a και b δύο ακέραιοι. Τότε:*

$$\mu\kappa\delta(a, b)\epsilon\kappa\pi(a, b) = |ab|.$$

Απόδειξη. Αν $a = 0$ ή $b = 0$, τότε η παραπάνω ισότητα προφανώς ισχύει. Ας υποθέσουμε λοιπόν ότι $a \neq 0$ και $b \neq 0$. Θέτουμε $d = \mu\kappa\delta(a, b)$. Θα δείξουμε ότι $\epsilon\kappa\pi(a, b) = |ab|/d$. Καθώς $d|a$ και $d|b$, ο ακέραιος $|ab|/d$ είναι ένα θετικό κοινό πολλαπλάσιο των a και b. Αν l είναι ένα θετικό κοινό πολλαπλάσιο των a και b, τότε ο $|ab|$ διαιρεί τους al, bl και επομένως τον $\mu\kappa\delta(la, lb)$. Από την Πρόταση 1.6(α) έχουμε $\mu\kappa\delta(la, lb) = ld$ και κατά συνέπεια ο ακέραιος $|ab|/d$ διαιρεί τον l. Άρα $\epsilon\kappa\pi(a, b) = |ab|/d$. □

Παράδειγμα 1.19 Θα προσδιορίσουμε όλους τους ακέραιους a, b με $0 < a < b$, $ab = 51840$ και $\epsilon\kappa\pi(a, b) = 2160$. Ας είναι $d = \mu\kappa\delta(a, b)$.

Τότε $a = dx$, $b = dy$, όπου $x, y \in \mathbb{Z}$ με $\mu\kappa\delta(x, y) = 1$. Από την Πρόταση 1.8, έχουμε $\delta\epsilon\kappa\pi(a, b) = ab$. Επομένως $2160 = \epsilon\kappa\pi(a, b) = dxy$. Από την άλλη πλευρά, έχουμε $51840 = ab = d^2xy$. Συνδυάζοντας τις δύο ισότητες παίρνουμε $d = 24$. Οπότε $xy = 90$. Καθώς $\mu\kappa\delta(x, y) = 1$ και $x < y$, έχουμε $(x, y) = (1, 90), (2, 45), (9, 10), (5, 18)$. Επομένως $(a, b) = (24, 2160), (48, 1080), (120, 432), (216, 240)$.

1.6 Ευκλείδειος Αλγόριθμος

Σ′ αυτή την ενότητα θα μελετήσουμε έναν αλγόριθμο για την εύρεση του μεγίστου κοινού διαιρέτη δύο ακεραίων που οφείλεται στον Ευκλείδη. Ας υποθέσουμε λοιπόν ότι θέλουμε να υπολογίσουμε τον μέγιστο κοινό διαιρέτη d των ακεραίων a και b. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $a > b > 0$. Θέτουμε $r_0 = a$ και $r_1 = b$. Σύμφωνα με το Θεώρημα 1.1, υπάρχουν ζεύγη ακεραίων (q_i, r_{i+1}) $(i = 1, \ldots, n)$ έτσι, ώστε να ισχύει:

$$r_{i-1} = r_i q_i + r_{i+1} \quad \text{και} \quad 0 \leq r_{i+1} < r_i$$

Οπότε, παίρνουμε:

$$0 \leq r_{n+1} < r_n < r_{n-1} < \ldots < r_2 < r_1.$$

Αν για κάθε ακέραιο $n \geq 1$ το υπόλοιπο r_{n+1} είναι $\neq 0$, τότε μεταξύ του 0 και του b θα υπήρχε άπειρο πλήθος διακεκριμμένων ακεραίων που είναι αδύνατο. Άρα, για κάποιο δείκτη n θα έχουμε $r_j \neq 0$ $(j = 2, \ldots, n)$ και $r_{n+1} = 0$. Από την Πρόταση 1.6(γ), έπεται:

$$d = \mu\kappa\delta(r_1, r_2) = \ldots = \mu\kappa\delta(r_{n-1}, r_n) = \mu\kappa\delta(r_n q_n, r_n) = r_n.$$

Η κατάστρωση του παραπάνω συστήματος Ευκλειδείων διαιρέσεων μέχρι του δείκτη n για τον οποίο ισχύει $r_j \neq 0$ $(j = 2, \ldots, n)$ και $r_{n+1} = 0$ καλείται *Ευκλείδειος αλγόριθμος* για τους ακέραιους a και b.

Παράδειγμα 1.20 Θα προσδιορίσουμε τον μέγιστο κοινό διαιρέτη των 576 και 123. Σύμφωνα με τα παραπάνω έχουμε:

$$\begin{aligned} 576 &= 123 \cdot 4 + 84, \\ 123 &= 84 \cdot 1 + 39, \\ 84 &= 39 \cdot 2 + 6, \\ 39 &= 6 \cdot 6 + 3 \\ 6 &= 3 \cdot 2. \end{aligned}$$

Άρα $\mu\kappa\delta(576, 123) = 3$.

Ο χρόνος που απαιτείται για την εκτέλεση της διαίρεσης του r_{k-1} με τον r_k είναι $O(\ell(r_k)(\ell(r_{k-1}) - \ell(r_k)))$. Άρα, ο συνολικός χρόνος που απαιτείται για την εκτέλεση όλων των διαιρέσεων είναι:

$$\begin{aligned} O\left(\sum_{k=1}^{n} \ell(r_k)(\ell(r_{k-1}) - \ell(r_k))\right) &= O\left(\ell(b)\sum_{k=1}^{n}(\ell(r_{k-1}) - \ell(r_k)\right) \\ &= O((\ell(b)\ell(a)). \end{aligned}$$

Συνεπώς, ο χρόνος που χρειάζεται για να εκτελεστεί ο Ευκλείδειος αλγόριθμος είναι $O(\ell(a)\ell(b))$. Επίσης, από την Πρόταση 1.8 έπεται ότι χρόνος για τον υπολογισμό του ελαχίστου κοινού πολλαπλασίου των a και b είναι $O(\ell(a)\ell(b))$.

Παρατηρούμε ότι $q_k \geq 1$ για $1 \leq k < n$ και $q_n \geq 2$. Πράγματι, καθώς $r_{k-1} > r_k > r_{k+1}$, έπεται ότι $q_k \geq 1$ για $1 \leq k \leq n$. Αν $q_n = 1$, τότε $r_{n-1} = r_n$ που είναι άτοπο. Συνεπώς $q_n \geq 2$.

Παρατήρηση 1.1 Αν $a < b$, τότε η πρώτη Ευκλείδεια διαίρεση είναι $b = a0 + b$, απ΄ όπου $q_1 = 0$, και στην συνέχεια εφαρμόζουμε τον Ευκλείδειο αλγόριθμο όπως παραπάνω.

Πρόταση 1.9 *Ας είναι $\Phi = (1 + \sqrt{5})/2$. Αν n είναι το πλήθος των βημάτων που χρειάζεται ο Ευκλείδειος αλγόριθμος για τον υπολογισμό του μεγίστου κοινού διαιρέτη d των a και b, τότε ισχύει:*

$$n \leq \frac{\log b}{\log \Phi} + 1.$$

Απόδειξη. Θ΄ αποδείξουμε με επαγωγή ότι $r_{n-k} \geq \Phi^k$. Για $k = 0, 1$, έχουμε:

$$r_n \geq 1 = \Phi^0, \quad r_{n-1} = q_n r_n \geq q_n \geq 2 > \Phi.$$

Ας υποθέσουμε ότι η ανισότητα αληθεύει για κάθε $l < k$. Τότε, ισχύει:

$$r_{n-k} = q_{n-(k-1)} r_{n-(k-1)} + r_{n-(k-2)} \geq r_{n-(k-1)} + r_{n-(k-2)}.$$

Οπότε, από την υπόθεση της επαγωγής, έχουμε:

$$r_{n-k} \geq \Phi^{k-1} + \Phi^{k-2} = \Phi^{k-1}\left(1 + \frac{1}{\Phi}\right) = \Phi^k.$$

Η παραπάνω ανισότητα για $k = n - 1$ δίνει $b = r_1 \geq \Phi^{n-1}$, απ' όπου παίρνουμε $n \leq (\log b / \log \Phi) + 1$. $\square$

Στη συνέχεια δίνουμε παρακάτω ένα παράδειγμα ακεραίων $a \geq b$ όπου το πλήθος των βημάτων του Ευκλείδειου αλγορίθμου είναι ακριβώς $\lfloor \log b / \log \Phi \rfloor + 1$.

Παράδειγμα 1.21 Η ακολουθία των αριθμών του Fibonacci (F_n) ορίζεται ως εξής:

$$F_0 = 0,\ F_1 = 1,\ F_k = F_{k-1} + F_{k-2},\quad k \geq 2.$$

Καθώς $F_{j-1} < F_j$, παρατηρούμε ότι η ακολουθία των ισοτήτων

$$F_k = F_{k-1} + F_{k-2} \quad (k = n+1, \ldots, 2)$$

δεν είναι παρά η κατάστρωση του Ευκλειδείου αλγόριθμου για τον υπολογισμό του μεγίστου κοινού διαιρέτη των F_n και F_{n+1}. Έτσι, έχουμε:

$$\mu\kappa\delta(F_n, F_{n+1}) = 1.$$

Το πλήθος των βημάτων που εκτέλεσε ο Ευκλείδειος αλγόριθμος είναι n. Θα δείξουμε ότι ισχύει:

$$n = \left\lfloor \frac{\log F_n}{\log \Phi} \right\rfloor + 1.$$

Πρώτα όμως θα αποδείξουμε ότι ισχύει η εξής ισότητα:

$$F_n = \frac{\Phi^n - (-\Phi)^{-n}}{\sqrt{5}}.$$

Θα εφαρμόσουμε επαγωγή επί του n. Για $n = 0$ και $n = 1$ επαληθεύουμε αμέσως την ισότητα. Υποθέτουμε ότι η παραπάνω ισότητα ισχύει για $n = k - 1, k$. Τότε, από την υπόθεση επαγωγής, έχουμε:

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} \\ &= \frac{1}{\sqrt{5}} \left(\Phi^k - (-\Phi)^{-k} + \Phi^{k-1} - (-\Phi)^{-(k-1)} \right) \\ &= \frac{1}{\sqrt{5}} \left(\Phi^{k-1}(\Phi + 1) - (-\Phi)^{-(k-1)}((-\Phi)^{-1} + 1) \right) \end{aligned}$$

Καθώς ισχύει $\Phi^2 - \Phi - 1 = 0$, παίρνουμε $\Phi + 1 = \Phi^2$ και $(-\Phi)^{-1} + 1 = \Phi^{-2}$. Έτσι, έχουμε:

$$F_{k+1} = \frac{\Phi^{k+1} - (-\Phi)^{-(k+1)}}{\sqrt{5}}.$$

Συνεπώς, η προς απόδειξη ισότητα ισχύει.

Στη συνέχεια, έχουμε:

$$\begin{aligned}
n &\leq \frac{\log F_n}{\log \Phi} + 1 \\
&= \frac{1}{\log \Phi} \log \left(\frac{\Phi^n - (-\Phi)^{-n}}{\sqrt{5}} \right) + 1 \\
&= \frac{1}{\log \Phi} \log(\Phi^n - (-\Phi)^{-n}) - \frac{\log \sqrt{5}}{\log \Phi} + 1 \\
&< \frac{1}{\log \Phi} \log(\Phi^n + 1) - \frac{\log \sqrt{5}}{\log \Phi} + 1 \\
&< \frac{1}{\log \Phi} \left(\log(\Phi^n) + \frac{1}{\Phi^n} \right) - \frac{\log \sqrt{5}}{\log \Phi} + 1 \\
&< n + \frac{1}{\Phi^n \log \Phi} - \frac{\log \sqrt{5}}{\log \Phi} + 1 \\
&< n + 1.
\end{aligned}$$

Επομένως, παίρνουμε:

$$n = \left\lfloor \frac{\log F_n}{\log \Phi} \right\rfloor + 1.$$

Σύμφωνα με το Θεώρημα 1.3 υπάρχουν ακέραιοι u, v έτσι, ώστε $ua + vb = d$. Η παρακάτω πρόταση μας δίνει μία μέθοδο για τον υπολογισμό των u και v.

Ορίζουμε ακεραίους $s_0, \ldots, s_{n+1}$ και $t_0, \ldots, t_{n+1}$ ως εξής:

$$s_0 = 1,\ s_1 = 0,\ t_0 = 0,\ t_1 = 1,$$

και για $i = 1, \ldots, n$,

$$s_{i+1} = s_{i-1} - s_i q_i, \quad t_{i+1} = t_{i-1} - t_i q_i.$$

Πρόταση 1.10 *Ισχύουν τα παρακάτω:*
(α) Για $i = 0, \ldots, n+1$, $s_i a + t_i b = r_i$. *Ειδικότερα,* $s_n a + t_n b = d$.
(β) Για $i = 0, \ldots, n$, $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$.
(γ) Για $i = 1, \ldots, n$, $t_i t_{i+1} \leq 0$, $|t_i| \leq |t_{i+1}|$, $s_i s_{i+1} \leq 0$, $|s_i| \leq |s_{i+1}|$.
(δ) Για $i = 0, \ldots, n+1$, $r_{i-1}|t_i| \leq a$, $r_{i-1}|s_i| \leq b$.

Απόδειξη. (α) Για $i = 0, 1$ η ισότητα είναι προφανής. Υποθέτουμε ότι για $i = 2, \ldots, k-1$ η ισότητα ισχύει. Τότε για $i = k$ έχουμε:

$$\begin{aligned} s_k a + t_k b &= (s_{k-2} - s_{k-1}q_{k-1})a + (t_{k-2} - t_{k-1}q_{k-1})b \\ &= (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)q_{k-1} \\ &= r_{k-2} - r_{k-1}q_{k-1} = r_k. \end{aligned}$$

(β) Για $i = 0$ η ισότητα είναι προφανής. Υποθέτουμε ότι για $i = 1, \ldots, k-1$ η ισότητα αληθεύει. Για $i = k$ έχουμε:

$$\begin{aligned} s_k t_{k+1} - t_k s_{k+1} &= s_k(t_{k-1} - t_k q_k) - t_k(s_{k-1} - s_k q_k), \\ &= -(s_{k-1}t_k - t_{k-1}s_k), \\ &= -(-1)^{k-1} = (-1)^k. \end{aligned}$$

(γ) Για $i = 0$ έχουμε $t_0 t_1 = 0$ και $|t_0| < t_1$. Ας υποθέσουμε ότι για κάθε $i \leq k$ ισχύουν οι ανισότητες. Έχουμε $t_{k+1} = t_{k-1} - t_k q_k$ και $t_{k-1}t_k < 0$, $|t_{k-1}| \leq |t_k|$. Οπότε ισχύει:

$$|t_{k+1}| = |t_{k-1}| + |t_k|q_k \geq |t_k|$$

και το πρόσημο του t_{k+1} διαφέρει από αυτό του t_k. Όμοια αποδεικνύεται ότι $s_i s_{i+1} \leq 0$ και $|s_i| \leq |s_{i+1}|$.

(δ) Θεωρούμε τις ισότητες:

$$s_{i-1}a + t_{i-1}b = r_{i-1}, \quad s_i a + t_i b = r_i.$$

Έχουμε:

$$\begin{aligned} t_i r_{i-1} - t_{i-1} r_i &= t_i(s_{i-1}a + t_{i-1}b) - t_{i-1}(s_i a + t_i b), \\ &= (t_i s_{i-1} - t_{i-1}s_i)a, \\ &= (-1)^{i+1}a. \end{aligned}$$

Καθώς τα t_i και t_{i-1} έχουν αντίθετα πρόσημα, έπεται:

$$a = |t_i r_{i-1} - t_{i-1} r_i| \geq |t_i| r_{i-1}.$$

Ανάλογα δουλεύουμε και για την απόδειξη της δεύτερης ανισότητας. □

Από την παραπάνω πρόταση έχουμε:

$$|s_i| \leq b/r_{n-1}, \quad |t_i| \leq a/r_{n-1} \quad (i = 1, \ldots, n)$$

και

$$s_n a + t_n b = d.$$

Στη συνέχεια θα υπολογίσουμε τον χρόνο εύρεσης των s_n και t_n. Έχουμε $s_2 = s_0 - s_1 q_1 = 1$, $t_2 = t_0 - t_1 q_1 = -q_1$ και επομένως ο χρόνος υπολογισμού των s_2 και t_2 είναι $O(\ell(q_1))$. Επίσης, ο χρόνος υπολογισμού κάθε ζεύγους

$$s_{i+1} = s_{i-1} - s_i q_i, \quad t_{i+1} = t_{i-1} - t_i q_i \quad (i = 2, \ldots, n-1)$$

είναι $O(\ell(a)\ell(q_i))$. Άρα ο χρόνος υπολογισμού όλων των s_i, t_i είναι:

$$\begin{aligned} O\left(\ell(q_1) + \sum_{i=2}^{n-1} \ell(a)\ell(q_i)\right) &= O\left(\ell(a)(1 + \sum_{i=2}^{n-1} \ell(q_i))\right), \\ &= O\left(\ell(a)(n + \sum_{i=2}^{n-1} \log q_i)\right), \\ &= O(\ell(a)(n + \log(q_2 \cdots q_n)). \end{aligned}$$

Έχουμε $q_2 \cdots q_n \leq b$ και από την Πρόταση 1.9 έπεται $n = O(\log b)$. Άρα ο χρόνος υπολογισμού των s_n και t_n είναι $O(\ell(a)\ell(b))$.

Ο Ευκλείδειος αλγόριθμος μαζί με τη διαδικασία εύρεσης των ακεραίων u, v καλείται *εκτεταμένος Ευκλείδειος αλγόριθμος*.

Παράδειγμα 1.22 Θα συνεχίσουμε το Παράδειγμα 1.20 και θα χρησιμοποιήσουμε την Πρόταση 1.10 για να υπολογίσουμε ακεραίους s, t τέτοιους ώστε να ισχύει $576s + 123t = 3$. Από το Παράδειγμα 1.20, έχουμε $q_1 = 4$, $q_2 = 1$, $q_3 = 2$, $q_4 = 6$ και $q_4 = 2$. Έτσι παίρνουμε:

$$(s_0, t_0) = (1, 0), \quad (s_1, t_1) = (0, 1), \quad (s_2, t_2) = (1, -4),$$

$$(s_3, t_3) = (-1, 5), \quad (s_4, t_4) = (3, -14), \quad (s_5, t_5) = (-19, 89).$$

Επομένως, οι ζητούμενοι ακεραίοι είναι $s = -19$ και $t = 89$.

Συνοψίζουμε τις παραπάνω διαδικασίες στον επόμενο αλγόριθμο:

Αλγόριθμος 1.4 Εκτεταμένος Ευκλείδειος Αλγόριθμος.
Είσοδος: $a > b > 0$.
Έξοδος: (d, s, t), όπου $d = \mu\kappa\delta(a, b)$ και $s, t \in \mathbb{Z}$ με $sa + tb = d$.

1. Θέτουμε $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$.

2. Για $j = 0, 1, \ldots$ κάνουμε τα εξής:

   (α′) Αν $r_{j+1} = 0$, τότε εξάγουμε την τριάδα (r_j, s_j, t_j).

   (β′) Αν όχι, υπολογίζουμε ακεραίους q_{j+1}, r_{j+2} με

   $$r_j = r_{j+1}q_{j+1} + r_{j+2} \quad \text{και} \quad 0 \leq r_{j+2} < r_{j+1}.$$

   και

   $$s_{j+1} = s_{j-1} - s_j q_j, \quad t_{j+1} = t_{j-1} - t_j q_j.$$

Έτσι, έχουμε το εξής θεώρημα:

Θεώρημα 1.4 *Ας είναι a, b ακέραιοι. Ο χρόνος εκτέλεσης του εκτεταμένου Ευκλείδειου αλγορίθμου για την εύρεση του μεγίστου κοινού διαιρέτη d των a, b και ακεραίων u, v με $|u| \leq |b|$ και $|v| \leq |a|$ έτσι, ώστε*

$$au + bv = d$$

είναι $O(\ell(a)\ell(b))$ δυαδικές ψηφιακές πράξεις.

Πόρισμα 1.3 *Ας είναι a και b δύο ακέραιοι. Ο χρόνος ο οποίος απαιτείται για την εύρεση του ελαχίστου κοινού πολλαπλασίου των a, b είναι $O(\ell(a)\ell(b))$.*

Απόδειξη. Από την Πρόταση 1.8 έχουμε ότι $\epsilon\kappa\pi(a, b) = |ab|/\mu\kappa\delta(a, b)$. Έτσι, ο χρόνος υπολογισμού του $\epsilon\kappa\pi(a, b)$ ισούται με το άθροισμα του χρόνου υπολογισμού των ποσοτήτων $|ab|$, $\mu\kappa\delta(a, b)$ και του πηλίκου τους. Άρα, ο υπολογισμός του $\epsilon\kappa\pi(a, b)$ απαιτεί χρόνο $O(\ell(a)\ell(b))$. □

Μία εφαρμογή του Θεωρήματος 1.4 είναι το επόμενο αποτέλεσμα το οποίο μας δίνει ένα τρόπο υπολογισμού όλων των ακεραίων x και y με $d = ax + by$.

Πρόταση 1.11 *Ας είναι $a, b, c \in \mathbb{Z}$ με $a \neq 0$, $b \neq 0$ και $d = \mu\kappa\delta(a, b)$. Η εξίσωση*

$$ax + by = c$$

έχει λύση $(x, y) \in \mathbb{Z}^2$, αν και μόνον αν $d|c$. Σ΄ αυτή την περίπτωση, αν $(x_0, y_0) \in \mathbb{Z}^2$ είναι μία λύση της, τότε όλες οι λύσεις $(x, y) \in \mathbb{Z}^2$ δίνονται από τις σχέσεις:

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

Απόδειξη. Ας υποθέσουμε ότι $d|c$. Τότε $c = ed$, όπου $e \in \mathbb{Z}$. Από την άλλη πλευρά, σύμφωνα με το Θεώρημα 1.4, υπάρχουν $x, y \in \mathbb{Z}$ με $d = ax + by$. Έτσι, έχουμε $a(ex) + b(ey) = c$ και επομένως το ζεύγος (ex, ey) είναι μία λύση της παραπάνω εξίσωσης. Αντίστροφα, αν $(x_0, y_0) \in \mathbb{Z}^2$ είναι μία λύση, τότε $ax_0 + by_0 = c$. Καθώς $d|a$ και $d|b$ προκύπτει $d|c$.

Θέτουμε $a = da'$ και $b = db'$, όπου $a', b' \in \mathbb{Z}$ και $\mu\kappa\delta(a', b') = 1$. Ας είναι $(x_0, y_0) \in \mathbb{Z}^2$ μία λύση της εξίσωσης. Για κάθε $t \in \mathbb{Z}$ έχουμε:

$$a(x_0 + b't) + b(y_0 - a't) = ax_0 + by_0 + ab't - ba't = c$$

και επομένως τα ζεύγη ακεραίων $(x_0 + b't, y_0 - a't)$, $t \in \mathbb{Z}$, είναι λύσεις της εξίσωσης. Ας είναι $(x', y') \in \mathbb{Z}$ μία λύση της εξίσωσης. Τότε:

$$ax_0 + by_0 = c = ax' + by'$$

απ΄ όπου:

$$a(x' - x_0) = b(y_0 - y')$$

και επομένως:

$$a'(x' - x_0) = b'(y_0 - y').$$

Άρα $a'|b'(y_0 - y')$. Καθώς $\mu\kappa\delta(a', b') = 1$, έχουμε $a'|y_0 - y'$. Έτσι, παίρνουμε $y_0 - y' = a't$ και $x' - x_0 = b't$, για κάποιο $t \in \mathbb{Z}$. □

Παράδειγμα 1.23 Θα βρούμε όλα τα ζεύγη ακεραίων που ικανοποιούν την εξίσωση

$$576x + 123y = 2.$$

Από τα Παραδείγματα 1.10 και 1.12 έχουμε $\mu\kappa\delta(576, 123) = 3$ και $3 = (-19) \cdot 576 + 89 \cdot 123$. Πολλαπλασιάζοντας και τα δύο μέλη της

προηγούμενης ισότητας με 2 βλέπουμε ότι το ζεύγος $(-38, 178)$ επαληθεύει την παραπάνω εξίσωση. Έτσι, από την Πρόταση 1.8 έπεται ότι τα ζεύγη ακεραίων (x, y) που ικανοποιούν την εξίσωση δίνονται από τις σχέσεις:

$$x = -38 + 41t, \quad y = 178 - 192t, \quad t \in \mathbb{Z}.$$

1.7 Ασκήσεις

1. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύουν τα εξής:

(α) $9|2^{4n+1} - 2^{2n} - 1$,

(β) $27|10^n + 18n - 1$,

(γ) $169|3^{3n+3} - 26n - 27$.

2. Να προσδιοριστούν οι θετικοί ακέραιοι a ο οποίοι διαιρούμενοι με τον 53 δίνουν πηλίκο ένα πολλαπλάσιο του 7 και υπόλοιπο το τετράγωνο του πηλίκου.

3. Να προσδιοριστούν όλοι οι θετικοί ακέραιοι a με $2|a+3$ και $a-2|20$.

4. Υπάρχει θετικός ακέραιος x τέτοιος ώστε $(57)_x + (33)_x = (112)_x$;

5. Να βρεθεί ο θετικός ακέραιος x με $(4x3)_5 = (x30)_9$.

6. Να δειχθεί ότι το πλήθος των πολυωνύμων $P(T)$ βαθμού $\leq n-1$ με ακέραιους συντελεστές μεταξύ του 0 και του n είναι $O(n^n)$.

7. Ας είναι n θετικός ακέραιος. Να εκτιμηθεί με τη βοήθεια μίας απλής συνάρτησης του n και τη χρήση του O-συμβολισμού, το πλήθος των δυαδικών ψηφιακών πράξεων που απαιτούνται για τον υπολογισμό του 3^n στο δυαδικό σύστημα. Να γίνει το ίδιο για τον ακέραιο n^n.

8. Θεωρούμε τον τύπο:

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Να εκτιμηθεί με τη βοήθεια μίας απλής συνάρτησης του n και τη χρήση του O-συμβολισμού, ο χρόνος που απαιτείται για να πραγματοποιηθεί ο υπολογισμός του αθροίσματος στο αριστερό μέρος της ισότητας. Να γίνει το ίδιο και για το δεξί μέρος.

9. Η ακολουθία των αριθμών του Fibonacci (F_n) ορίζεται ως εξής:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2},\ \ n \geq 2.$$

Να δειχθεί ότι ο F_k υπολογίζεται σε χρόνο $O(k^2)$.

10. Για κάθε φυσικό k να δειχθεί ότι $n^k = O(2^n)$.

11. Ας είναι d ένας θετικός διαιρέτης των ακεραίων $a_1, \ldots, a_n$. Τότε $d = \mu\kappa\delta(a_1, \ldots, a_n)$, αν και μόνον αν υπάρχουν ακέραιοι $k_1, \ldots, k_n$ με

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

12. Να εφαρμοστεί ο εκτεταμένος Ευκλείδειος αλγόριθμος για τον υπολογισμό του μεγίστου κοινού διαιρέτη d των ακεραίων 391 και 323, και την εύρεση των λύσεων της εξίσωσης

$$391x + 323y = d.$$

13. Να δειχθεί με ένα παράδειγμα ότι γενικά για $n \geq 3$ δεν ισχύει η εξής ισότητα:

$$\mu\kappa\delta(a_1, \ldots, a_n)\epsilon\kappa\pi(a_1, \ldots, a_n) = |a_1 \cdots a_n|.$$

14. Ας είναι $a_1, \ldots, a_n, b_1, \ldots, b_n$ ακέραιοι τέτοιοι, ώστε

$$a_1 b_1 = \ldots = a_n b_n = l \neq 0.$$

Να δειχθεί ότι ισχύει:

$$\epsilon\kappa\pi(a_1, \ldots, a_n)\mu\kappa\delta(b_1, \ldots, b_n) = |l|.$$

15. Ας είναι a, b, c περιττοί ακέραιοι και $d = \mu\kappa\delta(a, b, c)$. Να δειχθεί ότι

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

16. Να προσδιοριστούν όλοι οι ακέραιοι αριθμοί a με $a-3|a^3-3$.

17. Ας είναι $a_1,\ldots,a_n \in \mathbb{Z}\setminus\{0\}$ $(n\geq 3)$ με $\mu\kappa\delta(a_1,\ldots,a_n)=d$. Να δειχθεί ότι ισχύει:

$$d=\mu\kappa\delta(a_1,\ldots,a_\nu,\mu\kappa\delta(a_{\nu+1},\ldots,a_n)),$$

όπου $1\leq\nu\leq n-2$.

18. Ας είναι $a_1,\ldots,a_n \in \mathbb{Z}\setminus\{0\}$ $(n\geq 3)$ και $\epsilon\kappa\pi(a_1,\ldots,a_n)=m$. Να δειχθεί ότι ισχύουν τα εξής:
(α) $\epsilon\kappa\pi(la_1,\ldots,la_n)=|l|m$, όπου $l\in\mathbb{Z}\setminus\{0\}$.
(β) $\mu\kappa\delta(m/a_1,\ldots,m/a_n)=1$.
(γ) $m=\epsilon\kappa\pi(a_1,\ldots,a_\nu,\epsilon\kappa\pi(a_{\nu+1},\ldots,a_n))$, όπου $1\leq\nu\leq n-2$.

Βιβλιογραφία

[1] T. M. Apostol, *Εισαγωγή στην Αναλυτική Θεωρία Αριθμών,* Gutenberg 1986.

[2] E. Bach and J. Shallit, *Algorithmic Number Theory,* MIT Press, Cambridge, Massachusetts and London, England, 1996.

[3] M. W. Baldoni, C. Ciliberto and G. M. Piacentini Cattaneo, *Elementary Number Theory, Cryptography and Codes,* Springer-Verlag 2009.

[4] J. Buhler and S. Wagon, *Basic algorithms in number theory,* in Arithmetic Number Theory, MSRI Publications, Volume 44, 2008.

[5] T. H. Cormen, C. E. Leiserson and R. L. Rivest, *Introduction to Algorithms,* MIT Press, Cambridge, Massachusetts 1990.

[6] R. Crandall, *Topics in Advanced Scientific Computation*, TELOS/Springer-Verlag 1996.

[7] S. Dasgupta, C. Papadimitriou and U. Vazirani, *Algorithms,* Mc Graw Hill 2006.

[8] M. Fürer, Faster integer multiplication, *SIAM J. Comp.,* 39(3), (2009) 979-1005.

[9] V. Shoup, *Μία Υπολογιστική Εισαγωγή στη Θεωρία Αριθμών και την Άλγεβρα,* Εκδόσεις Κλειδάριθμος 2007.

[10] S. Y. Yan, *Number Theory for Computing,* Berlin, Heidelberg, Springer Verlag 2002.

[11] Δ. Πουλάκης, *Θεωρία Αριθμών*, Θεσσαλονίκη, Εκδόσεις Ζήτη 2001.

Κεφάλαιο 2

Συνεχή Κλάσματα

Σύνοψη
Σ' αυτή την ενότητα θα αντιστοιχήσουμε τους πραγματικούς αριθμούς με ακολουθίες ακεραίων δια μέσου της παράστασής τους σε συνεχές κλάσμα. Θα παρουσιάσουμε την ανάπτυξη των ρητών και αρρήτων αριθμών σε συνεχή κλασματα και θα εξετάσουμε τις βασικές ιδιότητές των. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να συμβουλευτεί τα εξής συγγράμματα: [1, 2, 3]

Προαπαιτούμενη γνώση
Κεφάλαιο 1.

2.1 Πεπερασμένα Συνεχή Κλάσματα

Καλούμε *πεπερασμένο συνεχές κλάσμα τάξης* n κάθε παράσταση της μορφής

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots \\ \qquad b_{n-1} + \cfrac{1}{b_n}}},$$

όπου $b_0, \ldots, b_n$ είναι πραγματικοί αριθμοί με $b_0 \geq 0$ και $b_i > 0$ $(i = 1, \ldots, n)$. Για συντομία, το παραπάνω συνεχές κλάσμα συμβολίζεται με

$$< b_0, \ldots, b_n > .$$

Ας είναι ρ ένας θετικός ρητός. Τότε υπάρχουν θετικοί ακέραιοι a, b πρώτοι μεταξύ τους έτσι, ώστε $\rho = a/b$. Εφαρμόζουμε τον Ευκλείδειο αλγόριθμο στους a και b. Έχουμε λοιπόν ακεραίους q_j $(j = 1, \ldots, n)$ και r_j $(j = 0, \ldots, n+1)$ τέτοιους, ώστε

$$r_{k-1} = q_k r_k + r_{k+1}, \quad 0 \leq r_{k+1} < r_k,$$

$r_0 = a$, $r_1 = b$, $r_n = 1$ και $r_{n+1} = 0$. Επίσης, ισχύει $q_1 > 0$ αν $\rho > 1$ και $q_1 = 0$ αν $\rho < 1$. Στην πρώτη περίπτωση έχουμε $n \leq 1 + \log b / \log \Phi$ ενώ στη δεύτερη $n - 1 \leq 1 + \log a / \log \Phi$. Οπότε, προκύπτει το παρακάτω ανάπτυγμα του ρ σε συνεχές κλάσμα:

$$\rho =< q_1, \ldots, q_n > .$$

Καθώς $q_n \geq 2$, προκύπτει και η εξής παράσταση του ρ σε συνεχές κλάσμα:

$$\rho =< q_1, \ldots, q_n - 1, 1 > .$$

Προφανώς, από τη μία από αυτές τις δύο παραστάσεις μπορούμε να πάρουμε αμέσως την άλλη. Από την προηγούμενη ενότητα συνάγεται ότι ο χρόνος που χρειάζεται για τον υπολογισμό των q_i $(i = 1, \ldots, n)$ και επομένως του συνεχούς κλάσματος του ρ είναι $O(\ell(a)\ell(b))$.

Ας υποθέσουμε τώρα ότι ο ρ έχει δύο παραστάσεις σε συνεχές κλάσμα της πρώτης μορφής. Δηλαδή, έχουμε:

$$< r_1, \ldots, r_k >= \rho =< s_1, \ldots, s_l >,$$

με $r_k \geq 2$ και $s_l \geq 2$. Ας υποθέσουμε $k \leq l$. Θα δείξουμε ότι $k = l$ και $r_i = s_i$ $(i = 1, \ldots, k)$. Θέτουμε:

$$x_i =< r_i, \ldots, r_k > \quad (i = 1, \ldots, k),$$

και

$$y_j =< s_j, \ldots, s_l > \quad (j = 1, \ldots, l).$$

Οποτε, έχουμε:

$$x_i = r_i + \frac{1}{x_{i+1}} \quad (i = 1, \ldots, k-1)$$

και

$$y_j = s_j + \frac{1}{s_{j+1}} \quad (j = 1, \ldots, l-1).$$

Καθώς $x_i > 0$ $(i = 2, \ldots, k)$, παίρνουμε $x_i > r_i \geq 1$ $(i = 2, \ldots, k-1)$. Επίσης, $x_k = r_k \geq 2$. Επομένως, έχουμε $\lfloor x_i \rfloor = r_i$ $(i = 1, \ldots, k-1)$. Όμοια, ισχύει: $\lfloor y_j \rfloor = s_j$ $(j = 1, \ldots, l-1)$ και $y_l = s_l \geq 2$. Από την ισότητα $x_1 = \rho = y_1$ παίρνουμε:

$$r_1 = \lfloor x_1 \rfloor = \lfloor y_1 \rfloor = s_1.$$

Υποθέτουμε ότι $x_\mu = y_\mu$ και $r_\mu = s_\mu$. Τότε:

$$\frac{1}{x_{\mu+1}} = x_\mu - r_\mu = y_\mu - s_\mu = \frac{1}{y_{\mu+1}},$$

απ΄ όπου $x_{\mu+1} = y_{\mu+1}$ και επομένως $r_\mu = \lfloor x_{\mu+1} \rfloor = \lfloor y_{\mu+1} \rfloor = s_{\mu+1}$. Άρα, για $i = 1, \ldots, k$, ισχύει $x_i = y_i$ και $r_i = s_i$. Αν $k < l$, τότε:

$$s_k < y_k = x_k = r_k = s_k$$

που είναι άτοπο. Συνεπώς $k = l$.

Παράδειγμα 2.1 Θα υπολογίσουμε τα αναπτύγματα σε συνεχές κλάσμα των ρητών $251/39$ και $47/151$. Αναπτύσσουμε τον Ευκλείδειο αλγόριθμο για τους ακεραίους 251, 39 και παίρνουμε:

$$\begin{aligned} 251 &= 39 \cdot 6 + 17 \\ 39 &= 17 \cdot 2 + 5 \\ 17 &= 5 \cdot 3 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2. \end{aligned}$$

Επομένως, τα δύο αναπτύγματα σε συνεχές κλάσμα του $251/39$ είναι:

$$251/39 =< 6, 2, 3, 2, 2 >=< 6, 2, 3, 2, 1, 1 > .$$

Επίσης, για τους ακέραιους 47, 151 έχουμε:

$$\begin{aligned} 47 &= 151 \cdot 0 + 47 \\ 151 &= 47 \cdot 3 + 10 \\ 47 &= 10 \cdot 4 + 7 \\ 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3. \end{aligned}$$

Συνεπώς, τα δύο αναπτύγματα σε συνεχές κλάσμα του $47/151$ είναι:

$$47/151 =< 0, 3, 4, 1, 2, 3 >=< 0, 3, 4, 1, 2, 2, 1 > .$$

Ας είναι $\rho =< a_0, \ldots, a_m >$. Οι *συγκλίνοντες ρητοί* στο ρ είναι τα κλάσματα

$$\frac{P_i}{Q_i} =< a_0, \ldots, a_i > \quad (i = 0, 1 \ldots, m),$$

όπου P_i, Q_i είναι ακέραιοι πρώτοι μεταξύ τους.

Πρόταση 2.1 *Ισχύουν τα παρακάτω:*
(α) Οι ακέραιοι P_i, Q_i ικανοποιούν τους αναγωγικούς τύπους:

$$P_0 = a_0, \quad P_1 = a_0a_1 + 1, \quad Q_0 = 1, \quad Q_1 = a_1,$$

$$P_k = a_kP_{k-1} + P_{k-2}, \quad Q_k = a_kQ_{k-1} + Q_{k-2} \quad (k = 2, \ldots, m).$$

(β) Για $k = 0, \ldots, m-1$ έχουμε:

$$P_kQ_{k+1} - P_{k+1}Q_k = (-1)^{k+1}.$$

(γ) Για $k = 0, \ldots, m-1$ ισχύει:

$$P_kQ_{k+2} - P_{k+2}Q_k = (-1)^{k+1}a_{k+2}.$$

Απόδειξη. (α) Θα αποδείξουμε με επαγωγή τους δύο τύπους. Εύκολα επαληθεύουμε ότι ισχύουν για $k = 0, 1, 2$. Στη συνέχεια υποθέτουμε ότι ισχύουν για $k = l - 1 \geq 2$. Ας είναι

$$\frac{r_j}{s_j} =< a_1, \ldots, a_{j+1} >, \quad (j = 0, \ldots, m-1),$$

όπου r_j, s_j είναι θετικοί ακέραιοι πρώτοι μεταξύ τους. Η υπόθεση της επαγωγής δίνει:

$$r_{l-1} = a_lr_{l-2} + r_{l-3}, \quad s_{l-1} = a_ls_{l-2} + s_{l-3}.$$

Έχουμε:

$$\frac{P_j}{Q_j} =< a_0, \ldots, a_j >= a_0 + \frac{1}{< a_1, \ldots, a_j >} = a_0 + \frac{1}{r_{j-1}/s_{j-1}},$$

απ΄ όπου προκύπτει:

$$P_j = a_0r_{j-1} + s_{j-1}, \quad Q_j = r_{j-1}.$$

Θέτοντας $j = l$ παίρνουμε:

$$P_l = a_0 r_{l-1} + s_{l-1} = a_l(a_0 r_{l-2} + s_{l-2}) + a_0 r_{l-3} + s_{l-3}$$

και

$$Q_l = a_l r_{l-2} + r_{l-3}.$$

Επίσης, για $j = l-1$ και $j = l-2$ παίρνουμε:

$$P_{l-1} = a_0 r_{l-2} + r_{l-2}, \quad Q_{l-1} = r_{l-2}$$

και

$$P_{l-2} = a_0 r_{l-3} + r_{l-3}, \quad Q_{l-2} = r_{l-3}.$$

Έτσι, έχουμε:

$$P_l = a_l P_{l-1} + P_{l-2}, \quad Q_l = a_l Q_{l-1} + Q_{l-2}.$$

Συνεπώς, οι δύο ισότητες ισχύουν για κάθε $k = 0, 1, \ldots, m$.

(β) Θα εφαρμόσουμε επαγωγή. Για $k = 0$ ισχύει:

$$P_0 Q_1 - P_1 Q_0 = a_0 - (a_0 a_1 + 1) = -1.$$

Υποθέτουμε ότι η ισότητα αληθεύει για $k = l-1$. Έχουμε:

$$\begin{aligned} P_l Q_{l+1} - P_{l+1} Q_l &= P_l(a_{l+1} Q_l + Q_{l-1}) - (a_{l+1} P_l + P_{l-1}) Q_l \\ &= -P_{l-1} Q_l + P_l Q_{l-1} \\ &= (-1)^{l+1}. \end{aligned}$$

Συνεπώς, η προς απόδειξη ισχύει.

(γ) Χρησιμοποιώντας τα παραπάνω παίρνουμε:

$$\begin{aligned} P_k Q_{k+2} - P_{k+2} Q_k &= P_k(a_{k+2} Q_{k+1} + Q_k) - (a_{k+2} P_{k+1} + P_k) Q_k \\ &= a_{k+2}(P_k Q_{k+1} - Pk + 1 Q_k) \\ &= a_{k+2}(-1)^{k+1}. \quad \square \end{aligned}$$

Ας είναι $\rho = a/b$, όπου a, b θετικοί ακέραιοι, πρώτοι μεταξύ τους. Θεωρούμε το ανάπτυγμα σε συνεχές κλάσμα $\rho =< q_1, \ldots, q_n >$, όπου $q_1, \ldots, q_n$ είναι τα διαδοχικά πηλίκα που προκύπτουν από την εφαρμογή του Ευκλειδείου αλγορίθμου επί των a και b (με αυτή τη σειρά). Θα προσδιορίσουμε τον χρόνο που χρειάζεται για τον υπολογισμό των

συγκλινόντων ρητών P_i/Q_i στο ρ. Καθώς $P_{n-1}/Q_{n-1} = a/b$, έπεται $P_{n-1} = a$ και $Q_{n-1} = b$. Άρα, $P_i \leq a$ και $Q_i \leq b$. Έτσι, για τον υπολογισμό κάθε ζεύγους P_i, Q_i $(i = 2, \ldots, n-1)$ απαιτείται χρόνος

$$O(\ell(q_{i+1})\ell(P_{i-1}) + \ell(Q_{i-1}))) = O(\ell(q_{i+1})(\ell(a) + \ell(b))).$$

Οπότε, ο χρόνος που χρειάζεται για τον υπολογισμό όλων των ζευγών P_i, Q_i $(i = 2, \ldots, n-1)$ είναι:

$$\begin{aligned} &O((\ell(q_3) + \cdots + \ell(q_n))(\ell(a) + \ell(b))) = \\ &\quad O((n + \log q_3 + \cdots + \log q_n)(\ell(a) + \ell(b))). \end{aligned}$$

Καθώς $n = O(\min\{\log a, \log b\})$ και $q_3 \cdots q_n \leq \min\{a, b\}$, συνάγεται ότι ο παραπάνω χρόνος ισούται με $O(\ell(a)\ell(b))$. Επίσης, ο υπολογισμός των ζευγών P_0, P_1 και Q_0, Q_1 γίνεται στον ίδιο χρόνο. Τέλος, στην περίπτωση όπου θεωρήσουμε το ανάπτυγμα $\rho =< q_1, \ldots, q_n - 1, 1 >$ βρίσκουμε επίσης τον ίδιο χρόνο.

Συνοψίζουμε όλα τα παραπάνω στο εξής θεώρημα:

Θεώρημα 2.1 *Αν είναι $\rho = a/b$, όπου a, b θετικοί ακέραιοι, πρώτοι μεταξύ τους. Επίσης, αν είναι $q_1, \ldots, q_n$ τα διαδοχικά πηλίκα που προκύπτουν από την εφαρμογή του Ευκλειδείου αλγορίθμου επί των a και b (με αυτή τη σειρά). Τότε οι μοναδικές παραστάσεις του ρ σε συνεχές κλάσμα είναι $\rho =< q_1, \ldots, q_n >$ και $\rho =< q_1, \ldots, q_n - 1, 1 >$. Ο χρόνος που απαιτείται για τον υπολογισμό αυτών των αναπτυγμάτων και όλων των συγκλινόντων ρητών στο ρ είναι $O(\ell(a)\ell(b))$.*

2.2 Άπειρα Συνεχή Κλάσματα

Ας είναι $a_0, a_1, a_2, \ldots$ μία ακολουθία ακεραίων με $a_k > 0$ $(k = 1, 2 \ldots)$. Θεωρούμε τα κλάσματα:

$$\frac{P_k}{Q_k} =< a_0, \ldots, a_k > \quad (k = 0, 1, 2 \ldots),$$

όπου P_k, Q_k είναι ακέραιοι πρώτοι μεταξύ τους. Καθώς για κάθε $n > 1$, τα κλάσματα P_k/Q_k $(k = 0, 1, \ldots, n)$ είναι οι συγκλίνοντες ρητοί στο P_n/Q_n, οι ακέραιοι P_k, Q_k ικανοποιούν τους αναγωγικούς τύπους της Πρότασης 2.1:

$$P_0 = a_0, \quad P_1 = a_0 a_1 + 1, \quad Q_0 = 1, \quad Q_1 = a_1,$$

$$P_k = a_k P_{k-1} + P_{k-2}, \quad Q_k = a_k Q_{k-1} + Q_{k-2} \quad (k = 2, 3 \ldots).$$

Επίσης, για κάθε $k = 0, 1, \ldots$, ισχύουν οι ισότητες:

$$P_k Q_{k+1} - P_{k+1} Q_k = (-1)^{k+1}$$

και

$$P_k Q_{k+2} - P_{k+2} Q_k = (-1)^{k+1} a_{k+2}.$$

Έχουμε:

$$\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{(-1)^{k+1}}{Q_k Q_{k+1}},$$

απ΄ όπου

$$\frac{P_k}{Q_k} = a_0 + \sum_{j=1}^{k} \frac{(-1)^{j+1}}{Q_j Q_{j-1}}.$$

Δηλαδή, το κλάσμα P_k/Q_k είναι το μερικό άθροισμα της σειράς

$$a_0 + \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{Q_j Q_{j-1}}$$

η οποία είναι εναλλάσσουσα. Καθώς η ακολουθία (Q_n) είναι γνησίως αύξουσα η σειρά αυτή, σύμφωνα με το κριτήριο του Leibnitz, συγκλίνει σ΄ ένα πραγματικό αριθμό x. Συνεπώς έχουμε:

$$\lim_{k \to \infty} \frac{P_k}{Q_k} = x.$$

Έτσι λοιπόν εισάγουμε την παράσταση:

$$< a_0, a_1, \ldots >= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

η οποία καλείται *άπειρο συνεχές κλάσμα* και ορίζεται να είναι

$$x =< a_0, a_1, \ldots > .$$

Καλούμε *συγκλίνοντες ρητούς* στο παραπάνω άπειρο συνεχές κλάσμα τα κλάσματα P_k/Q_k $(k = 0, 1, 2 \ldots)$.

Πρόταση 2.2 *Ισχύει:*

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \ldots < \frac{P_{2k}}{Q_{2k}} < x < \frac{P_{2k+1}}{Q_{2k+1}} < \ldots < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.$$

Επιπλέον, ο αριθμός x είναι άρρητος.

Απόδειξη. Οι ισότητες

$$P_kQ_{k+1} - P_{k+1}Q_k = (-1)^{k+1}, \quad P_kQ_{k+2} - P_{k+2}Q_k = (-1)^{k+1}a_{k+2}$$

δίνουν τις σχέσεις:

$$\frac{P_{2k}}{Q_{2k}} < \frac{P_{2k+1}}{Q_{2k+1}}, \quad \frac{P_{2k}}{Q_{2k}} < \frac{P_{2k+2}}{Q_{2k+2}}, \quad \frac{P_{2k+1}}{Q_{2k+1}} > \frac{P_{2k+3}}{Q_{2k+3}}.$$

Οι ακολουθίες P_{2k}/Q_{2k} και P_{2k+1}/Q_{2k+1} είναι γνησίως μονότονες, φραγμένες και συγκλίνουν στο x. Επομένως, $x > P_{2k}/Q_{2k}$ και $x < P_{2k+1}/Q_{2k+1}$ $(k = 0, 1, 2, \ldots)$.

Ας υποθέσουμε ότι $x = a/b$, όπου a και b ακέραιοι πρώτοι μεταξύ τους. Για κάθε $k = 0, 1, 2, \ldots$ έχουμε:

$$0 < \left| x - \frac{P_k}{Q_k} \right| < \left| \frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} \right| = \frac{1}{Q_kQ_{k+1}}.$$

Πολλαπλασιάζοντας με bQ_k παίρνουμε:

$$0 < |aQ_k - P_kb| < \frac{b}{Q_{k+1}}.$$

Επειδή η ακολουθία Q_k $(k = 1, 2, \ldots)$ είναι γνησίως αύξουσα, υπάρχει δείκτης k με $b < Q_{k+1}$ και επομένως έχουμε $0 < |aQ_k - P_kb| < 1$ που είναι άτοπο. Άρα ο αριθμός x είναι άρρητος. □

Ας είναι θ ένας πραγματικός αριθμός. Θέτουμε $\lfloor \theta \rfloor = a_0$. Αν $\theta \neq a_0$ τότε γράφουμε $\theta = a_0 + 1/\theta_1$, με $\theta_1 > 1$. Θέτουμε $a_1 = \lfloor \theta_1 \rfloor$. Πάλι, αν $\theta_1 \neq a_1$, τότε $\theta_1 = a_1 + 1/\theta_2$, με $\theta_2 > 1$. Συνεχίζοντας αυτή τη διαδικασία παίρνουμε θετικούς ακέραιους $a_1, a_2, \ldots$ και θετικούς πραγματικούς $\theta_1, \theta_2, \ldots$ έτσι, ώστε

$$\theta =< a_0, a_1, \ldots, a_{n-1}, \theta_n > .$$

Η διαδικασία αυτή σταματά αν και μόνον αν υπάρχει n τέτοιο ώστε $a_n = \theta_n$. Τότε $\theta =< a_0, \ldots, a_n >$ με $a_n \geq 2$ και $\theta_n = a_n$. Αυτό

όμως συμβαίνει αν και μόνον αν ο θ είναι ρητός. Σ' αυτή την περίπτωση παρατηρούμε ότι η προηγούμενη διαδικασία δεν είναι παρά η ανάπτυξη του θ σε συνεχές κλάσμα. Οι αριθμοί a_n και θ_n καλούνται *n-στο μερικό πηλίκο* και *n-στο πλήρες πηλίκο* του θ, αντίστοιχα.

Ας είναι P_i/Q_i $(i = 0, 1, \ldots)$ οι συγκλίνοντες ρητοί στο συνεχές κλάσμα που δημιουργείται από τους αριθμούς $a_0, a_1, \ldots$. Η παρακάτω πρόταση συνδέει τον θ με τους συγκλίνοντες ρητούς και τα πλήρη πηλίκα του.

Πρόταση 2.3 *Για κάθε $k \geq 1$ έχουμε:*

$$\theta = \frac{P_k\theta_{k+1} + P_{k-1}}{Q_k\theta_{k+1} + Q_{k-1}}.$$

Απόδειξη. Για $k = 1$ η Πρόταση 2.1 δίνει:

$$\theta =< a_0, a_1, \theta_2 >= \frac{(a_0a_1 + 1)\theta_2 + a_0}{a_1\theta_2 + 1} = \frac{P_1\theta_2 + P_0}{Q_1\theta_2 + Q_0}.$$

Υποθέτουμε ότι η ισότητα ισχύει για $k = l-1$. Καθώς $\theta_l = a_l + 1/\theta_{l+1}$, έχουμε:

$$\begin{aligned}\theta = \frac{P_{l-1}\theta_l + P_{l-2}}{Q_{l-1}\theta_l + Q_{l-2}} &= \frac{(a_l + 1/\theta_{l+1})P_{l-1} + P_{l-2}}{(a_l + 1/\theta_{l+1})Q_{l-1} + Q_{l-2}} \\ &= \frac{(a_lP_{l-1} + P_{l-2})\theta_{l+1} + P_{l-1}}{(a_lQ_{l-1} + Q_{l-2})\theta_{l+1} + Q_{l-1}}.\end{aligned}$$

Έτσι, παίρνουμε:

$$\theta = \frac{P_l\theta_{l+1} + P_{l-1}}{Q_l\theta_{l+1} + Q_{l-1}}.$$

Συνεπώς, η ισότητα ισχύει για κάθε $k \geq 1$. □

Ας υποθέσουμε τώρα ότι ο θ είναι άρρητος. Τότε από την παραπάνω διαδικασία παίρνουμε το άπειρο συνεχές κλάσμα $< a_0, a_1, \ldots >$. Θα δείξουμε ότι ισχύει $\theta =< a_0, a_1, \ldots >$. Από την Πρόταση 2.3 έχουμε:

$$\begin{aligned}\theta - \frac{P_k}{Q_k} &= \frac{P_k\theta_{k+1} + P_{k-1}}{Q_k\theta_{k+1} + Q_{k-1}} - \frac{P_k}{Q_k} \\ &= \frac{P_{k-1}Q_k - P_kQ_{k-1}}{Q_k(Q_k\theta_{k+1} + Q_{k-1})} \\ &= \frac{(-1)^k}{Q_k(Q_k\theta_{k+1} + Q_{k-1})},\end{aligned}$$

απ΄ όπου παίρνουμε:

$$\left|\theta - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k^2}.$$

Επομένως, καθώς η ακολουθία Q_k $(k \geq 0)$ είναι γνησίως αύξουσα, προκύπτει:

$$\lim_{k\to\infty} \frac{P_k}{Q_k} = \theta.$$

Συνεπώς, $\theta =< a_0, a_1, \ldots >$.

Ας υποθέσουμε στη συνέχεια ότι

$$< a_0, a_1, \ldots >= \theta =< b_0, b_1, \ldots > .$$

Θα δείξουμε ότι $a_i = b_i$ $(i = 0, 1, \ldots)$. Έχουμε $a_0 < \theta < a_0 + 1/a_1$, απ΄ όπου έπεται $\lfloor\theta\rfloor = a_0$. Όμοια, ισχύει $\lfloor\theta\rfloor = b_0$. Συνεπώς, έχουμε $a_0 = b_0$. Υποθέτουμε ότι $a_i = b_i$ $(i = 1, \ldots, k)$. Τότε παίρνουμε:

$$< a_{k+1}, a_{k+2}, \ldots >=< b_{k+1}, b_{k+2}, \ldots > .$$

Αν x είναι η τιμή του παραπάνω συνεχούς κλάσματος, τότε έχουμε $a_{k+1} = \lfloor x\rfloor = b_{k+1}$. Συνεπώς, ισχύει $a_i = b_i$ $(i = 0, 1, \ldots)$.

Συνοψίζουμε τα παραπάνω στο εξής θεώρημα:

Θεώρημα 2.2 *Κάθε πραγματικός άρρητος αριθμός θ αναλύεται με μοναδικό τρόπο σε άπειρο συνεχές κλάσμα.*

Παράδειγμα 2.2 Θα υπολογίσουμε το ανάπτυγμα σε συνεχές κλάσμα του $\sqrt{2}$. Έχουμε:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{1/(\sqrt{2} - 1)} = 1 + \frac{1}{\sqrt{2} + 1},$$

και

$$\sqrt{2} + 1 = 2 + (\sqrt{2} - 1) = 2 + \frac{1}{\sqrt{2} + 1}.$$

Έτσι, το ανάπτυγμα σε συνεχές κλάσμα του $\sqrt{2}$ είναι:

$$\sqrt{2} =< 1, 2, 2, \ldots > .$$

2.3 Προσέγγιση Άρρητου από Ρητούς

Σ′ αυτή την παράγραφο θα δώσουμε μερικές ιδιότητες της προσέγγισης ενός πραγματικού αριθμού θ από τους συγκλίνοντες ρητούς του, P_n/Q_n.

Πρόταση 2.4 *Για κάθε $n \geq 1$ ισχύει*

$$|Q_n\theta - P_n| < |Q_{n-1}\theta - P_{n-1}|.$$

Απόδειξη. Ας είναι a_n $(n = 0, 1, \ldots)$ τα μερικά πηλίκα και θ_n $(n = 1, 2, \ldots)$ τα πλήρη πηλίκα του θ. Ας είναι $n \geq 1$. Τότε έχουμε:

$$\begin{aligned} |Q_n\theta - P_n| &= \left| \frac{Q_n(P_n\theta_{n+1} + P_{n-1})}{Q_n\theta_{n+1} + Q_{n-1}} - P_n \right| \\ &= \left| \frac{Q_nP_{n-1} - Q_{n-1}P_n}{Q_n\theta_{n+1} + Q_{n-1}} \right| \\ &= \frac{1}{Q_n\theta_{n+1} + Q_{n-1}}. \end{aligned}$$

Από την άλλη πλευρά, παίρνουμε:

$$Q_n\theta_{n+1} + Q_{n-1} > Q_n + Q_{n-1} = (a_n + 1)Q_{n-1} + Q_{n-2}.$$

Έχουμε:

$$a_n + 1 = \theta_n + 1 - \frac{1}{\theta_{n+1}} > \theta_n,$$

απ′ όπου έπεται:

$$Q_n\theta_{n+1} + Q_{n-1} > (a_n + 1)Q_{n-1} + Q_{n-2} > \theta_nQ_{n-1} + Q_{n-2}$$

Επομένως, ισχύει:

$$|Q_n\theta - P_n| = \frac{1}{Q_n\theta_{n+1} + Q_{n-1}} < \frac{1}{\theta_nQ_{n-1} + Q_{n-2}} = |Q_{n-1}\theta - P_{n-1}|.$$

□

Η παρακάτω πρόταση δείχνει ότι οι συγκλίνοντες ρητοί προσεγγίζουν τον θ καλύτερα από οποιοδήποτε άλλον ρητό.

Πρόταση 2.5 *Ας είναι P και Q ακέραιοι με $0 < Q < Q_{n+1}$ και $(P, Q) \neq (P_n, Q_n)$. Τότε, ισχύει:*

$$|Q\theta - P| > |Q_n\theta - P_n|.$$

Απόδειξη. Θεωρούμε το γραμμικό σύστημα:

$$P_n x + P_{n+1} y = P, \quad Q_n x + Q_{n+1} y = Q.$$

Η λύση του είναι:

$$x = (-1)^{n+1}(PQ_{n+1} - QP_{n+1}), \quad y = (-1)^{n+1}(P_nQ - Q_nP).$$

Αν $x = 0$, τότε $P/Q = P_{n+1}/Q_{n+1}$. Καθώς $\mu\kappa\delta(P_{n+1}, Q_{n+1}) = 1$, έχουμε $Q_{n+1}|Q$ που είναι άτοπο γιατί $Q < Q_{n+1}$. Άρα $x \neq 0$. Ας είναι $y \neq 0$. Από τις σχέσεις $Q < Q_{n+1}$ και $Q_n x + Q_{n+1} y = Q$ έπεται ότι οι ακέραιοι x και y έχουν διαφορετικό πρόσημο. Από την άλλη πλευρά, από την Πρόταση 2.2 προκύπτει ότι οι $Q_n\theta - P_n$ και $Q_{n+1}\theta - P_{n+1}$ έχουν διαφορετικό πρόσημο. Επομένως, οι αριθμοί $x(Q_n\theta - P_n)$ και $y(Q_{n+1}\theta - P_{n+1})$ έχουν το ίδιο πρόσημο και κατά συνέπεια παίρνουμε:

$$|Q\theta - P| = |x(Q_n\theta - P_n) + y(Q_{n+1}\theta - P_{n+1})| > |Q_n\theta - P_n|.$$

Τέλος, αν $y = 0$, τότε έχουμε $Q_n x = Q$ και $P_n x = P$ με $x > 1$. Έτσι, παίρνουμε:

$$|Q\theta - P| = x|Q_n\theta - P_n| > |Q_n\theta - P_n|. \quad \square$$

Χρησιμοποιώντας τα παραπάνω, θα δείξουμε μία ικανή συνθήκη για να είναι ένα κλάσμα συγκλίνων ρητός σ΄ ένα πραγματικό αριθμό.

Πρόταση 2.6 *Ας είναι θ ένας θετικός πραγματικός αριθμός και P, Q θετικοί ακέραιοι, πρώτοι μεταξύ τους, με*

$$\left|\theta - \frac{P}{Q}\right| < \frac{1}{2Q^2}.$$

Τότε ο P/Q είναι ένας συγκλίνων ρητός στο θ.

Απόδειξη. Έχουμε $Q_n \leq Q < Q_{n+1}$, για κάποιο δείκτη n. Ας υποθέσουμε ότι $(P, Q) \neq (P_n, Q_n)$. Τότε από την Πρόταση 2.5 έχουμε: $|Q\theta - P| > |Q_n\theta - P_n|$. Έτσι παίρνουμε:

$$\left|\frac{P}{Q} - \frac{P_n}{Q_n}\right| \leq \left|\theta - \frac{P}{Q}\right| + \left|\theta - \frac{P_n}{Q_n}\right| < |Q\theta - P| \left(\frac{1}{Q} + \frac{1}{Q_n}\right).$$

Χρησιμοποιώντας στη συνέχεια τις ανισότητες $Q_n < Q$ και $|Q\theta - P| < 1/2Q$ προκύπτει:

$$\left|\frac{P}{Q} - \frac{P_n}{Q_n}\right| < \frac{1}{QQ_n},$$

απ' όπου έπεται $|PQ_n - QP_n| < 1$ και επομένως $(P, Q) = (P_n, Q_n)$ που είναι άτοπο. Έτσι, έχουμε $P/Q = P_n/Q_n$. □

2.4 Τετραγωνικοί Άρρητοι

Ας είναι $a_0, a_1, a_2, \ldots$ μία ακολουθία ακεραίων με $a_n > 0$ $(n = 1, 2 \ldots)$. Η ακολουθία (a_n) καλείται *περιοδική*, αν υπάρχουν φυσικοί m και k έτσι, ώστε να ισχύει $a_{m+n} = a_n$ για κάθε $n \geq k$. Αν οι φυσικοί m και k είναι οι μικρότεροι με αυτή την ιδιότητα, τότε η ακολουθία είναι:

$$a_0, \ldots, a_{k-1}, a_k, \ldots, a_{k+m-1}, a_k, \ldots, a_{k+m-1}, a_k, \ldots.$$

Ο φυσικός m καλείται *περίοδος* της ακολουθίας. Στη περίπτωση όπου $k = 0$, η (a_n) καλείται *γνήσια περιοδική*. Αν θ είναι ο πραγματικός άρρητος που αντιστοιχεί στην ακολουθία (a_n), τότε θα γράφουμε:

$$\theta = < a_0, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}} > .$$

Ο πραγματικός αριθμός θ καλείται *τετραγωνικός άρρητος*, αν είναι ρίζα μίας εξίσωσης της μορφής

$$ax^2 + bx + c = 0$$

με $a, b, c \in \mathbb{Z}$ και διακρίνουσα $d = b^2 - 4ac > 0$ η οποία δεν είναι τέλειο τετράγωνο. Τότε:

$$\theta = \frac{A + \sqrt{d}}{B},$$

όπου $A, B \in \mathbb{Z}$ και $B \neq 0$. Επίσης, θα γράφουμε:

$$\bar{\theta} = \frac{A - \sqrt{d}}{B}.$$

Αν $\eta_i = (Z_i - \sqrt{d})/H_i$ $(i = 1, 2)$, με $H_i \neq 0$, τότε εύκολα διαπιστώνουμε ότι ισχύουν τα εξής:

$$\overline{\eta_1 \pm \eta_2} = \bar{\eta}_1 \pm \bar{\eta}_2, \quad \overline{\eta_1 \eta_2} = \bar{\eta}_1 \, \bar{\eta}_2.$$

Ας είναι a_n και θ_n το n-μερικό πηλίκο και n-στο πλήρες πηλίκο του θ, αντίστοιχα. Θέτουμε $\theta_0 = \theta$. Θεωρούμε την ακολουθία:

$$A_0 = A, \quad B_0 = b,$$

και για κάθε $k \geq 1$,

$$A_{k+1} = a_k B_k - A_k, \quad B_{k+1} = \frac{d - A_{k+1}^2}{B_k}.$$

Πρόταση 2.7 *Για κάθε $k = 0, 1, \ldots$ έχουμε:*

$$\theta_k = \frac{A_k + \sqrt{d}}{B_k}, \quad a_k = \left\lfloor \frac{A_k + \sqrt{d}}{B_k} \right\rfloor.$$

Απόδειξη. Η πρόταση αληθεύει για $k = 0$. Ας υποθέσουμε ότι ισχύει για τον δείκτη k. Έχουμε:

$$\theta_k = a_k + \frac{1}{\theta_{k+1}},$$

απ΄ όπου

$$\begin{aligned}
\theta_{k+1} &= \frac{1}{\theta_k - a_k} \\
&= \frac{1}{(A_k + \sqrt{d})/B_k - a_k} \\
&= \frac{B_k}{A_k + \sqrt{d} - B_k a_k} \\
&= \frac{B_k}{\sqrt{d} - A_{k+1}} \\
&= \frac{B_k(\sqrt{d} + A_{k+1})}{d - A_{k+1}^2} \\
&= \frac{\sqrt{d} + A_{k+1}}{B_{k+1}}. \quad \square
\end{aligned}$$

Στο Παράδειγμα 2.2 είδαμε ότι $\sqrt{2} =< 1, \bar{2} >$. Στο επόμενο θεώρημα θα δείξουμε ότι οι περιοδικές ακολουθίες αντιστοιχούν στους τετραγωνικούς άρρητους.

Θεώρημα 2.3 *Ας είναι $\theta \in \mathbb{R}$. Ο θ είναι τετραγωνικός άρρητος αν και μόνον αν η ακολουθία (a_n) είναι περιοδική.*

Για την απόδειξη του θεωρήματος θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 2.1 *Ας είναι θ ένας τετραγωνικός άρρητος. Τότε υπάρχει ένας ακέραιος N τέτοιος, ώστε για κάθε $k \geq N$, έχουμε $\theta_k > 1$ και $-1 < \bar{\theta}_k < 0$.*

Απόδειξη. Ας είναι P_k/Q_k $(k = 0, 1, \ldots)$ οι συγκλίνοντες ρητοί στο θ. Σύμφωνα με την Πρόταση 2.3, για κάθε $k \geq 1$ έχουμε:

$$\theta = \frac{P_k\theta_{k+1} + P_{k-1}}{Q_k\theta_{k+1} + Q_{k-1}},$$

απ΄ όπου έπεται:

$$\bar{\theta} = \frac{P_k\bar{\theta}_{k+1} + P_{k-1}}{Q_k\bar{\theta}_{k+1} + Q_{k-1}}.$$

Από την παραπάνω σχέση παίρνουμε:

$$\bar{\theta}_{k+1} = -\frac{Q_{k-1}}{Q_k}\ \frac{\bar{\theta} - P_{k-1}/Q_{k-1}}{\bar{\theta} - P_k/Q_k}.$$

Καθώς $\lim_{k\to\infty} P_k/Q_k = \theta$, προκύπτει:

$$\lim_{k\to\infty} \bar{\theta}_{k+1}\frac{Q_k}{Q_{k-1}} = -1.$$

Συνεπώς, για k αρκετά μεγάλο έχουμε $\bar{\theta}_k < 0$. Επίσης, έχουμε:

$$\bar{\theta}_{k+1} = \frac{1}{\bar{\theta}_k - a_k}$$

και επειδή $a_k \geq 1$ συμπεραίνουμε ότι $-1 < \bar{\theta}_{k+1} < 0$. $\square$

Απόδειξη του Θεωρήματος 2.3. Σύμφωνα με το Λήμμα 2.1 υπάρχει ένας ακέραιος N τέτοιος, ώστε για κάθε $k \geq N$, να ισχύει $\theta_k > 1$ και $-1 < \bar{\theta}_k < 0$. Έτσι, από την Πρόταση 2.7, για κάθε $k \geq N$ έχουμε:

$$\theta_k = \frac{A_k + \sqrt{d}}{B_k} > 1$$

και

$$-1 < \bar{\theta}_k = \frac{A_k - \sqrt{d}}{B_k} < 0.$$

Από την πρώτη ανισότητα παίρνουμε:

$$B_k < A_k + \sqrt{d}.$$

Επίσης, αφαιρώντας την δεύτερη ανισότητα από την πρώτη προκύπτει $2\sqrt{d}/B_k > 0$ και επομένως $B_k > 0$. Έχουμε:

$$A_{k+1} = a_k B_k - A_k < \theta_k B_k - A_k = \sqrt{d}.$$

Επομένως, για κάθε $k > N$ ισχύει $A_k < \sqrt{d}$. Έτσι, για κάθε $k > N$ παίρνουμε:

$$B_k < A_k + \sqrt{d} < 2\sqrt{d}.$$

Επιπλέον, από την ανισότητα $-1 < (A_k - \sqrt{d})/B_k < 0$ έπεται:

$$A_k > -B_k + \sqrt{d} > -\sqrt{d}.$$

Δείξαμε λοιπόν ότι ισχύουν οι ανισότητες

$$0 < B_k < 2\sqrt{d}, \quad -\sqrt{d} < A_k < \sqrt{d}.$$

Συνεπώς, το πλήθος των διαφορετικών ζευγών (A_k, B_k) είναι πεπερασμένο και επομενως το συνεχές κλάσμα του θ, μετά από κάποιο δείκτη, είναι περιοδικό.

Αντίστροφα, ας υποθέσουμε ότι

$$\theta =< a_0, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}} > .$$

Τότε, έχουμε:

$$\theta =< a_0, \ldots, a_k, \theta_{k+1} >$$

και

$$\theta_{k+1} =< \overline{a_{k+1}, \ldots, a_{k+m}} > .$$

Οπότε, ισχύει:

$$\theta_{k+1} =< a_{k+1}, \ldots, a_{k+m}, \theta_{k+1} >$$

και από την Πρόταση 2.3 παίρνουμε:

$$\theta_{k+1} = \frac{a\theta_{k+1} + b}{c\theta_{k+1} + d},$$

όπου $a, b, c, d \in \mathbb{Z}$. Επομένως, το θ_{k+1} ικανοποιεί μία εξίσωση δευτέρου βαθμού με ακέραιους συντελεστές. Από την άλλη πλευρά, έχουμε:

$$\theta = \frac{a'\theta_{k+1} + b'}{c'\theta_{k+1} + d'},$$

όπου $a', b', c', d' \in \mathbb{Z}$. Έτσι, καθώς ο θ_{k+1} είναι τετραγωνικός άρρητος, εύκολα συμπεραίνουμε ότι ο θ είναι επίσης τετραγωνικός άρρητος. □

Στη συνέχεια θα δούμε σε ποιές περιπτώσεις το ανάπτυγμα σε συνεχές κλάσμα ενός τετραγωνικού άρρητο δίνεται από μία γνήσια περιοδική ακολουθία. Γι' αυτό τον σκοπό θα χρειαστούμε το εξής λήμμα.

Λήμμα 2.2 *Ας είναι θ ένας τετραγωνικός άρρητος με $\theta > 1$ και $-1 < \bar{\theta} < 0$. Αν $\theta = a + 1/y$ με $\lfloor \theta \rfloor = a$, τότε $y > 1$ και $-1 < \bar{y} < 0$.*

Απόδειξη. Από την σχέση $1/y = \theta - a < 1$ έχουμε $y > 1$. Από την άλλη πλευρά έχουμε:

$$\bar{\theta} = a + \frac{1}{\bar{y}}.$$

Οπότε, οι ανισότητες $-1 < \bar{\theta} < 0$ δίνουν:

$$-1 - a < \frac{1}{\bar{y}} = \bar{\theta} - a < -a.$$

Καθώς $\theta > 1$ και $y > 1$ έχουμε $a \geq 1$ και κατά συνέπεια $1/\bar{y} < -1$. Άρα, ισχύει:

$$-1 < \bar{y} < 0. \quad \square$$

Πρόταση 2.8 *Ας είναι θ ένας τετραγωνικός άρρητος. Η ακολουθία (a_n) είναι γνήσια περιοδική αν και μόνον αν $\theta > 1$ και $-1 < \bar{\theta} < 0$.*

Απόδειξη. Ας υποθέσουμε ότι η (a_n) είναι γνήσια περιοδική. Τότε $a_0 = a_{k+1}$ για κάποιο δείκτη $k \geq 0$. Άρα $a_0 > 1$ και επομένως $\theta > 1$. Επίσης, έχουμε $\theta = \theta_{k+1}$ και έτσι, από την Πρόταση 2.3, παίρνουμε:

$$\theta = \frac{P_k\theta + P_{k-1}}{Q_k\theta + Q_{k-1}},$$

όπου P_k/Q_k είναι ο k-στός συγκλίνων ρητός στο θ. Επομένως, ο θ είναι ρίζα της εξίσωσης

$$f(x) = Q_k x^2 + (Q_{k-1} - P_k)x - P_{k-1} = 0.$$

Ο $\bar{\theta}$ είναι η δεύτερη ρίζα αυτής της εξίσωσης. Καθώς έχουμε $f(0) = -P_{k-1} < 0$ και $f(-1) = Q_k - Q_{k-1} + P_k - P_{k-1} > 0$ συμπεραίνουμε ότι $-1 < \bar{\theta} < 0$.

Αντίστροφα, ας είναι $\theta > 1$ και $-1 < \bar{\theta} < 0$. Τότε, από το Λήμμα 2.2 έχουμε ότι για κάθε $k \geq 1$ ισχύει $-1 < \bar{\theta}_k < 0$. Η ισότητα $\theta_k = a_k + 1/\theta_{k+1}$ δίνει $\bar{\theta}_k = a_k + 1/\bar{\theta}_{k+1}$ και επομένως $a_k = \lfloor -1/\bar{\theta}_{k+1} \rfloor$. Από την άλλη πλευρά, σύμφωνα με το Θεώρημα 2.3, υπάρχουν δείκτες $n > m$ έτσι, ώστε $\theta_n = \theta_m$. Άρα έχουμε $1/\bar{\theta}_n = 1/\bar{\theta}_m$, απ' όπου $a_{n-1} = a_{m-1}$. Επομένως, παίρνουμε:

$$\theta_{n-1} = a_{n-1} + \frac{1}{\theta_n} = a_{m-1} + \frac{1}{\theta_m} = \theta_{m-1}.$$

Συνεχίζοντας αυτή την διαδικασία, προκύπτει $\theta = \theta_{n-m}$ και κατά συνέπεια η ακολουθία (a_n) είναι γνήσια περιοδική. □

Πόρισμα 2.1 *Ας είναι d ένας ακέραιος > 1, ελεύθερος τετραγώνου. Τότε το ανάπτυγμα σε συνεχές κλάσμα του αριθμού $\sqrt{d}$ είναι της μορφής $\sqrt{d} =< \lfloor \sqrt{d} \rfloor, \overline{a_1, \ldots, a_m} >$.*

Απόδειξη. Έχουμε $\lfloor \sqrt{d} \rfloor + \sqrt{d} > 1$ και $-1 < \lfloor \sqrt{d} \rfloor - \sqrt{d} < 0$. Έτσι, από την Πρόταση 2.8, έχουμε ότι $\lfloor \sqrt{d} \rfloor + \sqrt{d} =< \overline{a_0, \ldots, a_m} >$, όπου $a_0, \ldots, a_m$ είναι θετικοί ακέραιοι. Καθώς όμως $a_0 = 2\lfloor \sqrt{d} \rfloor$, προκύπτει $\sqrt{d} =< \lfloor \sqrt{d} \rfloor, \overline{a_1, \ldots, a_m, a_0} >$.

2.5 Ασκήσεις

1. Ας είναι x θετικός πραγματικός αριθμός με ανάπτυγμα σε συνεχές κλάσμα:

$$x =< a, a, \ldots >,$$

όπου a θετικός ακέραιος. Να βρεθεί ο αριθμός x.

2. Να υπολογιστεί το ανάπτυγμα σε συνεχές κλάσμα των αριθμών:

$$37/45,\ \ 13/25,\ \ 51/23,\ \ \sqrt{19},\ \ \sqrt{44}\ \ \text{και}\ \ \sqrt{8/3}.$$

3. Ας είναι n θετικός ακέραιος. Να δειχθεί ότι ισχύουν οι εξής:

(α) $\sqrt{n^2+1} =< n, \overline{2n} >$,

(β) $\sqrt{n^2-1} =< n-1, \overline{1, 2n-2} >$,

(γ) $\sqrt{n^2+2} =< n, \overline{n, 2n} >$.

4. Ας είναι θ ένας πραγματικός άρρητος αριθμός και P_n/Q_n, $n \geq 1$, η ακολουθία των συγκλινόντων ρητών στο θ. Να δειχθεί ότι για κάθε ζεύγος P_n/Q_n, P_{n+1}/Q_{n+1} τουλάχιστον ένας από τους δύο αυτούς ρητούς ικανοποιεί την ανισότητα:

$$\left|\theta - \frac{P}{Q}\right| < \frac{1}{2\,Q^2}.$$

5. Ας είναι θ ένας πραγματικός άρρητος αριθμός και P_n/Q_n, $n \geq 1$, η ακολουθία των συγκλινόντων ρητών στο θ. Να δειχθεί ότι για κάθε τριάδα P_n/Q_n, P_{n+1}/Q_{n+1}, P_{n+2}/Q_{n+2} τουλάχιστον ένας από τους τρείς αυτούς ρητούς ικανοποιεί την ανισότητα:

$$\left|\theta - \frac{P}{Q}\right| < \frac{1}{\sqrt{5}\,Q^2}.$$

6. Ας είναι a και b θετικοί ακέραιοι πρώτοι μεταξύ τους και p_{n-1}/q_{n-1} ο πρωτελευταίος συγκλίνων ρητός στον a/b. Τότε, να δειχθεί ότι μία λύση της εξισωσης $ax - by = 1$ είναι:

$$x = (-1)^n q_{n-1} \quad \text{και} \quad y = (-1)^n p_{n-1}.$$

7. Να υπολογιστούν τα συνεχή κλάσματα:

$$< \overline{4, 1, 3} >,\ \ < 1, 2, 3, \overline{1, 4} >,\ \ < 1, \overline{1, 1, 2} > .$$

8. Να βρεθούν τα 10 πρώτα μερικά πηλίκα του αριθμού e και κατόπιν να δειχθεί ότι υπάρχει σταθερά $c > 0$ τέτοια, ώστε για κάθε ρητό p/q, με $q > 1$, να ισχύει:

$$\left| e - \frac{p}{q} \right| > \frac{c}{q^2 \log q}.$$

9. Να βρεθεί το μήκος της περιόδου του συνεχούς κλάσματος του $\sqrt{13290059}$.

10. Ας είναι $a > 1$ ένας πραγματικός αριθμός. Να δειχθεί ότι ο n-οστός συγκλίνων ρητός του συνεχούς κλάσματος του $1/a$ ισούται με τον αντίστροφο του $(n-1)$-οστού συγλίνοντος ρητού του συνεχούς κλάσματος του a.

Βιβλιογραφία

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, 1976.

[2] D. Hensley, *Continued Fractions,* World Scientific Publishing Co. Pte. Ltd. 2006.

[3] Δ. Πουλάκης, *Θεωρία Αριθμών,* Θεσσαλονίκη, Εκδόσεις Ζήτη 2001.

Κεφάλαιο 3

Πρώτοι Αριθμοί

Σύνοψη
Σ′ αυτό το κεφάλαιο εισάγουμε τους πρώτους αριθμούς. Δίνουμε μία απόδειξη του Θεμελιώδους Θεωρήματος της αριθμητικής και βασικές εφαρμογές του στο μέγιστο κοινό διαιρέτη και ελάχιστο κοινό πολλαπλάσιο. Κατόπιν, παρουσιάζουμε μερικά αποτελέσματα σχετικά με τη κατανομή των πρώτων. Ειδικότερα, δίνουμε την απόδειξη του θεωρήματος του Chebyshev, μίας γενίκευσης της εικασίας του Bertrand καθώς και των τριών θεωρημάτων του Mertens. Επιπλέον, αναλύουμε το κόσκινο του Ερατοσθένη και παρουσιάζουμε ένα αποτέλεσμα που έχει τις ρίζες του σ′ ένα από τα βιβλία του Πλάτωνα. Τέλος, εισάγουμε τους πρώτους του Mersenne, του Fermat και της Gernain.

Προαπαιτούμενη γνώση
Κεφάλαιο 1.

3.1 Πρωτογενής Ανάλυση Ακεραίου

Σ′ αυτή την ενότητα θ′ ασχοληθούμε με την πρωτογενή ανάλυση ενός ακεραίου και θα δώσουμε μερικές εφαρμογές.

3.1.1 Το Θεμελιώδες Θεώρημα της Αριθμητικής

Ένας θετικός ακέραιος p καλείται *πρώτος*, αν οι μόνοι διαιρέτες του είναι οι ακέραιοι $\pm 1, \pm p$. Ένας θετικός ακέραιος $n > 1$ καλείται *σύνθετος*, αν δεν είναι πρώτος, δηλαδή, αν και μόνον αν υπάρχουν ακέραιοι a, b έτσι,

ώστε $n = ab$ και $1 < a \leq b < n$. Για παράδειγμα, οι ακέραιοι 2, 3, 5, 7, 11 είναι πρώτοι, ενώ οι 4, 6, 8, 9 σύνθετοι. Επίσης, ένας πρώτος αριθμός ο οποίος είναι διαιρέτης ενός ακεραίου n καλείται *πρώτος διαιρέτης* ή *πρώτος παράγοντας* του n.

Πρόταση 3.1 *Κάθε ακέραιος $a > 1$ έχει τουλάχιστον ένα πρώτο διαιρέτη.*

Απόδειξη. Ας είναι D το σύνολο των διαιρετών d του a με $d > 1$. Καθώς $a \in D$, έχουμε $D \neq \emptyset$. Συμβολίζουμε με p τον μικρότερο ακέραιο του D. Αν ο p είναι σύνθετος, τότε υπάρχουν ακέραιοι b, c έτσι, ώστε $p = bc$ και $1 < b \leq c < p$. Οπότε, έχουμε $b|p$ και $p|a$. Άρα $b \in D$ και $b < p$ που αντίκειται στον ορισμό του p. Συνεπώς, ο ακέραιος p είναι ένας πρώτος διαιρέτης του a. □

Μία σημαντική συνέπεια της προηγούμενης πρότασης είναι το επομένο θεώρημα που οφείλεται στον Ευκλείδη.

Θεώρημα 3.1 *Το πλήθος των πρώτων αριθμών είναι άπειρο.*

Απόδειξη. Ας υποθέσουμε ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο και ότι $p_1, \ldots, p_k$ είναι όλοι οι πρώτοι αριθμοί. Θέτουμε $\Pi = p_1 \cdots p_k + 1$. Από την Πρόταση 3.1 έπεται ότι υπάρχει δείκτης i έτσι, ώστε $p_i|\Pi$. Οι σχέσεις $p_i|\Pi$ και $p_i|p_1 \cdots p_k$, δίνουν $p_i|1$ που είναι αδύνατο. □

Μία άλλη ενδιαφέρουσα συνέπεια της Πρότασης 3.1 είναι η παρακάτω πρόταση η οποία μας δίνει ένα τρόπο για να ελέγχουμε αν ένας ακέραιος είναι πρώτος.

Πρόταση 3.2 *Κάθε σύνθετος ακέραιος $a > 1$ έχει τουλάχιστον ένα πρώτο διαιρέτη $p \leq \sqrt{a}$.*

Απόδειξη. Ο a είναι σύνθετος ακέραιος και επομένως υπάρχουν $b, c \in \mathbb{Z}$ με $a = bc$ και $1 < b \leq c < a$. Από την Πρόταση 3.1 έχουμε ότι ο b έχει ένα πρώτο διαιρέτη p και κατά συνέπεια ο p είναι ένας πρώτος διαιρέτης του a. Από την άλλη πλευρά, η σχέση $b^2 \leq bc = a$ μας δίνει $p \leq b \leq \sqrt{a}$. □

Πόρισμα 3.1 *Αν ένας ακέραιος $a > 1$ δεν έχει κανένα πρώτο διαιρέτη p, με $p \leq \sqrt{a}$, τότε ο a είναι πρώτος.*

Έτσι, σύμφωνα με το Πόρισμα 3.1, για να διαπιστώσουμε αν ο ακέραιος a είναι πρώτος, δεν έχουμε παρά να δοκιμάσουμε αν αυτός διαιρείται από όλους τους πρώτους $\leq \sqrt{a}$. Η διαδικασία αυτή καλείται *μέθοδος των διαδοχικών διαιρέσεων.*

Παράδειγμα 3.1 Θα χρησιμοποιήσουμε την παραπάνω μέθοδο για να διαπιστώσουμε αν ο ακέραιος 2243 είναι πρώτος. Έχουμε $\lfloor\sqrt{2593}\rfloor = 47$. Βρίσκουμε εύκολα ότι κανένας πρώτος ≤ 47 δεν διαιρεί τον 2243. Συνεπώς, ο 2243 είναι πρώτος.

Ας σημειωθεί ότι αυτή η μέθοδος δεν είναι εφαρμόσιμη στην περίπτωση όπου ο ακέραιος a είναι ένας πολύ μεγάλος πρώτος. Αν δεν γνωρίζουμε τους πρώτους που είναι $\leq \sqrt{a}$, τότε απαιτούνται $\lfloor\sqrt{a}\rfloor$ διαιρέσεις και επομένως ο απαιτούμενος χρόνος εκτέλεσης της μεθόδου είναι $O(\sqrt{n}(\log n)^2)$. Όμως και στη περίπτωση που είναι γνωστοί όλοι οι πρώτοι $\leq \sqrt{a}$, ο χρόνος αυτός, όπως θα δούμε, δεν βελτιώνεται σημαντικά (κοίτα Παρατήρηση 3.1).

Ένα από τα πλέον σημαντικά θεωρήματα της Θεωρίας Αριθμών είναι το παρακάτω το οποίο είναι γνωστό ως *Θεμελιώδες Θεώρημα της Αριθμητικής.*

Θεώρημα 3.2 *Κάθε ακέραιος $a > 1$ γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών.*

Για την απόδειξη του θεωρήματος θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 3.1 *Ας είναι $a_1, \ldots a_n$ ακέραιοι $\neq 0, \pm 1$ και p ένας πρώτος. Αν $p|a_1 \cdots a_n$, τότε $p|a_i$ για κάποιο δείκτης i με $1 \leq i \leq n$.*

Απόδειξη. Η πρόταση αληθεύει για $i = 1$. Υποθέτουμε ότι ισχύει για $n = k$ και $p|a_1 \cdots a_{k+1}$. Αν $p \not| a_{k+1}$, τότε $\mu\kappa\delta(p, a_{k+1}) = 1$ και από την Πρόταση 1.5 έπεται ότι $p|a_1 \cdots a_k$. Στη συνέχεια η υπόθεση της επαγωγής μας δίνει $p|a_i$ για κάποιο δείκτη i. □

Απόδειξη του Θεωρήματος 3.2. Θα εφαρμόσουμε τη μέθοδο της μαθηματικής επαγωγής επί του a. Για $a = 2$ αυτό προφανώς ισχύει. Υποθέτουμε ότι ο ισχυρισμός μας αληθεύει για κάθε ακέραιο m με $2 < m < a$. Αν ο a είναι πρώτος, τότε επίσης αληθεύει. Αν ο a είναι σύνθετος, τότε υπάρχουν ακέραιοι b, c με $1 < b \leq c < a$, ώστε $a = bc$. Σύμφωνα με την υπόθεση της επαγωγής, έχουμε $b = p_1 \cdots p_k$

και $c = q_1 \cdots q_l$, όπου $p_1, \ldots, p_k$ και $q_1, \ldots, q_l$ είναι πρώτοι. Επομένως $a = p_1 \cdots p_k q_1 \cdots q_l$.

Ας θεωρήσουμε δύο αναλύσεις του a σε γινόμενο πρώτων:

$$p_1 \cdots p_k = a = q_1 \cdots q_l.$$

Τότε $p_1 | q_1 \cdots q_l$ και από το Λήμμα 3.1 έπεται ότι υπαρχει δείκτης j με $p_1 | q_j$. Καθώς p_1 και q_j είναι πρώτοι, έχουμε $p_1 = q_j$. Αλλάζοντας την αρίθμηση των q_i, αν είναι αναγκαίο, έχουμε $p_1 = q_1$. Οπότε:

$$p_2 \cdots p_k = a/p_1 = q_2 \cdots q_l.$$

Καθώς $2 \leq a/p < a$, από την υπόθεση της επαγωγής, έχουμε ότι $k = l$ και υπάρχει μία μετάθεση σ του $\{1, \ldots, k-1\}$ έτσι, ώστε $p_i = q_{\sigma(i)}$ $(i = 1, \ldots, k-1)$. Άρα η γραφή του a σε γινόμενο πρώτων είναι μοναδική. □

Ας είναι P το σύνολο των πρώτων αριθμών. Σύμφωνα με το Θεώρημα 3.2, κάθε ακέραιος $a > 1$ γράφεται με μοναδικό τρόπο ως γινόμενο

$$a = \prod_{p \in P} p^{a_p},$$

όπου a_p είναι ακέραιοι ≥ 0 και μόνον ένα πεπερασμένο πλήθος από αυτούς δεν είναι μηδέν. Αν για κάθε θετικό εκθέτη a_p έχουμε $a_p = 1$, τότε ο a καλείται *ελεύθερος τετραγώνου*. Η γραφή αυτή του a καλείται *πρωτογενής ανάλυση* του a.

Στη περίπτωση όπου ο ακέραιος a είναι αρκετά μικρός η μέθοδος των διαδοχικών διαιρέσεων μας δίνει την πρωτογενή του ανάλυση. Για μεγάλους ακεραίους η μέθοδος αυτή δεν είναι αποτελεσματική. Στο Κεφάλαιο 7 θα περιγράψουμε αλγόριθμους για την παραγοντοποίηση ακεραίων.

Παράδειγμα 3.2 Θα βρούμε την πρωτογενή ανάλυση του 1253. Έχουμε $\lfloor \sqrt{1251} \rfloor = 35$. Οι πρώτοι που είναι ≤ 35 είναι οι

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31.$$

Ο πρώτος από αυτούς που διαιρεί τον 1251 είναι ο 3. Έχουμε $1251/3 = 417$. Ο 3 διαιρεί τον 417 και επομένως $417 = 3 \cdot 139$. Καθώς $\lfloor \sqrt{139} \rfloor = 11$ και κανένας από τους πρώτους 2, 3, 5, 7 και 11 δεν διαιρεί τον 139, έπεται ότι ο 139 είναι πρώτος. Επομένως, η πρωτογενής ανάλυση του 1251 είναι:

$$1251 = 3^2 \cdot 139.$$

Παράδειγμα 3.3 Ας είναι n θετικός ακέραιος και p πρώτος $< n$. Θα δείξουμε ότι αν p^r είναι η μεγαλύτερη δύναμη του p που διαιρεί τον $n!$, τότε:

$$r = \sum_{k \geq 1} \lfloor n/p^k \rfloor.$$

Το πλήθος των πολλαπλασίων του p μεταξύ των αριθμών $1, 2, \ldots, n$, είναι $\lfloor n/p \rfloor$. Το πλήθος όμως αυτών που είναι και πολλαπλάσια του p^2 είναι $\lfloor n/p^2 \rfloor$. Επίσης, το πλήθος αυτών που είναι και πολλαπλάσια του p^3 είναι $\lfloor n/p^3 \rfloor$ κ.ο.κ. Έτσι, ο μεγαλύτερος ακέραιος r τέτοιος, ώστε $p^r | n!$ είναι:

$$r = \sum_{k \geq 1} \lfloor n/p^k \rfloor.$$

Στις επόμενες προτάσεις θα δούμε μερικές ενδιαφέρουσες εφαρμογές της πρωτογενούς ανάλυσης.

Πρόταση 3.3 *Ας είναι a ένας ακέραιος > 1 με πρωτογενή ανάλυση*

$$a = \prod_{p \in P} p^{a_p}.$$

Τότε ο θετικός ακέραιος d διαιρεί τον a αν και μόνον αν ισχύει:

$$d = \prod_{p \in P} p^{d_p}, \quad 0 \leq d_p \leq a_p.$$

Απόδειξη. Ας υποθέσουμε ότι ο d έχει την παραπάνω πρωτογενή ανάλυση. Θεωρούμε τον ακέραιο

$$c = \prod_{p \in P} p^{c_p},$$

όπου $c_p = a_p - d_p$, για κάθε $p \in P$. Έτσι, έχουμε $a = dc$ και επομένως $d|a$. Αντίστροφα, ας υποθέσουμε ότι $d|a$. Οπότε, υπάρχει $c \in \mathbb{Z}$ με

$$dc = a = \prod_{p \in P} p^{a_p}.$$

Από τη μοναδικότητα της πρωτογενούς ανάλυσης προκύπτει:

$$d = \prod_{p \in P} p^{d_p}, \quad c = \prod_{p \in P} p^{c_p},$$

όπου $0 \leq d_p \leq a_p$, $0 \leq c_p \leq a_p$ και $a_p = d_p + c_p$, για κάθε $p \in P$. $\square$

Πόρισμα 3.2 *Ας είναι a και b θετικοί ακέραιοι με $\mu\kappa\delta(a,b) = 1$. Τότε οι ακέραιοι mn με $m, n \in \mathbb{N}$ και $m|a$, $n|b$ είναι διαφορετικοί ανά δύο και δίνουν όλους τους θετικούς διαιρέτες του ab.*

Απόδειξη. Ας είναι $a = p_1^{a_1} \cdots p_k^{a_k}$ και $b = q_1^{b_1} \cdots q_l^{b_l}$ οι πρωτογενείς αναλύσεις των a και b. Καθώς οι a και b είναι πρώτοι μεταξύ τους, οι πρώτοι $p_1, \ldots, p_k, q_1, \ldots, q_l$ είναι διαφορετικοί και επομένως η πρωτογενής ανάλυση του ab είναι:

$$ab = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_l^{b_l}.$$

Οπότε, κάθε θετικός διαιρέτης d του ab είναι της μορφής:

$$d = p_1^{c_1} \cdots p_k^{c_k} q_1^{d_1} \cdots q_l^{d_l},$$

με $0 \leq c_i \leq a_i$ και $0 \leq d_j \leq b_j$. Θέτοντας $m = p_1^{c_1} \cdots p_k^{c_k}$ και $n = q_1^{d_1} \cdots q_l^{d_l}$ παίρνουμε $d = mn$ με $m|a$ και $n|b$. Από τη μοναδικότητα της πρωτογενούς ανάλυσης του d, έπεται ότι η γραφή αυτή του d είναι μοναδική. Τέλος, κάθε αριθμός mn με $m, n \in \mathbb{N}$ και $m|a$, $n|b$ είναι διαιρέτης του ab. □

3.1.2 Οι Συναρτήσεις τ και σ

Ας είναι a ένας θετικός ακέραιος. Συμβολίζουμε με $\tau(a)$ και με $\sigma(n)$ το πλήθος και το άθροισμα των θετικών διαιρετών του n, αντίστοιχα. Στην περίπτωση όπου η πρωτογενής ανάλυση του a είναι γνωστή, οι τιμές των $\tau(a)$ και $\sigma(n)$ υπολογίζονται εύκολα, όπως δείχνουν οι παρακάτω προτάσεις.

Πρόταση 3.4 *Ας είναι a θετικός ακέραιος με πρωτογενή ανάλυση $a = p_1^{a_1} \cdots p_k^{a_k}$. Τότε:*

$$\tau(a) = (a_1 + 1) \cdots (a_k + 1).$$

Επίσης, αν a και b είναι θετικοί ακέραιοι με $\mu\kappa\delta(a,b) = 1$, τότε:

$$\tau(ab) = \tau(a)\tau(b).$$

Απόδειξη. Σύμφωνα με την Πρόταση 3.3, οι ακέραιοι

$$d = p_1^{b_1} \cdots p_k^{b_k}, \quad \text{με} \quad 0 \leq b_i \leq a_i \quad (i = 1, \ldots, k).$$

είναι όλοι οι θετικοί διαιρέτες του a. Επομένως, έχουμε:

$$\tau(a) = (a_1 + 1) \cdots (a_k + 1).$$

Ας είναι a, b ακέραιοι > 1 με $\mu\kappa\delta(a, b) = 1$ και πρωτογενείς αναλύσεις

$$a = p_1^{a_1} \cdots p_k^{a_k} \quad \text{και} \quad b = q_1^{b_1} \cdots q_l^{b_l}.$$

Καθώς $\mu\kappa\delta(a, b) = 1$, οι πρώτοι $p_1, \ldots, p_k, q_1, \ldots, q_l$ είναι διαφορετικοί. Επομένως, η πρωτογενής ανάλυση του ab είναι:

$$ab = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_l^{b_l}.$$

Άρα, έχουμε:

$$\tau(ab) = (a_1 + 1) \cdots (a_k + 1)(b_1 + 1) \cdots (b_l + 1) = \tau(a)\tau(b). \quad \square$$

Πρόταση 3.5 *Ας είναι a και b θετικοί ακέραιοι με $\mu\kappa\delta(a, b) = 1$. Τότε ισχύει:*

$$\sigma(ab) = \sigma(a)\sigma(b).$$

Επίσης, αν $a = p_1^{a_1} \cdots p_k^{a_k}$ είναι η πρωτογενής ανάλυση του ακέραιου $a > 1$, τότε:

$$\sigma(a) = \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{a_i}) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Απόδειξη. Ας είναι $a_1, \ldots, a_{\tau(a)}$ και $b_1, \ldots, b_{\tau(b)}$ όλοι οι θετικοί διαιρέτες των a και b, αντίστοιχα. Από το Πόρισμα 3.2 έπεται ότι όλοι οι θετικοί διαιρέτες του ab είναι οι ακέραιοι $a_i b_j$ $(i = 1, \ldots, \tau(a),\ j = 1, \ldots, \tau(b))$. Τοτε:

$$\sigma(ab) = \sum_{i=1}^{\tau(a)} \sum_{i=1}^{\tau(b)} a_i b_j = \left(\sum_{i=1}^{\tau(a)} a_i \right) \left(\sum_{i=1}^{\tau(b)} b_j \right) = \sigma(a)\sigma(b).$$

Για $i = 1, \ldots, k-1$ έχουμε $\mu\kappa\delta(p_i^{a_i}, p_{i+1}^{a_{i+1}} \cdots p_k^{a_k}) = 1$ και επομένως, εφαρμόζοντας διαδοχικά την προηγούμενη ισότητα, παίρνουμε:

$$\sigma(a) = \sigma(p_1^{a_1})\sigma(p_2^{a_2} \cdots p_k^{a_k}) = \ldots = \sigma(p_1^{a_1}) \cdots \sigma(p_k^{a_k}).$$

Οι θετικοί διαιρέτες του $p_i^{a_i}$ είναι οι ακέραιοι $1, p_i, \ldots, p_i^{a_i}$ και έτσι έχουμε:

$$\sigma(p_i^{a_i}) = 1 + p_i + \cdots + p_i^{a_i} = \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Συνδυάζοντας τις παραπάνω ισότητες προκύπτει η ζητουμένη σχέση για το $\sigma(a)$. $\square$

3.1.3 Εφαρμογή στον Μέγιστο Κοινό Διαιρέτη

Στη συνέχεια θα εκφράσουμε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο με τη βοηθεια της πρωτογενούς ανάλυσης.

Πρόταση 3.6 *Ας είναι $a_1, \ldots, a_n$ θετικοί ακέραιοι με πρωτογενείς αναλύσεις*

$$a_i = \prod_{p \in P} p^{a_{ip}}.$$

Τότε:

$$\mu\kappa\delta(a_1, \ldots, a_n) = \prod_{p \in P} p^{d_p}, \quad \epsilon\kappa\pi(a_1, \ldots, a_n) = \prod_{p \in P} p^{m_p},$$

όπου για κάθε $p \in P$ έχουμε

$$d_p = \min\{a_{1p}, \ldots, a_{np}\}, \quad m_p = \max\{a_{1p}, \ldots, a_{np}\}.$$

Απόδειξη. Θέτουμε

$$d = \prod_{p \in P} p^{d_p}, \quad m = \prod_{p \in P} p^{m_p}.$$

Καθώς $d_p \leq a_{jp}$ $(j = 1, \ldots, n)$, από την Πρόταση 3.3, έχουμε $d | a_i$ $(i = 1, \ldots, n)$. Αν δ είναι ένας θετικός ακέραιος με $\delta | a_i$ $(i = 1, \ldots, n)$, τότε η Πρόταση 3.3 δίνει:

$$\delta = \prod_{p \in P} p^{d_\delta},$$

με $0 \leq \delta_p \leq a_{ip}$ $(i = 1, \ldots, n,\ p \in P)$. Άρα $\delta_p \leq d_p$ $(j = 1, \ldots, k)$ και επομένως $\delta | d$. Συνεπώς $d = \mu\kappa\delta(a_1, \ldots, a_n)$.

Καθώς $a_{jp} \leq m_p$ $(j = 1, \ldots, n)$, έχουμε $a_i | m$ $(i = 1, \ldots, n)$. Αν

$$\mu = \prod_{p \in P} p^{\mu_p}$$

είναι θετικός ακέραιος με $a_i | \mu$ $(i = 1, \ldots, n)$, τότε $a_{ip} \leq \mu_p$ $(i = 1, \ldots, n, p \in P)$ και επομένως $m_p \leq \mu_p$, απ΄ όπου παίρνουμε $m | \mu$. Άρα $m = \epsilon\kappa\pi(a_1, \ldots, a_n)$. $\square$

Πρόταση 3.7 *Ας είναι $a, b_1, \ldots, b_n$ $(n \geq 2)$ ακέραιοι > 1 και οι $b_1, \ldots, b_n$ πρώτοι μεταξύ τους ανά δύο. Τότε:*

$$\mu\kappa\delta(a, b_1 \cdots b_n) = \mu\kappa\delta(a, b_1) \cdots \mu\kappa\delta(a, b_n).$$

Απόδειξη. Καθώς οι $b_1, \ldots, b_n$ είναι πρώτοι μεταξύ τους ανά δύο, οι πρωτογενείς τους αναλύσεις είναι:

$$b_i = p_{i1}^{b_{i1}} \cdots p_{i,k_i}^{b_{ik_i}} \quad (i = 1, \ldots, n),$$

όπου οι πρώτοι $p_{11}, \ldots p_{1,k_1}, \ldots, p_{n1}, \ldots p_{n,k_n}$ είναι διαφορετικοί ανά δύο. Άρα, η πρωτογενής ανάλυση του $b_1 \cdots b_n$ είναι:

$$b_1 \cdots b_n = p_{11}^{b_{11}} \cdots p_{1k_1}^{b_{1k_1}} \cdots p_{n1}^{b_{n1}} \cdots p_{nk_n}^{b_{nk_n}}.$$

Επίσης, έχουμε:

$$a = p_{11}^{a_{11}} \cdots p_{1k_1}^{a_{1k_1}} \cdots p_{n1}^{a_{n1}} \cdots p_{nk_n}^{a_{nk_n}} q_1^{c_1} \cdots q_r^{c_r},$$

όπου $q_1, \ldots, q_r$ είναι πρώτοι διαφορετικοί από τους p_{ij} και $a_{i,j}$, c_i είναι ακέραιοι ≥ 0. Οπότε:

$$\mu\kappa\delta(a, b_1 \cdots b_n) = \prod_{i=1}^{n} p_{i1}^{\min\{a_{i1}, b_{i1}\}} \cdots p_{i,k_i}^{\min\{a_{ik_i}, b_{ik_i}\}} = \prod_{i=1}^{n} \mu\kappa\delta(a, b_i).$$

$\square$

Πόρισμα 3.3 *Ας είναι $a, b_1, \ldots, b_n$ $(n \geq 2)$ ακέραιοι > 1 και οι $b_1, \ldots, b_n$ πρώτοι μεταξύ τους ανά δύο. Αν $b_1 | a, \ldots, b_n | a$, τότε $b_1 \cdots b_n | a$.*

Απόδειξη. Από την Πρόταση 3.7 έχουμε:

$$\mu\kappa\delta(a, b_1 \cdots b_n) = \mu\kappa\delta(a, b_1) \cdots \mu\kappa\delta(a, b_n) = b_1 \cdots b_n.$$

Επομένως $b_1 \cdots b_n | a$. $\square$

Παράδειγμα 3.4 Θα δείξουμε ότι για κάθε ακέραιο $n \geq 0$ ισχύει $42|n^7 - n$. Καθώς

$$n^7 - n = n(n^6 - 1) = n(n-1)(n+1)(n^4 + n^2 + 1),$$

από το Παράδειγμα 1.2, έπεται ότι $6|(n-1)n(n+1)$ και επομένως $6|n^7 - n$. Στη συνέχεια θα δείξουμε χρησιμοποιώντας επαγωγή ότι $7|n^7 - n$. Για $n = 0$ η προς απόδειξη σχέση προφανώς ισχύει. Ας υποθέσουμε ότι για $n = k$ ισχύει $7|k^7 - k$. Θεωρούμε τον ακέραιο:

$$(k+1)^7 - (k+1) = k^7 - k + 7k^6 + 21k^5 + 45k^4 + 45k^3 + 21k^2 + 7k.$$

Από την υπόθεση της επαγωγής, έχουμε $7|k^7 - k$ και οι υπόλοιποι συντελεστές διαιρούνται με τον 7. Συνεπώς, για κάθε ακέραιο $n \geq 0$ ισχύει $7|n^7 - n$. Καθώς $\mu\kappa\delta(7, 6) = 1$, από το Πόρισμα 3.2 έπεται ότι $42|n^7 - n$.

3.2 Κατανομή των Πρώτων Αριθμών

Σ′ αυτή την ενότητα θα δώσουμε μερικά θεωρήματα που αφορούν την κατανομή των πρώτων αριθμών.

3.2.1 Το Θεώρημα του *Chebyshev*

Ας είναι x ένας θετικός πραγματικός ακέραιος. Συμβολίζουμε με $\pi(x)$ το πλήθος των πρώτων $\leq x$. Στα 1849, ο Chebyshev, απέδειξε ότι για $n \geq 30$ ισχύει η ανισότητα:

$$c_1 \frac{n}{\log n} < \pi(n) < c_2 \frac{n}{\log n}.$$

με $c_1 = 0,92129$ και $c_2 = 1,1056$. Στα 1892, ο Sylvester βελτίωσε τις τιμές των σταθερών c_1 και c_2 σε $c_1 = 0,95695$ και $c_2 = 1,104423$.

Σ′ αυτή την ενότητα θα δώσουμε μία απλή απόδειξη αυτού του αποτελέσματος με λιγότερο καλά φράγματα.

Θεώρημα 3.3 *Έχουμε:*

$$\log 2 \ \frac{n-2}{\log n} \leq \pi(n) < 5 \ \frac{n}{\log n}.$$

Ας σημειωθεί ότι η απόδειξη της δεξιάς ανισότητας οφείλεται στον P. Erdős, ενώ της αριστερής στον M. Nair. Για την απόδειξη του Θεωρηματος 3.3 θα χρειαστούμε τα παρακάτω λήμματα.

Λήμμα 3.2 *Για κάθε θετικό ακέραιο n ισχύει:*

$$\prod_{p\leq n} p \leq 4^n,$$

όπου p διατρέχει το σύνολο των πρώτων $\leq n$.

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του n. Για τις τιμές $n = 1, 2, 3, 4$ διαπιστώνουμε εύκολα ότι η προς απόδειξη ανισότητα ισχύει. Υποθέτουμε ότι $n \geq 5$ και η ανισότητα ισχύει για κάθε θετικό ακέραιο μικρότερο του n. Ας είναι $n = 2m + 1$, όπου m ακέραιος. Τότε:

$$\prod_{p\leq 2m+1} p = \prod_{p\leq m+1} p \prod_{m+2\leq p\leq 2m+1} p.$$

Σύμφωνα με την υπόθεση της επαγωγής, το πρώτο γινόμενο του δεξιού σκέλους είναι $\leq 4^{m+1}$. Επίσης, κάθε πρώτος p με $m+2 \leq p \leq 2m+1$ διαιρεί τον ακέραιο

$$\binom{2m+1}{m} = \frac{(m+2)(m+3)\cdots(2m+1)}{m!}$$

και επομένως ισχύει:

$$\prod_{m+2\leq p\leq 2m+1} p \leq \binom{2m+1}{m}.$$

Καθώς οι ακέραιοι

$$\binom{2m+1}{m}, \quad \binom{2m+1}{m+1}$$

είναι ίσοι και είναι όροι του αναπτύγματος του $(1+1)^{2m+1}$, έχουμε:

$$\binom{2m+1}{m} \leq \frac{1}{2}\cdot 2^{2m+1} = 4^m.$$

Επομένως, συνδυάζοντας τις παραπάνω ανισότητες, παίρνουμε:

$$\prod_{p\leq n} p \leq 4^n.$$

Τέλος, αν ο n είναι άρτιος, τότε:

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p \leq 4^{n-1} < 4^n. \quad \square$$

Λήμμα 3.3 *Ας είναι n θετικός ακέραιος και d_n το ελάχιστο κοινό πολαπλάσιο των $1, 2, \ldots, n$. Τότε:*

$$d_n \geq 2^{n-2}.$$

Απόδειξη. Ας είναι m ένας θετικός ακέραιος και ας θέσουμε

$$I = \int_0^1 x^m (1-x)^m dx.$$

Για κάθε x με $0 \leq x \leq 1$ έχουμε $0 \leq x(1-x) \leq 1/4$ και επομένως προκύπτει:

$$0 \leq I \leq (1/4)^m.$$

Από την άλλη πλευρά έχουμε:

$$\begin{aligned} I &= \int_0^1 x^m \left(\sum_{k=0}^{m} (-1)^k \left(\begin{array}{c} m \\ k \end{array} \right) x^k \right) dx \\ &= \sum_{k=0}^{m} (-1)^k \left(\begin{array}{c} m \\ k \end{array} \right) \int_0^1 x^{m+k} dx \\ &= \sum_{k=0}^{m} (-1)^k \left(\begin{array}{c} m \\ k \end{array} \right) \frac{1}{m+k+1} \end{aligned}$$

και επομένως:

$$I = \frac{A}{d_{2m+1}},$$

όπου A είναι θετικός ακέραιος. Οπότε, έχουμε:

$$d_{2m+1} = \frac{A}{I} \geq 4^m.$$

Παρατηρούμε ότι η παραπάνω ανισότητα αληθεύει και για $m = 0$. Αν ο n είναι περιττός, τότε $n = 2m + 1$, για κάποιο ακέραιο $m \geq 1$, και επομένως ισχύει:

$$d_n = d_{2m+1} \geq 4^m = 2^{n-1}.$$

Αν ο n είναι άρτιος, τότε:

$$d_n \geq d_{n-1} \geq 2^{n-2}. \quad \square$$

Απόδειξη του Θεωρήματος 3.3. Έχουμε:

$$\begin{aligned} \sum_{p \leq n} \log p &\geq \sum_{\sqrt{n} \leq p \leq n} \log p \\ &\geq \sum_{\sqrt{n} \leq p \leq n} \log \sqrt{n} \\ &\geq (\pi(n) - \pi(\sqrt{n})) \log \sqrt{n} \end{aligned}$$

(όπου p πρώτος). Από το Λήμμα 3.2 παίρνουμε:

$$\sum_{p \leq n} \log p = \log \left(\prod_{p \leq n} p \right) \leq n \log 4 < 2n.$$

Από τις παραπάνω δύο ανισότητες προκύπτει:

$$\pi(n) < \pi(\sqrt{n}) + \frac{4n}{\log n}.$$

Έτσι, καθώς $\pi(\sqrt{n}) \leq \sqrt{n} \leq n/\log n$, παίρνουμε:

$$\pi(n) < 5 \frac{n}{\log n}.$$

Ας είναι $p_1, \ldots, p_k$ όλοι οι πρώτοι $\leq n$. Οπότε, καθε ακέραιος $m \in \{1, \ldots, n\}$ γράφεται:

$$m = \prod_{i=1}^{k} p_i^{a_{m,i}},$$

όπου $a_{m,i}$ είναι ακέραιοι ≥ 0 $(i = 1, \ldots, k)$. Επομένως, το ελάχιστο κοινό πολλαπλάσιο d_n των $1, \ldots, n$ είναι:

$$d_n = \prod_{i=1}^{k} p_i^{\max\{a_{1,i}, \ldots, a_{n,i}\}}.$$

Καθώς ισχύει

$$p_i^{\max\{a_{1,i},\ldots,a_{n,i}\}} \leq n,$$

έχουμε

$$d_n \leq n^{\pi(n)}$$

και χρησιμοποιώντας το Λήμμα 3.3, παίρνουμε:

$$2^{n-2} \leq n^{\pi(n)},$$

απ΄ όπου:

$$(n-2)\log 2 \leq \pi(n)\log n. \quad \square$$

Παρατήρηση 3.1 Ας είναι a ένας θετικός ακέραιος. Από το Θεώρημα 3.3 έχουμε ότι το πλήθος των πρώτων που είναι $< \sqrt{a}$ είναι $\Theta(\sqrt{a}/\log a)$. Έτσι, στην περίπτωση όπου όλοι οι πρώτοι $\leq \sqrt{a}$ είναι γνωστοί, η εφαρμογή της Μεθόδου των Διαδοχικών Διαιρέσεων, για να ελέγξουμε αν ο a είναι πρώτος, απαιτεί χρόνο $O(\sqrt{a}\log n)$. Αν ο a είναι πρώτος, τότε ο χρόνος που χρειάζεται για να το διαπιστώσουμε είναι $\Theta(\sqrt{a}\log a)$.

Το σημαντικότερο αποτέλεσμα στην κατανομή των πρώτων αριθμών είναι το ακόλουθο θεώρημα που αποδείχθηκε στα 1896 από τους J. Hadamard και C. de la Vallée Poussin, ανεξάρτητα.

Θεώρημα 3.4 *(Το Θεώρημα των Πρώτων Αριθμών) Ισχύει:*

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

Για μία απόδειξη αυτού του θεωρήματος ο ενδιαφερόμενος αναγνώστης μπορεί να συμβουλευτεί τα συγγράμματα [1, 4]. Επίσης, ένας αλγόριθμος για τον ακριβή υπολογισμό του $\pi(x)$ περιέχεται στο [2, Ενότητα 9.9].

3.2.2 Η Εικασία του *Bertrand*

Στα 1845 ο J. Bertrand διετύπωσε την εικασία ότι για κάθε ακέραιο ≥ 1 υπάρχει ένας πρώτος p με $n < p < 2n$ και την επαλήθευσε εμπειρικά για κάθε $n < 6000000$. Η απόδειξη αυτής της εικασίας δόθηκε στα 1852 από τον Chebyshev. Στη συνέχεια θα δώσουμε την απόδειξη ενός γενικότερου αποτελέσματος της εικασίας του Bertrand.

Θεώρημα 3.5 *Για κάθε θετικό ακέραιο n ισχύει:*

$$\pi(2n) - \pi(n) > \frac{n}{3\log(2n)}.$$

Θέτουμε:

$$C_n = \left(\begin{array}{c} 2n \\ n \end{array} \right).$$

Για την απόδειξη του θεωρήματος θα χρειαστούμε τα παρακάτω λήμματα.

Λήμμα 3.4 *Ας είναι n ακέραιος ≥ 3 και p πρώτος με $2n/3 < p \leq n$. Τότε ισχύει $p \not| C_n$.*

Απόδειξη. Έχουμε $p > 2$ και καθώς $3p > n$, τα μόνα πολλαπλάσια του p που είναι $\leq 2n$ είναι τα p και $2p$. Επομένως, η μεγαλύτερη δύναμη του p που διαιρεί τον $(2n)!$ είναι ο p^2. Από την άλλη πλευρά, το μοναδικό πολλαπλάσιο του p που είναι $\leq n$ είναι ο ίδιος ο p. Άρα, η μεγαλύτερη δύναμη του p που διαιρεί τον $(n!)^2$ είναι ο p^2. Συνεπώς, $p \not| C_n$ $\square$.

Λήμμα 3.5 *Ας είναι n ακέραιος ≥ 2 και p πρώτος με $p \leq 2n$. Αν r_p είναι ο μεγαλύτερος θετικός ακέραιος τέτοιος, ώστε $p^{r_p} < 2n$, τότε*

$$C_n \Bigg| \prod_{p<2n} p^{r_p}.$$

Επίσης, αν $p > n$, τότε ο p είναι μεγαλύτερη δύναμη του p που διαιρεί τον C_n.

Απόδειξη. Από το Παράδειγμα 3.3 έχουμε ότι ο εκθέτης της μεγαλύτερης δύναμης του p που διαιρεί τον $(2n)!$ είναι:

$$\sum_{m=1}^{r_p} \left\lfloor \frac{2n}{p^m} \right\rfloor.$$

ενώ ο εκθέτης της μεγαλύτερης δύναμης του p που διαιρεί τον $(n!)^2$ είναι:

$$2\sum_{m=1}^{r_p} \left\lfloor \frac{n}{p^m} \right\rfloor.$$

Επομένως, ο εκθέτης της μεγαλύτερης δύναμης του p που διαιρεί τον διωνυμικό συντελεστή C_n είναι:

$$\sum_{m=1}^{r_p} \left\{ \left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor \right\} \leq \sum_{m=1}^{r_p} 1 = r_p.$$

(Για κάθε πραγματικό αριθμό $x > 0$ ισχύει $2\lfloor x \rfloor \leq \lfloor 2x \rfloor \leq 2\lfloor x \rfloor + 1$.) Συνεπώς, η πρώτη σχέση διαιρετότητας ισχύει. Για τη δεύτερη σχέση παρατηρούμε ότι από τις ανισότητες $n < p < 2n$, έχουμε $p^2 > 2n$ και επομένως $p|(2n)!$ και $p^2 \not| (2n)!$, απ΄ όπου το αποτέλεσμα. □

Απόδειξη του Θεωρήματος 3.5. Ας είναι $n \geq 3$. Θέτουμε

$$P_n = \prod_{n<p<2n} p.$$

Από το Λήμμα 3.5 έχουμε ότι $P_n|C_n$ και επομένως υπάρχει θετικός ακέραιος Q_n με

$$C_n = P_n Q_n.$$

Επίσης, το τετράγωνο κανενός πρώτου παράγοντα του P_n δεν διαιρεί τον C_n. Αν p είναι ένας πρώτος διαιρέτης του C_n με $p \leq n$, τότε, σύμφωνα με το Λήμμα 3.4, έχουμε $p \leq 2n/3$. Έτσι, παίρνουμε:

$$Q_n = \prod_{p \leq 2n/3} p^{e_p},$$

όπου p διατρέχει το σύνολο των πρώτων $\leq 2n/3$ και e_p είναι ο μεγαλύτερος φυσικός με $p^{e_p}|C_n$.

Από την άλλη πλευρά, σύμφωνα με το Λήμμα 3.5, έχουμε:

$$C_n \Bigg| \prod_{q<2n} q^{r_q},$$

όπου q διατρέχει το σύνολο των πρώτων που είναι $< 2n$ και r_q ακέραιος με $q^{r_q} \leq 2n < q^{r_q+1}$. Έτσι, αν p είναι πρώτος διαιρέτης του Q_n και $e_p \geq 2$, τότε $p^{e_p} \leq 2n$. Επομένως, $p \leq \sqrt{2n}$ και κατά συνέπεια υπάρχουν το πολύ $\lfloor \sqrt{2n} \rfloor$ πρώτοι p στην πρωτογενή ανάλυση του Q_n με εκθέτη $e_p \geq 2$ και οι οποίοι, όπως είδαμε, ικανοποιούν την ανισότητα $p^{e_p} \leq 2n$. Οπότε, έχουμε:

$$Q_n \leq (2n)^{\lfloor \sqrt{2n} \rfloor} \prod_{p \leq 2n/3} p,$$

και, χρησιμοποιώντας το Λήμμα 3.2, παίρνουμε:

$$Q_n \leq (2n)^{\lfloor\sqrt{2n}\rfloor} 4^{2n/3}.$$

Ο C_n είναι ο μεγαλύτερος από τους $2n+1$ όρους του αναπτύγματος του διωνύμου του Νεύτωνα $(1+1)^{2n}$ και $C_n > 2$. Οπότε, έχουμε:

$$4^n \leq (2n-1)C_n + 2 < 2nC_n.$$

Έτσι, χρησιμοποιώντας τις δύο προηγούμενες ανισότητες, προκύπτει:

$$P_n = \frac{C_n}{Q_n} > \frac{4^{n/3}}{(2n)^{1+\lfloor\sqrt{2n}\rfloor}}.$$

Επομένως, ισχύει:

$$\pi(2n) - \pi(n) \geq \frac{\log P_n}{\log(2n)} > \frac{n\log 4}{3\log(2n)} - (1+\sqrt{2n}),$$

απ΄ όπου

$$\pi(2n) - \pi(n) > \frac{n}{3\log(2n)} + \frac{n(\log 4 - 1)}{3\log(2n)} - (1+\sqrt{2n}).$$

Για $n \geq 13.000$, έχουμε:

$$\frac{n(\log 4 - 1)}{3\log(2n)} - (1+\sqrt{2n}) \geq 0$$

και επομένως το θεώρημα ισχύει. Για $n < 13000$ το θεώρημα είναι δυνατόν να επαληθευθεί εύκολα με την βοήθεια ενός υπολογιστή. □

Παρατήρηση 3.2 Ας σημειωθεί ότι μπορούμε να κατασκευάσουμε διαστήματα ακεραίων όσο μεγάλα επιθυμούμε τα οποία δεν περιέχουν πρώτους αριθμούς. Πράγματι, αν k είναι θετικός ακέραιος > 1, τότε οι διαδοχικοί ακέραιοι $k!+2, k!+3, \ldots, k!+k$ είναι σύνθετοι γιατί διαιρούνται από τους $2, 3, \ldots, k$ και είναι μεγαλύτεροι από αυτούς.

3.2.3 Τα Θεωρήματα του *Mertens*

Στα 1874, ο F. Mertens δημοσίευσε τρία θεωρήματα επί της κατανομής των πρώτων αριθμών. Παρακάτω αποδεικνύουμε τρείς εκδοχές των.

Θεώρημα 3.6 *Για κάθε θετικό ακέραιο x ισχύει:*

$$\sum_{p\le x}\frac{\log p}{p}=\log x+O(1),$$

όπου p διατρέχει το σύνολο των πρώτων που είναι $\le x$.

Απόδειξη. Θέτουμε $n=\lfloor x\rfloor$. Από το Παράδειγμα 3.3 παίρνουμε:

$$\log(n!)=\sum_{p\le n}\sum_{k\ge 1}\lfloor n/p^k\rfloor\log p=\sum_{p\le n}\lfloor n/p\rfloor\log p+\sum_{p\le n}\sum_{k\ge 2}\lfloor n/p^k\rfloor\log p.$$

Θα υπολογίσουμε το τελευταίο άθροισμα. Έχουμε:

$$\begin{aligned}\sum_{p\le n}\log p\sum_{k\ge 2}\lfloor n/p^k\rfloor &\le n\sum_{p\le n}\log p\sum_{k\ge 2}\frac{1}{p^k}\\ &\le n\sum_{p\le n}\frac{\log p}{p^2}\frac{1}{1-1/p}\\ &\le n\sum_{p\le n}\frac{\log p}{p(p-1)}\\ &\le n\sum_{k\ge 2}\frac{\log k}{k(k-1)}=O(n).\end{aligned}$$

Άρα ισχύει:

$$\log(n!)=\sum_{p\le n}\left\lfloor\frac{n}{p}\right\rfloor\log p+O(n).$$

Χρησιμοποιώντας την σχέση $\lfloor n/p\rfloor=n/p+O(1)$ και κατόπιν το Λήμμα 3.2 παίρνουμε:

$$\log(n!)=\sum_{p\le n}\frac{n}{p}\log p+O(\sum_{p\le n}\log p)+O(n)=n\sum_{p\le n}\frac{\log p}{p}+O(n).$$

Από την άλλη πλευρά, το Παράδειγμα 1.11 μας δίνει:

$$\log(n!)=\sum_{k=1}^{n}\log k=n\log n-n+O(\log n).$$

Από τις δύο παραπάνω ισότητες έχουμε:

$$\sum_{p\le x}\frac{\log p}{p}=\log n+O(1)$$

και παρατηρώντας ότι $\log n = \log x + O(1)$ παίρνουμε το αποτέλεσμα. □

Θεώρημα 3.7 *Για κάθε θετικό ακέραιο x ισχύει:*

$$\sum_{p \le x} \frac{1}{p} = \log\log x + O(1),$$

όπου p διατρέχει το σύνολο των πρώτων $p \le x$.

Για την απόδειξη του θεωρήματος θα χρησιμοποιήσουμε το παρακάτω λήμμα.

Λήμμα 3.6 *Ας είναι $c_k, c_{k+1}, \ldots$ μία ακολουθία πραγματικών αριθμών, $A \subseteq \mathbb{R}$ με $a \in A$ και $f : A \to \mathbb{R}$ μία συνάρτηση με συνεχή παράγωγο στο διάστημα $[k, x] \subseteq A$. Θέτουμε*

$$C(t) = \sum_{k \le i < t} c_i.$$

Τότε:

$$\sum_{k \le i < x} c_i f(i) = C(x)f(x) - \int_k^x C(t)f'(t)\,dt.$$

Απόδειξη. Καταρχήν ας σημειωθεί ότι, καθώς η συνάρτηση $C(t)$ είναι κλιμακωτή, η συνάρτηση $C(t)f'(t)$ είναι κατά τμήματα συνεχής στο διάστημα $[k, x]$ και κατά συνέπεια ολοκληρώσιμη. Θέτουμε $n = \lfloor x \rfloor$. Έχουμε:

$$\sum_{i=k}^{n} c_i f(i) = C(k)f(k) + \sum_{i=k+1}^{n} [C(i) - C(i-1)]f(i),$$

απ' όπου:

$$\sum_{i=k}^{n} c_i f(i) = \sum_{i=k}^{n-1} C(i)[f(i) - f(i+1)] + C(n)[f(n) - f(x)] + C(x)f(x).$$

Για κάθε $t \in [i, i+1)$ ισχύει $C(t) = C(i)$ και επομένως:

$$C(i)[f(i) - f(i+1)] = -\int_i^{i+1} C(t)f'(t)\,dt \quad (i = k, k+1, \ldots, n-1).$$

Όμοια παίρνουμε:

$$C(n)[f(n) - f(x)] = -\int_n^x C(t)f'(t)\,dt.$$

Συνδυάζοντας τις παραπάνω ισότητες προκύπτει το αποτέλεσμα. □

Απόδειξη του Θεωρήματος 3.7. Θέτουμε $c_i = (\log i)/i$ αν ο ακέραιος i είναι πρώτος και $c_i = 0$ αν όχι. Επίσης, θέτουμε

$$C(t) = \sum_{2 \le i < t} c_i.$$

Θεωρούμε την συνάρτηση $f(t) = 1/\log t$ και χρησιμοποιώντας το Λήμμα 3.6 παίρνουμε:

$$\sum_{p \le x} \frac{1}{p} = \frac{C(x)}{\log x} + \int_2^x \frac{C(t)}{t(\log t)^2}\ dt.$$

Από το Θεώρημα 3.6 έχουμε:

$$C(t) = \sum_{p \le t} \frac{\log p}{p} = \log t + O(1).$$

Συνδυάζοντας τις δύο παραπάνω ισότητες, προκύπτει:

$$\begin{aligned}
\sum_{p \le x} \frac{1}{p} &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t \log t} + O\left(\int_2^x \frac{dt}{t(\log t)^2}\right) \\
&= O\left(\frac{1}{\log x}\right) + (\log\log x - \log\log 2) + O\left(\frac{1}{\log 2} - \frac{1}{\log x}\right) \\
&= \log\log x + O(1). \quad \square
\end{aligned}$$

Θεώρημα 3.8 *Ισχύει:*

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \Theta(1/\log x).$$

Για την απόδειξη του θεωρήματος θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 3.7 *Ισχύουν τα εξής:*
(α) Για κάθε $x \in \mathbb{R}$ έχουμε:

$$\log(1+x) \leq x.$$

(β) Για κάθε $x \in \mathbb{R}$ με $0 \leq x \leq 1/2$ έχουμε:

$$\log(1-x) \geq -x - x^2 \geq -2x.$$

Απόδειξη. Η απόδειξη αφήνεται ως άσκηση. □

Απόδειξη του Θεωρήματος 3.8. Συνδυάζοντας τις ανισότητες (α) και (β) του Λήμματος 3.7, για κάθε πρώτο p έχουμε:

$$-\frac{1}{p^2} \leq \frac{1}{p} + \log(1-1/p) \leq 0.$$

Ας είναι x θετικός πραγματικός αριθμός. Αθροίζοντας την παραπάνω ανισότητα πάνω σε όλους τους πρώτους $p \leq x$ προκύπτει:

$$-\sum_{p\leq x} \frac{1}{p^2} \leq \sum_{p\leq x} \frac{1}{p} + \log \prod_{p\leq x}(1-1/p) \leq 0.$$

Από την άλλη πλευρά, έχουμε:

$$\sum_{p\leq x} \frac{1}{p^2} < \sum_{i\geq 2} \frac{1}{i^2} < \infty.$$

Άρα, υπάρχει μία θετική σταθερά C τέτοια, ώστε να ισχύει:

$$-C \leq \sum_{p\leq x} \frac{1}{p} + \log \prod_{p\leq x}(1-1/p) \leq 0.$$

Χρησιμοποιώντας το Θεώρημα 3.7, παίρνουμε:

$$\log\log x + \log \prod_{p\leq x}(1-1/p) = O(1).$$

Επομένως, υπάρχει μία σταθερα $D > 0$ με

$$-D \leq \log\log x + \log \prod_{p\leq x}(1-1/p) \leq D.$$

Έτσι, έχουμε:

$$e^{-D} \leq \log x \prod_{p \leq x}(1 - 1/p) \leq e^{D}$$

και κατά συνέπεια παίρνουμε:

$$\prod_{p \leq x}(1 - 1/p) = \Theta(1/\log x). \quad \square$$

3.2.4 Το Κόσκινο του Ερατοσθένη

Μία κλασσική μέθοδος υπολογισμού όλων των πρώτων που είναι μικρότεροι ή ίσοι ενός θετικού ακεραίου A είναι ο παρακάτω αλγόριθμος ο οποίος είναι γνωστός ως *Κόσκινο του Ερατοσθένη*. Τα βήματά του είναι τα εξής:

Αλγόριθμος 3.1 Κόσκινο του Ερατοσθένη.
Είσοδος: Ένας θετικός ακέραιος A.
Έξοδος: Μία λίστα με τους πρώτους $\leq A$.

1. Δημιουργούμε μια λίστα με ακέραιους από το 2 μέχρι το A.
2. Διαγράφουμε από τη λίστα όλα τα πολλαπλάσια του 2.
3. Ο πρώτος αριθμός που δεν διαγράφηκε είναι ο 3. Διαγράφουμε από τη λίστα όλα τα πολλαπλάσια του 3 που είναι ≥ 9.
4. Ο πρώτος αριθμός που δεν διαγράφηκε είναι ο 5. Διαγράφουμε από τη λίστα όλα τα πολλαπλάσια του 5 που είναι ≥ 25.
5. Συνεχίζουμε αυτή τη διαδικασία με τους εναπομείναντες αριθμούς που είναι $\leq \sqrt{A}$. Οι αριθμοί που δεν έχουν διαγραφεί είναι όλοι οι πρώτοι $\leq A$.

Πρόταση 3.8 *Ας είναι A θετικός ακέραιος. Το κόσκινο του Ερατοσθένη υπολογίζει όλους τους πρώτους $\leq A$ σε χρόνο $\Theta(A \log\log A)$.*

Απόδειξη. Ας είναι m ένας σύνθετος ακέραιος $\leq A$. Τότε, σύμφωνα με την Πρόταση 3.2, ο m έχει ένα πρώτο διαιρέτη $q \leq \sqrt{m} \leq \sqrt{A}$. Έτσι, καθώς ο m είναι πολλαπλάσιο του q, ενός πρώτου $\leq \sqrt{A}$, θα έχει διαγραφεί από την παραπάνω λίστα.

Για κάθε πρώτο p διαγράφουμε $\lfloor A/p \rfloor$ ακέραιους απο τη λίστα. Έτσι, πραγματοποιούνται συνολικά

$$\sum_{p \leq \sqrt{A}} \lfloor A/p \rfloor$$

διαγραφές. Επομένως, από το Θεώρημα 3.7 έχουμε ότι ο χρόνος εκτέλεσης του κόσκινου του Ερατοσθένη είναι $\Theta(A \log \log A)$. $\square$

Η μέθοδος του Ερατοσθένη είναι δυνατόν να τροποποιηθεί σε μία μέθοδο η οποία, δοθέντων ενός θετικού πραγματικού αριθμού x και ενός θετικού ακεραίου m, θα δίνει όλα τους θετικούς ακέραιους που είναι $\leq x$ και πρώτοι προς τον m. Αυτό γίνεται ως εξής: Δημιουργούμε μία λίστα με όλους τους θετικούς που είναι $\leq x$ και διαγράφουμε από αυτήν όλα τα πολλαπλάσια των πρώτων διαιρετών του m. Οι ακέραιοι που δεν έχουν διαγραφεί είναι οι ζητούμενοι ακέραιοι. Συμβολίζουμε με $N_m(x)$ το πλήθος αυτών των ακεραίων.

Αν d είναι ένας θετικός ακέραιος > 1, τότε θα συμβολίζουμε με d^* και $\omega(d)$ το γινόμενο και το πλήθος των διαφορετικών πρώτων που διαιρούν τον d. Αν $d = 1$, τότε θέτουμε $d^* = 1$ και $\omega(d) = 0$. Η παρακάτω πρόταση μας δίνει ένα τύπο για τον υπολογισμό της ποσότητας $N_m(x)$.

Πρόταση 3.9 *Ισχύει*

$$N_m(x) = \sum_{d | m^*} (-1)^{\omega(d)} \lfloor x/d \rfloor.$$

Απόδειξη. Καταρχήν παρατηρούμε ότι $N_m(x) = N_{m^*}(x)$. Για την απόδειξη της παραπάνω ισότητας θα εφαρμόσουμε επαγωγή επί του πλήθους των διαφορετικών πρώτων παραγόντων του m^*. Αν $m^* = 1$, τότε $N_1(x) = \lfloor x \rfloor$. Υποθέτουμε ότι ο παραπάνω τύπος ισχύει στην περίπτωση όπου ο m^* είναι γινόμενο k πρώτων. Ας υποθέσουμε ότι $m^* = m_k p$, όπου m_k είναι γινόμενο k διακεκριμμένων πρώτων και p πρώτος με $\mu\kappa\delta(m_k, p) = 1$. Παρατηρούμε ότι οι μόνοι ακέραιοι οι οποίοι συνεισφέρουν στον υπολογισμό της ποσότητας $N_{m_k}(x)$ άλλα όχι της ποσότητας $N_{m_k p}(x)$ είναι της μορφής $np \leq x$, όπου n θετικός ακέραιος με $\mu\kappa\delta(n, m_k) = 1$. Οπότε έχουμε:

$$N_{m_k}(x) - N_{m_k p}(x) = N_{m_k}(x/p).$$

Έτσι, παίρνουμε:

$$\begin{aligned} N_{m^*}(x) &= N_{m_k}(x) - N_{m_k}(x/p) \\ &= \sum_{d|m_k} (-1)^{\omega(d)} \lfloor x/d \rfloor - \sum_{d|m_k} (-1)^{\omega(d)} \lfloor x/dp \rfloor \\ &= \sum_{d|m^*} (-1)^{\omega(d)} \lfloor x/d \rfloor. \end{aligned}$$

Συνεπώς, η προς απόδειξη ισότητα αληθεύει. □

Στη συνέχεια εισάγοντας τη συνάρτηση μ του Möbius θα δώσουμε άλλη μορφή στον παραπάνω τύπο. Η συνάρτηση αυτή ορίζεται ως εξής: Για κάθε θετικό ακέραιο n θέτουμε

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{αν ο } n \text{ είναι ελεύθερος τετραγώνου,} \\ 0, & \text{αν όχι.} \end{cases}$$

Μία σημαντική ιδιότητα της συνάρτησης μ δίνεται παρακάτω.

Πρόταση 3.10 *Ας είναι m, n θετικοί ακέραιοι πρώτοι μεταξύ τους. Τότε:*

$$\mu(mn) = \mu(m)\mu(n).$$

Απόδειξη. Αν $m = 1$ ή $n = 1$, τότε η ισότητα προφανώς ισχύει. Ας υποθέσουμε ότι $m > 1$ και $n > 1$. Αν $m = p_1 \cdots p_k$ και $n = q_1 \cdots q_l$, όπου $p_1, \ldots, p_k, q_1, \ldots, q_l$ είναι διακεκριμμένοι πρώτοι, τότε

$$\begin{aligned} \mu(mn) = (-1)^{\omega(mn)} = (-1)^{k+l} = \\ (-1)^k(-1)^l = (-1)^{\omega(m)}(-1)^{\omega(n)} = \mu(m)\mu(n). \end{aligned}$$

Στη περίπτωση όπου ένας από τους m και n δεν είναι ελεύθερος τετραγώνου, το ίδιο συμβαίνει και με τον mn και επομένως

$$\mu(mn) = 0 = \mu(n)\mu(n). \quad \square$$

Χρησιμοποιώντας τη συνάρτηση μ παίρνουμε τον τύπο του Legendre:

$$N_m(x) = \sum_{d|m} \mu(d) \lfloor x/d \rfloor.$$

Στη συνέχεια θεωρούμε το γινόμενο

$$m = \prod_{p \leq \sqrt{x}} p,$$

όπου p διατρέχει το σύνολο των πρώτων $\leq \sqrt{x}$. Παρατηρούμε ότι κάθε σύνθετος ακέραιος $n \in (\sqrt{x}, x]$ έχει ένα πρώτο διαιρέτη $\leq \sqrt{x}$ και επομένως $\mu\kappa\delta(m, n) > 1$. Άρα η ποσότητα $N_m(x)$ είναι το πλήθος των πρώτων του διαστήματος $(\sqrt{x}, x]$ συν ένα. Έτσι, έχουμε:

$$N_m(x) = \pi(x) - \pi(\sqrt{x}) + 1.$$

Για κάθε θετικό ακέραιο $d > 1$ συμβολίζουμε με $P(d)$ τον μεγαλύτερο πρώτο διαιρέτη του. Αν $d = 1$, τότε θέτουμε $P(d) = 1$. Η προηγούμενη ισότητα δίνει την εξής ισότητα που συνδέει τις συναρτήσεις $\pi(x)$ και $\mu(n)$:

$$\pi(x) = -1 + \pi(\sqrt{x}) + \sum_{P(d) \leq \sqrt{x}} \mu(d) \lfloor x/d \rfloor.$$

3.2.5 Το Κρυμμένο Θεώρημα του Πλάτωνα

Στα 1982, ο καθηγητής του Τμηματος Μαθηματικών του Πανεπιστημίου Αθηνών Ανδρέας Ζαχαρίου και η συζυγός του Ελένη, διατύπωσαν την εικασία ότι στο βιβλίο του Πλάτωνα "Νόμοι" υπάρχει σε καλυμμένη μορφή ένα θεώρημα που αφορά την κατανομή των πρώτων αριθμών το οποίο και διετύπωσαν [5, 6]. Η εικασία αυτή αποδείχθηκε στα 2003 από τον Peter Shiu. Μία άλλη πιο απλή απόδειξη δόθηκε στα 2007 από τον πρωτοετή φοιτητή της Ιατρικής Σχολής του Πανεπιστημίου Θεσσαλονίκης Γεώργιο Βελισάρη. Παρακάτω διατυπώνουμε το "Κρυμμένο Θεώρημα του Πλάτωνα" και παραθέτουμε την απόδειξη του Γ. Βελισάρη.

Θεώρημα 3.9 *Ας είναι $3 < p < q$ δύο διαδοχικοί πρώτοι. Τότε κάθε θετικός ακέραιος $n < q$ διαιρεί τον $p!$.*

Απόδειξη. Κάθε θετικος ακέραιος $\leq p$ διαιρεί τον $p!$. Θα εξετάσουμε αν αυτό συμβαίνει για τους ακεραίους του συνόλου

$$A = \{p + 1, p + 2, \ldots, q - 1\}.$$

Ας είναι $n \in A$. Τότε ο ακέραιος n είναι σύνθετος και επομένως $n = ab$, όπου $a, b \in \mathbb{Z}$ με $2 \leq a \leq b < n$. Ας υποθέσουμε ότι $p \leq b$. Τότε

έχουμε $2p \leq ab = n \leq q - 1$. Καθώς όμως ο q είναι ο επόμενος πρώτος μετά τον p, από το Θεώρημα 3.5, έχουμε $p < q < 2p$. Έτσι, καταλήγουμε σε άτοπο και κατά συνέπεια $b < p$.

Ας είναι $1 = d_1 < \ldots < d_m = n$ όλοι οι θετικοί διαιρέτες του n. Τότε $n = d_i d_{m-i+1}$, όπου $i \in \{1, \ldots, m\}$. Επειδή ο n είναι σύνθετος έχουμε $m \geq 3$. Αν $m > 3$, τότε $n = d_2 d_{m-1}$ και $d_2 < d_{m-1}$. Καθώς $d_{m-1} < p$, παίρνουμε $n|p!$. Ας είναι $m = 3$. Τότε $n = k^2$, όπου k πρώτος. Έχουμε:

$$k^2 \leq q - 1 < 2p.$$

Αν $k \neq 2, 3$, τότε $4k < k^2 < 2p$ και επομένως έχουμε $1 < k < 2k < p$. Άρα $n|p!$. Αν $k = 3$, τότε $n = 9$, $p = 7$, $q = 11$ και έχουμε $9|7!$. Αν $k = 2$, τότε $n = 4$, $p = 3$ και $q = 5$ που είναι άτοπο γιατί $p > 3$. □

Παρατήρηση 3.3 Αν $p = 3$, τότε έχουμε $q = 5$. Καθώς $4 \not| 3!$, το παραπάνω θεώρημα δεν ισχύει.

Το προηγούμενο θεώρημα μας δίνει τον παρακάτω αλγόριθμο με τον οποίο, δοθέντος ενός πρώτου p, μπορούμε να υπολογίσουμε τον αμέσως μεγαλύτερό του.

Αλγόριθμος 3.2 Εύρεση του επομένου πρώτου.
Είσοδος: Ένας πρώτος p.
Έξοδος: Ο επόμενος πρώτος μετά τον p.

1. Υπολογίζουμε τον ακέραιο $p!$.
2. Για κάθε $j = 1, 2, \ldots$ υπολογίζουμε τους αριθμούς $p!/(p + j)$ μέχρι να βρούμε θετικό ακέραιο s τέτοιο, ώστε ο $p!/(p + s)$ να μην είναι ακέραιος.
3. Υπολογίζουμε $q = p + s$ και εξάγουμε τον q.

Παράδειγμα 3.5 Χρησιμοποιώντας τον παραπάνω αλγόριθμο θα υπολογίσουμε τον επόμενο πρώτο μετά τον 23. Έχουμε λοιπόν

$$23! = 25852016738884976640000.$$

Κατόπιν υπολογίζουμε:

$$\begin{aligned} 23!/24 &= 1077167364120207360000, \\ 23!/25 &= 1034080669555399065600, \end{aligned}$$

$$\begin{aligned} 23!/26 &= 994308336110960640000, \\ 23!/27 &= 95748210144018432000, \\ 23!/28 &= 92328631210303488000, \\ 23!/29 &= 891448853064999194482 + 22/29. \end{aligned}$$

Καθώς ο αριθμός $23!/29$ δεν είναι ακέραιος παίρνουμε ότι ο 29 είναι πρώτος.

3.3 Πρώτοι Ειδικής Μορφής

Σ′ αυτή την ενότητα θα μελετήσουμε μερικές οικογένειες πρώτων ειδικής μορφής.

3.3.1 Πρώτοι του *Mersenne* και Τέλειοι Αριθμοί

Οι πρώτοι αριθμοί της μορφής $M_p = 2^p - 1$, όπου p ακέραιος > 1, καλούνται *πρώτοι του Mersenne*. Το ονομά τους οφείλεται στον Γάλλο μοναχό M. Mersenne ο οποίος πρώτος τους μελέτησε τον 17ο αιώνα. Γενικότερα, ένας αριθμός της μορφής $M_n = 2^n - 1$ καλείται *αριθμός του Mersenne*.

Πρόταση 3.11 *Αν M_p είναι ένας πρώτος του Mersenne, τότε ο p είναι πρώτος.*

Απόδειξη. Ας υποθέσουμε ότι ο p είναι σύνθετος. Τότε $p = rs$, όπου r και s είναι ακέραιοι > 1. Έτσι, έχουμε:

$$2^p - 1 = 2^{rs} - 1 = (2^r - 1)((2^r)^{s-1} + \cdots + 2^r + 1).$$

Οι δύο παράγοντες του δεύτερου μέλους της παραπάνω ισότητας είναι > 1 και επομένως ο ακέραιος $2^p - 1$ δεν είναι πρώτος που είναι άτοπο. Άρα ο p είναι πρώτος. □

Μέχρι σήμερα έχουν βρεθεί μόνον 48 πρώτοι του Mersenne. Από το 1997, όλοι οι πρώτοι του Mersenne που έγιναν γνωστοί ανακαλύφθηκαν από το "Great Internet Mersenne Prime Search" (GIMPS),

ένα κατανεμημένο υπολογιστικό πρόγραμμα στο Διαδίκτυο. Αυτοί είναι οι αριθμοί M_p που αντιστοιχούν στις εξής τιμές του πρώτου p:

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89,\ 107,\ 127,\ 501,\ 607,$$

$$1.279,\ 2.203,\ 2.281,\ 3.217,\ 4.253,\ 4.423,\ 9.689,\ 9.941$$

$$11.213,\ 19.937,\ 21.701,\ 23.209,\ 44.497,\ 86.243,\ 110.503,$$

$$132.049,\ 216.091,\ 756.839,\ 859.433,\ 1.257.787,\ 1.398.269,$$

$$2.976.221,\ 3.021.377, 6.972.593,\ 13,466,917,\ 20.996.011,$$

$$24.036.583,\ 25.964.951,\ 30.402.457,\ 32.582.657,\ 37.156.667,$$

$$42.643.801,\ 43.112.609,\ 57.885.161$$

Ας σημειωθεί ότι δεν είναι γνωστο αν το πλήθος των πρώτων του Mersenne είναι άπειρο.

Ένας θετικός ακέραιος n καλείται *τέλειος*, αν ισχύει $\sigma(n) = 2n$. Για παράδειγμα, εύκολα διαπιστώνουμε ότι οι αριθμοί 6 και 28 είναι τέλειοι. Όπως θα δούμε αμέσως οι αριθμοί αυτοί είναι στενά συνδεδεμένοι με τους πρώτους του Mersenne.

Το πρώτο ενδιαφέρον αποτέλεσμα για τους τέλειους αριθμούς συναντάται στα "Στοιχεία" του Ευκλείδη. Σύμφωνα μ΄ αυτό, αν ο ακέραιος M_p είναι πρώτος, τότε ο αριθμός $2^{p-1}M_p$ είναι τέλειος. Το αντίστροφο αποδείχθηκε από τον Euler. Η απόδειξη αυτού του αποτελέσματος δίνεται παρακάτω.

Πρόταση 3.12 *Ο άρτιος ακέραιος n είναι τέλειος αν και μόνον αν $n = 2^{p-1}M_p$, όπου M_p είναι ένας πρώτος του Mersenne.*

Απόδειξη. Ας υποθέσουμε ότι ο M_p είναι πρώτος του Mersenne. Ο n είναι άρτιος και επομένως $p \geq 3$. Καθώς $\mu\kappa\delta(2^{p-1}, M_p) = 1$, από την Πρόταση 3.5 έχουμε:

$$\begin{aligned} \sigma(n) &= \sigma(2^{p-1})\sigma(M_p) \\ &= (1 + \cdots + 2^{p-1})(M_p + 1) \\ &= (2^p - 1)2^p \\ &= 2n. \end{aligned}$$

Άρα ο n είναι τέλειος αριθμός.

Αντίστροφα, ας υποθέσουμε ότι ο άρτιος ακέραιος n είναι τέλειος. Τότε $n = 2^k m$, όπου $k \geq 1$ και m περιττός ακέραιος. Από την σχέση $\mu\kappa\delta(2^k, m) = 1$, έχουμε:

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

Από την άλλη πλευρά, επειδή ο n είναι τέλειος, ισχύει:

$$\sigma(n) = 2n = 2^{k+1}m.$$

Συνδυάζοντας τις δύο παραπάνω ισότητες, παίρνουμε:

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m).$$

Έτσι, έχουμε $2^{k+1} - 1 | 2^{k+1}m$. Καθώς $\mu\kappa\delta(2^{k+1} - 1, 2^{k+1}) = 1$, η Πρόταση 1.5 δίνει $2^{k+1} - 1 | m$ και επομένως $m = (2^{k+1} - 1)m'$. Αντικαθιστούμε τον m με τον ίσο του στην παραπάνω ισότητα και έχουμε:

$$\sigma(m) = 2^{k+1}m'.$$

Οι ακέραιοι m και m' είναι διαιρέτες του m με $m' < m$ και

$$m + m' = (2^{k+1} - 1)m' + m' = 2^{k+1}m' = \sigma(n).$$

Επομένως, οι m και m' είναι οι μόνοι διαιρέτες του m. Έτσι, έχουμε $m' = 1$ και ο m είναι πρώτος. Άρα $n = 2^k(2^{k+1} - 1)$ και ο αριθμός $2^{k+1} - 1$ είναι πρώτος. □

Από την παραπάνω πρόταση βλέπουμε ότι η ύπαρξη των άρτιων τέλειων αριθμών είναι στενά συνδεδεμένη με την ύπαρξη των πρώτων του Mersenne. Από την άλλη πλευρά, μέχρι σήμερα δεν έχει βρεθεί κανένας περιττός τέλειος αριθμός. Όπως έχει αποδειχθεί, αν n είναι ένας περιττός τέλειος αριθμός, τότε $n > 10^{1500}$ [3]. Τέτοια αποτελέσματα μας οδηγούν στην εικασία ότι περιττοί τέλειοι αριθμοί δεν υπάρχουν.

3.3.2 Πρώτοι του *Fermat*

Ένας θετικός ακέραιος της μορφής

$$F_n = 2^{2^n} + 1$$

καλείται *αριθμός του Fermat*. Ένας πρώτος αυτής της μορφής καλείται *πρώτος του Fermat*. Οι αριθμοί $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ και $F_3 = 257$

είναι τέτοιοι πρώτοι. Αντίστοιχα, ένας σύνθετος αυτής της μορφής καλείται *σύνθετος του* $Fermat$.

Στην παρακάτω πρόταση αποδεικνύεται ότι οι πρώτοι της μορφής $2^m + 1$ είναι ακριβώς οι πρώτοι του Fermat.

Πρόταση 3.13 *Αν ο ακέραιος* $p = 2^m+1$ *είναι πρώτος, τότε* $m = 2^n$, *όπου* n *είναι θετικός ακέραιος.*

Απόδειξη. Ας είναι $m = 2^n b$, όπου b περιττός θετικός ακέραιος. Ας υποθέσουμε ότι $b > 1$. Τότε έχουμε:

$$p = (2^{2^n} + 1)((2^{2^n})^{b-1} - (2^{2^n})^{b-2} + \cdots + 1).$$

Άρα $2^{2^n} + 1 | p$ και επομένως ο p δεν είναι πρώτος που είναι άτοπο. Συνεπώς, ισχύει $m = 2^n$. □

Στα 1640, ο Fermat διατύπωσε την εικασία ότι οι αριθμοί αυτοί είναι όλοι πρώτοι. Στα 1732, ο Euler έδειξε ότι αυτή η εικασία δεν είναι ορθή υπολογίζοντας την πρωτογενή ανάλυση του F_5:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641 \cdot 6700417.$$

Μέχρι το 2014 είναι γνωστό ότι οι αριθμοί F_n με $5 \leq n \leq 32$ είναι σύνθετοι αν και η πλήρης πρωτογενής ανάλυση του F_n είναι γνωστή μόνο για $n = 0, \ldots, 11$. Ο μεγαλύτερος αριθμός του Fermat για τον οποίο έχει αποδειχθεί ότι είναι σύνθετος είναι ο $F_{3329780}$. Από την άλλη πλευρά οι μόνοι γνωστοί πρώτοι του Fermat είναι οι τέσσερεις πρώτοι που παραθέσαμε παραπάνω. Δεν είναι γνωστό αν το πλήθος αυτών των πρώτων είναι άπειρο. Επίσης, δεν έχει αποδειχθεί αν το πλήθος των σύνθετων αριθμών του Fermat είναι άπειρο.

Ας σημειωθεί ότι οι αριθμοί F_n ικανοποιούν τον εξής τύπο:

$$F_{n+1} = (F_n - 1)^2 + 1$$

ή ισοδύναμα

$$F_{n+1} - 2 = F_n(F_n - 2),$$

απ΄ όπου προκύπτει η εξής ισότητα:

$$F_{n+1} - 2 = F_n F_{n-1} \cdots F_0.$$

Οι πρώτοι του Fermat είναι στενά συνδεδεμένοι με την κατασκευή των κανονικών πολυγώνων όπως φανερώνει το θεώρημα των Gauss - Wantzel:

Θεώρημα 3.10 *Ένα κανονικό πολύγωνο με n πλευρές είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνον αν $n = 2^k p_1 \cdots p_s$, όπου $k \geq 0$ και p_i είναι διακεκριμμένοι πρώτοι του Fermat.*

3.3.3 Πρώτοι της *Germain*

Ένας πρώτος αριθμός p καλείται *πρώτος της Germain*, αν ο αριθμός $2p+1$ είναι επίσης πρώτος. Τότε ο πρώτος $2p+1$ καλείται *ασφαλής*. Για παράδειγμα, ο 23 είναι ένας πρώτος της Germain. Πράγματι, έχουμε $2 \cdot 23 + 1 = 47$ ο οποίος είναι ένας πρώτος αριθμός. Στα 1825, η Sophie Germain απέδειξε ότι η πρώτη περίπτωση του τελευταίου θεωρήματος του Fermat αληθεύει για αυτούς τους πρώτους, δηλαδή, ισχύει το εξής:

Θεώρημα 3.11 *Αν p είναι ένας πρώτος της Germain, τότε δεν υπάρχουν μη-μηδενικοί ακέραιοι x, y, z με $p \nmid xyz$ τέτοιοι, ώστε*

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

Οι πρώτοι της Germain που είναι < 200 είναι οι εξής:

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191.$$

Έχει διατυπωθεί η εικασία ότι το πλήθος των πρώτων της Germain είναι άπειρο. Η εικασία αυτή παραμένει, μέχρι σήμερα αναπόδεικτη. Ο μεγαλύτερος πρώτος της Germain που έχει βρεθεί μέχρι τον Αύγουστο 2013 είναι ο αριθμός

$$18543637900515 \cdot 2^{666667} - 1.$$

3.4 Ασκήσεις

1. Να προσδιοριστούν όλοι οι πρώτοι της μορφής

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

όπου n φυσικός αριθμός.

2. Να δειχθεί ότι υπάρχουν άπειροι πρώτοι της μορφής $4k + 3$.

3. Να δειχθεί ότι υπάρχουν άπειροι πρώτοι της μορφής $6k + 5$.

4. Ας είναι $p_1, p_2, \ldots$ η ακολουθία των πρώτων αριθμών. Να δειχθεί ότι ισχύουν τα εξής:
(α) $p_n \leq p_1 \cdots p_{n-1} + 1$.
(β) $p_n < 2^{2^{n-1}}$.

5. Θα δείξουμε ότι για κάθε ακέραιο $n \geq 0$ ισχύει $30 | n^5 - n$.

6. Να βρεθεί η μεγαλύτερη δύναμη του 3 που διαιρεί τον 100!

7. Να βρεθούν οι πρωτογενείς αναλύσεις των ακεραίων $3^{12} - 1$, 235679 και 756943.

8. Να δειχθεί ότι ο φυσικός $\tau(n)$ είναι περιττός αν και μόνον αν ο n είναι τέλειο τετράγωνο.

9. Ας είναι n ακέραιος > 1 και $p_1, \ldots, p_k$ όλοι οι πρώτοι διαιρέτες του. Να δειχθεί ότι ισχύει:

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

10. Να δειχθεί ότι για κάθε ακέραιο $n \geq 3$ ισχύει:

$$\sum_{k=1}^{n} \mu(k!) = 1.$$

11. Να δειχθεί ότι για κάθε θετικό ακέραιο n ισχύει:

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

12. Ν′ αποδειχθεί ότι ο αριθμός του Fermat F_4 είναι πρώτος.

13. Ας είναι n ένας περιττός τέλειος ακέραιος και $n = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής ανάλυση του. Τότε $p_1 = 1 + 4b$, $a_1 = 1 + 4c$, όπου b, c είναι φυσικοί, και οι $a_2, \ldots, a_k$ άρτιοι.

14. Ας είναι n ένας φυσικός της μορφής $3k + 2$ (αντίστοιχα, $6k + 5$,

$4k+3$). Να δειχθεί ότι ένας τουλάχιστον πρώτος διαιρέτης του n είναι της μορφής $3k+2$ (αντίστοιχα, $6k+5$, $4k+3$).

15. Να υπολογιστεί ο χρόνος εκτέλεσης του Αλγορίθμου 3.2.

Βιβλιογραφία

[1] T. M. Apostol, *Εισαγωγή στην Αναλυτική Θεωρία Αριθμών,* Gutenberg 1986.

[2] E. Bach and J. Shallit, *Algorithmic Number Theory,* MIT Press, Cambridge, Massachusetts and London, England, 1996.

[3] P. Ochem, Pascal and M. Rao, Odd perfect numbers are greater than 10^{1500}, *Mathematics of Computation* 81 (279), 2012, 1869-1877.

[4] G. Tenenbaum and M. Mendès-France, *The Prime Numbers and Their Distribution,* Student Mathematical Library 6, AMS 2000.

[5] A. Vardulakis and C. Pugh, Plato's hidden theorem on the distribution of primes, *The Mathematical Intelligencer,* Summer 2008, Volume 30, Issue 3, 61-63.

[6] A. Zachariou and E. Zachariou. Abstracts of papers presented to the American Mathematical Society, February 1982, Issue 16, Volume 3, Number 2, pages 145-220.

Κεφάλαιο 4

Ομάδες - Δακτύλιοι - Πολυώνυμα

Σύνοψη
Σ′ αυτό το κεφάλαιο θα ασχοληθούμε με αλγεβρικές δομές οι οποίες θα μας χρησιμεύσουν στα επόμενα κεφάλαια. Πιο συγκεκριμένα, θα μελετήσουμε τις βασικές ιδιότητες των ομάδων, δακτυλίων και πολυωνύμων. Για πληρέστερη μελέτη αυτών των θεμάτων ο ενδιαφερόμενος αναγνώστης μπορεί να συμβουλευτεί τα εξής συγγράμματα: [1, 2, 3, 5].

Προαπαιτούμενη γνώση
Μαθηματικά Λυκείου.

4.1 Μονοειδή

Ας είναι A ένα μη κενό σύνολο. Καλούμε *πράξη* επί του A κάθε απεικόνιση της μορφής $f : A \times A \longrightarrow A$. Π.χ. η πρόσθεση και ο πολλαπλασιασμός είναι πράξεις επί του $\mathbb{Z}$. Η τιμή της f στο ζεύγος (a, b) θα συμβολίζεται με afb.

Ένα ζεύγος $(G, *)$, όπου το G είναι σύνολο και $*$ μία πράξη επί του G, καλείται *μονοειδές* αν ισχύουν οι εξής ιδιότητες:

1. $x * (y * z) = (x * y) * z$, για κάθε $x, y, z \in G$.

2. Υπάρχει $e \in G$ τέτοιο, ώστε $x * e = x = e * x$, για κάθε $x \in G$.

Αν υπάρχει και ένα άλλο στοιχείο $k \in G$ με την ιδιότητα (1), τότε για κάθε $x \in G$ έχουμε:

$$k * x = x = x * k.$$

Έτσι, παίρνουμε $k = e * k$ και $e * k = e$, απ' όπου $e = k$. Άρα, το στοιχείο e είναι μοναδικό και καλείται *ουδέτερο στοιχείο* του G.

Αν επιπλέον ισχύει $x * y = y * x$, για κάθε $x, y \in G$, τότε το μονοειδές $(G, *)$ καλείται *αντιμεταθετικό*.

Παράδειγμα 4.1 Τα ζεύγη $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ είναι αντιμεταθετικά μονοειδή με ουδέτερο στοιχείο το 0 και τα ζεύγη $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ είναι αντιμεταθετικά μονοειδή με ουδέτερο στοιχεία το 1.

Παράδειγμα 4.2 Ας είναι $(G_i, *_i)$ μονοειδές με ουδέτερο στοιχείο e_i $(i = 1, \ldots, k)$. Το σύνολο $G_1 \times \cdots \times G_k$ είναι μονοειδές με πράξη

$$(x_1, \ldots, x_k) * (y_1, \ldots, y_k) = (x_1 *_1 y_1, \ldots, x_k *_k y_k).$$

Το ουδέτερο στοιχείο του είναι το $(e_1, \ldots, e_k)$.

Παράδειγμα 4.3 Μία συνάρτηση με πεδίο ορισμού το σύνολο των θετικών ακεραίων και πεδίο τιμών το σύνολο των μιγαδικών αριθμών καλείται *αριθμητική*. Συμβολίζουμε με $\mathcal{A}$ το σύνολο των αριθμητικών συναρτήσεων. Καλούμε *ενελικτικό γινόμενο* των f και g την αριθμητική συνάρτηση:

$$f * g : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{C},\ n \longmapsto (f * g)(n) = \sum_{ab=n} f(a)g(b),$$

όπου τα ζεύγη (a, b) διατρέχουν όλους τους φυσικούς που το γινόμενό τους ισούται με n. Π.χ. για $n = 6$ έχουμε

$$(f * g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1).$$

Η αντιστοιχία $(f, g) \longmapsto f*g$ ορίζει μία πράξη επί του $\mathcal{A}$ η οποία καλείται *ενελικτικός πολλαπλασιασμός*. Θα δείξουμε ότι το ζεύγος $(\mathcal{A}, *)$ είναι ένα αντιμεταθετικό μονοειδές.

Ας είναι $f, g, h \in \mathcal{A}$. Τότε για κάθε φυσικό $n > 0$ έχουμε:

$$[f * (g * h)](n) = \sum_{ab=n} f(a)(g * h)(b) =$$
$$\sum_{ab=n} f(a) \sum_{cd=b} g(c)h(d) = \sum_{acd=n} f(a)g(c)h(d).$$

Όμοια παίρνουμε:

$$[(f * g) * h](n) = \sum_{acd=n} f(a)g(c)h(d).$$

Άρα, για κάθε φυσικό $n > 0$ ισχύει:

$$[f * (g * h)](n) = [(f * g) * h](n)$$

και επομένως $f * (g * h) = (f * g) * h$. Επίσης, έχουμε:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ab=n} g(a)f(b) = (g * f)(n),$$

απ' όπου έπεται $f * g = g * f$. Στη συνέχεια, ας θεωρήσουμε την αριθμητική συνάρτηση ϵ που ορίζεται από τις σχέσεις:

$$\epsilon(1) = 1 \quad \text{και} \quad \epsilon(n) = 0, \ \text{για κάθε φυσικό } n > 1.$$

Για κάθε $f \in \mathcal{A}$ και φυσικό $n > 1$ έχουμε:

$$(f * \epsilon)(n) = \sum_{ab=n} f(a)\epsilon(b) = f(n),$$

απ' όπου έπεται $f * \epsilon = f$. Καθώς η πράξη $*$ είναι αντιμεταθετική, ισχύει επίσης και η σχέση $\epsilon * f = f$. Άρα, η συνάρτηση ϵ είναι το ουδέτερο στοιχείο για τον ενελικτικό πολλαπλασιασμό. Επομένως, το ζεύγος $(\mathcal{A}, *)$ είναι ένα αντιμεταθετικό μονοειδές.

Ας είναι $(G, *)$ ένα μονοειδές και e το ουδέτερο στοιχείο του. Ένα υποσύνολο H του G καλείται *υπομονοειδές* του G αν $e \in H$ και για κάθε $x, y \in H$ ισχύει $x * y \in H$, δηλαδή το ζεύγος $(H, *)$ είναι και αυτό μονοειδές με ουδέτερο στοιχείο e.

Παράδειγμα 4.4 Το ζεύγος $(\mathbb{N}, +)$ είναι υπομονοειδές του $(\mathbb{Z}, +)$ και τα $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$ υπομονοειδή του $(\mathbb{Q}, +)$. Επίσης, το ζεύγος $(\mathbb{N}, \cdot)$ είναι υπομονοειδές του $(\mathbb{Z}, \cdot)$ και τα $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ υπομονοειδή του $(\mathbb{Q}, \cdot)$.

Ας είναι $f : A \to B$ μία απεικόνιση. 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. Η αντίστροφη απεικόνιση θα συμβολίζεται ως συνήθως με f^{-1}.

Ας είναι $(A, *)$ και $(B, \diamond)$ μονοειδή με ουδέτερα στοιχεία e_A και e_B, αντίστοιχα. Μία απεικόνιση $f : A \to B$ καλείται *μορφισμός μονοειδών,* αν ισχύουν τα εξής:

1. $f(e_A) = e_B$.
2. $f(x * y) = f(x) \diamond f(y)$, για κάθε $x, y \in A$.

Παράδειγμα 4.5 Η απεικόνιση

$$f : \mathbb{N} \longrightarrow \mathbb{Z},\ x \longmapsto 2^x$$

είναι ένας μορφισμός από το μονοειδές $(\mathbb{N}, +)$ στο $(\mathbb{Z}, \cdot)$. Πράγματι, έχουμε $f(0) = 1$ και για κάθε $x, y \in \mathbb{N}$ ισχύει:

$$f(x + y) = 2^{x+y} = 2^x 2^y = f(x)f(y).$$

Πρόταση 4.1 *Η σύνθεση δύο μορφισμών μονοειδών είναι μορφισμός μονοειδών.*

Απόδειξη. Ας είναι $(A, *)$, $(B, \diamond)$, $(C, \triangleright)$ μονοειδή με ουδέτερα στοιχεία e_A, e_B, e_C αντίστοιχα και $f : A \to B$, $f : B \to C$ μορφισμοί μονοειδών. Θα δείξουμε ότι η απεικόνιση $g \circ f$ είναι μορφισμός μονοειδών. Ας είναι $x, y \in A$. Τότε:

$$\begin{aligned}(g \circ f)(x * y) &= g(f(x * y)) = \\ &g(f(x) \diamond f(y)) = g(f(x)) \triangleright g(f(y)) = (g \circ f)(x) \triangleright (g \circ f)(y).\end{aligned}$$

Επίσης, ισχύει:

$$(g \circ f)(e_A) = g(f(e_A)) = g(e_B) = e_C. \quad \square$$

Ένας μορφισμός μονοειδών που είναι ένεση (αντίστοιχα *έφεση*) καλείται *μονομορφισμός* (αντίστοιχα *επιμορφισμός*). Ένας μορφισμός που είναι αμφίεση καλείται *ισομορφισμός* . Σ' αυτή την περίπτωση, λέμε ότι τα μονοειδή είναι *ισόμορφα* και γράφουμε $A \cong B$.

Πρόταση 4.2 *Η αντίστροφη απεικόνιση ενός ισομορφισμού μονοειδών είναι επίσης ισομορφισμός μονοειδών.*

Απόδειξη. Ας είναι $(M, *)$, $(N, \diamond)$ μονοειδή και $f : M \to N$ ισομορφισμός μονοειδών. Αν $y_1, y_2 \in N$, τότε υπάρχουν $x_1, x_2 \in M$ με $y_1 = f(x_1)$ και $y_2 = f(x_2)$. Έχουμε:

$$f^{-1}(y_1 \diamond y_2) = f^{-1}(f(x_1) \diamond f(x_2)) = f^{-1}(f(x_1 * x_2)) =$$
$$(f^{-1} \circ f)(x_1 * x_2) = I_G(x_1 * x_2) = x_1 * x_2 = f^{-1}(y_1) * f^{-1}(y_2).$$

Αν e_M, e_N είναι τα ουδέτερα στοιχεία των M και N, αντίστοιχα, τότε $f(e_M) = e_N$ και επομένως $f^{-1}(e_N) = e_M$. Συνεπώς, η f^{-1} είναι μορφισμός μονοειδών. □

Ας είναι $(G, *)$ μονοειδές με ουδέτερο στοιχείο e και $x \in G$. Ας υποθέσουμε ότι υπάρχει $y \in G$ τέτοιο, ώστε

$$x * y = e = y * x.$$

Σ′ αυτή την περίπτωση το στοιχείο y είναι μοναδικό. Πράγματι, αν y' είναι ένα άλλο στοιχείο με αυτή την ιδιότητα, τότε:

$$y = y * e = y * (x * y') = (y * x) * y' = e * y' = y'.$$

Το στοιχείο y καλείται *συμμετρικό* του x. Παρατηρούμε ότι το συμμετρικό του e είναι ο εαυτός του. Επίσης, το συμμετρικό του y είναι το x. Ας σημειωθεί ότι σ′ ένα μονοειδές κάθε στοιχείο δεν έχει πάντα συμμετρικό.

Παράδειγμα 4.6 Στο μονοειδές $(\mathbb{Z}, \cdot)$ το μόνο στοιχείο, εκτός του 1, που έχει συμμετρικό είναι το -1 και το συμμετρικό του είναι ο εαυτός του.

Παράδειγμα 4.7 Ας είναι f μία αριθμητική συνάρτηση. Αν η f έχει συμμετρικό στοιχείο g, τότε η g καλείται *ενελικτική αντίστροφος* της f και συμβολίζεται με f^*. Η αριθμητική συνάρτηση g είναι ενελικτική αντίστροφος της f αν και μόνον αν $g * f = \epsilon$, που ισοδυναμεί με $g(1)f(1) = 1$ και

$$\sum_{ab=n} g(a)f(b) = 0,$$

για κάθε φυσικό $n > 1$. Αντίστροφα, αν $f(1) \neq 0$, τότε μπορούμε να υπολογίσουμε επαγωγικά τις τιμές της f^* από το παραπάνω άθροισμα. Δηλαδή, έχουμε $f^*(1) = 1/f(1)$, $f^*(2) = -f(2)f^*(1)/f(1)$ και

γενικότερα για κάθε φυσικό $n > 1$ ισχύει

$$f^*(n) = -\frac{1}{f(1)} \sum_{st=n,\ t<n} f(s)f^*(t).$$

Συνεπώς, η f έχει ενελικτική αντίστροφο αν και μόνον αν $f(1) \neq 0$.

Συχνά συμβολίζουμε μία πράξη σ΄ ένα σύνολο E είτε ως πρόσθεση είτε ως πολλαπλασιασμό. Στην πρώτη περίπτωση, το αποτέλεσμα της εφαρμογής της πράξης σε δύο στοιχεία $x, y \in E$ συμβολίζεται με $x + y$ και καλείται *άθροισμα* των x και y. Αν η πράξη έχει ουδέτερο στοιχείο, τότε αυτό συμβολίζεται με 0 και καλείται *μηδενικό*. Το συμμετρικό στοιχείο ενός $x \in E$ συμβολίζεται με $-x$ και καλείται *αντίθετο* του x. Στη δεύτερη περίπτωση, το αποτέλεσμα της εφαρμογής της πράξης στα x και y συμβολίζεται με xy και καλείται γινόμενο των x και y. Το ουδέτερο στοιχείο της πράξης, αν υπάρχει, συμβολίζεται με 1 και καλείται *μοναδιαίο*. Επίσης, το συμμετρικό στοιχείο ενός $x \in E$ συμβολίζεται με x^{-1} και καλείται *αντίστροφο* του x. Ένα μονοειδές στο οποίο η πράξη συμβολίζεται ως πρόσθεση (αντίστοιχα πολλαπλασιασμός) καλείται προσθετικό (αντίστοιχα πολλαπλασιαστικό). Ανάλογη ονομασία δίνουμε και στις ομάδες.

Ας είναι A ένα πολλαπλασιαστικό μονοειδές. Συμβολίζουμε με A^* το σύνολο των στοιχείων του A που έχουν αντίστροφο. Παρατηρούμε ότι $1 \in A^*$ και επομένως $A \neq \emptyset$. Αν τα στοιχεία $a, b \in A^*$ έχουν αντίστροφο, τότε $ab, a^{-1} \in A^*$ και ισχύουν τα εξής:

$$(ab)^{-1} = b^{-1}a^{-1}, \quad (a^{-1})^{-1} = a.$$

Πράγματι, έχουμε:

$$(ab)(b^{-1}a^{-1}) = (a(b(b^{-1}a^{-1}))) = (a((bb^{-1})a^{-1})) = aa^{-1} = 1.$$

Όμοια παίρνουμε:

$$(b^{-1}a^{-1})(ab) = 1.$$

Συνεπώς, $(ab)^{-1} = b^{-1}a^{-1}$. Επίσης, από τις σχέσεις

$$aa^{-1} = 1 \quad \text{και} \quad a^{-1}a = 1$$

έπεται $(a^{-1})^{-1} = a$. Από τα παραπάνω προκύπτει αμέσως, ότι αν $a, b \in A^*$, τότε έχουμε $ab \in A^*$ και $a^{-1} \in A^*$.

Ας είναι $f : A \to B$ ένας μορφισμός (πολλαπλασιαστικών) μονοειδών. Αν ένα στοιχείο $x \in A$ έχει αντίστροφο, τότε το $f(x)$ έχει αντίστροφο στοιχείο και ισχύει $f(x)^{-1} = f(x^{-1})$. Πράγματι, έχουμε:

$$1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}).$$

Όμοια, παίρνουμε $f(x^{-1})f(x) = 1$. Συνεπώς, $f(x)^{-1} = f(x^{-1})$. Άρα $f(A^*) \subseteq B^*$. Αν ο μορφισμός f είναι ισομορφισμός, τότε έχουμε $f^{-1}(B^*) \subseteq A^*$, απ' όπου $B^* \subseteq f(A^*)$. Συνεπώς, σ' αυτή την περίπτωση, ισχύει $f(A^*) = B^*$.

Ας είναι A ένα πολλαπλασιαστικό μονοειδές και $a \in A$. Για κάθε φυσικό n ορίζουμε $a^0 = 1$ και $a^n = a^{n-1}a$. Αν το στοιχείο a είναι αντιστρέψιμο και $n = -m$, όπου m θετικός ακέραιος, τότε ορίζουμε $a^n = (a^{-1})^m$. Για κάθε ζεύγος φυσικών k, l ισχύουν τα εξής:

$$a^{k+l} = a^k a^l, \quad (a^k l)^n = a^{kl}.$$

Αν το a είναι αντιστρέψιμο, τότε οι παραπάνω ιδιότητες ισχύουν γενικότερα για ακέραιους k, l.

Πρόταση 4.3 *Ας είναι A ένα πολλαπλασιαστικό μονοειδές, $a \in A$ και k θετικός ακέραιος. Τότε ο υπολογισμός του a^k απαιτεί λιγότερο από $2\ell(k)$ πράξεις μεσα στο A.*

Απόδειξη. Ας είναι $k = e_1 2^{l-1} + \cdots + e_l$ η δυαδική παράσταση του k. Οπότε, έχουμε:

$$a^k = \prod_{i=0}^{l-1} (a^{2^i})^{e_{l-i}}.$$

Πρώτα υπολογίζουμε το a^2 και κατόπιν το $a^{e_l + 2e_{l-1}}$. Στη συνέχεια, υπολογίζουμε το a^4 (υψώνοντας στο τετράγωνο τον a^2 που έχουμε ήδη βρεί) και μετά προσδιορίζουμε το $a^{e_l + e_{l-1}2 + e_{l-2}2^2}$. Συνεχίζοντας μ' αυτό τον τρόπο παίρνουμε το αποτέλεσμα. Η συνολική διαδικασία ολοκληρώθηκε σε λιγότερο από $2l$ βήματα. □

4.2 Ομάδες

Η ενότητα αυτή είναι αφιερωμένη στην περιγραφή βασικών ιδιοτήτων μίας από των σημαντικότερων αλγεβρικών δομών, των ομάδων.

4.2.1 Ορισμός -Παραδείγματα

Ένα μονοειδές τέτοιο, ώστε κάθε στοιχείο του έχει συμμετρικό καλείται *ομάδα.* Αν επιπλέον αυτό το μονοειδές είναι και αντιμεταθετικό, τότε καλείται *αντιμεταθετική ή αβελιανή ομάδα.* Θα υιοθετήσουμε για απλότητα τον πολλαπλασιαστικό συμβολίσμό για τις ομάδες.

Αν G είναι ομάδα, τότε για κάθε $a, b, x \in G$ ισχύουν οι εξής νόμοι απλοποίησης:

$$xa = xb \Longrightarrow a = b, \qquad ax = bx \Longrightarrow a = b.$$

Πολλαπλασιάζοντας την ισότητα $xa = xb$ από αριστερά με x^{-1} παίρνουμε

$$x^{-1}(xa) = x^{-1}(xb) \Longrightarrow (x^{-1}x)a = (x^{-1}x)b \Longrightarrow 1a = 1b$$

και επομένως $a = b$. Η απόδειξη της δεύτερης συνεπαγωγής είναι ανάλογη.

Παράδειγμα 4.8 Τα ζεύγη $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ και $(\mathbb{Q} \setminus \{0\}, \cdot)$ είναι αντιμεταθετικές ομάδες.

Παράδειγμα 4.9 Αν G_i $(i = 1, \ldots, k)$ είναι πολλαπλασιαστικές ομάδες, τότε το μονοειδές $G_1 \times \cdots \times G_k$ είναι ομάδα. Το αντίστροφο ενός στοιχείου $(x_1, \ldots, x_n)$ είναι το $(x_1^{-1}, \ldots, x_n^{-1})$.

Παράδειγμα 4.10 Ας είναι A ένα πολλαπλασιαστικό μονοειδές και A^* το σύνολο των στοιχείων του A που έχουν αντίστροφο. Είδαμε στην προηγούμενη ενότητα ότι για κάθε $a, b \in A^*$ έχουμε $ab \in A^*$, $1 \in A^*$ και $a^{-1} \in A^*$. Επίσης, ισχύει η προσεταιριστική ιδιότητα για τον πολλαπλασιασμό. Συνεπώς, το ζεύγος $(A^*, \cdot)$ αποτελεί ομάδα.

Παράδειγμα 4.11 Μία αριθμητική συνάρτηση f καλείται *πολλαπλασιαστική,* αν είναι μη μηδενική, δηλαδή υπάρχει $n \in \mathbb{N}\setminus\{0\}$ με $f(n) \neq 0$, και για κάθε $a, b \in \mathbb{N} \setminus \{0\}$ με $\mu\kappa\delta(a, b) = 1$ ισχύει $f(ab) = f(a)f(b)$. Παραδείγματα τέτοιων συναρτήσεων είναι οι τ, σ και μ. Θα δείξουμε ότι το σύνολο των πολλαπλασιαστικών συναρτήσεων $\mathcal{M}$, εφοδιασμένο με τον ενελικτικό πολλαπλασιασμό, αποτελεί ομάδα.

Ας είναι $f, g \in \mathcal{M}$ και $a, b \in \mathbb{N} \setminus \{0\}$ με $\mu\kappa\delta(a, b) = 1$. Έχουμε

$$(f * g)(ab) = \sum_{cd=ab} f(c)g(d) = \sum_{d|ab} f(d)g(ab/d),$$

όπου (c, d) διατρέχει το σύνολο των ζευγών φυσικών αριθμών που το γινόμενό τους ισούται με ab και d διατρέχει το σύνολο των φυσικών διαιρετών του ab. Σύμφωνα με το Πόρισμα 3.2, οι ακέραιοι mn με $m, n \in \mathbb{N}$ και $m|a$, $n|b$ είναι διαφορετικοί ανά δύο και δίνουν όλους τους φυσικούς διαιρέτες του ab. Καθώς $\mu\kappa\delta(a, b) = 1$ συνεπάγεται ότι $\mu\kappa\delta(m, n) = \mu\kappa\delta(a/m, b/n) = 1$. Έτσι, έχουμε:

$$\begin{aligned}(f * g)(ab) &= \sum_{m|a,n|b} f(mn)g(ab/mn) \\ &= \sum_{m|a,n|b} f(m)f(n)g(a/m)g(b/n) \\ &= \left(\sum_{m|a} f(m)g(a/m)\right)\left(\sum_{n|b} f(n)g(b/n)\right) \\ &= (f * g)(a)(f * g)(b).\end{aligned}$$

Συνεπώς, ο ενελικτικός πολλαπλασιασμός είναι μία πράξη επί του $\mathcal{M}$.

Για κάθε $f \in \mathcal{M}$ ισχύει $f(1) = 1$. Πράγματι, επειδή η f είναι μη μηδενική, υπάρχει $n \in \mathbb{N} \setminus \{0\}$ με $f(n) \neq 0$. Έχουμε:

$$f(n) = f(1n) = f(1)f(n),$$

απ' όπου έπεται $f(1) = 1$. Οπότε, η f έχει ενελικτή αντίστροφο f^*. Θα δείξουμε ότι η συνάρτηση f^* είναι πολλαπλασιαστική. Τότε $f^*(1) = 1/f(1) = 1$ και επομένως $f^*(1) = 1 = f^*(1)f^*(1)$. Ας είναι k ακέραιος > 1 και ας υποθέσουμε ότι για κάθε $s, t \in \mathbb{N} \setminus \{0\}$ με $\mu\kappa\delta(s, t) = 1$ και $st < k$ ισχύει $f^*(st) = f^*(s)f^*(t)$. Θεωρούμε $a, b \in \mathbb{N} \setminus \{0\}$ με $\mu\kappa\delta(a, b) = 1$ και $ab = k$. Από την ισότητα $\epsilon(ab) = \epsilon(a)\epsilon(b)$ έχουμε:

$$(f^* * f)(ab) = (f^* * f)(a)(f^* * f)(b)$$

και επομένως ισχύει:

$$\sum_{m|a,n|b} f^*(mn)f(ab/mn) = \left(\sum_{m|a} f^*(m)f(a/m)\right)\left(\sum_{n|b} f^*(n)f(b/n)\right),$$

όπου m και n διατρέχουν το σύνολο των θετικών διαιρετών του a και b αντίστοιχα. Έτσι, παίρνουμε:

$$\sum_{m|a,n|b} (f^*(mn) - f^*(m)f^*(n))f(ab/mn) = 0.$$

Από την υπόθεση της επαγωγής ισχύει $f^*(mn) = f^*(m)f^*(n)$ για κάθε $m, n \in \mathbb{N} \setminus \{0\}$ με $\mu\kappa\delta(m, n) = 1$ και $mn < ab$. Επίσης, έχουμε $mn = ab$, αν και μόνον αν $m = a$ και $n = b$. Συνεπώς $f^*(ab) = f^*(a)f^*(b)$. Άρα η συνάρτηση f^* είναι πολλαπλασιαστική. Καθώς ο ενελικτικός πολλαπλασιασμός είναι προσεταιριστική και αντιμεταθετική πράξη, έπεται ότι το ζεύγος $(\mathcal{M}, *)$ είναι μία αντιμεταθετική ομάδα.

Παράδειγμα 4.12 Ας είναι X ένα μη κενό σύνολο. Το σύνολο των αμφιέσεων $S(X)$ από το X στο X με πράξη την σύνθεση απεικονίσεων αποτελεί ομάδα. Πράγματι, για κάθε τριάδα απεικονίσεων $f : X \to X$, $g : X \to X$ και $h : X \to X$ ισχύει $f \circ (g \circ h) = (f \circ g) \circ h$. Αν I_X είναι η ταυτοτική απεικόνιση του X, δηλαδή ισχύει $I_X(x) = x$, για κάθε $x \in X$, τότε $f \circ I_X = f = I_X \circ f$ και επομένως η I_X είναι το ουδέτερο στοιχείο για την σύνθεση απεικονίσεων. Τέλος, για κάθε αμφίεση από το X στο X υπάρχει η αντίστροφή της η οποία είναι επίσης αμφίεση.

Παράδειγμα 4.13 Ας είναι $E_n = \{1, 2, \ldots, n\}$ και S_n το σύνολο των αμφιέσεων από το E_n στο E_n. Σύμφωνα με το προηγούμενο παράδειγμα, το σύνολο S_n είναι ομάδα με πράξη την σύνθεση απεικονίσεων η οποία καλείται *συμμετρική ομάδα βαθμού* n. Τα στοιχεία της καλούνται *μεταθέσεις*. Θα συμβολίζουμε πιο απλά την σύνθεση δύο μεταθέσεων σ και τ με $\sigma\tau$ και με e την ταυτοτική μετάθεση.

Κάθε $\sigma \in S_n$ μπορεί να παρασταθεί από ένα πίνακα της μορφής

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Για παράδειγμα, ο πίνακας

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 3 & 2 \end{pmatrix}$$

παριστάνει την μετάθεση $\sigma \in S_4$ με $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 3$ και $\sigma(4) = 2$.

Για να ορίσουμε μία μετάθεση σ του S_n μπορούμε να πάρουμε ως $\sigma(1)$ οποιοδήποτε από τους αριθμούς $1, 2, \ldots, n$ και επομένως υπάρχουν n τρόποι για να γίνει αυτό. Κατόπιν, μπορούμε να πάρουμε ως $\sigma(2)$ οποιοδήποτε από τους υπόλοιπους $n - 1$ αριθμούς και υπάρχουν $n - 1$ τρόποι για να γίνει αυτό. Δηλαδή υπάρχουν $n(n - 1)$ τρόποι για να

επιλέξουμε τα στοιχεία $\sigma(1)$ και $\sigma(2)$. Συνεχίζοντας αυτή τη διαδικασία, βλέπουμε ότι υπάρχουν

$$n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 = n!$$

τρόποι για να επιλέξουμε τα στοιχεία $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Συνεπώς, το σύνολο S_n έχει $n!$ στοιχεία.

4.2.2 Υποομάδες

Ας είναι G ομάδα και H ένα μη κενό υποσύνολο του G. Το H καλείται *υποομάδα* της G αν το H είναι υπομονοειδές της G και για κάθε $x \in H$ έχουμε $x^{-1} \in H$. Δηλαδή, το H είναι ομάδα με πράξη τον περιορισμό της πράξης της G στα στοιχεία του H. Εύκολα διαπιστώνουμε ότι το H είναι υποομάδα αν και μόνον αν ισχύουν τα εξής:

1. Για κάθε $x, y \in H$ έχουμε $xy \in H$.
2. Για κάθε $x \in H$ ισχύει $x^{-1} \in H$.

Οι δύο ιδιότητες μπορούν να συνοψιστούν σε μία όπως βλέπουμε στην παρακάτω πρόταση.

Πρόταση 4.4 *Το σύνολο H είναι υποομαδα του G αν και μόνον αν για κάθε $x, y \in H$ ισχύει $xy^{-1} \in H$.*

Απόδειξη. Ας υποθέσουμε ότι το H είναι υποομαδα του G. Αν $x, y \in H$, τότε $x, y^{-1} \in H$ και επομένως $xy^{-1} \in H$. Αντίστροφα, ας υποθέσουμε ότι για κάθε $x, y \in H$ ισχύει $xy^{-1} \in H$. Αν $x \in H$, τότε $1 = xx^{-1} \in H$. Έτσι, για κάθε $y \in H$ έχουμε $y^{-1} = 1y^{-1} \in H$. Επίσης, για κάθε $x, y \in H$ έχουμε $x, y^{-1} \in H$ και καθώς $(y^{-1})^{-1} = y$, έχουμε $xy \in H$. Άρα το H είναι υποομάδα της G. □

Παράδειγμα 4.14 Ας είναι G ομάδα. Τα σύνολα G και $\{1\}$ αποτελούν υποομάδες της G οι οποίες καλούνται *τετριμμένες*. Κάθε άλλη υποομάδα της G καλείται *μη τετριμμένη ή γνήσια*.

Παράδειγμα 4.15 Ας είναι S ένα μη-κενό υποσύνολο της G. Θα δείξουμε ότι το σύνολο

$$\langle S \rangle = \{x_1^{a_1} \cdots x_n^{a_n} / \ n \geq 1,\ x_i \in S,\ a_i \in \mathbb{Z}\}.$$

είναι μία υποομάδα της G που περιέχει το S και καλείται *υποομάδα παραγόμενη από το* S.

Πράγματι, αν $z = x_1^{a_1} \cdots x_m^{a_m}$ και $w = y_1^{b_1} \cdots y_r^{b_r}$ είναι δύο στοιχεία του $\langle S \rangle$ έχουμε:

$$zw^{-1} = x_1^{a_1} \cdots x_m^{a_m} (y_1^{b_1} \cdots y_r^{b_r})^{-1} = x_1^{a_1} \cdots x_m^{a_m} y_r^{-b_r} \cdots y_1^{-b_1}$$

και επομένως $zw^{-1} \in H$. Έτσι, το $\langle S \rangle$ είναι υποομάδα. Επίσης, από τον ορισμό της $\langle S \rangle$ έχουμε $S \subseteq \langle S \rangle$.

Αν $S = \{a_1, \ldots, a_k\}$, τότε θα γράφουμε πιο απλά $\langle a_1, \ldots, a_k \rangle$ αντί $\langle \{a_1, \ldots, a_k\} \rangle$.

Παράδειγμα 4.16 Εύκολα βλέπουμε ότι τα ζεύγη $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ και $(\mathbb{R}, +)$ είναι υποομάδες της $(\mathbb{C}, +)$. Επίσης, τα ζεύγη $(\mathbb{Q} \setminus \{0\}, \cdot)$ και $(\mathbb{R} \setminus \{0\}, \cdot)$ είναι υποομάδες της $(\mathbb{C} \setminus \{0\}, \cdot)$.

Παράδειγμα 4.17 Ας είναι n ακέραιος ≥ 2. Ένας μιγαδικός αριθμός z τέτοιος, ώστε $z^n = 1$ καλείται *n-οστή ρίζα της μονάδας*. Συμβολίζουμε με $\mathcal{M}_n$ το σύνολο όλων των n-οστών ριζών της μονάδας. Καθώς $1 \in \mathcal{M}_n$, έχουμε $\mathcal{M}_n \neq \emptyset$. Επίσης, $\mathcal{M}_n \subset \mathbb{C}^\star$. Για κάθε ζεύγος $x, y \in \mathcal{M}_n$ έχουμε $x^n = y^n = 1$ και επομένως $(xy^{-1})^n = 1$, απ' όπου $xy^{-1} \in \mathcal{M}_n$. Άρα, το σύνολο $\mathcal{M}_n$ είναι υποομάδα της $\mathbb{C}^\star$.

4.2.3 Τάξη Στοιχείου - Κυκλικές Ομάδες

Ας είναι G ομάδα. Αν υπάρχει $a \in G$ τέτοιο, ώστε $G = \langle a \rangle$, τότε η G καλείται *μονογενής* και το στοιχείο a *γεννήτορας* της G. Διακρίνουμε τις εξής περιπτώσεις:

(α) Για κάθε ζεύγος ακεραίων k, l με $k \neq l$ έχουμε $a^k \neq a^l$. Τότε η ομάδα G έχει άπειρο πλήθος στοιχείων.

(β) Υπάρχουν ακέραιοι k, l με $k < l$ έτσι, ώστε $a^k = a^l$. Τότε $a^{l-k} = 1$. Ας είναι m ο μικρότερος θετικός τέτοιος, ώστε $a^m = 1$. Τότε τα στοιχεία $1, a, \ldots, a^{m-1}$ είναι διαφορετικά ανά δύο και είναι όλα τα στοιχεία της G. Πράγματι, αν $a^r = a^s$ με $0 \leq r < s < m$, τότε έχουμε $a^{r-s} = 1$ και $0 < r - s < m$ που είναι άτοπο. Άρα, τα στοιχεία $1, a, \ldots, a^{m-1}$ είναι διαφορετικά ανά δύο. Αν $x = a^n$ είναι στοιχείο της G, τότε υπάρχουν $q, r \in \mathbb{Z}$ με $n = qm + r$ και $0 \leq r < m$. Επομένως:

$$x = a^n = a^{qm+r} = (a^m)^q a^r = a^r$$

και κατά συνέπεια το x είναι κάποιο από τα $1, a, \ldots, a^{m-1}$.

Στην περίπτωση (α) λέμε ότι το στοιχείο a έχει *άπειρη τάξη* ενώ στη (β) ο θετικός ακέραιος m καλείται *τάξη* του a και η ομάδα $G = \{1, a, \ldots, a^{m-1}\}$ *κυκλική τάξης* m με γεννήτορα το a. Η τάξη του a συμβολίζεται με $\mathrm{ord}(a)$.

Γενικότερα, καλούμε *τάξη* μίας ομάδας το πλήθος των στοιχείων της.

Παράδειγμα 4.18 Η ομάδα $(\mathbb{Z}, +)$ είναι μονογενής ομάδα με γεννήτορες τα στοιχεία 1 και -1 τα οποία είναι άπειρης τάξης.

Παράδειγμα 4.19 Θεωρούμε την ομάδα $\mathcal{M}_n$ του Παραδείγματος 4.17. Ας είναι

$$z = re^{\pi\theta\imath} = r(\cos\theta + \imath\sin\theta),$$

(όπου $\imath = \sqrt{-1}$) ένας μιγαδικός αριθμός με $z^n = 1$. Τότε

$$r^n(\cos(n\theta) + \imath\sin(n\theta)) = 1,$$

απ' όπου $r = 1$ και $\theta = 2k\pi/n$, όπου $k \in \mathbb{Z}$. Επομένως, οι n-οστές ρίζες της μονάδας είναι οι αριθμοί:

$$z_k = \cos\frac{2k\pi}{n} + \imath\sin\frac{2k\pi}{n}, \quad k \in \mathbb{Z}.$$

Έχουμε $z_l = z_m$, αν και μόνον αν $2l\pi/n = 2m\pi/n + 2k\pi$ με $k \in \mathbb{Z}$. Συνεπώς, οι διαφορετικές ανά δύο n-οστές ρίζες της μονάδες είναι οι αριθμοί:

$$z_k = z_1^k, \quad (k = 0, 1, \ldots, n-1).$$

Άρα, η ομάδα $\mathcal{M}_n$ είναι κυκλική με γεννήτορα το στοιχείο z_1 το οποίο έχει τάξη n.

Πρόταση 4.5 *Ας είναι G ομάδα και $a \in G$. Τότε $\mathrm{ord}(a) = m$ αν και μόνον αν για κάθε θετικό ακέραιο k ισχύει το εξής:*

$$a^k = 1 \iff m|k.$$

Απόδειξη. Ας υποθέσουμε ότι $\mathrm{ord}(a) = m$. Αν $a^k = 1$, τότε υπάρχουν ακέραιοι q, r με $k = mq + r$ και $0 \le r < m$. Έτσι, έχουμε:

$$1 = a^k = a^{mq+r} = (a^m)^q a^r = a^r.$$

Αν $r > 0$, τότε, καθώς $a^r = 1$ και $r < m$, καταλήγουμε σε άτοπο. Άρα $r = 0$ και επομένως $m|k$. Αντίστροφα, αν $m|k$, τότε η ισότητα $a^m = 1$ δίνει $a^k = 1$.

Στη συνέχεια, ας υποθέσουμε ότι ισχύει:

$$a^k = 1 \iff m|k.$$

Η σχέση $m|m$ δίνει $a^m = 1$. Επίσης, αν $a^k = 1$, τότε $m|k$ και επομένως $m \leq k$. Άρα έχουμε $\mathrm{ord}(a) = m$. □

Πόρισμα 4.1 *Ας είναι G ομάδα και $a \in G$ ένα στοιχείο τάξης m. Ισχύει:*

$$a^k = a^l \iff m|k-l.$$

Απόδειξη. Χρησιμοποιώντας την Πρόταση 4.5 παίρνουμε:

$$a^k = a^l \Longleftrightarrow a^k(a^l)^{-1} = 1 \Longleftrightarrow a^{k-l} = 1 \Longleftrightarrow m|k-l. \quad \square$$

Πόρισμα 4.2 *Ας είναι G μία ομάδα τάξης $m < \infty$. Αν $a \in G$, τότε $a^m = 1$ και $\mathrm{ord}(a)|m$.*

Απόδειξη. Θεωρούμε την απεικόνιση

$$f : G \longrightarrow G,\ x \longmapsto ax.$$

Αν $f(x) = f(y)$, τότε $ax = ay$ και επομένως $x = y$. Άρα, η f είναι ένεση και καθώς η ομάδα G είναι πεπερασμένη, είναι και αμφίεση. Έτσι, αν $G = \{x_1, \ldots, x_m\}$, τότε $G = \{ax_1, \ldots, ax_m\}$. Επομένως, έχουμε:

$$a^m x_1 \cdots x_m = x_1 \cdots x_m,$$

απ'οπου παίρνουμε $a^m = 1$. Επίσης, από την Πρόταση 4.5 έχουμε $\mathrm{ord}(a)|m$. □

Πρόταση 4.6 *Ας είναι $G = \{1, a, \ldots, a^{m-1}\}$ μία κυκλική ομάδα τάξης m. Σε κάθε θετικό διαιρέτη q του m αντιστοιχεί η υποομάδα τάξης m/q,*

$$\langle a^q \rangle = \{1, a^q, a^{2q}, \ldots, a^{(m/q-1)q}\},$$

και κάθε υποομάδα της G είναι της παραπάνω μορφής.

Απόδειξη. Ας είναι H μία υποομάδα της G. Αν $H = \{1\}$, τότε έχουμε $H = \langle 1 \rangle$. Ας υποθέσουμε ότι $H \neq \{1\}$ και ας είναι q ο μικρότερος θετικός ακέραιος τέτοιος, ώστε $a^q \in H$. Έχουμε $\langle a^q \rangle \subseteq H$. Από την άλλη πλευρά, ας είναι $a^k \in H$. Υπάρχουν s και r ακέραιοι με $k = sq + r$ και $0 \leq r < q$. Τότε, έχουμε

$$a^k = a^{sq+r} = a^{sq} a^r$$

και επομένως

$$a^r = a^k (a^{sq})^{-1}.$$

Καθώς $a^k, a^{sq} \in H$, έχουμε $a^r \in H$. Αν $r > 0$, τότε καταλήγουμε σε άτοπο γιατί ο q είναι ο μικρότερος θετικός εκθέτης με $a^q \in H$. Άρα $r = 0$ και επομένως $a^k = a^{sq}$, απ' όπου $a^k \in \langle a^q \rangle$. Συνεπώς, $H = \langle a^q \rangle$.

Θα δείξουμε στη συνέχεια ότι $q|m$. Έχουμε $m = qd + e$, όπου d, e ακέραιοι και $0 \leq e < q$. Οπότε

$$1 = a^m = a^{qd+e} = (a^q)^d a^e$$

και επομένως $a^e = (a^q)^{-d} \in H$. Αν $e > 0$, τότε καταλήγουμε σε άτοπο γιατί ο q είναι ο μικρότερος θετικός ακέραιος με $a^q \in H$. Άρα $e = 0$ και επομένως $q|m$.

Έχουμε $(a^q)^{m/q} = 1$. Από την άλλη πλευρά, αν t είναι θετικός ακέραιος με $(a^q)^t = 1$, τότε $m|qt$ και επομένως $(m/q)|t$. Άρα, σύμφωνα με την Πρόταση 4.5, έχουμε $\mathrm{ord}(a^q) = m/q$. □

Πρόταση 4.7 *Ας είναι $G = \{1, a, \ldots, a^{m-1}\}$ μία κυκλική ομάδα τάξης m. Αν $k \in \{0, 1, \ldots, m-1\}$ και $d = \mu\kappa\delta(m, k)$, τότε ισχύει $\langle a^k \rangle = \langle a^d \rangle$ και $\mathrm{ord}(a^k) = m/d$.*

Απόδειξη. Καθώς $d|k$, υπάρχει ακέραιος l με $k = dl$ και επομένως $a^k = (a^d)^l$. Άρα $a^k \in \langle a^d \rangle$ και κατά συνέπεια $\langle a^k \rangle \subseteq \langle a^d \rangle$. Από την άλλη πλευρά, υπάρχουν ακέραιοι x, y έτσι, ώστε $d = kx + my$. Οπότε:

$$a^d = a^{kx+my} = (a^k)^x (a^m)^y = (a^k)^x 1^y = (a^k)^x$$

και επομένως $a^d \in \langle a^k \rangle$. Άρα $\langle a^d \rangle \subseteq \langle a^k \rangle$. Έτσι, παίρνουμε $\langle a^d \rangle = \langle a^k \rangle$.

Επίσης, έχουμε:

$$(a^k)^{m/d} = (a^{dl})^{m/d} = a^{lm} = 1.$$

Αν s είναι θετικός ακέραιος με $(a^k)^s = 1$, τότε

$$(a^d)^s = a^{kxs} = 1.$$

Από την Πρόταση 4.6 έχουμε $\mathrm{ord}(a^d) = m/d$ και επομένως $(m/d)|s$. Άρα $\mathrm{ord}(a^k) = m/d$. $\square$

Πόρισμα 4.3 *Ας είναι $G = \{1, a, \ldots, a^{m-1}\}$ μία κυκλική ομάδα τάξης m. Τότε, ισχύει:*

$$G = \langle a^k \rangle \iff \mu\kappa\delta(m, k) = 1.$$

4.2.4 Μορφισμοί Ομάδων

Ας είναι A και B ομάδες. Μία απεικόνιση $f : A \to B$ καλείται *μορφισμός ομάδων,* αν για κάθε $x, y \in A$ ισχύει $f(xy) = f(x)f(y)$. Τότε, έχουμε:

$$f(1) = f(1 \cdot 1) = f(1)f(1).$$

Πολλαπλασιάζοντας και τα δύο μέλη με το αντίστροφο στοιχείο του $f(1)$, παίρνουμε $f(1) = 1$. Συνεπώς, ένας μορφισμός ομάδων δεν είναι παρά ένας μορφισμός των αντίστοιχων μονοειδών. Έτσι από την Πρόταση 4.1 έπεται αμέσως η σύνθεση δύο μορφισμών ομάδων είναι μορφισμός ομάδων.

Ένας μορφισμός ομάδων καλείται *μονομορφισμός, επιμορφισμός, ισομορφισμός,* αν αντίστοιχα είναι ένεση, έφεση, αμφίεση. Αν η απεικόνιση f είναι ισομορφισμός, τότε οι ομάδες A και B καλούνται *ισόμορφες* και γράφουμε $A \cong B$. Σ′ αυτή την περίπτωση, από την Πρόταση 4.2 έχουμε ότι και η απεικόνιση $f^{-1} : B \to A$ είναι ισομορφισμός ομάδων. Ένας μορφισμός $f : G \to G$ καλείται *ενδομορφισμός*. Αν ένας ενδομορφισμός είναι αμφίεση, τότε καλείται *αυτομορφισμός*.

Παράδειγμα 4.20 Η απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Q},\ x \longmapsto 2^x$$

είναι ένας μορφισμός από την ομάδα $(\mathbb{Z}, +)$ στη $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Ας είναι $f : G \to H$ ένας μορφισμός ομάδων. Το σύνολο

$$\mathrm{Ker}(f) = \{x \in G/\ f(x) = 1\}$$

καλείται *πυρήνας* του f.

Πρόταση 4.8 *Ο πυρήνας του f είναι υποομάδα του G. Επίσης, ο μορφισμός f είναι ένεση αν και μόνον αν* $\mathrm{Ker}(f) = \{1\}$.

Απόδειξη. Καθώς ισχύει $f(1) = 1$, το σύνολο $\mathrm{Ker}(f)$ είναι μη κενό. Ας είναι $x, y \in \mathrm{Ker}(f)$. Τότε, έχουμε:

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1$$

και κατά συνέπεια $xy^{-1} \in \mathrm{Ker}(f)$. Επομένως, το σύνολο $\mathrm{Ker}(f)$ είναι υποομάδα της G.

Αν ο μορφισμος f είναι ένεση, τότε για κάθε $x \in G$ με $f(x) = 1$ έχουμε $x = 1$ και επομένως $\mathrm{Ker}(f) = \{1\}$. Αντίστροφα, ας είναι $\mathrm{Ker}(f) = \{1\}$. Αν $f(x) = f(y)$, τότε έχουμε $f(x)f(y)^{-1} = 1$, απ΄ όπου $f(xy^{-1}) = 1$ και επομένως $xy^{-1} \in \mathrm{Ker}(f)$. Έτσι, έχουμε $xy^{-1} = 1$ και κατά συνέπεια $x = y$. Άρα η f είναι ένεση. □

Παράδειγμα 4.21 Θεωρούμε τον μορφισμό $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ του Παραδείγματος 4.20. Έχουμε $f(x) = 1$ αν και μόνον αν $2^x = 1$, δηλαδή αν και μόνον αν $x = 0$. Επομένως $\mathrm{Ker}(f) = \{1\}$ και κατά συνέπεια η f είναι ένεση.

4.3 Δακτύλιοι

Ας είναι A ένα μη κενό σύνολο εφοδιασμένο με δύο πράξεις, μία πρόσθεση $(x, y) \to x + y$ και ένα πολλαπλασιασμό $(x, y) \to xy$. Η τριάδα $(A, +, \cdot)$ καλείται *δακτύλιος* αν οι παραπάνω πράξεις έχουν τις εξής ιδιότητες:

1. Το ζεύγος $(A, +)$ είναι μία αβελιανή ομάδα.
2. Το ζεύγος $(A, \cdot)$ είναι ένα μονοειδές.
3. Ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση, δηλαδή για κάθε $x, y, z \in A$ έχουμε:

$$(x + y)z = xz + yz \qquad \text{και} \qquad x(y + z) = xy + xz.$$

Αν επιπλέον για κάθε $x, y \in A$ ισχύει $xy = yx$, τότε ο δακτύλιος A καλείται *αντιμεταθετικός*. Συμβολίζουμε με A^* το σύνολο των στοιχείων του A που έχουν αντίστροφο. Το ζεύγος $(A^*, \cdot)$ αποτελεί ομάδα. Ένας αντιμεταθετικός δακτύλιος A καλείται *σώμα*, αν $A^* = A \setminus \{0\}$.

Ας είναι A δακτύλιος. Τότε, εύκολα διαπιστώνουμε, ότι για κάθε $x \in A$ ισχύουν οι σχέσεις:

$$0x = 0 = x0, \quad (-1)x = -x = x(-1).$$

Αν $0 = 1$, τότε για κάθε $x \in A$ ισχύει:

$$x = x1 = x0 = 0$$

και επομένως $A = \{0\}$. Επίσης, για κάθε $x, y \in A$ ισχύουν οι σχέσεις:

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

Ας είναι A και B δακτύλιοι. Μία απεικόνιση $f : A \to B$ καλείται *μορφισμός δακτυλίων,* αν είναι μορφισμός για τις αντίστοιχες δομές ομάδας και μονοειδούς των A και B, δηλαδή αν έχει τις εξής ιδιότητες:

(α) $f(a + b) = f(a) + f(b)$, για κάθε $a, b \in A$,

(β) $f(ab) = f(a)f(b)$, για κάθε $a, b \in A$,

(γ) $f(1) = 1$.

Ένας μορφισμός δακτυλίων καλείται *μονομορφισμός, επιμορφισμός, ισομορφισμός,* αν αντίστοιχα είναι ένεση, έφεση, αμφίεση. Αν η απεικόνιση f είναι ισομορφισμός, τότε οι δακτύλιοι A και B καλούνται *ισόμορφοι* και γράφουμε $A \cong B$. Ένας μορφισμός $f : A \to A$ καλείται *ενδομορφισμός* και ένας ισομορφισμός $f : A \to A$ *αυτομορφισμός.*

Το σύνολο

$$\mathrm{Ker}(f) = \{x \in A / \ f(x) = 0\}$$

καλείται *πυρήνας* του f. Σύμφωνα με την Πρόταση 4.8, ο πυρήνας του f είναι υποομάδα της $(A, +)$ και ο f είναι ένεση αν και μόνον αν $\mathrm{Ker}(f) = \{0\}$.

Στη περίπτωση όπου οι δακτύλιοι A και B είναι σώματα, η απεικόνιση $f : A \to B$ είναι ένας *μορφισμός σωμάτων,* αν οι απεικονίσεις $f : (A, +) \to (B, +)$ και $f : (A^*, \cdot) \to (B^*, \cdot)$ είναι μορφισμοί ομάδων, δηλαδή αν για κάθε $x, y \in A$ έχουμε:

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y).$$

Ας είναι $f : A \to B$ μορφισμός δακτυλίων και ας υποθέσουμε ότι ο A είναι σώμα και $B \neq \{0\}$. Τότε, ο f είναι ένεση. Πράγματι, αν $x \in A \setminus \{0\}$ με $f(x) = 0$, τότε έχουμε:

$$1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) = 0$$

και επομένως $B = \{0\}$ που είναι άτοπο. Άρα, $\mathrm{Ker}(f) = \{0\}$ και κατά συνέπεια ο f είναι ένεση.

Παράδειγμα 4.22 Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ είναι αντιμεταθετικοί δακτύλιοι με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού. Οι δακτύλιοι $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ είναι σώματα, ενώ ο δακτύλιος $\mathbb{Z}$ δεν είναι.

Παράδειγμα 4.23 Θεωρούμε το σύνολο $B = \{0, 1\}$ εφοδιασμένο με μία πρόσθεση και ένα πολλαπλασιασμό που ορίζονται ως εξής:

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0$$

και

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Το σύνολο B με αυτές τις δύο πράξεις αποτελεί σώμα.

Παράδειγμα 4.24 Αν A_i $(i = 1, \ldots, k)$ είναι δακτύλιοι, τότε το σύνολο $A_1 \times \cdots \times A_k$ δομείται σε δακτύλιο με πράξεις πρόσθεσης και πολλαπλασιασμού ορισμένες όπως στο Παράδειγμα 4.2. Εύκολα βλέπουμε ότι ισχύει:

$$(A_1 \times \cdots \times A_k)^* = A_1^* \times \cdots \times A_k^*.$$

Ας είναι A δακτύλιος. Ένα μη κενό υποσύνολο B του A καλείται *υποδακτύλιος* του A, αν $1 \in B$ και για κάθε $x, y \in B$ έχουμε $x-y, xy \in B$. Παρατηρούμε ότι ένας υποδακτύλιος του A είναι ένα υποσύνολο του A που είναι και αυτό δακτύλιος με τους περιορισμούς των πράξεων του A σ΄ αυτό. Ας υποθέσουμε ότι ο δακτύλιος A είναι σώμα. Το μη κενό υποσύνολο B του A καλείται *υπόσωμα* του A, αν για κάθε $x, y \in B$ έχουμε $x - y, xy^{-1} \in B$.

Παράδειγμα 4.25 Ο δακτύλιος $\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Q}$. Επίσης, τα σώματα $\mathbb{Q}$ και $\mathbb{R}$ είναι υποσώματα του $\mathbb{C}$.

Παράδειγμα 4.26 Ας είναι d ένας ακέραιος με $d \neq 0, 1$ που είναι ελεύθερος τετραγώνου. Το σύνολο

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} / \ a, b \in \mathbb{Z}\}$$

εφοδιασμένο με τη συνηθισμένη πρόσθεση και πολλαπλασιασμό είναι ένας υποδακτύλιος του $\mathbb{C}$. Πράγματι, αν $x, y \in \mathbb{Z}[\sqrt{d}]$, τότε υπάρχουν $r, s, t, u \in \mathbb{Z}$ με $x = r + s\sqrt{d}$, $y = t + u\sqrt{d}$ και επομένως έχουμε:

$$x - y = r - t + (s - u)\sqrt{d}, \quad xy = rt + sud + (ru + st)\sqrt{d}.$$

Άρα $x-y, xy \in \mathbb{Z}[\sqrt{d}]$. Καθώς επίσης $1 \in \mathbb{Z}[\sqrt{d}]$ έχουμε ότι το σύνολο $\mathbb{Z}[\sqrt{d}]$ είναι υποδακτύλιος του $\mathbb{C}$.

Ας είναι A δακτύλιος και $x \in A \setminus \{0\}$. Το στοιχείο x καλείται *διαιρέτης του μηδενός*, αν υπάρχει $y \in A \setminus \{0\}$ τέτοιο, ώστε $xy = 0$. Ένας αντιμεταθετικός δακτύλιος $A \neq \{0\}$ χωρίς διαιρέτες του μηδενός καλείται *πεδίο ακεραιότητας (ή ακεραία περιοχή)*.

Παράδειγμα 4.27 Ο δακτύλιος $\mathbb{C}$ και κάθε υποδακτύλιός του είναι πεδία ακεραιότητας.

Σε πεδίο ακεραιότητας A ισχύει ο νόμος απλοποίησης για τον πολλαπλασιασμό. Δηλαδή, αν $a, x, y \in A$ και $a \neq 0$, τότε έχουμε:

$$ax = ay \Longrightarrow x = y.$$

Πράγματι, από την ισότητα $ax = ay$ έχουμε $a(x - y) = 0$. Έτσι, αν $x - y \neq 0$, έπεται ότι το a είναι ένας διαιρέτης του μηδενός που είναι άτοπο. Άρα $x = y$.

Πρόταση 4.9 *Κάθε πεπερασμένο πεδίο ακεραιότητας είναι σώμα.*

Απόδειξη. Ας είναι A ένα πεπερασμένο πεδίο ακεραιότητας και $a \in A \setminus \{0\}$. Καθώς ισχύει ο νόμος απλοποίησης για τον πολλαπλασιασμό, η απεικόνιση

$$\phi_a : A \longrightarrow A,\ x \longmapsto ax$$

είναι ένεση και κατά συνέπεια αμφίεση γιατί το σύνολο A είναι πεπερασμένο. Τότε υπάρχει $b \in A$ με $ab = 1$. Επομένως, το πεδίο ακεραιότητας A είναι σώμα. □

Ας είναι A ένας δακτύλιος με μηδενικό και μοναδιαίο στοιχείο 0_A και e_A, αντίστοιχα. Θεωρούμε την ακολουθία $e_A, 2e_A, 3e_A, \ldots$. Αν κανένας από τους όρους αυτής της ακολουθίας δεν είναι το μηδενικό στοιχείο του A, τότε λέμε ότι ο A έχει *χαρακτηριστική* 0. Αν κάποιος από τους όρους της ακολουθίας είναι το μηδενικό στοιχείο, τότε ο μικρότερος ακέραιος $n > 0$ με $ne_A = 0$ καλείται *χαρακτηριστική* του A. Η χαρακτηριστική του A συμβολίζεται με $\mathrm{char}A$. Εύκολα διαπιστώνουμε ότι τα σώματα $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ έχουν χαρακτηριστική 0 ενώ ο δακτύλιος B του Παραδείγματος 4.23 έχει χαρακτηριστική 2. □

Πρόταση 4.10 *Ας υποθέσουμε ότι ο δακτύλιος A είναι πεδίο ακεραιότητας. Τότε η χαρακτηριστική του A είναι είτε 0 είτε ένας πρώτος αριθμός.*

Απόδειξη. Ας είναι $\mathrm{char}(A) = n > 0$. Αν $n = n_1 n_2$ με $1 < n_i < n$ $(i = 1, 2)$, τότε έχουμε:

$$0_A = ne_A = (n_1 n_2)e_A = (n_1 e_A)(n_2 e_A)$$

και κατά συνέπεια $n_1 e_A = 0_A$ ή $n_2 e_A = 0_A$ που είναι άτοπο. Άρα, ο ακέραιος n είναι πρώτος. Συνεπώς η χαρακτηριστική του A είναι είτε 0 είτε ένας πρώτος αριθμός. □

Πόρισμα 4.4 *Ας είναι K ένα πεπερασμένο σώμα. Τότε η χαρακτηριστική του K είναι ένας πρώτος αριθμός.*

Απόδειξη. Αν $\mathrm{char}K = 0$, τότε όλα τα στοιχεία της ακολουθίας $e_K, 2e_K, 3e_K, \ldots$ είναι διαφορετικά και επομένως το K περιέχει άπειρο πλήθος στοιχείων που είναι άτοπο. Άρα η χαρακτηριστική του K είναι πεπερασμένη και επομένως, σύμφωνα με την Πρόταση 4.10, ένας πρώτος αριθμός. □

Πρόταση 4.11 *Ας υποθέσουμε ότι ο δακτύλιος A είναι πεδίο ακεραιότητας, $x \in A$ και $n \in \mathbb{Z}$. Αν $\mathrm{char}A = p > 0$, τότε ισχύει:*

$$nx = 0_A \Longleftrightarrow p|n \ \ \text{ή} \ \ x = 0_A.$$

Αν $\mathrm{char}A = 0$, τότε έχουμε:

$$nx = 0_A \Longleftrightarrow n = 0 \ \ \text{ή} \ \ x = 0_A.$$

Απόδειξη. Καθώς ο δακτύλιος A δεν έχει διαιρέτες του μηδενός, η ισότητα

$$0 = nx = n(e_A x) = (ne_A)x$$

ισοδυναμεί με $x = 0_A$ ή $ne_A = 0_A$. Αν $\mathrm{char}A = 0$, τότε $ne_A = 0_A$, αν και μόνον αν $n = 0$. Ας είναι $\mathrm{char}A = p > 0$. Τότε, έχουμε $n = vp + u$, με $u, v \in \mathbb{Z}$ και $0 \leq u < p$. Επομένως, ισχύει:

$$ne_A = (vp + u)e_A = v(pe_A) + ue_A = ue_A.$$

Ας είναι $ne_A = 0_A$. Αν $u > 0$, τότε $ue_A = 0$ και $0 < u < p$ που είναι άτοπο. Άρα $u = 0$ και επομένως $p|n$. Αντίστροφα, αν $p|n$, τότε

$n = mp$, όπου $m \in \mathbb{Z}$, και επομένως $ne_A = m(pe_A) = 0_A$. Άρα $ne_A = 0_A$, αν και μόνον αν $p|n$. $\square$

Ας είναι $k, n \in \mathbb{N}$ με $0 \leq k \leq n$. Θέτουμε

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!},$$

όπου $0! = 1$ και $n! = 1 \cdot 2 \cdots (n-1)n$, αν $n > 0$.

Πρόταση 4.12 *(Διώνυμο του Newton) Ας είναι n φυσικός > 0, A δακτύλιος και $x, y \in A$ με $xy = yx$. Τότε, ισχύει:*

$$(x+y)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^{n-k} y^k.$$

Απόδειξη. Θα χρησιμοποιήσουμε τη μέθοδο της Μαθηματικής Επαγωγής. Για $n = 1$ διαπιστώνουμε αμέσως ότι η ισότητα ισχύει. Υποθέτουμε ότι η ισότητα ισχύει για $n = m$. Έχουμε:

$$(x+y)^{m+1} = (x+y)(x+y)^m = (x+y) \sum_{k=0}^{m} \left(\begin{array}{c} m \\ k \end{array} \right) x^{m-k} y^k =$$

$$x^{m+1} + \sum_{k=1}^{m} \left[\left(\begin{array}{c} m \\ k-1 \end{array} \right) + \left(\begin{array}{c} m \\ k \end{array} \right) \right] x^{(m+1)-k} y^k + y^{m+1}.$$

Για κάθε $k \in \mathbb{N}$, με $0 < k < n$, ισχύει:

$$\begin{aligned} \left(\begin{array}{c} m \\ k-1 \end{array} \right) + \left(\begin{array}{c} m \\ k \end{array} \right) &= \frac{m!}{(m-k+1)!(k-1)!} + \frac{m!}{(m-k)!k!} \\ &= \frac{m!}{(m-k)!(k-1)!} \left(\frac{1}{m-k+1} + \frac{1}{k} \right) \\ &= \frac{(m+1)!}{k!(m-k+1)!} \\ &= \left(\begin{array}{c} m+1 \\ k \end{array} \right). \end{aligned}$$

Επομένως, έχουμε:

$$(x+y)^{m+1} = \sum_{k=0}^{m+1} \left(\begin{array}{c} m+1 \\ k \end{array} \right) x^{m+1-k} y^k.$$

Άρα, η ισότητα ισχύει για κάθε φυσικό $n > 0$. $\square$

Παρατήρηση 4.1 Οι αριθμοί

$$\left(\begin{array}{c} n \\ k \end{array} \right)$$

παρουσιάζονται ως συντελεστές στο διώνυμο $(x+y)^n$ και κατά συνέπεια είναι φυσικοί > 0.

4.4 Πολυώνυμα

Σ΄ αυτή την ενότητα θα μελετήσουμε τον δακτύλιο των πολυωνύμων και ιδιαίτερα τη διαιρετότητά του. Επίσης, θα υπολογίσουμε τον χρόνο των βασικών πράξεων σ΄ αυτό.

4.4.1 Ο Δακτύλιος των Πολυωνύμων

Ας είναι A ένας αντιμεταθετικός δακτύλιος και A^* η ομάδα των αντιστρεψίμων στοιχείων του. Καλούμε *πολυώνυμο* ως προς την απροσδιόριστη (ή μεταβλητή) x κάθε τυπική έκφραση της μορφής

$$p = a_0 + a_1 x + 2x^2 + \cdots + a_n x^n,$$

όπου $a_0, \ldots, a_n \in A$. Τα στοιχεία $a_0, \ldots, a_n$ καλούνται *συντελεστές* του p. Αν $a_n \neq 0$, τότε ο φυσικός n καλείται *βαθμός* του p και συμβολίζεται με $\deg p$. Ως βαθμός του 0 ορίζεται να είναι το $-\infty$. Αν $a_n = 1$, τότε το πολυώνυμο p καλείται *κανονικό*. Θα συμβολίζουμε με $A[x]$ το σύνολο των πολυωνύμων με συντελεστές από τον δακτύλιο A. Για μία πιο τυπική θεμελίωση της έννοιας του πολυωνύμου ο ενδιαφερόμενος αναγνώστης μπορεί να συμβουλευτεί το σύγγραμα [5].

Ας είναι

$$p = a_0 + a_1 x + \cdots + a_n x^n, \quad q = b_0 + b_1 x + \cdots + b_m x^m$$

δύο πολυώνυμα του $A[x]$ με $m \leq n$. Καλούμε *άθροισμα* και *γινόμενο* των p και q τα πολυώνυμα

$$p + q = \sum_{i=0}^{n} (a_i + b_i) x^i, \quad pq = \sum_{i=0}^{n+m} \left(\sum_{k+l=i} a_k b_l \right) x^i,$$

αντίστοιχα. Το σύνολο $A[x]$ εφοδιασμένο με αυτή την πρόσθεση και πολλαπλασιασμό δομείται σε αντιμεταθετικό δακτύλιο. Τα ουδέτερα στοιχεία για την πρόσθεση και πολλαπλασιασμό είναι τα 0 και 1, αντίστοιχα. Επίσης, το αντίθετο του πολυωνύμου p είναι το $-p = (-1)p$. Εύκολα παίρνουμε:

$$\deg pq \leq \deg p + \deg q, \quad \deg(p+q) \leq \max\{\deg p, \deg q\}.$$

Πρόταση 4.13 *Ας είναι A ένα πεδίο ακεραιότητας. Ισχύουν τα εξής:*
(α) Αν $f, g \in A[x]$, τότε $\deg fg = \deg f + \deg g$.
(β) Ο δακτύλιος $A[x]$ είναι ένα πεδίο ακεραιότητας.
(γ) Η ομάδα των αντιστρεψίμων στοιχείων του $A[x]$ συμπίπτει με την ομάδα A^*.

Απόδειξη. Ας είναι

$$f = a_0 + a_1 x + \cdots + a_r x^r, \quad g = b_0 + b_1 x + \cdots + b_s x^s$$

δύο πολυώνυμα του $A[x]$ με $a_r \neq 0$ και $b_s \neq 0$. Τότε:

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_r b_s x^{r+s}.$$

Καθώς ο A είναι πεδίο ακεραιότητας, έχουμε $a_r b_s \neq 0$ και επομένως $fg \neq 0$. Άρα έχουμε $fg \neq 0$ και κατά συνέπεια ο δακτύλιος $A[x]$ είναι ένα πεδίο ακεραιότητας. Επίσης, ισχύει $\deg fg = \deg f + \deg g$.

Ας είναι f ένα αντιστρέψιμο στοιχείο του $A[x]$. Τότε υπάρχει $g \in A[x]$ με $fg = 1$. Επομένως $\deg f + \deg g = 0$. Άρα $\deg f = 0$ και κατά συνέπεια $f \in A$. Συνεπώς, η ομάδα των αντιστρεψίμων στοιχείων του $A[x]$ συμπίπτει με την A^*. □

Στη συνέχεια θα υπολογίσουμε τον χρόνο που απαιτείται για την εκτελεση της πρόσθεσης/αφαίρεσης και του πολλαπλασιασμού μέσα στο $A[x]$. Θα καλούμε πράξη μέσα στο A κάθε πολλαπλασιασμό και πρόσθεση/αφαίρεση στοιχείων του A, καθώς και τον υπολογισμό του αντιστρόφου ενός στοιχείου (αν υπάρχει).

Πρόταση 4.14 *Ας είναι $f, g \in A[x]$ με $n = \deg f \geq \deg g = m$. Τότε έχουμε τα εξής:*
(α) Ο υπολογισμός του $f \pm g$ απαιτεί $O(m)$ προσθέσεις/αφαιρέσεις μέσα στο A.
(β) Ο υπολογισμός του fg απαιτεί $O(mn)$ πράξεις μέσα στο A.

Απόδειξη. (α) Ας είναι

$$f = a_0 + a_1x + \cdots + a_nx^n, \quad g = b_0 + b_1x + \cdots + b_mx^m.$$

Για τον υπολογισμό του $f + g$ (αντίστοιχα του $f - g$) απαιτούνται m προσθέσεις (αντίστοιχα αφαιρέσεις) στοιχείων του A.

(β) Για τον υπολογισμό του fg απαιτείται ο υπολογισμός των ποσοτήτων

$$\sum_{k+l=i} a_kb_l \quad (i = 0, \ldots, n + m).$$

Για κάθε μία τέτοια ποσότητα χρειάζεται να πραγματοποιήσουμε $m + 1$ το πολύ πολλαπλασιασμούς και το πολύ m προσθέσεις. Επομένως, απαιτούνται $O(m)$ πράξεις μέσα στο A. Άρα, για τον υπολογισμό του fg απαιτούνται $O(m(m + n)) = O(mn)$ πράξεις μέσα στο A. □

Πόρισμα 4.5 *Ας είναι $f, g \in \mathbb{Z}[x]$ με $n = \deg f \geq \deg g = m$. Ας υποθέσουμε ότι τα μήκη των απολύτων τιμών των συντελεστών των f και g είναι $\leq k$. Τότε έχουμε τα εξής:*
(α) Ο υπολογισμός του $f \pm g$ απαιτεί $O(km)$ δυαδικές ψηφιακές πράξεις.
(β) Ο υπολογισμός του fg απαιτεί $O(mnk^2)$ δυαδικές ψηφιακές πράξεις.

Παρατήρηση 4.2 Αλγόριθμοι για ταχύτερο πολλαπλασιασμό πολυωνύμων περιγράφονται στα συγγράμματα [9, 4].

4.4.2 Ευκλείδεια Διαίρεση Πολυωνύμων

Σ′ αυτή την ενότητα θα δώσουμε ένα θεώρημα ανάλογο με αυτό της Ευκλείδειας διαίρεσης ακεραίων. Συμβολίζουμε με A έναν αντιμεταθετικό δακτύλιο και με A^* την ομάδα των αντιστρεψίμων στοιχείων του. Ας είναι $f = c_0 + c_1x + \cdots + c_nx^n$ ένα πολυώνυμο του $A[x]$ βαθμού n και $a \in A$. Το στοιχείο $f(a) = c_0 + c_1a + \cdots + c_na^n$ καλείται *τιμή* του f στο a. Η συνάρτηση

$$\Sigma_f : A \longrightarrow A, \ a \longmapsto f(a)$$

καλείται *πολυωνυμική συνάρτηση* που αντιστοιχεί στο f. Αν $f(a) = 0$, τότε το a καλείται *ρίζα* του f. Θα συμβολίζουμε με $lc(f)$ τον συντελεστή c_n του f. Επίσης, εύκολα αποδεικνύεται ότι για κάθε $f, g \in A[x]$ ισχύουν τα εξής:

$$(f + g)(a) = f(a) + g(a), \quad (fg)(a) = f(a)g(a).$$

Θεώρημα 4.1 *Ας είναι f, g μη μηδενικά πολυώνυμα του $A[x]$. Αν $lc(g) \in A^*$, τότε υπάρχουν $q, r \in A[x]$ έτσι, ώστε*

$$f = gq + r \quad \text{και} \quad \deg r < \deg g.$$

Απόδειξη. Αν $\deg f < \deg g$, τότε θέτουμε $q = 0$ και $r = f$. Ας υποθέσουμε λοιπόν ότι $m = \deg f \geq \deg g = n$. Θα εφαρμόσουμε την μέθοδο της επαγωγής επί του m. Θέτουμε $a = lc(f)$ και $b = lc(g)$. Αν $m = 0$, τότε $f = b$ και $g = a$. Επομένως, για $q = a^{-1}b$ και $r = 0$ έχουμε $f = gq + r$.

Ας υποθέσουμε τώρα ότι $m > 0$ και ότι η προς απόδειξη πρόταση ισχύει για κάθε μη μηδενικό πολυώνυμο βαθμού $\leq m - 1$. Ο βαθμός του πολυωνύμου $af - bx^{m-n}g$ είναι $\leq m - 1$. Έτσι, σύμφωνα με την υπόθεση επαγωγής, υπάρχουν $q_1, r_1 \in A[x]$ έτσι, ώστε

$$af - bx^{m-n}g = gq_1 + r_1 \quad \text{και} \quad \deg r_1 < \deg g.$$

Επομένως

$$f = a^{-1}(bx^{m-n} + q_1)g + a^{-1}r_1.$$

Ας είναι (q_1, r_1), (q_2, r_2) δύο ζεύγη πολυωνύμων του $A[x]$ με

$$f = gq_i + r_i \quad \text{και} \quad \deg r_i < \deg g \quad (i = 1, 2).$$

Τότε $g(q_1 - q_2) = r_2 - r_1$ και επομένως

$$\deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1) < \deg g.$$

Άρα $\deg(q_1 - q_2) < 0$ και κατά συνέπεια έχουμε $q_1 = q_2$. Έτσι, παίρνουμε

$$r_1 = f - gq_1 = f - qg_2 = r_2. \quad \square$$

Ο ακέραιος q καλείται *πηλίκο* της διαίρεσης του f δια g και ο r *υπόλοιπο*. Οι σχέσεις του Θεωρήματος 4.1 καλούνται *Ευκλείδεια διαίρεση*.

Παράδειγμα 4.28 Ας είναι $f = x^7 + 2x^5 + x^4 + x^3 + 3x + 4$ και $g = x^4 + 1$ δύο πολυώνυμα του $\mathbb{Z}[x]$. Η διαίρεση του f διά g δίνει πηλίκο $q = x^3 + 2x + 1$ και υπόλοιπο $r = x + 3$.

Πόρισμα 4.6 *Ας είναι $f \in A[x]$ και $a \in A$. Τότε το a είναι ρίζα του f, αν και μόνον αν υπάρχει $q \in A[x]$ έτσι, ώστε $f = (x - a)q$.*

Απόδειξη. Σύμφωνα με το Θεώρημα 4.1, υπάρχει $q \in A[x]$ έτσι, ώστε $f = (x-a)q + r$ και $r \in A$. Οπότε, $r = 0$, αν και μόνον αν $f(a) = 0$. □

Πόρισμα 4.7 *Ας υποθέσουμε ότι ο δακτύλιος A είναι ένα πεδίο ακεραιότητας και $f \in A[x] \setminus A$. Αν $a_1, \ldots, a_m$ είναι όλες οι διαφορετικές ρίζες του f μέσα στο A, τότε $m \leq \deg f$ και υπάρχει $q \in A[x]$ έτσι, ώστε να ισχύει:*

$$f = (x - a_1) \cdots (x - a_m)q.$$

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή επί του m. Για $m = 1$, αυτό προκύπτει από το Πόρισμα 4.6. Ας υποθέσουμε ότι υπάρχει $g \in A[x]$ έτσι, ώστε

$$f = (X - a_1) \cdots (x - a_{m-1})g.$$

Καθώς το A δεν έχει διαιρέτες του μηδενός, οι σχέσεις $f(a_m) = 0$ και $a_m - a_j \neq 0$ $(j = 1, \ldots, m-1)$ δίνουν $g(a_m) = 0$. Έτσι, από το Πόρισμα 4.6 έπεται ότι υπάρχει $p \in A[x]$ έτσι, ώστε $g = (x-a)p$. Αντικαθιστώντας στην παραπάνω ισότητα το g με το ίσο του παίρνουμε

$$f = (x - a_1) \cdots (x - a_m)q.$$

Καθώς ο δακτύλιος A είναι ένα πεδίο ακεραιότητας, έχουμε $\deg f = m + \deg q$ και κατά συνέπεια $m \leq \deg f$. □

Πόρισμα 4.8 *Ας υποθέσουμε ότι ο δακτύλιος A είναι ένα πεδίο ακεραιότητας. Αν f και g είναι δύο πολυώνυμα του $A[X]$ που έχουν την ίδια πολυωνυμική συνάρτηση, τότε $f = g$.*

Απόδειξη. Καθώς τα f και g έχουν την ίδια πολυωνυμική συνάρτηση, έχουμε $f(x) = g(x)$, για κάθε $x \in K$. Οπότε, το πολυώνυμο $f - g$ έχει άπειρο πλήθος ριζών και έτσι, από την Πόρισμα 4.7, έχουμε ότι $f - g = 0$, απ΄ όπου $f = g$. □

Η απόδειξη του Θεωρήματος 4.1 μας δίνει τον παρακάτω αλγόριθμο για την Ευκλείδεια διαίρεση πολυωνύμων.

Αλγόριθμος 4.1 Ευκλείδεια διαίρεση πολυωνύμων.
Είσοδος: Πολυώνυμα $f, g \in A[x] \setminus \{0\}$ τέτοια, ώστε $\deg f \geq \deg g$ και ο συντελεστής του μεγιστοβαθμίου όρου του g ν΄ ανήκει στο A^*.
Έξοδος: Το πηλίκο q και το υπόλοιπο r της διαίρεσης του f με το g.

1. Θέτουμε $f_0 = f$, $m = \deg g$ και $b = lc(g)$.

2. Για $i = 0, 1, 2, \ldots$ κάνουμε τα εξής:

   (α′) Αν $\deg f_{i+1} < \deg g$, τότε εξάγουμε τα πολυώνυμα

   $$q = \sum_{s=0}^{i} lc(f_s) b^{-1} x^{\deg f_s - m}, \quad r = f_{i+1}.$$

   (β′) Αν όχι, τότε υπολογίζουμε

   $$f_{i+1} = f_i - lc(f_i) b^{-1} x^{\deg f_i - m} g.$$

Παρατηρούμε ότι $i \leq n - m$. Στη συνέχεια θα υπολογίσουμε τον χρόνο λειτουργίας αυτού του αλγόριθμου.

Πρόταση 4.15 *Ας είναι $f, g \in A[x] \setminus \{0\}$ με $lc(g) \in A^*$ και $n = \deg f \geq \deg g = m$. Τότε, ο υπολογισμός του πηλίκου και του υπολοίπου της διαίρεσης του f με το g απαιτεί $O(m(n-m))$ πράξεις μέσα στο A.*

Απόδειξη. Για τον προσδιορισμό του f_{i+1} κάνουμε τα εξής:

1. Υπολογίζουμε το b^{-1}.

2. Υπολογίζουμε το γινόμενο $lc(f_i)b^{-1}$.

3. Υπολογίζουμε το γινόμενο του $lc(f_i)b^{-1}$ με κάθε ένα από τους συντελεστή του g.

4. Υπολογίζουμε την διαφορά πολυωνύμων $f_i - lc(f_i)b^{-1}x^{\deg f_i - m}g$.

Τα Βήματα 1 και 2 πραγματοποιούνται με δύο συνολικά πράξεις μέσα στο A. Το Βήμα 3 χρειάζεται $m+1$ πράξεις μέσα στο A και το Βήμα 4 επίσης $m+1$ πράξεις. Επομένως, ο χρόνος υπολογισμού του f_{i+1} είναι $O(m)$ πράξεις. Η διαδικασία αυτή επαναλαμβάνεται το πολύ $n - m + 1$ φορές και κατά συνέπεια ο χρόνος εκτέλεσης του αλγόριθμου είναι $O(m(n-m))$ πράξεις μέσα στο A. □

Πόρισμα 4.9 *Ας είναι $f \in A[x] \setminus \{0\}$ με $n = \deg f \geq 1$ και $a \in A$. Ο υπολογισμός της τιμής $f(a)$ απαιτεί $O(n)$ πράξεις μέσα στο A.*

Απόδειξη. Σύμφωνα με το Θεώρημα 4.1 υπάρχουν $q, r \in A[x]$ έτσι, ώστε

$$f = (x - a)q + r \quad \text{και} \quad \deg r < 1.$$

Άρα, έχουμε $f(a) = r$. Έτσι, από την Πρόταση 4.15 έπεται το αποτέλεσμα. □

Παρατήρηση 4.3 Για μία αποτελεσματικότερη μέθοδο για τον υπολογισμό της τιμής $f(a)$, ο αναγνώστης μπορεί να συμβουλευτεί τα συγγράμματα [1, σελ. 105], [4, σελ.42].

4.4.3 Μέγιστος Κοινός Διαιρέτης Πολυωνύμων

Στην ενότητα αυτή θα εξετάσουμε βασικές ιδιότητες της διαιρετότητας των πολυωνύμων. Ας υποθέσουμε ότι ο δακτύλιος A είναι πεδίο ακεραιότητας. Ας είναι $f, g \in A[x]$ και $f \neq 0$. Λέμε ότι το πολυώνυμο f *διαιρεί* το g και το συμβολίζουμε με $f|g$, αν υπάρχει $h \in K[x]$ έτσι, ώστε $g = fh$. Επίσης, λέμε ότι το g είναι *πολλαπλάσιο* του f ή ότι το f είναι *διαιρέτης* του g. Για παράδειγμα, μέσα στο δακτύλιο $\mathbb{Q}[x]$, το πολυώνυμο $x^3 + 1$ διαιρεί το $x^5 + x^4 + x^3 + x^2 + x + 1$. Πράγματι, ισχύει

$$x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + 1)(x^2 + x + 1).$$

Μερικές βασικές ιδιότητες της διαιρετότητας δίνονται στην παρακάτω πρόταση.

Πρόταση 4.16 *Ας είναι $f, g, h \in A[x]$. Τότε ισχύουν τα εξής:*
(α) Έχουμε $f|f$ και $f|0$.
(β) Αν $f|g$ και $f|h$, τότε $f|ag + bh$ για κάθε $a, b \in A[x]$.
(γ) Αν $f|g$ και $g|h$, τότε $f|h$.
(δ) Αν $f|g$ και $g \neq 0$, τότε $\deg f \leq \deg g$.
(ε) Αν $fg \neq 0$, τότε $f|g$ και $g|f$, αν και μόνον αν $f = kg$ και $k \in A^*$.

Απόδειξη. Θα αποδείξουμε μόνο την (ε). Η απόδειξη των άλλων αφήνεται ως άσκηση. Αν $f|g$ και $g|f$, τότε $f = kg$ και $g = lf$, όπου $k, l \in A[x]$. Έτσι, έχουμε $f = klf$ και επομένως $kl = 1$. Συνεπώς, από την Πρόταση 4.13(γ) προκύπτει $k \in A^*$. Αντίστροφα, αν $f = kg$ και $k \in A^*$, τότε $k^{-1}f = g$ και επομένως έχουμε $f|g$ και $g|f$. □

4.4.4 Πολυώνυμα με Συντελεστές σ΄ ένα Σώμα

Ας είναι K σώμα. Καλούμε *κοινό διαιρέτη* των $f_1, \ldots, f_n \in K[x]$ κάθε $b \in K[x]$ τέτοιο, ώστε $b|f_1, \ldots f|a_n$. Ας σημειωθεί ότι κάθε $k \in K\backslash\{0\}$ είναι κοινός διαιρέτης των $f_1, \ldots, f_n$. Ένα κανονικό πολυώνυμο D του $K[x]$ καλείται *μέγιστος κοινός διαιρέτης* των $f_1, \ldots, f_n$, και το συμβολίζουμε με $\mu\kappa\delta(f_1, \ldots, f_n)$, αν ισχύουν τα εξής:
(α) το D είναι κοινός διαιρέτης των $f_1, \ldots, f_n$.
(β) αν $\Delta \in K[x]$ και $\Delta|f_1, \ldots, \Delta|f_n$, τότε $\Delta|D$.

Αν D και D' είναι δύο μέγιστοι κοινοί διαιρέτες για τα πολυώνυμα $f_1, \ldots, f_n$, τότε $D|D'$ και $D'|D$. Έτσι, από την Πρόταση 4.16(ε), έχουμε $D = kD'$, όπου $k \in K$. Καθώς τα πολυώνυμα D και D' είναι κανονικά, έχουμε $D = D'$.

Αν $\mu\kappa\delta(f_1, \ldots, f_n) = 1$, τότε λέμε ότι τα $f_1, \ldots, f_n$ είναι *πρώτα μεταξύ τους*. Για παράδειγμα τα πολυώνυμα του $\mathbb{Q}[x]$, x και $x^2 + 1$ είναι πρώτα μεταξύ τους.

Χρησιμοποιώντας το Θεώρημα 4.1 θα αποδείξουμε ότι κάθε ζεύγος πολυωνύμων έχει μέγιστο κοινό διαιρέτη και ταυτόχρονα θα περιγράψουμε μία συστηματική διαδικασία για την εύρεσή του, αντίστοιχη μ΄ αυτή του Ευκλείδειου αλγόριθμου για την εύρεση του μ.κ.δ. δύο ακεραίων. Γι΄ αυτό τον σκοπό θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 4.1 *Ας είναι $f, g, q \in K[x]$. Τότε:*

$$\mu\kappa\delta(f, g) = \mu\kappa\delta(fq + g, f).$$

Απόδειξη. Η απόδειξη της πρότασης είναι ανάλογη μ΄ αυτή της Πρότασης 1.6(γ) και γι΄ αυτό παραλείπεται. □

Ας είναι $f, g \in K[x]$. Σύμφωνα, με το Θεώρημα 4.1, υπάρχουν $q_j \in K[x]$ $(j = 1, \ldots, l)$ και $r_j \in K[x]$ $(j = 0, \ldots, l + 1)$ τέτοια, ώστε $r_0 = f$, $r_1 = g$ και

$$r_{j-1} = q_j r_j + r_{j+1}, \quad \deg r_{j+1} < \deg r_j.$$

Έχουμε:

$$\deg r_{l+1} < \deg r_l < \deg r_{l-1} < \ldots < \deg g$$

και επομένως για κάποιο δείκτη n ισχύει $r_j \neq 0$ $(j = 2, \ldots, l)$ και $r_{l+1} = 0$. Από το Λήμμα 4.1 έχουμε:

$$lc(r_l)^{-1} r_l = \mu\kappa\delta(r_{l-1}, r_l) = \mu\kappa\delta(r_{l-2}, r_{l-1}) = \ldots = \mu\kappa\delta(r_0, r_1)$$

και επομένως ο ζητούμενος μέγιστος κοινός διαιρέτης είναι το πολυώνυμο $d = lc(r_n)^{-1} r_n$. Η παραπάνω διαδικασία είναι γνωστή ως *Ευκλείδειος αλγόριθμος* για πολυώνυμα.

Στη συνέχεια θα δώσουμε ένα αποτέλεσμα ανάλογο της Πρότασης 1.10. Ορίζουμε πολυώνυμα $s_0, \ldots, s_{l+1}$ και $t_0, \ldots, t_{l+1}$ ως εξής:

$$s_0 = 1,\ s_1 = 0,\ t_0 = 0,\ t_1 = 1,$$

και για $i = 1, \ldots, l$,

$$s_{i+1} = s_{i-1} - s_i q_i, \quad t_{i+1} = t_{i-1} - t_i q_i.$$

Πρόταση 4.17 *Ισχύουν τα παρακάτω:*
(α) Για $i = 0, \ldots, l+1$, $s_i f + t_i g = r_i$. Ειδικότερα,

$$s_l f + t_l g = lc(r_l)\, \mu\kappa\delta(f, g).$$

(β) Για $i = 0, \ldots, l$, $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$.
(γ) Για $i = 1, \ldots, l+1$,

$$\deg t_i = \deg f - \deg r_{i-1}.$$

(δ) Για $2 = 1, \ldots, l+1$,

$$\deg s_i = \deg g - \deg r_{i-1}.$$

Απόδειξη. Οι σχέσεις στα (α) και (β) αποδεικνύονται όπως και στη Πρόταση 1.10. Θα αποδείξουμε την ισότητα στο (γ) ενώ το (δ) αφίεται ως άσκηση. Θα εφαρμόσουμε επαγωγή επί του i. Για $i = 1$ ισχύει, καθώς $r_0 = f$. Για $i = 2$, έχουμε $t_2 = -q_1$ και $f = r_1 q_1 + r_2$ με $\deg r_2 < \deg r_1$. Έτσι, παίρνουμε:

$$\deg t_2 = \deg q_1 = \deg f - \deg r_1.$$

Ας υποθέσουμε ότι $i \geq 3$ και ότι η πρόταση ισχύει για κάθε δείκτη $\leq i - 1$. Τότε έχουμε:

$$\deg(t_{i-1} q_{i-1}) = \deg t_{i-1} + \deg q_{i-1} = \deg f - \deg r_{i-2} + \deg q_{i-1}.$$

Από τις σχέσεις $r_{i-2} = q_{i-1} r_{i-1} + r_i$ και $\deg r_i < \deg r_{i-1}$ προκύπτει:

$$\deg q_{i-1} = \deg r_{i-2} - \deg r_{i-1}$$

και έτσι έχουμε:

$$\deg(t_{i-1}q_{i-1}) = \deg f - \deg r_{i-1}.$$

Καθώς $\deg r_{i-1} < \deg r_{i-3}$, ισχύει:

$$\deg(t_{i-1}q_{i-1}) > \deg f - \deg r_{i-3} = \deg t_{i-2}.$$

Έτσι, η ισότητα $t_i = t_{i-2} - t_{i-1}q_{i-1}$ δίνει $\deg t_i = \deg(t_{i-1}q_{i-1})$. Επομένως, έχουμε:

$$\deg f - \deg r_{i-1} = \deg(t_{i-1}q_{i-1}) = \deg t_i.$$

Όμοια αποδεικνύεται η ισότητα του (δ). □

Πόρισμα 4.10 *Αν $d = \gcd(f, g)$, τότε υπάρχουν $u, v \in K[x]$ με $\deg u \leq \deg g$ και $\deg v \leq \deg f$ τέτοια, ώστε να ισχυει:*

$$d = uf + vg.$$

Πόρισμα 4.11 *Ας είναι $a, b, c \in K[x]$ με $a|bc$. Αν μκδ$(a, b) = 1$, τότε $a|c$.*

Απόδειξη. Σύμφωνα με την Πρόταση 4.22(α) υπάρχουν $s, t \in K[x]$ τέτοια, ώστε $sa + tb = 1$. Οπότε $sac + tbc = c$ και καθώς $a|bc$ έχουμε $a|c$. □

Ο Ευκλείδειος αλγόριθμος μαζί με την διαδικασία εύρεσης των u και v καλείται *εκτεταμένος Ευκλείδειος αλγόριθμος.*

Παράδειγμα 4.29 Θα υπολογίσουμε τον μέγιστο κοινό διαιρέτη των πολυωνύμων

$$f(x) = x^4 + x^3 + 3x - 9 \quad \text{και} \quad g(x) = 2x^3 - x^2 + 6x - 3.$$

Έχουμε

$$\begin{aligned} x^4 + x^3 + 3x - 9 &= (2x^3 - x^2 + 6x - 3)\left(\frac{1}{2}x + \frac{3}{4}\right) - \frac{9}{4}x^2 - \frac{27}{4}, \\ 2x^3 - x^2 + 6x - 3 &= \left(-\frac{9}{4}x^2 - \frac{27}{4}\right)\left(-\frac{8}{9}x + \frac{4}{9}\right). \end{aligned}$$

Άρα

$$\mu\kappa\delta(f,g) = x^2 + 3.$$

Επίσης, έχουμε

$$x^2 + 3 = (2x^3 - x^2 + 6x - 3)\frac{4}{9}\left(\frac{1}{2}x + \frac{3}{4}\right) - \frac{4}{9}(x^4 + x^3 + 3x - 9),$$

Συνοψίζουμε παρακάτω την εκτέλεση των διαδικασιών του εκτεταμένου Ευκλείδειου αλγόριθμου.

Αλγόριθμος 4.2 Εκτεταμένος Ευκλείδειος Αλγόριθμος.
Είσοδος: Πολυώνυμα $f, g \in K[x]$ με $\deg f \geq \deg g \geq 0$.
Έξοδος: (d, s, t), όπου $d = \mu\kappa\delta(f,g)$ και $s, t \in K[x]$ με $sa + tb = d$.

1. Θέτουμε $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$.
2. Για $j = 0, 1, \ldots$ κάνουμε τα εξής:

   (α′) Αν $r_{j+1} = 0$, τότε εξάγουμε την τριάδα (r_j, s_j, t_j).

   (β′) Αν όχι, τότε υπολογίζουμε ακεραίους q_{j+1}, r_{j+2} με

   $$r_j = r_{j+1}q_{j+1} + r_{j+2}, \quad \deg r_{j+2} < \deg r_{j+1}$$

   και

   $$s_{j+1} = s_{j-1} - s_j q_j, \quad t_{j+1} = t_{j-1} - t_j q_j.$$

Στη συνέχεια θα υπολογίσουμε τον χρόνο λειτουργίας αυτού του αλγόριθμου.

Πρόταση 4.18 *Ας είναι $f, g \in K[x]$ με $n = \deg f \geq \deg g = m$. Ο υπολογισμός του μέγιστου κοινού διαιρέτη d των f και g και πολυωνύμων $s, t \in K[x]$ με $\deg s \leq m$ και $\deg t \leq n$ έτσι, ώστε*

$$sf + tg = d$$

απαιτεί $O(mn)$ πράξεις μέσα στο K.

Απόδειξη. Για την εύρεση του d ο Ευκλείδειος αλγόριθμος πραγματοποιεί τις Ευκλείδειες διαιρέσεις

$$r_{j-1} = q_j r_j + r_{j+1} \quad (j = 1, \ldots, l).$$

Το πλήθος των πράξεων μέσα στο K που χρειάζεται η κάθε μία από αυτές είναι $O((\deg r_j)(\deg r_{j-1}))$. Επομένως, το πλήθος των πράξεων μέσα στο K που απαιτεί η εκτέλεση όλων αυτών των διαιρέσεων είναι:

$$O\left(\sum_{j=1}^{l}(\deg r_j)(\deg r_{j-1})\right) = O(mn).$$

Επιπλέον, ο αλγόριθμος υπολογίζει το αντίστροφο στοιχείο του $lc(r_n)$. Έτσι, ο υπολογισμός του d χρειάζεται $O(mn)$ πράξεις μέσα στο K.

Θα προσδιορίσουμε στη συνέχεια τον χρόνο που απαιτείται για τον υπολογισμό των s_i και t_i $(i = 1, \ldots, l+1)$. Από την ισότητα $r_{i-1} = r_i q_i + r_{i+1}$ έχουμε $\deg q_i \leq \deg r_{i-1}$. Έτσι, από την Πρόταση 4.17(δ) παίρνουμε:

$$\deg(s_i q_i) \leq \deg s_i + \deg q_i \leq \deg g - \deg r_{i-1} + \deg r_{i-1} = \deg g.$$

Έχουμε $s_2 = 1$ και $s_{i+1} = s_{i-1} - s_i q_i$ $(i = 2, \ldots, l+1)$. Ο υπολογισμός του $s_i q_i$ απαιτεί $O((\deg s_i)(\deg q_i))$ πράξεις μέσα στο K. Καθώς ισχύει $\deg s_{i-1}, \deg(s_i q_i) \leq m$, ο υπολογισμός του s_{i+1} απαιτεί $O(m + (\deg s_i)(\deg q_i))$ πράξεις μέσα στο K. Έτσι, χρησιμοποιώντας την ανισότητα $\sum_{i=2}^{l} \deg q_i \leq m$, παίρνουμε ότι το πλήθος των πράξεων μέσα στο K που χρειάζεται για τον υπολογισμό όλων των s_i είναι:

$$O\left(\sum_{i=2}^{l}(m + (\deg s_i)(\deg q_i))\right) = O\left(ml + m\sum_{i=2}^{l}\deg q_i\right) = O(m^2).$$

Όμοια, ο υπολογισμός όλων των t_i απαιτεί $O(nm)$ πράξεις μέσα στο K. Συνεπώς, ο χρόνος εκτέλεσης του εκτεταμένου Ευκλείδειου αλγόριθμου είναι $O(mn)$ πράξεις μέσα στο K. □

Καλούμε *κοινό πολλαπλάσιο* των $f_1, \ldots, f_n \in K[x]$ κάθε $b \in K[x]$ τέτοιο, ώστε $f_1|b, \ldots, f_n|b$. Ένα κανονικό πολυώνυμο M του $K[x]$ καλείται *ελάχιστο κοινό πολλαπλάσιο* των $f_1, \ldots, f_n$, και το συμβολίζουμε με $\epsilon\kappa\pi(f_1, \ldots, f_n)$, αν ισχύουν τα εξής:
(α) το M είναι κοινό πολλαπλάσιο των $f_1, \ldots, f_n$.
(β) αν $E \in K[x]$ και $E|f_1, \ldots, E|f_n$, τότε $M|E$.

Αν M και M' είναι δύο ελάχιστα κοινά πολλαπλάσια για τα πολυώνυμα $f_1, \ldots, f_n$, τότε $M|M'$ και $M'|M$. Έτσι, από την Πρόταση 4.16(ε), έχουμε $M = kM'$, όπου $k \in K$. Καθώς τα πολυώνυμα M και M' είναι κανονικά, έχουμε $M = M'$.

Πρόταση 4.19 *Ας είναι $f, g \in K[x]$ με συντελεστές των μεγιστοβαθμίων όρων των, a και b, αντίστοιχα. Αν $D = \mu\kappa\delta(f, g)$, τότε το ελάχιστο κοινό πολλαπλάσιο των f και g είναι το πολυώνυμο $M = fg/abD$.*

Απόδειξη. Αν $f = 0$ ή $g = 0$, τότε η παραπάνω ισότητα αληθεύει. Ας υποθέσουμε λοιπόν ότι $f \neq 0$ και $g \neq 0$. Θα δείξουμε ότι $\epsilon\kappa\pi(f, g) = fg/abD$. Έχουμε $D|f$ και $D|g$ και επομένως το κανονικό πολυώνυμο fg/abD είναι ένα κοινό πολλαπλάσιο των f και g. Αν L είναι ένα κοινό πολλαπλάσιο των f και g, τότε το fg διαιρεί τους fL, gL και κατά συνέπεια διαιρεί τον LD. Άρα, το fg/abD διαιρεί το L. Συνεπώς, έχουμε $\epsilon\kappa\pi(a, b) = fg/abD$. □

4.4.5 Παράγωγος Πολυωνύμου

Ας είναι K ένα σώμα,

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

ένα πολυώνυμο του $K[X]$ και $a \in K$ μία ρίζα του f. Τότε, σύμφωνα με το Πόρισμα 4.6, έχουμε $(x - a)|f$. Έτσι, υπάρχει, θετικός ακέραιος $\mu \leq \deg f$ τέτοιος, ώστε $(x - a)^\mu|f$ και $(x - a)^{\mu+1} \not| f$. Ο φυσικός μ καλείται *πολλαπλότητα* της ρίζας a. Επομένως, το a είναι μία ρίζα πολλαπλότητας μ του f αν και μόνον αν υπάρχει $q \in K[x]$ τέτοιο, ώστε $f = (x - a)^\mu q$ και $x - a \not| q$. Από το Πόρισμα 4.6 έπεται ότι $(x - a) \not| q$ ισοδυναμεί με $q(a) \neq 0$. Άρα, το a είναι ρίζα πολλαπλότητας h του f αν και μόνον αν υπάρχει $q \in A[x]$ τέτοιο, ώστε $f = (x - a)^\mu q$ και $q(a) \neq 0$. Αν η πολλαπλότητα της ρίζας a είναι 1, τότε αυτή καλείται *απλή*.

Καλούμε *τυπική παράγωγο* ή απλώς *παράγωγο* του $f(X)$ το πολυώνυμο

$$f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Για κάθε φυσικό $n \geq 2$, ορίζουμε επαγωγικά την n-οστή παράγωγο $f^{(n)}(X)$ του $f(X)$ ως την παράγωγο του $f^{(n-1)}(X)$. Βασικές ιδιότητες της παραγώγου δίνονται στη παρακάτω προταση.

Πρόταση 4.20 *Ας είναι $f, g \in K[x]$. Τότε ισχύουν οι εξής ιδιότητες:*
(α) $(f + g)' = f' + g'$,
(β) $(fg)' = fg' + f'g$,
(γ) $(f^m)' = mf^{m-1}f'$, *για κάθε θετικό ακέραιο m.*

Απόδειξη. Ας είναι

$$f = a_0 + a_1x + \cdots + a_kx^k, \quad g = b_0 + b_1x + \cdots + b_lx^l$$

με $k \geq l$. Τότε, έχουμε:

$$f' = a_1 + 2a_2x + \cdots + ka_kx^{k-1}, \quad g' = b_1 + 2b_1x + \cdots + lb_lx^{l-1}$$

και επομένως ισχύει:

$$f' + g' = \sum_{i=1}^{k} ia_ix^{i-1} + \sum_{i=1}^{l} ib_ix^{i-1} = \sum_{i=1}^{k} i(a_i + b_i)x^{i-1} = (f + g)'.$$

Άρα αληθεύει η (α).

Για την απόδειξη της (β) έχουμε:

$$\begin{aligned} fg' + f'g &= \left(\sum_{i=0}^{k} a_ix^i\right)\left(\sum_{j=1}^{l} jb_jx^{j-1}\right) + \left(\sum_{i=1}^{k} ia_ix^{i-1}\right)\left(\sum_{j=0}^{l} b_jx^j\right) \\ &= \sum_{m=1}^{k+l}\left(\sum_{i+j=m} ja_ib_j\right)x^{m-1} + \sum_{m=1}^{k+l}\left(\sum_{i+j=m} ia_ib_j\right)x^{m-1} \\ &= \sum_{m=1}^{k+l} m\left(\sum_{i+j=m} a_ib_j\right)x^{m-1} = (fg)'. \end{aligned}$$

Για ν΄ αποδείξουμε την (γ) θα εφαρμόσουμε τη μέθοδο της μαθηματικής επαγωγής επί του m. Η περίπτωση $m = 1$ είναι προφανής. Ας υποθέσουμε ότι ισχύει για $m = k \geq 1$. Τότε ισχύει $(f^k)' = kf^{k-1}f'$. Από αυτή την ισότητα και την (β) παίρνουμε:

$$(f^{k+1})' = (f^kf)' = f^kf' + (f^k)'f = f^kf' + kf^kf' = (k + 1)f^kf'.$$

Συνεπώς, ισχύει και η (γ). □

Πρόταση 4.21 *Ας είναι $f \in K[x]$ με $\deg f = d \geq 2$ και $a \in K$ μία ρίζα του f. Το a είναι ρίζα πολλαπλότητας $k > 1$ αν και μόνον αν $f'(a) = 0$.*

Απόδειξη. Ας υποθέσουμε ότι το a είναι ρίζα πολλαπλότητας $k > 1$ του f. Τότε υπάρχει $g \in K[x]$ έτσι, ώστε $f = (x-a)^k g$. Έτσι, έχουμε:

$$f' = (x-a)^k g' + k(x-a)^{k-1} g$$

και επομένως $f'(a) = 0$. Αντίστροφα, ας υποθέσουμε ότι το $a \in K$ είναι μία ρίζα του f και $f'(a) = 0$. Γράφουμε:

$$f = a_0 + a_1(x-a) + \cdots + a_d(x-a)^d.$$

Τότε $a_0 = f(a) = 0$ και $a_1 = f'(a) = 0$. Έτσι, έχουμε:

$$f = (x-a)^2(a_2 + a_3(x-a) + \cdots + a_d(x-a)^{d-2})$$

και κατά συνέπεια η ρίζα a έχει πολλαπλότητα ≥ 2. □

4.4.6 Ανάγωγα Πολυώνυμα

Ας είναι K σώμα. Σ′ αυτή την ενότητα ϑ′ ασχοληθούμε με μία οικογένεια πολυωνύμων τα οποία έχουν ανάλογες ιδιότητες μ′ αυτές των πρώτων αριθμών.

Ένα πολυώνυμο $f \in K[x]$ καλείται *ανάγωγο* στο $K[x]$, αν δεν είναι δυνατόν να γραφεί ως γινόμενο $f = g_1 g_2$, όπου $g_1, g_2 \in K[x]$ με $0 < \deg g_i < \deg f \ \ (i = 1, 2)$. Ισοδύναμα, το πολυώνυμο f είναι ανάγωγο, αν και μόνον αν τα μόνα κανονικά πολυώνυμα που το διαιρούν είναι το 1 και το κανονικό πολυώνυμο που αντιστοιχεί στο f.

Παράδειγμα 4.30 Τα πολυώνυμα $ax+b$ με $a, b \in K$ και $a \neq 0$ είναι ανάγωγα.

Το παρακάτω ϑεώρημα είναι γνωστό ως *κριτήριο αναγωγιμότητας του Eisenstein.*

Θεώρημα 4.2 *Ας είναι $f = a_n x^n + \cdots + a_0$ ένα πολυώνυμο με ακέραιους συντελεστές και $n \geq 1$. Αν υπάρχει πρώτος p τέτοιος, ώστε $p | a_i$ $(i = 0, \ldots, n-1)$, $p \nmid a_n$ και $p^2 \nmid a_0$, τότε το f είναι ανάγωγο μέσα στο $\mathbb{Q}[x]$.*

Για την απόδειξη του ϑεωρήματος ϑα χρειαστούμε το εξής λήμμα:

Λήμμα 4.2 *Ας είναι $f = a_n x^n + \cdots + a_0$ πολυώνυμο του $\mathbb{Z}[x]$ βαθμού $n \geq 1$. Αν $f = GH$ με $G, H \in \mathbb{Q}[x] \setminus \mathbb{Q}$, τότε υπάρχουν $g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$ έτσι, ώστε $f = gh$ και τα g, h είναι του ίδιου βαθμού με τα G, H, αντιίστοίχα.*

Απόδειξη. Ας είναι $f = GH$ με $G, H \in \mathbb{Q}[x]$ με $\deg G = k \geq 1$ και $\deg H = l \geq 1$. Τότε υπάρχουν $a, b \in \mathbb{Z}$ με $aG, bH \in \mathbb{Z}[x]$. Πολλαπλασιάζοντας και τα δύο μέλη της ισότητας $f = GH$ με ab και κάνοντας όλες τις απλοποιήσεις έχουμε:

$$m(a_n X^n + \cdots + a_0) = c(\beta_k x^k + \cdots + \beta_0)(\gamma_l X^l + \cdots + \gamma_0),$$

όπου $m, c, \beta_i, \gamma_j \in \mathbb{Z}$, $\mu\kappa\delta(\beta_0, \ldots, \beta_k) = \mu\kappa\delta(\gamma_0, \ldots, \gamma_k) = 1$, $m > 0$, $c > 0$ και $\mu\kappa\delta(m, c) = 1$.

Ας υποθέσουμε ότι $m \neq 1$ και p πρώτος με $p|m$. Καθώς έχουμε $\mu\kappa\delta(\beta_0, \ldots, \beta_k) = 1$, υπάρχει δείκτης s με $p|\beta_0, \ldots, p|\beta_{s-1}$ και $p \not| \beta_s$. Όμοια, υπάρχει δείκτης t με $p|\gamma_0, \ldots, p|\gamma_{t-1}$ και $p \not| \gamma_t$. Έτσι, ο πρώτος p διαιρεί τους αριθμούς

$$\sum_{i=0}^{s-1} \beta_i \gamma_{s+t-i}, \quad \sum_{i=s+1}^{s+t} \beta_i \gamma_{s+t-i}$$

και επομένως η ισότητα

$$ma_{s+t} = c\left(\sum_{i=0}^{s+t} \beta_i \gamma_{s+t-i}\right)$$

δίνει $p|c\beta_s\gamma_t$. Καθώς $\mu\kappa\delta(m, c) = 1$, έχουμε $p|\beta_s\gamma_t$, απ΄ όπου $p|\beta_s$ ή $p|\gamma_t$ που είναι άτοπο. Άρα $m = 1$ και κατά συνέπεια το f αναλύεται σε γινόμενο δύο πολυωνύμων του $\mathbb{Z}[x]$ θετικού βαθμού. □

Απόδειξη του Θεωρήματος 4.2. Ας υποθέσουμε ότι το f δεν είναι ανάγωγο μέσα στο $\mathbb{Q}[x]$. Οπότε, σύμφωνα με το Λήμμα 4.2 υπάρχουν $g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$ έτσι, ώστε $f = gh$. Θέτουμε

$$g = b_q x^q + \cdots + b_0, \quad h = c_m x^m + \cdots + c_0$$

με $q, m > 0$ και $b_q \neq 0$, $c_m \neq 0$. Καθώς το $a_0 = b_0 c_0$ διαιρείται από το p, έχουμε $p|b_0$ ή $p|c_0$. Από την άλλη πλευρά όμως η σχέση $p^2 \not| a_0$, συνεπάγεται ότι κάποιο από τα στοιχεία b_0 και c_0 δεν διαιρείται από το

p. Ας είναι $p \not| b_0$ και $p|c_0$. Το p δεν διαιρεί το $a_n = b_q c_m$ και επομένως δεν διαιρεί κανένα από τα b_q και c_m. Ας είναι r ο πιο μικρός δείκτης τέτοιος, ώστε $p \not| c_r$. Έχουμε

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0$$

και $p|c_i$ $(i = 0, \ldots, r-1)$, $p \not| c_r$, $p \not| b_0$. Έτσι, παίρνουμε $p \not| a_r$. Από την άλλη πλευρά, καθώς $r \leq m < n$, έχουμε $p|a_r$ και κατά συνέπεια καταλήγουμε σε άτοπο. Επομένως, το f είναι ανάγωγο μέσα στον δακτύλιο $\mathbb{Q}[x]$. □

Παράδειγμα 4.31 Θα δείξουμε ότι το πολυώνυμο $f(x) = x^4 + 1$ είναι ανάγωγο μέσα στο $\mathbb{Q}[x]$. Το κριτήριο του Eisenstein. Παρατηρούμε ότι το $f(x)$ είναι ανάγωγο αν και μόνον αν το $f(x+1)$ είναι ανάγωγο. Το κριτήριο του Eisenstein εφαρμόζεται στο

$$f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$$

με $p = 2$ και κατά συνέπεια το $f(x+1)$ είναι ανάγωγο. Άρα, το $f(x)$ είναι επίσης ανάγωγο.

Πρόταση 4.22 *Ας είναι $f \in K[x]$ με $\deg f > 0$. Τότε υπάρχει ανάγωγο πολυώνυμο $p \in K[x]$ με $p|f$.*

Απόδειξη. Θεωρούμε το σύνολο

$$E = \{n \in \mathbb{N} / \text{ υπάρχει } h \in K[x] \text{ με } h|f \text{ και } \deg h = n\}.$$

Το σύνολο E περιέχει τον ακέραιο $\deg f$ και επομένως $E \neq \emptyset$. Ας είναι m το μικρότερο στοιχείο του E. Τότε υπάρχει $p \in K[x]$ με $p|f$ και $\deg p = m$. Αν το p δεν είναι ανάγωγο, τότε υπάρχει $g \in K[x]$ με $g|p$ και $0 < \deg g < m$. Από τις σχέσεις $g|p$ και $p|f$, παίρνουμε $g|f$, απ' όπου $\deg g \in E$. Καθώς όμως $0 < \deg g < m$ καταλήγουμε σε άτοπο. Άρα, το πολυώνυμο p είναι ανάγωγο. □

Πρόταση 4.23 *Ας είναι $p, q_1, \ldots, q_n \in K[x]$ ανάγωγα πολυώνυμα με $p|q_1 \cdots q_n$. Τότε έχουμε $q_i = ap$ για κάποιο δείκτη i και $a \in K$.*

Απόδειξη. Θα χρησιμοποιήσουμε την μέθοδο επαγωγής επί του n. Για $n = 1$ έχουμε $p|q_1$. Καθώς τα p και q_1 είναι ανάγωγα, παίρνουμε $q_1 = ap$, όπου $a \in K$. Υποθέτουμε ότι η προς απόδειξη πρόταση

αληθεύει για $n = k$. Για $n = k+1$ έχουμε $p|(q_1 \cdots q_k)q_{k+1}$. Αν $p|q_{k+1}$, τότε $q_{k+1} = ap$, όπου $a \in K$. Αν $p \not| q_{k+1}$, τότε $\mu\kappa\delta(p, q_{k+1}) = 1$ και από το Πόρισμα 4.11 έχουμε $p|q_1 \cdots q_k$. Έτσι, από την υπόθεση επαγωγής έπεται ότι υπάρχει δείκτης i και $a \in K$ με $q_i = ap$. Άρα, η πρόταση ισχύει για κάθε n. □

Θα χρησιμοποιήσουμε την παραπάνω πρόταση στην απόδειξη του εξής βασικού θεωρήματος.

Θεώρημα 4.3 *Αν είναι $f \in K[x]$ με $\deg f = n > 0$. Τότε υπάρχουν $a \in K$ και κανονικά ανάγωγα πολυώνυμα $p_1, \ldots, p_k$ έτσι, ώστε να έχουμε:*

$$f = ap_1 \cdots p_k.$$

Η γραφή αυτή του f είναι μοναδική.

Απόδειξη. Πρώτα θ′ αποδείξουμε την ύπαρξη μίας τέτοιας γραφής χρησιμοποιώντας επαγωγή επί του n. Ας είναι $f = ax + b$. Οπότε, έχουμε $f = a(x+b/a)$ και το $x+b/a$ είναι ανάγωγο. Υποθέτουμε ότι κάθε πολυώνυμο βαθμού $< n$ γράφεται με αυτόν τον τρόπο. Ας είναι $f \in K[x]$ με $\deg f = n$. Αν το f είναι ανάγωγο, τότε ο ισχυρισμός μας αληθεύει. Αν το f δεν είναι ανάγωγο, τότε, από την Πρόταση 4.22 έχουμε ότι υπάρχει ανάγωγο πολυώνυμο $p \in K[x]$ με $p|f$. Επομένως, $f = pg$, όπου $g \in K[x]$ και $0 < \deg g < n$. Έτσι, από την υπόθεση επαγωγής έπεται ότι υπάρχει $a \in K$ και κανονικά ανάγωγα πολυώνυμα $p_1, \ldots, p_k$ τέτοια, ώστε $g = ap_1 \cdots p_k$. Συνεπώς, $f = app_1 \cdots p_k$.

Στη συνέχεια θ′ αποδείξουμε την μοναδικότητα αυτής της γραφής. Ας είναι $a, b \in K$ και $p_1, \ldots, p_k, q_1, \ldots, q_l$ με $k \leq l$ ανάγωγα κανονικά πολυώνυμα του $K[x]$ τέτοια, ώστε

$$ap_1 \cdots p_k = bq_1 \cdots q_l.$$

Τα πολυώνυμα $p_1 \cdots p_k$ και $q_1 \cdots q_l$ είναι κανονικά και έτσι έχουμε $a = b$. Η ισότητα $p_1 \cdots p_k = q_1 \cdots q_l$ δίνει $p_1|q_1 \cdots q_l$. Καθώς τα πολυώνυμα p_1 και $q_1, \ldots, q_l$ είναι ανάγωγα, η Πρόταση 4.24 δίνει $q_{\sigma(1)} = p_1$ για κάποιο δείκτη $\sigma(1) \in \{1, \ldots, l\}$. Έτσι, παίρνουμε

$$p_2 \cdots p_k = q_1 \cdots q_{\sigma(1)-1} q_{\sigma(1)+1} \cdots q_l.$$

Συνεχίζοντας με τον ίδιο τρόπο, έχουμε ότι για κάθε $i \in \{1, \ldots, k-1\}$ υπάρχει δείκτης $\sigma(i)$ με $q_{\sigma(i)} = p_i$. Οπότε, προκύπτει

$$p_k = r_1 \cdots r_{l-k+1}$$

όπου $r_1, \ldots, r_{l-k+1}$ είναι κάποια από τα $q_1, \ldots, q_l$. Καθώς το πολυώνυμο p_k είναι κανονικό και ανάγωγο, έπεται $k = l$ και $p_k = r_1$. $\square$

Ας είναι P το σύνολο των κανονικών αναγώγων πολυωνύμων του $K[x]$. Σύμφωνα με το παραπάνω θεώρημα κάθε πολυώνυμο $f \in K[x]$ γράφεται ως εξής:

$$f = c \prod_{p \in P} p^{a_p},$$

όπου $c \in K$, $p \in P$ και a_p ακέραιοι ≥ 0. Επισης, πεπερασμένο πλήθος εκθετών a_p είναι $\neq 0$. Η γραφή αυτή μας επιτρέπει να προσδιορίζουμε εύκολα τους διαιρέτες του f.

Πρόταση 4.24 *Ας είναι*

$$f = c \prod_{p \in P} p^{a_p},$$

με $c \neq 0$. *Ένα πολυώνυμο* $g \in K[x]$ *διαιρεί το* f *αν και μόνον αν*

$$g = d \prod_{p \in P} p^{b_p},$$

όπου $d \in K \setminus \{0\}$ *και* $0 \leq b_p \leq a_p$ *για κάθε* $p \in P$.

Απόδειξη. Ας είναι

$$g = d \prod_{p \in P} p^{b_p},$$

όπου $d \in K \setminus \{0\}$ και $0 \leq b_p \leq a_p$ για κάθε $p \in P$. Θέτουμε

$$h = ad^{-1} \prod_{p \in P} p^{a_p - b_p},$$

όπου $c_p = a_p - b_p$ για κάθε $p \in P$. Τότε $gh = f$ και επομένως $g|f$.

Αντίστροφα, ας υποθέσουμε ότι $g|f$. Τότε υπάρχει $h \in K[x]$ με $f = gh$. Έτσι, η μοναδικότητα της γραφής του g ως γινόμενο κανονικών αναγώγων πολυωνύμων, δίνει:

$$g = d \prod_{p \in P} p^{b_p},$$

όπου $d \in K \setminus \{0\}$ και $0 \leq b_p \leq a_p$ για κάθε $p \in P$. $\square$

Πρόταση 4.25 *Ας είναι*

$$f = c\prod_{p\in P} p^{a_p}, \quad g = d\prod_{p\in P} p^{b_p},$$

όπου $c, d \in K$. *Τοτε*

$$\mu\kappa\delta(f,g) = \prod_{p\in P} p^{\min\{a_p,b_p\}}, \quad \epsilon\kappa\pi(f,g) = \prod_{p\in P} p^{\max\{a_p,b_p\}}.$$

Απόδειξη. Από την Πρόταση 4.24 έχουμε ότι το κανονικό πολυώνυμο

$$D = \prod_{p\in P} p^{\min\{a_p,b_p\}}$$

διαιρεί τα f και g. Από την άλλη πλευρά, αν $h|f$ και $h|g$, τότε

$$h = \prod_{p\in P} p^{h_p},$$

με $h_p \leq a_p$ και $h_p \leq b_p$ για κάθε $p \in P$, απ' όπου $h_p \leq \min\{a_p, b_p\}$ για κάθε $p \in P$ και επομένως $h|D$. Άρα $D = \mu\kappa\delta(f,g)$. Ανάλογα αποδεικνύεται και η δεύτερη ισότητα. □

4.5 Ασκήσεις

1. Ας είναι E ένα σύνολο και $\mathcal{P}(E)$ το δυναμοσύνολό του. Να δειχθεί ότι τα ζεύγη $(\mathcal{P}(E), \cap)$ και $(\mathcal{P}(E), \cup)$ είναι μονοειδή και η απεικόνιση

$$f : \mathcal{P}(E) \longrightarrow \mathcal{P}(E),\ A \longmapsto A^c$$

ένας ισομορφισμός μονοειδών.

2. Ας είναι $f : G \to H$ ένας μορφισμός μονοειδών. Να δειχθεί ότι ισχύουν τα εξής:
(α) Αν S είναι υπομονοειδές της G, τότε η εικόνα της $f(S)$ είναι υπομονοειδές της H.
(β) Αν T είναι υπομονοειδές της H, τότε η αντίστροφη εικόνα της $f^{-1}(T)$ είναι υπομονοειδές της G.

3. Ας είναι $(H_i)_{i\in I}$ μία οικογένεια υποομάδων της G. Να δειχθεί ότι η τομή $\cap_{i\in I} H_i$ είναι υποομάδα της G.

4. Πάνω σ' ένα κύκλο C θεωρούμε ένα σημείο O. Για κάθε ζεύγος σημείων (M_1, M_2) του C συμβολίζουμε με $\ell(M_1, M_2)$ την ευθεία που διέρχεται από τα M_1 και M_2. Από το O φέρουμε την παράλληλο ευθεία προς την $\ell(M_1, M_2)$ η οποία τέμνει τον C στο σημείο $M_1 * M_2$. Αν $M_1 = M_2$, τότε η $\ell(M_1, M_2)$ είναι η εφαπτόμενη ευθεία στο M_1. Να δειχθεί ότι η αντιστοιχία $(M_1, M_2) \to M_1 * M_2$ ορίζει μία πράξη επί του C. Να δειχθεί ότι ο κύκλος C με αυτή την πράξη είναι μία αβελιανή ομάδα.

5. Ας είναι f αριθμητική συνάρτηση και F η αριθμητική συνάρτηση που ορίζεται από τη σχέση

$$F(n) = \sum_{d|n} f(d),$$

για κάθε θετικό ακέραιο n. Να δειχθεί ότι η συνάρτηση f είναι πολλαπλασιαστική αν και μόνον αν η F είναι πολλαπλασιαστική.

6. Να δειχθεί ότι για κάθε θετικό ακέραιο n ισχύουν οι σχέσεις:

$$\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d}\tau(d), \quad \sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d).$$

7. Να προσδιοριστούν οι ενδομορφισμοί και αυτομορφισμοί των ομάδων $(\mathbb{Z}, +)$ και $(\mathbb{Q}, +)$.

8. Να προσδιοριστούν οι ενδομορφισμοί και αυτομορφισμοί μίας κυκλικής ομάδας.

9. Ας είναι S ένα μη-κενό υποσύνολο της G. Τότε:

$$< S > = \{x_1^{a_1} \cdots x_n^{a_n} / \ n \geq 1, \ x_i \in S, \ a_i \in \mathbb{Z}\}.$$

10. Να δειχθεί ότι η ομάδα S_3 δεν είναι αντιμεταθετική και να βρεθούν όλες οι υποομάδες της.

11. Μία μετάθεση του S_n της μορφής

$$(a_1, \ldots, a_k) = \begin{pmatrix} a_1 & a_2 & \ldots & a_k & a_{k+1} & \ldots & a_n \\ a_2 & a_3 & \ldots & a_1 & a_{k+1} & \ldots & a_n \end{pmatrix}$$

καλείται *κύκλος μήκους* k. Δύο κύκλοι $(a_1, \ldots, a_k)$ και $(b_1, \ldots, b_l)$ καλούνται *ξένοι μεταξύ τους*, αν $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$. Να δειχθεί ότι κάθε μετάθεση αναλύεται κατά μοναδικό τρόπο σε γινόμενο κύκλων ξένων μεταξύ τους ανά δύο.

12. Να δειχθούν τα εξής:
(α) Η σύνθεση δύο μορφισμών δακτυλίων είναι μορφισμός.
(β) Η αντίστροφη απεικόνιση ενός ισομορφισμού δακτυλίων είναι ισομορφισμός.
(γ) Αν $f : A \to B$ είναι μορφισμός δακτυλίων, τότε το σύνολο $f(A)$ είναι υποδακτύλιος του B.

13. Να δειχθεί ότι ο μοναδικός ενδομορφισμός του δακτυλίου $\mathbb{Z}$ είναι η ταυτοτική απεικόνιση.

14. Ας είναι K είναι ένα σώμα χαρακτηριστικής 0, $g(x)$ ένα πολυώνυμο του $K[x]$ βαθμού d και $a \in K$. Τότε να δειχθεί ότι ισχύει

$$g(x+a) = g(a) + xg'(a) + \frac{1}{2!}x^2 g^{(2)}(a) + \cdots + \frac{1}{d!}x^d g^{(d)}(a).$$

15. Ας υποθέσουμε ότι K είναι ένα σώμα χαρακτηριστικής 0. Να δειχθεί ότι στοιχείο $a \in K$ είναι ρίζα πολλαπλότητας k του πολυωνύμου $f \in K[x]$ αν και μόνον αν ισχύουν τα εξής:

$$f(a) = 0, \;\; f'(a) = 0, \ldots, f^{(k-1)}(a) = 0 \;\; \text{και} \;\; f^{(k)}(a) \neq 0.$$

16. Να δειχθεί ότι το πολυώνυμο

$$P = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

δεν έχει ρίζα με πολλαπλότητα > 1 μέσα στο $\mathbb{C}$.

17. Ας είναι m και n δύο ακέραιοι > 0. Αν r είναι το υπόλοιπο της διαίρεσης του m με τον n, τότε $x^r - 1$ είναι το υπόλοιπο της διαίρεσης του $x^m - 1$ με το $x^n - 1$ μέσα στο $K[x]$, όπου K είναι σώμα.

18. Ας είναι $f = a_0 + a_1 x + \cdots + a_n x^n$ και $g = b_0 + b_1 x + \cdots + b_m x^m$

πολυώνυμα του $\mathbb{Z}[x]$. Να σχεδιαστεί ένας αλγόριθμος ο οποίος να υπολογίζει το πολυώνυμο $f(g) = a_0 + a_1(g(x)) + \cdots + a_n(g(x))^n$.

19. Θεωρούμε τα πολυώνυμα $f = 2x^4+5x^2-x+10$ και $g = x^3+5x+1$. Να υπολογιστεί ο μέγιστος κοινός διαιρέτης d των f, g και πολυώνυμα u, v τέτοια, ώστε $d = uf + vg$.

20. Ας είναι $f, g \in \mathbb{Z}[x]$ με $n = \deg f \geq \deg g$ και $lc(g) = \pm 1$. Ας υποθέσουμε ότι τα μήκη των απολύτων τιμών των συντελεστών των f και g είναι $\leq k$. Να βρεθεί το πλήθος των δυαδικών ψηφιακών πράξεων που απαιτείται για τον υπολογισμό του πηλίκου και του υπολοίπου της διαίρεσης του f με το g.

21. Αν $f \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ και οι απόλυτες τιμές των συντελεστών του f και του a έχουν μήκος $\leq k$, τότε να βρεθεί το πλήθος των δυαδικών ψηφιακών πράξεων που χρειάζεται για τον υπολογισμό της τιμής $f(a)$.

Βιβλιογραφία

[1] M. W. Baldoni, C. Ciliberto and G. M. Piacentini Cattaneo, *Elementary Number Theory, Cryptography and Codes,* Springer-Verlag 2009.

[2] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra,* Cambridge University Press 1999.

[3] V. Shoup, *Μία Υπολογιστική Εισαγωγή στη Θεωρία Αριθμών και την Άλγεβρα,* Εκδόσεις Κλειδάριθμος 2007.

[4] F. Winkler, *Polynomial Algorithms in Computer Algebra,* Springer-Verlag 1996.

[5] Δ. Πουλάκης, *Άλγεβρα,* Εκδόσεις Ζήτη, Θεσσαλονίκη 2015.

Κεφάλαιο 5

Ισοτιμίες

Σύνοψη
Το κεφάλαιο αυτό είναι αφιερωμένο στις Ισοτιμίες των ακεραίων αριθμών. Μελετάμε τις βασικές ιδιότητες των ισοτιμιών και περιγράφουμε την επίλυση των γραμμικών ισοτιμιών καθώς και των συστημάτων τους. Εισάγουμε την συνάρτηση ϕ του Euler και προσδιορίζουμε τους θετικούς ακεραίους n για τους οποίους υπάρχουν πρωτογενείς ρίζες κατά μέτρο n. Επίσης εισάγουμε τα σύμβολα των Legendre και Jacobi και μελετάμε την επίλυση των τετραγωνικών ισοτιμιών. Τέλος, περιγράφουμε την κατασκευή των πεπερασμένων σωμάτων και δίνουμε μερικές βασικές τους ιδιότητες. Περισσότερες πληροφορίες ο αναγνώστης μπορεί να βρεί στα συγγράμματα [1, 2, 3, 5].

Προαπαιτούμενη γνώση
Κεφάλαια 1, 3 και 4.

5.1 Σχέσεις Ισοτιμίας

Ας είναι n θετικός ακέραιος και $a, b \in \mathbb{Z}$. Λέμε ότι ο a είναι *ισότιμος κατά μέτρο* n προς τον b, και γράφουμε $a \equiv b \pmod{n}$, αν $n|a-b$. Αν δεν συμβαίνει αυτό, τότε λέμε ότι οι a και b είναι *ανισότιμοι* κατά μέτρο n και γράφουμε $a \not\equiv b \pmod{n}$.

Παράδειγμα 5.1 Έχουμε $17 \equiv 5 \pmod{6}$ και $39 \equiv 5 \pmod{17}$, γιατί $6|17-5$ και $17|39-5$, αντίστοιχα. Επίσης, παρατηρούμε ότι $17 \not\equiv 7 \pmod{6}$ και $39 \not\equiv 9 \pmod{17}$.

Άμεση συνέπεια του ορισμού είναι τα εξής:

1. $a \equiv 0 \pmod{n} \Leftrightarrow n|a$.
2. Ο ακέραιος a είναι άρτιος, αν και μόνον αν $a \equiv 0 \pmod{2}$.
3. Ο ακέραιος a είναι περιττός, αν και μόνον αν $a \equiv 1 \pmod{2}$.
4. Αν $a \equiv b \pmod{n}$ και m φυσικός με $m|n$, τότε $a \equiv b \pmod{m}$.
5. Για κάθε ζεύγος ακεραίων ισχύει $a \equiv b \pmod{1}$.

Πρόταση 5.1 *Ας είναι $a, b, c \in \mathbb{Z}$. Τότε ισχύουν τα εξής:*
(α) $a \equiv a \pmod{n}$, για κάθε $a \in A$.
(β) Αν $a \equiv b \pmod{n}$, τότε $b \equiv a \pmod{n}$.
(γ) Αν $a \equiv b \pmod{n}$ και $b \equiv c \pmod{n}$, τότε $a \equiv c \pmod{n}$.

Απόδειξη. (α) Για κάθε $a \in \mathbb{Z}$ έχουμε $n|0$ και επομένως $n|a-a$, απ' όπου $a \equiv a \pmod{n}$.

(β) Αν $a \equiv b \pmod{n}$, τότε $n|a-b$, απ' όπου $n|b-a$ και επομένως $b \equiv a \pmod{n}$.

(γ) Ας είναι $a \equiv b \pmod{n}$ και $b \equiv c \pmod{n}$. Τότε $n|a-b$ και $n|b-c$. Οπότε $n|(a-b)+(b-c)$ και επομένως $n|a-c$ που δίνει $a \equiv c \pmod{n}$. □

Πρόταση 5.2 *Έχουμε $a \equiv b \pmod{n}$ αν και μόνον αν η διαίρεση των a και b με n δίνει το ίδιο υπόλοιπο.*

Απόδειξη. Σύμφωνα με το Θεώρημα 1.1, υπάρχουν ακέραιοι u, v, r, s τέτοιοι, ώστε

$$a = un + r, \quad b = vn + s \quad \text{και} \quad 0 \leq r, s < n.$$

Έχουμε $n|a-b$ αν και μόνον αν $n|r-s$. Καθώς όμως $0 \leq |r-s| < n$, έχουμε $n|r-s$ αν και μόνον αν $r = s$. □

Πρόταση 5.3 *Για κάθε $a, b, c, d \in \mathbb{Z}$ με $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$ έχουμε:*

$$a + c \equiv b + d \pmod{n} \quad \text{και} \quad ac \equiv bd \pmod{n}.$$

Απόδειξη. Από τις σχέσεις $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$ παίρνουμε $n|a-b$ και $n|c-d$. Έτσι, έχουμε $n|(a+c)-(b+d)$ και επομένως $a+c \equiv b+d \pmod{n}$. Επίσης, έχουμε $n|c(a-b)$ και $n|b(c-d)$, απ΄ όπου προκύπτει $n|ac-bd$ και κατά συνέπεια $ac \equiv bd \pmod{n}$. □

Πόρισμα 5.1 *Ας είναι $a, b \in \mathbb{Z}$ με $a \equiv b \pmod{n}$. Τότε, για κάθε $m \in \mathbb{N}$ έχουμε:*

$$ma \equiv mb \pmod{n} \quad \textit{και} \quad a^m \equiv b^m \pmod{n}.$$

Απόδειξη. Θα αποδείξουμε τη δεύτερη σχέση εφαρμόζοντας επαγωγή επί του m. Για $m = 0$ προφανώς ισχύει. Ας υποθέσουμε ότι ισχύει για $m = k$. Τότε έχουμε $a^k \equiv b^k \pmod{n}$. Καθώς $a \equiv b \pmod{n}$, η Πρόταση 5.3 μας δίνει $a^{k+1} \equiv b^{k+1} \pmod{n}$. Συνεπώς, για κάθε $m \in \mathbb{N}$, ισχύει $a^m \equiv b^m \pmod{n}$. Όμοια παίρνουμε και την πρώτη σχέση. □

Πόρισμα 5.2 *Ας είναι $a, b \in \mathbb{Z}$ με $a \equiv b \pmod{n}$ και $f(x) \in \mathbb{Z}[x]$. Τότε $f(a) \equiv f(b) \pmod{n}$.*

Απόδειξη. Ας είναι $f(x) = c_0 + c_1 x + \cdots + c_m x^m$. Σύμφωνα με το Πόρισμα 5.1, για κάθε $i = 0, \ldots, m$ έχουμε $a^i \equiv b^i \pmod{n}$ και στη συνέχεια $c_i a^i \equiv c_i b^i \pmod{n}$. Οπότε, η Πρόταση 5.3 δίνει $f(a) \equiv f(b) \pmod{n}$.

Παράδειγμα 5.2 Θα υπολογίσουμε το υπόλοιπο της διαίρεσης του $8^{20}11^{15}$ με τον 9. Έχουμε $8 \equiv -1 \pmod{9}$. Οπότε

$$8^{20} \equiv (-1)^{20} \equiv 1 \pmod{9}.$$

Επίσης, $11 \equiv 2 \pmod{9}$ και επομένως

$$11^{15} \equiv (2^3)^5 \equiv 8^5 \equiv -1 \equiv 8 \pmod{9}.$$

Άρα, έχουμε

$$8^{20}11^{15} \equiv 8 \pmod{9}$$

και επομένως υπάρχει ακέραιος a τέτοιος, ώστε

$$8^{20}11^{15} = 9a + 8.$$

Συνεπώς, το υπόλοιπο της διαίρεσης του $8^{20}11^{15}$ με τον 9 είναι 8.

Παράδειγμα 5.3 Ας είναι $a, b \in \mathbb{Z}$ και p ένας πρώτος. Θα δείξουμε ότι ισχύει:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Από την Πρόταση 4.12 έχουμε:

$$(a+b)^p = \sum_{k=0}^{n} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} b^k.$$

Για κάθε $k = 1, 2, \ldots, p-1$ έχουμε:

$$\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p(p-1)\cdots(p-k+1)}{k!}.$$

Επομένως

$$p \Big| k! \left(\begin{array}{c} p \\ k \end{array} \right) \quad \text{και} \quad \mu\kappa\delta(p, k!) = 1.$$

Έτσι, παίρνουμε:

$$p \Big| \left(\begin{array}{c} p \\ k \end{array} \right) \quad (k = 1, 2, \ldots, p-1)$$

και κατά συνέπεια ισχύει:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

5.2 Κλάσεις Ισοτιμίας

Ας είναι $n, a \in \mathbb{Z}$ και $n > 0$. Το σύνολο

$$[a]_n = \{x \in \mathbb{Z} / \ x \equiv a \pmod{n}\}$$

καλείται *κλάση ισοτιμίας του a κατά μέτρο n*. Συμβολίζουμε με $\mathbb{Z}/(n)$ το σύνολο όλων των κλάσεων ισοτιμίας. Από την Πρόταση 5.1 έχουμε $a \in [a]_n$ και επομένως συνάγεται ότι $[a]_n \neq \emptyset$. Επιπλέον, η ένωση όλων των κλάσεων δίνει το σύνολο $\mathbb{Z}$.

Πρόταση 5.4 *Ας είναι $a, b \in \mathbb{Z}$. Τότε ισχύουν τα εξής:*
(α) $a \equiv b \pmod{n}$ *αν και μόνον αν* $[a]_n = [b]_n$.
(β) Αν $[a]_n \neq [b]_n$, *τότε* $[a]_n \cap [b]_n = \emptyset$.

Απόδειξη. (α) Ας είναι $a \equiv b \pmod{n}$. Αν $x \in [a]_n$, τότε $x \equiv a \pmod{n}$. Καθώς $a \equiv b \pmod{n}$, από την Πρόταση 5.1 παίρνουμε $x \equiv b \pmod{n}$ και επομένως $x \in [b]_n$. Συνεπώς $[a]_n \subseteq [b]_n$. Όμοια προκύπτει $[b]_n \subseteq [a]_n$ και έτσι έχουμε $[a]_n = [b]_n$. Αντίστροφα, ας υποθέσουμε ότι $[a]_n = [b]_n$. Έχουμε $a \in [a]_n$ και επομένως $a \in [b]_n$, απ΄ όπου $a \equiv b \pmod{n}$.

(β) Ας υποθέσουμε ότι $[a]_n \neq [b]_n$. Αν $[a]_n \cap [b]_n \neq \emptyset$, τότε υπάρχει $x \in [a]_n \cap [b]_n$. Άρα έχουμε $x \equiv a \pmod{n}$ και $x \equiv b \pmod{n}$, απ΄ όπου έπεται $a \equiv b \pmod{n}$. Έτσι, από την (α) έχουμε $[a]_n = [b]_n$ που είναι άτοπο. Άρα $[a]_n \cap [b]_n = \emptyset$. □

Πρόταση 5.5 *Οι κλάσεις $[0]_n, [1]_n, \ldots, [n-1]_n$ είναι όλα τα διακεκριμμένα στοιχεία του $\mathbb{Z}/(n)$.*

Απόδειξη. Ας είναι $a \in \mathbb{Z}$. Τότε υπάρχουν $q, r \in \mathbb{Z}$ με $a = nq + r$ και $0 \leq r < n$. Έτσι, έχουμε $n|a - r$ και επομένως $a \equiv r \pmod{n}$. Οπότε, η Πρόταση 5.4 δίνει $[a]_n = [r]_n$. Από την άλλη πλευρά, από την Πρόταση 5.2 έπεται ότι οι αριθμοί $0, 1, \ldots, n-1$ είναι ανά δύο ανισότιμοι κατά μέτρο n και επομένως οι κλάσεις $[0]_n, [1]_n, \ldots, [n-1]_n$ είναι διαφορετικές ανά δύο. Άρα, οι κλάσεις $[0]_n, [1]_n, \ldots, [n-1]_n$ είναι όλα τα διακεκριμμένα στοιχεία του $\mathbb{Z}/(n)$. □

Από την Πρόταση 5.3 έχουμε ότι για κάθε $a, b, c, d \in \mathbb{Z}$ με $[a]_n = [b]_n$ και $[c]_n = [d]_n$ ισχύει

$$[a + c]_n = [b + d]_n \quad \text{και} \quad [ac]_n = [bd]_n.$$

Έτσι, μπορούμε να ορίσουμε δύο πράξεις επί του $\mathbb{Z}/(n)$ θέτοντας

$$[a]_n + [b]_n = [a + b]_n \quad \text{και} \quad [a]_n \cdot [b]_n = [ab]_n,$$

για κάθε $[a]_n, [b]_n \in \mathbb{Z}/(n)$. Οι πράξεις αυτές καλούνται *πρόσθεση* και *πολλαπλασιασμός*, αντίστοιχα. Εύκολα αποδεικνύεται ότι το σύνολο $\mathbb{Z}/(n)$ με αυτές τις πράξεις αποτελεί αντιμεταθετικό δακτύλιο. Παρατηρούμε ότι $n[1]_n = [n]_n = [0]_n$ και για κάθε θετικό ακέραιο $k < n$ ισχύει $k[1]_n = [k]_n \neq [0]_n$. Άρα $\mathrm{char}\mathbb{Z}/(n) = n$. Θα συμβολίζουμε με $(\mathbb{Z}/(n))^*$ το σύνολο των κλάσεων που έχουν αντίστροφο στοιχείο.

Πρόταση 5.6 *Ας είναι $a \in \mathbb{Z}$. Έχουμε $[a]_n \in (\mathbb{Z}/(n))^*$ αν και μόνον $\mu\kappa\delta(a, n) = 1$.*

Απόδειξη. Η κλάση $[a]_n$ είναι αντιστρέψιμη αν και μόνον αν υπάρχει $[b]_n \in \mathbb{Z}/(n)$ έτσι, ώστε $[a]_n \cdot [b]_n = [1]_n$ που είναι ισοδύναμο με $ab \equiv 1 \pmod{n}$. Αυτό όμως ισχύει αν και μόνον αν υπάρχει $k \in \mathbb{Z}$ με $ab + kn = 1$ που ισοδυναμεί με $\mu\kappa\delta(a, n) = 1$. □

Πόρισμα 5.3 *Ο δακτύλιος $\mathbb{Z}/(n)$ είναι σώμα αν και μόνον αν ο n είναι πρώτος.*

Απόδειξη. Όλες οι κλάσεις του $\mathbb{Z}/(n) \setminus \{[0]_n\}$ έχουν αντίστροφο αν και μόνον αν $\mu\kappa\delta(i, n) = 1$ $(i = 1, \ldots, n-1)$ που ισχύει αν και μόνον αν ο n είναι πρώτος. □

Πόρισμα 5.4 *Ας είναι n, a, b, c ακέραιοι με $n > 1$, $\mu\kappa\delta(a, n) = 1$ και $ab \equiv ac \pmod{n}$. Τότε $b \equiv c \pmod{n}$.*

Απόδειξη. Καθώς $\mu\kappa\delta(a, n) = 1$, σύμφωνα με την Πρόταση 5.6, υπάρχει ακέραιος a' τέτοιος, ώστε $a'a \equiv 1 \pmod{n}$ και επομένως πολλαπλασιάζοντας και τα δύο μέλη της $ab \equiv ac \pmod{n}$ με a' παίρνουμε $b \equiv c \pmod{n}$. □

Παράδειγμα 5.4 Οι ακέραιοι 17 και 63 είναι πρώτοι μεταξύ τους. Θα υπολογίσουμε την αντιστροφο κλάση της $[17]_{63}$. Από τον εκτεταμένο Ευκλείδιο αλγόριθμο παίρνουμε:

$$26 \cdot 17 + 63 \cdot 7 = 1.$$

Έτσι, έχουμε $26 \cdot 17 \equiv 1 \pmod{63}$ και κατά συνέπεια $[26]_{63} = [17]_{63}^{-1}$.

Στην Ενότητα 1.4 εισαγάγαμε τον συμβολισμό $a \bmod b$ για το υπόλοιπο της διαίρεσης ενός ακεραίου a μ΄ ένα θετικό ακέραιο b. Έτσι, η γραφή $r = a \bmod b$ συμβολίζει ότι ο ακέραιος r είναι το υπόλοιπο της διαίρεσης του a με το b, απ΄ όπου έπεται ότι $r \equiv a \pmod{b}$.

Θεωρούμε το σύνολο $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ και τις παρακάτω πράξεις, πρόσθεση και πολλαπλασιασμό

$$a \oplus b = a + b \bmod n, \quad a \odot b = ab \bmod n.$$

Εύκολα αποδεικνύεται ότι το $\mathbb{Z}_n$ με αυτές τις πράξεις αποτελεί αντιμεταθετικό δακτύλιο. Συμβολίζουμε με $\mathbb{Z}_n^*$ το σύνολο των στοιχείων του $\mathbb{Z}_n$ που έχουν αντίστροφο. Π.χ. $\mathbb{Z}_{12} = \{1, 5, 7, 11\}$. Τέλος, αν $a \in \mathbb{Z}_n^*$, τότε θα συμβολίζουμε το αντίστροφο του a με $a^{-1} \bmod n$.

Η απεικόνιση

$$\pi_n : \mathbb{Z}_n \longrightarrow \mathbb{Z}/(n),\ a \longmapsto [a]_n.$$

είναι αμφίεση και για κάθε $a, b \in \mathbb{Z}_n$ έχουμε

$$\pi_n(a \oplus b) = [a+b]_n = [a]_n + [b]_n = \pi_n(a) + \pi_n(b)$$

και

$$\pi_n(a \odot b) = [ab]_n = [a]_n[b]_n = \pi_n(a)\pi_n(b).$$

Άρα, η π_n είναι ισομορφισμός δακτυλίων με αντίστροφη απεικόνιση

$$\pi_n^{-1} : \mathbb{Z}/(n) \longrightarrow \mathbb{Z}_n,\ [a]_n \longmapsto a \bmod n.$$

Έτσι, έχουμε $\pi_n(\mathbb{Z}_n^*) = (\mathbb{Z}/(n))^*$ και κατά συνέπεια $a \in \mathbb{Z}_n^*$ αν και μόνον αν $\mu\kappa\delta(a, n) = 1$. Επίσης, ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνον αν ο n είναι πρώτος. Επομένως, στην πράξη θα χρησιμοποιούμε τον δακτύλιο $\mathbb{Z}_n$. Θα εξετάσουμε στη συνέχεια το κόστος των πράξεων σ΄ αυτόν.

Πρόταση 5.7 *Ας είναι $a, b \in \mathbb{Z}_n$. Ο υπολογισμός του αθροίσματος $a + b \bmod n$ και του γινομένου $ab \bmod n$ χρειάζονται $O(\ell(n))$ και $O(\ell(n)^2)$ δυαδικές ψηφιακές πράξεις, αντίστοιχα. Επίσης, αν $a \in \mathbb{Z}_n^*$, τότε ο υπολογισμός του αντιστρόφου $a^{-1} \bmod n$ χρειάζεται $O(\ell(n)^2)$ δυαδικές ψηφιακές πράξεις.*

Απόδειξη. Καθώς $0 \leq a, b \leq n-1$, έχουμε $0 \leq a+b < 2n$ και επομένως $a + b \bmod n = a + b$, αν $a + b < n$ και $a + b \bmod n = a+b-n$ διαφορετικά. Ο υπολογισμός του $a+b$ καθώς και της διαφοράς $a + b - n$ χρειάζεται $O(\ell(n))$ δυαδικές ψηφιακές πράξεις. Συνεπώς, ο υπολογισμός του $a + b \bmod n$ χρειάζεται $O(\ell(n))$ δυαδικές ψηφιακές πράξεις.

Ο υπολογισμός του ab απαιτεί $O(\ell(n)^2)$ δυαδικές ψηφιακές πράξεις. Το ίδιο και ο υπολογισμός του υπολοίπου της διαίρεσης του ab με το n. Επομένως, ο υπολογισμός του $ab \bmod n$ απαιτεί $O(\ell(n)^2)$ δυαδικές ψηφιακές πράξεις.

Ας είναι τώρα $a \in \mathbb{Z}_n^*$. Τότε $\mu\kappa\delta(a, n) = 1$. Σύμφωνα με την Πρόταση 1.10 μπορούμε να βρούμε $u, v \in \mathbb{Z}$ με $au + nv = 1$ και $|u| < n$. Κατόπιν, υπολογίζουμε $v = u \bmod n$ που είναι το στοιχείο $a^{-1} \bmod n$. Ο χρόνος εκτέλεσης των υπολογισμών είναι $O(\ell(n)^2)$ δυαδικές ψηφιακές πράξεις. □

Ας είναι $a \in \mathbb{Z}_n$ και k θετικός ακέραιος. Ο υπολογισμός του $a^k \bmod n$ είναι σημαντικός σε πολλά κρυπτογραφικά σχήματα. Για να τον πραγματοποιήσουμε υπολογίζουμε πρώτα τον ακέραιο a^k και στη συνέχεια το υπόλοιπο της διαίρεσης του a^k με τον n ή για κάθε $i = 1, \ldots, k$ υπολογίζουμε τον $a^i \bmod n$ πολλαπλασιάζοντας τον $a^{i-1} \bmod n$ με τον a και κατόπιν διαιρώντας το αποτέλεσμα με τον n. Στην πρώτη περίπτωση ο υπολογισμός του a^k απαιτεί $O((k\ell(a))^2)$ δυαδικές ψηφιακές πράξεις και η διαίρεση του a^k με τον n, $O(\ell(n)k\ell(a))$ δυαδικές ψηφιακές πράξεις. Έτσι, συνολικά στην πρώτη περίπτωση χρειάζονται $O((k\ell(n))^2)$ δυαδικές ψηφιακές πράξεις. Στη δεύτερη περίπτωση ο υπολογισμός του $a^i \bmod n$ από τον $a^{i-1} \bmod n$ και τον a απαιτεί $O(\ell(n)^2)$ δυαδικές ψηφιακές πράξεις και αυτή η διαδικασία γίνεται $k-1$ φορές. Άρα, ο χρόνος υπολογισμού στη δεύτερη περίπτωση είναι $O(k\ell(n)^2)$ δυαδικές ψηφιακές πράξεις. Παρακάτω θα δώσουμε μία ταχύτερη μέθοδο για αυτόν τον υπολογισμό.

Πρόταση 5.8 *Ας είναι $a \in \mathbb{Z}_n$ και k θετικός ακέραιος. Τότε ο υπολογισμός του $a^k \bmod n$ χρειάζεται $O(\ell(n)^2\ell(k))$ δυαδικές ψηφιακές πράξεις.*

Απόδειξη. Άμεση συνέπεια της Πρότασης 4.3. □

Ο παρακάτω αλγόριθμος βασίζεται στη Πρόταση 5.8.

Αλγόριθμος 5.1 Ύψωση σε δύναμη κατά μέτρο n με τετραγωνισμό και πολλαπλασιασμό.
Είσοδος: $a \in \mathbb{Z}_n$ και k θετικός ακέραιος με $k = k_t 2^t + \cdots + k_0$.
Έξοδος: $a^k \bmod n$.

1. Θέτουμε $A_0 = a$ και $P_0 = a^{k_0}$.
2. Για $i = 1, \ldots, t$ υπολογίζουμε τα παρακάτω:
   (α′) $A_i = A_{i-1}^2 \bmod n$.
   (β′) $P_i = A_i^{k_i} P_{i-1} \bmod n$.
3. Εξάγουμε τη τιμή P_t.

Παράδειγμα 5.5 Θα υπολογίσουμε τον ακέραιο $17^{23} \bmod 111$ χρησιμοποιώντας τον παραπάνω αλγόριθμο. Η δυαδική παράσταση του 23 είναι:

$$23 = \sum_{i=0}^{4} k_i 2^i = (10111)_2.$$

Έχουμε $A_0 = 17$ και $P_0 = 17$. Για $i = 1$ παίρνουμε:

$$A_1 = 17^2 \bmod 111 = 67, \quad P_1 = A_1^{k_1} P_0 = 67 \cdot 17 \bmod 111 = 29.$$

Για $i = 2$ έχουμε:

$$A_2 = 67^2 \bmod 111 = 49, \quad P_2 = A_2^{k_2} P_1 = 49 \cdot 29 \bmod 111 = 89.$$

Για $i = 3$ παίρνουμε:

$$A_3 = 49^2 \bmod 111 = 70, \quad P_3 = A_3^{k_3} P_2 = P_2 = 89.$$

Τέλος, για $i = 4$ προκύπτει:

$$A_4 = 70^2 \bmod 111 = 16, \quad P_4 = A_4^{k_4} P_3 = 16 \cdot 89 \bmod 111 = 92.$$

Συνεπώς, ισχύει:

$$17^{23} \bmod 111 = 92.$$

5.3 Γραμμικές Ισοτιμίες

Ας είναι n θετικός ακέραιος και $f(x) = a_0 x^k + \cdots + a_k$ πολυώνυμο με ακέραιους συντελεστές. Μία ισοτιμία της μορφής

$$f(x) \equiv 0 \pmod{n},$$

όπου x άγνωστος ακέραιος καλείται *πολυωνυμική*. Λέμε ότι ένας ακέραιος x_0 *επαληθεύει* ή *πληροί* την πολυωνυμική ισοτιμία, αν ισχύει $f(x_0) \equiv 0 \pmod{n}$. Τότε για κάθε ακέραιο y με $y \equiv x_0 \pmod{n}$ έχουμε $f(y) \equiv f(x_0) \equiv b \pmod{n}$ και επομένως ο y πληροί επίσης την πολυωνυμική ισοτιμία. Έτσι, θα καλούμε *λύση* της παραπάνω ισοτιμίας κάθε κλάση $[x_0]_n$ της οποίας ένας αντιπρόσωπος (και επομένως όλοι) την επαληθεύει. Τότε θα λέμε ότι η πολυωνυμική ισοτιμία έχει τη λύση $x \equiv x_0 \pmod{n}$. Αν $a_0 \equiv \cdots \equiv a_{k-m-1} \equiv 0 \pmod{n}$ και $a_{k-m} \not\equiv 0 \pmod{n}$, τότε έχουμε

$$f(x) \equiv a_{k-m} x^m + \cdots + a_k \equiv 0 \pmod{n}.$$

Ο ακέραιος m καλείται *βαθμός* της $f(x) \equiv 0 \pmod{n}$. Αν $m = 1$, τότε η πολυωνυμική ισοτιμία καλείται *γραμμική* και αν $m = 2$ τετραγωνική.

Παράδειγμα 5.6 Ας θεωρήσουμε τη γραμμική ισοτιμία

$$2x \equiv 6 \pmod{10}.$$

Δοκιμάζοντας και τα 10 στοιχεία του $\mathbb{Z}_{10}$ βρίσκουμε ότι όλες οι λύσεις της γραμμικής ισοτιμίας είναι $x \equiv 3, 8 \pmod{10}$.

Παρατηρούμε ότι οι λύσεις της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod{n}$ συμπίπτουν με τις λύσεις της εξίσωσης $\bar{f}(x) = [0]_n$ μέσα $\mathbb{Z}/(n)$, όπου $\bar{f}(x) = [a_0]_n x^k + \cdots + [a_k]_n$. Πράγματι, η κλάση $[x_0]_n$ είναι λύση της πολυωνυμικής ισοτιμίας αν και μόνον αν ισχύει $f(x_0) \equiv 0 \pmod{n}$ που ισοδυναμεί με $\bar{f}([x_0]_n) = [0]_n$. Ισοδύναμα, οι λύσεις της $f(x) \equiv 0 \pmod{n}$ είναι οι κλάσεις των λύσεων της εξίσωσης $\tilde{f}(x) = 0$ μέσα $\mathbb{Z}_n$, όπου $\tilde{f}(x) = \alpha_0 x^k + \cdots + \alpha_n$ και $\alpha_i \equiv a_i \bmod n$ $(i = 0, \ldots, n)$. Έτσι, το Πόρισμα 4.7 δίνει το εξής αποτέλεσμα:

Πρόταση 5.9 *Ας είναι p πρώτος. Αν $f(x) \equiv 0 \pmod{p}$ είναι μία πολυωνυμική ισοτιμία βαθμού m, τότε αυτή έχει το πολύ m διαφορετικές λύσεις.*

Στη συνέχεια θ′ ασχοληθούμε με τις γραμμικές ισοτιμίες.

Πρόταση 5.10 *Ας είναι n ακέραιος > 1, $a, b \in \mathbb{Z}_n$ και $d = \mu\kappa\delta(a, n)$. Η γραμμική ισοτιμία $ax \equiv b \pmod{n}$ έχει λύση αν και μόνον αν $d|b$. Αν x_0 είναι ένας ακέραιος που επαληθεύει τη γραμμική ισοτιμία, τότε όλες οι διαφορετικές λύσεις της είναι:*

$$x \equiv x_0, x_0 + \frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d} \pmod{n}.$$

Ο χρόνος υπολογισμού ενός τέτοιου ακεραίου x_0 είναι $O(\ell(n)^2)$.

Απόδειξη. Ας υποθέσουμε ότι ο ακέραιος x_0 επαληθεύει τη γραμμική ισοτιμία. Άρα, έχουμε $ax_0 \equiv b \pmod{n}$ και επομένως $ax_0 - b = kn$, όπου $k \in \mathbb{Z}$. Έτσι, καθώς $d|a$ και $d|n$, έχουμε $d|b$. Αντίστροφα, ας υποθέσουμε ότι $d|b$. Τότε $b = de$, όπου $e \in \mathbb{Z}$. Από την άλλη πλευρά, υπάρχουν ακέραιοι u, v με $au + nv = d$ και επομένως $a(ue) + n(ve) = b$.

Άρα $a(ue) \equiv b \pmod{n}$ και κατά συνέπεια η γραμμική ισοτιμία έχει λύση.

Ας υποθέσουμε ότι $d|b$. Θέτουμε $a' = a/d$, $b' = b/d$, $n' = n/d$. Έτσι, για έναν ακέραιο z έχουμε $az \equiv b \pmod{n}$ αν και μόνον αν $a'z \equiv b' \pmod{n'}$. Δηλαδή, οι γραμμικές ισοτιμίες $ax \equiv b \pmod{n}$ και $a'x \equiv b' \pmod{n'}$ επαληθεύονται από το ίδιο σύνολο ακεραίων. Καθώς $\mu\kappa\delta(a', n') = 1$, υπάρχει $c \in \mathbb{Z}$ με $a'c \equiv 1 \pmod{n'}$ και επομένως πολλαπλασιάζοντας και τα δύο μέλη της $a'x \equiv b' \pmod{n'}$ με c παίρνουμε $x \equiv cb' \pmod{n'}$. Θέτουμε $x_0 = cb'$. Οπότε, το σύνολο των ακεραίων που επαληθεύουν την $ax \equiv b \pmod{n}$ αποτελείται από τους $x_0 + kn'$, με $k \in \mathbb{Z}$. Έχουμε:

$$x_0 + k_1 n' \equiv x_0 + k_2 n' \pmod{n} \Longleftrightarrow k_1 \equiv k_2 \pmod{d}.$$

Συνεπώς, όλες οι διαφορετικές λύσεις της $ax \equiv b \pmod{n}$ είναι:

$$x \equiv x_0, x_0 + n', \ldots, x_0 + (d-1)n' \pmod{n}.$$

Ο χρόνος υπολογισμού των d, a', b' και n' είναι $O(\ell(n)^2)$. Από την Πρόταση 5.7 έπεται ότι ο χρόνος υπολογισμού του c είναι $O(\ell(n)^2)$. Συνεπώς, ο χρόνος υπολογισμού του x_0 είναι $O(\ell(n)^2)$. □

Παράδειγμα 5.7 Θα βρούμε τις λύσεις της γραμμικής ισοτιμίας

$$55x \equiv 20 \pmod{75}.$$

Έχουμε $\mu\kappa\delta(55, 75) = 5$ και $5|75$. Έτσι, σύμφωνα με την Πρόταση 5.10, η παραπάνω γραμμική ισοτιμία έχει λύση. Το σύνολο των ακεραίων που την επαληθεύουν συμπίπτει με το σύνολο των ακεραίων που επαληθεύουν τη γραμμική ισοτιμία

$$11x \equiv 4 \pmod{15}.$$

Υπολογίζουμε $11^{-1} \bmod 15 = 11$ και πολλαπλασιάζοντας και τα δύο μέλη της παραπάνω ισοτιμίας με 11 παίρνουμε

$$x \equiv 14 \pmod{15}.$$

Άρα, σύμφωνα με την Πρόταση 5.10, οι ζητούμενες λύσεις είναι:

$$x \equiv 14, 29, 44, 59, 74 \pmod{75}.$$

Καλούμε *λύση* του συστήματος γραμμικών ισοτιμιών

$$a_1x \equiv b_1 \pmod{n_1}, \ldots, a_kx \equiv b_k \pmod{n_k}$$

κάθε ακέραιο που επαληθεύει κάθε μία από τις γραμμικές ισοτιμίες που το αποτελούν. Π.χ. μία λύση του συστήματος

$$2x \equiv 2 \pmod{10}, \quad 3x \equiv 5 \pmod{13}$$

είναι $x = 6$. Ας σημειωθεί ότι υπάρχουν συστήματα που δεν έχουν λύση. Π.χ. αν ο ακέραιος x_0 είναι λύση του συστήματος $x \equiv 3 \pmod{4}$ και $x \equiv 2 \pmod{14}$, τότε ο x_0 είναι ταυτόχρονα άρτιος και περιττός που είναι άτοπο. Συνεπώς, το σύστημα δεν έχει λύση, αν και κάθε μία από τις δύο ισοτιμίες έχει λύση. Θα λέμε ότι ένα σύστημα έχει λύση $x \equiv a \pmod{n}$, αν όλα τα στοιχεία της κλάσης του a κατά μέτρο n είναι λύσεις του συστήματος.

Πρόταση 5.11 *Ας είναι $n_1, \ldots, n_k$ ακέραιοι ≥ 2, πρώτοι μεταξύ τους ανά δύο και $a_1, \ldots, a_k$ ακέραιοι με $0 \leq a_i < n_i$ $(i = 1, \ldots, k)$. Θέτουμε $n = n_1 \cdots n_k$. Το σύστημα γραμμικών ισοτιμιών*

$$x \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k)$$

έχει μοναδική λύση

$$x \equiv \sum_{i=1}^{k} a_i y_i N_i \pmod{n},$$

όπου $N_i = n/n_i$ και $y_i = N_i^{-1} \bmod n_i$. Η λύση αυτή μπορεί να υπολογιστεί σε χρόνο $O(\ell(n)^2)$.

Απόδειξη. Καθώς $\mu\kappa\delta(n_i, N_i) = 1$, από την Πρόταση 5.10 έπεται ότι υπάρχει ακέραιος y_i, με $1 \leq y_i < n_i$ και $y_iN_i \equiv 1 \pmod{n_i}$ $(i = 1, \ldots, k)$. Θέτουμε:

$$x_0 = a_1y_1N_1 + \cdots + a_ky_kN_k.$$

Έχουμε $a_iy_iN_i \equiv a_i \pmod{n_i}$ και καθώς $n_i | N_j$ για $i \neq j$ παίρνουμε $a_jy_jN_j \equiv 0 \pmod{n_i}$. Έτσι, προκύπτει:

$$x_0 \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k).$$

Εύκολα αποδεικνύεται ότι ένας ακέραιος επαληθεύει το σύστημα, αν και μόνον αν βρίσκεται στην κλάση του x_0 κατά μέτρο n.

Για να προσδιορίσουμε τον χρόνο που απαιτεί ο υπολογισμός του ακεραίου x_0 πρέπει να εκτιμήσουμε τις εξής ποσότητες:

1. Χρόνος υπολογισμού του n και των N_i $(i = 1, \ldots, k)$.
2. Χρόνος υπολογισμού των y_i $(i = 1, \ldots, k)$.
3. Χρόνος υπολογισμού του αθροίσματος $a_1y_1N_1 + \cdots + a_ky_kN_k$.

Σύμφωνα με το Παράδειγμα 1.12, ο χρόνος για τον υπολογισμό του n είναι $O(\ell(n)^2)$. Επίσης, ο χρόνος για τον υπολογισμό του N_i είναι $O(\ell(n)\ell(n_i))$ και επομένως ο χρόνος υπολογισμού όλων των N_i είναι

$$O(\ell(n)(k + \log n_1 + \cdots + \log n_k)).$$

Έχουμε $n \geq 2^k$, απ' όπου $k = O(\log n)$ και επομένως ο χρόνος υπολογισμού όλων των N_i είναι $O(\ell(n)^2)$. Για τον υπολογισμό του y_i πρώτα υπολογίζουμε $\nu_i = N_i \bmod n_i$ σε χρόνο $O(\ell(N_i)\ell(n_i))$ και κατόπιν, σύμφωνα με την Πρόταση 5.7, υπολογίζουμε $y_i = \nu_i^{-1} \bmod n_i$ σε χρόνο $O(\ell(n_i)^2)$. Άρα, ο χρόνος για τον υπολογισμό του y_i είναι $O(\ell(n)\ell(n_i))$. Οπότε, ο χρόνος υπολογισμού όλων των y_i είναι:

$$O(\ell(n)(k + \log n_1 + \cdots + \log n_k)) = O(\ell(n)^2).$$

Ο χρόνος υπολογισμού του $a_iy_iN_i$ είναι:

$$O(\ell(y_i)\ell(N_i) + \ell(y_iN_i)\ell(a_i))$$

Καθώς $y_iN_i \leq n$, ο παραπάνω χρόνος ισούται με $O(\ell(n_i)\ell(n))$. Οπότε, ο χρόνος υπολογισμού του αθροίσματος $a_1y_1N_1 + \cdots + a_ky_kN_k$ είναι:

$$O(\ell(n)(k + \log n_1 + \cdots + \log n_k)) = O(\ell(n)^2).$$

Συνεπώς, ο συνολικός χρόνος που απαιτείται για την επίλυση του συστήματος είναι $O(\ell(n)^2)$. □

Πόρισμα 5.5 *Αν είναι $n_1, \ldots, n_k$ ακέραιοι ≥ 2, πρώτοι μεταξύ τους ανά δύο και $n = n_1 \cdots n_k$. Τότε:*

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

και

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_k).$$

Απόδειξη. Θα συμβολίζουμε την πρόσθεση και τον πολλαπλασιασμό μέσα στο $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ επίσης με $\oplus$ και $\odot$, αντίστοιχα. Θεωρούμε την απεικόνιση

$$\pi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},\ a \longmapsto (a \bmod n_1, \ldots, a \bmod n_k).$$

Για κάθε $a, b \in \mathbb{Z}_n$ έχουμε:

$$\begin{aligned} \pi(a \oplus b) &= (a + b \bmod n_1, \ldots, a + b \bmod n_k) \\ &= (a \bmod n_1, \ldots, a \bmod n_k) \oplus (b \bmod n_1, \ldots, b \bmod n_k) \\ &= \pi(a) \oplus \pi(b) \end{aligned}$$

και

$$\begin{aligned} \pi(a \odot b) &= (ab \bmod n_1, \ldots, ab \bmod n_k) \\ &= (a \bmod n_1, \ldots, a \bmod n_k) \odot (b \bmod n_1, \ldots, b \bmod n_k) \\ &= \pi(a) \odot \pi(b). \end{aligned}$$

Επομένως, η απεικόνιση π είναι μορφισμός δακτυλίων.

Αν $(a_1, \ldots, a_k) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, τότε, σύμφωνα με την Πρόταση 5.11, υπάρχει $a \in \mathbb{Z}$ έτσι, ώστε $a_1 = a \bmod n_1, \ldots, a_k = a \bmod n_k$ και κατά συνέπεια έχουμε $\pi(a) = (a_1, \ldots, a_k)$. Άρα, η απεικόνιση π είναι έφεση. Καθώς οι δύο δακτύλιοι έχουν το ίδιο πλήθος στοιχείων, η απεικόνιση π είναι ένεση. Επομένως, η π είναι ισομορφισμός.

Ο δεύτερος ισομορφισμός προκύπτει αμέσως από την ισομορφία των δακτυλίων $\mathbb{Z}_m$ και $\mathbb{Z}/(m)$. $\square$

Στον παρακάτω αλγόριθμο συνοψίζουμε τη μέθοδο της επίλυσης ενός συστήματος γραμμικών ισοτιμιών που δόθηκε κατά την απόδειξη της Πρότασης 5.11.

Αλγόριθμος 5.2 Επίλυση συστήματος γραμμικών ισοτιμιών.
Είσοδος: Ακέραιοι $n_1, \ldots, n_k \geq 2$, πρώτοι μεταξύ τους ανά δύο και $a_1, \ldots, a_k$ ακέραιοι με $0 \leq a_i < n_i$ $(i = 1, \ldots, k)$.
Έξοδος: Ακέραιος x με $x \equiv a_i \pmod{n_i}$ $(i = 1, \ldots, k)$.

1. Για $i = 1, \ldots, k$ υπολογιζουμε $N_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$ και $y_i = N_i^{-1} \bmod n_i$,
2. Υπολογίζουμε $x_0 = a_1 y_1 N_1 + \cdots + a_k y_k N_k$ και εξάγουμε τον x_0.

Παράδειγμα 5.8 Θα λύσουμε το σύστημα:

$$x \equiv 3 \pmod 5, \quad x \equiv 4 \pmod 7, \quad x \equiv 5 \pmod{11}.$$

Οι ακέραιοι 5, 7, 11 είναι πρώτοι μεταξύ τους ανά δύο και επομένως, σύμφωνα με την Πρόταση 5.11, το σύστημα έχει λύση. Χρησιμοποιώντας τον αλγόριθμο 5.2 θέτουμε $n_1 = 5$, $n_2 = 7$, $n_3 = 11$ και $N_1 = 77$, $N_2 = 55$, $N_3 = 35$ και έχουμε τις γραμμικές ισοτιμίες:

$$77x \equiv 1 \pmod 5, \quad 55x \equiv 1 \pmod 7, \quad 35x \equiv 1 \pmod{11}$$

ή ισοδύναμα:

$$2x \equiv 1 \pmod 5, \quad 6x \equiv 1 \pmod 7, \quad 2x \equiv 1 \pmod{11}.$$

Οι λύσεις τους, αντίστοιχα, είναι:

$$x \equiv 3 \pmod 5, \quad x \equiv 6 \pmod 7, \quad x \equiv 6 \pmod{11}.$$

Επομένως, η λύση του συστήματος είναι:

$$x \equiv 77 \cdot 3 \cdot 3 + 55 \cdot 6 \cdot 4 + 35 \cdot 6 \cdot 5 \equiv 368 \pmod{385}.$$

5.4 Η συνάρτηση ϕ του *Euler*

Ας είναι n θετικός ακέραιος. Συμβολίζουμε με $\phi(n)$ το πλήθος των ακεραίων a με $1 \leq a \leq n$ και $\mu\kappa\delta(a, n) = 1$. Η συνάρτηση

$$\phi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}, \; n \longmapsto \phi(n)$$

κατέχει βασική θέση στη Θεωρία Αριθμών και είναι γνωστή ως συνάρτηση του Euler. Παρατηρούμε αμέσως ότι $|\mathbb{Z}_n^*| = \phi(n)$.

Πρόταση 5.12 *Για κάθε $m, n \in \mathbb{N} \setminus \{0\}$ με $\mu\kappa\delta(m, n) = 1$ ισχύει:*

$$\phi(mn) = \phi(m)\phi(n).$$

Απόδειξη. Σύμφωνα με το Πόρισμα 5.5 έχουμε:

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Έτσι, από το Παράδειγμα 4.24 προκύπτει:

$$(\mathbb{Z}_{mn})^* \cong (\mathbb{Z}_m)^* \times (\mathbb{Z}_n)^*.$$

Άρα, ισχύει: $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*|$, απ' όπου $\phi(mn) = \phi(m)\phi(n)$. □

Πόρισμα 5.6 *Ας είναι $n \in \mathbb{N} \setminus \{0\}$ με πρωτογενή ανάλυση*

$$n = p_1^{a_1} \cdots p_k^{a_k}.$$

Τότε:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Απόδειξη. Για $i = 1, \ldots, k-1$ έχουμε $\mu\kappa\delta(p_i^{a_i}, p_{i+1}^{a_{i+1}} \cdots p_k^{a_k}) = 1$ και επομένως από την Πρόταση 5.12 έπεται:

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2} \cdots p_k^{a_k}) = \ldots = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}).$$

Ας είναι x ακέραιος με $1 \leq x \leq p_i^{a_i}$. Έχουμε $\mu\kappa\delta(x, p_i^{a_i}) > 1$, αν και μόνον αν $p_i | x$, δηλαδή αν και μόνον αν το x είναι στοιχείο του συνόλου $S_i = \{kp_i / \ k = 1, \ldots, p_i^{a_i - 1}\}$. Καθώς $|S_i| = p_i^{a_i - 1}$ παίρνουμε $\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1}$. Έτσι, ισχύει:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right). \quad \square$$

Πόρισμα 5.7 *Ας είναι n ακέραιος > 2. Τότε, ο ακέραιος $\phi(n)$ είναι άρτιος.*

Απόδειξη. Ας είναι $n = 2^m$ και $m \geq 2$. Τότε από το Πόρισμα 5.6 έχουμε $\phi(n) = \phi(2^m) = 2^{m-1}$ και επομένως ο $\phi(n)$ είναι άρτιος. Στη συνέχεια, ας υποθέσουμε ότι $n = p^r A$, όπου p πρώτος > 2, $r > 0$ και A ακέραιος με $\mu\kappa\delta(p, A) = 1$. Τότε, από το Πόρισμα 5.6 έχουμε:

$$\phi(n) = \phi(p^r)\phi(A) = p^{r-1}(p-1)\phi(A).$$

Συνεπώς, ο ακέραιος $\phi(n)$ είναι άρτιος. $\square$

Πρόταση 5.13 *Ας είναι n θετικός ακέραιος. Τότε ισχύει:*

$$\sum_{d|n} \phi(d) = n,$$

όπου d διατρέχει το σύνολο των θετικών διαιρετών του n.

Απόδειξη. Θεωρούμε το σύνολο

$$A = \{0/n, 1/n, \ldots, (n-1)/n\}$$

και για κάθε θετικό διαιρέτη d του n το σύνολο

$$A_d = \{a/d : \ 0 \leq a \leq d, \ \mu\kappa\delta(a,d) = 1\}.$$

Ας είναι $x \in A$. Τότε υπάρχει θετικός διαιρέτης d του n με $x = a/d$, όπου a ακέραιος με $0 \leq a \leq d$ και $\mu\kappa\delta(a,d) = 1$. Άρα $x \in A_d$ και επομένως $A \subseteq \cup_{d|n} A_d$. Από την άλλη πλευρά, για κάθε θετικό διαιρέτη d του n έχουμε $A_d \subseteq A$. Οπότε ισχύει $A = \cup_{d|n} A_d$. Καθώς τα σύνολα A_d είναι ξένα ανά δύο και $|A_d| = \phi(d)$ έχουμε:

$$n = |A| = \sum_{d|n} |A_d| = \sum_{d|n} \phi(d). \quad \square$$

Καθώς έχουμε $|\mathbb{Z}_n^*| = \phi(n)$, το Πορίσμα 4.2 έχει ως άμεση συνέπεια το παρακάτω αποτέλεσμα που είναι γνωστό ως θεώρημα των Fermat-Euler.

Θεώρημα 5.1 *Ας είναι $n, a \in \mathbb{Z}$ με $n > 1$ και $\mu\kappa\delta(a,n) = 1$. Τότε ισχύει:*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Το επόμενο πόρισμα είναι γνωστό ως *Μικρό Θεώρημα του Fermat*.

Πόρισμα 5.8 *Ας είναι p πρώτος και a ακέραιος με $p \not| a$. Τότε ισχύει:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Απόδειξη. Έχουμε $\phi(p) = p - 1$ και $\mu\kappa\delta(a,p) = 1$. Άρα, το Θεώρημα 5.1 δίνει την αποδεικτέα σχέση. $\square$

Πόρισμα 5.9 *Ας είναι p πρώτος και a ακέραιος. Τότε ισχύει:*

$$a^p \equiv a \pmod{p}.$$

Απόδειξη. Αν $p \not| a$, τότε το Πόρισμα 5.8 δίνει $a^{p-1} \equiv 1 \pmod{p}$ και επομένως $a^p \equiv a \pmod{p}$. Αν $p|a$, τότε $a^p \equiv 0 \equiv a \pmod{p}$. $\square$

Παράδειγμα 5.9 Θα δείξουμε ότι κάθε ακέραιος a που είναι πρώτος προς το 561 ικανοποιεί την ισοτιμία

$$a^{560} \equiv 1 \pmod{561}.$$

Έχουμε $561 = 3 \cdot 11 \cdot 17$ και από το Πόρισμα 5.8 ισχύει:

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Καθώς $2|560$, $10|560$ και $16|560$ έχουμε:

$$a^{560} \equiv 1 \pmod{3}, \quad a^{560} \equiv 1 \pmod{11}, \quad a^{560} \equiv 1 \pmod{17}.$$

Άρα $3|a^{560}-1$, $11|a^{560}-1$, $17|a^{560}-1$. Έτσι, καθώς οι ακέραιοι 3, 11, 17 είναι πρώτοι μεταξύ τους ανά δύο, το Πόρισμα 3.3 δίνει $561|a^{560}-1$, απ' όπου παίρνουμε το ζητούμενο. Επιπλέον, ας σημειωθεί ότι ενώ ο ακέραιος 561 δεν είναι πρώτος επαληθεύει την ισοτιμία του Πορίσματος 5.8 που ισχύει για πρώτους αριθμούς.

Πόρισμα 5.10 *Ας είναι p πρώτος. Τότε, μέσα στον δακτύλιο $\mathbb{Z}_p[x]$, ισχύει:*

$$x^{p-1} - 1 = (x-1)\cdots(x-(p-1)).$$

Απόδειξη. Σύμφωνα με το Πόρισμα 5.8, για κάθε ακέραιο a με $p \not| a$ ισχύει $a^{p-1} \equiv 1 \pmod{p}$ και κατά συνέπεια τα στοιχεία του $\mathbb{Z}_p^*$ είναι όλες οι ρίζες του $x^{p-1}-1$ μέσα στο $\mathbb{Z}_p$. Έτσι, από το Πόρισμα 4.7 έχουμε την εξής ισότητα μέσα στο $\mathbb{Z}_p[x]$:

$$x^{p-1} - 1 = (x-1)\cdots(x-(p-1)). \quad \square$$

Τέλος δίνουμε μία ικανή και αναγκαία συνθήκη για να είναι ένας θετικός ακέραιος πρώτος, γνωστή ως *Θεώρημα του Wilson*.

Θεώρημα 5.2 *Ένας ακέραιος $p > 1$ είναι πρώτος αν και μόνον αν ισχύει*

$$(p-1)! \equiv -1 \pmod{p}.$$

Απόδειξη. Από το Πόρισμα 5.10 έχουμε την εξής ισότητα μέσα στο $\mathbb{Z}_p$:

$$x^{p-1} - 1 = (x-1)\cdots(x-(p-1)).$$

Εξισώνοντας τους συντελεστές των σταθερών όρων παίρνουμε:

$$(p-1)! \equiv -1 \pmod{p}.$$

Αντίστροφα, ας υποθέσουμε ότι p είναι ένας θετικός ακέραιος που επαληθεύει αυτή την σχέση. Αν $p = de$, όπου d, e είναι θετικοί ακέραιοι με $1 < d \leq e < p$, τότε $d|(p-1)!$ και $d|p$. Από την παραπάνω ισοτιμία έχουμε $p|(p-1)! + 1$. Συνδυάζοντας αυτές τις σχέσεις παίρνουμε $d|1$ που είναι άτοπο. □

5.5 Τάξη ακεραίου κατά μέτρο n

Ας είναι $a, n \in \mathbb{Z}$ με $n > 1$ και $\mu\kappa\delta(a, n) = 1$. Καλούμε *τάξη του ακεραίου a κατά μέτρο n* την τάξη της κλάσης του a μέσα στην ομάδα $(\mathbb{Z}/(n))^*$. Δηλαδή, η τάξη του a κατά μέτρο n είναι ο μικρότερος θετικός ακέραιος r με $a^r \equiv 1 \pmod{n}$. Γράφουμε $r = \mathrm{ord}_n(a)$. Άμεση συνέπεια του ορισμού είναι ότι για κάθε ακέραιο b με $b \equiv a \pmod{n}$ έχουμε $\mathrm{ord}_n(b) = \mathrm{ord}_n(a)$.

Άμεση συνέπεια της Πρότασης 4.5 και των Πορισμάτων 4.1 και 4.2 είναι οι εξής βασικές ιδιότητες της τάξης ενός ακεραίου τις οποίες δίνουμε στη παρακάτω πρόταση.

Πρόταση 5.14 *Ας είναι $r = \mathrm{ord}_n(a)$. Τότε ισχύουν τα εξής:*
(α) $a^k \equiv a^h \pmod{n} \Leftrightarrow k \equiv h \pmod{r}$.
(β) $a^k \equiv 1 \pmod{n} \Leftrightarrow r|k$.
(γ) Οι ακέραιοι $1, a, \ldots, a^{r-1}$ *είναι ανά δύο ανισότιμοι κατά μέτρο n.*
(δ) $r|\phi(n)$.

Απόδειξη. (α) Άμεση συνέπεια του ορισμού και του Πορίσματος 4.1.

(β) Η (β) προκύπτει αμέσως από την (α) για $h = 0$.

(γ) Οι ακέραιοι $0, 1, \ldots, r-1$ είναι ανά δύο ανισότιμοι κατά μέτρο r. Οπότε, από την (α) παίρνουμε ότι οι $1, a, \ldots, a^{r-1}$ είναι ανισότιμοι κατά μέτρο n.

(δ) Καθώς $|(\mathbb{Z}/(n))^*| = \phi(n)$, το Πόρισμα 4.2 δίνει το αποτέλεσμα. □

Παράδειγμα 5.10 Θα προσδιορίσουμε την τάξη $\mathrm{ord}_{19}(3)$. Καθώς $\mathrm{ord}_{19}(3)|\phi(19)$ και $\phi(19) = 18$, παίρνουμε $\mathrm{ord}_{19}(3) \in \{1, 2, 3, 6, 9, 18\}$. Αμέσως βλέπουμε ότι $\mathrm{ord}_{19}(3) \neq 1, 2$. Υπολογίζουμε τις δυνάμεις:

$$3^3 \equiv 8 \pmod{19}, \quad 3^6 \equiv 7 \pmod{19}, \quad 3^9 \equiv 18 \pmod{19}.$$

Οπότε $\mathrm{ord}_{19}(3) \neq 3, 6, 9$ και κατά συνέπεια $\mathrm{ord}_{19}(3) = 18$.

Ο ακέραιος a καλείται *αρχική ή πρωτογενής ρίζα κατά μέτρο* n αν ισχύει $\mathrm{ord}_n(a) = \phi(n)$. Σύμφωνα με το Παράδειγμα 5.10, ο 3 είναι αρχική ρίζα κατά μέτρο 19. Αν ο a είναι αρχική ρίζα κατά μέτρο n, τότε από την Πρόταση 5.14(γ) έπεται ότι οι ακέραιοι $1, a, \ldots, a^{\phi(n)-1}$ είναι ανά δύο ανισότιμοι κατά μέτρο n και κατά συνέπεια έχουμε:

$$(\mathbb{Z}/(n))^* = \langle [a]_n \rangle = \{[1]_n, [a]_n, \ldots, [a]_n^{\phi(n)-1}\}$$

ή ισοδύναμα:

$$\mathbb{Z}_n^* = \langle a \bmod n \rangle = \{1, a \bmod n, a^2 \bmod n, \ldots, a^{\phi(n)-1} \bmod n\}.$$

Αντίστροφα, αν ισχύει η παραπάνω ισότητα, τότε ο a είναι αρχική ρίζα κατά μέτρο n.

Πρόταση 5.15 *Ας είναι K ένα σώμα. Αν G είναι μία πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας $K \setminus \{0\}$, τότε η ομάδα G είναι κυκλική και έχει ακριβώς $\phi(n)$ γεννήτορες.*

Απόδειξη. Ας είναι $|G| = n \geq 3$. Συμβολίζουμε με $\psi(d)$ το πλήθος των στοιχείων της G που έχουν τάξη ίση με d. Από το Πόρισμα 4.2 έχουμε $d|n$. Έτσι, ισχύει:

$$n = \sum_{d|n} \psi(d),$$

όπου d διατρέχει το σύνολο των θετικών διαιρετών του n.

Αν η G δεν περιέχει κανένα στοιχείο τάξης d, τότε $\psi(d) = 0$. Αν η G περιέχει ένα τέτοιο στοιχείο, τότε αυτό παράγει μία κυκλική υποομάδα H της G τάξης d. Τα στοιχεία της H είναι ρίζες του πολυωνύμου $x^d - 1$. Σύμφωνα με το Πόρισμα 4.7 το $x^d - 1$ έχει το πολύ d ρίζες και επομένως το σύνολο των ριζών του είναι η ομάδα H. Αν a είναι ένα στοιχείο της G με τάξη d, τότε $a^d = 1$ και επομένως $a \in H$. Άρα η H περιέχει όλα τα στοιχεία τάξης d της G. Αυτά παράγουν την H και επομένως από το Πόρισμα 4.3 προκύπτει ότι $\psi(d) = \phi(d)$. Έτσι, έχουμε $\psi(d) = 0$ ή $\phi(d)$.

Από την άλλη πλευρά, σύμφωνα με την Πρόταση 5.13 ισχύει:

$$n = \sum_{d|n} \phi(d),$$

όπου d διατρέχει το σύνολο των θετικών διαιρετών του n. Έτσι, έχουμε:

$$\sum_{d|n} \psi(d) = n = \sum_{d|n} \phi(d).$$

Άρα, $\psi(d) = \phi(d)$, για κάθε θετικό διαιρέτη του d. Ειδικότερα, έχουμε $\psi(n) = \phi(n) \geq 1$ και επομένως η ομάδα G είναι κυκλική με $\phi(n)$ γεννήτορες. □

Πόρισμα 5.11 *Ας είναι p πρώτος. Τότε υπάρχουν $\phi(p-1)$ στοιχεία του $\mathbb{Z}_p^*$ που είναι αρχικές ρίζες κατά μέτρο p.*

Ας σημειωθεί ότι, για πολύ μεγάλους πρώτους p, δεν υπάρχει αποτελεσματική μέθοδος για τον υπολογισμό των αρχικών ριζών. Απο την άλλη πλευρά, αν g_p είναι η μικρότερη αρχική ρίζα κατά μέτρο p, τότε $g_p < p^{1/4+o(1)}$, όπου $o(1)$ είναι μία συνάρτηση που τείνει στο 0 για $p \to \infty$ [4]. Στη περίπτωση όπου είναι δυνατόν να υπολογιστεί η παραγοντοποίηση του $p-1$, ένας αλγόριθμος για την εύρεση μίας πρωτογενούς ριζας κατά μέτρο p δίνεται παρακάτω.

Αλγόριθμος 5.3 Εύρεση μίας πρωτογενούς ριζας κατά μέτρο p.
Είσοδος: Ένας πρώτος αριθμός $p > 2$.
Έξοδος: Μία πρωτογενής ρίζα κατά μέτρο p.

1. Υπολογίζουμε την πρωτογενή ανάλυση του $p-1$,
$$p - 1 = q_1^{a_1} \cdots q_k^{a_k}.$$
2. Επιλέγουμε τυχαία $a \in \{2, \ldots, p-2\}$ και για κάθε $i = 1, \ldots, k$ υπολογίζουμε
$$a^{(p-1)/q_i} \mod p.$$
3. Αν για κάθε $i = 1, \ldots, k$ έχουμε
$$a^{(p-1)/q_i} \mod p \neq 1,$$
τότε εξάγουμε τον a. Αν όχι επιλέγουμε άλλο a και επαναλαμβάνουμε τη διαδικασία.

Παρατηρούμε ότι $\mathrm{ord}_p(a) = p-1$ αν και μόνον αν για κάθε $i = 1, \ldots, k$ ισχύει $a^{(p-1)/q_i} \not\equiv 1 \,(\mathrm{mod}\, p)$ $(i = 1, \ldots, k)$. Έτσι, ο a είναι πρωτογενής ρίζα κατά μέτρο p αν και μόνον αν $a^{(p-1)/q_i} \not\equiv 1 \,(\mathrm{mod}\, p)$ $(i = 1, \ldots, k)$.

Παράδειγμα 5.11 Θα χρησιμοποιήσουμε τον παραπάνω αλγόριθμο για να βρούμε μία πρωτογενή ριζα κατά μέτρο 1129. Πρώτα υπολογίζουμε την πρωτογενή ανάλυση του 1128 και βρίσκουμε:

$$1128 = 2^3 \cdot 3 \cdot 47.$$

Επιλέγουμε τον 3 και υπολογίζουμε τις δυνάμεις $3^{1028/2}$, $3^{1028/3}$ και $3^{1028/47}$ κατά μέτρο 1029. Καθώς βρίσκουμε

$$3^{1028/2} \mod 1029 = 1,$$

επιλέγουμε άλλον ακέραιο. Για τον 11 έχουμε:

$$11^{1028/2} \mod 1029 = 1128, \quad 11^{1028/3} \mod 1029 = 387$$

και

$$11^{1028/47} \mod 1029 = 338.$$

Επομένως, ο 11 είναι μία πρωτογενής ρίζα κατά μέτρο 1129.

Πρόταση 5.16 *Ας είναι p πρώτος > 2 και r ακέραιος ≥ 1. Τότε υπάρχουν πρωτογενείς ρίζες κατά μέτρο p^r και $2p^r$.*

Για την απόδειξη της πρότασης θα χρησιμοποιήσουμε το εξής λήμμα:

Λήμμα 5.1 *Ας είναι a μία πρωτογενή ρίζα κατά μέτρο p. Τότε υπάρχει ακέραιος x τέτοιος, ώστε για τον ακέραιο $b = a + px$ να ισχύει:*

$$b^{p^{j-1}(p-1)} = 1 + p^j z_j \quad (j = 0, 1, \ldots),$$

όπου z_j ακέραιος με $p \not| z_j$.

Απόδειξη. Θέτουμε $b = a + px$, όπου $x \in \mathbb{Z}$. Καθώς ισχύει $a^{p-1} \equiv 1 \pmod{p}$, υπάρχει ακέραιος y με $a^{p-1} = 1 + py$. Οπότε προκύπτει:

$$b^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} a^k (px)^{p-k} = 1 + py + \sum_{k=0}^{p-2} \binom{p-1}{k} a^k (px)^{p-1-k}.$$

Επομένως, $b^{p-1} = 1 + pz_1$, όπου z_1 ακέραιος με

$$z_1 \equiv y + (p-1)a^{p-2}x \pmod{p}.$$

Ο ακέραιος $(p-1)a^{p-2}$ δεν διαιρείται από τον p και έτσι μπορούμε να επιλέξουμε τον x έτσι, ώστε $p \not| z_1$. Συνεπώς, η προς απόδειξη σχέση για $j=1$ ισχύει. Ας υποθέσουμε ότι αληθεύει για $j=m>1$. Δηλαδή, έχουμε:

$$b^{p^{m-1}(p-1)} = 1 + p^m z_m,$$

όπου z_m ακέραιος με $p \not| z_m$. Επομένως, ισχύει:

$$b^{p^m(p-1)} = (1+p^m z_m)^p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) (p^m z_m)^k = 1 + p^{m+1} z_{m+1},$$

όπου

$$z_{m+1} = z_m + \sum_{k=2}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) z_m^k p^{m(k-1)-1}.$$

Καθώς $p \not| z_m$ και κάθε άλλος όρος του παραπάνω αθροίσματος διαιρείται από τον p, παίρνουμε ότι $p \not| z_{m+1}$. Επομένως, η προς απόδειξη σχέση ισχύει για $j=m+1$ και κατά συνεπεια ισχύει για κάθε θετικό ακέραιο j. □

Απόδειξη της Πρότασης 5.16. Σύμφωνα με το Πόρισμα 5.11 υπάρχει μία πρωτογενής ρίζα a κατά μέτρο p. Από το Λήμμα 5.1 έχουμε ότι υπάρχει $x \in \mathbb{Z}$ έτσι, ώστε για τον $b = a + px$ να ισχύει:

$$b^{p^{j-1}(p-1)} = 1 + p^j z_j \quad (j = 0, 1, \ldots),$$

όπου z_j ακέραιος με $p \not| z_j$. Καθώς $b \equiv a \pmod p$, ο b είναι μία πρωτογενής ρίζα κατά μέτρο p. Ας είναι $d = \mathrm{ord}_{p^r}(b)$. Τότε $d|\phi(p^r)$. Από την άλλη πλευρά, έχουμε $b^d \equiv 1 \pmod p$ και επομένως $d = (p-1)c$, όπου c ακέραιος. Έτσι, έχουμε $(p-1)c|(p-1)p^{r-1}$ και κατά συνέπεια $c = p^s$, όπου $0 \leq s \leq r-1$. Άρα $d = (p-1)p^s$. Επομένως, υπάρχει $z \in \mathbb{Z}$ με

$$b^{p^s(p-1)} = 1 + zp^r.$$

Έτσι προκύπτει $p^{s+1} z_{s+1} = zp^r$. Αν $s < r-1$, τότε έχουμε $p|z_{s+1}$ που είναι άτοπο. Άρα $s = r-1$ και επομένως $d = \phi(p^r)$, δηλαδή ο b είναι μία πρωτογενής ρίζα κατά μέτρο p^r.

Στη συνέχεια θα αποδείξουμε την ύπαρξη των πρωτογενών ριζών κατά μέτρο $2p^r$. Ας είναι b μία πρωτογενής ρίζα κατά μέτρο p^r. Τότε ο ακέραιος $b + p^r$ είναι επίσης μία πρωτογενής ρίζα κατά μέτρο p^r. Ένας από τους b, $b + p^r$ είναι περιττός και τον συμβολίζουμε με g. Έχουμε

$\mu\kappa\delta(g, 2p^r) = 1$. Αν $d = \mathrm{ord}_{2p^r}(b)$, τότε $d|\phi(2p^r)$. Καθώς $\phi(2p^r) = \phi(p^r)$, έχουμε $d|\phi(p^r)$. Από την άλλη πλευρά, έχουμε $g^d \equiv 1 \,(\mathrm{mod}\ p^r)$ και επομένως $\phi(p^r)|d$. Άρα, ισχύει $d = \phi(p^r) = \phi(2p^r)$ και κατά συνέπεια ο g είναι μία πρωτογενής ρίζα κατά μέτρο $2p^r$. □

Πρόταση 5.17 *Ας είναι n ακέραιος > 5 ο οποίος δεν είναι της μορφής p^r ή $2p^r$, όπου p πρώτος > 2 και $r > 0$. Τότε δεν υπάρχουν πρωτογενείς ρίζες κατά μέτρο n.*

Απόδειξη. Ας υποθέσουμε πρώτα ότι $n = 2^m$, όπου $m \geq 3$. Θα δείξουμε ότι για κάθε περιττό ακέραιο a ισχύει:

$$a^{\phi(n)/2} \equiv 1 \,(\mathrm{mod}\, n).$$

Εύκολα επαληθεύουμε ότι $a^2 \equiv 1 \,(\mathrm{mod}\, 8)$. Καθώς $\phi(8) = 4$, βλέπουμε ότι η προς απόδειξη ισοτιμία ισχύει για $m = 3$. Ας υποθέσουμε ότι ισχύει για $m = k > 3$. Τότε υπάρχει ακέραιος t με

$$a^{\phi(2^k)/2} = 1 + 2^k t.$$

Οπότε, έχουμε

$$a^{\phi(2^k)} = (1 + 2^k t)^2 = 1 + 2^{k+1}t + (2^k t)^2 \equiv 1 \,(\mathrm{mod}\, 2^{k+1}).$$

Καθώς $\phi(2^{k+1})/2 = 2^{k-1} = \phi(2^k)$, η ισοτιμία ισχύει και για $m = k+1$. Συνεπώς, η προς απόδειξη ισοτιμία ισχύει για κάθε $m \geq 3$. Άρα δεν υπάρχουν πρωτογενείς ρίζες κατά μέτρο 2^m, όπου $m \geq 3$.

Ας υποθέσουμε τώρα ότι $n = rs$, όπου r, s ακέραιοι > 2 με $\mu\kappa\delta(r, s) = 1$. Θα δείξουμε ότι για κάθε ακέραιο a με $\mu\kappa\delta(a, n) = 1$ ισχύει:

$$a^{\phi(n)/2} \equiv 1 \,(\mathrm{mod}\, n).$$

Επειδή $\mu\kappa\delta(r, s) = 1$ έχουμε ότι $\phi(n) = \phi(r)\phi(s)$. Επίσης, καθώς $r > 2$, $s > 2$, το Πόρισμα 5.7 έπεται ότι οι $\phi(r)$, $\phi(s)$ είναι άρτιοι. Οπότε ισχύει:

$$a^{\phi(n)/2} \equiv (a^{\phi(r)})^{\phi(s)/2} \equiv 1 \,(\mathrm{mod}\, r),$$

απ' όπου $r|a^{\phi(n)/2} - 1$. Όμοια προκύπτει $s|a^{\phi(n)/2} - 1$. Καθώς ισχύει $\mu\kappa\delta(r, s) = 1$, έχουμε $n|a^{\phi(n)/2} - 1$ και επομένως η προς απόδειξη ισοτιμία αληθεύει. Συνεπώς, δεν υπάρχουν πρωτογενείς ρίζες κατά μέτρο $n = rs$, όπου r, s ακέραιοι > 2 με $\mu\kappa\delta(r, s) = 1$. □

Πρόταση 5.18 *Ας είναι n ακέραιος > 1 και $a \in \mathbb{Z}_n^*$ μία αρχική ρίζα κατά μέτρο n. Τότε υπάρχουν ακριβώς $\phi(\phi(n))$ διακεκριμμένες αρχικες ρίζες κατά μέτρο n μέσα στο $\mathbb{Z}_n^*$. Ένα τέτοιο σύστημα αρχικών ριζών δίνεται από τους ακέραιους $a^k \bmod n$, όπου $1 \leq k \leq \phi(n)$ και $\mu\kappa\delta(k, \phi(n)) = 1$.*

Απόδειξη. Ας είναι k ακέραιος με $1 \leq k \leq \phi(n)$ και $\mu\kappa\delta(k, \phi(n)) = 1$. Τότε από το Πόρισμα 4.3 έχουμε $\mathrm{ord}_n(a^k) = \phi(n)$ και επομένως οι ακέραιοι a^k, όπου $1 \leq k \leq \phi(n)$ και $\mu\kappa\delta(k, \phi(n)) = 1$, είναι αρχικες ρίζες κατά μέτρο n. Επίσης, από την Πρόταση 5.14 έπεται ότι οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μέτρο n.

Αντίστροφα, ας είναι $g \in \mathbb{Z}_n^*$ μία αρχική ρίζα κατά μέτρο n. Τότε υπάρχει $k \in \{1, \ldots, \phi(n)\}$ με $g \equiv a^k \bmod n$. Οπότε, ισχύει $\mathrm{ord}_n(a^k) = \phi(n)$. Έτσι, από την Πρόταση 4.7, έχουμε $\mu\kappa\delta(k, \phi(n)) = 1$. Τέλος, το πλήθος των ακεραίων $1 \leq k \leq \phi(n)$ με $\mu\kappa\delta(k, \phi(n)) = 1$ είναι $\phi(\phi(n))$. □

Συνοψίζουμε τα παραπάνω συμπεράσματα για τις πρωτογενείς ρίζες στο εξής θεώρημα:

Θεώρημα 5.3 *Ας είναι n ακέραιος > 1. Τότε υπάρχουν αρχικές ρίζες κατά μέτρο n αν και μόνον αν $n = 2, 4, p^r, 2p^r$, όπου p πρώτος > 2 και $r > 0$. Το πλήθος των αρχικών ριζών κατά μέτρο n μέσα στο $\mathbb{Z}_n^*$ είναι $\phi(\phi(n))$. Αν $a \in \mathbb{Z}_n^*$ είναι μία αρχική ρίζα κατά μέτρο n, τότε ένα τέτοιο σύστημα αρχικών ριζών δίνεται από τους ακέραιους $a^k \bmod n$, όπου $1 \leq k \leq \phi(n)$ και $\mu\kappa\delta(k, \phi(n)) = 1$.*

Παράδειγμα 5.12 Θα προσδιορίσουμε τις πρωτογενείς ρίζες κατά μετρο 34. Έχουμε $34 = 2 \cdot 17$ και $\phi(34) = 16$. Επομένως, σύμφωνα με το Θεώρημα 5.4, υπάρχουν $\phi(\phi(34)) = 8$ πρωτογενείς ρίζες κατά μέτρο 34 μέσα στο $\mathbb{Z}_{34}^*$. Θα βρούμε την τάξη του 3 κατά μέτρο 34. Καθώς $\mathrm{ord}_{34}(3) \in \{1, 2, 4, 8, 16\}$ και $3^i \not\equiv 1 \,(\mathrm{mod}\, 34)$ $(i = 1, 2, 3)$, υπολογίζουμε $3^4 \equiv 13 \,(\mathrm{mod}\, 34)$ και $3^8 \equiv 13^2 \equiv -1 \,(\mathrm{mod}\, 34)$. Άρα $\mathrm{ord}_{34}(3) = 16$ και επομένως ο 3 είναι μία πρωτογενής ρίζα κατά μέτρο 34. Οι άλλες πρωτογενείς ρίζες μέσα στο $\mathbb{Z}_{34}^*$ είναι οι $3^i \bmod 34$ $(i = 3, 5, 7, 9, 11, 13, 15)$, δηλαδή οι ακέραιοι 5, 7, 11, 23, 27, 29 και 31.

5.6 Υπόλοιπα m-οστής δύναμης

Ας είναι n, m ακέραιοι με > 1 και a ακέραιος με $\mu\kappa\delta(a, n) = 1$. Ο a καλείται *υπόλοιπο m-οστής δύναμης κατά μέτρο n* αν η πολυωνυμική ισοτιμία

$$x^m \equiv a \pmod{n}$$

έχει λύση. Ισοδύναμα, ένα υπόλοιπο m-οστής δύναμης κατά μέτρο n είναι ένας ακέραιος του οποίου η κλάση μέσα στον δακτύλιο $\mathbb{Z}/(n)$ είναι η m-οστή δύναμη ενός στοιχείου. Για κάθε m ο 1 είναι υπόλοιπο m-οστής δύναμης κατά μέτρο n, γιατί η ισοτιμία $x^m \equiv 1 \pmod{n}$ έχει πάντα λύση. Προφανώς, αν ο a είναι υπόλοιπο m-οστής δύναμης κατά μέτρο n και $b \equiv a \pmod{n}$, τότε και ο b είναι υπόλοιπο m-οστής δύναμης κατά μέτρο n. Αν $m = 2$, τότε το υπόλοιπο δεύτερης δύναμης καλείται και *τετραγωνικό*. Σ' αυτή την ενότητα θ' ασχοληθούμε κυρίως με τα τετραγωνικά υπόλοιπα.

Παράδειγμα 5.13 Θα προσδιορίσουμε τα τετραγωνικά υπόλοιπα του $\mathbb{Z}_{14}$. Έχουμε

$$5^2 \equiv 9^2 \equiv 11 \pmod{14}$$

και επομένως όλα τα τετραγωνικά υπόλοιπα του $\mathbb{Z}_{14}$ είναι οι αριθμοί 1, 9, 11.

Πρόταση 5.19 *Ας είναι $a \in \mathbb{Z}$ με $\mu\kappa\delta(a, n) = 1$. Αν ο a είναι υπόλοιπο m-οστής δύναμης κατά μέτρο n, τότε οι πολυωνυμικές ισοτιμίες*

$$x^m \equiv a \pmod{n} \quad \text{και} \quad x^m \equiv 1 \pmod{n}$$

έχουν το ίδιο πλήθος λύσεων.

Απόδειξη. Ας είναι $u_1, \ldots, u_k$ οι ακέραιοι του $\mathbb{Z}_n$ που αντιπροσωπεύουν τις λύσεις της $x^m \equiv 1 \pmod{n}$. Ο a είναι υπόλοιπο m-οστής δύναμης κατά μέτρο n και επομένως υπάρχει $y \in \mathbb{Z}_n$ με $a = y^m \bmod n$. Καθώς $\mu\kappa\delta(y, n) = 1$, οι ακέραιοι $yu_1 \bmod n, \ldots, yu_k \bmod n$ είναι διακεκριμμένοι και επαληθεύουν την ισοτιμία $x^m \equiv a \pmod{n}$. Ας είναι $z \in \mathbb{Z}_n$ ένας ακέραιος με $y \neq z$ που επαληθεύει αυτή την ισοτιμία. Τότε:

$$y^m \equiv a \equiv z^m \pmod{n}.$$

Αν $y' = y^{-1} \pmod n$, τότε ο ακέραιος $u = zy' \bmod n$ επαληθεύει την $x^m \equiv 1 \pmod n$. Άρα, υπάρχει $j \in \{1, \ldots, k\}$ με $u = u_j$ και επομένως έχουμε:

$$z = yu \bmod n = yu_j \bmod n.$$

Έτσι, όλες οι λύσεις της $x^m \equiv a \pmod n$ μέσα στο $\mathbb{Z}_n$ είναι οι ακέραιοι $yu_1 \bmod n, \ldots, yu_k \bmod n$ και επομένως το πλήθος των λύσεών της είναι το ίδιο μ' αυτό της $x^m \equiv 1 \pmod n$. □

Πρόταση 5.20 *Ας είναι $n = 2, 4, p^r, 2p^r$, όπου p πρώτος > 2 και r ακέραιος ≥ 1, και a ακέραιος με $\mu\kappa\delta(a, n) = 1$. Θέτουμε $d = \mu\kappa\delta(m, \phi(n))$. Τότε ο a είναι υπόλοιπο m-οστής δύναμης κατά μέτρο n αν και μόνον αν ισχύει*

$$a^{\phi(n)/d} \equiv 1 \pmod n.$$

Σ' αυτή την περίπτωση, το πλήθος των υπολοίπων m-οστής δύναμης κατά μέτρο n μέσα στο $\mathbb{Z}_n^*$ είναι $\phi(n)/d$ και καθένα από αυτά είναι η m-οστή δύναμη ακριβώς d ακεραίων του $\mathbb{Z}_n^*$.

Απόδειξη. Σύμφωνα με το Θεώρημα 5.4 υπάρχει μία αρχική ρίζα $g \in \mathbb{Z}_n^*$ κατά μέτρο n. Θεωρούμε την πολυωνυμική ισοτιμία

$$x^m \equiv a \pmod n.$$

Καθώς κάθε στοιχείο του $\mathbb{Z}_n^*$ γράφεται ως δύναμη του g, υπάρχουν $w, b \in \{0, \ldots, \phi(n) - 1\}$ με $x = g^w \bmod n$ και $a = g^b \bmod n$. Έτσι, έχουμε:

$$g^{mw} \equiv g^b \pmod n.$$

Η ισοτιμία αυτή, σύμφωνα με την Πρόταση 5.14, είναι ισοδύναμη με τη γραμμική ισοτιμία

$$mw \equiv b \pmod{\phi(n)}.$$

Η ισοτιμία αυτή έχει λύση, αν και μόνον αν $d|b$ που ισοδυναμεί με

$$\frac{\phi(n)}{d} b \equiv 0 \pmod{\phi(n)}.$$

Αυτή η ισοτιμία ισχύει, αν και μόνον αν

$$a^{\phi(n)/d} \equiv 1 \pmod n.$$

Ας είναι $k \in \{1, \ldots, \phi(n)\}$. Έχουμε:

$$g^{k\phi(n)/d} \equiv 1 \pmod{n}$$

αν και μόνον αν $\phi(n)|k\phi(n)/d$ που ισοδυναμεί με $d|k$. Οπότε, οι ακέραιοι $g^d \mod n$, $g^{2d} \mod n, \ldots, g^{(\phi(n)/d)d} \mod n$ είναι όλα τα διαφορετικά στοιχεία του $\mathbb{Z}_n^*$ που είναι υπόλοιπα m-οστής δύναμης κατά μέτρο n. Τέλος, από την Πρόταση 5.20 έπεται ότι οι πολυωνυμικές ισοτιμίες

$$x^m \equiv g^{k\phi(n)/d} \pmod{n} \quad (k = 1, \ldots, \phi(n)/d)$$

έχουν όλες το ίδιο πλήθος λύσεων που είναι d. □

Πόρισμα 5.12 *Ας είναι p πρώτος > 2 και g μία αρχική ρίζα κατά μέτρο p. Τότε ο g δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο p και ισχύει*

$$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

Απόδειξη. Καθώς ο g είναι μία αρχική ρίζα κατά μέτρο p έχουμε $\mathrm{ord}_n(g) = p - 1$ και κατά συνέπεια ισχύει:

$$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

Έτσι, από την Πρόταση 5.20 παίρνουμε ότι ο g δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο p. □

Πόρισμα 5.13 *Ας είναι p πρώτος > 2 και g μία αρχική ρίζα κατά μέτρο p. Τα τετραγωνικά υπόλοιπα κατά μέτρο p είναι μόνο οι ακέραιοι των οποίων οι κλάσεις μέσα στο $\mathbb{Z}/(p)$ είναι οι άρτιες δυνάμεις της $[g]_p$.*

Απόδειξη. Η τετραγωνική ισοτιμία $x^2 \equiv g^{2k} \pmod{p}$ έχει τις λύσεις $x \equiv \pm g^k \pmod{p}$. Αν υπάρχει ακέραιος z τέτοιος, ώστε $z^2 \equiv g^{2k+1} \pmod{p}$, τότε $g \equiv a^2 \pmod{p}$, όπου $a = z(g^k)^{-1} \mod p$, και επομένως ο g είναι τετραγωνικό υπόλοιπο κατά μέτρο p. Αυτό όμως δεν συμβαίνει σύμφωνα με το Πόρισμα 5.12. Άρα, οι ακέραιοι των οποίων οι κλάσεις είναι οι περιττές δυνάμεις της $[g]_p$ δεν είναι τετραγωνικά υπόλοιπα κατά μέτρο p. □

Πόρισμα 5.14 *Ας είναι t και n ακέραιοι > 1, ο n περιττός και $n = p_1^{h_1} \cdots p_k^{h_k}$ η πρωτογενής ανάλυση του n. Θέτουμε $d_i = \mu\kappa\delta(t, \phi(p_i^{h_i}))$*

$(i = 1, \ldots, k)$. *Αν ο ακέραιος* n *είναι* t*-οστό υπόλοιπο κατά μέτρο* n*, τότε το πλήθος των λύσεων της πολυωνυμικής ισοτιμίας*

$$x^t \equiv a \pmod{n}$$

ισούται με $d_1 \cdots d_k$.

Απόδειξη. Από την Πρόταση 5.20 έπεται ότι το πλήθος των λύσεων της πολυωνυμικής ισοτιμίας

$$x^t \equiv a \pmod{p_i^{h_i}} \quad (i = 1, \ldots, k)$$

ισούται με d_i. Έτσι, χρησιμοποιώντας την Πρόταση 5.11 παίρνουμε το ζητούμενο. □

5.6.1 Το σύμβολο του *Legendre*

Συμβολίζουμε με T_p το σύνολο των τετραγωνικών υπολοίπων κατά μέτρο p. Στη συνέχεια ορίζουμε το *σύμβολο του Legendre* ως εξής:

$$(a/p) = \begin{cases} 0, & \text{αν} \quad p|a, \\ 1, & \text{αν} \quad a \in T_p, \\ -1, & \text{αν} \quad a \notin T_p. \end{cases}$$

Από τον ορισμό του συμβόλου του Legendre προκύπτει αμέσως ότι αν $a \equiv b \pmod{p}$, τότε ισχύει $(a/p) = (b/p)$. Επίσης, για κάθε ακέραιο a έχουμε $(a^2/p) = 1$.

Πρόταση 5.21 *Ας είναι* a*,* b *ακέραιοι. Τότε ισχύουν τα εξής:*
(α) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.
(β) $(ab/p) = (a/p)(b/p)$.

Απόδειξη. (α) Ας είναι g αρχική ρίζα κατά μέτρο p. Τότε υπάρχει θετικός ακέραιος k με $a \equiv g^k \pmod{p}$ και επομένως από την Πρόταση 5.19 έχουμε:

$$a^{(p-1)/2} \equiv g^{k(p-1)/2} \equiv (-1)^k \pmod{p}.$$

Από την άλλη πλευρά, η Πρόταση 5.20 συνεπάγεται ότι $(a/p) = 1$ αν και μόνον αν ο k είναι άρτιος. Τότε ισχύει:

$$(a/p) \equiv a^{(p-1)/2} \pmod{p}.$$

(β) Έχουμε:

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}. \quad \square$$

Πόρισμα 5.15 *Ισχύει:*

$$(-1/p) = \begin{cases} 1, & \alpha\nu \quad p \equiv 1 \pmod 4, \\ -1, & \alpha\nu \quad p \equiv 3 \pmod 4. \end{cases}$$

Παράδειγμα 5.14 Θα υπολογίσουμε το σύμβολο $(-28/11)$. Έχουμε:

$$(-28/11) = (-4/11)(7/11) = (-1/11)(7/11) = -(-1) = 1.$$

Θεώρημα 5.4 *Ας είναι a ακέραιος ο οποίος δεν διαιρείται από τον p και $a_j = ja \mod p$ $(j = 1, \ldots, (p-1)/2)$. Αν n είναι το πλήθος των δεικτών j με $a_j > p/2$, τότε:*

$$(a/p) = (-1)^n$$

και

$$n \equiv (a-1)\frac{p^2-1}{8} + \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor \pmod 2.$$

Απόδειξη. Αν $a_k = a_l$ με $k \neq l$, τότε $ka = la \pmod p$ και επομένως $k = l$ που είναι άτοπο. Άρα, οι ακέραιοι a_j $(j = 1, \ldots, (p-1)/2)$ είναι διαφορετικοί ανά δύο. Συμβολίζουμε με $r_1, \ldots, r_n$ και $s_1, \ldots, s_m$ τους ακέραιους μεταξύ αυτών που είναι $> p/2$ και $< p/2$, αντίστοιχα. Ας υποθέσουμε ότι υπάρχουν δείκτες i και j έτσι, ώστε $p - r_i = s_j$. Από την άλλη πλευρά, έχουμε $r_i = ua \mod p$ και $s_j = va \mod p$ με $u, v \in \{1, \ldots, (p-1)/2)\}$. Τότε, ισχύει $(u+v)a \equiv 0 \pmod p$ και επομένως $p|(u+v)a$. Καθώς $p \not| a$, έχουμε $p|u+v$ με $1 \leq u+v \leq p-1$ που είναι άτοπο. Συνεπώς, $p - r_i \neq s_j$ για κάθε ζεύγος i, j. Έτσι, οι θετικοί $p - r_1, \ldots, p - r_n, s_1, \ldots, s_m$ είναι διαφορετικοί ανά δύο και $< p/2$. Άρα οι αριθμοί αυτοί είναι οι $1, \ldots, (p-1)/2$. Τότε έχουμε:

$$\left(\frac{p-1}{2}\right)! \equiv r_1 \cdots r_n s_1 \cdots s_m \equiv (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p,$$

απ΄ όπου προκύπτει:

$$a^{(p-1)/2} \equiv (-1)^n \pmod p.$$

Τέλος, από την Πρόταση 5.21 παίρνουμε $(a/p) = (-1)^n$.

Έχουμε:

$$ja = \left\lfloor \frac{ja}{p} \right\rfloor p + \alpha_j, \quad 0 \le \alpha_j < p \quad (j = 1, \ldots, (p-1)/2)).$$

Έτσι, παίρνουμε:

$$\sum_{j=0}^{(p-1)/2} ja = p \sum_{j=0}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j.$$

Καθώς $\{1, \ldots, (p-1)/2\} = \{p - r_1, \ldots, p - r_n, s_1, \ldots, s_m\}$, έχουμε:

$$\sum_{j=0}^{(p-1)/2} j \equiv \sum_{j=1}^{n} (p - r_j) + \sum_{j=1}^{m} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j.$$

Αφαιρώντας τις δύο παραπάνω ισότητες προκύπτει:

$$(a-1) \sum_{j=0}^{(p-1)/2} j = p \left(\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor - n \right) + 2 \sum_{j=1}^{n} r_j.$$

Έτσι, έχουμε:

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2,$$

απ΄ όπου το αποτέλεσμα. □

Πόρισμα 5.16 *Έχουμε:*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

Ειδικότερα, ισχύει:

$$(2/p) = \begin{cases} 1, & \text{αν} \quad p \equiv \pm 1 \pmod 8, \\ -1, & \text{αν} \quad p \equiv \pm 3 \pmod 8. \end{cases}$$

Απόδειξη. Για κάθε $j = 1, \ldots, (p-1)/2$ ισχύει $\lfloor 2j/p \rfloor = 0$ και επομένως το Θεώρημα 5.4 δίνει:

$$(2/p) = (-1)^{(p^2-1)/8}.$$

Επίσης, ο ακέραιος $(p^2-1)/8$ είναι άρτιος αν $p \equiv \pm 1 \pmod 8$ και περιττός αν $p \equiv \pm 3 \pmod 8$. $\square$

Το παρακάτω θεώρημα είναι γνωστό ως *νόμος της τετραγωνικής αμοιβαιότητας*. Διατυπώθηκε στα 1783 από τον Euler και αποδείχθηκε στα 1796 από τον Gauss.

Θεώρημα 5.5 *Ας είναι p και q δύο διαφορετικοί περιττοί πρώτοι. Τότε ισχύει:*

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

Απόδειξη. Θεωρούμε το σύνολο

$$D = \{(x,y) \in \mathbb{Z}^2 / \ 1 \le x \le (p-1)/2, \ 1 \le y \le (q-1)/2\}.$$

Αν $(x,y) \in D$ με $qx = py$, τότε $q|y$ που είναι άτοπο, καθώς ισχύει $1 \le y \le (q-1)/2$. Άρα για καθε $(x,y) \in D$ έχουμε $qx \neq py$. Συμβολίζουμε με D_1 το σύνολο που περιέχει τα ζεύγη $(x,y) \in D$ με $qx > py$ και με D_2 το σύνολο που περιέχει τα ζεύγη $(x,y) \in D$ με $qx < py$. Έτσι, έχουμε $(x,y) \in D_1$ αν και μόνον αν $1 \le x \le (p-1)/2$ και $1 \le y \le \lfloor qx/p \rfloor$. Επομένως, ισχύει:

$$|D_1| = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor.$$

Όμοια παίρνουμε:

$$|D_2| = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor.$$

Επομένως, έχουμε:

$$\frac{(p-1)(q-1)}{4} = |D| = |D_1| + |D_2| = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor.$$

Έτσι, χρησιμοποιώντας το Θεώρημα 5.4 παίρνουμε το αποτέλεσμα. $\square$

Παράδειγμα 5.15 Θα εξετάσουμε αν η πολυωνυμική ισοτιμία

$$x^2 + 5x + 16 \equiv 0 \pmod{19}$$

έχει λύση. Έχουμε $2^{-1} \mod 19 = 10$ και επομένως $5 \cdot 2^{-1} \mod 19 = 12$. Άρα, η ισοτιμία παίρνει τη μορφή:

$$(x + 12)^2 \equiv 14 \pmod{19}.$$

Έχουμε:

$$(14/19) = (2/19)(7/19) = -(7/19) = -(-1)(19/7) = (5/7) = -1.$$

Επομένως, το 14 δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο 19 και κατά συνέπεια η ισοτιμία δεν έχει λύση.

5.6.2 Το σύμβολο του *Jacobi*

Σ′ αυτή την ενότητα θα γενικεύσουμε το σύμβολο του Legendre. Ας είναι a ακέραιος και n θετικός περιττός ακέραιος > 1 με πρωτογενή ανάλυση

$$n = p_1^{a_1} \cdots p_k^{a_k}.$$

Ορίζουμε το *σύμβολο του Jacobi* κατά μέτρο n ως εξής:

$$(a/n) = (a/p_1)^{a_1} \cdots (a/p_k)^{a_k},$$

όπου (a/p_i) είναι το σύμβολο του Legendre. Αν ο n είναι πρώτος, τότε το σύμβολο του Jacobi συμπίπτει με το σύμβολο του Legendre. Επίσης, ορίζουμε $(a/1) = 1$. Παρατηρούμε ότι $(a/n) = 0$ αν και μόνον αν $\mu\kappa\delta(a, n) > 1$.

Αν ο a είναι τετραγωνικό υπόλοιπο κατά μέτρο n, τότε ο a είναι τετραγωνικό υπόλοιπο κατά μέτρο p_i και επομένως $(a/p_i) = 1$ $(i = 1, \ldots, k)$. Έτσι, έχουμε ότι $(a/n) = 1$. Αν όμως έχουμε $(a/n) = 1$, τότε δεν συνεπάγεται πάντα ότι ο a είναι τετραγωνικό υπόλοιπο κατά μέτρο n. Για παράδειγμα, ισχύει:

$$(3/35) = (3/5)(3/7) = (-1)(-1) = 1.$$

Από την άλλη πλευρά, αν το 3 είναι είναι τετραγωνικό υπόλοιπο κατά μέτρο 35, τότε είναι τετραγωνικό υπόλοιπο κατά μέτρο 5 και 7 που δεν συμβαίνει.

Οι παρακάτω ιδιότητες αποδεικνύονται εύκολα ως συνέπεια του ορισμού του συμβόλου του Jacobi. Ας είναι n και m περιττοί θετικοί ακέραιοι. Τότε για κάθε $a, b \in \mathbb{Z}$ ισχύουν τα εξής:
(α) $(ab/n) = (a/n)(b/n)$.

(β) $(a/nm) = (a/n)(a/m)$.
(γ) $a \equiv b \pmod n \Rightarrow (a/n) = (b/n)$.
(δ) $(ab^2/n) = (a/n)$.

Στη συνέχεια αποδεικνύουμε ιδιότητες του συμβόλου του Jacobi ανάλογες μ΄ αυτές των Πορισμάτων 5.15 και 5.16.

Πρόταση 5.22 *Ας είναι n περιττός ακέραιος > 1. Τότε έχουμε:*

$$(-1/n) = (-1)^{(n-1)/2}, \quad (2/n) = (-1)^{(n^2-1)/8}.$$

Απόδειξη. Ας είναι a και b είναι περιττοί ακέραιοι. Θα δείξουμε ότι ισχύουν οι ισοτιμίες:

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$$

και

$$\frac{(ab)^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2.$$

Για την απόδειξη της πρώτης, έχουμε:

$$(a-1)(b-1) \equiv 0 \pmod 4,$$

απ΄ όπου:

$$ab - 1 \equiv a + b - 2 \pmod 4$$

και διαιρώντας με τον 2 παίρνουμε το αποτέλεσμα. Για την απόδειξη της δεύτερης ισοτιμίας έχουμε $a^2 \equiv b^2 \equiv (ab)^2 \equiv 1 \pmod 8$ και επομένως ισχύει

$$(a^2-1)(b^2-1) \equiv 0 \pmod{64},$$

απ΄ όπου παίρνουμε:

$$(ab)^2 - 1 \equiv (a^2-1) + (b^2-1) \pmod{64}$$

και διαιρώντας με το 8 προκύπτει το αποτέλεσμα.

Ας είναι

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

η πρωτογενής ανάλυση του n. Χρησιμοποιώντας το Πόρισμα 5.15 έχουμε:

$$(-1/n) = \prod_{i=1}^{k} (-1/p_i)^{a_i} = \prod_{i=1}^{k} (-1)^{a_i(p_i-1)/2} = (-1)^{\sum_{i=1}^{k} a_i(p_i-1)/2}$$

και εφαρμοζοντας διαδοχικά την πρώτη από τις παραπάνω ισοτιμίες παίρνουμε:

$$(-1/n) = (-1)^{(n-1)/2}.$$

Στη συνέχεια το Πόρισμα 5.16 δίνει:

$$(2/n) = \prod_{i=1}^{k}(2/p_i)^{a_i} = \prod_{i=1}^{k}(-1)^{a_i(p_i^2-1)/8} = (-1)^{\sum_{i=1}^{k} a_i(p_i^2-1)/8}$$

και εφαρμοζοντας διαδοχικά τη δεύτερη από τις παραπάνω ισοτιμίες έχουμε:

$$(2/n) = (-1)^{(n^2-1)/8}. \quad \square$$

Όπως βλέπουμε στην παρακάτω πρόταση ο νόμος της τετραγωνικής αμοιβαιότητας ισχύει και για το σύμβολο του Jacobi.

Πρόταση 5.23 *Ας είναι m και n θετικοί περιττοί ακέραιοι πρώτοι μεταξύ τους. Τότε, έχουμε:*

$$(m/n)(n/m) = (-1)^{(m-1)(n-1)/4}.$$

Απόδειξη. Για $m = 1$ ή $n = 1$ η ισότητα προφανώς ισχύει. Υποθέτουμε ότι $m > 1$ και $n > 1$. Καθώς $\mu\kappa\delta(m, n) = 1$, έχουμε: $n = p_1 \cdots p_k$ και $m = q_1 \cdots q_l$, όπου $p_1, \ldots, p_k$ και $q_1, \ldots, q_l$ πρώτοι με $p_i \neq q_j$ για κάθε ζεύγος δεικτών i, j με $i \neq j$. Οι πρώτοι $p_1, \ldots, p_k$ δεν είναι κατ' ανάγκη διαφορετικοί και το ίδιο ισχύει για τους $q_1, \ldots, q_l$. Έχουμε:

$$(m/n)(n/m) = \prod_{i=1}^{k}(m/p_i)\prod_{j=1}^{l}(n/q_j) = \prod_{i=1}^{k}\prod_{j=1}^{l}(p_i/q_j)(q_j/p_i) = (-1)^S,$$

όπου

$$S = \frac{1}{4}\sum_{i=1}^{k}\sum_{j=1}^{l}(p_i - 1)(q_j - 1) = \frac{1}{4}\left(\sum_{i=1}^{k}(p_i - 1)\right)\left(\sum_{j=1}^{l}(q_j - 1)\right).$$

Από την απόδειξη της Πρότασης 5.22 έχουμε:

$$\frac{1}{2}\sum_{i=1}^{k}(p_i - 1) \equiv \frac{n-1}{2} \pmod 2, \quad \frac{1}{2}\sum_{j=1}^{l}(q_j - 1) \equiv \frac{m-1}{2} \pmod 2.$$

Έτσι, έχουμε $S \equiv (n-1)(m-1)/4 \pmod 2$ και επομένως ισχύει:

$$(m/n)(n/m) = (-1)^{(m-1)(n-1)/4}. \quad \square$$

Παράδειγμα 5.16 Θα υπολογίσουμε το σύμβολο $(-616/323)$. Έχουμε $616 = 2^3 \cdot 7 \cdot 11$. Τότε:

$$(-616/323) = (-2 \cdot 7 \cdot 11/323)$$

και επομένως έχουμε:

$$(-616/323) = (-1/323)(2/323)(7/323)(11/323).$$

Εφαρμόζοντας την Προτάση 5.22 παίρνουμε:

$$(-616/323) = (-1)^{(323-1)/2}(-1)^{(323^2-1)/8}(7/323)(11/323)$$

και επομένως έχουμε:

$$(-616/323) = (7/323)(11/323).$$

Τέλος, η Πρόταση 5.23 δίνει:

$$(7/323) = (-1)^{(323-1)(7-1)/4}(323/7) = -(1/7) = -1$$

και

$$(11/323) = (-1)^{(323-1)(11-1)/4}(323/11) = (-1)(4/11) = -1.$$

Συνεπώς, έχουμε $(-616/323) = 1$.

Στη συνέχεια χρησιμοποιώντας τα παραπάνω αποτελέσματα δίνουμε έναν αλγόριθμο για τον υπολογισμό του συμβόλου του Jacobi.

Αλγόριθμος 5.4 Υπολογισμός του συμβόλου του Jacobi.
Είσοδος: $M, N \in \mathbb{Z}$ με $M \neq 0$, N περιττός > 1, και $\mu\kappa\delta(M, N) = 1$.
Έξοδος: Η τιμή (M/N).

1. Θέτουμε $S_0 = 1$ ή $S_0 = (-1)^{(N-1)/2}$ αν αντίστοιχα ο M είναι θετικός ή αρνητικός $n_0 = N$ και $m_0 = |M| \mod n_0$.

2. Για $i = 0, 1, \ldots$ κάνουμε τα εξής:

   (α′) Υπολογίζουμε $m_i = 2^{k_i} m_i'$, όπου m_i' θετικός περιττός ακέραιος και k_i ακέραιος ≥ 0.

(β′) Υπολογίζουμε

$$S_{i+1} = (-1)^{e_i(n_i^2-1)/8+(n_i-1)(m_i'-1)/4}\, S_i,$$

όπου $e_i = 0$ ή 1, αν αντίστοιχα ο k_i είναι άρτιος ή περιττός.

(γ′) Θέτουμε $n_{i+1} = m_i'$ και αν $m_i' > 1$, τότε υπολογίζουμε $m_{i+1} = n_i \bmod m_i'$.

3. Όταν βρούμε $m_{i+1} = 1$ ή $n_{i+1} = 1$, τότε σταματάμε και εξάγουμε τον αριθμό S_{i+1}.

Πρόταση 5.24 *Ο παραπάνω αλγόριθμος υπολογίζει σωστά την τιμή του συμβόλου (M/N) σε $O(\ell(M)\ell(N))$ δυαδικές ψηφιακές πράξεις.*

Απόδειξη. Πρώτα θα δείξουμε ότι για κάθε i έχουμε $\mu\kappa\delta(m_i, n_i) = 1$. Για $i = 0$ ισχύει $\mu\kappa\delta(m_0, n_0) = \mu\kappa\delta(N, M) = 1$. Υποθέτουμε ότι $\mu\kappa\delta(m_s, n_s) = 1$. Έχουμε $m_s = 2^{k_s} m_s'$ και $n_{s+1} = m_s'$. Επίσης, $m_{s+1} = n_s \bmod m_s'$. Έτσι, παίρνουμε:

$$\mu\kappa\delta(m_{s+1}, n_{s+1}) = \mu\kappa\delta(n_s \bmod m_s', m_s') = \mu\kappa\delta(n_s, m_s') \le \mu\kappa\delta(m_s, n_s) = 1,$$

απ′ όπου έχουμε $\mu\kappa\delta(m_{s+1}, n_{s+1}) = 1$. Επομένως $\mu\kappa\delta(m_i, n_i) = 1$, για κάθε i.

Παρατηρούμε ότι αν για κάποιο i έχουμε $m_{i+1} = 0$, τότε $m_i' | n_i$ και κατά συνέπεια $\mu\kappa\delta(m_i, n_i) > 1$ που είναι άτοπο. Έτσι, ισχύει

$$1 \le n_{i+1} = m_i' \le m_i < n_i, \quad 1 \le m_{i+1} < m_i' \le m_i.$$

Επομένως, στο Βήμα 2, η διαδικασία ολοκληρώνεται μετά από ένα πεπερασμένο πλήθος υπολογισμών.

Στο Βήμα 1, από την Πρόταση 5.22 έπεται:

$$(M/N) = S_0\,(|M|/N).$$

Επίσης, στο Βήμα 2, για κάθε δείκτη $i = 0, 1, \ldots,$ έχουμε:

$$\begin{aligned}(m_i/n_i) &= (-1)^{e_i(n_i^2-1)/8}(m_i'/n_i)\\ &= (-1)^{e_i(n_i^2-1)/8}(-1)^{(n_i-1)(m_i'-1)/4}(m_{i+1}/n_{i+1}).\end{aligned}$$

Η διαδικασία αυτή σταματά μόνο όταν βρεθεί δείκτης i έτσι, ώστε $m_{i+1} = 1$ ή $n_{i+1} = 1$, πράγμα που συμβαίνει γιατί, όπως είδαμε παραπάνω, ισχύουν οι ανισότητες $1 \leq n_{i+1} < n_i$ και $1 \leq m_{i+1} < m_i$. Ας υποθέσουμε ότι για $i = t$ έχουμε $m_{t+1} = 1$ ή $n_{t+1} = 1$ και επομένως $(m_{t+1}/n_{t+1}) = 1$. Έτσι, από τα παραπάνω, παίρνουμε:

$$\begin{aligned}(M,N) &= S_0\,(m_0/n_0)\\ &= S_0\,(-1)^{e_0(n_0^2-1)/8}(-1)^{(n_0-1)(m_0'-1)/4}\,(m_1/n_1)\\ &= S_1\,(m_1/n_1)\\ &= \ldots\\ &= S_t\,(m_t/n_t)\\ &= S_{t+1}.\end{aligned}$$

Συνεπώς, ο αλγόριθμος υπολογίζει την ποσότητα S_{t+1} που είναι πράγματι η τιμή του συμβόλου (M/N).

Τέλος, θα προσδιορίσουμε τον χρόνο που απαιτείται γι' αυτόν τον υπολογισμό. Το Βήμα 1 απαιτεί $O(\ell(M)\ell(N))$ δυαδικές ψηφιακές πράξεις. Ας υποθέσουμε ότι για $i = t$ ο αλγόριθμος περατώνει τη λειτουργία του. Στο Βήμα 2, για κάθε i, έχουμε να υπολογίσουμε τις ποσότητες m_i', S_{i+1} και m_{i+1}. Ο πλέον χρονοβόρος υπολογισμός είναι ο προσδιορισμός του m_{i+1}, καθώς ο υπολογισμός του m_i' γίνεται με μία δεξιά μετατόπιση των ψηφίων του m_i και του S_{i+1} με τον έλεγχο διαιρετότητας των ακεραίων $(n_i \pm 1)/2$, $n_i - 1$ και $m_i' - 1$ από το 4.

Έχουμε λοιπόν $n_{i+1} = m_i'$ και αν $m_i' > 1$, τότε $n_i = q_i m_i' + m_{i+1}$, όπου q_i θετικός ακέραιος. Έτσι, ο υπολογισμός του m_{i+1} απαιτεί $O(\ell(q_i)\ell(m_i'))$ δυαδικές ψηφιακές πράξεις. Έτσι, για τον υπολογισμό όλων των m_{i+1}, ο αριθμός των απαιτουμένων δυαδικών ψηφιακών πράξεων είναι:

$$\begin{aligned}O\left(\sum_{i=0}^{t}\ell(q_i)\ell(m_i')\right) &= O\left(\sum_{i=0}^{t}(\ell(n_i)-\ell(m_i'))\ell(m_i')\right)\\ &= O\left(\ell(m_0')\sum_{i=0}^{t}(\ell(n_i)-\ell(n_{i+1}))\right)\\ &= O(\ell(m_0')\ell(n_0)).\end{aligned}$$

Συνεπώς, ο χρόνος που χρειάζεται για να εκτελεστεί ο αλγόριθμος με είσοδο τους αριθμούς M και N είναι $O(\ell(M)\ell(N))$ δυαδικές ψηφιακές πράξεις. □

Παρατήρηση 5.1 Ας είναι p ένας πρώτος. Για να βρούμε ένα τετραγωνικό υπόλοιπο κατά μέτρο p επιλέγουμε τυχαία έναν αριθμό $a \in \mathbb{Z}_p^*$. Σύμφωνα με την Πρόταση 5.20, η πιθανότητα μία τέτοια επιλογή να δίνει ένα τετραγωνικό υπόλοιπο κατά μέτρο p είναι $1/2$. Ο χρόνος για να διαπιστωθεί, με τον παραπάνω αλγόριθμο, αν ισχύει $(a/p) = 1$ είναι $O(\ell(a)\ell(p))$ δυαδικές ψηφιακές πράξεις. Έτσι, ο αναμενόμενος χρόνος για να βρεθεί ένα τετραγωνικό υπόλοιπο κατά μέτρο p με αυτή τη διαδικασία είναι $O(\ell(p)^2)$ δυαδικές ψηφιακές πράξεις. Ο ίδιος χρόνος βέβαια χρειάζεται και για την εύρεση ενός μη τετραγωνικού υπόλοιπου κατά μέτρο p.

5.6.3 Επίλυση Τετραγωνικών Ισοτιμιών

Ας είναι n και c ακέραιοι με $n > 1$. Θα μελετήσουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$x^2 \equiv c \pmod{n},$$

οι οποίες καλούνται *τετραγωνικές ρίζες* του c κατά μέτρο n. Πρώτα θεωρούμε την περίπτωση όπου $n = p > 2$ πρώτος. Ας υποθέσουμε ότι $p \not| c$ και ότι η παραπάνω τετραγωνική ισοτιμια έχει λύση. Τότε, σύμφωνα με το Πόρισμα 4.7, η ισοτιμία αυτή έχει δύο ακριβώς λύσεις. Στη συνέχεια θα εξετάσουμε μεθόδους για τον προσδιορισμό τους. Καταρχήν θα θεωρήσυμε την εξής ειδική περίπτωση:

Πρόταση 5.25 *Ας είναι πρώτος $p > 2$ με $p \equiv 3 \pmod 4$ και c ένα τετραγωνικό υπόλοιπο κατά μέτρο p. Τότε οι λύσεις της τετραγωνικής ισοτιμίας*

$$x^2 \equiv c \pmod{p}$$

είναι

$$x \equiv \pm c^{(p+1)/4} \pmod{p}.$$

Απόδειξη. Ας είναι b ακέραιος με $c \equiv b^2 \pmod{p}$. Τότε, ισχύει:

$$(\pm c^{(p+1)/4})^2 \equiv c^{(p+1)/2} \equiv c^{(p-1)/2} c \equiv b^{p-1} c \equiv c \pmod{p}$$

και επομένως οι λύσεις της $x^2 \equiv c \pmod{p}$, είναι:

$$x \equiv \pm c^{(p+1)/4} \pmod{p}. \quad \square$$

Παράδειγμα 5.17 Σύμφωνα με τα παραπάνω, οι λύσεις της τετραγωνικής ισοτιμίας

$$x^2 \equiv 13 \,(\mathrm{mod}\, 127)$$

είναι:

$$x \equiv \pm 13^{(127+1)/4} \equiv \pm 34 \,(\mathrm{mod}\, 127).$$

Στη συνέχεια θ΄ ασχοληθούμε με την γενική περίπτωση και θα περιγράψουμε έναν αλγόριθμο ο οποίος είναι γνωστός ως αλγόριθμος των Tonelli - Shanks.

Αλγόριθμος 5.5 Αλγόριθμος των Tonelli - Shanks.
Είσοδος: Ένας πρώτος $p > 2$ και c ένα τετραγωνικό υπόλοιπο κατά μέτρο p.
Έξοδος: Οι τετραγωνικές ρίζες του c κατά μέτρο p.

1. Υπολογίζουμε $p - 1 = 2^s t$, όπου s ακέραιος ≥ 1 και t περιττός ακέραιος.

2. Επιλέγουμε έναν ακέραιο a ο οποίος δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο p και θέτουμε $z = a^t \mod p$.

3. Θέτουμε $(b_0, x_0, y_0, r_0) = (c^t \mod p, c^{(t+1)/2} \mod p, z, s-1)$.

4. Για κάθε $i = 0, \ldots, s-1$ θέτουμε $r_{i+1} = r_i - 1$ και

$$(b_{i+1}, x_{i+1}, y_{i+1}) = (b_i, x_i, y_i^2 \mod p)$$

αν $b_i^{2^{r_i - 1}} \equiv 1 \,(\mathrm{mod}\, p)$ και

$$(b_{i+1}, x_{i+1}, y_{i+1}) = (b_i y_i^2 \mod p,\ x_i y_i \mod p,\ y_i^2 \mod p),$$

αν $b_i^{2^{r_i - 1}} \equiv -1 \,(\mathrm{mod}\, p)$.

5. Εξάγουμε τους ακεραίους $\pm x_{s-1}$.

Πρόταση 5.26 *Ας είναι πρώτος $p > 2$ και c ένα τετραγωνικό υπόλοιπο κατά μέτρο p. Ο παραπάνω αλγόριθμος υπολογίζει σωστά τις τετραγωνικές ρίζες του c κατά μέτρο p και ο αναμενόμενος χρόνος για την εκτέλεση του είναι $O(\ell(p)^4)$ δυαδικές ψηφιακές πράξεις.*

Απόδειξη. Πρώτα θα δείξουμε ότι ισχύει:

$$z^{2^{s-1}} \equiv -1 \pmod{p}.$$

Ας υποθέσουμε ότι η παραπάνω ισοτιμία δεν ισχύει. Τότε έχουμε $z^{2^{s-1}} \equiv 1 \pmod{p}$ και επομένως $a^{(p-1)/2} \equiv 1 \pmod{p}$. Αν g είναι μία αρχική ρίζα κατά μέτρο p, τότε υπάρχει $l \in \{1, \ldots, p-2\}$ με $a \equiv g^l \pmod{p}$. Έτσι, έχουμε $g^{l(p-1)/2} \equiv 1 \pmod{p}$ και επομένως $l = 2m$, όπου m ακέραιος. Άρα $a \equiv (g^m)^2 \pmod{p}$ που είναι άτοπο. Συνεπώς, η προς απόδειξη ισοτιμία αληθεύει.

Ας είναι h ακέραιος με $c \equiv h^2 \pmod{p}$. Έχουμε:

$$cb_0 \equiv c^{t+1} \equiv x_0^2 \pmod{p}, \quad y_0^{2^{r_0}} \equiv z^{2^{s-1}} \equiv -1 \pmod{p}$$

και

$$b_0^{2^{r_0}} \equiv (c^t)^{2^{s-1}} \equiv c^{(p-1)/2} \equiv h^{p-1} \equiv 1 \pmod{p}.$$

Ας υποθέσουμε ότι ισχύει:

$$cb_i \equiv x_i^2 \pmod{p}, \quad y_i^{2^{r_i}} \equiv -1 \pmod{p}, \quad b_i^{2^{r_i}} \equiv 1 \pmod{p}.$$

Τότε, αν $b_i^{2^{r_i-1}} \equiv 1 \pmod{p}$, έχουμε:

$$cb_{i+1} \equiv cb_i \equiv x_i^2 \equiv x_{i+1}^2 \pmod{p},$$

$$y_{i+1}^{2^{r_{i+1}}} \equiv (y_i^2)^{2^{r_i-1}} \equiv y_i^{2^{r_i}} \equiv -1 \pmod{p},$$

$$b_{i+1}^{2^{r_{i+1}}} \equiv b_i^{2^{r_i-1}} \equiv 1 \pmod{p}$$

και αν $b_i^{2^{r_i-1}} \equiv -1 \pmod{p}$, έχουμε:

$$cb_{i+1} \equiv cb_i y_i^2 \equiv x_i^2 y_i^2 \equiv x_{i+1}^2 \pmod{p},$$

$$y_{i+1}^{2^{r_{i+1}}} \equiv (y_i^2)^{2^{r_i-1}} \equiv y_i^{2^{r_i}} \equiv -1 \pmod{p},$$

$$b_{i+1}^{2^{r_{i+1}}} \equiv b_i^{2^{r_i-1}} (y_i^2)^{2^{r_i-1}} \equiv 1 \pmod{p}.$$

Συνεπώς, για κάθε $i = 0, \ldots, s-1$ ισχύει:

$$cb_i \equiv x_i^2, \quad y_i^{2^{r_i}} \equiv -1 \pmod{p}, \quad b_i^{2^{r_i}} \equiv 1 \pmod{p}.$$

Καθώς $b_i^{2^{r_i}} \equiv 1 \pmod{p}$, συνάγεται ότι $b_i^{2^{r_i-1}} \equiv \pm 1 \pmod{p}$ και επομένως για κάθε $i = 0, \ldots, s-1$ έχουμε μία τιμή για τη τετράδα

(b_i, x_i, y_i, r_i). Για $i = s-1$ παίρνουμε $r_{s-1} = 0$. Οπότε $b_{s-1} \equiv 1 \pmod{p}$ και κατά συνέπεια $c \equiv x_{s-1}^2 \pmod{p}$.

Ας υποθέσουμε ότι έχει επιλεγεί ένας ακέραιος a ο οποίος δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο p. Οι υπολογισμοί στα Βήματα 2 και 3 απαιτούν $O(\ell(p)^3)$ δυαδικές ψηφιακές πράξεις. Στο Βήμα 4, για κάθε i έχουμε $O(\ell(p)^3)$ δυαδικές ψηφιακές πράξεις και καθώς $s = O(\ell(p))$, ο χρόνος εκτέλεσης του Βήματος 4 είναι $O(\ell(p)^4)$. Συνεπώς, δεδομένου του a ο χρόνος εκτέλεσης του αλγορίθμου είναι $O(\ell(p)^4)$. Τέλος, σύμφωνα με την Παρατήρηση 5.1, ο αναμενόμενος χρόνος για την εύρεση του a είναι $O(\ell(p)^2)$ δυαδικές ψηφιακές πράξεις. Συνεπώς, ο αναμενόμενος χρόνος για την εκτέλεση του αλγορίθμου είναι $O(\ell(p)^4)$ δυαδικές ψηφιακές πράξεις. □

Παρατήρηση 5.2 Στην περίπτωση όπου $p \equiv \pm 3 \pmod{8}$ από το Πόρισμα 5.15 έχουμε ότι ο 2 δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο p και επομένως μπορούμε να τον χρησιμοποιήσουμε στον παραπάνω αλγόριθμο. Τότε ο χρόνος εκτέλεσης του αλγορίθμου είναι $O(\ell(p)^3)$ δυαδικές ψηφιακές πράξεις.

Παράδειγμα 5.18 Ο ακέραιος 8757 είναι ένα τετραγωνικό υπόλοιπο κατά μέτρο 9013. Εφαρμόζοντας τον αλγόριθμο των Tonelli-Shanks θα υπολογίσουμε τις τετραγωνικές ρίζες του 8757 κατά μέτρο 9013.

Έχουμε $9012 = 2^2 \cdot 2253$. Επομένως $s = 2$ και $t = 2253$. Καθώς $9013 \equiv -3 \bmod 8$, ο 2 δεν είναι τετραγωνικό υπόλοιπο κατά μέτρο 9013. Οπότε παίρνουμε $z = 2^{2253} \bmod 9013 = 1658$. Επομένως, $r_0 = 1$ και

$$b_0 = 8757^{2253} \bmod 9013 = 9012, \quad x_0 = 8757^{1127} \bmod 9013 = 8997,$$

$$y_0 = z = 1658.$$

Καθώς

$$8757^{2253} \equiv -1 \pmod{9013}$$

έχουμε $r_1 = 0$ και

$$b_1 = 8757^{2253}(2^{2253})^2 \bmod 9013 = 4175,$$

$$x_1 = 8757^{1127}2^{2253} \bmod 9013 = 511,$$

$$y_1 = (2^{2253})^2 \bmod 9013 = 9012.$$

Άρα οι τετραγωνικές ρίζες του 8757 κατά μέτρο 9013 είναι οι κλάσεις των ακεραίων $\pm 511 \pmod{9013}$.

Ας είναι p και q δύο διαφορετικοί περιττοί πρώτοι και $n = pq$. Θα εξετάσουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$x^2 \equiv c \pmod{n}.$$

Αν x_0 είναι ένας ακέραιος που την επαληθεύει, τότε έχουμε:

$$x_0^2 \equiv c \pmod{p}, \quad x_0^2 \equiv c \pmod{q}.$$

Αντίστροφα, αν ισχύουν οι δύο αυτές ισοτιμίες, τότε οι πρώτοι p και q διαιρούν τον $x_0^2 - c$ και επομένως $n|x_0^2 - c$, απ΄ όπου $x_0^2 \equiv c \pmod{n}$. Βλέπουμε λοιπόν ότι ένας ακέραιος ικανοποιεί την παραπάνω πολυωνυμική ισοτιμία αν και μόνον αν ικανοποιεί τις πολυωνυμικές ισοτιμίες:

$$x^2 \equiv c \pmod{p}, \quad x^2 \equiv c \pmod{q}.$$

Ας υποθέσουμε ότι οι λύσεις των πολυωνυμικών ισοτιμιών

$$x^2 \equiv c \pmod{p}, \quad x^2 \equiv c \pmod{q}$$

είναι:

$$x \equiv \pm m_p \pmod{p}, \quad x \equiv \pm m_q \pmod{q},$$

αντίστοιχα. Χρησιμοποιώντας τον εκτεταμένο Ευκλείδειο αλγόριθμο, βρίσκουμε ακεραίους u, v με $up + vq = 1$. Θέτουμε

$$z = upm_q + vqm_p \quad \text{και} \quad w = upm_q - vqm_p.$$

Έχουμε:

$$z \equiv m_p \pmod{p}, \quad z \equiv m_q \pmod{q}$$

και

$$w \equiv -m_p \pmod{p}, \quad w \equiv m_q \pmod{q}.$$

Επομένως, $z^2 \equiv c \pmod{n}$ και $w^2 \equiv c \pmod{n}$. Από την άλλη πλευρά, αν y είναι ακέραιος με $y^2 \equiv c \pmod{n}$, τότε $y \equiv m_p \pmod{p}$ ή $y \equiv -m_p \pmod{p}$ και $y \equiv m_q \pmod{q}$ ή $y \equiv -m_q \pmod{q}$, απ΄ όπου έχουμε ότι ο y είναι ισότιμος με κάποιον από τους $\pm z, \pm w$ κατά μέτρο n. Συνεπώς, οι λύσεις της $x^2 \equiv c \pmod{n}$ είναι: $x \equiv \pm z, \pm w \pmod{n}$.

Έτσι, στην περίπτωση όπου υπάρχει ακέραιος b με $b^2 \equiv c \pmod{n}$, η πολυωνυμική ισοτιμία $x^2 \equiv c \pmod{n}$ έχει ακριβώς 4 διαφορετικές λύσεις αν $\mu\kappa\delta(c, n) = 1$, δύο διαφορετικές λύσεις αν $\mu\kappa\delta(c, n) = p$ ή q και μία λύση αν $n|c$.

Παράδειγμα 5.19 Θα προσδιορίσουμε τις λύσεις της τετραγωνικής ισοτιμίας

$$x^2 \equiv 699 \,(\mathrm{mod}\, 4757).$$

Όπως είδαμε, το σύνολο των ακεραίων που την επαληθεύει συμπίπτει με το σύνολο των ακεραίων που ικανοποιεί το σύστημα

$$x^2 \equiv 60 \,(\mathrm{mod}\, 71), \quad x^2 \equiv 29 \,(\mathrm{mod}\, 67).$$

Έχουμε $71 \equiv 67 \equiv 3 \,(\mathrm{mod}\, 4)$ και επομένως από την Πρόταση 5.25 έπεται ότι οι λύσεις των παραπάνω ισοτιμιών είναι:

$$x \equiv 29^{(67+1)/2} \equiv 37 \,(\mathrm{mod}\, 67), \quad x \equiv 60^{(71+1)/2} \equiv 29 \,(\mathrm{mod}\, 71).$$

Στη συνέχεια εφαρμόζοντας τον εκτεταμένο Ευκλείδειο αλγόριθμο βρίσκουμε την ισότητα

$$-18 \cdot 67 + 19 \cdot 71 = 1.$$

Κατόπιν, υπολογίζουμε τους ακεραίους:

$$z = -18 \cdot 67 \cdot 29 + 19 \cdot 71 \cdot 37 = 14939,$$

$$w = -18 \cdot 67 \cdot 29 - 19 \cdot 71 \cdot 37 = -84887.$$

Έτσι, οι ζητούμενες λύσεις είναι:

$$x \equiv \pm 14939, \pm 84887 \equiv \pm 668, \pm 739 \,(\mathrm{mod}\, 4757).$$

5.7 Πεπερασμένα Σώματα

Σ′ αυτή την ενότητα εισάγουμε την έννοια της ισοτιμίας σε πολυωνυμικό δακτύλιο και μελετάμε τη δομή τω πεπερασμένων σωμάτων.

5.7.1 Ισοτιμία Πολυωνύμων

Ας είναι A ένας αντιμεταθετικός δακτύλιος και A^* η ομάδα των αντιστρεψίμων στοιχείων του. Θεωρούμε ένα πολυώνυμο $f \in A[x]$ με $lc(f) \in A^*$ και $\deg f = d \geq 1$. Αν $g, h \in A[x]$, τότε λέμε ότι το πολυώνυμο g είναι *ισότιμο κατά μέτρο* f με το h, και γράφουμε $g \equiv h \,(\mathrm{mod}\, f)$, αν $f|(g-h)$. Αν δεν συμβαίνει αυτό, τότε λέμε ότι τα g και h είναι *ανισότιμα* κατά μέτρο f και γράφουμε $g \not\equiv h \,(\mathrm{mod}\, f)$.

Οι παρακάτω προτάσεις έχουν όμοιες αποδείξεις με αυτές των Προτάσεων 5.1, 5.2, 5.3 και του Πορίσματος 5.1.

Πρόταση 5.27 *Ισχύουν τα εξής:*
(α) $g \equiv g \,(\mathrm{mod}\, f)$*, για κάθε* $g \in A[x]$*.*
(β) Αν $g \equiv h \,(\mathrm{mod}\, f)$*, τότε* $h \equiv g \,(\mathrm{mod}\, f)$*.*
(γ) Αν $g \equiv h \,(\mathrm{mod}\, f)$ *και* $h \equiv e \,(\mathrm{mod}\, f)$*, τότε* $g \equiv e \,(\mathrm{mod}\, f)$*.*

Πρόταση 5.28 *Έχουμε* $g \equiv h \,(\mathrm{mod}\ f)$ *αν και μόνον αν τα υπόλοιπα των διαιρέσεων των* g *και* h *με το* f *είναι ίσα.*

Πρόταση 5.29 *Για κάθε* $a, b, c, d \in A[x]$ *με* $a \equiv b \,(\mathrm{mod}\, f)$ *και* $c \equiv d \,(\mathrm{mod}\, f)$ *ισχύει:*

$$a + c \equiv b + d \,(\mathrm{mod}\, f) \quad \textit{και} \quad ac \equiv bd \,(\mathrm{mod}\, f).$$

Επίσης, για κάθε $m \in \mathbb{N}$ *ισχύει:*

$$ma \equiv mb \ (\mathrm{mod}\, f) \quad \textit{και} \quad a^m \equiv b^m \ (\mathrm{mod}\ f).$$

Ας είναι $g \in A[x]$. Καλούμε *κλάση ισοτιμίας του* g *κατά μέτρο* f το σύνολο

$$[g]_f = \{h \in A[x] / \ h \equiv g \,(\mathrm{mod}\, f)\}.$$

Συμβολίζουμε με $A[x]/(f)$ το σύνολο όλων των κλάσεων ισοτιμίας των πολωνύμων του $A[x]$ κατά μέτρο f.

Από την Πρόταση 5.27 έχουμε ότι για κάθε $g \in A[x]$ ισχύει $g \in [g]_f$ και επομένως $[g]_f \neq \emptyset$. Επίσης, παρατηρούμε ότι η ένωση όλων των κλάσεων δίνει το σύνολο $A[x]$.

Πρόταση 5.30 *Ας είναι* $g, h \in A[x]$*. Τότε ισχύουν το εξής:*
(α) $g \equiv h \ (\mathrm{mod}\ f)$ *αν και μόνον αν* $[g]_f = [h]_f$*.*
(β) Αν $[g]_f \neq [h]_f$*, τότε* $[g]_f \cap [h]_f = \emptyset$*.*

Απόδειξη. Η απόδειξη είναι όμοια μ΄ αυτή της Πρότασης 5.4. □

Συμβολίζουμε με $A[x]_f$ το σύνολο των πολυωνύμων $g \in A[x]$ με $\deg g < \deg f$. Ας σημειωθεί ότι το σύνολο $A[x]_f$ είναι πεπερασμένο, αν και μόνον αν ο δακτύλιος A είναι πεπερασμένος. Σ΄ αυτή την περίπτωση, έχουμε $|A[x]_f| = |A|^d$.

Πρόταση 5.31 *Οι κλάσεις των στοιχείων του* $A[x]_f$ *είναι όλα τα διακεκριμμένα στοιχεία του* $A[x]/(f)$*.*

Απόδειξη. Η απόδειξη είναι όμοια μ΄ αυτή της Πρότασης 5.5. □

Από την Πρόταση 5.29 έχουμε ότι για κάθε $a, b, c, d \in A[x]$ με $[a]_f = [b]_f$ και $[c]_f = [d]_f$ ισχύει:

$$[a + c]_f = [b + d]_f \quad \text{και} \quad [ac]_f = [bd]_f.$$

Έτσι, μπορούμε να ορίσουμε δύο πράξεις επί του $A[x]/(f)$ θέτοντας

$$[a]_f + [b]_f = [a + b]_f \quad \text{και} \quad [a]_f \cdot [b]_f = [ab]_f,$$

για κάθε $[a]_f, [b]_f \in A[x]/(f)$. Οι πράξεις αυτές καλούνται *πρόσθεση* και *πολλαπλασιασμός*, αντίστοιχα. Εύκολα αποδεικνύεται ότι το σύνολο $A[x]/(f)$ με αυτές τις πράξεις αποτελεί αντιμεταθετικό δακτύλιο με $\mathrm{char}A[x]/(f) = \mathrm{char}A$. Συμβολίζουμε με $(A[x]/(f))^*$ το σύνολο των κλάσεων που έχουν αντίστροφο στοιχείο.

Αν r είναι το υπόλοιπο της διαίρεσης ενός πολυωνύμου $g \in A[x]$ με το f, τότε θα γράφουμε $r = g \mod f$. Ας είναι $g, h \in A[x]_f$. Ορίζουμε το άθροισμα και το γινόμενο των a και b μέσα στο $A[x]_f$ ως εξής:

$$a \oplus b = a + b \mod f, \quad a \odot b = ab \mod f.$$

Εύκολα βλέπουμε ότι το $A[x]_f$ με αυτές τις πράξεις αποτελεί αντιμεταθετικό δακτύλιο. Συμβολίζουμε με $(A[x]_f)^*$ το σύνολο των αντιστρεψίμων στοιχείων του $A[x]_f$. Τέλος, αν $a \in (A[x]_f)^*$, τότε θα συμβολίζουμε το αντίστροφο του a με $a^{-1} \mod f$.

Η απεικόνιση

$$\pi_f : A[x]_f \longrightarrow A[x]/(f),\ a \longmapsto [a]_f.$$

είναι αμφίεση και για κάθε $a, b \in A[x]_f$ έχουμε:

$$\pi_f(a \oplus b) = [a + b]_f = [a]_f + [b]_f = \pi_f(a) + \pi_f(b)$$

και

$$\pi_f(a \odot b) = [ab]_f = [a]_f[b]_f = \pi_f(a)\pi_f(b).$$

Άρα, η π_f είναι ισομορφισμός δακτυλίων με αντίστροφη απεικόνιση

$$\pi_f^{-1} : A[x]/(f) \longrightarrow A[x]_f,\ [a]_f \longmapsto a \mod f.$$

Ειδικότερα, έχουμε $\pi_f((A[x]_f)^*) = (A[x]/(f))^*$.

Πρόταση 5.32 *Ας είναι $h, g \in A[x]_f$. Τότε έχουμε τα εξής:*
(α) Ο υπολογισμός του $h \pm g \mod f$ απαιτεί $O(d)$ προσθέσεις/αφαιρέσεις μέσα στο A.
(β) Ο υπολογισμός του $hg \mod f$ απαιτεί $O(d^2)$ πράξεις μέσα στο A.

Απόδειξη. (α) Σύμφωνα με την Πρόταση 4.18, ο υπολογισμός του $h \pm g$ απαιτεί $O(d)$ προσθέσεις/αφαιρέσεις. Καθώς $\deg h, \deg g < d$, έχουμε $h \pm g \in A[x]_f$.

(β) Από την Πρόταση 4.18, ο υπολογισμός του hg απαιτεί $O(d^2)$ πράξεις μέσα στο A. Σύμφωνα με την Πρόταση 4.15, ο υπολογισμός του υπολοίπου της διαίρεσης του gh με το f απαιτεί $O(d^2)$ πράξεις μέσα στο A. Συνδυάζοντας τις προηγούμενες εκτιμήσεις, έχουμε ότι ο υπολογισμός του $hg \mod f$ απαιτεί $O(d^2)$ πράξεις μέσα στο A. □

Πόρισμα 5.17 *Ας είναι $h, g \in \mathbb{Z}_n[x]_f$. Τότε έχουμε τα εξής:*
(α) Ο υπολογισμός του $h \pm g \mod f$ απαιτεί $O(d \log n)$ δυαδικές ψηφιακές πράξεις.
(β) Ο υπολογισμός του $hg \mod f$ απαιτεί $O(d^2 (\log n)^2))$ δυαδικές ψηφιακές πράξεις.

Απόδειξη. Σύμφωνα με την Πρόταση 5.7, η πρόσθεση/αφαίρεση μέσα στο $\mathbb{Z}_n$ απαιτεί $O(\log n)$ δυαδικές ψηφιακές πράξεις. Επιπλέον, ο πολλαπλασιασμός και ο υπολογισμός αντιστρόφου απαιτούν $O((\log n)^2)$ δυαδικές ψηφιακές πράξεις. Επομένως, η Πρόταση 5.32 δίνει το αποτέλεσμα. □

Πρόταση 5.33 *Ας είναι $g \in \mathbb{Z}_n[x]_f$ και m θετικός ακέραιος. Τότε ο υπολογισμός του $g^m \mod f$ απαιτεί $O(d^2 (\log n)^2 \log m))$ δυαδικές ψηφιακές πράξεις.*

Απόδειξη. Η απόδειξη είναι συνέπεια των Προτάσεων 4.3 και του Πορίσματος 5.17. □

Τελειώνοντας την ενότητα, δίνουμε μία ικανή και αναγκαία συνθήκη για να είναι ο δακτύλιος $K[x]_f$ σώμα (όπου K είναι σώμα).

Πρόταση 5.34 *Ας είναι K ένα σώμα και $f \in K[x]$. Τότε ο δακτύλιος $K[x]_f$ είναι σώμα αν και μόνον αν το πολυώνυμο f είναι ανάγωγο.*

Απόδειξη. Ας υποθέσουμε ότι το f είναι ανάγωγο. Τότε για καθε $g \in K[x]_f \setminus \{0\}$ ισχύει $\mu\kappa\delta(f,g) = 1$ και επομένως, σύμφωνα με το Πόρισμα 4.10, υπαρχουν $u, v \in K[x]$ με $\deg u \leq \deg g$ και $\deg v \leq \deg f$ έτσι, ώστε $uf + vg = 1$. Έπομένως, έχουμε $v \in K[x]_f$ και $vg \equiv 1 \,(\mathrm{mod}\ f)$. Συνεπώς, $g \in (K[x]_f)^*$. Άρα, ο δακτύλιος $K[x]_f$ είναι σώμα.

Αντίστροφα, ας υποθέσουμε ότι ο δακτύλιος $K[x]_f$ είναι σώμα. Έτσι, για κάθε $g \in K[x]_f \setminus K$ υπάρχει $h \in K[x]_f$ με $gh \equiv 1 \,(\mathrm{mod}\, f)$. Επομένως, υπάρχει $u \in K[x]_f$ με $gh + uf = 1$. Άρα, για κάθε $g \in K[x]$ με $\deg g < \deg f$ ισχύει $g \not| f$ και κατά συνέπεια το f είναι ανάγωγο. □

Πόρισμα 5.18 *Ο δακτύλιος $K[x]/(f)$ είναι σώμα αν και μόνον αν το πολυώνυμο f είναι ανάγωγο.*

Παράδειγμα 5.20 Θεωρούμε το σώμα $\mathbb{Z}_2$ και το πολυώνυμο $f = x^2 + x + 1$. Το f είναι ανάγωγο επί του $\mathbb{Z}_2$ και επομένως, σύμφωνα με την Πρόταση 5.34 ο δακτύλιος $K = \mathbb{Z}_2[x]_f$ είναι ένα σώμα με τέσσερα στοιχεία. Ειδικότερα, έχουμε $K = \{0, 1, x, 1 + x\}$.

5.7.2 Δομή Πεπερασμένων Σωμάτων

Ας είναι K ένα πεπερασμένο σώμα. Τότε από το Πόρισμα 4.4 έπεται ότι η χαρακτηριστική του K είναι ένας πρώτος αριθμός p.

Πρόταση 5.35 *Αν* $\mathrm{char}K = p > 0$, *τότε η απεικόνιση*

$$\tau : \mathbb{Z}_p \longrightarrow K,\ n \longmapsto ne_A$$

είναι μονομορφισμός.

Απόδειξη. Ας είναι e το μοναδιαίο στοιχείο του K. Θεωρούμε την απεικόνιση

$$\sigma : \mathbb{Z}_p \longrightarrow K,\ n \longmapsto ne.$$

Για κάθε $n, m \in \mathbb{Z}_p$ έχουμε:

$$\sigma(n \oplus m) = (n + m)e = ne + me = \sigma(n) + \sigma(m).$$

και

$$\sigma(n \odot m) = (nm)e = (ne)(me) = \sigma(n)\sigma(m).$$

Άρα, η απεικόνιση σ είναι ένας μορφισμός σωμάτων και κατά συνέπεια είναι ένεση. $\square$

Σύμφωνα με την Πρόταση 5.35 μπορούμε να θεωρούμε ότι το $\mathbb{Z}_p$ περιέχεται σε κάθε σώμα χαρακτηριστικής p.

Από την Πρόταση 5.15 έχουμε ότι η ομάδα K^* είναι κυκλική. Θέτουμε $|K^*| = m$. Τότε, για κάθε $a \in K^*$ ισχύει $a^m = 1$ και επομένως το a είναι ρίζα του $x^m - 1$. Ας είναι L ένα υπόσωμα του K. Από το Θεώρημα 4.3 έπεται ότι το a είναι ρίζα ενός κανονικού αναγώγου πολυωνύμου $f \in L[x]$ με $f|x^m - 1$.

Ας υποθέσουμε ότι $g \in L[x] \setminus \{0\}$ με $g(a) = 0$. Θέτουμε $D = \mu\kappa\delta(f, g)$. Σύμφωνα με το Πόρισμα 4.10, υπάρχουν $u, v \in L[x]$ τέτοια, ώστε

$$D = fu + gv.$$

Τότε $D(a) = 0$. Έτσι, έχουμε $D \neq 1$ και καθώς το f είναι ανάγωγο, παίρνουμε $f|g$ Συνεπώς, το f είναι το μοναδικό κανονικό ανάγωγο πολυώνυμο του $L[x]$ που έχει ρίζα το a και κάθε άλλο πολυώνυμο του $L[x]$ που έχει ρίζα το a διαιρείται από αυτό. Το πολυώνυμο f καλείται *ελάχιστο πολυώνυμο* του a επί του L. Στην περίπτωση, όπου $K = L[x]_f$, τότε το ελάχιστο πολυώνυμο του x επί του L είναι το f.

Θεωρούμε την απεικόνιση

$$\tau : L[x]_f \longrightarrow K,\ h \longmapsto h(a).$$

Εύκολα επαληθεύουμε ότι η τ είναι μορφισμός σωμάτων. Συμβολίζουμε με $L(a)$ την εικόνα του τ και έχουμε $L[x]_f \cong L(a)$. Αν $s = \deg f$, τότε:

$$L(a) = \{c_0 + c_1 a + \cdots + c_{s-1}a^{s-1} /\ c_0, \ldots, c_{s-1} \in L\}.$$

Αν M είναι ένα υπόσωμα του K που περιέχει το a και το L, τότε προφανώς κάθε στοιχείο του $L(a)$ ανήκει σ΄ αυτό. Συνεπώς, το $L(a)$ είναι το μικρότερο υπόσωμα του K που περιέχει το a και το L.

Θεώρημα 5.6 *Ας είναι K ένα πεπερασμένο σώμα χαρακτηριστικής $p > 0$. Ισχύουν τα εξής:*
(α) Αν L είναι ένα υπόσωμα του K και f το ελάχιστο πολυώνυμο ενός γεννήτορα a της ομάδας K^* επί του L, τότε $K = L(a) \cong L[x]_f$ και

$|K| = |L|^s$, *όπου* $s = \deg f$. *Ειδικότερα, ισχύει* $|K| = p^n$.
(β) Έχουμε:

$$x^{p^n} - x = \prod_{b \in K} (x - b).$$

(γ) Αν L *είναι ένα υπόσωμα του* K, *τότε* $|L| = p^r$, *με* $r|n$.
(δ) Για κάθε διαιρέτη r *του* n *υπάρχει ένα μοναδικό υπόσωμα του* K *με* p^r *στοιχεία. Αυτό είναι το σύνολο των στοιχείων* $b \in K$ *με* $b^{p^r} = b$.

Απόδειξη. (α) Καθώς το a είναι γεννήτορας της ομάδας K^* και όλες οι δυνάμεις του a ανήκουν στο $L(a)$, έχουμε $K \subseteq L(a)$ και επομένως $K = L(a) \cong L[x]_f$. Άμεση συνέπεια αυτή της ισομορφίας είναι ότι $|K| = |L|^s$, όπου $s = \deg f$. Παίρνοντας $L = \mathbb{Z}_p$, έχουμε $|K| = p^n$.

(β) Καθώς $|K| = p^n$, για κάθε $b \in K^*$ έχουμε $b^{p^n-1} = 1$. Έτσι, το πολυώνυμο $x^{p^n} - x$ έχει p^n διακεκριμμένες ρίζες και κατά συνέπεια ισχύει:

$$x^{p^n} - x = \prod_{b \in K} (x - b).$$

(γ) Από το (α) έχουμε $|L| = p^r$ και $|K| = |L|^s$. Τότε ισχύει $p^n = p^{rs}$ και επομένως $r|n$.

(δ) Ας είναι r θετικός διαιρέτης του n. Το σύνολο

$$M = \{b \in K / \ b^{p^r} = b\}$$

είναι ένα υπόσωμα του K. Πράγματι, για κάθε $u, v \in M$ έχουμε:

$$(u - v)^{p^r} = u^{p^r} - v^{p^r} = u - v$$

και επομένως $u - v \in M$. Αν επί πλέον $v \neq 0$, τότε:

$$(uv^{-1})^{p^r} = u^{p^r}(v^{-1})^{p^r} = u^{p^r}(v^{p^r})^{-1} = uv^{-1}$$

και κατά συνέπεια $uv^{-1} \in M$. Άρα, το M είναι ένα υπόσωμα του K.

Καθώς τα στοιχεία του M είναι ρίζες του πολυωνύμου $x^{p^r} - x$, έχουμε $|M| \leq p^r$. Από την άλλη πλευρά, υπάρχει θετικός ακέραιος m με $n = rm$. Έτσι, έχουμε:

$$p^n - 1 = (p^r)^m - 1 = (p^r - 1)[(p^r)^{m-1} + \cdots + p^r + 1]$$

και επομένως $p^r - 1|p^n - 1$. Οπότε, καθώς η ομάδα K^* είναι κυκλική τάξης $p^n - 1$, υπάρχει $a \in K^*$ με $\mathrm{ord}(a) = p^r - 1$. Έτσι, όλα τα

στοιχεία $0, 1, a, \ldots, a^{p^r-2}$ είναι ρίζες του $X^{p^r} - X$, διαφορετικές ανά δύο. Άρα $|M| = p^r$. Τέλος, αν M' είναι ένα άλλο υπόσωμα του K με p^r στοιχεία, τότε από το (β) έχουμε ότι για κάθε $b \in M'$ ισχύει $b^{p^r} = b$ και επομένως $M = M'$. □

Θεώρημα 5.7 *Για κάθε πρώτο αριθμό p και κάθε θετικό ακέραιο n, υπάρχει ένα πεπερασμένο σώμα K με $|K| = p^n$.*

Για την απόδειξη του Θεωρήματος 5.7 θα χρειαστούμε το εξής λήμμα:

Λήμμα 5.2 *Ας είναι K ένα πεπερασμένο σώμα και $f \in K[x] \setminus K$. Τότε το K είναι υπόσωμα ενός πεπερασμένου σώματος L στο οποίο το f αναλύεται σε γινόμενο γραμμικών παραγόντων.*

Απόδειξη. Αν $\deg f = 1$, τότε το K είναι το ζητούμενο σώμα. Ας υποθέσουμε ότι για κάθε πολυώνυμο βαθμού $< n$ η προς απόδειξη πρόταση αληθεύει. Αν το f δεν είναι ανάγωγο επί του K, τότε υπάρχουν πολυώνυμα $g, h \in K[x]$ με $0 < \deg f, \deg g < n$ έτσι, ώστε $f = gh$. Έτσι, εφαρμόζοντας την υπόθεση της επαγωγής στα g και h παίρνουμε το αποτέλεσμα.

Ας είναι υποθέσουμε τώρα ότι το f είναι ανάγωγο και $\deg f = n$. Τότε, σύμφωνα με την Πρόταση 5.34, ο δακτύλιος $L = K[x]_f$ είναι σώμα. Το K είναι υπόσωμα του $K[x]_f$ και το x είναι μία ρίζα του f μέσα στο L. Οπότε, υπάρχει πολυώνυμο $g \in L[T]$ έτσι, ώστε $f = (T - \rho)g$. Καθώς $\deg g < n$, τότε, σύμφωνα με την υπόθεση της επαγωγής, το L είναι υπόσωμα ενός πεπερασμένου σώματος M στο οποίο το g αναλύεται σε γινόμενο γραμμικών παραγόντων και κατά συνέπεια το ίδιο συμβαίνει και για το f. □

Απόδειξη του Θεωρήματος 5.2. Θεωρούμε το πολυώνυμο $\Pi = x^{p^n} - x$ επί του σώματος $\mathbb{Z}_p$. Σύμφωνα με το Λήμμα 5.2, υπάρχει ένα πεπερασμένο σώμα K στο οποίο το Π αναλύεται σε γινόμενο γραμμικών παραγόντων. Καθώς η παράγωγος του Π είναι το πολυώνυμο

$$\Pi' = p^n x^{p^n-1} - 1 = -1 \neq 0,$$

η Πρόταση 4.21 δίνει ότι το Π έχει p^n διαφορετικές ρίζες. Ας είναι M το σύνολο των ριζών του Π. Από την απόδειξη του Θεωρήματος 5.6 έχουμε ότι το M είναι ένα υπόσωμα του K. Άρα το M είναι ένα σώμα με p^n στοιχεία. □

Πόρισμα 5.19 *Για κάθε πρώτο p και κάθε θετικό ακέραιο n υπάρχει ανάγωγο πολυώνυμο βαθμού n επί του $\mathbb{F}_p$.*

Απόδειξη. Σύμφωνα με το Θεώρημα 5.7, υπάρχει ένα πεπερασμένο σωμα K με p^n στοιχεία και από το Θεώρημα 5.6 έχουμε $K = \mathbb{Z}_p[x]_f$, όπου f είναι το ελάχιστο πολυώνυμο ενός γεννήτορα της ομάδας K^*. Τότε, το f είναι ένα ανάγωγο πολυώνυμο βαθμού n. □

Τέλος, θα δείξουμε ότι ουσιαστικά για κάθε πρώτο p και θετικό ακέραιο n υπάρχει ένα ακριβώς σώμα με p^n στοιχεία.

Θεώρημα 5.8 *Αν K_1 και K_2 είναι δύο σώματα με p^n στοιχεία, τότε $K_1 \cong K_2$.*

Απόδειξη. Σύμφωνα με το Πόρισμα 5.19 υπάρχει ένα ανάγωγο πολυώνυμο f βαθμού n επί του $\mathbb{Z}_p$. Από την Πρόταση 5.34, έχουμε ότι ο δακτύλιος $L = \mathbb{Z}_p[x]_f$ είναι σώμα με p^n στοιχεία. Το f είναι το ελάχιστο πολυώνυμο του x και $x^{p^n} = x$ μέσα στο L. Συμβολίζουμε με T την μεταβλητή των πολυωνύμων πάνω από το L. Έτσι, έχουμε $f|T^{p^n} - T$.

Από την άλλη πλευρά, ας είναι K ένα σώμα με p^n στοιχεία. Καθώς το K είναι το σύνολο των ριζών του $T^{p^n} - T$ και $f|T^{p^n} - T$, υπάρχει $a \in K$ με $f(a) = 0$. Οπότε το f είναι το ελάχιστο πολυώνυμο του a και επομένως $\mathbb{Z}_p(a) \cong L$. Έτσι, έχουμε $|\mathbb{Z}_p(a)| = p^n$ και κατά συνέπεια $K = \mathbb{Z}_p(a)$. Άρα $K \cong L$. Συνεπώς, δύο οποιαδήποτε σώματα με p^n στοιχεία είναι ισόμορφα. □

Ας είναι p ένας πρώτος αριθμός και n ένας θετικός ακέραιος. Θέτουμε $q = p^n$. Θα συμβολίζουμε με $\mathbb{F}_q$ το μοναδικό σώμα (κατά προσέγγιση ισομορφίας) με q στοιχεία. Έτσι, θα συμβολίζουμε το σώμα $\mathbb{Z}_p$ και με $\mathbb{F}_p$.

Καλούμε *πρωτογενή ρίζα της μονάδας* στο $\mathbb{F}_q$ κάθε γεννήτορα της κυκλικής ομάδας $\mathbb{F}_q^*$.

Ας είναι a μία πρωτογενής ρίζα της μονάδας στο $\mathbb{F}_q$ και

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

το ελάχιστο πολυώνυμό της. Τότε $\mathbb{F}_q = \{0, 1, a, \ldots, a^{p^n-2}\}$. Καθώς $f(a) = 0$, έχουμε:

$$a^n = -a_{n-1}a^{n-1} - \cdots - a_1 a - a_0.$$

Πολλαπλασιάζοντας και τα δύο μέλη της παραπάνω ισότητας με a, παίρνουμε:

$$a^{n+1} = -a_{n-1}a^n - \cdots - a_1a^2 - a_0a.$$

Αντικαθιστώντας το a^n με το ίσο του, έχουμε:

$$a^{n+1} = a_{n-1}(a_{n-1}a^{n-1} + \cdots + a_1a + a_0) - \cdots - a_1a^2 - a_0a.$$

Άρα:

$$a^{n+1} = -b_{n-1}a^{n-1} - \cdots - b_1a - b_0,$$

όπου

$$b_{n-1} = a_{n-2} - a_{n-1}^2, \ldots, b_1 = a_0 - a_{n-1}a_1, b_0 = a_{n-1}a_0.$$

Συνεχίζοντας μ΄ αυτό τον τρόπο, μπορούμε να εκφράσουμε τα στοιχεία $a^{n+2}, \ldots, a^{p^n-2}$ ως γραμμικούς συνδυασμούς με στοιχεία από το $\mathbb{F}_p$.

Για να υπολογίσουμε το άθροισμα $a^i + a^j$, αρκεί να υπολογίσουμε το άθροισμα των αντίστοιχων συντελεστών των εκφράσεων a^i και a^j ως γραμμικών συνδυασμών των $1, a, \ldots, a^{n-1}$. Για το γινόμενο των a^i και a^j, έχουμε $a^ia^j = a^r$, όπου r είναι το υπόλοιπο της διαίρεσης του $i + j$ με το $p^n - 1$ (γιατί για κάθε $x \in \mathbb{F}_q \setminus \{0\}$ ισχύει $x^{p^n-1} = 1$).

Παράδειγμα 5.21 Θα κατασκευάσουμε το σώμα $\mathbb{F}_8$. Θα χρειαστούμε ένα κανονικό ανάγωγο πολυώνυμο βαθμού 3 επί του $\mathbb{F}_2$. Ας θεωρήσουμε το πολυώνυμο $f = x^3 + x + 1$. Καθώς $f(0) = f(1) = 1$, το f δεν έχει ρίζες επί του $\mathbb{F}_2$ και επομένως είναι ανάγωγο. Το σώμα $\mathbb{F}_2[x]_f$ αποτελείται από τα στοιχεία

$$0,\ 1,\ x,\ x^2,\ 1+x,\ 1+x+x^2,\ x+x^2,\ 1+x^2.$$

Επίσης, έχουμε:

$$\begin{aligned} x^3 &= x+1, \\ x^4 &= x^2+x, \\ x^5 &= x^3+x^2 = x^2+x+1, \\ x^6 &= x^3+x^2+x = x^2+1, \\ x^7 &= x^3+x = 1. \end{aligned}$$

Συνεπώς, το x είναι πρωτογενής ρίζα της μονάδας στο $\mathbb{F}_8$.

5.8 Ασκήσεις

1. Να υπολογιστεί το υπόλοιπο της διαίρεσης του $12^{23}19^{37}$ με το 8.

2. Ας είναι $a, b, k \in \mathbb{Z}$ με $k \neq 0$ και $d = \mu\kappa\delta(n, k)$. Να δειχθεί ότι:

$$ka \equiv kb \pmod{n} \iff a \equiv b \pmod{n/d}.$$

3. Ας είναι a και b ακέραιοι που δεν διαιρούνται από το 3. Να δειχθεί ότι ο ακέραιος $a^2 + b^2$ δεν είναι τέλειο τετράγωνο ακεραίου.

4. Να δειχθεί ότι για κάθε ακέραιο n ισχύει:

$$2730 | n^{13} - n.$$

5. Να δειχθεί ότι ο αριθμός

$$\frac{7 \cdot 1968^{1968} - 3 \cdot 68^{78}}{10}$$

είναι ακέραιος.

6. Ας είναι f μία πολλαπλασιαστική συναρτηση. Να δειχθεί ότι η συνάρτηση F που ορίζεται από τη σχέση

$$F(n) = \sum_{d|n} f(d),$$

για κάθε ακέραιο $n > 0$, είναι πολλαπλασιαστική.

7. Να βρεθεί η ενελικτική αντίστροφος της συνάρτησης μ.

8. Ας είναι f και g είναι αριθμητικές συναρτησεις. Να δειχθεί ότι για κάθε θετικό ακέραιο n ισχύει:

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) g(n/d).$$

9. Να δειχθεί ότι για κάθε θετικό ακέραιο n ισχύουν τα εξής:

$$\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d} \tau(d), \quad \sum_{d|n} \frac{n}{d} \sigma(d) = \sum_{d|n} d\tau(d).$$

10. Ας είναι p περιττός πρώτος και $S = (p-1)/2$. Να δειχθεί ότι $S!^2 \equiv -1 \pmod{p}$ αν $p \equiv 1 \pmod{4}$ και $S!^2 \equiv 1 \pmod{p}$ αν $p \equiv 3 \pmod{4}$.

11. Ας είναι p περιττός πρώτος. Να δειχθεί ότι η πολυωνυμική ισοτιμία $x^2 + 1 \equiv 0 \pmod{p}$ έχει λύση αν και μόνον αν $p \equiv 1 \pmod{4}$.

12. Να λυθούν οι γραμμικές ισοτιμίες:

$$21x \equiv 12 \pmod{33}, \quad 7x \equiv 17 \pmod{120}, \quad -671 \equiv 121 \pmod{737}.$$

13. Να λυθούν τα παρακάτω συστήματα γραμμικών ισοτιμιών:
(α) $x \equiv 12 \pmod{17}$, $x \equiv 5 \pmod{21}$, $x \equiv 11 \pmod{25}$.
(β) $x \equiv 4 \pmod{5}$, $x \equiv -27 \pmod{22}$, $x \equiv -31 \pmod{39}$.
(γ) $3x \equiv 15 \pmod{55}$, $x \equiv 7 \pmod{23}$, $x \equiv 11 \pmod{31}$.

14. Να δειχθεί ότι το σύστημα γραμμικών ισοτιμιών:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}$$

έχει λύση αν και μόνον αν ισχύει $\mu\kappa\delta(n_1, n_2) | b_1 - b_2$. Σ' αυτή την περίπτωση, το σύστημα έχει μοναδική λύση $x \equiv x_0 \pmod{\epsilon\kappa\pi(n_1, n_2)}$.

15. Ας είναι $a, b, n \in \mathbb{Z}$ με $\mu\kappa\delta(a, n) = \mu\kappa\delta(b, n) = 1$. Αν ισχύει $\mu\kappa\delta(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1$, τότε να δειχθεί ότι

$$\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\mathrm{ord}_n(b).$$

16. Ας είναι $n, a, b \in \mathbb{Z}$ με $n > 1$ και $ab \equiv 1 \pmod{n}$. Να δειχθεί ότι $\mathrm{ord}_n(a) = \mathrm{ord}_n(b)$.

17. Ας είναι $m, n \in \mathbb{Z}$ με $m > 1$, $n > 1$ και $\mu\kappa\delta(m, n) = 1$. Να δειχθεί ότι:

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

18. Ας είναι d και n θετικοί ακέραιοι με $d|n$. Να δειχθεί ότι $\phi(d)|\phi(n)$.

19. Ας είναι $a, n \in \mathbb{Z}$ με $n > 2$ και $\mu\kappa\delta(a, n) = 1$. Να δειχθεί ότι ο a είναι αρχική ρίζα κατά μέτρο n αν και μόνον αν για κάθε πρώτο διαιρέτη p του $\phi(n)$ ισχύει

$$a^{\phi(n)/p} \not\equiv 1 \pmod{n}.$$

20. Να βρεθούν όλες οι αρχικές ρίζες κατά μέτρο 49.

21. Ας είναι p πρώτος > 2, r ακέραιος > 0 και a ακέραιος με $p \not| a$. Να δειχθεί ότι η τετραγωνική ισοτιμία $x^2 \equiv a \pmod{p^r}$ έχει λύση αν και μόνον αν η $x^2 \equiv a \pmod{p}$ έχει λύση. Σ′ αυτή την περίπτωση η ισοτιμία $x^2 \equiv a \pmod{p^r}$ έχει δύο ακριβώς λύση.

22. Ας είναι a ένας περιττός ακέραιος και r ακέραιος ≥ 3. Να δειχθεί ότι η τετραγωνική ισοτιμία $x^2 \equiv a \pmod{2^r}$ έχει λύση αν και μόνον αν $a \equiv 1 \pmod{8}$. Σ′ αυτή την περίπτωση η ισοτιμία έχει ακριβώς 4 λύσεις.

23. Ας είναι n θετικός ακέραιος και ας υποθέσουμε ότι η πρωτογενής ανάλυση του, $n = p_1^{a_1} \cdots p_k^{a_k}$, είναι γνωστή, καθώς και για κάθε $i = 1, \ldots, k$, η πρωτογενής ανάλυση του $p_i - 1$ είναι γνωστή. Να κατασκευαστεί ένας αλγόριθμος πολυωνυμικού χρόνου ως προς $\log n$, για τον υπολογισμό της ποσότητας $\mathrm{ord}_p(a)$, όπου $a \in \mathbb{Z}_n^*$.

24. Ας είναι p πρώτος ≥ 7. Να δειχθεί ότι ισχύουν τα εξής:
(α) Αν $p = 4q + 1$ και q πρώτος > 2, τότε ο 2 είναι αρχική ρίζα κατά μέτρο p.
(β) Αν $p = 2q + 1$ και q πρώτος της μορφής $4k + 1$, τότε ο 2 είναι αρχική ρίζα κατά μέτρο p.
(γ) Αν $p = 2q + 1$ και q πρώτος της μορφής $4k - 1$, τότε ο -2 είναι αρχική ρίζα κατά μέτρο p.

25. Ας είναι p ένας πρώτος του Fermat. Να δειχθούν τα εξής:
(α) Να δειχθεί ότι κάθε ακέραιος $a \in \{1, \ldots, p - 1\}$ με $(a/p) = -1$ είναι αρχική ρίζα κατά μέτρο p.
(β) Να δειχθεί ότι ο 5 είναι αρχική ρίζα κατά μέτρο p, για $p \neq 5$.
(γ) Να δειχθεί ότι ο 7 είναι αρχική ρίζα κατά μέτρο p, για $p \neq 3$.

26. Ας είναι p πρώτος > 2. Να δειχθεί ότι ισχύει:

$$(3/p) = \begin{cases} 1, & \text{αν} \quad p \equiv \pm 1 \pmod{12}, \\ -1, & \text{αν} \quad p \equiv \pm 5 \pmod{12}. \end{cases}$$

27. Ας είναι p πρώτος > 2. Να δειχθεί ότι ισχύει:

$$\sum_{a=1}^{p-1} (a/p) = 0.$$

28. Να βρεθούν οι λύσεις των παρακάτω τετραγωνικών ισοτιμιών:

$$x^2 - 6x - 13 \equiv 0 \pmod{127}, \quad x^2 + 6x - 154 \equiv 0 \pmod{399}.$$

29. Να δειχθεί ότι αν p είναι ένας πρώτος διαιρέτης του M_q, τότε $p \equiv \pm 1 \pmod 8$ και $p \equiv 1 \pmod q$.

30. Να υπολογιστουν τα σύμβολα του Jacobi:

$$(102/231),\ (131/1999),\ (1704/3535),\ (2166/31625).$$

31. Ας είναι n περιττός θετικός ακέραιος. Να δειχθεί ότι ισχύει:

$$(6/n) = \begin{cases} 1, & \text{αν} \quad n \equiv \pm 1, \pm 5 \pmod{24}, \\ -1, & \text{αν} \quad n \equiv \pm 7, \pm 11 \pmod{24}. \end{cases}$$

32. Να λυθεί η τετραγωνική ισοτιμία:

$$x^2 + 4322 \equiv 0 \pmod{10961}.$$

33. Να κατασκευαστούν τα σώματα $\mathbb{F}_{16}$, $\mathbb{F}_{25}$ και να προσδιοριστεί από μία πρωτογενή ρίζα της μονάδας σε καθένα από αυτά.

Βιβλιογραφία

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, 1976.

[2] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications,* Cambridge University Press 1986.

[3] V. Shoup, *Μία Υπολογιστική Εισαγωγή στη Θεωρία Αριθμών και την Άλγεβρα,* Εκδόσεις Κλειδάριθμος 2007.

[4] Y. Wang, On the least primitive root of a prime, *Scientia Sinica,* 10(1), (1961), 1-14.

[5] Δ. Πουλάκης, *Θεωρία Αριθμών,* Θεσσαλονίκη, Εκδόσεις Ζήτη 2001.

Κεφάλαιο 6

Πιστοποίηση Πρώτου

Σύνοψη
Σ′ αυτό το κεφάλαιο θα περιγράψουμε μερικές κλασικές μεθόδους πιστοποίησης πρώτου βασισμένων επί των θεωρημάτων των Lucas, Pocklington, τη μέθοδο του Fermat, των Solovay-Strassen και των Miller-Rabin. Τέλος, θα μελετήσουμε τον αλγόριθμο AKS, ο οποίος εφευρέθηκε στα 2002 από τους Ινδούς Μαθηματικούς M. Agrawal, N. Kayal και N. Saxena, και είναι πρώτος αιτιοκρατικός αλγόριθμος πολυωνυμικού χρόνου για πιστοποίηση πρώτου. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να συμβουλευτεί τις εξής πηγές: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Προαπαιτούμενη γνώση
Κεφάλαια 1,3,4 και 5.

6.1 Τα Κριτήρια των *Lucas* και *Pocklington*

Η πιο απλή και παλιά μέθοδος για την πιστοποίηση πρώτου βασίζεται στο Πόρισμα 3.1, σύμφωνα με το οποίο αν ένας ακέραιος $a > 1$ δεν έχει κανένα πρώτο διαιρέτη p, με $p \leq \sqrt{a}$, τότε ο a είναι πρώτος. Σύμφωνα όμως με την Παρατήρηση 3.1, η μέθοδος αυτή δεν είναι αποτελεσματική (ιδιαίτερα στη περίπτωση όπου ο a είναι ένας μεγάλος πρώτος).

Σ′ αυτή την ενότητα θα δώσουμε μερικά κλασικά κριτήρια πιστοποίησης πρώτου που βασίζονται σε βασικές ιδιότητες των ισοτιμιών. Θα αρχίσουμε με το παρακάτω θεώρημα που οφείλεται σε ιδέα του E. Lucas και διατυπώθηκε στα 1876.

Θεώρημα 6.1 *Ας είναι n ένας περιττός θετικός ακέραιος. Τότε ο n είναι πρώτος, αν και μόνον αν υπάρχει ακέραιος $a > 1$ τέτοιος, ώστε*

$$a^{n-1} \equiv 1 \pmod{n} \quad \textit{και} \quad a^{(n-1)/p} \not\equiv 1 \pmod{n}$$

για κάθε πρώτο διαιρέτη p του $n-1$.

Απόδειξη. Ας υποθέσουμε ότι ο n είναι πρώτος. Τότε οι παραπάνω σχέσεις ικανοποιούνται από μία αρχική ρίζα κατά μέτρο n. Αντίστροφα, ας υποθέσουμε ότι υπάρχει ακέραιος a που να ικανοποιεί αυτές τις σχέσεις. Τότε έχουμε $\mu\kappa\delta(a,n) = 1$ και $\mathrm{ord}_n(a) = n-1$. Οπότε $n-1 | \phi(n)$ και καθώς $\phi(n) \leq n-1$ έπεται $\phi(n) = n-1$, απ' όπου έπεται ότι ο n είναι πρώτος. □

Η παρούσα εκδοχή του θεωρήματος οφείλεται στον Lehmer. Ο Lucas το είχε διατυπώσει για κάθε θετικό διαιρέτη του $n-1$ στη θέση των πρώτων p.

Είναι δυνατόν να χρησιμοποιήσουμε αυτό το θεώρημα για να κατασκευάσουμε μεγάλους πρώτους. Θεωρούμε μερικούς γνωστούς πρώτους $p_1, \ldots, p_k$ και θετικούς ακέραιους $e_0, e_1, \ldots, e_k$. Θέτουμε

$$n = 1 + 2^{e_0} p_1^{e_1} \cdots p_k^{e_k}$$

και επιλέγοντας τυχαία έναν ακέραιο a ελέγχουμε αν οι υποθέσεις του παραπάνω θεωρήματος ικανοποιούνται. Αυτό είναι εύκολο γιατί γνωρίζουμε τους πρώτους p_i. Αν μετά από μερικές επιλογές του a βλέπουμε ότι οι υποθέσεις του θεωρήματος δεν ικανοποιούνται, τότε θεωρούμε έναν άλλο n.

Ο χρόνος που απαιτείται για τον υπολογισμό του $a^{n-1} \mod n$ είναι $O((\log n)^3)$. Επίσης, για τον υπολογισμό κάθε $a^{(n-1)/p} \mod n$ χρειάζεται χρόνος $O((\log n)^2(\log n/p))$. Καθώς το πλήθος των πρώτων διαιρετών του n είναι $O(\log n)$ έπεται ότι για κάθε a ο χρόνος που απαιτείται για να εφαρμόσουμε την παραπάνω διαδικασία είναι $O((\log n)^4)$. Ένα μειονέκτημα του κριτηρίου αυτού είναι ότι για την εφαρμογή του απαιτείται η γνώση όλων των πρώτων διαιρετών του $n-1$.

Παράδειγμα 6.1 Θεωρούμε τον ακέραιο

$$n = 1 + 2 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 101 = 11135251.$$

Για να εφαρμόσουμε το Θεώρημα 6.1 εκτελούμε τους εξής υπολογισμούς:

$$2^{n-1} \equiv 1 \pmod{n}, \quad 2^{(n-1)/2} \equiv -1 \pmod{n},$$

$$2^{(n-1)/3} \equiv 7009340 \pmod{n}, \quad 2^{(n-1)/5} \equiv 390964 \pmod{n},$$
$$2^{(n-1)/7} \equiv 6654420 \pmod{n}, \quad 2^{(n-1)/101} \equiv 6577006 \pmod{n}.$$

Έτσι, σύμφωνα με το Θεώρημα 5.1, ο ακέραιος 11135251 είναι πρώτος.

Στα 1877, ο Pepin έδωσε το εξής κριτήριο για τους αριθμούς του Fermat.

Πρόταση 6.1 *Ας είναι $F_n = 2^{2^n} + 1$ με $n \geq 2$ και k ακέραιος ≥ 2. Τότε ο F_n είναι πρώτος και $(k/F_n) = -1$ αν και μόνον αν ισχύει*

$$k^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Απόδειξη. Ας υποθέσουμε ότι ο F_n είναι πρώτος και $(k/F_n) = -1$. Από την Πρόταση 5.21 έπεται:

$$k^{(F_n-1)/2} \equiv (k/F_n) \equiv -1 \pmod{F_n}.$$

Αντίστροφα, ας υποθέσουμε ότι ισχύει η ισοτιμία

$$k^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Τότε έχουμε:

$$k^{F_n-1} \equiv 1 \pmod{F_n}$$

και, καθώς ο μόνος πρώτος που διαιρεί τον $F_n - 1 = 2^{2^n}$ είναι ο 2, το Θεώρημα 6.1 συνεπάγεται ότι ο F_n είναι πρώτος. Επιπλέον, έχουμε:

$$(k/F_n) \equiv k^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \quad \square$$

Παρατήρηση 6.1 Μπορούμε να εφαρμόσουμε το παραπάνω κριτήριο για $k = 3, 5, 10$. Πράγματι, έχουμε:

$$F_n \equiv 2 \pmod{3}, \quad F_n \equiv 2 \pmod{5}, \quad F_n \equiv 1 \pmod{8}$$

και επομένως χρησιμοποιώντας τον νόμο της τετραγωνικής αμοιβαιότητας για το σύμβολο του Jacobi και την Πρόταση 5.22 παίρνουμε:

$$(3/F_n) = (F_n/3) = (2/3) = -1,$$
$$(5/F_n) = (F_n/5) = (2/5) = -1,$$
$$(10/F_n) = (2/F_n)(5/F_n) = -1.$$

Ο Lucas χρησιμοποίησε το παραπάνω κριτήριο για να αποδείξει ότι ο αριθμός του Fermat F_6 είναι σύνθετος. Αργότερα, στα 1880, ο Landry βρήκε την παραγοντοποίηση του F_6:

$$F_6 = 274177 \times 67280421310721.$$

Η παρακάτω πρόταση που συνδέει τους πρώτους της Germain με τους αριθμους του Mersenne διατυπώθηκε στα 1750 από τον Euler και αποδείχθηκε στα 1775 από τον Lagrange και στα 1878 από τον Lucas με τη χρήση του κριτηρίου του.

Πρόταση 6.2 *Ας είναι q ένας πρώτος με $q \equiv 3 \pmod 4$. Τότε ο $2q+1$ διαιρεί τον αριθμό του Mersenne M_q αν και μόνον αν ο $2q+1$ είναι πρώτος της Germain. Σ' αυτή την περίπτωση αν $q > 3$, τότε ο M_q είναι σύνθετος.*

Απόδειξη. Ας υποθέσουμε ότι ο ακέραιος $n = 2q+1$ διαιρεί τον M_q. Έχουμε:

$$(-2)^{(n-1)/q} \equiv 2^2 \not\equiv 1 \pmod n,$$
$$(-2)^{(n-1)/2} \equiv (-2)^q \equiv -1 \not\equiv 1 \pmod n,$$
$$(-2)^{n-1} - 1 \equiv 2^{2q} - 1 \equiv (2^q+1)M_q \equiv 0 \pmod n.$$

Επομένως, από το Θεώρημα 6.1 έπεται ότι ο n είναι πρώτος.

Αντίστροφα, ας υποθέσουμε ότι ο ακέραιος $p = 2q+1$ είναι πρώτος. Καθώς $p \equiv 7 \pmod 8$, από το Πόρισμα 5.16 έχουμε $(2/p) = -1$ και επομένως υπάρχει ακέραιος m τέτοιος, ώστε $2 \equiv m^2 \pmod p$. Έτσι, έχουμε:

$$2^q \equiv 2^{(p-1)/2} \equiv m^{p-1} \equiv 1 \pmod p,$$

απ' όπου προκύπτει $p|M_q$. Αν $q > 3$, τότε $M_q = 2^q - 1 > 2q+1 = p$ και επομένως ο M_q είναι σύνθετος. □

Παρατήρηση 6.2 Παρατηρούμε ότι αν $q = 11, 23, 83, 131, 179, 191, 239, 251$, τότε ο M_q έχει παράγοντα τον $23, 47, 167, 263, 359, 383, 479, 503$, αντίστοιχα.

Για την εφαρμογή του Θεωρήματος 6.1 είναι αναγκαίο να γνωρίζουμε όλους τους πρώτους παράγοντες του $n-1$. Στα 1914, ο Pocklington έδωσε το παρακάτω κριτήριο για την εφαρμογή του οποίου είναι αναγκαίο να γνωρίζουμε μέρος μόνο της παραγοντοποίησης του $n-1$.

Θεώρημα 6.2 *Ας είναι n ένας περιττός θετικός ακέραιος. Ας υποθέσουμε ότι $n-1 = fr$, όπου f, r είναι ακέραιοι με $f > 1$, $\mu\kappa\delta(f,r) = 1$ και η πρωτογενής ανάλυση του f είναι γνωστή. Αν υπάρχει ακέραιος $a > 1$ ο οποίος να ικανοποιεί τις σχέσεις:*

$$a^{n-1} \equiv 1 \pmod{n} \quad \textit{και} \quad \mu\kappa\delta(a^{(n-1)/q} - 1, n) = 1,$$

για κάθε πρώτο διαιρέτη q του f, τότε για κάθε πρώτο διαιρέτη p του n ισχύει $p \equiv 1 \pmod{f}$.

Απόδειξη. Από την πρώτη ισοτιμία της υπόθεσης έχουμε $\mu\kappa\delta(a,n) = 1$. Ας είναι p ένας πρώτος διαιρέτης του n. Τοτε έχουμε:

$$(a^r)^f \equiv a^{n-1} \equiv 1 \pmod{n}$$

και επομένως $\mathrm{ord}_p(a^r) | f$. Απο την δεύτερη σχέση της υπόθεσης έπεται ότι $\mathrm{ord}_p(a^r) = f$. Άρα $f | p-1$ και κατά συνέπεια $p \equiv 1 \pmod{f}$. □

Πόρισμα 6.1 *Αν επιπλέον των υποθέσεων του Θεωρήματος 6.2, έχουμε $f > \sqrt{n}$, τότε ο n είναι πρώτος.*

Απόδειξη. Από το Θεώρημα 6.2 έχουμε ότι για κάθε πρώτο διαιρέτη p του n ισχύει $f | p-1$. Αν ο n είναι σύνθετος, τότε υπάρχει πρώτος διαιρέτη p του n με $p \leq \sqrt{n} < f$ που είναι άτοπο. Συνεπώς, ο n είναι πρώτος. □

Μία ενδιαφέρουσα συνέπεια του Πορίσματος 6.1 είναι το παρακάτω κριτήριο του Proth που διατυπώθηκε στα 1878.

Πόρισμα 6.2 *Ας είναι $n = 2^m h + 1$ με h περιττό και $2^m > h$. Αν υπάρχει ένας ακέραιος $a > 1$ τέτοιος, ώστε*

$$a^{(n-1)/2} \equiv -1 \pmod{n},$$

τότε ο n είναι πρώτος.

Απόδειξη. Έχουμε $n - 1 = 2^m h$ με h περιττό και $a^{n-1} \equiv 1 \pmod{n}$. Από την ισοτιμία της υπόθεσης, παίρνουμε $a^{(n-1)/2} = -1 + kn$, όπου k ακέραιος και επομένως ισχύει:

$$\mu\kappa\delta(a^{(n-1)/2} - 1, n) = \mu\kappa\delta(-2, n) = 1.$$

Έτσι, καθώς $2^m > h$, εφαρμόζοντας το Πόρισμα 6.1 με $f = 2^m$ και $r = h$, παίρνουμε ότι ο n είναι πρώτος. □

Παράδειγμα 6.2 Θα δείξουμε ότι ο ακέραιος $n = 18433$ είναι πρώτος χρησιμοποιώντας το Πόρισμα 6.2. Έχουμε $n = 2^{11}9+1$ και $2^{11} > 9$. Επιπλέον, ισχύει:

$$10^{(n-1)/2} \equiv 10^{9216} \equiv -1 \,(\mathrm{mod}\, n).$$

Έτσι, από το Πόρισμα 6.2 έπεται ότι ο n είναι πρώτος.

6.2 Αριθμοί του *Carmichael*

Μία από τις πλέον κλασικές μεθόδους για να διαπιστώσουμε ότι ένας θετικός ακέραιος είναι σύνθετος βασίζεται στο Πόρισμα 5.8. Έτσι, αν ο n είναι θετικός ακέραιος και βρεθεί ακέραιος a με

$$a^{n-1} \not\equiv 1 \pmod{n},$$

τότε ο n είναι σύνθετος. Η μέθοδος αυτή καλείται *κριτήριο του Fermat.*
Από την άλλη πλευρά, στη περίπτωση όπου έχουμε

$$a^{n-1} \equiv 1 \pmod{n}$$

δεν μπορούμε να συμπεράνουμε αν ο n είναι πρώτος ή σύνθετος.

Παράδειγμα 6.3 Έχουμε $91 = 13 \cdot 7$ και επομένως ο αριθμός 91 είναι σύνθετος. Καθώς ισχύει

$$2^{90} \equiv 64 \pmod{91},$$

το κριτήριο του Fermat για $a = 2$ αποδεικνύει ότι αριθμός 91 είναι σύνθετος. Από την άλλη πλευρά, ας σημειωθεί ότι για $a = 3$ ισχύει

$$3^{90} \equiv 1 \pmod{91}$$

και κατά συνέπεια το κριτήριο δεν δίνει αποτέλεσμα.

Ας είναι n ένας περιττός σύνθετος ακέραιος και a ακέραιος με

$$a^{n-1} \equiv 1 \pmod{n}.$$

Τότε ο n καλείται *ψευδοπρώτος του Fernat ως προς βάση* a. Για παράδειγμα, ο 91 είναι ψευδοπρώτος του Fermat ως προς βάση 3. Ο ακέραιος n καλείται *αριθμός του Carmichael* αν ο n είναι ψευδοπρώτος του Fermat ως προς βάση a, για κάθε ακέραιο a με $\mu\kappa\delta(a, n) = 1$. Σ′ αυτή την περίπτωση το κριτήριο του Fermat δεν ειναι δυνατόν να διαπιστώσει ότι ο n είναι σύνθετος.

Παράδειγμα 6.4 Από το Παράδειγμα 5.9 έχουμε ότι ο 561 είναι αριθμός του Carmichael.

Θεώρημα 6.3 *Ένας περιττός σύνθετος ακέραιος $n > 3$ είναι αριθμός του Carmichael, αν και μόνον αν ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει $p - 1|n - 1$.*

Απόδειξη. Ας υποθέσουμε ότι ο n είναι αριθμός του Carmichael. Θα δείξουμε πρώτα ότι ο n είναι ελεύθερος τετραγώνου. Πράγματι, αν υπάρχει πρώτος p τέτοιος, ώστε $n = p^2m$, όπου m ακέραιος, τότε έχουμε $1 + pm \not\equiv 1 \,(\mathrm{mod}\, n)$ και

$$(1 + pm)^p \equiv 1 \,(\mathrm{mod}\, n),$$

απ΄ όπου έχουμε $\mathrm{ord}_n(1 + pm) = p$. Από την άλλη πλευρά, επειδή ο n είναι αριθμός του Carmichael, ισχύει:

$$(1 + pm)^{n-1} \equiv 1 \,(\mathrm{mod}\, n).$$

Έτσι, έχουμε $p|n - 1$ που είναι άτοπο. Άρα, $n = p_1 \cdots p_k$, όπου $p_1, \ldots, p_k$ είναι διαφορετικοί ανά δύο πρώτοι. Ας είναι g_i πρωτογενής ρίζα κατά μέτρο p_i $(i = 1, \ldots, k)$. Τότε, από την Πρόταση 5.11 έπεται ότι υπάρχει ακέραιος g τέτοιος, ώστε

$$g \equiv g_i \,(\mathrm{mod}\, p_i) \quad (i = 1, \ldots, k).$$

Καθώς ο n είναι αριθμός του Carmichael, έχουμε

$$g^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$$

και έτσι παίρνουμε

$$g_i^{n-1} \equiv g^{n-1} \equiv 1 \,(\mathrm{mod}\, p_i) \quad (i = 1, \ldots, k),$$

απ΄ όπου έπεται $p_i - 1|n - 1$ $(i = 1, \ldots, k)$ γιατί ο g_i είναι πρωτογενής ρίζα κατά μέτρο p_i.

Αντίστροφα, ας υποθέσουμε ότι ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει $p - 1|n - 1$. Ας είναι a ακέραιος με $\mu\kappa\delta(a, n) = 1$. Αν p είναι πρώτος διαιρέτης του n, τότε

$$a^{p-1} \equiv 1 \ (\mathrm{mod}\ p)$$

και καθώς $p-1|n-1$, έχουμε

$$a^{n-1} \equiv 1 \pmod{p}.$$

Τέλος, επειδή ο n είναι ελεύθερος τετραγώνου, ισχύει:

$$a^{n-1} \equiv 1 \pmod{n}. \quad \square$$

Πόρισμα 6.3 *Ένας αριθμός του Carmichael έχει τουλάχιστον τρείς πρώτους παράγοντες.*

Απόδειξη. Ας είναι n ένας αριθμός του Carmichael. Τότε ο n είναι σύνθετος. Ας υποθέσουμε ότι $n = pq$, όπου p, q είναι πρώτοι με $p > q$. Από το Θεώρημα 6.3 έχουμε $p-1|n-1$. Καθώς $n-1 = (p-1)q+q-1$, παίρνουμε $p-1|q-1$ και επομένως $p \leq q$ που είναι άτοπο. Άρα, ο n έχει τουλάχιστον τρείς πρώτους παράγοντες. $\square$

Παράδειγμα 6.5 Αν t είναι ακέραιος τέτοιος, ώστε οι αριθμοί $6t+1$, $12t+1$ και $18t+1$ είναι πρώτοι, τότε, σύμφωνα με το Θεώρημα 6.3, ο ακέραιος

$$n = (6t+1)(12t+1)(18t+1)$$

είναι ένας αριθμός του Carmichael. Για $t = 1$ παίρνουμε τον αριθμό $1729 = 7 \cdot 13 \cdot 19$ ο οποίος έχει αυτή την ιδιότητα.

6.3 Κριτήριο των *Solovay – Strassen*

Μία άλλη μέθοδος για να διαπιστώσουμε αν ένας αριθμός είναι σύνθετος βασίζεται στη Πρόταση 5.21(α). Σύμφωνα με αυτή την πρόταση, αν n είναι ένας θετικός περιττός ακέραιος, a ένας ακέραιος πρώτος προς τον n και ισχύει

$$(a/n) \not\equiv a^{(n-1)/2} \pmod{n},$$

τότε ο n είναι σύνθετος. Στη περίπτωση όμως που ισχύει

$$(a/n) \equiv a^{(n-1)/2} \pmod{n}$$

δεν μπορούμε να συμπεράνουμε αν ο n είναι πρώτος ή σύνθετος. Η παραπάνω σχέση μας δίνει ένα τρόπο για να διαπιστώνουμε αν ένας αριθμός είναι σύνθετος, ακόμη και στη περίπτωση όπου n είναι ένας αριθμός του Carmichael, όπως δείχνει το παρακάτω παράδειγμα. Η μέθοδος αυτή καλείται *Κριτήριο των Solovay – Strassen*.

Παράδειγμα 6.6 Σύμφωνα με το Παράδειγμα 6.4, ο 561 είναι ένας αριθμός του Carmichael. Χρησιμοποιώντας την Πρόταση 5.23 παίρνουμε:

$$(5/561) = (-1)^{(561-1)(5-1)/4}(561/5) = 1.$$

Από την άλλη πλευρά, υπολογίζουμε:

$$5^{(561-1)/2} \equiv 5^{280} \equiv 67 \pmod{561}.$$

Καθώς έχουμε $67 \not\equiv 1 \pmod{561}$, έπεται ότι ο 561 είναι σύνθετος.

Ας είναι n ένας περιττός σύνθετος ακέραιος > 1 και a ακέραιος με $\mu\kappa\delta(a, n) = 1$ τέτοιος, ώστε

$$(a/n) \equiv a^{(n-1)/2} \pmod{n}.$$

Τότε ο n καλείται *ψευδοπρώτος του Euler ως προς βάση* a. Παρατηρούμε αμέσως ότι αν n είναι ένας ψευδοπρώτος του Euler ως προς βάση a, τότε έχουμε

$$a^{n-1} \equiv (a/n)^2 \equiv 1 \pmod{n}$$

και επομένως ο n είναι ένας ψευδοπρώτος του Fermat ως προς βάση a.

Παράδειγμα 6.7 Θεωρούμε τον ακέραιο $15841 = 7 \cdot 31 \cdot 73$. Από την Πρόταση 5.22 έχουμε $(2/15841) = 1$. Από την άλλη πλευρά, θα δείξουμε ότι

$$2^{(15841-1)/2} \equiv 2^{7920} \equiv 1 \pmod{15841}.$$

Έχουμε $6|7920$, $30|7920$, $72|7920$ και επομένως ισχύουν

$$2^{7920} \equiv 1 \pmod{7}, \quad 2^{7920} \equiv 1 \pmod{31}, \quad 2^{7920} \equiv 1 \pmod{73},$$

απ΄ όπου παίρνουμε

$$2^{7920} \equiv 1 \pmod{15841}.$$

Συνεπώς, ο 15841 είναι ένας ψευδοπρώτος του Euler ως προς βάση 2.

Σύμφωνα με την επόμενη πρόταση, αν ο n είναι ένας περιττός σύνθετος ακέραιος > 1, τότε υπάρχει ακέραιος a με $\mu\kappa\delta(a, n) = 1$ τέτοιος, ώστε ο n δεν είναι ψευδοπρώτος του Euler ως προς βάση a. Έτσι, το κριτήριο των Solovay-Strassen εφαρμοζόμενο επί του a δείχνει ότι ο n είναι σύνθετος.

Πρόταση 6.3 *Ας είναι $n \geq 3$ ένας περιττός ακέραιος. Αν για κάθε ακέραιο a με $\mu\kappa\delta(a,n) = 1$ ισχύει*

$$(a/n) \equiv a^{(n-1)/2} \pmod{n},$$

τότε ο n είναι πρώτος.

Απόδειξη. Αν n είναι ένας πρώτος αριθμός, τότε από την Πρόταση 5.21 έχουμε ότι για κάθε ακέραιο a με $\mu\kappa\delta(a,n) = 1$ ισχύει η παραπάνω ισοτιμία. Αντίστροφα, ας υποθέσουμε ότι ισχύει αυτή η ισοτιμία και ότι ο n δεν είναι πρώτος. Τότε για κάθε ακέραιο a με $\mu\kappa\delta(a,n) = 1$ ισχύει

$$a^{n-1} \equiv (a/n)^2 \equiv 1 \pmod{n}$$

και επομένως ο n είναι αριθμός του Carmichael. Από το Θεώρημα 6.3 έχουμε ότι ο n είναι ελεύθερος τετραγώνου και επομένως $n = p_1 \cdots p_k$, όπου $p_1, \ldots, p_k$ $(k \geq 3)$ είναι διαφορετικοί ανά δύο πρώτοι. Επιλέγουμε ακεραίους $a_1, \ldots, a_k$ με $\mu\kappa\delta(a_i, p_i) = 1$ $(i = 1, \ldots, k)$ έτσι, ώστε

$$(a_1/p_1) \cdots (a_k/p_k) \not\equiv a_1^{(n-1)/2} \pmod{p_1}.$$

Σύμφωνα με την Πρόταση 5.11, υπάρχει ακέραιος a τέτοιος, ώστε

$$a \equiv a_i \pmod{p_i} \quad (i = 1, \ldots, k).$$

Από τις σχέσεις $\mu\kappa\delta(a_i, p_i) = 1$ $(i = 1, \ldots, k)$ παίρνουμε $\mu\kappa\delta(a,n) = 1$ και επομένως ισχύει

$$(a/n) \equiv a^{(n-1)/2} \pmod{n},$$

απ΄ όπου έχουμε

$$(a_1/p_1) \cdots (a_k/p_k) \equiv a_1^{(n-1)/2} \pmod{p_1},$$

που είναι άτοπο. Συνεπώς, ο n είναι πρώτος. □

Πρόταση 6.4 *Ας είναι $n \geq 3$ ένας περιττός σύνθετος ακέραιος και R το σύνολο των ακεραίων $a \in \mathbb{Z}_n^*$ οι οποίοι ικανοποιούν την ισοτιμία*

$$(a/n) \equiv a^{(n-1)/2} \pmod{n}.$$

Τότε ισχύει $|R| \leq \phi(n)/2$.

Απόδειξη. Από την Πρόταση 6.3 έχουμε ότι υπάρχει $b \in \mathbb{Z}_n^* \setminus R$. Συμβολίζουμε με bR το σύνολο των γινομένων $ba \mod n$ και θεωρούμε την απεικόνιση $f : R \to bR$ με $f(a) = ba \mod n$, για κάθε $a \in R$. Η f είναι προφανώς έφεση. Θα δείξουμε ότι είναι και ένεση. Πράγματι, αν $ba \equiv ba' \pmod n$, τότε πολλαπλασιάζοντας και τα δύο μέλη με το $b^{-1} \mod n$ παίρνουμε $a = a'$. Άρα, η f είναι αμφίεση και κατά συνέπεια ισχύει $|R| = |bR|$. Επίσης, εύκολα διαπιστώνουμε ότι τα στοιχεία του bR δεν ικανοποιούν την παραπάνω ισοτιμία και επομένως $R \cap bR = \emptyset$. Έτσι, παίρνουμε $2|R| \leq \phi(n)$. $\square$

Τα προηγούμενα αποτελέσματα δίνουν τον εξής πιθανοτικό Monte Carlo αλγόριθμο για να ελέγχουμε αν ένας αριθμός είναι πρώτος.

Αλγόριθμος 6.1 Αλγόριθμος των Solovay-Strassen.
Είσοδος: Περιττός ακέραιος $n > 3$ και θετικός ακέραιος $t \geq 1$.
Έξοδος: Η απάντηση "n σύνθετος" ή "n πιθανώς πρώτος".

1. Εκτελούμε τα παρακάτω το πολύ t φορές:
   (α′) Επιλέγουμε τυχαίο $a \in \{2, \ldots, n-1\}$ και υπολογίζουμε τον $\mu\kappa\delta(a, n)$.
   (β′) Αν $\mu\kappa\delta(a, n) > 1$, τότε επιστρέφουμε την απάντηση "n σύνθετος".
   (γ′) Διαφορετικά, υπολογίζουμε (a/n) και $a^{(n-1)/2} \mod n$.
   (δ′) Αν $(a/n) \not\equiv a^{(n-1)/2} \pmod n$, τότε επιστρέφουμε την απάντηση "n σύνθετος".
2. Σε κάθε άλλη περίπτωση, επιστρέφουμε την απάντηση "n πιθανώς πρώτος".

Στο Βήμα 1(α′) ο υπολογισμός του $\mu\kappa\delta(a, n)$ απαιτεί $O((\log n)^2)$ δυαδικές ψηφιακές πράξεις και στο Βήμα 1(γ′) ο υπολογισμός των (a/n) και $a^{(n-1)/2} \mod n$ χρειάζεται $O((\log n)^2)$ και $O((\log n)^3)$ δυαδικές ψηφιακές πράξεις, αντίστοιχα. Επομένως, ο χρόνος εκτέλεσης του αλγορίθμου είναι $O(t(\log n)^3)$ δυαδικές ψηφιακές πράξεις. Συνεπώς, για μικρές τιμές του t, π.χ. $t < \log n$, ο αλγόριθμος είναι πολυωνυμικού χρόνου.

Αν ισχύει $\mu\kappa\delta(a, n) > 1$ ή $(a/n) \not\equiv a^{(n-1)/2} \pmod n$, τότε ο n σύνθετος και επομένως ο αλγόριθμος δίνει ως έξοδο το σωστό αποτέλεσμα. Ας είναι R το σύνολο των ακεραίων $a \in \mathbb{Z}_n^*$ με $(a/n) \equiv$

$a^{(n-1)/2} \pmod n$. Ας υποθέσουμε ότι $a \in R$. Σύμφωνα με την Πρόταση 6.4, αν ο n είναι σύνθετος, τότε $|R| \leq \phi(n)/2$. Καθώς η επιλογή των αριθμών a είναι τυχαία, η πιθανότητα ο n να είναι σύνθετος και $a \in R$ είναι $\leq 1/2$. Επομένως στη περίπτωση όπου η εξόδος είναι "n πιθανώς πρώτος" και ο n είναι σύνθετος, έχουν χρησιμοποιηθεί t αριθμοί a οι οποίοι όλοι ανήκουν στο R. Η πιθανότητα αυτού του γεγονότος είναι $\leq 1/2^t$. Συνεπώς, η πιθανότητα ο n να είναι πρώτος είναι $\geq 1 - 1/2^t$.

6.4 Κριτήριο των $Miller - Rabin$

Σ′ αυτή την ενότητα θα δώσουμε ένα ισχυρότερο κριτήριο για να ελέγχουμε αν ένας ακέραιος είναι πρώτος. Το κριτήριο αυτό βασίζεται στη παρακάτω πρόταση.

Πρόταση 6.5 *Ας είναι n πρώτος και $n - 1 = 2^s d$, όπου d περιττός και s θετικός ακέραιος. Αν a είναι ένας ακέραιος ο οποίος δεν διαιρείται από τον n, τότε είτε ισχύει*

$$a^d \equiv 1 \pmod n$$

είτε υπάρχει $r \in \{0, 1, \ldots, s-1\}$ με

$$a^{2^r d} \equiv -1 \pmod n.$$

Απόδειξη. Ας είναι $k = \mathrm{ord}_n(a^d)$. Καθώς ο n είναι πρώτος, έχουμε

$$(a^d)^{2^s} \equiv 1 \pmod n$$

και επομένως ο k διαιρεί τον 2^s. Αν $k = 1$, τότε

$$a^d \equiv 1 \pmod n.$$

Αν $k > 1$, τότε $k = 2^l$ με $1 \leq l \leq s$ και επομένως $\mathrm{ord}_n(a^{2^{l-1}d}) = 2$. Από την άλλη πλευρά, μόνον η κλάση του -1 μέσα στο $\mathbb{Z}_n^*$ έχει τάξη ίση με 2 και κατά συνέπεια έχουμε

$$a^{2^{l-1}d} \equiv -1 \pmod n. \quad \square$$

Ας είναι n ένας περιττός ακέραιος $n > 1$. Για να διαπιστώσουμε αν είναι πρώτος εργαζόμαστε ως εξής: Γράφουμε $n-1 = 2^s d$, όπου d περιττός και s θετικός ακέραιος. Επιλέγουμε τυχαία $a \in \{2, \ldots, n-2\}$. Αν $\mu\kappa\delta(a,n) > 1$, τότε ο n είναι σύνθετος. Αν $\mu\kappa\delta(a,n) = 1$, τότε υπολογίζουμε τις δυνάμεις:

$$a^d \bmod n, a^{2d} \bmod n, \ldots, a^{2^{s-1}d} \bmod n.$$

Στη περίπτωση όπου

$$a^d \not\equiv \pm 1 \pmod{n} \quad \text{και} \quad a^{2^r d} \not\equiv -1 \pmod{n} \ (r = 1, \ldots, s-1),$$

η Πρόταση 6.5 συνεπάγεται ότι ο n είναι σύνθετος. Ο ακέραιος a καλείται *μάρτυρας* για την συνθετότητα του n. Η διαδικασία αυτή είναι γνωστή ως *Κριτήριο των Miller-Rabin.*

Παράδειγμα 6.8 Με το κριτήριο των Miller-Rabin θα δείξουμε ότι ο αριθμός του Carmichael 561 είναι σύνθετος. Έχουμε $n-1 = 560 = 2^4 35$. Κάνουμε τους υπολογισμούς:

$$2^{35} \equiv 263 \pmod{561}, \quad 2^{2\cdot 35} \equiv 166 \pmod{561},$$

$$2^{4\cdot 35} \equiv 67 \pmod{561}, \quad 2^{8\cdot 35} \equiv 1 \pmod{561}.$$

Οπότε, βλέπουμε ότι ο 2 είναι ένας μάρτυρας για την συνθετότητα του 561.

Ας είναι n περιττός σύνθετος ακέραιος > 0 και $b \in \{1, \ldots, n-1\}$ με $\mu\kappa\delta(b,n) = 1$. Γράφουμε $n = 2^s d + 1$, όπου d περιττός και s θετικός ακέραιος. Ο n καλείται *ισχυρός ψευδοπρώτος* ως προς βάση b αν ισχύει

$$b^d \equiv 1 \pmod{n}$$

ή υπάρχει $r \in \{0, 1, \ldots, s-1\}$ με

$$b^{2^r d} \equiv -1 \pmod{n}.$$

Παράδειγμα 6.9 Ο αριθμός 25 είναι ισχυρός ψευδοπρώτος ως προς βάση 7. Πράγματι, έχουμε $25 = 3 \cdot 2^3 + 1$ και $7^2 \equiv -1 \,(\mathrm{mod}\, 25)$, απ' όπου $7^{3\cdot 2} \equiv -1 \,(\mathrm{mod}\, 25)$. Έτσι, ο 25 είναι ισχυρός ψευδοπρώτος ως προς βάση 7.

Στη συνέχεια θα δείξουμε ότι το σύνολο των ισχυρών ψευδοπρώτων ως πρός βάση b είναι υποσύνολο του συνόλου των ψευδοπρώτων του Euler ως πρός βάση b.

Πρόταση 6.6 *Ας είναι n περιττός σύνθετος ακέραιος > 0 με $n \equiv 3 \pmod 4$ και $b \in \{1, \ldots, n-1\}$ με $\mu\kappa\delta(b, n) = 1$. Τότε ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b αν και μόνον αν ο n είναι ψευδοπρώτος του Euler ως προς βάση b.*

Απόδειξη. Καταρχήν παρατηρούμε ότι από την σχέση $n \equiv 3 \pmod 4$, έπεται $n = 2d + 1$, όπου d περιττός, και επομένως έχουμε ότι ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b αν και μόνον αν ισχύει:

$$b^{(n-1)/2} \equiv \pm 1 \pmod n.$$

Αν ο n είναι ψευδοπρώτος του *Euler* ως προς βάση b, τότε έχουμε:

$$b^{(n-1)/2} \equiv (b/n) = \pm 1 \pmod n.$$

Άρα, ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b. Αντίστροφα, ας υποθέσουμε ότι ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b. Τότε $b^{(n-1)/2} \equiv \pm 1 \pmod n$. Επίσης, καθώς $n \equiv 3 \pmod 4$, από την Πρόταση 5.22 έχουμε $(\pm 1/n) = \pm 1$. Έτσι, παίρνουμε:

$$\begin{aligned}(b/n) = (b/n)(b^{(n-3)/4}/n)^2 = \\ (b^{(n-1)/2}/n) = (\pm 1/n) = \pm 1 \equiv b^{(n-1)/2} \pmod n.\end{aligned}$$

Επομένως, ο n είναι ψευδοπρώτος του *Euler* ως προς βάση b. □

Πρόταση 6.7 *Ας είναι n περιττός σύνθετος ακέραιος > 0 και $b \in \{1, \ldots, n-1\}$ με $\mu\kappa\delta(b, n) = 1$. Αν ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b, τότε ο n είναι ψευδοπρώτος του Euler ως προς βάση b.*

Απόδειξη. Ας είναι $n - 1 = 2^s t$, όπου t περιττός και s θετικός ακέραιος. Πρώτα θεωρούμε την περίπτωση, όπου $b^t \equiv 1 \pmod n$. Αν p είναι ένας πρώτος διαιρέτης του n, τότε $\mathrm{ord}_p(b) | t$ και, καθώς ο t είναι περιττός, έχουμε ότι η τάξη $\mathrm{ord}_p(b)$ είναι περιττός αριθμός. Επομένως, ισχύει $b^{(p-1)/2} \equiv 1 \pmod p$ και από την Πρόταση 5.21 έπεται ότι $(b/p) = 1$. Άρα έχουμε $(b/n) = 1$. Από την άλλη πλευρά, παίρνουμε:

$$b^{(n-1)/2} \equiv (b^t)^{2^{s-1}} \equiv 1 \pmod n.$$

Έτσι, έχουμε $b^{(n-1)/2} \equiv (b/n) \pmod{n}$ και κατά συνέπεια ο n είναι ψευδοπρώτος του *Euler* ως προς βάση b.

Στη συνέχεια υποθέτουμε ότι υπάρχει $r \in \{0, 1, \ldots, s-1\}$ έτσι, ώστε $b^{2^r t} \equiv -1 \pmod{n}$. Ας είναι p ένας πρώτος διαιρέτης του n. Τότε έχουμε $b^{2^{r+1}t} \equiv 1 \pmod{p}$ και επομένως $\mathrm{ord}_p(b) | 2^{r+1}t$. Καθώς $b^{2^r t} \equiv -1 \pmod{p}$, συμπεραίνουμε ότι $\mathrm{ord}_p(b) = 2^{r+1}s$, όπου s ακέραιος με $1 \leq s \leq t$. Επίσης, ισχύει $2^{r+1}s | p-1$, απ΄ όπου $p = 2^{r+1}d + 1$, όπου d είναι θετικός ακέραιος. Τότε έχουμε:

$$(b/p) \equiv b^{(p-1)/2} \equiv$$
$$(b^{\mathrm{ord}_p(b)/2})^{(p-1)/\mathrm{ord}_p(b)} \equiv (-1)^{(p-1)/\mathrm{ord}_p(b)} \equiv (-1)^{d/s} \pmod{p}.$$

Καθώς ο s είναι περιττός, παίρνουμε $(b/p) = (-1)^d$.

Ας είναι $n = p_1^{h_1} \cdots p_m^{h_m}$ η πρωτογενής ανάλυση του n. Από τα παραπάνω έχουμε $p_i = 2^{r+1}d_i + 1$ $(i = 1, \ldots, m)$. Τότε:

$$n \equiv \prod_{i=1}^{m} (2^{r+1}d_i + 1)^{h_i} \equiv$$
$$\prod_{i=1}^{m} (1 + 2^{r+1}d_i h_i) \equiv 1 + 2^{r+1} \sum_{i=1}^{m} h_i d_i \pmod{2^{r+2}}.$$

Επομένως, ισχύει:

$$2^{s-1}t \equiv \frac{n-1}{2} \equiv 2^r \sum_{i=1}^{m} h_i d_i \pmod{2^{r+1}},$$

απ΄ όπου:

$$2^{s-1-r}t \equiv \sum_{i=1}^{m} h_i d_i \pmod{2}.$$

Επίσης, έχουμε:

$$b^{(n-1)/2} \equiv b^{2^{s-1}t} \equiv (b^{2^r t})^{2^{s-r-1}} \equiv (-1)^{2^{s-r-1}} \pmod{n}$$

και

$$(b/n) \equiv \prod_{i=1}^{m} (p_i/n)^{h_i} \equiv \prod_{i=1}^{m} (-1)^{d_i h_i} \equiv (-1)^{\sum_{i=1}^{m} h_i d_i} \pmod{n}.$$

Αν $r < s-1$, τότε $b^{(n-1)/2} \equiv 1 \pmod{n}$ και ο αριθμός $\sum_{i=1}^{m} h_i d_i$ είναι άρτιος. Έτσι, έχουμε $(b/n) \equiv b^{(n-1)/2} \pmod{n}$ και κατά συνέπεια ο n είναι ψευδοπρώτος του Euler ως πρός βάση b. Αν $r = s-1$,

τότε ο αριθμός $\sum_{i=1}^{m} h_i d_i$ είναι περιττός και $b^{(n-1)/2} \equiv -1 \pmod{n}$. Οπότε, συμπεραίνουμε επίσης ότι ο n είναι ψευδοπρώτος του Euler ως πρός βάση b. $\square$

Η παρακάτω πρόταση μας εξασφαλίζει την ύπαρξη ενός ικανοποιητικού πλήθους μαρτύρων της συνθετότητας ενός σύνθετου ακεραίου. Αυτό είναι σημαντικό για την απολεσματικότητα του κριτηρίου των Miller-Rabin.

Πρόταση 6.8 *Αν ο n είναι ένας περιττός σύνθετος, τότε το σύνολο $\{1, \ldots, n-1\}$ περιέχει το πολύ $(n-1)/4$ ακεραίους που είναι πρώτοι προς τον n και δεν είναι μάρτυρες της συνθετότητας του.*

Απόδειξη. Ας είναι b θετικός ακέραιος τέτοιος, ώστε ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b. Τότε ο b επαληθεύει την ισοτιμία

$$x^{n-1} \equiv 1 \pmod{n}.$$

Ας είναι $n = p_1^{h_1} \cdots p_k^{h_k}$ η πρωτογενής ανάλυση του n. Θέτουμε $d_i = \mu\kappa\delta(n-1, \phi(p_i^{h_i}))$ $(i = 1, \ldots, k)$. Εύκολα διαπιστώνουμε ότι $d_i = \mu\kappa\delta(n-1, p_i - 1)$. Τότε, από το Πόρισμα 5.14 έχουμε ότι το πλήθος των λύσεων της προηγούμενης πολυωνυμικής ισοτιμίας ισούται με $d_1 \cdots d_k$.

Θεωρούμε πρώτα την περίπτωση όπου $h_1 > 1$. Έχουμε:

$$\frac{p_1^{h_1}}{p_1 - 1} \geq \frac{p_1^2}{p_1 - 1} = p_1 + 1 + \frac{1}{p_1 - 1} > 4.$$

Τότε:

$$d_1 \cdots d_k \leq \prod_{i=1}^{k} (p_i - 1) < \frac{1}{4} p_1^{h_1} \prod_{i=2}^{k} p_i \leq \frac{n}{4},$$

απ΄ όπου προκύπτει το ζητούμενο.

Ας είναι τώρα $h_1 = \ldots = h_k = 1$. Θέτουμε

$$n - 1 = 2^s t, \quad p_i - 1 = 2^{s_i} t_i \ \ (i = 1, \ldots, k),$$

όπου οι ακέραιοι t, $t_1, \ldots, t_k$ είναι περιττοί και $s_1 \leq \cdots \leq s_k$. Τότε, ισχύει:

$$\mu\kappa\delta(n-1, p_i - 1) = 2^{\sigma_i} \tau_i \quad (i = 1, \ldots, k),$$

όπου $\sigma_i = \min\{s, s_i\}$ και $\tau_i = \mu\kappa\delta(t, t_i)$ $(i = 1, \ldots, k)$ και

$$\mu\kappa\delta(t, p_i - 1) = \mu\kappa\delta(t, t_i) = \tau_i \quad (i = 1, \ldots, k).$$

Έτσι, από το Πόρισμα 5.14 παίρνουμε ότι το πλήθος των λύσεων της πολυωνυμικής ισοτιμίας

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

είναι $\tau = \tau_1 \cdots \tau_k$.

Στη συνέχεια θεωρούμε την πολυωνυμική ισοτιμία

$$x^{2^r t} \equiv -1 \,(\mathrm{mod}\, n),$$

όπου r ακέραιος με $0 \leq r < s$. Έχουμε:

$$\mu\kappa\delta(2^r t, p_i - 1) = \mu\kappa\delta(2^r t, 2^{s_i} t_i) = 2^{\mu_i}\tau_i \quad (i = 1, \ldots, k),$$

όπου $\mu_i = \min\{r, s_i\}$. Από την Πρόταση 5.11 έχουμε ότι -1 είναι $2^r t$-οστό υπόλοιπο κατά μέτρο n αν και μόνον είναι $2^r t$-οστό υπόλοιπο κατά μέτρο p_i. Σύμφωνα όμως με την Πρόταση 5.20, αυτό συμβαίνει αν και μόνον αν ο $(p_i - 1)/2^{\mu_i}\tau_i$ είναι άρτιος. Καθώς $p_i - 1 = 2^{s_i} t_i$, αυτό ισχύει μόνο στη περίπτωση όπου $r < s_i$. Έτσι, η παραπάνω πολυωνυμική ισοτιμία έχει λύσεις μόνο στη περίπτωση όπου $r \leq s_1 - 1 \leq s_i - 1$ $(i = 1, \ldots, k)$. Τότε έχουμε $\mu_i = r$ και από το Πόρισμα 5.14 παίρνουμε ότι το πλήθος των λύσεων της πολυωνυμικής ισοτιμίας είναι $\delta = 2^{kr}\tau$.

Συνοψίζοντας, δείξαμε ότι το πλήθος των ακεραίων $b \in \mathbb{Z}_n^*$ που είναι τέτοιοι, ώστε ο n να είναι ισχυρός ψευδοπρώτος ως προς βάση b είναι:

$$N(n) = \tau\left(1 + \sum_{r=0}^{s_1 - 1} 2^{kr}\right) = \tau\left(1 + \frac{2^{ks_1} - 1}{2^k - 1}\right).$$

Έχουμε:

$$\phi(n) = \phi(p_1) \cdots \phi(p_k) = 2^{s_1 + \cdots + s_k} T,$$

όπου $T = t_1 \cdots t_k$. Καθώς ισχύει $\tau \leq T$, για να αποδείξουμε την ανισότητα

$$N(n) \leq \frac{\phi(n)}{4}$$

αρκεί να αποδείξουμε ότι

$$\left(1 + \frac{2^{ks_1} - 1}{2^k - 1}\right) \leq \frac{1}{4}\, 2^{s_1 + \cdots + s_k}.$$

Καθώς $s_1 \leq \cdots \leq s_k$, έχουμε:

$$\begin{aligned}\frac{1}{2^{s_1+\cdots+s_k}}\left(1+\frac{2^{ks_1}-1}{2^k-1}\right) &\leq \frac{1}{2^{ks_1}}\left(1+\frac{2^{ks_1}-1}{2^k-1}\right)\\ &\leq \frac{1}{2^{ks_1}}+\frac{1}{2^k-1}-\frac{1}{2^{ks_1}(2^k-1)}\\ &\leq \frac{1}{2^k-1}+\frac{2^k-2}{2^{ks_1}(2^k-1)}\\ &\leq \frac{2}{2^k-1}.\end{aligned}$$

Αν $k \geq 4$, τότε $2/(2^k-1) < 1/4$ και επομένως $N(n) \leq \phi(n)/4$. Αν $k = 3$, τότε έχουμε:

$$\frac{1}{2^k-1}+\frac{2^k-2}{2^{ks_1}(2^k-1)} \leq \frac{1}{4}$$

και κατά συνέπεια η προς απόδειξη ανισότητα αληθεύει. Ας είναι $k = 2$. Τότε έχουμε:

$$\frac{1}{2^{s_1+s_2}}\left(1+\frac{2^{2s_1}-1}{3}\right) = \frac{1}{2^{s_2-s_1}}\left(\frac{1}{3}+\frac{1}{3\cdot 2^{2s_1-1}}\right)$$

Αν $s_2 > s_1$, τότε η παραπάνω ποσότητα είναι $< 1/4$. Ας υποθέσουμε ότι $s_2 = s_1 = \sigma$. Τότε η σχέση $n = p_1p_2 = (2^\sigma t_1+1)(2^\sigma t_2+1)$ συνεπάγεται $\sigma \leq s$. Ας είναι $p_1 > p_2$. Αν $\tau_1 = t_1$, τότε $p_1 - 1 = 2^\sigma\tau_1$. Καθώς $n-1 = 2^s t$, $\sigma \leq s$ και $t_1|t$, παίρνουμε $p_1 - 1|n-1$. Τότε:

$$1 \equiv n \equiv p_1p_2 \equiv p_2 \pmod{(p_1-1)},$$

απ' όπου $p_1 - 1|p_2 - 1$ που είναι άτοπο γιατί $p_1 > p_2$. Τότε έχουμε $\tau_1 < t_1$. Καθώς $\tau_1|t_1$ και οι τ_1, t_1 είναι περιττοί, παίρνουμε $\tau_1 \leq t_1/3$ και επομένως $\tau \leq T/3$. Οπότε, έχουμε:

$$N(n)\tau\left(1+\frac{2^{2\sigma}-1}{3}\right) \leq \frac{T2^{2\sigma}}{6} = \frac{\phi(n)}{6}.$$

Συνεπώς, σε όλες τις περιπτώσεις η προς απόδειξη ισότητα ισχύει. □

Τα παραπάνω αποτελέσματα δίνουν τον εξής πιθανοτικό Monte Carlo αλγόριθμο για να διαπιστώνουμε αν ένας αριθμός είναι πρώτος.

Αλγόριθμος 6.2 Αλγόριθμος των Miller-Rabin.
Είσοδος: Περιττός ακέραιος $n > 3$ και θετικός ακέραιο $t \geq 1$.
Έξοδος: Η απάντηση "n σύνθετος" ή "n πιθανώς πρώτος".

1. Υπολογίζουμε ακέραιους s, d έτσι, ώστε $n - 1 = 2^s d$ και d περιττός.

2. Εκτελούμε τα παρακάτω το πολύ t φορές:

   (α′) Επιλέγουμε τυχαία $a \in \{2, \ldots, n-1\}$ και υπολογίζουμε τον $\mu\kappa\delta(a, n)$.

   (β′) Αν $\mu\kappa\delta(a, n) > 1$, τότε επιστρέφουμε την απάντηση: "n σύνθετος".

   (γ′) Διαφορετικά, υπολογίζουμε $a^d \bmod n$. Αν ισχύει $a^d \not\equiv \pm 1 \pmod{n}$, τότε επιστρέφουμε την απάντηση: "n σύνθετος".

   (δ′) Αν $a^d \equiv \pm 1 \pmod{n}$, τότε για $r = 1, \ldots, s-1$ κάνουμε τα εξής:

      i. Υπολογίζουμε $a^{2^r d} \bmod n$.

      ii. Αν $a^{2^r d} \not\equiv -1 \pmod{n}$, τότε επιστρέφουμε την απάντηση: "n σύνθετος".

3. Σε κάθε άλλη περίπτωση, επιστρέφουμε την απάντηση "n πιθανώς πρώτος".

Για την εφαρμογή του αλγορίθμου υπολογίζουμε τους ακεραίους:

$$\mu\kappa\delta(a, n),\ a^d \bmod n,\ (a^d)^2 \bmod n, \ldots,\ (a^{d2^{r-1}})^2 \bmod n.$$

Ο χρόνος που απαιτείται για τον πρώτον υπολογισμό είναι $O((\log n)^2)$, τον δεύτερο $O((\log n)^2(\log d))$ ενώ για κάθε μία από τους υπόλοιπους $O((\log n)^2)$. Συνολικά, ο χρόνος εκτέλεσης όλων αυτών των υπολογισμών είναι:

$$O((\log n)^2(s + \log d)) = O((\log n)^3).$$

Καθώς αυτή η διαδικασία γίνεται t το πολύ φορές, συνάγεται ότι ο χρόνος εκτέλεσης του αλγορίθμου των Miller-Rabin είναι $O(t(\log n)^3)$ δυαδικές ψηφιακές πράξεις. Επομένως, για μικρές τιμές του t, π.χ. $t < \log n$, ο αλγόριθμος αυτός είναι πολυωνυμικού χρόνου.

Από την Πρόταση 6.8 έπεται ότι η πιθανότητα ο n να είναι σύνθετος και ο τυχαίος ακέραιος a που επιλέγουμε να μήν είναι μάρτυρας για την

συνθετότητα του n είναι $\leq 1/4$. Επομένως στη περίπτωση όπου η εξόδος του αλγόριθμου είναι "n πιθανώς πρώτος" και ο n είναι σύνθετος, έχουν χρησιμοποιηθεί t αριθμοί a οι οποίοι δεν είναι μάρτυρες για την συνθετότητα του n. Η πιθανότητα αυτού του γεγονότος είναι $\leq 1/4^t$. Συνεπώς, η πιθανότητα ο n να είναι πρώτος είναι $\geq 1 - 1/4^t$. Για $t = 10$ βλέπουμε ότι η πιθανότητα ο n να είναι σύνθετος είναι $\leq 1/2^{20}$ και συνεπώς η πιθανότητα ο n να είναι πρώτος είναι μεγαλύτερη απο $0,999999$.

6.5 Αλγόριθμος AKS

Σ' αυτή την ενότητα θα περιγράψουμε μία βελτίωση του αλγόριθμου AKS που οφείλεται στον H. W. Lenstra, Jr.

6.5.1 Μία Γενίκευση του Θεωρήματος του $Fermat$

Ας είναι p ένας πρώτος. Από το Πόρισμα 5.9 έχουμε ότι για κάθε $a \in \mathbb{Z}_p$ ισχύει $a^p = a$. Παρακάτω δίνουμε μία γενίκευση αυτού του πορίσματος.

Θεώρημα 6.4 *Ας είναι p πρώτος. Τότε, για κάθε $P(x) \in \mathbb{Z}_p[x]$ ισχύει*

$$P(x)^p = P(x^p).$$

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του $\deg P$. Για $\deg P = 0$, το Πόρισμα 5.9 δίνει το ζητούμενο. Στη συνέχεια υποθέτουμε ότι το θεώρημα ισχύει για κάθε πολυώνυμο βαθμού $\leq d$. Ας είναι $\deg P = d + 1$. Γράφουμε

$$P = ax^{d+1} + Q,$$

όπου $Q \in \mathbb{Z}_p[x]$ με $\deg Q \leq d$. Από την Πρόταση 4.12, έχουμε:

$$\begin{aligned} P(x)^p &= (ax^{d+1} + Q(x))^p \\ &= (ax^{d+1})^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} (ax^{d+1})^k Q(x)^{p-k} \right) + Q(x)^p. \end{aligned}$$

Η υπόθεση επαγωγής δίνει $Q(x)^p = Q(x^p)$. Χρησιμοποιώντας το Πόρισμα 5.9 έχουμε:

$$(ax^{d+1})^p = a^p (x^{d+1})^p = a(x^p)^{d+1}.$$

Επίσης, από το Παράδειγμα 5.3 παίρνουμε:

$$\left(\begin{array}{c} p \\ k \end{array} \right) \equiv 0 \,(\mathrm{mod}\, p).$$

Συνδυάζοντας τα παραπάνω, προκύπτει $P(x)^p = P(x^p)$. $\square$

Θα δούμε παρακάτω ότι δεν υπάρχει σύνθετος ακέραιος n τέτοιος, ώστε για κάθε πολυώνυμο $P(x) \in \mathbb{Z}_p[x]$ να ισχύει $P(x)^n = P(x^n)$. Για τον σκοπό αυτό θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 6.1 *Ας είναι n ένας ακεραιος ≥ 2 και p ένας πρώτος διαιρέτης του n. Τότε, ο n δεν διαιρεί τον ακέραιο*

$$\left(\begin{array}{c} n \\ p \end{array} \right).$$

Απόδειξη. Ας είναι j ο μεγαλύτερος θετικός ακέραιος με $p^j | n$. Έχουμε:

$$p! \left(\begin{array}{c} n \\ p \end{array} \right) = (n-p+1) \cdots (n-1)n.$$

Οι ακέραιοι $n-p+1, \ldots, n-1$ δεν διαιρούνται από τον p και κατά συνέπεια το δεξί μέρος της παραπάνω ισότητας διαιρείται από τον p^j και δεν διαιρείται από τον p^{j+1}. Έτσι, αν

$$n \Big| \left(\begin{array}{c} n \\ p \end{array} \right),$$

τότε το αριστερό μέρος της ισότητας διαιρείται από τον p^{j+1} που είναι άτοπο. Συνεπώς, το λήμμα αληθεύει. $\square$

Θεώρημα 6.5 *Ας είναι n ακέραιος ≥ 2. Αν ο n είναι σύνθετος, τότε για κάθε πολυώνυμο $P(x) \in \mathbb{Z}_n[x]$, με δύο συντελεστές πρώτους προς τον n, ισχύει:*

$$P(x)^n \neq P(x^n).$$

Απόδειξη. Ας είναι $P(x)$ ένα πολυώνυμο του $\mathbb{Z}_n[x]$ με $\deg P = d \geq 1$. Γράφουμε $P(x) = ax^d + Q(x)$, όπου $a \in \mathbb{Z}_n$ και $Q(x) \in \mathbb{Z}_n[x]$ με $\deg Q = m < d$. Αν p είναι ένας πρώτος διαιρέτης του n, τότε, σύμφωνα με το Λήμμα 6.1, ο n δεν διαιρεί τον ακέραιο $\left(\begin{array}{c} n \\ p \end{array} \right)$. Συμβολίζουμε με

k τον μεγαλύτερο θετικό ακέραιο $\leq n-1$ ο οποίος είναι τέτοιος, ώστε ο ακέραιος $\left(\begin{array}{c} n \\ k \end{array} \right)$ δεν διαιρείται με τον n. Έχουμε:

$$P(x)^n = (ax^d + Q(x))^n = a^n x^{dn} + \sum_{j=0}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (ax^d)^j Q(x)^{n-j}.$$

Για κάθε ακέραιο r, με $0 \leq r < k$ ισχύει:

$$dr + m(n-r) < dk + m(n-k).$$

Έτσι, ο συντελεστή του $x^{dk+m(n-k)}$ στο $P(x)^n$ είναι ο ακέραιος

$$A = \left(\begin{array}{c} n \\ k \end{array} \right) a^k b^{n-k},$$

όπου b είναι ο συντελεστής του x^m στο $Q(x)$. Από την υπόθεση έχουμε $\mu\kappa\delta(a,n) = \mu\kappa\delta(b,n) = 1$ και επιπλέον ισχύει $n \not\mid \left(\begin{array}{c} n \\ k \end{array} \right)$. Επομένως $n \not\mid A$ και κατά συνέπεια $A \mod n \neq 0$. Καθώς έχουμε:

$$dn > dk + m(n-k) > mn,$$

ο συντελεστής του $x^{dk+m(n-k)}$ στο $P(x^n)$ είναι 0. Συνεπώς, ισχύει $P(x)^n \neq P(x^n)$. $\square$

Πόρισμα 6.4 *Ας είναι n ακέραιος ≥ 2. Τότε, ο n είναι πρώτος αν και μόνον αν για κάθε $a \in \mathbb{Z}_n^*$ ισχύει*

$$(x+a)^n = x^n + a.$$

Παρατήρηση 6.3 Το παραπάνω θεώρημα δεν ισχύει αν υπάρχουν συντελεστές του πολυωνύμου $P(x)$ που δεν είναι πρώτοι προς τον n. Για παράδειγμα έχουμε $(4x+3)^6 = 4x^6 + 3$ μέσα στο $\mathbb{Z}_6$.

Το Πόρισμα 6.4 δίνει ένα τρόπο για να ελέγχουμε αν ο ακέραιος n είναι πρώτος. Η μέθοδος όμως αυτή είναι μη αποτελεσματική, καθώς απαιτεί τον υπολογισμό όλων των συντελεστών του $(x+a)^n$ και κατά συνέπεια ο χρόνος εκτέλεσης της είναι εκθετικός ως προς $\ell(n)$. Όπως θα δούμε παρακάτω, ο αλγόριθμος AKS, βασίζεται στον έλεγχο ισοτιμιών της μορφής $(x+a)^n \equiv x^n + a \pmod{Q}$, όπου Q είναι πολυώνυμο ειδικής μορφής και μικρού βαθμού έτσι, ώστε ο χρόνος εκτέλεσής του να είναι πολυωνυμικός ως προς $\ell(n)$.

6.5.2 Μερικά Λήμματα

Σ′ αυτή την ενότητα θα παρουσιάσουμε μερικά λήμματα τα οποία θα χρειαστούμε για την απόδειξη της ορθότητας του αλγόριθμου AKS και στην εκτίμηση του χρόνου που απαιτείται για την εκτέλεσή του.

Λήμμα 6.2 *Για κάθε περιττό $n > 1$ υπάρχει πρώτος r, που δεν διαιρεί τον n και $\mathrm{ord}_r(n) > 4(\log_2 n)^2 + 2$. Για τον μικρότερο πρώτο r με αυτή την ιδιότητα ισχύει*

$$r = O((\log n)^5).$$

Απόδειξη. Θέτουμε $T = 4(\log_2 n)^2 + 2$. Ας είναι R θετικός ακέραιος τέτοιος, ώστε κάθε ακέραιος $r \in \{1, \ldots, R\}$ είναι πρώτος προς τον n και $\mathrm{ord}_r(n) \leq T$. Συμβολίζουμε με d_R το ελάχιστο κοινό πολλαπλάσιο των $1, 2, \ldots, R$. Κάθε θετικός ακέραιος $r \leq R$ διαιρεί το γινόμενο

$$\prod_{i=1}^{T}(n^i - 1)$$

και επομένως έχουμε:

$$d_R \leq \prod_{i=1}^{T}(n^i - 1) \leq n^{T^2}.$$

Σύμφωνα με το Λήμμα 3.3, ισχύει:

$$2^{R-2} \leq d_R.$$

Συνδυάζοντας τις παραπάνω ανισότητες προκύπτει:

$$2^{R-2} \leq n^{T^2},$$

απ′ όπου:

$$R \leq T^2 \log_2 n + 2.$$

Ας είναι $B = T^2 \log_2 n + 2$. Χρησιμοποιώντας το Θεώρημα 3.5, έχουμε:

$$\pi(2B) - \pi(B) > \frac{B}{3\log(2B)} > \log_2 n.$$

Καθώς, το πλήθος των πρώτων διαιρετών του n είναι $\leq \log_2 n$, έπεται ότι υπάρχει πρώτος $r \leq 2B$ με $r \not| n$. Επιπλέον, καθώς $r > B \geq R$, ισχύει $\mathrm{ord}_r(n) > 4(\log_2 n)^2 + 2$. Τέλος, η ανισότητα $r \leq 2B$ δίνει $r = O((\log n)^5)$. □

Λήμμα 6.3 *Ας είναι p πρώτος, $a \in \mathbb{Z}_p$. Αν για τους θετικούς ακέραιους m_1, m_2 ισχύει η ισοτιμία*

$$(x-a)^{m_i} \equiv x^{m_i} - a \pmod{x^r - 1} \quad (i = 1, 2),$$

μέσα στο $\mathbb{Z}_p[x]$, τότε έχουμε:

$$(x-a)^{m_1 m_2} \equiv x^{m_1 m_2} - a \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_p[x]$.

Απόδειξη. Καθώς

$$(x-a)^{m_2} \equiv x^{m_2} - a \pmod{x^r - 1},$$

υπάρχει $g(x) \in \mathbb{Z}_p[x]$ έτσι, ώστε

$$(x-a)^{m_2} - (x^{m_2} - a) = (x^r - 1)g(x).$$

Αντικαθιστώντας το x με το x^{m_1} παίρνουμε:

$$(x^{m_1} - a)^{m_2} - (x^{m_1 m_2} - a) = (x^{m_1 r} - 1)g(x^{m_1}).$$

Καθώς το $x^r - 1$ διαιρεί το $x^{m_1 r} - 1$, έχουμε ότι το $x^r - 1$ διαιρεί το $(x^{m_1} - a)^{m_2} - (x^{m_1 m_2} - a)$ και επομένως:

$$(x^{m_1} - a)^{m_2} \equiv x^{m_1 m_2} - a \pmod{x^r - 1}.$$

Από την άλλη πλευρά, καθώς

$$(x-a)^{m_1} \equiv x^{m_1} - a \pmod{x^r - 1},$$

έπεται

$$(x-a)^{m_1 m_2} \equiv (x^{m_1} - a)^{m_2} \pmod{x^r - 1},$$

και επομένως ισχύει:

$$(x-a)^{m_1 m_2} \equiv x^{m_1 m_2} - a \pmod{x^r - 1}. \quad \square$$

Λήμμα 6.4 *Ας είναι n θετικός ακέραιος ο οποίος δεν είναι δύναμη πρώτου, t θετικός ακέραιος και p πρώτος. Τότε το σύνολο*

$$E = \{n^i p^j / \ 0 \le i, j \le \lfloor \sqrt{t} \rfloor\}$$

έχει περισσότερα από t στοιχεία.

Απόδειξη. Ας είναι $0 \leq i, j \leq \lfloor \sqrt{t} \rfloor$ και $0 \leq r, s \leq \lfloor \sqrt{t} \rfloor$ με $n^i p^j = n^r p^s$. Θα δείξουμε ότι $(i, j) = (r, s)$. Αν ο p δεν διαιρεί τον n αυτό είναι προφανές. Ας υποθέσουμε στη συνέχεια ότι $n = p^k a$ με $k \geq 1$ και a ακέραιος που δεν διαιρείται από τον p. Καθώς ο n δεν είναι δύναμη πρώτου, έχουμε $a > 1$. Τότε

$$a^i p^{ik+j} = a^r p^{rk+s}.$$

Επειδή ο p δεν διαιρεί τον a έπεται $a^i = a^r$ και καθώς $a > 1$ έχουμε $i = r$. Οπότε $p^{ik+j} = p^{rk+s}$ και επομένως $j = s$. Άρα

$$|E| = (1 + \lfloor \sqrt{t} \rfloor)^2 > t. \quad \square$$

Λήμμα 6.5 *Ας είναι p και r πρώτοι με $r \neq p$. Τότε υπάρχει ένα πεπερασμένο σώμα K χαρακτηριστικής p και $w \in K$ έτσι, ώστε η τάξη του w μέσα στη πολαπλασιαστική ομάδα του K να ισούται με r.*

Απόδειξη. Θεωρούμε το πολυώνυμο $x^r - 1$ του $\mathbb{Z}_p[x]$. Σύμφωνα με την Πρόταση 4.22 υπάρχει ανάγωγο πολυώνυμο $P \in \mathbb{Z}_p[x]$ με $P | x^r - 1$. Καθώς το P είναι ανάγωγο, η Πρόταση 5.34 συνεπάγεται ότι ο δακτύλιος $K = (\mathbb{Z}_p[x])_P$ είναι σώμα. Τότε έχουμε $P(x) = 0$ μέσα στο K και επομένως $x^r = 1$. Καθώς ο r είναι πρώτος, η τάξη του x μέσα στο K ισούται με r. $\square$

6.5.3 Περιγραφή του Αλγορίθμου AKS

Στη συνέχεια παρουσιάζουμε τον αλγόριθμο AKS.

Αλγόριθμος 6.3 Αλγόριθμος AKS.
Είσοδος: Περιττός ακέραιος $n > 3$.
Έξοδος: Η απάντηση "n σύνθετος" ή "n πρώτος".

1. Εξετάζουμε αν υπάρχουν ακέραιοι $a \geq 2$ και $k \geq 2$ με $n = a^k$. Αν ναι, τότε εξάγουμε: "n σύνθετος".

2. Βρίσκουμε τον μικρότερο πρώτο r με $\mathrm{ord}_r(n) \geq 4(\log_2 n)^2 + 2$. Θέτουμε $l = \lfloor 2\sqrt{r} \log_2 n \rfloor + 1$.

3. Αν κάποιος από τους ακέραιους $2, 3, \ldots, l$ διαιρεί τον n, τότε εξάγουμε: "n σύνθετος".

4. Εξετάζουμε αν ισχύει

$$(x-a)^n \not\equiv x^n - a \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_n[x]$, για κάποιο $a \in \{1, \ldots, l\}$. Αν ναι, τότε εξάγουμε: "n σύνθετος".

5. Αν ο n δεν έχει βρεθεί σύνθετος σε κάποιο από τα προηγούμενα βήματα, τότε εξάγουμε: "n πρώτος".

Υπολογισμός του Χρόνου Εκτέλεσης του AKS. Καταρχήν θα εκτιμήσουμε τον χρόνο εκτέλεσης του AKS. Σύμφωνα με το Παράδειγμα 1.13, ο χρόνος που απαιτείται για το πρώτο βήμα είναι $O((\log n)^4)$.

Θέτουμε $M = \lfloor 4(\log_2 n)^2 \rfloor + 2$. Παρατηρούμε ότι $r \geq M + 1$. Η εύρεση του r γίνεται ως εξής: Για κάθε $q = M + 1, \ldots$ υπολογίζουμε $n^i \mod q$ $(i = 1, \ldots, M)$. Αν $n^i \not\equiv 1 \pmod{q}$ για κάθε $i = 1, 2, \ldots, M$, τότε εξετάζουμε αν ο q είναι πρώτος εφαρμόζοντας την Μέθοδο των Διαδοχικών Διαιρέσεων.

Ο υπολογισμός του $n \mod q$ απαιτεί χρόνο $O((\log n)(\log q))$. Σύμφωνα με την Πρόταση 5.8, ο υπολογισμός του $n^i \mod q$ χρειάζεται χρόνο $O((\log q)^2(\log i))$. Άρα, ο χρόνος υπολογισμού των $n^i \mod q$ $(i = 1, \ldots, M)$ είναι:

$$O((\log n)(\log q) + (\log q)^2 \sum_{i=1}^{M} \log i) = O((\log q)^2 (\log n)^2 \log\log n).$$

Η εφαρμογή της Μεθόδου των Διαδοχικών Διαιρέσεων απαιτεί χρόνο $O(\sqrt{q}(\log q)^2)$. Από το Λήμμα 6.2 έχουμε $r = O((\log n)^5)$ και επομένως $q = O((\log n)^5)$. Επίσης, για τον προσδιορισμό του r θα εξετάσουμε $O((\log n)^5)$ θετικούς q. Συνδυάζοντας τα παραπάνω, παίρνουμε ότι ο χρόνος που απαιτείται για να βρεθεί ο r είναι $O((\log n)^8)$.

Στο τρίτο βήμα, η εκτέλεση όλων των διαιρέσεων απαιτεί χρόνο $O((\log n)^5)$. Τέλος, από το Λήμμα 6.2 και την Πρόταση 5.33 έπεται ότι ο χρόνος που χρειάζεται για το τέταρτο βήμα είναι $O((\log n)^{17})$. Συνεπώς, ο χρόνος που απαιτείται για την εκτέλεση του αλγόριθμου AKS είναι $O((\log n)^{17})$. □

Απόδειξη της Ορθότητας του AKS. Καταρχήν, ας υποθέσουμε ότι ο ακέραιος n είναι πρώτος. Από τα Βήματα 1 και 3 δεν συνάγεται ότι ο n είναι σύνθετος. Στο Βήμα 4, έχουμε:

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_n[x]$, για κάθε $a \in \{1, \ldots, l\}$, σύμφωνα με το Πόρισμα 6.4. Οπότε, ο αλγόριθμος διαπιστώνει ότι ο n είναι πρώτος.

Ας υποθέσουμε τώρα ότι ο ακέραιος n είναι σύνθετος. Θα δείξουμε ότι, στην περίπτωση αυτή, ο αλγόριθμος είναι αδύνατον να διαπιστώσει ότι ο ν είναι πρώτος. Πράγματι, ας υποθέσουμε ότι ο αλγόριθμος είχε καταλήξει στο συμπέρασμα "ο ν είναι πρώτος". Τότε, στο Βήμα 4, θα είχε διαπιστωθεί ότι για $a = 1, \ldots, l$ ισχύει:

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_n[x]$. Ας είναι p ένας διαιρέτης του n. Αφού στο Βήμα 3 ο αλγόριθμος δεν διαπίστωσε ότι ο ν είναι σύνθετος, έπεται ότι $p > l$. Έχουμε:

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_p[x]$. Από την άλλη πλευρά, μέσα στο $\mathbb{Z}_p[x]$, ισχύει:

$$(x-a)^p \equiv x^p - a \pmod{x^r - 1}.$$

Συνδυάζοντας τις παραπάνω σχέσεις και το Λήμμα 6.3, συμπεραίνουμε ότι για κάθε ζεύγος ακεραίων $i \geq 0$, $j \geq 0$ και $a = 1, \ldots, l$ ισχύει:

$$(x-a)^{p^i n^j} \equiv x^{p^i n^j} - a \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_p[x]$.

Ας είναι H η υποομάδα της $\mathbb{Z}_r^*$, την οποία παράγουν οι p, n, θεωρούμενοι ως στοιχεία της $\mathbb{Z}_r^*$, και t η τάξη της H. Από την άλλη μεριά, θεωρούμε το σύνολο

$$E = \{n^i p^j / \ 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor\}.$$

Από το Λήμμα 6.4 έχουμε ότι $|E| > t$. Αυτό σημαίνει ότι υπάρχουν δύο διαφορετικά στοιχεία του συνόλου E, τα οποία, θεωρούμενα ως στοιχεία της ομάδας H, ταυτίζονται. Μ' άλλα λόγια, υπάρχουν δύο ακεραιοι $m_1 = p^{i_1} n^{j_1}$ και $m_2 = p^{i_2} n^{j_2}$ του E με $(i_1, j_1) \neq (i_2, j_2)$ και $m_1 \equiv m_2 \pmod{\text{r}}$. Άρα, υπάρχει ακέραιος k με $m_2 = m_1 + kr$ και ισχύει:

$$(x-a)^{m_2} \equiv x^{m_1+kr} - a \equiv x^{m_1} - a \equiv (x-a)^{m_1} \pmod{x^r - 1},$$

μέσα στο $\mathbb{Z}_p[x]$. Συνεπώς, για $a = 1, \ldots, l$, δειξαμε ότι για το πολυώνυμο $x - a$ του $\mathbb{Z}_p[x]$, ισχύει:

$$(x-a)^{m_2} \equiv (x-a)^{m_1} \pmod{x^r - 1}.$$

Σύμφωνα με το Λήμμα 6.5 υπάρχει ένα πεπερασμένο σώμα K χαρακτηριστικής p και $w \in K$ έτσι, ώστε η τάξη του w μέσα στη πολλαπλασιαστική ομάδα του K να ισούται με r. Καθώς η χαρακτηριστική του K ισούται με p, μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι το $\mathbb{Z}_p$ είναι υπόσωμα του K. Οπότε, για $a = 1, \ldots, l$ έχουμε $(w-a)^{m_1} = (w-a)^{m_2}$ και επομένως το $w-a$ είναι ρίζα του πολυωνύμου $F(x) = x^{m_1} - x^{m_2}$ μέσα στο K. Θέτουμε $L = \lfloor 2\sqrt{t}\log_2 n \rfloor + 1$. Παρατηρούμε ότι αν ρ_1, ρ_2 είναι ρίζες του $F(x)$, τότε το γινόμενο $\rho_1\rho_2$ είναι επίσης ρίζα του $F(x)$ και επομένως κάθε στοιχείο του συνόλου

$$S = \left\{ \prod_{a=1}^{L} (w-a)^{e_a} / \ e_a \in \{0,1\} \right\}$$

είναι ρίζα του $F(x)$. Θα δείξουμε ότι τα στοιχεία του S είναι διακεκριμμένα.

Από το Βήμα 3 του αλγόριθμου έχουμε ότι κανένας από τους ακέραιους $2, 3, \ldots, l$ δεν διαιρεί τον n. Καθώς $t \leq r-1$, έχουμε $L \leq l$ και επομένως $L < p$. Άρα, οι κλάσεις των ακεραίων $1, \ldots, L$ κατά μέτρο p είναι διαφορετικές ανά δύο και κατά συνέπεια τα πολυώνυμα του $\mathbb{Z}_p[x]$, της μορφής $g(x) = \prod_{a=1}^{L}(x-a)^{e_a}$, είναι διακεκριμμένα. Παρατηρούμε ότι τα στοιχεία του S είναι της μορφής $g(w)$. Από το Λήμμα 6.3, για κάθε ζεύγος ακεραίων $i \geq 0$, $j \geq 0$, έχουμε:

$$g(x)^{n^i p^j} \equiv g(x^{n^i p^j}) \pmod{x^r - 1},$$

και επομένως $g(w)^{n^i p^j} = g(w^{n^i p^j})$.

Ας είναι $g_1(x)$ και $g_2(x)$ πολυώνυμα της παραπάνω μορφής με $g_1(w) = g_2(w)$. Οπότε, για κάθε ζεύγος ακεραίων $i \geq 0$, $j \geq 0$, έχουμε $g_1(w^{n^i p^j}) = g_2(w^{n^i p^j})$. Καθώς η τάξη του w ισούται με r, το $w^{n^i p^j}$ παίρνει τόσες διακεκριμμένες τιμές όσο είναι το πλήθος των διακεκριμμένων κλάσεων κατά μέτρο r των στοιχείων $n^i p^j$. Άρα, το πολυώνυμο $g_1(x) - g_2(x)$ έχει τουλάχιστον t ρίζες μέσα στο K. Από την άλλη πλευρά, έχουμε:

$$t \geq \mathrm{ord}_r(n) \geq 4(\log_2 n)^2 + 2$$

και επομένως ισχύει:

$$L \leq 2\sqrt{t}\log_2 n + 1 \leq \sqrt{t^2 - 2t} + 1 < t.$$

Καθώς το $g_1(x) - g_2(x)$ έχει βαθμό $\leq L$ και τουλάχιστον t ρίζες, παίρνουμε $g_1(x) = g_2(x)$. Επομένως, τα στοιχεία του S είναι διακεκριμμένα και κατά συνέπεια $|S| = 2^L$. Έτσι, το $F(x)$ έχει τουλάχιστον

2^L ρίζες μέσα στο K. Από την άλλη πλευρά ο βαθμός του $F(x)$ είναι $\max\{m_1, m_2\} \leq n^{2\lfloor\sqrt{t}\rfloor} < 2^L$. Συνεπώς, το $F(x)$ είναι το μηδενικό πολυώνυμο και επομένως $m_1 = m_2$, δηλαδή $p^{i_1}n^{j_1} = p^{i_2}n^{j_2}$. Καθώς $(i_1, j_1) \neq (i_2, j_2)$, παίρνουμε $n = p^s$ για κάποιο ακέραιο $s \geq 1$. Αν $s > 1$, τότε από το Βήμα 1 θα είχαμε ότι ο n είναι σύνθετος, ενώ αν $s = 1$, τότε ο n είναι πρώτος. Και στις δύο περιπτώσεις καταλήγουμε σε άτοπο γιατί υποθέσαμε ότι ο n είναι σύνθετος και ότι ο αλγόριθμος διαπιστώνει ότι είναι πρώτος. Συνεπώς, αν ο n είναι σύνθετος, τότε ο αλγόριθμος το διαπιστώνει σε κάποιο από τα βήματά του. □

6.6 Ασκήσεις

1. Να βρεθούν οι μικρότεροι ψευδοπρώτοι του Fermat ως προς βάσεις 2 και 5 αντίστοιχα.

2 Να βρεθούν όλες οι βάσεις ως προς τις οποίες ο 15 είναι ψευδοπρώτος του Fermat.

3. Ας είναι $n = pq$, όπου p και q διαφορετικοί πρώτοι, και $d = \mu\kappa\delta(p-1, q-1)$. Να δειχθεί ότι ο n είναι ψευδοπρώτος του Fermat ως προς βάση b, αν και μόνον αν

$$b^d \equiv 1 \pmod{n}.$$

4. Να δειχθει με τη χρήση του κριτηρίου του Fermat ότι οι αριθμοί 1111 και 2047 είναι σύνθετοι.

5. Να δειχθεί ότι για κάθε πρώτο r υπαρχει το πολύ πεπερασμένο πλήθος αριθμών του Carmichael της μορφής pqr, όπου p, q είναι πρώτοι. Κατόπιν, να βρεθούν όλοι οι αριθμοί του Carmichael της μορφής $3pq$ και $5pq$.

6. Να δειχθεί ότι ο πέμπτος αριθμός του Fermat $F_5 = 2^{2^5} + 1$ είναι σύνθετος. Αν p είναι ένας πρώτος παράγοντας του F_5, τότε να δειχθεί ότι $p \equiv 1 \pmod{64}$. Κατόπιν να βρεθεί η πρωτογενής ανάλυση του.

7. Δώστε ένα παράδειγμα συνθέτου ακεραίου $n > 1$ και μιας βάσης b

έτσι, ώστε

$$b^{(n-1)/2} \equiv \pm 1 \pmod{n}$$

και ο n δεν είναι ψευδοπρώτος του Euler ως προς βάση b.

8. Αν ο ακέραιος n είναι ψευδοπρώτος του Euler ως προς βάση $b \in \mathbb{Z}_n$, τότε να δειχθεί ότι ο n είναι ψευδοπρώτος του Euler ως προς τις βάσεις $-b \mod n$ και $b^{-1} \mod n$.

9. Αν ο n είναι ψευδοπρώτος του Fermat ως προς βάση 2, τότε να δειχθεί ότι ο $N = 2^n - 1$ είναι ισχυρός ψευδοπρώτος και ένας ψευδοπρώτος του Euler ως προς βάση 2. Επιπλέον, να δειχθεί ότι υπάρχει άπειρο πλήθο ισχυρών ψευδοπρώτων και ψευδοπρώτων του Euler ως προς βάση 2.

10. Αν ο n είναι ισχυρός ψευδοπρώτος ως προς την βάση 2, τότε να δειχθεί ότι είναι ισχυρός ψευδοπρώτος ως προς βάση b^k για κάθε θετικό ακέραιο k.

11. Ας είναι $n = p^a$, όπου p πρώτος και a ακέραιος > 1. Να δειχθεί ότι ο n είναι ισχυρός ψευδοπρώτος ως προς βάση b αν και μόνον αν ο n είναι ψευδοπρώτος του Fermat ως προς βάση b.

12. Να χρησιμοποιηθεί ο αλγόριθμος AKS για να δειχθεί ότι ο ακεραιος 16493 είναι πρώτος.

Βιβλιογραφία

[1] E. Bach and J. Shallit, *Algorithmic Number Theory,* MIT Press, Cambridge, Massachusetts and London, England, 1996.

[2] M. W. Baldoni, C. Ciliberto and G. M. Piacentini Cattaneo, *Elementary Number Theory, Cryptography and Codes,* Springer-Verlag 2009.

[3] D. M. Bressoud, *Factorization and Primality Testing,* New York, Berlin, Heidelberg, Springer Verlag 1989.

[4] D. M. Bressoud and S. Wagon, *A Course in Computational Number Theory,* New York, Berlin, Heidelberg, Springer Verlag 2000.

[5] R. Crandall and C. Pomerance, *Prime Numbers, A Computational Perspective,* New York, Berlin, Heidelberg, Springer Verlag 2001.

[6] M. Demazure, *Cours d'algèbre,* Cassini 1997.

[7] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra,* Cambridge University Press 1999.

[8] L. Rempe-Gillen and R. Waldecker, *Primality Testing for Beginners,* Student Mathematical Library, Vol. 70, AMS 2014.

[9] P. Ribenboim, *Nombres Premiers: mystères et records,* Presses Univérsitaires de France 1994.

[10] S. Y. Yan, *Number Theory for Computing,* Berlin, Heidelberg, Springer Verlag 2002.

Κεφάλαιο 7

Παραγοντοποίηση Ακεραίων

Σύνοψη
Το κεφάλαιο αυτό είναι αφιερωμένο σε ένα από τα πλέον σημαντικά θέματα της Υπολογιστικης Θεωρίας Αριθμών που είναι η παραγοντοποίηση ακεραίων. Θα περιγράψουμε τις μεθόδους παραγοντοποίησης των Fermat, Legendre, Dixon, των συνεχών κλασμάτων και τους αλγόριθμους $p-1$ και ρ του Pollard. Ας σημειωθεί ότι αλγόριθμος πολυωνυμικού χρόνου για την παραγοντοποίηση ενός ακεραίου δεν έχει ακόμη ανακαλυφθεί. Οι πλέον αποτελεσματικοί αλγόριθμοι παραγοντοποίησης σήμερα είναι το *κόσκινο των σωμάτων αλγεβρικών αριθμών* [6, 8, 10] και η *μέθοδος των ελλειπτικών καμπυλών* [5, 10] των οποίων όμως η περιγραφή εκφεύγει από το πλαίσιο του παρόντος συγγράμματος.

Προαπαιτούμενη γνώση
Κεφάλαια 1,2,3 και 5.

7.1 Μέθοδος του *Fermat*

Η πρώτη μέθοδος παραγοντοποίησης με την οποία θ΄ ασχοληθούμε είναι αρκετά παλιά και οφείλεται στον Fermat. Η ιδέα της μεθόδου βασίζεται στην επόμενη πρόταση.

Πρόταση 7.1 *Ας είναι n θετικός περιττός ακέραιος. Τότε υπάρχει μία αμφίεση μεταξύ των παραγοντοποιήσεων του n της μορφής $n = ab$,*

όπου a, b ακέραιοι με $a \geq b > 0$ και των παραστάσεων του n της μορφής $t^2 - s^2$, όπου s και t είναι ακέραιοι ≥ 0. Η αμφίεση αυτή δίνεται από τις σχέσεις:

$$t = \frac{a+b}{2}, \quad s = \frac{a-b}{2}$$

και

$$a = t + s, \quad b = t - s.$$

Απόδειξη. Ας είναι $n = ab$, όπου a, b ακέραιοι με $a \geq b > 0$. Τότε:

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

Έτσι, θέτοντας $t = (a+b)/2$ και $s = (a-b)/2$, έχουμε $n = t^2 - s^2$. Αντίστροφα, αν $n = t^2 - s^2$, όπου s και t είναι θετικοί ακέραιοι, τότε:

$$n = (t+s)(t-s).$$

Συνεπώς, οι αντιστοιχίες

$$(a,b) \longmapsto ((a+b)/2, (a-b)/2), \quad (s,t) \longmapsto (t+s, t-s)$$

δίνουν μία αμφίεση μεταξύ των δύο τρόπων γραφής του n. □

Για να παραγοντοποιήσουμε λοιπόν τον n μπορούμε να εργαστούμε ως εξής: Παίρνουμε $t = \lfloor\sqrt{n}\rfloor + 1, \lfloor\sqrt{n}\rfloor + 2, \ldots$ και υπολογίζουμε τις τιμές $t^2 - n$ μέχρι να βρούμε ακέραιο s τέτοιον, ώστε να ισχύει $t^2 - n = s^2$. Τότε, θα έχουμε $n = (t+s)(t-s)$. Η μέθοδος αυτή είναι γνωστή ως *μέθοδος του* Fermat.

Αν $n = ab$, τότε θα χρειαστεί να εξετάσουμε όλους τους θετικούς ακέραιους μέχρι τον $(a+b)/2 - \lfloor\sqrt{n}\rfloor$. Έτσι, στην περίπτωση όπου οι ακέραιοι a και b βρίσκονται πολύ κοντά, τότε ο $s = (a-b)/2$ είναι πολύ μικρός και επομένως ο $t = (a+b)/2$ είναι λίγο μεγαλύτερος από τον $\lfloor\sqrt{n}\rfloor$. Τότε, η μέθοδος θα μας δώσει την παραγοντοποίηση του n μετά από ένα μικρό πλήθος δοκιμών για τον t, όπως στο παρακάτω παράδειγμα.

Παράδειγμα 7.1 Θα παραγοντοποιήσουμε τον ακέραιο 318901. Έχουμε $\lfloor\sqrt{318901}\rfloor = 564$. Βρίσκουμε $565^2 - 318901 = 18^2$. Οπότε $318901 = 547 \cdot 583$.

Η παρακατω πρόταση μας δίνει μία εκτίμηση του πλήθους των βημάτων που απαιτεί η μέθοδος του Fermat στην περίπτωση όπου ο ακέραιος n είναι το γινόμενο δύο πρώτων.

Πρόταση 7.2 *Ας είναι $n = pq$, όπου p και q πρώτοι με $p > q$, και A το πλήθος των βημάτων που απαιτεί η μέθοδος του Fermat για την παραγοντοποίηση του n. Τότε ισχύει:*

$$A = \left\lceil \frac{(\sqrt{p} - \sqrt{q})^2}{2} \right\rceil < \frac{(p-q)^2}{8\lfloor\sqrt{n}\rfloor} + 1.$$

Απόδειξη. Η εφαρμογή της μεθόδου του Fermat για την παραγοντοποίηση του n απαιτεί τον υπολογισμό όλων των ποσοτήτων $t^2 - n$ με $t = \lfloor\sqrt{n}\rfloor + 1, \lfloor\sqrt{n}\rfloor + 2, \ldots, (p+q)/2$. Οπότε, το πλήθος των βημάτων που απαιτεί η μέθοδος είναι:

$$A = \frac{p+q}{2} - (\lfloor\sqrt{n}\rfloor + 1) + 1 = \frac{p+q}{2} - \lfloor\sqrt{n}\rfloor.$$

Έτσι, έχουμε:

$$A = \left\lceil \frac{p+q}{2} - \sqrt{p}\sqrt{q} \right\rceil = \left\lceil \frac{(\sqrt{p} - \sqrt{q})^2}{2} \right\rceil.$$

Από την άλλη πλευρά, καθώς $(p+q)/2 = \lfloor\sqrt{n}\rfloor + A$, παίρνουμε:

$$(\lfloor\sqrt{n}\rfloor + A)^2 - n = \left(\frac{p-q}{2}\right)^2.$$

Έτσι, έχουμε:

$$A^2 + 2A\lfloor\sqrt{n}\rfloor = \left(\frac{p-q}{2}\right)^2 + n - \lfloor\sqrt{n}\rfloor^2,$$

απ΄ όπου προκύπτει:

$$A < \frac{(p-q)^2}{8\lfloor\sqrt{n}\rfloor} + \frac{n - \lfloor\sqrt{n}\rfloor^2}{2\lfloor\sqrt{n}\rfloor}.$$

Εύκολα βλέπουμε ότι ισχύει:

$$\frac{n - \lfloor\sqrt{n}\rfloor^2}{2\lfloor\sqrt{n}\rfloor} < 1$$

και κατά συνέπεια έχουμε:

$$A < \frac{(p-q)^2}{8\lfloor\sqrt{n}\rfloor} + 1. \quad \square$$

Πόρισμα 7.1 *Ας είναι $n = pq$, όπου p και q πρώτοι με $p > q$. Αν $p - q < \sqrt{8}\sqrt[4]{n}$, τότε η μέθοδος του Fermat παραγοντοποιεί τον n σε ένα βήμα.*

Αν για κάθε παραγοντοποίηση $n = ab$ του n, οι ακέραιοι a και b βρισκονται αρκετά μακριά, τότε θα χρειαστεί ένα μεγάλο πλήθος δοκιμών για τον t. Για να επιταγχυνθεί η διαδικασία σ΄ αυτή την περίπτωση, μπορούμε να χρησιμοποιήσουμε την εξής γενίκευση της μεθόδου του Fermat:

Επιλέγουμε ένα μικρό θετικό ακέραιο k και, παίρνοντας διαδοχικά $t = \lfloor\sqrt{kn}\rfloor + 1, \lfloor\sqrt{kn}\rfloor + 2 \ldots$, υπολογίζουμε τις τιμές $t^2 - kn$ μέχρι να βρούμε ακέραιο s τέτοιον, ώστε $t^2 - kn = s^2$. Τότε:

$$(t + s)(t - s) = kn.$$

Καθώς οι ακέραιοι t και s βρίσκονται αρκετά μακρυά και ο k είναι μικρός, έχουμε $k < t - s < t + s < n$. Οπότε, υπάρχει διαιρέτης δ του $t \pm s$ που δεν διαιρεί τον k και κατά συνέπεια υπάρχει πρώτος διαιρέτης του δ που διαιρεί τον n. Άρα, έχουμε $1 < \mu\kappa\delta(t \pm s, n) < n$ και επομένως οι ακέραιοι $\mu\kappa\delta(t \pm s, n)$ είναι γνήσιοι παράγοντες του n.

Παράδειγμα 7.2 Θα εφαρμόσουμε την παραπάνω γενίκευση της μεθόδου του Fermat για να παραγοντοποιήσουμε τον ακέραιο 329345.

Υπολογίζουμε την ποσότητα $\lfloor\sqrt{3 \cdot 329345}\rfloor = 993$. Για $t = 994$, παίρνουμε $994^2 - 3 \cdot 329345 = 1$. Επομένως, $3 \cdot 329345 = 995 \cdot 993$. Κατόπιν, υπολογίζουμε $\mu\kappa\delta(329345, 995) = 995$. Έτσι, βρίσκουμε $329345 = 331 \cdot 995$.

Από την άλλη πλευρά, ακολουθώντας την κλασσική μέθοδο του Fermat υπολογίζουμε $\lfloor\sqrt{329345}\rfloor = 573$ και στη συνέχεια, για κάθε $t = 574, 575, \ldots$, την ποσότητα $\sqrt{t^2 - 329345}$. Για $t = 663$, παίρνουμε $\sqrt{663^2 - 329345} = 332$, απ΄ όπου προκύπτει η παραγοντοποίηση $329345 = 331 \cdot 995$. Παρατηρούμε ότι η κλασσική μέθοδος απαιτεί τον έλεγχο 90 τιμών του t ενώ η γενικευμένη μόνο μίας.

7.2 Βάσεις Παραγοντοποίησης

Είδαμε στην προηγούμενη ενότητα ότι για να παραγοντοποιήσουμε ένα σύνθετο θετικό ακέραιο n αρκεί να βρούμε ακέραιους t, s και έναν

αρκετά μικρό θετικό k έτσι, ώστε να ισχύει $t^2 - s^2 = kn$. Τότε βέβαια έχουμε $t^2 \equiv s^2 \pmod{n}$. Σ΄ αυτή την ενότητα θα εξετάσουμε πώς να κατασκευάζουμε τέτοιες ισοτιμίες.

7.2.1 Μέθοδος του *Legendre*

Σύμφωνα με μία παρατήρηση του Legendre, αν προσδιορίσουμε ακεραίους $t > s$ με

$$t^2 \equiv s^2 \pmod{n} \quad \text{και} \quad t \not\equiv \pm s \pmod{n},$$

τότε οι $\mu\kappa\delta(t \pm s, n)$ είναι μη τετριμμένοι παράγοντες του n. Πράγματι, σ΄ αυτή την περίπτωση, υπάρχει ακέραιος k με $t^2 - s^2 = kn$ και επομένως ισχύει $kn = (t+s)(t-s)$. Από την σχέση $t \not\equiv \pm s \pmod{n}$ έπεται ότι υπάρχουν πρώτοι διαιρέτες p και q του n με $p \not| t+s$, $p|t-s$ και $q|t+s$, $q \not| t-s$. Έτσι, έχουμε $1 < \mu\kappa\delta(t \pm s, n) < n$ και επομένως οι ακέραιοι $\mu\kappa\delta(t \pm s, n)$ είναι μη τετριμμένοι παράγοντες του n. Από την άλλη πλευρά έχουμε την εξής πρόταση:

Πρόταση 7.3 *Ας είναι $n = ab$, όπου $a, b \in \mathbb{Z}$ με $a, b > 1$ και $\mu\kappa\delta(a, b) = 1$. Τότε υπάρχουν $t, s \in \mathbb{Z}$ τέτοιοι, ώστε $t^2 \equiv s^2 \pmod{n}$ και $t \not\equiv \pm s \pmod{n}$.*

Απόδειξη. Θεωρούμε $y \in \mathbb{Z}$ με $\mu\kappa\delta(y, n) = 1$. Από την Πρόταση 5.11 έχουμε ότι υπάρχει $x \in \mathbb{Z}$ με $x \equiv y \pmod{a}$ και $x \equiv -y \pmod{b}$. Τότε $a|x-y$ και $b|x+y$. Έτσι, έχουμε $n|x^2 - y^2$ και επομένως $x^2 \equiv y^2 \pmod{n}$.

Αν $x \equiv y \pmod{n}$, τότε $x \equiv y \pmod{b}$ και επομένως $b|x-y$. Είδαμε παραπάνω ότι $b|x+y$. Έτσι, έχουμε $b|2y$. Καθώς $\mu\kappa\delta(y, n) = 1$, έπεται $\mu\kappa\delta(y, b) = 1$ και κατά συνέπεια $b = 2$ που είναι άτοπο γιατί ο n είναι περιττός. Αν $x \equiv -y \pmod{n}$, τότε έχουμε $x \equiv -y \pmod{a}$ και επομένως $a|x+y$. Καθώς $a|x-y$, παίρνουμε $a|2y$, απ΄ όπου καταλήγουμε, όπως παραπάνω, σε άτοπο. Άρα, ισχύει $x \not\equiv \pm y \pmod{n}$. □

Στο επόμενο παράδειγμα δίνουμε την παραγοντοποίηση ενός ακεραίου εφαρμόζοντας την παρατήρηση του Legendre.

Παράδειγμα 7.3 Θα παραγοντοποιήσουμε τον ακέραιο $n = 697483$. Έχουμε $\lfloor \sqrt{697483} \rfloor = 835$. Θεωρούμε τις τιμές $t = 835, 836, \ldots$ και

υπολογίζουμε τον ακέραιο $t^2 \mod n$. Για $t = 838$, βρίσκουμε:

$$838^2 \equiv 3^2\, 23^2 \,(\mathrm{mod}\, 697483).$$

Για $s = 3{\cdot}23$, υπολογίζουμε $\mu\kappa\delta(t{+}s, n) = 907$ και $\mu\kappa\delta(t{-}s, n) = 769$. Έτσι, έχουμε $n = 907 \cdot 769$.

7.2.2 Αλγόριθμος του *Dixon*

Στη συνέχεια θα περιγράψουμε τον αλγόριθμο του J. D. Dixon που δημοσιοποιήθηκε στα 1981 και μας δίνει μία πιο συστηματική μέθοδο για την εύρεση ακεραίων s και t με $t^2 \equiv s^2 \,(\mathrm{mod}\, n)$ και $t \not\equiv \pm s \,(\mathrm{mod}\, n)$. Πρώτα όμως θα εισάγουμε μερικές έννοιες που θα μας βοηθήσουν στη περιγραφή του αλγορίθμου.

Καλούμε *βάση παραγοντοποίησης* ένα σύνολο $B = \{-1, p_1, \ldots, p_h\}$, όπου $p_1, \ldots, p_h$ είναι διακεκριμμένοι πρώτοι. Ένας ακέραιος καλείται B-*λείος* αν γράφεται ως γινόμενο στοιχείων του B. Επίσης, ένας ακέραιος b καλείται B-*προσαρμοσμένος* ως προς τον θετικό ακέραιο n, αν υπάρχει B-λείος ακέραιος c, με $-n/2 \le c \le n/2$ και $b^2 \equiv c \,(\mathrm{mod}\, n)$.

Παράδειγμα 7.4 Ας είναι $B = \{-1, 2, 3, 5, 7\}$. Τότε οι ακέραιοι $40 = 2^3 \cdot 5$ και $63 = 3^2 \cdot 7$ είναι B-λείοι. Έχουμε

$$59^2 \equiv 40 \,(\mathrm{mod}\, 1147) \quad \text{και} \quad 71^2 \equiv 63 \,(\mathrm{mod}\, 2489).$$

Οπότε οι ακέραιοι 59 και 71 είναι B-προσαρμοσμένοι ως προς τους 1147 και 2489, αντίστοιχα.

Αλγόριθμος 7.1 Αλγόριθμος του Dixon.
Είσοδος: Περιττός σύνθετος ακέραιος $n > 3$.
Έξοδος: Ένας μη τετριμμένος παράγοντας του n.

1. Επιλέγουμε ένα θετικό ακέραιο y και θεωρούμε τη βάση παραγοντοποίησης B που σχηματίζεται από όλους τους πρώτους $p_1, \ldots, p_{\pi(y)}$ που είναι $\le y$.

2. Αν κανένα στοιχείο της B δεν διαιρεί τον n, τότε βρίσκουμε ακέραιους $b_i \in \{2, \ldots, n-1\}$ $(i = 1, \ldots, \pi(y) + 2)$ που είναι B-προσαρμοσμένοι ως προς τον n.

3. Γράφουμε
$$b_i^2 \equiv (-1)^{a_{i0}} p_1^{a_{i1}} \cdots p_{\pi(y)}^{a_{i\pi(y)}} \pmod{n},$$
και αντιστοιχούμε στο b_i το διάνυσμα $u_i = (u_{i0}, \ldots, u_{i\pi(y)})$, όπου $u_{ij} = 0$ αν ο a_{ij} είναι άρτιος και $u_{ij} = 1$ αν ο a_{ij} είναι περιττός.

4. Βρίσκουμε $T \subseteq \{1, \ldots, \pi(y)+2\}$ έτσι, ώστε να ισχύει
$$\sum_{i \in T} u_i = 0,$$
μέσα στο $\mathbb{Z}_2^{\pi(y)+1}$.

5. Υπολογίζουμε τις ποσότητες:
$$b = \prod_{i \in T} b_i, \quad c = p_1^{\gamma_1} \cdots p_{\pi(y)}^{\gamma_{\pi(y)}}$$
με
$$\gamma_j = \frac{1}{2} \sum_{i \in T} a_{i,j} \quad (j = 1, \ldots, \pi(y)).$$

6. Αν $b \not\equiv \pm c \pmod{n}$, τότε υπολογίζουμε τον $\mu\kappa\delta(b+c, n)$ ο οποίος είναι ένας μη τετριμμένος παράγοντας του n. Αν $b \equiv \pm c \pmod{n}$, τότε επιλέγουμε (αν είναι δυνατόν) άλλο σύνολο T ή παίρνουμε ένα μεγαλύτερο y και επαναλαμβάνουμε την διαδικασία.

Απόδειξη της Ορθότητας του Αλγόριθμου 7.1. Στο Βήμα 4, το πλήθος των διανυσμάτων u_i $(i = 1, \ldots, \pi(y)+2)$ είναι μεγαλύτερο από την διάσταση του διανυσματικού χώρου $\mathbb{Z}_2^{\pi(y)+1}$ και επομένως τα διανύσματα αυτά είναι γραμμικά εξαρτημένα. Έτσι, το σύνολο T υπάρχει πάντοτε και προσδιορίζεται εύκολα με απαλοιφή. Από την κατασκευή των b και c έχουμε $b^2 \equiv c^2 \pmod{n}$ και κατά συνέπεια, στην περίπτωση όπου $b \not\equiv \pm c \pmod{n}$, ο ακέραιος $\mu\kappa\delta(b+c, n)$ είναι ένας μη τετριμμένος παράγοντας του n. □

Παρατήρηση 7.1 Καθώς οι $p_1, \ldots, p_{\pi(y)}$ δεν διαιρούν τον n, έχουμε $\mu\kappa\delta(b, n) = 1$. Έτσι, αν ο n έχει r πρώτους παράγοντες $(r \geq 2)$, τότε, η πολυωνυμική ισοτιμία $x^2 \equiv b^2 \pmod{n}$ έχει ακριβώς 2^r λύσεις. Οπότε, η πιθανότητα να έχουμε $b \equiv \pm c \pmod{n}$ ισούται με $1/2^{r-1}$.

Ας σημειωθεί ότι στη περίπτωση όπου έχει επιλεγεί κατάλληλη βάση παραγοντοποίησης, ο χρόνος εκτέλεσης του αλγόριθμου είναι $O(e^{c\sqrt{\log n \log\log n}})$, όπου c είναι μία σταθερά (βλ. [9, Ενότητα 5.6.3] και [1, Ενότητα 8.3]).

Ένας απλός τρόπος εύρεσης των ακεραίων b_i είναι να δοκιμάζουμε ακέραιους της μορφής $\lfloor\sqrt{kn}\rfloor + j$ $(j = 0, 1, \ldots,\ k = 1, 2, \ldots)$. Ο μικρότερος κατ' απόλυτη τιμή ακέραιος της κλάσης του τετραγώνου τέτοιων ακεραίων κατά μέτρο n είναι αρκετά μικρός και κατά συνέπεια έχουν μεγάλη πιθανότητα να ειναι B-προσαρμοσμένοι ως προς τον n.

Παράδειγμα 7.5 Θα βρούμε την πρωτογενή ανάλυση του $n = 24139$. Θεωρούμε την βάση παραγοντοποίησης $B = \{-1, 2, 3, 5, 7, 11\}$. Καθώς η βάση B έχει 6 στοιχεία, θα προσδιορίσουμε τουλάχιστον 7 B-προσαρμοσμένους ακέραιους ως προς τον n. Δοκιμάζουμε ακέραιους της μορφής $\lfloor\sqrt{kn}\rfloor + j$, με $k, j = 1, \ldots,$ και προκύπτουν οι εξής ισοτιμίες:

$$\begin{aligned}
158^2 &\equiv 3 \cdot 5^2 \cdot 11 \pmod{n},\\
161^2 &\equiv 2 \cdot 3^4 \cdot 11 \pmod{n},\\
163^2 &\equiv 2 \cdot 3^5 \cdot 5 \pmod{n},\\
167^2 &\equiv 2 \cdot 3 \cdot 5^4 \pmod{n},\\
273^2 &\equiv 2^6 \cdot 3 \cdot 11 \pmod{n},\\
316^2 &\equiv 2^2 \cdot 3 \cdot 5^2 \cdot 11 \pmod{n},\\
392^2 &\equiv -3^7 \cdot 7 \pmod{n}.
\end{aligned}$$

Οπότε, παίρνουμε τα εξής διανύσματα του $\mathbb{Z}_2^6$:

$$\begin{aligned}
u_1 &= (0, 0, 1, 0, 0, 1),\\
u_2 &= (0, 1, 0, 0, 0, 1),\\
u_3 &= (0, 1, 1, 1, 0, 0),\\
u_4 &= (0, 1, 1, 0, 0, 0),\\
u_5 &= (0, 0, 1, 0, 0, 1),\\
u_6 &= (0, 0, 1, 0, 0, 1),\\
u_7 &= (1, 0, 1, 0, 1, 0).
\end{aligned}$$

Θεωρούμε το ομογενές γραμμικό σύστημα:

$$x_1u_1 + \cdots + x_7u_7 = 0,$$

με αγνώστους τους $x_1, \ldots, x_7$. Ισοδύναμα, έχουμε:

$$\begin{aligned} x_7 &= 0, \\ x_2 + x_3 + x_4 &= 0, \\ x_1 + x_3 + x_4 + x_5 + x_6 + x_7 &= 0, \\ x_3 &= 0, \\ x_1 + x_2 + x_5 + x_6 &= 0. \end{aligned}$$

Μία λύση του συστήματος είναι:

$$x_1 = x_5 = 1, \quad x_2 = x_3 = x_4 = x_6 = x_7 = 0.$$

Τότε παίρνουμε:

$$b = 158 \cdot 273 \bmod n = 18995 \quad \text{και} \quad c = 2^3 \cdot 3 \cdot 5 \cdot 11 = 1320.$$

Επίσης, ισχύει $-b \bmod n = 5144$. Επομένως, $b \not\equiv \pm c \pmod{n}$. Συνεπώς, δύο παράγοντες του n είναι οι $\mu\kappa\delta(b \pm c, n) = 239, 101$ οι οποίοι είναι πρώτοι. Άρα, η πρωτογενής ανάλυση του 24139 είναι: $24139 = 101 \cdot 239$.

7.2.3 Παραγοντοποίηση με Συνεχή Κλάσματα

Μία μέθοδος εύρεσης των ακεραίων b_i του Αλγορίθμου 7.1 είναι η δοκιμή μεταξύ των αριθμητών των συγκλινόντων ρητών του συνεχούς κλάσματος του $\sqrt{kn}$. Η χρήση των συνεχών κλασμάτων για παραγοντοποίηση ακεραίων ανάγεται στον M. Kraitchik (1920) και στους D. H. Lehmer και R. E. Powers (1931). Στα 1970, οι M. A. Morisson και J. Brillard υλοποίησαν την μέθοδο αυτή σε υπολογιστή και επέτυχαν την παραγοντοποίηση του έβδομου αριθμού του Fermat:

$$F_7 = 2^{128} + 1 = 59649589127497217 \times 5704689200685129054721.$$

Η χρήση των συνεχών κλασμάτων βασίζεται στην παρακάτω πρόταση:

Πρόταση 7.4 *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 $\sqrt{n}$. Τότε ισχύει:*

$$|P_k^2 - nQ_k^2| < 2\sqrt{n}.$$

Απόδειξη. Θα δείξουμε ότι $|P_k^2 - nQ_k^2| < 2\sqrt{n}$. Χρησιμοποιώντας την Πρόταση 2.2 παίρνουμε:

$$\begin{aligned} |P_k^2 - nQ_k^2| &= Q_k^2 \left|\sqrt{n} - \frac{P_k}{Q_k}\right| \left|\sqrt{n} + \frac{P_k}{Q_k}\right|, \\ &\leq Q_k^2 \left|\sqrt{n} - \frac{P_k}{Q_k}\right| \left(2\sqrt{n} + \left|\sqrt{n} - \frac{P_k}{Q_k}\right|\right), \\ &< Q_k^2 \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| \left(2\sqrt{n} + \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right|\right). \end{aligned}$$

Στη συνέχεια η ισότητα $P_kQ_{k+1} - P_{k+1}Q_k = (-1)^{k+1}$ δίνει:

$$|P_k^2 - nQ_k^2| < \frac{Q_k}{Q_{k+1}} \left(2\sqrt{n} + \frac{1}{Q_kQ_{k+1}}\right).$$

Έτσι, έχουμε:

$$\begin{aligned} |P_k^2 - nQ_k^2| - 2\sqrt{n} &< 2\sqrt{n} \left(-1 + \frac{Q_k}{Q_{k+1}} + \frac{1}{2\sqrt{n}\,Q_{k+1}^2}\right), \\ &< 2\sqrt{n} \left(-1 + \frac{Q_k}{Q_{k+1}} + \frac{1}{Q_{k+1}}\right), \\ &< 2\sqrt{n} \left(-1 + \frac{Q_{k+1}}{Q_{k+1}}\right) = 0 \end{aligned}$$

και επομένως ισχύει $|P_k^2 - nQ_k^2| < 2\sqrt{n}$. □

Πόρισμα 7.2 *Ο αντιπρόσωπος της κλάσης του P_k^2 κατά μέτρο n, που βρίσκεται μεταξύ του $-n/2$ και $n/2$, είναι ο $W_k = P_k^2 - nQ_k^2$. Επίσης, αν p είναι ένας πρώτος διαιρέτης του W_k, τότε $(n/p) = 1$.*

Απόδειξη. Καθώς ισχύει $P_k^2 \equiv P_k^2 - nQ_k^2 \pmod{n}$ και η Πρόταση 7.4 συνεπάγεται ότι $|P_k^2 - nQ_k^2| < 2\sqrt{n}$, παίρνουμε ότι ο $W_k = P_k^2 - nQ_k^2$ είναι ο αντιπρόσωπος της κλάσης του P_k^2 κατά μέτρο n που περιέχεται μεταξύ του $-n/2$ και $n/2$. Ας είναι p ένας πρώτος με $p|W_k$. Έτσι, έχουμε $P_k^2 \equiv nQ_k^2 \pmod{p}$. Αν $p|Q_k$, τότε $p|P_k$ και επομένως $\mu\kappa\delta(P_k, Q_k) > 1$ που είναι άτοπο. Άρα, ισχύει $p \not| Q_k$, και έτσι παίρνουμε $n \equiv (P_k/Q_k)^2 \pmod{p}$, απ' όπου $(n/p) = 1$. □

Καθώς έχουμε $|W_k| < 2\sqrt{n}$ και $P_k^2 \equiv W_k \pmod{n}$ μπορούμε να αναζητήσουμε τους ακέραιους b_i που χρησιμοποιούνται στον αλγόριθμο

του Dixon μεταξύ των P_k. Σ′ αυτή την περίπτωση, ο n είναι τετραγωνικό υπόλοιπο κατά μέτρο p για κάθε πρώτο διαιρέτη του W_k και κατά συνέπεια οι πρώτοι που αποτελούν την βάση παραγοντοποίησης θα πρέπει να επιλέγονται μεταξύ πρώτων p με $(n/p) = 1$. Έτσι, προκύπτει ο εξής αλγόριθμος:

Αλγόριθμος 7.2 Παραγοντοποίηση με συνεχή κλάσματα
Είσοδος: Περιττός σύνθετος ακέραιος $n > 3$.
Έξοδος: Ένας μη τετριμμένος παράγοντας του n.

1. Επιλέγουμε ένα θετικό ακέραιο y και θεωρούμε τη βάση παραγοντοποίησης B που σχηματίζεται από όλους τους πρώτους $p_1, \ldots, p_m$ που είναι $\leq y$ και ικανοποιούν την σχέση $(n/p_i) = 1$.

2. Αν κανένα στοιχείο της B δεν διαιρεί τον n, τότε για κάθε $i = 0, 1, \ldots$ κάνουμε τα εξής:

   (α′) Υπολογίζουμε τον συγκλίνοντα ρητό P_i/Q_i στο $\sqrt{n}$.

   (β′) Παραγοντοποιούμε τον $P_i^2 - nQ_i^2$, ώστε να ελέγξουμε αν ο P_i^2 είναι B-προσαρμοσμένος ως προς τον n.

   (γ′) Σταματάμε την διαδικασία όταν βρούμε ακέραιους $P_{i(j)}^2$ $(j = 1, \ldots, m+2)$ που είναι B-προσαρμοσμένοι ως προς τον n.

3. Ακολουθούμε τα Βήματα (3)-(5) του Αλγόριθμου 7.1 και βρίσκουμε ακέραιους b, c με $b^2 \equiv c^2 \pmod{n}$.

4. Αν $b \not\equiv \pm c \pmod{n}$, τότε υπολογίζουμε τον $\mu\kappa\delta(b+c, n)$ ο οποίος δίνει ένα μη τετριμμένο παράγοντα του n. Αν $b \equiv \pm c \pmod{n}$, τότε επιλέγουμε (αν είναι δυνατόν) άλλο σύνολο T, ή παίρνουμε ένα μεγαλύτερο y και επαναλαμβάνουμε την διαδικασία.

Παράδειγμα 7.6 Θα παραγοντοποιήσουμε τον ακέραιο $n = 13493$ χρησιμοποιώντας τον παραπάνω αλγόριθμο. Θεωρούμε την βάση παραγοντοποίησης $B = \{-1, 2, 7, 13, 31\}$. Η ανάπτυξη του $\sqrt{13493}$ σε συνεχές κλάσμα είναι:

$$\sqrt{13493} = [116, \overline{6, 3, 1, 1, 1, 3, 1, 4, 1, 7, 2, 7, 1, 4, 1, 3, 1, 1, 1, 3, 6, 232}].$$

Οι δέκα πρώτοι συγκλίνοντες ρητοί P_i/Q_i $(i = 0, \ldots, 9)$ στη τετραγωνική ρίζα $\sqrt{13493}$ είναι, αντίστοιχα, οι εξής:

$$116, \frac{697}{6}, \frac{2207}{19}, \frac{2904}{25}, \frac{5111}{44}, \frac{8015}{69}, \frac{29156}{251}, \frac{37171}{320}, \frac{177840}{1531}, \frac{215011}{1851}.$$

Θέτουμε $W_i = P_i^2 - nQ_i^2$ $(i = 0, \ldots, 8)$. Υπολογίζουμε:

$$W_0 = -37, \quad W_1 = 61, \quad W_2 = -2^2 \cdot 31, \quad W_3 = 7 \cdot 13, \quad W_4 = -127,$$

$$W_5 = 2^2 \cdot 13, \quad W_6 = -157, \quad W_7 = 41, \quad W_8 = -173, \quad W_9 = 2^2 \cdot 7.$$

Παρατηρούμε ότι μόνο οι ακέραιοι W_2, W_3, W_5, W_9 είναι B-λείοι και κατά συνέπεια οι P_2, P_3, P_5, P_9 είναι B-προσαρτημένοι ως προς τον n. Παίρνοντας $b = P_3P_5P_9$ και $c = 2^2 \cdot 7 \cdot 13 = 364$ προκύπτει η ισοτιμία $b^2 \equiv c^2 \pmod{n}$. Καθώς $\pm b \equiv 3042, 10451 \pmod{n}$, έχουμε $\pm b \not\equiv c \pmod{n}$. Έτσι, ο ακέραιος $\mu\kappa\delta(3042 + 364, 13493) = 131$ είναι ένας μη τετριμμένος παράγοντας του n. Οπότε, η πρωτογενής ανάλυση του n είναι $n = 131 \cdot 103$.

Η επιτυχία του παραπάνω αλγόριθμου συνίσταται κατά ένα μέρος στην ύπαρξη αρκετών διαφορετικών αριθμών της μορφής $P_i^2 - nQ_i^2$. Το πλήθος αυτών των αριθμών, όπως θα δούμε στην επόμενη πρόταση, ισούται με την περίοδο του συνεχούς κλάσματος του $\sqrt{n}$.

Πρόταση 7.5 *Ας είναι n ένας θετικός ακέραιος ο οποίος δεν είναι τετράγωνο ακεραίου, P_k/Q_k $(k = 0, 1, \ldots)$ οι συγκλίνοντες ρητοί στο $\sqrt{n}$ και m η περίοδος του συνεχούς κλάσματός του $\sqrt{n}$. Τότε η ακολουθία $|P_k^2 - nQ_k^2|$ $(k = 1, \ldots)$ είναι γνήσια περιοδική με περίοδο m. Επιπλέον, έχουμε $P_k^2 - nQ_k^2 > 0$ αν και μόνον αν ο k είναι περιττός.*

Απόδειξη. Ας είναι θ_k το k-στο πλήρες πηλίκο του $\sqrt{n}$. Σύμφωνα με την Πρόταση 2.3, για κάθε $k \geq 1$ ισχύει:

$$\sqrt{n} = \frac{P_k\theta_{k+1} + P_{k-1}}{Q_k\theta_{k+1} + Q_{k-1}},$$

απ' όπου παίρνουμε:

$$\theta_{k+1} = \frac{P_{k-1} - Q_{k-1}\sqrt{n}}{Q_k\sqrt{n} - P_k} = \frac{(Q_{k-1}\sqrt{n} - P_{k-1})(P_k + Q_k\sqrt{n})}{P_k^2 - nQ_k^2}.$$

Από την Πρόταση 3.1 έχουμε ότι η ακολουθία θ_k $(k = 1, 2, \ldots)$ είναι περιοδική με περίοδο m. Έτσι, από την παραπάνω ισότητα συνεπάγεται ότι η ακολουθία $|P_k^2 - nQ_k^2|$ $(k = 1, 2, \ldots)$ είναι επίσης περιοδική με περίοδο m. Επιπλέον, από την Πρόταση 2.2 έπεται ότι $P_k^2 - nQ_k^2 > 0$ για k περιττό και $P_k^2 - nQ_k^2 < 0$ για k άρτιο. □

Από τα παραπάνω βλέπουμε ότι στην περίπτωση όπου η περίοδος του συνεχούς κλάσματός του $\sqrt{n}$ είναι πολύ μικρή, είναι δυνατόν να έχουμε πολύ λίγους αριθμούς της μορφής $P_i^2 - nQ_i^2$ και κατά συνέπεια πολύ μικρή πιθανότητα να επιτύχουμε την παραγοντοποίηση του n. Το πρόβλημα αυτό παρουσιάστηκε κατά την προσπάθεια παραγοντοποίησης του έβδομου αριθμού του του Fermat F_7, καθώς η περίοδος του συνεχούς κλάσματος του $\sqrt{F_7}$ είναι 1 [7]. Σε τέτοιες περιπτώσεις, είναι δυνατόν να επιτευχθεί η παραγοντοποίηση του n, με την εφαρμογή του αλγορίθμου επί ενός αριθμού kn, όπου k είναι μικρός θετικός ακέραιος. Η μόνη διαφορά είναι ότι εξετάζουμε αν οι αριθμοί της μορφής $P_i^2 - knQ_i^2$ που προκύπτουν είναι B-προσαρμοσμένοι ως προς n και κατόπιν οι θεωρούμενες ισοτιμίες είναι κατά μέτρο n (και όχι ως προς kn). Επίσης, ο k πρέπει να είναι τετοιος, ώστε το ανάπτυγμα σε συνεχές κλάσμα του $\sqrt{kn}$ να έχει αρκετά μεγάλη περίοδο. Για την περίπτωση του F_7 χρησιμοποιήθηκε η τιμή $k = 257$. Δίνουμε στη συνέχεια ένα παράδειγμα μίας τέτοιας παραγοντοποίησης.

Παράδειγμα 7.7 Θα εφαρμόσουμε την παραπάνω μέθοδο για να παραγοντοποιήσουμε τον ακέραιο $n = 10001$. Το ανάπτυγμα σε συνεχές κλάσμα του $\sqrt{10001}$ είναι $\sqrt{10001} = [100, \overline{200}]$. Έτσι, αν P_i/Q_i $(i = 0, 1, \ldots)$ είναι οι συγκλίνοντες ρητοί στο $\sqrt{10001}$ και $W_i = P_i^2 - nQ_i^2$, τότε η ακολουθία $|W_i|$ $(i = 0, 1, \ldots)$ είναι περιοδική με περίοδο 1. Οι τέσσερεις πρώτοι συγκλίνοντες ρητοί είναι:

$$100, \quad \frac{20001}{200}, \quad \frac{4000300}{40001}, \quad \frac{800080001}{8000400}.$$

Έχουμε:

$$W_0 = -1, \quad W_1 = 1, \quad W_2 = -1, \quad W_3 = 1.$$

Έτσι, από την Πρόταση 7.5, έχουμε ότι $W_k = 1$, αν ο k είναι περιττός και $W = -1$, αν ο k είναι αρτιος. Τότε, έχουμε $P_i^2 \equiv \pm 1 \pmod{n}$, αν ο k είναι περιττός ή άρτιος, αντίστοιχα.

Στη συνέχεια, θα δείξουμε το εξής:

$$P_i \equiv \begin{cases} 100 \pmod{n} & \text{αν} \quad i \equiv 0 \pmod{4}, \\ -1 \pmod{n} & \text{αν} \quad i \equiv 1 \pmod{4}, \\ -100 \pmod{n} & \text{αν} \quad i \equiv 2 \pmod{4}, \\ 1 \pmod{n} & \text{αν} \quad i \equiv 3 \pmod{4}. \end{cases}$$

Έχουμε $P_0 = 100$, $P_1 = 20001 \equiv -1 \pmod{n}$, $P_2 = 4000300 \equiv -100 \pmod{n}$ και $P_3 = 800080001 \equiv 1 \pmod{n}$. Υποθέτουμε ότι οι

παραπάνω σχέσεις ισχύουν για κάθε θετικό ακέραιο $i \leq m$. Ας είναι $i = m + 1$. Αν $m + 1 \equiv 0 \pmod 4$, τότε $m - 1 \equiv 2 \pmod 4$ και $m \equiv 3 \pmod 4$. Έτσι, έχουμε:

$$P_{m+1} = 200P_m + P_{m-1} \equiv 200 \cdot 1 - 100 \equiv 100 \pmod n.$$

Αν $m + 1 \equiv 1 \pmod 4$, τότε $m - 1 \equiv 3 \pmod 4$ και $m \equiv 0 \pmod 4$. Οπότε, προκύπτει:

$$P_{m+1} = 200P_m + P_{m-1} \equiv 200 \cdot 100 + 1 \equiv -1 \pmod n.$$

Όμοια, αν $m + 1 \equiv 2, 3 \pmod 4$, έχουμε $P_{m+1} \equiv -100, 1 \pmod n$, αντίστοιχα. Συνεπώς, οι ακέραιοι P_i ικανοποιούν τις παραπάνω ισοτιμίες.

Έτσι, αν και για i περιττό ισχύει $P_i^2 \equiv 1 \pmod n$, καθώς έχουμε $P_i \equiv \pm 1 \pmod n$, οι ισοτιμίες αυτές δεν δίνουν την παραγοντοποίηση του n. Για i άρτιο έχουμε $P_i^2 \equiv -1 \pmod n$ και επομένως για i και j άρτια παίρνουμε $(P_iP_j)^2 \equiv 1 \pmod n$. Καθώς όμως ισχύει $P_iP_j \equiv \pm 10^4 \equiv \pm 1 \pmod n$, πάλι δεν μπορούμε να χρησιμοποιήσουμε αυτές τις σχέσεις για την παραγοντοποίηση του n. Συνεπώς, ο Αλγόριθμος 7.2 δεν μπορεί να παραγοντοποιήσει τον n.

Στη συνέχεια παίρνουμε $k = 2$ και θεωρούμε τον ακέραιο $kn = 20002$. Το ανάπτυγμα σε συνεχές κλάσμα του $\sqrt{2002}$ είναι:

$$\sqrt{20002} =< 141, \overline{2, 2, 1, 140, 1, 2, 2, 282} > .$$

Ο πρώτος συγκλίνων ρητός είναι ο 141 που δίνει την σχέση:

$$141^2 - 20002 = -11^2.$$

Ο δεύτερος συγκλίνων ρητός είναι ο $283/2$ που δίνει την ισότητα:

$$283^2 - 20002 \cdot 2^2 = 3^4,$$

απ΄ όπου έχουμε:

$$283^2 \equiv 9^2 \pmod{10001}.$$

Επιπλέον, ισχύει $283 \not\equiv \pm 9 \pmod{10001}$ και κατά συνέπεια ο ακέραιος $\mu\kappa\delta(283 + 9, 10001) = 73$ είναι ένας παράγοντας του n. Έτσι, παίρνουμε $10001 = 73 \cdot 137$.

7.3 Αλγόριθμος $p-1$ του *Pollard*

Σ′ αυτή την ενότητα θα περιγράψουμε τον αλγόριθμο $p-1$ ο οποίος δημοσιοποιήθηκε από τον J. Pollard στα 1974. Ο αλγόριθμος αυτός είναι αποτελεσματικός σε σύνθετους ακέραιους οι οποίοι έχουν ένα πρώτο παράγοντα p τέτοιον, ώστε ο $p-1$ να είναι γινόμενο μικρών πρώτων.

Αλγόριθμος 7.3 Αλγόριθμος $p-1$.
Είσοδος: Περιττός σύνθετος ακέραιος $n > 3$.
Έξοδος: Ένας μη τετριμμένος παράγοντας του n.

1. Επιλέγουμε έναν ακέραιο $B > 0$ και υπολογίζουμε το γινόμενο
$$k = \prod_{q \le B} q^{\lfloor \log_q B \rfloor},$$
όπου q διατρέχει το σύνολο των πρώτων $\le B$.
2. Επιλέγουμε $a \in \{2, \ldots, n-1\}$ και υπολογίζουμε $\delta = \mu\kappa\delta(a, n)$.
3. Αν $\delta > 1$, τότε ο δ είναι ένας μη τετριμμένος παράγοντας του n. Αν $\delta = 1$, τότε υπολογίζουμε $d = \mu\kappa\delta(a^k - 1, n)$.
4. Αν $1 < d < n$, τότε εξάγουμε τον d ο οποίος είναι ένας μη τετριμμένος παράγοντας του n. Αν $d = 1$ ή n, τότε επιλέγουμε έναν άλλο ακέραιο B και επαναλαμβάνουμε τα παραπάνω βήματα.

Απόδειξη της Ορθότητας του Αλγορίθμου 7.3. Ας είναι p ένας πρώτος παράγοντας του n τέτοιος, ώστε κάθε δύναμη πρώτου που διαιρεί τον $p-1$ είναι $\le B$. Τότε ο $p-1$ διαιρεί τον k και κατά συνέπεια ισχύει:
$$a^k \equiv 1 \pmod{p}.$$
Επομένως, ο p διαιρεί τον $a^k - 1$. Έτσι, αν $d \neq n$, τότε $1 < d < n$ και επομένως ο d είναι ένας μη τετριμμένος παράγοντας του n. □

Χρόνος Εκτέλεσης του Αλγορίθμου. Καθώς $k < B^B$, το Παράδειγμα 1.12 μας δίνει ότι ο χρόνος που απαιτεί ο υπολογισμός του k είναι $O((B \log B)^2)$ δυαδικές ψηφιακές πράξεις. Για τον υπολογισμό του $d = \mu\kappa\delta(a^k - 1, n)$, πρώτα υπολογίζουμε $b = a^k \bmod n$ και κατόπιν $\mu\kappa\delta(b, n)$. Οι χρόνοι που απαιτούνται γι′ αυτούς τους υπολογισμούς είναι $O(B(\log B)(\log n)^2)$ και $O((\log n)^2)$, αντίστοιχα. Άρα,

για τον υπολογισμό του d χρειάζονται $O(B(\log B)(\log n)^2)$ δυαδικές ψηφιακές πράξεις. Τέλος, ο χρόνος για τον υπολογισμό του $\mu\kappa\delta(a, n)$ είναι $O((\log n)^2)$. Συνεπώς, ο χρόνος που απαιτείται για την εκτέλεση του αλγόριθμου είναι

$$O(B(\log B)((\log n)^2 + B \log B))$$

δυαδικές ψηφιακές πράξεις. □

Παρατηρούμε ότι, αν χρησιμοποιήσουμε μικρό B, τότε ο αλγόριθμος είναι αρκετά ταχύς. Η πιθανότητα επιτυχίας του όμως είναι πολύ μικρή. Μόνο στη περίπτωση οπου ο n έχει ένα πρώτο παράγοντα p έτσι, ώστε ο $p-1$ να έχει αρκετά μικρούς πρώτους παράγοντες, ο αλγόριθμος θα μας δώσει γρήγορα αποτέλεσμα. Από την άλλη πλευρά, αν επιλέξουμε ένα μεγάλο B, τότε η πιθανότητα επιτυχίας του είναι αρκετά μεγάλη. Ένα σημαντικό μειονέκτημα σ΄ αυτή την περίπτωση είναι ότι ο αλγόριθμος γίνεται πολύ αργός.

Μπορούμε να κατασκευάσουμε ακέραιους οι οποίοι να παραγοντοποιούνται δύσκολα από αυτή την μέθοδο. Ας είναι p_1 και q_1 δύο αρκετά μεγάλοι πρώτοι της Germain. Τότε οι ακεραιοι $p = 2p_1 + 1$ και $q = 2q_1 + 1$ είναι πρώτοι. Σ΄ αυτή την περίπτωση, ο αλγόριθμος $p - 1$ δεν θα μπορέσει να παραγοντοποιήσει τον ακέραιο $n = pq$.

Παράδειγμα 7.8 Θα παραγοντοποιήσουμε τον ακέραιο 456917. Παίρνουμε $B = 17$ και υπολογίζουμε:

$$k = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 6126120.$$

Κατόπιν, έχουμε:

$$\mu\kappa\delta(2^{6126120} - 1, 456917) = 521.$$

Οπότε, παίρνουμε την παραγοντοποίηση $456917 = 521 \cdot 877$. Τέλος, εύκολα επαληθεύουμε ότι οι αριθμοί 521 και 877 είναι πρώτοι.

7.4 Αλγόριθμος ρ του *Pollard*

Στα 1975, ο J. Pollard δημοσιοποίησε τον αλγόριθμο παραγοντοποίησης ρ, τον οποίο παρουσιάζουμε σ΄ αυτή την ενότητα.

Αλγόριθμος 7.4 Αλγόριθμος ρ.
Είσοδος: Περιττός σύνθετος ακέραιος $n > 3$.
Έξοδος: Ένας μη τετριμμένος παράγοντας του n.

1. Επιλέγουμε $x_0 \in \{0, \ldots, n-1\}$, $f(x) \in \mathbb{Z}[x]$ και ορίζουμε την ακολουθία ακεραίων:
$$x_i = f(x_{i-1}) \bmod n \quad (i = 0, 1, \ldots).$$
2. Υπολογίζουμε τους $\mu\kappa\delta(x_i - x_{2i}, n)$ $(i = 0, 1, \ldots)$ μέχρι να βρούμε δείκτη k τέτοιον, ώστε να ισχύει $1 < \mu\kappa\delta(x_k - x_{2k}, n) < n$.
3. Εξάγουμε τον $\mu\kappa\delta(x_k - x_{2k}, n)$ ο οποίος είναι ένας μη τετριμμένος παράγοντας του n. Αν τέτοιος δείκτης k δεν είναι δυνατόν να προσδιοριστεί, τότε επαναλαμβάνουμε την διαδικασία παίρνοντας άλλη τιμή για το x_0 ή άλλο πολυώνυμο $f(x)$.

Απόδειξη της Ορθότητας του Αλγορίθμου 7.4. Ας είναι p ένας πρώτος διαιρέτης του n. Τότε για κάποιους δείκτες i, j με $i < j$ έχουμε $x_i \equiv x_j \pmod{p}$. Θα δείξουμε ότι για κάθε ακέραιο $m \geq 0$ ισχύει:
$$x_{i+m} \equiv x_{j+m} \pmod{p}.$$
Πράγματι, έχουμε:
$$f(x_i) \equiv f(x_j) \pmod{p}$$
και
$$x_{i+1} \equiv f(x_i) \pmod{n}, \quad x_{j+1} \equiv f(x_j) \pmod{n}.$$
Έτσι, παίρνουμε:
$$x_{i+1} \equiv x_{j+1} \pmod{p}.$$
Ας υποθέσουμε στη συνέχεια ότι για $m = k$ η προς απόδειξη σχέση ισχύει. Τότε, με τον ίδιο τρόπο, όπως παραπάνω, συμπεραίνουμε ότι ισχύει και για $m = k + 1$. Συνεπώς, ισχύει για κάθε ακέραιο $m \geq 0$.

Ας υποθέσουμε τώρα ότι i και j είναι οι μικρότεροι δείκτες με $i < j$ και $x_i \equiv x_j \pmod{p}$. Θέτουμε $l = j - i$. Οπότε, για κάθε ακέραιο $t \geq i$ έχουμε:
$$x_t \equiv x_{t+l} \pmod{p}.$$
Ας είναι r, s δείκτες με $s > r \geq i$ και $s - r \equiv 0 \pmod{l}$. Τότε $s = r + Al$ για κάποιο ακέραιο A. Έχουμε:
$$x_r \equiv x_{l+r} \equiv \ldots \equiv x_{(A-1)l+r} \equiv x_s \pmod{p}.$$

Μεταξύ των ακεραίων $i, \ldots, j-1$ υπάρχει ένας ο οποίος διαιρείται από τον l. Αν b είναι αυτός ο ακεραιος, τότε, σύμφωνα με τα παραπάνω, ισχύει:

$$x_b \equiv x_{2b} \pmod{p}.$$

Αν επί πλέον έχουμε:

$$x_b \not\equiv x_{2b} \pmod{n},$$

τότε $p \leq \mu\kappa\delta(x_b - x_{2b}, n) < n$ και επομένως ο $\mu\kappa\delta(x_b - x_{2b}, n)$ είναι ένας μη τετριμμένος παράγοντας του n. □

Ας είναι G το γράφημα το οποίο έχει ως κορυφές τους ακεραίους x_t $(t = 0, 1, \ldots)$ και πλευρές προσανατολισμένες από τον x_t στον x_{t+1}. Επομένως, το G αποτελείται από μία ουρά:

$$x \longrightarrow x_1 \longrightarrow \cdots \longrightarrow x_{i-1}$$

και ένα κύκλο μήκους l:

$$x_i \longrightarrow x_{i+1} \longrightarrow \cdots \longrightarrow x_j = x_i$$

ο οποίος επαναλαμβάνεται χωρίς τέλος. Έτσι, το γράφημα G έχει την μορφή του γράμματος ρ, απ΄ όπου προέρχεται το όνομα αλγόριθμος ρ.

Παρατηρούμε ότι αν στη παραπάνω απόδειξη ισχύει $x_i = x_j$, τότε για κάθε ζεύγος δεικτών s, t με $l|t-s$ έχουμε $x_s = x_t$. Οπότε, σ΄ αυτή την περίπτωση ο αλγόριθμος δεν δίνει αποτέλεσμα.

Παράδειγμα 7.9 Θα παραγοντοποιήσουμε τον ακέραιο $n = 7663$. Θεωρούμε το πολυώνυμο $f(x) = x^2 + 1$ και την τιμή $x_0 = 5$. Κατόπιν υπολογίζουμε τις τιμές:

$$x_1 = 26, \quad x_2 = 677, \quad x_3 = 6213, \quad x_4 = 2839$$

$$x_5 = 6109, \quad x_6 = 1072, \quad x_7 = 7398, \quad x_8 = 1259.$$

Τέλος, υπολογίζουμε τους μέγιστους κοινούς διαιρέτες:

$$\mu\kappa\delta(x_i - x_{2i}, n) = 1, \quad (i = 1, 2, 3)$$

και

$$\mu\kappa\delta(x_4 - x_8, n) = 79.$$

Οπότε, ο 79 είναι ένας παράγοντας του n και κατά συνέπεια έχουμε την παραγοντοποίηση $7663 = 79 \cdot 97$.

Στη συνέχεια θα υπολογίσουμε τον χρόνο που απαιτείται μέχρι να βρούμε δείκτες i και j έτσι, ώστε ο $x_j - x_i$ να διαιρείται από ένα πρώτο διαιρέτη του n.

Πρόταση 7.6 *Ας είναι S ένα σύνολο με m στοιχεία και ας υποθέσουμε ότι έχουμε την ομοιόμορφη κατανομή επί του S^k, όπου $m \geq k$. Αν*

$$k \geq \frac{1 + \sqrt{1 + 8m \log 2}}{2},$$

τότε η πιθανότητα ένα στοιχείο του S^k να έχει τουλάχιστον δύο συντεταγμένες ίδιες είναι $> 1/2$.

Απόδειξη. Συμβολίζουμε με D το υποσύνολο του S^k του οποίου τα στοιχεία έχουν συντεταγμένες διαφορετικές ανά δύο. Η πρώτη συνταταγμένη ενός τέτοιου στοιχείου μπορεί να επιλεγεί με m διαφορετικούς τρόπους, η δεύτερη με $m-1$ κ.ο.κ. Επομένως, έχουμε:

$$|D| = m(m-1)\cdots(m-k+1).$$

Καθώς έχουμε την ομοιόμορφη κατανομή επί του S^k, η πιθανότητα που αντιστοιχεί σε κάθε στοιχείο του S^k ισούται με $1/m^k$. Επομένως, η πιθανότητα του ενδεχομένου ένα στοιχείο του S^k ν΄ ανήκει στο D είναι:

$$q = \frac{m(m-1)\cdots(m-k+1)}{m^k} = \left(1 - \frac{1}{m}\right)\cdots\left(1 - \frac{k-1}{m}\right).$$

Χρησιμοποιώντας την ανισότητα:

$$1 + x \leq e^x, \quad \text{για κάθε } x \in \mathbb{R},$$

παίρνουμε:

$$q \leq e^{-(1+\cdots+(k-1))/m} = e^{-(k(k-1))/2m}.$$

Από την υπόθεση, έχουμε:

$$k \geq \frac{1 + \sqrt{1 + 8m\log 2}}{2},$$

και έτσι παίρνουμε $q \leq 1/2$. Άρα, η πιθανότητα ένα στοιχείο του S^k να έχει τουλάχιστον δύο συντεταγμένες ίδιες είναι $> 1/2$. □

Υποθέτουμε ότι η ακολουθία ακεραίων x_i έχει "τυχαία" συμπεριφορά και ότι

$$k \geq \frac{1+\sqrt{1+8p\log 2}}{2}.$$

Τότε, σύμφωνα με την Πρόταση 7.6, η πιθανότητα να υπάρχουν δείκτες $s < t \leq k$ με

$$x_s \equiv x_t \pmod{p}$$

είναι $> 1/2$. Σ' αυτή την περίπτωση, όπως είδαμε παραπάνω, υπάρχει δείκτης i με $s \leq i \leq t-1$ και

$$x_i \equiv x_{2i} \pmod{p}.$$

Επίσης, ο χρόνος που απαιτείται για τον υπολογισμό του x_i και του $\mu\kappa\delta(x_i - x_{2i}, n)$ είναι $O((\log n)^2)$. Έτσι, αν $p \leq \sqrt{n}$, τότε η πιθανότητα να βρεθεί i που να ικανοποιεί την παραπάνω ισοτιμία σε χρόνο $O(\sqrt[4]{n}(\log n)^2)$ είναι $> 1/2$.

7.5 Ασκήσεις

1. Να χρησιμοποιηθεί η μέθοδος του Fermat για να παραγοντοποιηθούν οι ακέραιοι 4601, 8633, 13199, 809009.

2. Να χρησιμοποιηθεί η γενίκευση της μεθόδου του Fermat για να παραγοντοποιηθούν οι αριθμοί 141467 και 68987.

3. Ας είναι $n = 4633$. Να βρεθεί η μικρότερη βάση παραγοντοποίησης B η οποία είναι τέτοια, ώστε οι αριθμοί 68, 69 και 96 είναι B-προσαρμοσμένοι ως προς n και με την βοήθεια της B να παραγοντοποιηθεί ο n.

4. Να χρησιμοποιηθεί ο αλγόριθμος του Dixon για να παραγοντοποιηθούν οι ακέραιοι 256961 και 1829.

5. Να χρησιμοποιηθεί η μέθοδος των συνεχών κλασμάτων για την παραγοντοποίηση των ακεραίων 17873, 13561 και 25511.

6. Να χρησιμοποιηθεί ο αλγόριθμος $p-1$ του Pollard για την παραγοντοποίηση των ακεραίων 16867 και 29651.

7. Να χρησιμοποιηθεί ο αλγόριθμος ρ του Pollard για την παραγοντοποίηση των ακεραίων 5141, 262063 και 25279.

8. Ας είναι m, n, a, b και c θετικοί ακέραιοι:
(α) Αν $m|b^a-1$, $m|b^c-1$ και $d=\mu\kappa\delta(a,c)$, τότε να δειχθεί ότι $m|b^d-1$.
(β) Αν p είναι ένας πρώτος διαιρέτης του b^n-1, τότε να δειχθεί ότι $p|b^\delta-1$ για κάποιο θετικό διαιρέτη δ του n με $\delta<n$ ή $p\equiv 1\,(\mathrm{mod}\,n)$. Αν $p>2$ και ο n είναι περιττός, τότε στη δεύτερη περίπτωση ισχύει $p\equiv 1\,(\mathrm{mod}\,2n)$.
(γ) Να χρησιμοποιηθεί το παραπάνω αποτέλεσμα για την παραγοντοποίηση των ακεραίων $2^{11}-1$ και $3^{12}-1$.

9. Ας είναι b και m ακέραιοι ≥ 2. Ένας πρώτος $p>2$ είναι παράγοντας του b^m+1 αν και μόνον αν είναι παράγοντας του $b^{2m}-1$.

Βιβλιογραφία

[1] J. A. Buchmann, *Introduction to Cryptography,* New York, Berlin, Heidelberg, Springer Verlag 2001.

[2] D. M. Bressoud, *Factorization and Primality Testing,* New York, Berlin, Heidelberg, Springer Verlag 1989.

[3] D. M. Bressoud and S. Wagon, *A Course in Computational Number Theory,* New York, Berlin, Heidelberg, Springer Verlag 2000.

[4] R. Crandall and C. Pomerance, *Prime Numbers, A Computational Perspective,* New York, Berlin, Heidelberg, Springer Verlag 2001.

[5] H. W. Lenstra Jr., Factoring integers with elliptic curves", *Annals of Mathematics* 126 (3) (1987), 649-673.

[6] A. K. Lenstra and H. W. Lenstra Jr, *The Develpment of the Number Field Sieve,* LNM vol. 1554, Springer 1993.

[7] M. A. Morrison and J. Brillhart, A method of factoring and the factorization of F_7, *Math. Comp.* 29 (1975), 183-205.

[8] C. Pomerance, A Tale of Two Sieves, Notices of the American Mathematical Society, 1996, 1473-1485.

[9] D. Stinson, *Cryptography - Theory and Practice,* Boca Raton, Florida, CRC Press 2002.

[10] S. Wagstaff, Jr, *The Joy of Factoring,* Student Mathematical Library 68, AMS 2013.

Κεφάλαιο 8

Διακριτός Λογάριθμος

Σύνοψη
Σ′ αυτό το κεφάλαιο θ′ ασχοληθούμε με το πρόβλημα του Διακριτού Λογαρίθμου και θα περιγράψουμε μερικούς βασικούς αλγόριθμους για την επίλυσή του. Πιο συγκεκριμένα, θα μελετήσουμε τον αλγόριθμο του Shanks, τον αλγόριθμο ρ του Pollard, τον αλγόριθμο των Pohlig-Hellman και τον αλγόριθμο του Adleman. Περισσότερες πληροφορίες μπορεί να βρεί ο αναγνώστης στις εξής πηγές: [1, 2, 3, 6, 5].

Προαπαιτούμενη γνώση
Κεφάλαια 1, 3, 4 και 5.

8.1 Πρόβλημα του Διακριτού Λογαρίθμου

Ας είναι $(G, \cdot)$ μία κυκλική ομάδα τάξης n και g ένας γεννήτοράς της. Τότε για κάθε $a \in G$ υπάρχει μοναδικός ακέραιος x με $0 \leq x \leq n-1$ τέτοιος, ώστε $a = g^x$. Ο ακέραιος x καλείται *διακριτός λογάριθμος* του a ως προς βάση g και συμβολίζεται με $\log_g a$. Το πρόβλημα της εύρεσης του x όταν είναι γνωστά τα g και a καλειται *Πρόβλημα του Διακριτού Λογαρίθμου.*

Η πιο απλή μέθοδος για τον υπολογισμό του διακριτού λογάριθμου είναι η *μέθοδος της απαρίθμησης,* δηλαδή, ο υπολογισμός των δυνάμεων $g, g^2, g^3, \ldots$, ώσπου να βρούμε x με $a = g^x$. Η μέθοδος αυτή όμως δεν είναι πρακτική στην περίπτωση όπου ο λογάριθμος x είναι αρκετά μεγάλος. Για παράδειγμα, αν έχουμε

$$1363^{337743} \equiv 63386 \pmod{356731},$$

τότε ο υπολογισμός του διακριτού λογαρίθμου απαιτεί 337742 πολλαπλασιασμούς μέσα στην ομάδα $\mathbb{Z}^*_{356731}$.

Η εύρεση του διακριτού λογάριθμου για πολλές ομάδες, όπως οι υποομάδες της πολλαπλασιαστικής ομάδας ενός πεπερασμένου σώματος $\mathbb{F}^*_q$, θεωρείται δύσκολο πρόβλημα και αλγόριθμος πολυωνυμικού χρόνου για την επίλυσή του δεν είναι γνωστός. Η δυσκολία αυτού του προβλήματος σε συνδυασμό με την ευκολία του υπολογισμού μίας δύναμης μέσα σε ένα πεπερασμένο σώμα κάνουν το πρόβλημα αυτό βάση για αρκετές κρυπτογραφικές εφαρμογές. Ας σημειωθεί ότι σήμερα ο ταχύτερος αλγόριθμος για την επίλυση του προβλήματος του διακριτού λογαρίθμου είναι υποεκθετικού χρόνου και οφείλεται στον D. M. Gordon. [2]

8.2 ''Βήμα βρέφους - βήμα γίγαντα''

Σ′ αυτή την ενότητα θα δώσουμε έναν αλγόριθμο για την εύρεση του διακριτού λογαρίθμου που προτάθηκε στα 1969 από τον D. Shanks [4].

Αλγόριθμος 8.1 ''Βήμα βρέφους - βήμα γίγαντα''.
Είσοδος: Μία κυκλική ομάδα $(G, \cdot)$ τάξης $n > 1$, g ένας γεννήτοράς της και $a \in G$.
Έξοδος: $x = \log_g a$.

1. Θέτουμε $m = \lfloor \sqrt{n} \rfloor + 1$.
2. Υπολογίζουμε τα στοιχεία του συνόλου
$$B = \{(ag^{-r}, r)/\ r = 0, \ldots, m-1\}.$$
Αν r είναι ο μικρότερος ακέραιος του $\{0, \ldots, m-1\}$ με $ag^{-r} = 1$, τότε εξάγουμε $x = r$.
3. Αν δεν βρούμε ένα τέτοιο r, τότε υπολογίζουμε $d = g^m$.
4. Για $q = 1, 2, 3, \ldots$ υπολογίζουμε τις δυνάμεις d^q μέχρις ότου να βρούμε $d^q = ag^{-r}$, για κάποιο $r \in \{0, \ldots, m-1\}$.
5. Εξάγουμε τον ακέραιο $x = qm + r$.

Απόδειξη της Ορθότητας του Αλγορίθμου. Αν υπάρχει ακέραιος $r \in \{0, \ldots, m-1\}$ με $ag^{-r} = 1$, τότε ισχύει $a = g^r$ και επομένως ο

μικρότερος εκθέτης r μ΄ αυτή την ιδιότητα είναι ο διακριτός λογάριθμος x. Ας υποθέσουμε ότι τέτοιος ακέραιος r δεν υπάρχει. Αν q είναι ο μικρότερος θετικός ακέραιος, ώστε να υπάρχει $r \in \{0, \ldots, m-1\}$ με $d^q = ag^{-r}$, τότε έχουμε $g^{mq+r} = a$. Ο $mq + r$ είναι ο μικρότερος θετικός ακέραιος μ΄ αυτή την ιδιότητα και επομένως είναι ο διακριτός λογάριθμος x.

Αντίστροφα, αν $x < m$, τότε στο δεύτερο βήμα του αλγόριθμου βρίσκουμε ακέραιο $r \in \{0, \ldots, m-1\}$ με $x = r$. Αν $x \geq m$, τότε υπάρχουν ακέραιοι q, r με $q > 0$ και $r \in \{0, \ldots, m-1\}$, ώστε $x = mq + r$ και επομένως $(g^m)^q = ag^{-r}$. Οπότε, στο τέταρτο βήμα του αλγόριθμου εντοπίζουμε τους ακέραιους q και r και κατά συνέπεια τον διακριτό λογάριθμο x. Συνεπώς, και στις δύο περιπτώσεις ο αλγόριθμος δίνει τον διακριτό λογάριθμο x. □

Οι υπολογισμοί του Βήματος 2 αναφέρονται ως ''βήματα βρέφους" και οι υπολογισμοί του Βήματος 4 ως ''βήματα γίγαντα''.

Παρατηρούμε ότι για το Βήμα 2 του αλγόριθμου μας απαιτείται ο υπολογισμός του αντιστρόφου του g, δηλαδή του g^{n-1}, και το πολύ m πολλαπλασιασμοί. Για τα Βήματα 3 και 4 απαιτείται η ύψωση του g στη δύναμη m και το πολύ m πολλαπλασιασμοί. Έτσι, από την Πρόταση 4.3 έχουμε ότι ο αλγόριθμος χρειάζεται $O(\sqrt{n})$ πράξεις μέσα στη G για να εκτελέσει τον υπολογισμό.

Αν $G = \mathbb{Z}_p^*$, τότε ο χρόνος εκτέλεσης των απαιτούμενων υπολογισμών είναι $O(\sqrt{p}\,(\log p)^2)$. Για τις κρυπτογραφικές εφαρμογές χρησιμοποιούνται πρώτοι $p > 2^{160}$ και επομένως ο αλγόριθμος αυτός δεν είναι αποτελεσματικός.

Επίσης, ας σημειωθεί ότι κατά την εκτέλεση του αλγορίθμου θα πρέπει να αποθηκευτούν τα στοιχεία του B και να συγκριθούν τα στοιχεία που παίρνουμε στο Βήμα 4 με τα στοιχεία του συνόλου B που προκύπτουν στο Βήμα 2.

Παράδειγμα 8.1 Θεωρούμε την ομάδα $\mathbb{Z}_{113}^*$. Ο ακέραιος 113 είναι πρώτος. Μία αρχική ρίζα κατά μέτρο 113 είναι ο ακέραιος 3. Χρησιμοποιώντας τον αλγόριθμο του Shanks θα υπολογίσουμε τον διακριτό λογάριθμο $\log_3 107$.

Έχουμε $\lfloor\sqrt{112}\rfloor + 1 = 11$. Πρώτα, υπολογίζουμε τα στοιχεία $3^{-r}107 \bmod 113$ $(r = 0, \ldots, 10)$ του συνόλου B και έτσι προκύπτουν τα εξής ζευγάρια:

$$(107, 0),\ (111, 1),\ (37, 2),\ (50, 3),\ (92, 4),\ (106, 5),$$

$$(73,6),\ (62,7),\ (96,8),\ (32,9),\ (86,10).$$

Έχουμε $3^{11} = 76 \bmod 113$. Κατόπιν υπολογίζουμε τις δυνάμεις:

$$76^2 \bmod 113 = 13,\ 76^3 \bmod 113 = 84,\ 76^4 \bmod 113 = 56,$$

$$76^5 \bmod 113 = 75,\ 76^6 \bmod 113 = 50.$$

Βλέπουμε ότι ο ακέραιος 50 είναι το πρώτο στοιχείο του τετάρτου ζεύγους της παραπάνω λίστας. Συνεπώς, έχουμε $\log_3 107 = 11 \cdot 6 + 3 = 69$.

8.3 Αλγόριθμος ρ του *Pollard*

Σ′ αυτή την ενότητα θα περιγράψουμε έναν αλγόριθμο για τον υπολογισμό του διακριτού λογάριθμου ο οποίος προτάθηκε στα 1978 από τον J. Pollard.

Αλγόριθμος 8.2 Αλγόριθμος ρ.
Είσοδος: Μία κυκλική ομάδα $(G, \cdot)$ τάξης $n > 1$, g ένα γεννήτοράς της και $\beta \in G$ με $\beta \neq 1$.
Έξοδος: $x = \log_g \beta$.

1. Θεωρούμε τρία μη κενά υποσύνολα S_1, S_2, S_3 του G με $S_1 \cup S_2 \cup S_3 = G$, $1 \notin S_2$ και $S_i \cap S_j = \emptyset$ για $i \neq j$ και ορίζουμε την απεικόνιση:

$$f : G \times \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow G \times \mathbb{Z}_n \times \mathbb{Z}_n$$

με

$$f(x,a,b) = \begin{cases} (\beta x, a, b+1 \bmod n) & \text{αν} \quad x \in S_1, \\ (x^2, 2a \bmod n, 2b \bmod n) & \text{αν} \quad x \in S_2, \\ (gx, a+1 \bmod n, b) & \text{αν} \quad x \in S_3. \end{cases}$$

2. Ορίζουμε την ακολουθία:

$$(x_i, a_i, b_i) = \begin{cases} (1,0,0) & \text{αν} \quad i = 0, \\ f(x_{i-1}, a_{i-1}, b_{i-1}) & \text{αν} \quad i \geq 1. \end{cases}$$

3. Συγκρίνουμε τις τριάδες (x_i, a_i, b_i) και (x_{2i}, a_{2i}, b_{2i}) μέχρι να βρούμε $i \geq 1$, ώστε $x_{2i} = x_i$.

4. Επιλύουμε την γραμμική ισοτιμία:

$$(b_{2i} - b_i)z \equiv a_i - a_{2i} \pmod{n}.$$

5. Μία από τις λύσεις της παραπάνω ισοτιμίας είναι ο ζητούμενος λογάριθμος $x = \log_g \beta$.

Απόδειξη της Ορθότητας του Αλγορίθμου. Καθώς $1 \notin S_2$, έχουμε $(x_1, a_1, b_1) \neq (1, 0, 0)$ και κατά συνέπεια η ακολουθία (x_i, a_i, b_i) $(i = 0, 1, \ldots)$ έχει στοιχεία διαφορετικά από το $(1, 0, 0)$. Εύκολα διαπιστώνουμε ότι αν μία τριάδα (x, a, b) ικανοποιεί την ισότητα $x = g^a\beta^b$, τότε η $f(x, a, b)$ επίσης την ικανοποιεί. Η τριάδα $(1, 0, 0)$ έχει αυτή την ιδιότητα και επομένως ισχύει:

$$x_i = g^{a_i}\beta^{b_i} \quad (i = 1, 2, \ldots).$$

Η ομάδα G είναι πεπερασμένη και έτσι υπάρχουν ακέραιοι λ και $\mu \in$ τέτοιοι, ώστε $x_\lambda = x_{\lambda+\mu}$. Ας υποθέσουμε ότι λ και μ είναι οι μικρότεροι ακέραιοι μ΄ αυτή την ιδιότητα. Καθώς η κατασκευή του x_{s+1} εξαρτάται από το x_s, η ακολουθία $x_\lambda, x_{\lambda+1}, \ldots$ είναι περιοδική με μήκος περιόδου ίσο με μ.

Θέτουμε:

$$i = \mu(1 + \lfloor \lambda/\mu \rfloor).$$

Έχουμε $\lambda < i \leq \lambda + \mu$ και $x_i = x_{2i}$. Άρα

$$g^{a_{2i}}\beta^{b_{2i}} = g^{a_i}\beta^{b_i}.$$

Αν $w = \log_g \beta$, τότε

$$g^{a_{2i}+wb_{2i}} = g^{a_i+wb_i}$$

και επομένως

$$a_{2i} + wb_{2i} \equiv a_i + wb_i \pmod{n}.$$

Συνεπώς, ο ακέραιος w είναι μία λύση της γραμμικής ισοτιμίας

$$(b_{2i} - b_i)z \equiv a_i - a_{2i} \pmod{n}. \quad \square$$

Υποθέτοντας ότι η ακολουθία $x_0, x_1, \ldots$ έχει "τυχαία" συμπεριφορά, συμπεραίνουμε από την Πρόταση 7.6 ότι η πιθανότητα εύρεσης δεικτών i και j με $x_i = x_j$, μετά από $O(\sqrt{n})$ βήματα, είναι $> 1/2$.

Επομένως, η πιθανότητα να ισχύει $\lambda + \mu = O(\sqrt{n})$ είναι $> 1/2$. Έτσι, η πιθανότητα της εύρεσης δείκτη i με $x_i = x_{2i}$ και $i = O(\sqrt{n})$ είναι $> 1/2$. Βλέπουμε λοιπόν ότι σε κυκλικές ομάδες πολύ μεγάλης τάξης ο αλγόριθμος αυτός δεν είναι γενικά αποτελεσματικός.

Παράδειγμα 8.2 Ο ακέραιος 809 είναι πρώτος. Θα υπολογίσουμε την τάξη του 7 μέσα στην ομάδα $\mathbb{Z}^*_{809}$. Έχουμε $\phi(809) = 808$ και η πρωτογενής ανάλυση του 808 είναι $808 = 2^3 \cdot 101$. Άρα, έχουμε $\mathrm{ord}_{809}7 \in \{2, 4, 8, 101, 202, 404, 808\}$. Καθώς

$$7^2 \mod 809 = 49, \quad 7^4 \mod 809 = 783,$$

$$7^8 \mod 809 = 676, \quad 7^{101} \mod 809 = 1,$$

παίρνουμε $\mathrm{ord}_{809}7 = 101$.

Συμβολίζουμε με G την υποομάδα της $\mathbb{Z}^*_{809}$ που παράγεται από το 7. Θα εξετάσουμε αν ο ακέραιος 422 ανήκει στη G και αν ναι θα βρούμε ταυτόχρονα τον διακριτό λογάριθμο $\log_7 422$ εφαρμόζοντας τον αλγόριθμο ρ. Θεωρούμε τα παρακάτω υποσύνολα του G:

$$S_1 = \{x \in G / \ x \equiv 1 \pmod 3\},$$

$$S_2 = \{x \in G / \ x \equiv 0 \pmod 3\},$$

$$S_3 = \{x \in G / \ x \equiv 2 \pmod 3\},$$

και ορίζουμε την απεικόνιση

$$f : G \times \mathbb{Z}_{101} \times \mathbb{Z}_{101} \longrightarrow G \times \mathbb{Z}_{101} \times \mathbb{Z}_{101}$$

θέτοντας

$$\begin{aligned} f(x, a, b) &= (422x \mod 809, a, b + 1 \mod 101) \\ &= (x^2 \mod 809, 2a \mod 101, 2b \mod 101) \\ &= (7x \mod 809, a + 1 \mod 101, b), \end{aligned}$$

για $x \in S_1$, $x \in S_2$ και $x \in S_3$, αντίστοιχα.

Υπολογίζουμε τις τριάδες (x_i, a_i, b_i) και (x_{2i}, a_{2i}, b_{2i}) μέχρι να βρούμε $i \geq 1$, ώστε $x_{2i} = x_i$. Έτσι προκύπτει ο παρακάτω πίνακας:

i	(x_i, a_i, b_i)	(x_{2i}, a_{2i}, b_{2i})
1	$(422, 0, 1)$	$(527, 1, 1)$
2	$(527, 1, 1)$	$(532, 4, 2)$
3	$(453, 2, 1)$	$(649, 8, 6)$
4	$(532, 4, 2)$	$(349, 8, 8)$
5	$(411, 4, 3)$	$(700, 8, 10)$
6	$(649, 8, 6)$	$(799, 8, 12)$
7	$(436, 8, 7)$	$(578, 8, 14)$
8	$(349, 8, 8)$	$(422, 9, 15)$
9	$(40, 8, 9)$	$(453, 11, 15)$
10	$(700, 8, 10)$	$(411, 22, 31)$
11	$(115, 8, 11)$	$(436, 44, 63)$
12	$(799, 8, 12)$	$(40, 44, 65)$
13	$(634, 8, 13)$	$(115, 44, 67)$
14	$(578, 8, 14)$	$(634, 44, 69)$
15	$(1, 9, 14)$	$(1, 45, 70)$

Έχουμε $x_{15} = x_{30}$ και επομένως ο ζητούμενος λογάριθμος επαληθεύει την ισοτιμία

$$(70 - 14)z \equiv 9 - 45 \pmod{101}$$

η οποία έχει μοναδική λύση $z \equiv 21 \pmod{101}$. Άρα, ο ακέραιος 422 ανήκει στη G και ισχύει $\log_7 422 = 21$.

8.4 Αλγόριθμος των *Pohlig – Hellman*

Ας είναι $(G, \cdot)$ μία κυκλική ομάδα τάξης $n > 1$. Υποθέτουμε ότι η πρωτογενής ανάλυση του n είναι γνωστή και έχουμε:

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

όπου $p_1, \ldots, p_k$ διαφορετικοί πρώτοι και $e_1, \ldots, e_k$ θετικοί ακέραιοι.

Σ′ αυτή την ενότητα θα περιγράψουμε έναν αλγόριθμο που προτάθηκε στα 1978 από τους των S. Pohlig και M. Hellman, ο οποίος ανάγει τον υπολογισμό ενός διακριτού λογαρίθμου μέσα στη G σε προβλήματα υπολογισμού διακριτών λογαρίθμων μέσα σε k υποομάδες της G τάξης $p_1, \ldots, p_k$, αντίστοιχα.

Αλγόριθμος 8.3 Αλγόριθμος των Pohlig-Hellman. .
Είσοδος: Μία κυκλική ομάδα $(G,\cdot)$ τάξης $n>1$, η πρωτογενής ανάλυση του n, $n=p_1^{e_1}\cdots p_k^{e_k}$, όπου $p_1,\ldots,p_k$ διαφορετικοί πρώτοι και $e_1,\ldots,e_k$ θετικοί ακέραιοι, g ένα γεννήτοράς της G και $a\in G$.
Έξοδος: $x=\log_g a$.

1. Για κάθε $i=1,\ldots,k$ υπολογίζουμε τις ποσότητες: $n_i=n/p_i^{e_i}$, $g_i=g^{n_i}$, $a_i=a^{n_i}$ και $\gamma_i=g_i^{p_i^{e_i-1}}$ $(i=1,\ldots,k)$.

2. Για κάθε $i=1,\ldots,k$ υπολογίζουμε τους διακριτούς λογάριθμους: $x_{i,0}=\log_{\gamma_i} a_i^{p_i^{e_i-1}}$ και

$$x_{i,j}=\log_{\gamma_i}(a_i g_i^{-(x_{i,0}+\cdots+x_{i,j-1}p_i^{j-1})})^{p_i^{e_i-1-j}} \quad (j=1,\ldots,e_i-1).$$

3. Για κάθε $i=1,\ldots,k$ υπολογίζουμε το άθροισμα:

$$x_i=x_{i,0}+x_{i,1}p_i+\cdots+x_{i,e_i-1}p_i^{e_i-1}.$$

4. Υπολογίζουμε έναν ακέραιο x με $0\le x\le n-1$ και

$$x\equiv x_i \pmod{p_i^{e_i}} \quad (i=1,\ldots,k).$$

5. Ο ακέραιος x είναι ο διακριτός λογάριθμος $x=\log_g a$.

Απόδειξη της Ορθότητας του Αλγορίθμου. Πρώτα, παρατηρούμε ότι το g_i παράγει μία κυκλική ομάδα τάξης $p_i^{e_i}$. Έτσι, καθώς $a_i=g_i^x$, έχουμε $a_i\in\langle g_i\rangle$. Θέτουμε $x_i=\log_{g_i} a_i$ $(i=1,\ldots,k)$. Η παράσταση του x_i στη κλίμακα του p_i είναι:

$$x_i=x_{i,0}+x_{i,1}p_i+\cdots+x_{i,e_i-1}p_i^{e_i-1},$$

όπου $x_{i,j}\in\{0,\ldots,p_i-1\}$. Η ισότητα $a_i=g_i^{x_i}$ δίνει:

$$a_i^{p_i^{e_i-1}}=g_i^{x_i p_i^{e_i-1}}=(g_i^{p_i^{e_i-1}})^{x_{i,0}}.$$

Η τάξη του στοιχείου $g_i^{p_i^{e_i-1}}$ είναι p_i και επομένως ο ακέραιος $x_{i,0}$ είναι ο διακριτός λογάριθμος του $a_i^{p_i^{e_i-1}}$ ως προς βάση $g_i^{p_i^{e_i-1}}$. Ας υποθέσουμε ότι έχουμε προσδιορίσει τους ακέραιους $x_{i,0},\ldots,x_{i,j-1}$. Τότε:

$$g_i^{x_{i,j}p_i^j+\cdots+x_{i,e_i}p_i^{e_i-1}}=a_i g_i^{-(x_{i,0}+\cdots+x_{i,j-1}p_i^{j-1})}.$$

Υψώνοντας και τα δύο μέλη της ισότητας στη δύναμη $p_i^{e_i-1-j}$ παίρνουμε:

$$(g_i^{p_i^{e_i-1}})^{x_{i,j}} = (a_i g_i^{-(x_{i,0}+\cdots+x_{i,j-1}p_i^{j-1})})^{p_i^{e_i-1-j}}.$$

Οπότε ο διακριτός λογάριθμος του $(a_i g_i^{-(x_{i,0}+\cdots+x_{i,j-1}p_i^{j-1})})^{p_i^{e_i-1-j}}$ ως προς βάση $g_i^{p_i^{e_i-1}}$ είναι ο $x_{i,j}$. Έτσι, αφού έχουμε υπολογίσει τους ακεραίους $x_{i,j}$ $(j = 0, \ldots, p_i - 1)$, παίρνουμε τον x_i.

Σύμφωνα με την Πρόταση 5.11, υπάρχει $x \in \{0, \ldots, n-1\}$ έτσι, ώστε να ισχύει:

$$x \equiv x_i \,(\mathrm{mod}\, p_i^{e_i}) \quad (i = 1, \ldots, k).$$

Τότε, έχουμε:

$$(g^{-x}a)^{n_i} = g_i^{-x_i} a_i = 1 \quad (i = 1, \ldots, k).$$

Οπότε, η τάξη του $g^{-l}a$ διαιρεί καθένα από τα n_i και επομένως διαιρεί τον μέγιστο κοινό διαιρέτη τους που είναι ο 1. Άρα, $g^x = a$ και κατά συνέπεια $\log_g a = x$. □

Ο υπολογισμός των δυνάμεων g_i, a_i και γ_i απαιτεί $O(\log n)$ πράξεις μέσα στην ομάδα G. Για τον προσδιορισμό κάθε $x_{i,j}$ απαιτούνται $O(\log n)$ πράξεις μέσα στη G για τον υπολογισμό των δυνάμεων και $O(\sqrt{p_i})$ πράξεις μέσα στη G για τον υπολογισμό του διακριτού λογάριθμου με τον αλγόριθμο του Shanks. Επομένως, για τον προσδιορισμό του x_i χρειάζονται $O(e_i(\log n + \sqrt{p_i}))$ πράξεις μέσα στη G. Συνεπώς, ο χρόνος εκτέλεσης του αλγορίθμου απαιτεί $O(\sum_{i=1}^{k} e_i(\log n + \sqrt{p_i}))$ πράξεις μέσα στην ομάδα G. Τέλος, ο χρόνος επίλυσης του συστήματος των γραμμικών ισοτιμιών στο Βήμα 4 είναι $O((\log n)^2)$ δυαδικές ψηφιακές πράξεις.

Παρατηρούμε ότι αν όλοι οι πρώτοι παράγοντες του n είναι μικροί, ο υπολογισμός του διακριτού λογάριθμου είναι σχετικά εύκολος. Για παράδειγμα, Ο ακέραιος $p = 2 \cdot 3 \cdot 5^{278} + 1$ είναι πρώτος και το μήκος του ισούται με 649. Ο πρώτοι διαιρέτες της τάξης $p-1$ της ομάδας $\mathbb{Z}_p^*$ είναι οι 2, 3, 5 και επομένως ο υπολογισμός ενός διακριτού λογάριθμου σ΄ αυτή την ομάδα είναι αρκετά ταχύς.

Παράδειγμα 8.3 Ο ακέραιος 929 είναι πρώτος και ο 3 μία αρχική ρίζα κατά μέτρο 929. Οπότε, ο ακέραιος 3 είναι ένας γεννήτορας της

ομάδας $\mathbb{Z}_{929}^*$. Η πρωτογενής ανάλυση της τάξης της είναι $929 = 2^5 29$. Χρησιμοποιώντας τον αλγόριθμο των Pohlig-Hellman θα υπολογίσουμε τον διακριτό λογάριθμο $\log_3 79$ μέσα στην ομάδα $\mathbb{Z}_{929}^*$.

Πρώτα υπολογίζουμε τις ποσότητες:

$$n_1 = 29, \quad g_1 = 3^{29} \bmod 929 = 701, \quad a_1 = 79^{29} \bmod 929 = 759,$$

$$n_2 = 32, \quad g_2 = 3^{32} \bmod 929 = 347, \quad a_2 = 79^{32} \bmod 929 = 537,$$

$$\gamma_1 = g_1^{2^4} = 701^{16} \bmod 929 = 928, \quad \gamma_2 = g_2 = 347.$$

Κατόπιν, υπολογίζουμε:

$$(759 \cdot 701^{-1})^8 \bmod 929 = 928, \quad (759 \cdot 701^{-3})^4 \bmod 929 = 1,$$

$$(759 \cdot 701^{-3})^2 \bmod 929 = 1, \quad 759 \cdot 701^{-3} \bmod 929 = 1$$

και παίρνουμε:

$$x_{1,0} = \log_{\gamma_1} a_1^{16} = \log_{928} 928 = 1,$$

$$x_{1,1} = \log_{\gamma_1} (a_1 g_1^{-x_{1,0}})^8 = \log_{928} 928 = 1,$$

$$x_{1,2} = \log_{\gamma_1} (a_1 g_1^{-x_{1,0} - x_{1,1} 2})^4 = \log_{928} 1 = 0,$$

$$x_{1,3} = \log_{\gamma_1} (a_1 g_1^{-x_{1,0} - x_{1,1} 2 - x_{1,2} 2^2})^2 = \log_{928} 1 = 0,$$

$$x_{1,4} = \log_{\gamma_1} a_1 g_1^{-x_{1,0} - x_{1,1} 2 - x_{1,2} 2^2 - x_{1,3} 2^3} = \log_{928} 1 = 0.$$

Εφαρμόζοντας έναν από τους αλγόριθμους των δύο προηγουμένων ενοτήτων, προκύπτει:

$$x_{2,0} = \log_{\gamma_2} a_2 = \log_{347} 537 = 6.$$

Έτσι, έχουμε:

$$x_1 = x_{1,0} + x_{1,1} 2 + x_{1,2} 2^2 + x_{1,3} 2^3 + x_{1,4} 2^4 = 3$$

και

$$x_2 = x_{2,0} = 6.$$

Τέλος, λύνουμε το σύστημα

$$x \equiv 3 \pmod{32}, \quad x \equiv 6 \pmod{29}$$

και παίρνουμε $x = 35$. Άρα $\log_3 79 = 35$.

8.5 Λογισμός Δεικτών

Σ΄ αυτή την ενότητα θα περιγράψουμε έναν απλό αλγόριθμο για τον υπολογισμό του διακριτού λογάριθμου μέσα στην ομάδα $\mathbb{Z}_p^*$, όπου p πρώτος Η τελική μορφή του παρουσιάστηκε στα 1979 και οφείλεται στον L. M. Adleman [1].

Αλγόριθμος 8.4 Αλγόριθμος Λογισμού Δεικτών.
Είσοδος: Ένας πρώτος αριθμός p, μία αρχική ρίζα g κατά μέτρο p, με $g \in \{1, \ldots, p-1\}$, και $a \in \{1, \ldots, p-1\}$.
Έξοδος: $x = \log_g a$.

1. Επιλεγουμε ένα θετικό ακέραιο B, με $B < p$, και θεωρούμε το σύνολο $F(B)$ όλων των πρώτων $\leq B$.

2. Για κάθε $q \in F(B)$, υπολογίζουμε τον διακριτό λογάριθμο $x(q) = \log_g q$, μέσα στην ομάδα $\mathbb{Z}_p^*$.

3. Προσδιορίζουμε $y \in \{0, \ldots, p-1\}$ έτσι, ώστε

$$ag^y \equiv \prod_{q \in F(B)} q^{e(q)} \pmod{p},$$

   όπου $e(q)$ είναι ακέραιοι ≥ 0.

4. Ο ζητούμενος διακριτός λογάριθμος ορίζεται από την εξής σχέση:

$$\log_g a \equiv \sum_{q \in F(B)} x(q)e(q) - y \pmod{p-1}.$$

Απόδειξη της Ορθότητας του Αλγορίθμου. Ισχύει:

$$ag^y \equiv \prod_{q \in F(B)} q^{e(q)} \equiv \prod_{q \in F(B)} g^{x(q)e(q)} \equiv g^{\sum_{q \in F(B)} x(q)e(q)} \pmod{p},$$

απ΄ όπου:

$$a \equiv g^{\sum_{q \in F(B)} x(q)e(q) - y} \pmod{p}.$$

Συνεπώς, έχουμε:

$$\log_g a \equiv \sum_{q \in F(B)} x(q)e(q) - y \pmod{p-1}. \quad \square$$

Θα δούμε στη συνέχεια την μέθοδο υπολογισμού των διακριτών λογαρίθμων $x(q)$ των στοιχείων του $F(B)$. Επιλέγουμε τυχαία ακέραιους $z \in \{1, \ldots, p-1\}$ και υπολογίζουμε τις δυνάμεις g^z. Αν ισχύει

$$g^z \equiv \prod_{q \in F(B)} q^{f(q,z)} \pmod{p},$$

όπου $f(q,z)$ είναι ακέραιοι ≥ 0, τότε

$$g^z \equiv \prod_{q \in F(B)} g^{x(q)f(q,z)} \equiv g^{\sum_{q \in F(B)} x(q)f(q,z)} \pmod{p},$$

και επομένως παίρνουμε:

$$z \equiv \sum_{q \in F(B)} x(q)f(q,z) \pmod{p-1}.$$

Βρίσκουμε λοιπόν τουλάχιστον τόσους τέτοιους ακέραιους z όσο είναι το πλήθος των στοιχείων του $F(B)$ έτσι, ώστε το σύστημα που θα προκύψει από γραμμικές ισοτιμίες της παραπάνω μορφής να έχει μοναδική λύση. Συνεπώς, η λύση αυτού του συστήματος δίνει τους διακριτούς λογάριθμους $x(q)$, $q \in F(B)$.

Ο χρόνος που απαιτείται για την λειτουργία του αλγορίθμου του λογισμού δεικτών είναι $L_p(1/2; c + o(1))$, όπου $o(1)$ είναι μία συνάρτηση η οποία συγκλίνει στο μηδέν όταν ο πρώτος p τείνει στο άπειρο και c μία σταθερά. Καθώς οι τρείς αλγόριθμοι που περιγράψαμε στις προηγούμενες ενότητες είναι εκθετικού τύπου, ο αλγόριθμος του λογισμού δεικτών είναι ταχύτερος από αυτούς και κατά συνέπεια είναι προτιμότερος για την περίπτωση της ομάδας $\mathbb{Z}_p^*$.

Παράδειγμα 8.4 Ο ακέραιος $p = 1013$ είναι πρώτος και ο 3 μία αρχική ρίζα κατά μέτρο p. Θα υπολογίσουμε, χρησιμοποιώντας τη μέθοδο του λογισμού δεικτών τον διακριτό λογάριθμο $\log_3 745$.

Παίρνουμε $B = 11$. Οπότε $F(B) = \{2, 3, 5, 7, 11\}$. Θα υπολογίσουμε τους διακριτούς λογάριθμους των κλάσεων 2, 3, 5, 7 και 11. Έχουμε:

$$\begin{aligned} 3^{53} &\equiv 2^2 \cdot 5 \cdot 11 \,(\mathrm{mod}\, 1013), \\ 3^{56} &\equiv 5^3 \cdot 7 \,(\mathrm{mod}\, 1013), \\ 3^{58} &\equiv 2^4 \cdot 7^2 \,(\mathrm{mod}\, 1013), \\ 3^{73} &\equiv 2^3 \,(\mathrm{mod}\, 1013). \end{aligned}$$

Ας είναι $x(2)$, $x(3)$, $x(5)$, $x(7)$ και $x(11)$ οι διακριτοί λογάριθμοι των κλάσεων 2,3, 5, 7 και 11, αντίστοιχα ως προς βάση 3. Τότε έχουμε $x(3) = 1$ και το εξής σύστημα γραμμικών ισοτιμιών:

$$\begin{aligned} 2x(2) + x(5) + x(11) &\equiv 53 \,(\mathrm{mod}\, 1012), \\ 3x(5) + x(7) &\equiv 56 \,(\mathrm{mod}\, 1012), \\ 4x(2) + 2x(7) &\equiv 58 \,(\mathrm{mod}\, 1012), \\ 3x(2) &\equiv 73 \,(\mathrm{mod}\, 1012). \end{aligned}$$

Η λύση του είναι: $x(2) = 699$, $x(5) = 475$, $x(7) = 655$, $x(11) = 204$.

Από την άλλη πλευρά, έχουμε:

$$745 \cdot 3^{11} \equiv 5^3 \cdot 7 \,(\mathrm{mod}\, 1013).$$

Έτσι, παίρνουμε:

$$\log_3 745 = 3 \cdot 475 + 655 - 11 \mod 1012 = 45.$$

8.6 Ασκήσεις

1. Να χρησιμοποιηθεί ο αλγόριθμος του Shanks για τον υπολογισμό του διακριτού λογάριθμου του 23 ως προς βάση g μέσα στην ομάδα $\mathbb{Z}^*_{211}$, όπου g είναι η μικρότερη αρχική ρίζα κατά μέτρο 211.

2. Ο ακέραιος 347 είναι πρώτος και $173|346$. Να βρεθεί ο μικρότερος γεννήτορας g της μοναδικής κυκλικής υποομάδας G της $\mathbb{Z}^*_{347}$ τάξης 173. Να δειχθεί ότι ο ακέραιος 243 ανήκει στη G και να υπολογιστεί ο διακριτός λογάριθμος $\log_g 243$.

3 Να χρησιμοποιηθεί ο αλγόριθμος του Pollard για τον υπολογισμό του διακριτού λογάριθμου του 507 ως προς βάση 5 μέσα στην ομάδα $\mathbb{Z}^*_{647}$.

4. Να δειχθεί ότι ο 3 είναι η μικρότερη αρχική ρίζα κατά μέτρο 449 και να υπολογιστεί ο διακριτός λογάριθμος της κλάσης 13 ως προς βάση 3 μέσα στην ομάδα $\mathbb{Z}^*_{449}$ με την μέθοδο του λογισμού δεικτών.

5. Ας είναι p πρώτος, q ένας πρώτος με $q|p-1$, $\gamma \in \mathbb{Z}^*_p$ ένα στοιχείο που παράγει την μοναδική ομάδα G τάξης q και $\alpha \in G$. Για $\delta \in G$,

καλούμε *αναπαράσταση του δ ως προς τα γ και α*, ένα ζεύγος ακεραίων (r, s) με $0 \leq r, s < q$ με $\delta = \gamma^r \alpha^s$. Να δειχθούν τα εξής:
(α) Για κάθε $\delta \in G$, υπάρχουν ακριβώς q αναπαραστάσεις (r, s) του δ ως προς τα γ και α και μεταξύ αυτών υπάρχει μία ακριβώς με $s = 0$.
(β) Αν είναι γνωστή μία αναπαράσταση (r, s) του 1, με $s \neq 0$, ως προς τα γ και α, τότε ο διακριτός λογάριθμος $\log_\gamma \alpha$ υπολογίζεται σε πολυωνυμικό χρόνο.
(γ) Δοθέντος $\delta \in G$, μαζί με δύο διακεκριμμένες αναπαραστάσεις του δ ως προς τα γ και α, τότε ο διακριτός λογάριθμος $\log_\gamma \alpha$ υπολογίζεται σε πολυωνυμικό χρόνο.

6. Ας είναι $n = pq$, όπου p και q είναι δύο περιττοί πρώτοι με $p \neq q$. Θέτουμε $\lambda = \epsilon\kappa\pi(p-1, q-1)$. Υποθέτουμε ότι διαθέτουμε έναν αλγόριθμο ο οποίος δέχεται ως είσοδο ακεραίους a και b με $a^x \equiv b \pmod{n}$, όπου x θετικός ακέραιος, και υπολογίζει τον x.
(α) Να δειχθεί ότι το σύνολο

$$K = \{z \in \mathbb{Z}_n^* / \ z^{\lambda/2} \equiv \pm 1 \mod n\}$$

είναι γνήσια υποομάδα του $\mathbb{Z}_n^*$.
(β) Ας είναι $a \in \mathbb{Z}_n^* \setminus K$ και $x = \mathrm{ord}_n(a)$. Να δειχθεί ότι υπάρχει ακέραιος k με $1 \leq k < \log_2 x$ έτσι, ώστε να ισχύει $a^{x/2^k} \not\equiv \pm 1 \pmod{n}$ και $(a^{x/2^k})^2 \equiv 1 \pmod{n}$.
(γ) Να δειχθεί ότι ο ακέραιος $\mu\kappa\delta(a^{x/2^k} + 1, n)$ είναι $\neq 1, n$ και επομένως ένας μη τετριμμένος διαιρέτης του n.

7. Ας είναι p πρώτος, a μία πρωτογενής ρίζα κατά μέτρο p και x θετικός ακέραιος. Αν ο ακέραιος $y = a^x \mod p$ είναι γνωστός, τότε να δειχθεί ότι είναι δυνατόν να συμπεράνουμε σε πολυωνυμικό χρόνο, αν ο x είναι άρτιος ή περιττός.

8. Ας είναι n θετικός ακέραιος. Να δειχθούν τα εξής:
(α) Ο ακέραιος 2 είναι πρωτογενής ρίζα κατά μέτρο 3^n.
(β) Για κάθε $a \in \mathbb{Z}_{3^n}^*$, το πρόβλημα της εύρεσης του λογαρίθμου $\log_2 a$ μέσα στην ομάδα $\mathbb{Z}_{3^n}^*$ είναι ισοδύναμο με την επίλυση της

$$4^x c \equiv 1 \pmod{3^n},$$

όπου $c \in \mathbb{Z}_{3^n}^*$ και $c \equiv 1 \pmod{3}$.
(γ) Να βρεθεί ένας αλγόριθμος επίλυσης της παραπάνω ισοτιμίας και να υπολογιστεί ο χρόνος εκτέλεσής του.

Βιβλιογραφία

[1] L. Adleman, A subexponential algorithm for the discrete logarithm problem with applications to cryptography, In 20th Annual Symposium on Foundations of Computer Science, 1979, 55-60.

[2] D. M. Gordon, Discrete Logarithms in GF(p) using the Number Field Sieve, *SIAM Journal on Discrete Mathematics,* 6, 1 (1993), 312-323.

[3] C. Pomerance, Elementary Thoughts on Discrete Logarithms, Arithmetic Number Theory, MSRI Publications, Volume 44, 2008.

[4] D. Shanks, Class number, a theory of factorization, and genera, in Proceedings of Symposia in Pure Mathematics, Vol 20 (1969), 415-440.

[5] Schirokauer, D. Weber and T. Denny, Discrete logarithms: the effectiveness of the index calculus method. In H. Cohen, editor, *ANTS II,* LNCS 1122, Berlin, Springer-Verlag 1996.

[6] V. Shoup, *Μία Υπολογιστική Εισαγωγή στη Θεωρία Αριθμών και την Άλγεβρα,* Εκδόσεις Κλειδάριθμος 2007.