2 ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ – ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ

Η θεωρία αριθμών και οι αλγεβρικές δομές τα τελευταία χρόνια χρησιμοποιούνται όλο και περισσότερο στην κρυπτολογία. Αριθμο-θεωρητικοί αλγόριθμοι χρησιμοποιούνται σήμερα ευρέως εξαιτίας εν μέρει της ανακάλυψης των κρυπτογραφικών σχημάτων τα οποία στηρίζονται σε μεγάλους πρώτους αριθμούς. Από την άλλη μεριά αν ο ακέραιος n είναι πρώτος τότε οι ακέραιοι modulo n αποκτούν τη δομή ενός πεπερασμένου σώματος. Επίσης οι ελλειπτικές καμπύλες επί πεπερασμένων σωμάτων παρέχουν παραδείγματα ομάδων των οποίων η δομή είναι εξ ίσου απλή ή απλούστερη από τη δομή της πολλαπλασιαστικής ομάδας $(\boldsymbol{Z}_p^*, \cdot)$. Σ' αυτό το κεφάλαιο παρουσιάζουμε βασικά στοιχεία από τη θεωρία αριθμών και τις αλγεβρικές δομές και σε συνδυασμό με όσα εκτίθενται στο Παράρτημα πιστεύουμε ότι θα εφοδιάσουν τον αναγνώστη με τα απαραίτητα Μαθηματικά ώστε να είναι σε θέση να κατανοήσει καλύτερα το τι και πως διαδραματίζεται στα υπόλοιπα κεφάλαια του βιβλίου αυτού.

2.1. Βασικές έννοιες της θεωρίας αριθμών

Στη θεωρία αριθμών ασχολούμαστε με το σύνολο $\boldsymbol{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ των ακεραίων και το σύνολο $\boldsymbol{N} = \{0, 1, 2, \ldots\}$ των φυσικών αριθμών. Μια από τις κεντρικές έννοιες είναι αυτή της διαιρετότητας. Έστω δύο ακέραιοι a και d. Ο d ***διαιρεί*** τον a, συμβολικά $d \mid a$, σημαίνει ότι $a = kd$ για κάποιον ακέραιο k. Κάθε ακέραιος διαιρεί το 0. Αν $a > 0$ και $d \mid a$, τότε $|d| \le a$. Αν $d \mid a$, τότε λέμε και ότι ο a είναι ***πολλαπλάσιο*** του d. Αν τώρα ο d δεν διαιρεί τον a, γράφουμε $d \nmid a$.

Αν $d \mid a$ και $d \ge 0$, ο d λέγεται ***διαιρέτης*** του a. Αν $d \mid a$, τότε $a = kd$ ή ισοδύναμα $a = (-k)(-d)$, που σημαίνει ότι $d \mid a$ αν και μόνον αν $-d \mid a$, οπότε χωρίς βλάβη της γενικότητας μπορούμε να ορίσουμε τους διαιρέτες να είναι μη αρνητικοί, έχοντας κατά νου ότι ο αντίθετος (αρνητικός) οποιουδήποτε διαιρέτη του a διαιρεί επίσης τον a. Αν d είναι ένας διαιρέτης ενός ακέραιου $a \ne 0$ τότε ισχύει $1 \le d \le |a|$. Για παράδειγμα, οι διαιρέτες του 18 είναι 1, 2, 3, 6, 9 και 18.

Κάθε ακέραιος a έχει σαν ***τετριμμένους διαιρέτες*** τους 1 και a. Οι μη τετριμμένοι διαιρέτες του a λέγονται και ***παράγοντες*** του a. Για παράδειγμα, οι παράγοντες του 24 είναι 2, 3, 4, 6, 8 και 12. Ένας ακέραιος $a > 1$ του οποίου οι μόνοι δι-

αιρέτες είναι οι τετριμμένοι διαιρέτες 1 και a λέγεται ότι είναι ***πρώτος αριθμός*** ή απλά ***πρώτος***. Οι πρώτοι παίζουν σημαντικότατο ρόλο στη θεωρία αριθμών επειδή έχουν χαρακτηριστικές ιδιότητες. Κατά σειρά αύξοντος μεγέθους οι ακέραιοι

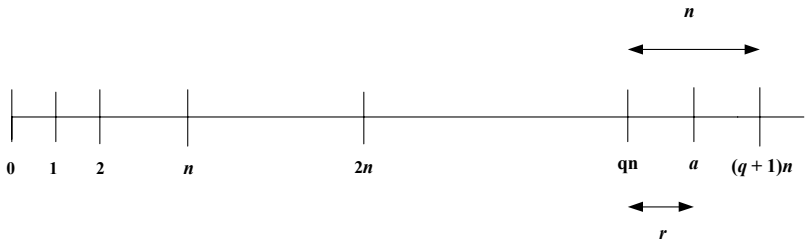
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, …, 389, …, 2003

είναι πρώτοι. Αποδεικνύεται ότι υπάρχουν άπειροι πρώτοι. Ένας ακέραιος $a > 1$ ο οποίος δεν είναι πρώτος λέγεται ότι είναι ***σύνθετος αριθμός*** ή απλά ***σύνθετος***. Για παράδειγμα, ο 15 είναι σύνθετος γιατί $3 \mid 15$. Κατά σειρά αύξοντος μεγέθους οι ακέραιοι

4, 6, 8, 9, 10, …, $666 = 2 \cdot 3^2 \cdot 37$, …, $2001 = 3 \cdot 23 \cdot 29$, …

είναι σύνθετοι. Ο ακέραιος 1 δεν είναι πρώτος ούτε σύνθετος. Ένας λόγος γι αυτό είναι ότι, όπως θα δούμε παρακάτω, το Θεώρημα 2.5 λέει ότι ένας σύνθετος γράφεται κατά μοναδικό τρόπο ως γινόμενο πρώτων οπότε αν ο 1 ήταν πρώτος η μοναδικότητα θα τινάζονταν στον αέρα. Επίσης να αναφέρουμε ότι ο 1 λέγεται ότι είναι μια ***μονάδα*** (unit), γιατί έχει αντίστροφο στο $\boldsymbol{Z}$. Παρόμοια, ο ακέραιος 0 και όλοι οι αρνητικοί ακέραιοι δεν είναι ούτε πρώτοι ούτε σύνθετοι.

Η έννοια της διαίρεσης είναι στενά συνδεδεμένη με την πρόσθεση και μάλιστα με το πρόβλημα της καλύτερης προσέγγισης ενός φυσικού αριθμού a από τον φυσικό αριθμό n, με $n < a$. Για τον λόγο αυτό θεωρούμε την ακολουθία a, $a - n$, $a - 2n$, …, $a - qn$, … . Η καλύτερη προσέγγιση επιτυγχάνεται όταν η διαφορά $a - qn$ είναι θετική και γίνει η μικρότερη δυνατή.



Η τιμή του q για την οποία συμβαίνει αυτό είναι το γνωστό μας πηλίκο της διαίρεσης a δια n και ο αριθμός $r = a - qn$ είναι το υπόλοιπο. Έτσι ο φυσικός a γράφεται στη μορφή $a = qn + r$ όπου το υπόλοιπο είναι αυστηρά μικρότερο του n αφού διαφορετικά η διαφορά $a - (q + 1)n$ θα ήταν η καλύτερη προσέγγιση. Τα παραπάνω μας οδηγούν, γενικεύοντας στους ακέραιους, στο γνωστό ***Θεώρημα της Διαίρεσης***.

ΘΕΩΡΗΜΑ 2.1 – Για κάθε ακέραιο a και οποιονδήποτε θετικό ακέραιο n, υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε $0 \le r < n$ και $a = qn + r$.

Η τιμή q, συμβολικά a div n, είναι το πηλίκο της διαίρεσης και είναι $q = \lfloor a/n \rfloor$, όπου $\lfloor x \rfloor$ είναι ο μεγαλύτερος ακέραιος που δεν υπερβαίνει τον αριθμό x. Η τιμή r είναι το ***υπόλοιπο*** της διαίρεσης και συμβολίζεται με a mod n:

$$a \bmod n = a - \lfloor a/n \rfloor n \tag{2.1}$$

Έτσι, για κάθε ακέραιο a και θετικό ακέραιο n μπορούμε πάντα να γράφουμε

$$a = \lfloor a/n \rfloor n + a \bmod n$$

όπου ο a mod n είναι ένας ακέραιος στο διάστημα, $0 \le a \bmod n < n$. Έχουμε ότι $n \mid a$ αν και μόνον αν a mod $n = 0$. Καλούμε το a mod n ως το μικρότερο μη αρνητικό ***κατάλοιπο*** του a, modulo n. Επίσης, λέμε ότι το a mod n είναι το αποτέλεσμα της ***αναγωγής*** του a, modulo n. Για παράδειγμα, αν $a = 73$, $n = 17$, τότε $q = 4$ και $r = 5$. Έτσι, 73 mod 17 = 5 και 73 div 17 = 4. Επίσης αν $a = 34$, $n = 17$, τότε 34 mod 17 = 0 αφού $34 = 2 \cdot 17$.

Γενικεύοντας την (2.1) μπορούμε να ορίσουμε μια συνάρτηση ‘‘mod’’ ως εξής:

$$a \bmod n = \begin{cases} a, & \text{αν } n = 0 \\ a - \lfloor a/n \rfloor n, & \text{διαφορετικα} \end{cases}$$

Να σημειώσουμε ότι ο ορισμός αυτός έχει νόημα για όλους τους ακέραιους a και n.

ΘΕΩΡΗΜΑ 2.2 (*Αρχή της modular αριθμητικής*) – Έστω a_1 και a_2 ακέραιοι και $*$ μια από τις πράξεις +, –, ή ·. Τότε η αναγωγή mod n είναι ένας ομομορφισμός* από τους ακέραιους στους ακέραιους mod n (βλ. Σχήμα 2.1), δηλαδή

$$(a_1 * a_2) \bmod n = [(a_1 \bmod n) * (a_2 \bmod n)] \bmod n.$$

Απόδειξη Μπορούμε να γράψουμε

$$a_1 = k_1 n + r_1, \quad 0 \le r_1 \le n - 1$$
$$a_2 = k_2 n + r_2, \quad 0 \le r_2 \le n - 1$$

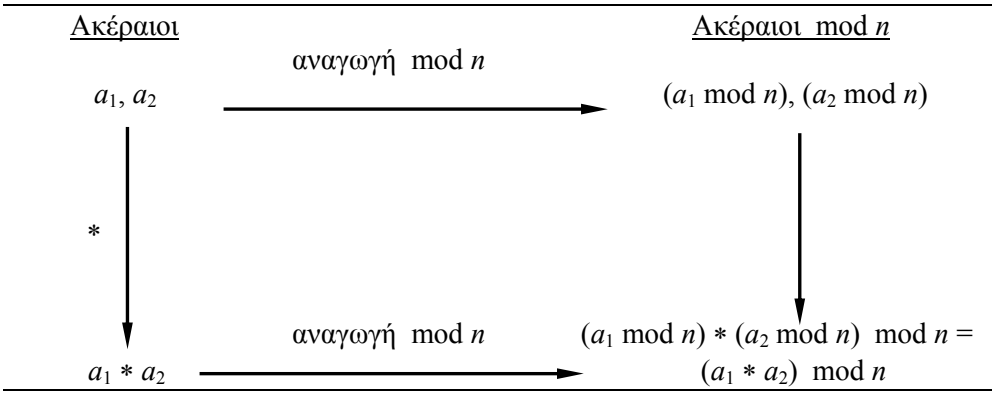
Έτσι, για την πρόσθεση έχουμε

$$\begin{aligned} (a_1 + a_2) \bmod n &= [(k_1 n + r_1) + (k_2 n + r_2)] \bmod n \\ &= [(k_1 + k_2)n + (r_1 + r_2)] \bmod n \\ &= [r_1 + r_2] \bmod n \\ &= [(a_1 \bmod n) + (a_2 \bmod n)] \bmod n. \end{aligned}$$

Για την αφαίρεση δουλεύουμε παρόμοια. Για τον πολλαπλασιασμό,

* Για ομομορφισμό βλ. § 2.5

$$
\begin{aligned}
(a_1 \cdot a_2) \bmod n &= [(k_1 n + r_1) \cdot (k_2 n + r_2)] \bmod n \\
&= [(k_1 k_2 n + r_1 k_2 + r_2 k_1) n + r_1 r_2] \bmod n \\
&= [r_1 \cdot r_2] \bmod n \\
&= [(a_1 \bmod n) \cdot (a_2 \bmod n)] \bmod n. \_
\end{aligned}
$$



Σχήμα 2.1 Αρχή της modular αριθμητικής

Δοθείσης τώρα μιας καλώς ορισμένης έννοιας του υπόλοιπου ενός ακέραιου όταν διαιρείται με έναν άλλο, είναι καλό να καθιερώσουμε έναν ειδικό συμβολισμό ο οποίος να δηλώνει ισότητα υπόλοιπων. Αν $a \bmod n = b \bmod n$, γράφουμε $a \equiv b \pmod n$[†] και λέμε ότι "ο a είναι ***ισότιμος*** ή ***ισοϋπόλοιπος*** ή ***ισοδύναμος*** με τον b, modulo n". Ο θετικός αριθμός n λέγεται ότι είναι το ***modulus***. Με άλλα λόγια,

$a \equiv b \pmod n$ αν οι a και b έχουν το ίδιο υπόλοιπο όταν διαιρούνται με τον n.

Ισοδύναμα,

$a \equiv b \pmod n$ αν και μόνον αν ο $n \mid (b - a)$.

Πράγματι, αν είναι $a \equiv b \pmod n$, τότε $a \bmod n = b \bmod n$, ή $a - \lfloor a/n \rfloor n = b - \lfloor b/n \rfloor n$, ή $b - a = \lfloor b/n \rfloor n - \lfloor a/n \rfloor n = (\lfloor b/n \rfloor - \lfloor a/n \rfloor)n$, που σημαίνει ότι $n \mid (b - a)$ αφού $(\lfloor b/n \rfloor - \lfloor a/n \rfloor)$ είναι ακέραιος. Αντίστροφα, αν $n \mid (b - a)$, τότε $b - a = kn$ για κάποιον ακέραιο k, ή $b = a + kn$ και επομένως,

$$
\begin{aligned}
b \bmod n &= a + kn \bmod n \\
&= a + kn - \left\lfloor \frac{a + kn}{n} \right\rfloor n
\end{aligned}
$$

[†] Προσοχή στη χρήση των παρενθέσεων!

$$= a + kn - \left\lfloor \frac{a}{n} + k \right\rfloor n$$

$$= a + kn - \left(\left\lfloor \frac{a}{n} \right\rfloor + k \right) n$$

$$= a + kn - \left\lfloor \frac{a}{n} \right\rfloor n - kn$$

$$= a - \left\lfloor \frac{a}{n} \right\rfloor n = a \bmod n. \_$$

Γράφουμε $a \quad b \pmod{n}$ αν ο a είναι δεν είναι ισοδύναμος με b, modulo n. Για τη σχέση "$\equiv \pmod{n}$" ισχύει το ακόλουθο θεώρημα του οποίου την απόδειξη αναφέρουμε στο Παράρτημα, § Α.3.

ΘΕΩΡΗΜΑ 2.3 – Έστω n θετικός ακέραιος. Τότε, αν a, b και c είναι ακέραιοι:

i) $a \equiv a \pmod{n}$

ii) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Με βάση το θεώρημα αυτό βλέπουμε ότι οι ακέραιοι μπορούν να διαμεριστούν σε n κλάσεις ισοδυναμίας σύμφωνα με τα υπόλοιπά τους modulo n (βλ. Παράρτημα, § Α.3). Η ***κλάση ισοδυναμίας modulo n*** ή η ***κλάση κατάλοιπου modulo n*** που περιέχει τον ακέραιο a είναι

$$[a]_n = \{a + kn : k \in \boldsymbol{Z}\} = \{x \in \boldsymbol{Z} : x \equiv a \pmod{n}\}$$

Για παράδειγμα, $[3]_4 = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$. Άλλες δηλώσεις γι' αυτό το σύνολο είναι $[-5]_4$ και $[11]_4$. Μπορούμε να πούμε ότι γράφοντας $b \in [a]_n$ είναι το ίδιο με το να γράψουμε ότι $b \equiv a \pmod{n}$. Το σύνολο όλων αυτών των κλάσεων ισοδυναμίας είναι

$$\boldsymbol{Z}_n = \{[a]_n : 0 \le a \le n - 1\} = \{[0], [1], \ldots, [n-1]\} \tag{2.2}$$

Συχνά γράφουμε

$$\boldsymbol{Z}_n = \{0, 1, \ldots, n - 1\} \tag{2.3}$$

που πρέπει να θεωρείται ως ισοδύναμος ορισμός με αυτόν της (2.2) με την έννοια ότι το 0 αναπαριστά την $[0]_n$, το 1 αναπαριστά την $[1]_n$, κοκ. Κάθε κλάση αναπαρίσταται με το μικρότερό της μη αρνητικό στοιχείο.[‡] Θα πρέπει όμως να μη ξεχνάμε τις κλάσεις ισοδυναμίας που είναι πίσω από το σύμβολο του ακέραιου. Για παράδειγμα, η αναφορά στον – 2 ως μέλος του $\boldsymbol{Z}_n$ είναι μια αναφορά στην $[n-2]_n$,

[‡] Από το Θεώρημα 2.1 προκύπτει ότι $a \equiv r \pmod{n}$, $0 \le r < n$, δηλ. ότι κάθε ακέραιος a είναι ισοδύναμος, modulo n, με έναν μοναδικό ακέραιο r, $0 \le r \le n - 1$.

αφού $-2 \equiv n-2 \pmod{n}$. Τέλος, για προφανείς πλέον λόγους, συχνά το $\boldsymbol{Z}_n$ λέγεται και ***σύνολο των ακεραίων modulo n***.

Αν τώρα ο d είναι διαιρέτης του a και ο d είναι επίσης διαιρέτης του b, τότε ο d είναι ένας κοινός διαιρέτης των a και b. Για παράδειγμα, οι διαιρέτες του 24 είναι 1, 2, 3, 4, 6, 8, 12 και 24, οπότε οι κοινοί διαιρέτες των 18 και 24 είναι οι 1, 2, 3, και 6. Ας παρατηρήσουμε ότι ο 1 είναι κοινός διαιρέτης δύο οποιωνδήποτε ακεραίων. Μια σημαντική ιδιότητα των κοινών διαιρετών είναι ότι

$$\text{αν } d \mid a \text{ και } d \mid b \text{ τότε } d \mid (ax + by), \ \forall x, y \in \boldsymbol{Z} \tag{2.4}$$

που εξειδικεύεται στην

$$\text{αν } d \mid a \text{ και } d \mid b \text{ τότε } d \mid (a + b) \text{ και } d \mid (a - b). \tag{2.5}$$

Επίσης, αν $a \mid b$, τότε είτε $|a| \le |b|$ ή $b = 0$ οπότε έχουμε ότι

$$\text{αν } a \mid b \text{ και } b \mid a \text{ τότε } a = \pm b. \tag{2.6}$$

Ο ***μέγιστος κοινός διαιρέτης***, συμβολικά $\gcd(a, b)$, δύο ακεραίων a και b, που δεν είναι και οι δύο μηδέν, είναι ο μεγαλύτερος από τους κοινούς διαιρέτες των a και b. Για παράδειγμα, $\gcd(18, 24) = 6$, $\gcd(7, 11) = 1$ και $\gcd(0, 6) = 6$. Προφανώς αν $a \mid b$ τότε $\gcd(a, b) = a$. Αν a και b είναι μη μηδενικοί ακέραιοι, τότε ο $\gcd(a, b)$ είναι ένας ακέραιος μεταξύ του 1 και του $\min(|\alpha|, |b|)$. Ορίζουμε τον $\gcd(0, 0)$ να είναι 0 προκειμένου να αποκτήσουν καθολική ισχύ τυπικές ιδιότητες της συνάρτησης gcd όπως η (2.10) παρακάτω. Μερικές απλές ιδιότητες της συνάρτησης gcd είναι οι ακόλουθες:

$$\gcd(a, b) = \gcd(b, \alpha) \tag{2.7}$$

$$\gcd(a, b) = \gcd(-\alpha, b) \tag{2.8}$$

$$\gcd(a, b) = \gcd(|\alpha|, |b|) \tag{2.9}$$

$$\gcd(a, 0) = |\alpha| \tag{2.10}$$

$$\gcd(a, ka) = |\alpha| \quad \forall k \in \boldsymbol{Z} \tag{2.11}$$

$$\gcd(a, n) = \gcd(a + kn, n) \quad \forall k, n \in \boldsymbol{Z} \tag{2.12}$$

Ας θεωρήσουμε τώρα δύο ακέραιους a και b, οι οποίοι δεν είναι και οι δύο μηδέν, και το σύνολο $\{xa + yb : x, y \in \boldsymbol{Z}\}$ των γραμμικών συνδυασμών τους. Αν συμβολίσουμε με d_0 το μικρότερο θετικό στοιχείο αυτού του συνόλου, τότε θα είναι $d_0 = x_0a + y_0b$ για κάποιους $x_0, y_0 \in \boldsymbol{Z}$ και κάθε διαιρέτης d των a και b θα είναι και διαιρέτης του d_0. Πράγματι, γράφοντας $a = kd$ και $b = md$ με $k, m \in \boldsymbol{Z}$, έχουμε

$$\begin{aligned} d_0 &= x_0a + y_0b \\ &= x_0kd + y_0md \end{aligned}$$

$= (x_0k + y_0m)d.$

Από την άλλη μεριά, αν χρησιμοποιήσουμε το Θεώρημα της Διαίρεσης για να γράψουμε $a = qd_0 + r$, με $0 \le r < d_0$, τότε

$$r = a - qd_0$$
$$= a - q(x_0a + y_0b)$$
$$= (1 - qx_0)a + (-y_0)b$$

δηλαδή ο r εκφράστηκε κι αυτός ως $x'a + y'b$ όπου $x', y' \in \boldsymbol{Z}$. Επειδή όμως $r < d_0$ και d_0 είναι ο μικρότερος θετικός ακέραιος που μπορεί να εκφραστεί έτσι, θα πρέπει $r = 0$ και συνεπώς $d_0 \mid a$. Παρόμοια, $d_0 \mid b$.

Δείξαμε λοιπόν το ακόλουθο θεώρημα, το οποίο πέρα απ' όλα τα άλλα, μας παρέχει έναν χρήσιμο τρόπο χαρακτηρισμού του gcd(a, b).

ΘΕΩΡΗΜΑ 2.4 – Αν a, b είναι δύο ακέραιοι, όχι και οι δύο μηδέν, τότε ο gcd(a, b) είναι το μικρότερο θετικό στοιχείο του συνόλου $\{xa + yb : x, y \in \boldsymbol{Z}\}$ των γραμμικών συνδυασμών των a και b.

Επειδή τώρα ο gcd(a, b) είναι ένας γραμμικός συνδυασμός των a και b, από την (2.4) εύκολα προκύπτει το εξής

ΠΟΡΙΣΜΑ 2.1 – Για οποιουσδήποτε ακέραιους a και b, αν $d \mid a$ και $d \mid b$ τότε $d \mid$ gcd(a, b).

Εύκολα επίσης προκύπτουν και τα ακόλουθα δύο πορίσματα.

ΠΟΡΙΣΜΑ 2.2 – Για όλους τους ακέραιους a και b και οποιονδήποτε μη αρνητικό ακέραιο n,

gcd(na, nb) = n gcd(a, b).

ΠΟΡΙΣΜΑ 2.3 – Για όλους τους θετικούς ακέραιους n, a και b, αν $n \mid ab$ και gcd(a, n) = 1, τότε $n \mid b$.

Αν δύο ακέραιοι a και b έχουν μοναδικό κοινό διαιρέτη τον 1, δηλαδή αν gcd(a, b) = 1, τότε λέγονται ***πρώτοι μεταξύ τους*** ή ***σχετικά πρώτοι***. Για παράδειγμα, οι διαιρέτες του 7 είναι οι 1 και 7, ενώ οι διαιρέτες του 27 είναι οι 1, 3, 9 και 27, οπότε ο 1 είναι ο μοναδικός κοινός τους διαιρέτης ή gcd(7, 27) = 1 και κατά συνέπεια οι ακέραιοι 7 και 27 είναι σχετικά πρώτοι. Τι γίνεται αν δύο ακέραιοι a και b είναι ο καθένας τους σχετικά πρώτος με έναν τρίτο ακέραιο p; Επειδή gcd(a, p) = 1 και gcd(b, p) = 1, από το Θεώρημα 2.4 προκύπτει ότι υπάρχουν ακέραιοι x_1, y_1, x_2 και y_2 τέτοιοι ώστε

$$ax_1 + py_1 = 1$$
$$bx_2 + py_2 = 1$$

Πολλαπλασιάζοντας κατά μέλη τις σχέσεις αυτές προκύπτει εύκολα η σχέση

$ab(x_1x_2) + p(y_1bx_2 + y_2ax_2 + py_1y_2) = 1$

από την οποία με βάση πάλι το Θεώρημα 2.4 έχουμε ότι gcd(ab, p) = 1. Δηλαδή αποδείξαμε στην ουσία το

ΘΕΩΡΗΜΑ 2.5 – Αν για τους ακέραιους a, b και p είναι gcd(a, p) = 1 και gcd(b, p) = 1, τότε gcd(ab, p) = 1.

Αν τώρα έχουμε τους ακέραιους k_1, k_2, …, k_n λέμε ότι είναι ***ανά δύο σχετικά πρώτοι***, αν $i \neq j \Rightarrow$ gcd(k_i, k_j) = 1.

Τελειώνοντας αυτήν τη μάλλον σύντομη εισαγωγή στη θεωρία αριθμών, θα πρέπει να αναφέρουμε δύο σημαντικά θεωρήματα που έχουν να κάνουν με τη διαιρετότητα με πρώτους.

ΘΕΩΡΗΜΑ 2.6 – Για όλους τους πρώτους p και τους ακέραιους a, b, αν $p \mid ab$, τότε $p \mid a$ ή $p \mid b$.

Απόδειξη Για την απόδειξη χρησιμοποιούμε εις άτοπο απαγωγή. Έστω ότι $p \mid ab$ αλλά $p \nmid a$ και $p \nmid b$. Τότε επειδή ο p είναι πρώτος, gcd(a, p) = 1 και gcd(b, p) = 1. Από το Θεώρημα 2.5 προκύπτει τότε ότι gcd(ab, p) = 1, όπερ άτοπο γιατί η υπόθεση ότι $p \mid ab$ συνεπάγεται την gcd(ab, p) = p._

Χρησιμοποιώντας το παραπάνω θεώρημα μπορεί κανείς να αποδείξει ότι ένας ακέραιος παραγοντοποιείται κατά μοναδικό τρόπο σε πρώτους:

ΘΕΩΡΗΜΑ 2.7 – Ένας σύνθετος a μπορεί να γραφεί κατά μοναδικό τρόπο ως ένα γινόμενο της μορφής

$$a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} = \prod_{i=1}^{s} p_i^{e_i}$$

όπου οι p_1, p_2, …, p_s είναι πρώτοι, $p_1 < p_2 < \ldots < p_s$ και οι e_1, e_2, …, e_s είναι θετικοί ακέραιοι. Αν S_p είναι το σύνολο όλων των πρώτων, τότε μπορούμε να γράψουμε το παραπάνω γινόμενο στην ακόλουθη μορφή

$$a = \prod_{p \in S_p} p^{a_p}\ ,\ \text{όπου κάθε } a_p \geq 0$$

Το γινόμενο στο δεξί μέλος της ισότητας αναφέρεται σε όλους τους δυνατούς πρώτους p και για μια συγκεκριμένη τιμή του a οι περισσότεροι από τους εκθέτες e_p θα είναι 0. Η τιμή για έναν δοσμένο θετικό ακέραιο μπορεί να καθοριστεί δίνοντας απλά όλους τους μη μηδενικούς εκθέτες που εμφανίζονται στο γινόμενο. Για παράδειγμα, ο ακέραιος a = 18 αναπαρίσταται με $\{a_2 = 1, a_3 = 2\}$ και ο b = 3600 με $\{b_2 = 4, b_3 = 2, b_5 = 2\}$. Ο πολλαπλασιασμός δύο ακεραίων είναι ισοδύναμος με την πρόσθεση των αντίστοιχων εκθετών:

$c = ab \;\rightarrow\; c_p = a_p + b_p \quad \forall\, p \in S_p$

Στο παράδειγμά μας με $a = 18$ και $b = 3600$, έχουμε

$c = 18 \cdot 3600 = 64800$
$c_2 = 1 + 4 = 5,\; c_3 = 2 + 2 = 4,\; c_5 = 0 + 2 = 2$
$64800 = 2^5 \cdot 3^4 \cdot 5^2.$

Επειδή τώρα ένας ακέραιος της μορφής p^k μπορεί να διαιρεθεί μόνον από ακέραιο ο οποίος είναι της μορφής p^m με $m \le k$ (μικρότερη ή ίση δύναμη του ιδίου πρώτου), μπορούμε να πούμε ότι

$a \mid b \;\rightarrow\; a_p \le b_p$ για όλους τους πρώτους p

Για παράδειγμα, $12 \mid 36$ και είναι

$a = 12 = 2^2 \cdot 3,\; b = 36 = 2^2 \cdot 3^2$
$a_2 = 2 = b_2,\; a_3 = 1 \le 2 = b_3.$

Είναι ‘‘εύκολο’’ να υπολογίσουμε τον μέγιστο κοινό διαιρέτη δύο θετικών ακεραίων αν εκφράσουμε τον καθένα ως γινόμενο πρώτων. Για παράδειγμα, αν $a = 18$ και $b = 3600$, έχουμε

$18 = 2^1 \cdot 3^2 = 2^1 \cdot 3^2 \cdot 5^0,\; 3600 = 2^4 \cdot 3^2 \cdot 5^2$
$\gcd(18, 3600) = 2^1 \cdot 3^2 \cdot 5^0 = 18.$

2.2. Αλγόριθμος του Ευκλείδη

Προκειμένου να περιγράψουμε τον αλγόριθμο του Ευκλείδη ας πούμε μερικά πράγματα ακόμα. Μπορούμε σ’ αυτήν την ενότητα, χωρίς βλάβη της γενικότητας, να περιοριστούμε στους μη αρνητικούς ακέραιους, και τούτο γιατί, $\gcd(a, b) = \gcd(|a|, |b|)$ (βλ. (2.9)).

Κατ’ αρχήν, μπορούμε όπως είπαμε στο τέλος της προηγούμενης ενότητας, να υπολογίσουμε τον $\gcd(a, b)$ για θετικούς ακέραιους a και b από την παραγοντοποίησή τους σε πρώτους. Πράγματι, αν

$$a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \tag{2.13}$$
$$b = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s} \tag{2.14}$$

όπου χρησιμοποιήσαμε μηδενικούς εκθέτες προκειμένου να είναι το σύνολο των πρώτων $p_1, p_2, \ldots, p_s$ το ίδιο για τους a και b, τότε μπορεί κανείς να δείξει ότι

$d = \gcd(a, b) \;\rightarrow\; d_p = \min(a_p, b_p)$ για όλους τους p

δηλαδή

$$\gcd(a,b) = p_1^{\min(e_1,h_1)} p_2^{\min(e_2,h_2)} \cdots p_s^{\min(e_s,h_s)} \tag{2.15}$$

Επειδή όμως οι αλγόριθμοι που έχουμε μέχρι τώρα για την παραγοντοποίηση δεν τρέχουν σε πολυωνυμικό χρόνο, αυτή η προσέγγιση για τον υπολογισμό μέγιστων κοινών διαιρετών δεν φαίνεται να αποδίδει έναν αποτελεσματικό αλγόριθμο.

Για τον υπολογισμό μέγιστων κοινών διαιρετών έχουμε και τον αλγόριθμο του Ευκλείδη ο οποίος εκφράζεται ως ένα επαναληπτικό είτε ως ένα αναδρομικό πρόγραμμα το οποίο βασίζεται στο ακόλουθο θεώρημα.

ΘΕΩΡΗΜΑ 2.8 – Για οποιονδήποτε μη αρνητικό ακέραιο a και οποιονδήποτε θετικό ακέραιο b,

$$\gcd(a, b) = \gcd(b, a \bmod b). \tag{2.16}$$

Απόδειξη Χάριν συντομίας, ας είναι $d_1 = \gcd(a, b)$ και $d_2 = \gcd(b, a \bmod b)$. Θα δείξουμε ότι $d_1 \mid d_2$ και $d_2 \mid d_1$ οπότε επειδή d_1, d_2 είναι μη αρνητικοί, από την (2.6) προκύπτει ότι πρέπει να είναι $d_1 = d_2$. Επειδή $d_1 \mid a$, $d_1 \mid b$ και $a \bmod b = a - \lfloor a/b \rfloor b$, από την (2.4) έχουμε ότι $d_1 \mid (a \bmod b)$. Επειδή τώρα $d_1 \mid b$ και $d_1 \mid (a \bmod b)$, από το Πόρισμα 2.1 προκύπτει ότι $d_1 \mid d_2$. Παρόμοια δείχνουμε ότι $d_2 \mid d_1$. Επειδή $d_2 \mid b$, $d_2 \mid (a \bmod b)$ και $a = \lfloor a/b \rfloor b + (a \bmod b)$, από την (2.4) έχουμε ότι $d_2 \mid a$. Επειδή τώρα $d_2 \mid b$ και $d_2 \mid a$, από το Πόρισμα 2.1 προκύπτει ότι $d_2 \mid d_1$.▁

Για παράδειγμα, για τον υπολογισμό του gcd(24, 32), έχουμε

$$\begin{aligned}\gcd(32, 24) &= \gcd(24, 32 \bmod 24)\\ &= \gcd(24, 8)\\ &= \gcd(8, 24 \bmod 8)\\ &= \gcd(8, 0)\\ &= 8.\end{aligned}$$

Από την (2.16) έχουμε τον ακόλουθο αλγόριθμο στον οποίο τα εισαγόμενα a και b είναι μη αρνητικοί ακέραιοι.

Ευκλείδης(a, b)

```
1  if b = 0
2  then return a
3     else while b ≠ 0 do
4        {r ← a mod b
5         a ← b
6         b ← r}
7     return a
```

Υπάρχει και η αναδρομική έκδοση του αλγόριθμου του Ευκλείδη. Ο αλγόριθμος ορίζει μια συνάρτηση η οποία καλεί τον εαυτό της με απλούστερα ορίσματα:

Ευκλείδης1(a, b)

```
1  if b = 0
2     then return a
3     else return Ευκλείδης1(b, a mod b)
```

Για παράδειγμα, τρέχοντας τον παραπάνω αλγόριθμο για τον υπολογισμό του gcd(57, 21) προκύπτει:

$$\begin{aligned}\text{Ευκλείδης1}(57, 21) &= \text{Ευκλείδης1}(21, 15)\\ &= \text{Ευκλείδης1}(15, 6)\\ &= \text{Ευκλείδης1}(6, 3)\\ &= \text{Ευκλείδης1}(3, 0)\\ &= 3.\end{aligned}$$

Για πρακτικούς λόγους είναι χρήσιμη μια μορφή του παραπάνω αλγόριθμου γνωστή ως ***ανεπτυγμένη μορφή*** του αλγόριθμου του Ευκλείδη. Είναι δηλαδή σκόπιμο να ξαναγράψουμε τον αλγόριθμο του Ευκλείδη προκειμένου να υπολογίζει τους ακέραιους συντελεστές x και y στον γραμμικό συνδυασμό

$$d = \gcd(a, b) = xa + yb \tag{2.17}$$

που αναφέρεται στο Θεώρημα 2.4. Ο λόγος που λέμε ότι είναι σκόπιμο οφείλεται στο γεγονός ότι οι παραπάνω συντελεστές θα είναι χρήσιμοι αργότερα στον υπολογισμό των modular πολλαπλασιαστικών αντίστροφων. Ο αλγόριθμος αυτός έχει ως είσοδο ένα ζεύγος μη αρνητικών ακεραίων a και b και ως έξοδο μια τριάδα της μορφής (d, x, y) η οποία ικανοποιεί την (2.17). Ένα απλό βήμα του αρχικού αλγόριθμου του Ευκλείδη μετέτρεψε το πρόβλημα εύρεσης του $\gcd(a, b)$ σ' αυτό της εύρεσης του $\gcd(b, a \bmod b)$. Υποθέτουμε, επαγωγικά, ότι όχι μόνον ξέρουμε τον $\gcd(b, a \bmod b)$ αλλά ότι ξέρουμε επίσης τους συντελεστές x', y' για την εξίσωση

$$d = x'b + y'(a \bmod b) \tag{2.18}$$

Μπορούμε να βγάλουμε, στο επόμενο βήμα, τους αντίστοιχους συντελεστές x, y για την (2.17); Μπορούμε όντως, γιατί αντικαθιστώντας στην (2.18)

$$a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b$$

βρίσκουμε ότι

$$d = x'b + y'\left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right) a \bmod b = y'a + \left(x' - y'\left\lfloor \frac{a}{b} \right\rfloor\right) b\,.$$

Επομένως ο κανόνας με τον οποίο οι x', y' για την (2.18) μετασχηματίζονται στους x, y για την (2.17) είναι ο ακόλουθος

$$x = y'$$

$$y = x' - \left\lfloor \frac{a}{b} \right\rfloor y' .$$

Μπορούμε τώρα να διατυπώσουμε την ανεπτυγμένη μορφή του αλγόριθμου του Ευκλείδη (στην αναδρομική της έκδοση):

Ευκλείδης2(a, b)

```
1  if b = 0
2    then return (a, 1, 0)
3  (d′, x′, y′) ← Ευκλείδης2(b, a mod b)
4  (d, x, y) ← (d′, y′, x′ − ⌊a/b⌋ y′)
5  return (d, x, y)
```

Για παράδειγμα, ας περιγράψουμε την εκτέλεση της συνάρτησης Ευκλείδης2(a, b) αν κληθεί με (a, b) = (14, 11). Στην πρώτη κλήση της συνάρτησης Ευκλείδης2(14, 11) η συνάρτηση καλεί τον εαυτό της με ορίσματα (11, 3). Μετά καλεί τον εαυτό της διαδοχικά με (3, 2), (2, 1) και (1, 0). Όταν εκτελεί με (a, b) = (1, 0) αντιμετωπίζει την εντολή ‘‘if b = 0’’, οπότε θέτει $d \leftarrow 1$, $x \leftarrow 1$, $y \leftarrow 0$. Τώρα μπορεί να ολοκληρώσει την εκτέλεση της κλήσης με (a, b) = (2, 1), η οποία ήταν σε αναμονή. Για να γίνει αυτό, θέτει

$$y \leftarrow x - \left\lfloor \frac{a}{b} \right\rfloor y = 1, \quad x \leftarrow 0.$$

Η κλήση με (a, b) = (2, 1) έχει τώρα ολοκληρωθεί. Η κλήση της συνάρτησης με (a, b) = (3, 2) μπορεί στη συνέχεια να εκτελεστεί με αποτέλεσμα

$$y \leftarrow 0 - \left\lfloor \frac{3}{2} \right\rfloor 1 = -1, \quad x \leftarrow 1.$$

Τώρα έχει σειρά η κλήση της συνάρτησης με (a, b) = (11, 3) η οποία έχει ως αποτέλεσμα

$$y \leftarrow 1 - \left\lfloor \frac{11}{3} \right\rfloor (-1) = 4, \quad x \leftarrow -1.$$

Τελικά, η αρχική κλήση της συνάρτησης από τον χρήστη με (a, b) = (14, 11), μπορεί να ολοκληρωθεί, με αποτέλεσμα

$$y \leftarrow -1 - \left\lfloor \frac{14}{11} \right\rfloor 4 = -5, \quad x \leftarrow 4.$$

Επομένως, η Ευκλείδης2(14, 11) μας επιστρέφει τις τιμές (d, x, y) = (1, 4, –5), που σημαίνει ότι gcd(14, 11) = 1 = 4 · 14 + (–5) · 11.

2.3. Modular αριθμητική - Ομάδες

Όπως είδαμε στην § 2.1, μπορούμε να θεωρήσουμε την modular αριθμητική ως τη συνήθη αριθμητική στο σύνολο των ακεραίων, εκτός του ότι δουλεύουμε modulo n, οπότε κάθε αποτέλεσμα a αντικαθίσταται από το στοιχείο του συνόλου $\{0, 1, \ldots, n-1\}$ το οποίο είναι ισοϋπόλοιπο με το a, modulo n (δηλ. το a αντικαθίσταται με $a \bmod n$). Αυτό το μοντέλο για modular αριθμητική επαρκεί όσο έχουμε να κάνουμε με τις πράξεις της πρόσθεσης, αφαίρεσης και πολλαπλασιασμού. Όπως όμως θα διαπιστώσουμε στην πορεία, είναι σκόπιμο να περιγράψουμε ένα πιο τυπικό μοντέλο για modular αριθμητική και αυτό περιγράφεται καλύτερα στα πλαίσια της θεωρίας ομάδων.

Οι διάφορες δομές ανάλογα με τον αριθμό των εσωτερικών πράξεων και τις ιδιότητες που έχουν οι πράξεις αυτές, χωρίζονται σε διάφορες κατηγορίες. Στην κατηγορία των δομών με μία πράξη υπάγονται οι λεγόμενες ομάδες.

ΟΡΙΣΜΟΣ 2.1 – Ένα σύνολο G εφοδιασμένο με την πράξη[§] $\oplus$ λέγεται ***ομάδα*** (*group*), όταν η πράξη $\oplus$ είναι προσεταιριστική, υπάρχει το ουδέτερο στοιχείο $e \in G$ ως προς την πράξη $\oplus$ και κάθε στοιχείο του G έχει συμμετρικό στοιχείο.

Ώστε, η δομή $(G, \oplus)$, είναι ομάδα, όταν:

A.1. $\forall a, b, c \in G, \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$

A.2. $\exists\, e \in G, \forall a \in G, \quad a \oplus e = e \oplus a = a$

A.3. $\forall a \in G, \exists\, a' \in G, \quad a \oplus a' = a' \oplus a = e$

Αν επιπλέον η πράξη $\oplus$ είναι αντιμεταθετική, τότε η δομή $(G, \oplus)$ λέγεται ***αντιμεταθετική ή αβελιανή ομάδα***, δηλαδή όταν επιπλέον:

A.4. $\forall a, b \in G, \quad a \oplus b = b \oplus a$

Αν η πράξη σημειώνεται με + ή $\cdot$ τότε πρόκειται περί μιας προσθετικής ή πολλαπλασιαστικής ομάδας, αντίστοιχα. Για παράδειγμα, η δομή $(\boldsymbol{Z}, +)$ είναι μια αβελιανή προσθετική ομάδα στην οποία το ουδέτερο στοιχείο είναι το 0 και κάθε στοιχείο a του $\boldsymbol{Z}$ έχει αντίθετο στοιχείο το $-a$. Αντίθετα η δομή $(\boldsymbol{Z}, \cdot)$ δεν είναι πολλαπλασιαστική ομάδα, γιατί δεν υπάρχει στο $\boldsymbol{Z}$ ο αντίστροφος κάθε $\alpha \in \boldsymbol{Z}$ (αντίστροφο έχει μόνο ο 1).

Σε μια ομάδα $(G, \oplus)$ αποδεικνύεται ότι ισχύουν οι παρακάτω ιδιότητες:

- Το ουδέτερο στοιχείο $e \in G$ είναι μοναδικό.
- Κάθε στοιχείο του συνόλου G έχει ένα μόνο συμμετρικό στοιχείο ως προς την πράξη $\oplus$.

[§] βλ. και Παράρτημα § Α.4.

- Κάθε στοιχείο $\alpha \in G$ είναι απλοποιήσιμο, που σημαίνει ότι

  $\forall a, b, c \in G\ ,\ a \oplus b = a \oplus c \ \Rightarrow\ b = c$ και $b \oplus a = c \oplus a \ \Rightarrow\ b = c$

- Αν $a, b \in G$, τότε η εξίσωση

  $\alpha \oplus \mathrm{x} = \beta$

  έχει μοναδική λύση στο G, την

  $x = a' \oplus b$

- Αν $a, b \in G$, τότε η εξίσωση

  $x \oplus a = b$

  έχει μοναδική λύση στο G, την

  $x = b \oplus a'$

Αν βέβαια είμαστε σε αντιμεταθετική ομάδα οι παραπάνω δύο εξισώσεις είναι ισοδύναμες και έχουν μοναδική λύση την $x = a' \oplus b = b \oplus a'$. Ειδικότερα σε μια προσθετική αντιμεταθετική ομάδα η μοναδική λύση των εξισώσεων αυτών γράφεται $x = b + (–a) = b – a$, ενώ σε μια πολλαπλασιαστική αντιμεταθετική ομάδα γράφεται $\mathrm{x} = b \cdot a^{-1}$.

ΟΡΙΣΜΟΣ 2.2 – Μια ομάδα $(G, \oplus)$ είναι ***πεπερασμένη*** αν το σύνολο G έχει πεπερασμένο πλήθος στοιχείων, δηλ. αν είναι πεπερασμένος ο πληθάριθμος $|G|$. Σ' αυτήν την περίπτωση ο $|G|$ λέγεται ***τάξη*** (*order*) της ομάδας. Αν το G δεν είναι πεπερασμένο τότε λέμε ότι αυτό είναι απείρου τάξεως.

Μπορούμε να σχηματίσουμε δύο πεπερασμένες αντιμεταθετικές ομάδες χρησιμοποιώντας τις πράξεις της πρόσθεσης και του πολλαπλασιασμού modulo n, όπου n είναι ένας θετικός ακέραιος. Αυτές οι ομάδες βασίζονται στις κλάσεις ισοδυναμίας των ακεραίων modulo n, οι οποίες ορίσθηκαν στην § 2.1. Το σύνολο G στην περίπτωσή μας είναι αρχικά το $\boldsymbol{Z_n}$ και είναι εύκολο να δούμε ότι η κλάση ισοδυναμίας δύο ακεραίων προσδιορίζει μονοσήμαντα την κλάση ισοδυναμίας του αθροίσματος ή του γινομένου τους. Με άλλα λόγια,

αν $a \equiv a' \pmod n$ και $b \equiv b' \pmod n$, τότε
$a + b \equiv a' + b' \pmod n$
$a \cdot b \equiv a' \cdot b' \pmod n$

Έτσι, ορίζουμε πρόσθεση και πολλαπλασιασμό modulo n, συμβολικά $+_n$ και $\cdot_n$ ως ακολούθως:

$$[a]_n +_n [b]_n = [a + b]_n \qquad (2.19)$$
$$[a]_n \cdot_n [b]_n = [a \cdot b]_n$$

Στην ουσία τα παραπάνω δικαιολογούν την κοινή και βολική πρακτική κατά την οποία χρησιμοποιεί κανείς το μικρότερο μη αρνητικό στοιχείο κάθε κλάσης ισοδυναμίας ως αντιπρόσωπό της κατά την εκτέλεση υπολογισμών στο $\boldsymbol{Z_n}$. Η πρόσθεση και ο πολλαπλασιασμός εκτελούνται, κατά τον συνήθη τρόπο, επί των αντιπροσώπων αλλά το κάθε αποτέλεσμα x αντικαθίσταται με τον αντιπρόσωπο της κλάσης του, δηλ. με $x \bmod n$ (αναγωγή του x modulo n).

Χρησιμοποιώντας τον παραπάνω ορισμό της πρόσθεσης modulo n, ορίζουμε τη δομή $(\boldsymbol{Z_n}, +_n)$ που την ονομάζουμε ***προσθετική ομάδα modulo n*** και για την οποία αποδεικνύεται ότι είναι μια αβελιανή ομάδα.

ΘΕΩΡΗΜΑ 2.9 – Η δομή $(\boldsymbol{Z_n}, +_n)$ είναι μια πεπερασμένη αντιμεταθετική ομάδα τάξεως n.

Απόδειξη Επειδή η πράξη + είναι προσεταιριστική και αντιμεταθετική, έχουμε

$$\begin{aligned}([a]_n +_n [b]_n) +_n [c]_n &= [a + b]_n +_n [c]_n \\ &= [(a + b) + c]_n \\ &= [a + (b + c)]_n \\ &= [a]_n +_n [b + c]_n \\ &= [a]_n +_n ([b]_n +_n [c]_n)\end{aligned}$$

και

$$\begin{aligned}[a]_n +_n [b]_n &= [a + b]_n \\ &= [b + a]_n \\ &= [b]_n +_n [a]_n \,.\end{aligned}$$

Το ουδέτερο (μηδενικό) στοιχείο υπάρχει και είναι το $[0]_n$, γιατί

$[a]_n +_n [0]_n = [a + 0]_n = [a]_n$, για κάθε $[a]_n \in \boldsymbol{Z_n}$

και κάθε στοιχείο $[a]_n$ έχει αντίθετο το $[-a]_n$, γιατί

$[a]_n +_n [-a]_n = [a + (-a)]_n = [a - a]_n = [0]_n$, για κάθε $[a]_n \in \boldsymbol{Z_n}$.

Προφανώς, επειδή $|\boldsymbol{Z_n}| = n$, η τάξη της ομάδας αυτής είναι n._

Στη συνέχεια θεωρούμε το σύνολο

$$\boldsymbol{Z}_n^* = \{[a]_n \in \boldsymbol{Z_n} : \gcd(a, n) = 1\}$$

των κλάσεων ισοδυναμίας των ακεραίων που είναι σχετικά πρώτοι με τον n. Για $0 \le a < n$ και για κάθε ακέραιο k, έχουμε $a \equiv a + kn \pmod n$, οπότε από την (2.12) προκύπτει ότι η $\gcd(a, n) = 1$ συνεπάγεται την $\gcd(a + kn, n) = 1$. Έτσι, επειδή $[a]_n = \{a + kn : k \in \boldsymbol{Z}\}$, καταλήγουμε στο ότι το σύνολο $\boldsymbol{Z}_n^*$ είναι καλώς ορισμένο. Για παράδειγμα, $\boldsymbol{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ όπου, χάριν απλότητας, το στοιχείο $[a]_{21}$ το συμβολίσαμε ως a. Π.χ. συμβολίσαμε το $[10]_{21}$ ως 10. Όταν δεν υπάρχει κίνδυνος σύγχυσης θα χρησιμοποιούμε παρόμοιο συμβολισμό (βλ.

σχετικά και (2.2), (2.3)). Ειδικά, αν p είναι πρώτος τότε, $\boldsymbol{Z}_p^* = \{[a]_p \in \boldsymbol{Z_p} : 1 \le a \le p-1\} = \{1, 2, \ldots, p-1\}$.

Η τάξη του $\boldsymbol{Z}_n^*$, συμβολικά $\phi(n)$, είναι συνάρτηση του n η οποία είναι γνωστή ως η ***συνάρτηση ϕ του Euler***. Ειδικά, αν p είναι πρώτος τότε $\phi(p) = p - 1$. Αν n είναι σύνθετος, τότε $\phi(n) < n$ και αποδεικνύεται ότι αν $\prod_{i=1}^{k} p_i^{e_i}$ είναι η παραγοντοποίησή του σε πρώτους, τότε η τιμή $\phi(n)$ της συνάρτησης του Euler μπορεί να υπολογιστεί από τον τύπο

$$\phi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \tag{2.20}$$

Για παράδειγμα, επειδή $21 = 3 \cdot 7$, που είναι πρώτοι, είναι οι 3 και 7,

$$\begin{aligned}\phi(21) &= 21\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)\\ &= 21\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\\ &= 12\end{aligned}$$

Δύο άλλοι χρήσιμοι τύποι για τη συνάρτηση του Euler, των οποίων την απόδειξη παραλείπουμε, είναι οι ακόλουθοι:

- Αν p είναι πρώτος και $k \ge 1$, τότε $\phi(p^k) = p^k - p^{k-1}$.
- Αν $\gcd(a, b) = 1$, τότε $\phi(ab) = \phi(a)\phi(b)$.

Η χρήση τους απλοποιεί τη διαδικασία υπολογισμού της τιμής $\phi(n)$. Για παράδειγμα,

$$\begin{aligned}\phi(1512) = \phi(2^3 \cdot 3^3 \cdot 7) &= \phi(2^3)\phi(3^3)\,\phi(7) = (2^3 - 2^2)(3^3 - 3^2)(7 - 1) = 4 \cdot 18 \cdot 6\\ &= 432.\end{aligned}$$

Δηλαδή υπάρχουν 432 ακέραιοι μεταξύ των 1 και 1512 οι οποίοι είναι σχετικά πρώτοι με τον 1512.

ΠΑΡΑΔΕΙΓΜΑ 2.1 – Σύνολα ακεραίων οι οποίοι είναι σχετικά πρώτοι με τον n

n	$\{a \in \boldsymbol{Z} : 1 \le a \le n-1$ και $\gcd(a, n) = 1\}$
1	{1}
2	{1}
3	{1, 2}
4	{1, 3}
5	{1, 2, 3, 4}

6	{1, 5}
7	{1, 2, 3, 4, 5, 6}
8	{1, 3, 5, 7}
9	{1, 2, 4, 5, 7, 9}
10	{1, 3, 7, 9}

Από τον παραπάνω πίνακα προκύπτουν οι εξής τιμές της συνάρτησης $\phi(a)$ για $1 \leq a \leq 10$. Έτσι

a	1	2	3	4	5	6	7	8	9	10
$\phi(a)$	1	1	2	2	4	2	6	4	6	4

Από το Θεώρημα 2.5 προκύπτει ότι η πράξη $\cdot_n$ είναι εσωτερική στο $\boldsymbol{Z}_n^*$, οπότε μπορούμε να ορίσουμε τη δομή $(\boldsymbol{Z}_n^*, \cdot_n)$, ονομάζοντάς την ***πολλαπλασιαστική ομάδα modulo n***, και να αποδείξουμε ότι είναι μια πεπερασμένη αβελιανή ομάδα.

ΘΕΩΡΗΜΑ 2.10 – Η δομή $(\boldsymbol{Z}_n^*, \cdot_n)$ είναι μια πεπερασμένη αντιμεταθετική ομάδα τάξεως $\phi(n)$.

Απόδειξη Η απόδειξη της προσεταιριστικότητας και της αντιμεταθετικότητας της $\cdot_n$ (πολλαπλασιασμός modulo n) μπορεί να γίνει παρόμοια με την απόδειξη για την $+_n$ στο Θεώρημα 2.9. Το ουδέτερο στοιχείο είναι προφανώς $[1]_n$ και μένει να δείξουμε την ύπαρξη του αντίστροφου. Ας θεωρήσουμε ότι $a \in \boldsymbol{Z}_n^*$ και έστω ότι η τριάδα (d, x, y) είναι το εξαγόμενο της διαδικασίας Ευκλείδης2(a, n). Επειδή $a \in \boldsymbol{Z}_n^*$, είναι $d = 1$ και $ax + ny = 1$, ή ισοδύναμα, $ax \equiv 1 \pmod{n}$. Έτσι, $[x]_n$ είναι ένα πολλαπλασιαστικό αντίστροφο του $[a]_n$, modulo n._

Ας δούμε δύο παραδείγματα υπολογισμού πολλαπλασιαστικών αντίστροφων. Έστω $a = 8$ και $n = 21$. Τότε ο αλγόριθμος Ευκλείδης2(a, n) επιστρέφει $(d, x, y) = (1, 8, -3)$ έτσι ώστε $1 = 8 \cdot 8 + 21 \cdot (-3)$. Έτσι, ο 8 (δηλ. $[8]_{21}$) είναι πολλαπλασιαστικός αντίστροφος του 8 modulo 21. Πράγματι, $8 \cdot 8 = 64 \equiv 1 \pmod{21}$.

Έστω $a = 5$ και $n = 11$. Τότε $(d, x, y) = (1, -2, 1)$ και επομένως ο $-2 \equiv 9 \pmod{11}$ είναι ένας πολλαπλασιαστικός αντίστροφος του 5 modulo 11.

Να παρατηρήσουμε ότι η δομή $(\boldsymbol{Z_n}, \cdot_n)$ δεν είναι ομάδα γιατί δεν έχουν όλα τα στοιχεία του $\boldsymbol{Z_n}$ πολλαπλασιαστικούς αντίστροφους.

Θα συμφωνήσουμε ότι όταν δουλεύουμε από εδώ και πέρα με τις ομάδες $(\boldsymbol{Z_n}, +_n)$ και $(\boldsymbol{Z}_n^*, \cdot_n)$ θα ακολουθήσουμε τη βολική πρακτική του να συμβολίζουμε τις κλάσεις ισοδυναμίας με τους αντιπρόσωπούς τους σημειώνοντας τις πράξεις $+_n$ και $\cdot_n$ με τα συνήθη αριθμητικά σύμβολα + και · (ή παραλείποντας την ·) αντίστοιχα. Επίσης, οι ισοδυναμίες modulo n μπορούν να ερμηνευθούν και ως εξισώσεις στο $\boldsymbol{Z_n}$. Για παράδειγμα, οι ακόλουθες σχέσεις

$ax \equiv b \pmod{n}$

$[a]_n \cdot_n [x]_n = [b]_n$

είναι ισοδύναμες.

Το (πολλαπλασιαστικό) αντίστροφο ενός στοιχείου a θα συμβολίζεται με $a^{-1} \bmod n$ και μπορούμε να ορίσουμε διαίρεση στο $\boldsymbol{Z}_n^*$ με τη σχέση $a/b \equiv ab^{-1} \pmod{n}$. Για παράδειγμα, στο $\boldsymbol{Z}_9^*$ έχουμε ότι $4^{-1} = 7$, δηλ. $4^{-1} \equiv 7 \pmod 9$ γιατί $4 \cdot 7 = 28 \equiv 1 \pmod 9$.

Θα συμφωνήσουμε επίσης ότι όταν από τα συμφραζόμενα φαίνεται ποια είναι η πράξη στην οποία αναφερόμαστε, αντί να γράφουμε η ομάδα (G, ⊕) θα γράφουμε απλά η ομάδα G. Έτσι μπορούμε να αναφερόμαστε στις ομάδες $(\boldsymbol{Z_n}, +_n)$ και $(\boldsymbol{Z}_n^*, \cdot_n)$ ως $\boldsymbol{Z_n}$ και $\boldsymbol{Z}_n^*$, αντίστοιχα.

ΟΡΙΣΜΟΣ 2.3 – Η δομή $(G_0, \oplus)$ λέγεται ***υποομάδα*** μιας ομάδας $(G, \oplus)$ όταν $G_0 \subseteq G$ και η ίδια είναι ομάδα. Αν μάλιστα $G_0 \neq G$, τότε λέγεται ***γνήσια*** υποομάδα.

Για παράδειγμα, το σύνολο των άρτιων είναι μια προσθετική υποομάδα της ομάδας $(\boldsymbol{Z}, +)$. Αντίθετα, η ομάδα $\boldsymbol{Z_n}$ δεν είναι υποομάδα της ομάδας $(\boldsymbol{Z}, +)$ γιατί οι πράξεις της πρόσθεσης είναι διαφορετικές.

Το ουδέτερο στοιχείο e μιας ομάδας (G, ⊕) είναι και ουδέτερο στοιχείο κάθε υποομάδας της, γιατί αν υποθέσουμε ότι e_1 είναι το ουδέτερο στοιχείο μιας υποομάδας $(G_0, \oplus)$ και $\alpha \in G_0$, τότε $\alpha \oplus e_1 = \alpha = \alpha \oplus e \Rightarrow e_1 = e$.

Ένα χρήσιμο κριτήριο για το χαρακτηρισμό μιας δομής ως υποομάδας, είναι το ακόλουθο:

ΘΕΩΡΗΜΑ 2.11 – Αν (G, ⊕) είναι μια ομάδα και G_0 ένα μη κενό υποσύνολο του G, η δομή $(G_0, \oplus)$ είναι μια υποομάδα της (G, ⊕) αν και μόνον αν:

i) Το G_0 είναι κλειστό ως προς την πράξη ⊕
ii) Το συμμετρικό κάθε στοιχείου του G_0 είναι στοιχείο του G_0.

Πράγματι, αν υποθέσουμε ότι ισχύουν οι (i) και (ii), τότε αν a' είναι το συμμετρικό του $a \in G_0$ θα είναι $a' \in G_0$ και συνεπώς $a \oplus a' \in G_0$. Δηλαδή το ουδέτερο στοιχείο $e = a \oplus a'$ είναι στοιχείο του G_0, που σημαίνει ότι η δομή $(G_0, \oplus)$ είναι ομάδα άρα και υποομάδα. Αντίστροφα, αν υποθέσουμε ότι η $(G_0, *)$ είναι υποομάδα της (G, ⊕), τότε είναι ομάδα ως προς την πράξη ⊕ και συνεπώς ισχύουν οι (i) και (ii).▁

Το Θεώρημα 2.11 είναι γνωστό και ως ‘‘έλεγχος δύο βημάτων’’ (two step test). Υπάρχει η δυνατότητα να διατυπωθεί και ως έλεγχος ενός βήματος. Πρόκειται για το

ΘΕΩΡΗΜΑ 2.12 – Αν (G, ⊕) είναι μια ομάδα και G_0 ένα μη κενό υποσύνολο του G, η δομή $(G_0, \oplus)$ είναι μια υποομάδα της (G, ⊕) αν και μόνον αν $a \oplus b' \in G_0$ για κάθε $a, b' \in G_0$.

Ειδικά αν το G_0 είναι *πεπερασμένο* υποσύνολο του G τότε το Θεώρημα 2.11 διατυπώνεται ως εξής:

ΘΕΩΡΗΜΑ 2.13 – Αν (G, ⊕) είναι μια ομάδα και G_0 ένα μη κενό πεπερασμένο υποσύνολο του G, η δομή (G_0, ⊕) είναι μια υποομάδα της (G, ⊕) αν και μόνον αν το G_0 είναι κλειστό ως προς την πράξη ⊕.

Οι αποδείξεις των δύο τελευταίων θεωρημάτων δίνονται ως άσκηση.

Χρήσιμη πληροφορία για την τάξη μιας υποομάδας μας δίνει το ακόλουθο θεώρημα, γνωστό ως θεώρημα του ***Lagrange***, και το πόρισμα που ακολουθεί (η απόδειξή τους παραλείπεται).

ΘΕΩΡΗΜΑ 2.14 – Αν (G, ⊕) είναι μια πεπερασμένη ομάδα και (G_0, ⊕) είναι μια υποομάδα της, τότε ο $|G_0|$ είναι διαιρέτης του |G|.

ΠΟΡΙΣΜΑ 2.4– Αν (G_0, ⊕) είναι μια γνήσια υποομάδα μιας πεπερασμένης ομάδας (G, ⊕), τότε $|G_0| \le |G| / 2$.

Είναι χρήσιμο να ορίσουμε σε μια πεπερασμένη ομάδα την ‘‘εκθετοποίηση’’ ως επανειλημμένη εφαρμογή της πράξης, με

$$\underbrace{\alpha \oplus \alpha \oplus \ldots \oplus \alpha}_{k} = \bigoplus_{i=1}^{k} a^{(k)}, \ \alpha^{(0)} = e \text{ και } a^{(-k)} = (a')^{(k)}, \text{ όπου } k \in \boldsymbol{N}^*$$

Εδώ ο συμβολισμός προσομοιάζει αυτού που θα χρησιμοποιούσαμε εάν η πράξη είναι πολλαπλασιασμός. Οποτεδήποτε η πράξη είναι πρόσθεση, αν $k \in \boldsymbol{N}^*$, $a^{(k)}$ σημαίνει

$$\underbrace{\alpha + \alpha + \ldots + \alpha}_{k} = ka$$

και $a^{(-k)}$ σημαίνει

$$\underbrace{-\alpha + (-\alpha) + \ldots + (-\alpha)}_{k} = k(-a)$$

ενώ $\alpha^{(0)}$ σημαίνει 0. Να σημειωθεί ότι *nα* είναι συντομογραφία και δε θα πρέπει να θεωρηθεί ως το γινόμενο του $n \in \boldsymbol{Z}$ με το $\alpha \in$ G.

Για παράδειγμα, αν θεωρήσουμε $\alpha = 2$ στην ομάδα $\boldsymbol{Z}_6$, η ακολουθία $\alpha^{(1)}$, $\alpha^{(2)}$, $\alpha^{(3)}$, … είναι 2, 4, 0, 2, 4, 0, 2, 4, 0, …. Στην ομάδα $\boldsymbol{Z}_n$ έχουμε, $\alpha^{(k)} = ka \bmod n$ και στην ομάδα $\boldsymbol{Z}_n^*$ έχουμε, $\alpha^{(k)} = a^k \bmod n$.

Αν τώρα (G, ⊕) είναι πεπερασμένη ομάδα και $\alpha \in G$, τότε το σύνολο

$$\langle \alpha \rangle = \{\alpha^{(k)} : k \in \boldsymbol{N}^*\}$$

όλων των ‘‘δυνάμεων’’ του α ορίζει μια υποομάδα της G που λέγεται ότι είναι η ***υποομάδα που δημιουργείται από το α*** και συμβολίζεται με ($\langle \alpha \rangle$, ⊕) ή με $\langle \alpha \rangle$. Λέ-

με επίσης ότι το α ***δημιουργεί*** την υποομάδα $\langle\alpha\rangle$ ή ότι α είναι ένας ***γεννήτορας*** (generator) της $\langle\alpha\rangle$. Για παράδειγμα, στην ομάδα $\boldsymbol{Z}_6$ έχουμε

$\langle 0\rangle = \{0\}$

$\langle 1\rangle = \{0, 1, 2, 3, 4, 5\}$

$\langle 2\rangle = \{0, 2, 4\}$

και στο $\boldsymbol{Z}_7^*$ παρόμοια έχουμε

$\langle 1\rangle = \{1\}$

$\langle 2\rangle = \{1, 2, 4\}$

$\langle 3\rangle = \{1, 2, 3, 4, 5, 6\}$

Η ***τάξη*** (order) ενός στοιχείου $\alpha \in$ G, συμβολικά ord(α), ορίζεται ως ο μικρότερος θετικός ακέραιο t για τον οποίο είναι,

$\alpha^{(t)} = e$

όπου e είναι το ουδέτερο στοιχείο της ομάδας (G, $\oplus$). Για την τάξη ενός στοιχείου ας αποδείξουμε το ακόλουθο

ΘΕΩΡΗΜΑ 2.15 – Αν (G, $\oplus$) είναι μια πεπερασμένη ομάδα και $a \in$ G, τότε ord(α) = $|\langle\alpha\rangle|$.

Απόδειξη Θα αποδείξουμε ότι η τάξη ενός στοιχείου είναι ίση με την τάξη της υποομάδας που δημιουργείται από το στοιχείο αυτό. Έστω t = ord(α). Επειδή $\alpha^{(t)} = e$ και $\alpha^{(t+k)} = a^{(t)} \oplus a^{(k)} = e \oplus a^{(k)} = a^{(k)}$, $k \in \boldsymbol{N}^*$, αν $m > t$, τότε $a^{(m)} = a^{(s)}$, για κάποιο $s < m$. Έτσι, δεν εμφανίζονται άλλα στοιχεία μετά το $\alpha^{(t)}$, που σημαίνει ότι $\langle\alpha\rangle = \{\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}\}$ και $|\langle\alpha\rangle| \le t$. Αρκεί τώρα να δείξουμε ότι $|\langle\alpha\rangle| \ge t$. Χρησιμοποιούμε εις άτοπο απαγωγή. Υποθέτουμε δηλαδή ότι $|\langle\alpha\rangle| < t$ οπότε θα είναι $\alpha^{(i)} = \alpha^{(j)}$ για κάποια i, j τέτοια ώστε $1 \le i < j \le t$. Τότε, $\alpha^{(i+k)} = \alpha^{(j+k)}$ για $k \ge 0$, οπότε θα είναι $\alpha^{(i+(t-j))} = \alpha^{(j+(t-j))} = e$, άτοπο γιατί $i + (t - j) < t$ και t είναι ο μικρότερος θετικός ακέραιος για τον οποίο είναι $\alpha^{(t)} = e$._

ΠΟΡΙΣΜΑ 2.5 – Η ακολουθία των ‘‘δυνάμεων’’ του στοιχείου a : $a^{(1)}, a^{(2)}, \ldots$ είναι περιοδική με περίοδο t = ord(a), που σημαίνει ότι
$\alpha^{(k)} = \alpha^{(m)}$ αν και μόνον αν $k \equiv m \pmod t$.

Με βάση το παραπάνω πόρισμα είναι συνεπές μ’ αυτό να ορίσουμε

$a^{(0)} = e$
$a^{(k)} = a^{(k \bmod t)}$, όπου t = ord(a), $k \in \boldsymbol{Z}$.

ΠΟΡΙΣΜΑ 2.6 – Αν (G, $\oplus$) είναι μια πεπερασμένη ομάδα και $a \in$ G, τότε
$a^{(|G|)} = e$.

Πράγματι, από το Θεώρημα 2.14 προκύπτει ότι ord(a) | |G|, οπότε αν t = ord(a), είναι |G| ≡ 0 (mod t) και συνεπώς, $a^{(|G|)} = a^{(0)} = e$.

2.4. Επίλυση modular γραμμικών εξισώσεων

Όπως θα δούμε στο Κεφάλαιο 6, ένα τμήμα της διαδικασίας εύρεσης κλειδιών στο κρυπτοσύστημα δημόσιου κλειδιού RSA έχει να κάνει με την εύρεση λύσεων εξίσωσης της μορφής

$$ax \equiv b \pmod{n}, \quad a > 0, n > 0 \tag{2.21}$$

Υπάρχουν βέβαια και άλλες εφαρμογές αυτού του προβλήματος. Υποθέτουμε ότι είναι δεδομένα τα a, b και n και ζητάμε τις τιμές του x, modulo n, οι οποίες ικανοποιούν την εξίσωση (2.21).

Έστω $\langle\alpha\rangle$ η υποομάδα της ομάδας $\boldsymbol{Z_n}$ που δημιουργείται από το a. Επειδή

$$\langle\alpha\rangle = \{a^{(x)} : x > 0\} = \{ax \bmod n : x > 0\}$$

η εξίσωση (2.21) έχει λύση αν και μόνον αν $b \in \langle\alpha\rangle$. Το Θεώρημα 2.14 του Lagrange μας λέει ότι ο $|\langle\alpha\rangle|$ πρέπει να είναι διαιρέτης του n. Ένας ακριβής χαρακτηρισμός του $\langle\alpha\rangle$ δίνεται από το ακόλουθο θεώρημα.

ΘΕΩΡΗΜΑ 2.16 – Αν a και n είναι θετικοί ακέραιοι και d = gcd(a, n), τότε

$$\langle\alpha\rangle = \langle d\rangle = \{0, d, 2d, \ldots, ((n/d) - 1)d\} \tag{2.22}$$

στο $\boldsymbol{Z_n}$ και $|\langle\alpha\rangle| = n/d$.

Απόδειξη Από τον αλγόριθμο του Ευκλείδη στην ανεπτυγμένη του μορφή (αλγόριθμος Ευκλείδης2) προκύπτουν, όπως έχουμε δει, ακέραιοι x' και y' τέτοιοι ώστε $ax' + ny' = d$, που σημαίνει ότι $ax' \equiv d \pmod{n}$, οπότε συμπεραίνουμε ότι $d \in \langle\alpha\rangle$. Επειδή τώρα $d \in \langle\alpha\rangle$, κάθε πολλαπλάσιο του d ανήκει και αυτό στο $\langle\alpha\rangle$ επειδή οποιοδήποτε πολλαπλάσιο ενός πολλαπλάσιου του α είναι ένα πολλαπλάσιο του α. Έτσι, το $\langle\alpha\rangle$ περιέχει κάθε στοιχείο από το σύνολο $\{0, d, 2d, \ldots, ((n/d) - 1)d\}$, που σημαίνει ότι $\langle d\rangle \subseteq \langle\alpha\rangle$. Προκειμένου τώρα να δείξουμε ότι $\langle\alpha\rangle = \langle d\rangle$ αρκεί να δείξουμε ότι $\langle\alpha\rangle \subseteq \langle d\rangle$. Έστω $m \in \langle\alpha\rangle$. Τότε, $m = ax \bmod n$ για κάποιον ακέραιο x και επομένως, $m = ax + ny$ για κάποιον ακέραιο y. Αλλά, $d \mid a$ και $d \mid n$ και από την (2.4) έχουμε ότι $d \mid m$, άρα $m \in \langle d\rangle$. Συνεπώς, $\langle\alpha\rangle \subseteq \langle d\rangle$. Για το ότι $|\langle\alpha\rangle| = n/d$, αρκεί να παρατηρήσουμε ότι υπάρχουν ακριβώς n/d πολλαπλάσια του d μεταξύ των ακέραιων 0 και $n - 1$ (συμπεριλαμβανομένων).▁

ΠΟΡΙΣΜΑ 2.7 – Η εξίσωση $ax \equiv b \pmod{n}$ έχει μία τουλάχιστον λύση αν και μόνον αν $d \mid b$, με d = gcd(a, n).

ΘΕΩΡΗΜΑ 2.17 – Η εξίσωση $ax \equiv b \pmod{n}$ είτε έχει d (= gcd(a, n)) διακεκριμένες λύσεις modulo n, ή είναι αδύνατη.

Απόδειξη Έστω ότι η εξίσωση $ax \equiv b \pmod{n}$ έχει λύση. Τότε θα είναι ο b στοιχείο του $\langle\alpha\rangle$. Επειδή $\text{ord}(\alpha) = |\langle\alpha\rangle|$ (βλ. Θεώρημα 2.15), από το ΠΟΡΙΣΜΑ 2.5 και το Θεώρημα 2.16 συνεπάγεται ότι η ακολουθία $ak \bmod n$, $k = 0, 1, \ldots$, είναι περιοδική με περίοδο $t = |\langle\alpha\rangle| = n/d$. Αν $b \in \langle\alpha\rangle$ τότε ο b θα εμφανίζεται ακριβώς d φορές στην πεπερασμένη ακολουθία $ak \bmod n$, όπου $k = 0, 1, \ldots, n-1$, το μήκους (n/d) τμήμα τιμών $\langle\alpha\rangle$ επαναλαμβάνεται ακριβώς d φορές καθώς ο k αυξάνει από το 0 έως τον $n-1$. Στην ουσία, οι δείκτες x των d θέσεων για τους οποίους είναι, $ax = b \pmod{n}$, αποτελούν τις λύσεις της εξίσωσης $ax \equiv b \pmod{n}$.▁

ΘΕΩΡΗΜΑ 2.18 – Έστω $d = \gcd(a, n) = ax' + ny'$ για κάποιους ακέραιους x', y'. Αν $d \mid b$, τότε μια λύση x_0 της εξίσωσης $ax \equiv b \pmod{n}$ δίνεται από τον τύπο

$$x_0 = x'(b/d) \bmod n.$$

Απόδειξη Έχουμε διαδοχικά

$$\begin{aligned} ax_0 &\equiv ax'(b/d) \pmod{n} \\ &\equiv d(b/d) \pmod{n} \\ &\equiv b \pmod{n} \end{aligned}$$

όπου χρησιμοποιήσαμε το γεγονός ότι από την $d = ax' + ny'$ συνεπάγεται ότι $ax' \equiv d \pmod{n}$.▁

Ένα πιο γενικό θεώρημα από το παραπάνω, είναι το ακόλουθο

ΘΕΩΡΗΜΑ 2.19 – Έστω ότι η εξίσωση $ax \equiv b \pmod{n}$ είναι τέτοια ώστε $d \mid b$, όπου $d = \gcd(a, n)$ και μια οποιαδήποτε λύση της είναι ο ακέραιος x_0. Τότε η εξίσωση αυτή έχει ακριβώς d διακεκριμένες λύσεις, modulo n, οι οποίες δίνονται από τον τύπο

$$x_k = x_0 + k(n/d), \quad k = 0, 1, \ldots, d-1.$$

Απόδειξη Οι ακέραιοι $x_0, x_1, \ldots, x_{d-1}$ είναι όλοι διακεκριμένοι, modulo n, επειδή $n/d > 0$ και $0 \le k(n/d) < n$, $k = 0, 1, \ldots, d-1$. Επίσης, επειδή x_0 είναι λύση της εξίσωσης $ax \equiv b \pmod{n}$, έχουμε $ax_0 \bmod n = b$, οπότε για $k = 0, 1, \ldots, d-1$, είναι

$$\begin{aligned} ax_k \bmod n &= a(x_0 + kn/d) \bmod n \\ &= (ax_0 + akn/d) \bmod n \\ &= ax_0 \bmod n \\ &= b \end{aligned}$$

που σημαίνει ότι x_k είναι επίσης μια λύση. Το Θεώρημα 2.15 όμως μας λέει ότι υπάρχουν ακριβώς d λύσεις και κατά συνέπεια όλες αυτές οι λύσεις πρέπει να είναι οι $x_0, x_1, \ldots, x_{d-1}$.▁

Ο παρακάτω αλγόριθμος επιστρέφει όλες τις λύσεις της εξίσωσης $ax \equiv b \pmod{n}$ για οποιουσδήποτε εισαγόμενους θετικούς ακέραιους a, n και ακέραιο b.

ΛυτηςΜοdΓραμμικηΕξισωση(a, b, n)

```
1  (d, x′, y′) ← Ευκλείδης2(a, n)
2  if d | b
3     then x_0 ← x′(b/d) mod n
4          for k ← 0 to d – 1
5               do τύπωσε (x_0 + kn/d) mod n
6     else τύπωσε ‘‘αδύνατη’’
```

Ιδιαίτερο ενδιαφέρον έχουν και τα ακόλουθα πορίσματα.

ΠΟΡΙΣΜΑ 2.8 – Για οποιονδήποτε ακέραιο $n > 1$, αν $\gcd(a, n) = 1$, τότε η εξίσωση $ax \equiv b \pmod{n}$ έχει μοναδική λύση, modulo n.

Αν τώρα $b = 1$, τότε ο x που ψάχνουμε να βρούμε ως λύση της $ax \equiv 1 \pmod{n}$, είναι ένας πολλαπλασιαστικός αντίστροφος του a, modulo n.

ΠΟΡΙΣΜΑ 2.9 – Για οποιονδήποτε ακέραιο $n > 1$, αν $\gcd(a, n) = 1$, τότε η εξίσωση $ax \equiv 1 \pmod{n}$ έχει μία μόνο λύση, modulo n. Διαφορετικά, είναι αδύνατη.

Αν λοιπόν $\gcd(a, n) = 1$, τότε μία λύση της εξίσωσης $ax \equiv 1 \pmod{n}$ είναι ο ακέραιος x που επιστρέφει ο αλγόριθμος Ευκλείδης2, γιατί από την εξίσωση

$$\gcd(a, n) = 1 = ax + ny$$

προκύπτει ότι $ax \equiv 1 \pmod{n}$. Αυτό σημαίνει ότι μπορούμε να υπολογίσουμε τον $a^{-1} \bmod n$ αρκετά αποτελεσματικά χρησιμοποιώντας τον αλγόριθμο Ευκλείδης2.

2.5. Δακτύλιοι - Σώματα

Στην § 2.3 γνωρίσαμε αλγεβρικές δομές με μία εσωτερική πράξη. Στο κεφάλαιο αυτό θα δούμε αλγεβρικές δομές με δύο εσωτερικές πράξεις τις οποίες θα συμβολίσουμε με + και · και θα τις ονομάσουμε πρόσθεση και πολλαπλασιασμό, αντίστοιχα.

ΟΡΙΣΜΟΣ 2.4 – Ένα σύνολο R εφοδιασμένο με τις πράξεις + και · λέγεται ***δακτύλιος*** (ring), όταν: (1) η δομή $(R, +)$ είναι αβελιανή προσθετική ομάδα, (2) ο πολλαπλασιασμός είναι προσεταιριστικός και (3) ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση.

Ώστε η δομή $(R, +, \cdot)$ είναι δακτύλιος όταν:

A.1. $\forall a, b, c \in R, \quad (a + b) + c = a + (b + c)$

A.2. $\exists\, 0 \in R, \forall a \in R, \quad a + 0 = 0 + a = a$

A.3. $\forall a \in R, \exists\, (-a) \in R, \quad a + (-a) = (-a) + a = 0$

A.4. $\forall a, b \in R, \quad a + b = b + a$

A.5. $\forall a, b, c \in R, \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

A.6. $\forall a, b, c \in R, \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{cases}$

Αν επιπλέον ο πολλαπλασιασμός είναι αντιμεταθετικός, τότε ο δακτύλιος $(R, +, \cdot)$ λέγεται ***αντιμεταθετικός***, δηλαδή όταν επιπλέον:

A.7. $\forall a, b \in R, \quad a \cdot b = b \cdot a$

Ο δακτύλιος $(R, +, \cdot)$ λέγεται ***δακτύλιος με μοναδιαίο στοιχείο***, όταν υπάρχει μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό, δηλαδή

A.8. $\exists\, 1 \in R, \forall a \in R, \quad a \cdot 1 = 1 \cdot a = a$

Για παράδειγμα, η δομή $(\boldsymbol{Z}, +, \cdot)$ είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο τον ακέραιο 1, όπως μπορούμε να δούμε εύκολα αν ανακαλέσουμε στη μνήμη μας τις γνωστές ιδιότητες της πρόσθεσης και του πολλαπλασιασμού ακεραίων. Η δομή $(\boldsymbol{Z_n}, +_n, \cdot_n)$ είναι, σύμφωνα με όσα έχουμε μέχρι τώρα αναφέρει, αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και μπορούμε να αναφερόμαστε σ' αυτόν ως ο δακτύλιος $\boldsymbol{Z_n}$.

Οι βασικές ιδιότητες σε δακτύλιο είναι αντίστοιχες στις ιδιότητες εκείνες στο $\boldsymbol{Z}$, οι οποίες δεν αναφέρονται στην αντιμεταθετικότητα του πολλαπλασιασμού και το αντίστροφο ενός στοιχείου. Εδώ θα αναφέρουμε τις δυο σημαντικότερες ιδιότητες ενός δακτυλίου.

1. Αν $(R, +, \cdot)$ είναι ένας δακτύλιος, τότε

$\forall a \in R, \quad a \cdot 0 = 0 \cdot a = 0$

2. Αν $(R, +, \cdot)$ είναι ένας δακτύλιος, τότε $\forall a, b \in R$, είναι:

i) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
ii) $(-a) \cdot (-b) = a \cdot b$

ΟΡΙΣΜΟΣ 2.5 – Αν $(R, +, \cdot)$ είναι δακτύλιος, λέμε ***χαρακτηριστική*** του τον μικρότερο θετικό ακέραιο n, αν υπάρχει, που είναι τέτοιος ώστε να είναι

$\forall\, a \in R$: $na = a + a + \ldots + a = 0$

Αν δεν υπάρχει τέτοιος ακέραιος τότε λέμε ότι η χαρακτηριστική του δακτυλίου είναι μηδέν.

ΟΡΙΣΜΟΣ 2.6 – Αν $(R, +, \cdot)$ είναι δακτύλιος, ένα στοιχείο $a \neq 0$ του R λέμε ότι είναι ***διαιρέτης του*** **0** αν υπάρχει στοιχείο $b \neq 0$ του R τέτοιο ώστε να είναι

$a \cdot b = 0$ ή $b \cdot a = 0$

ΟΡΙΣΜΟΣ 2.7 – Ένας μη μηδενικός[**] αντιμεταθετικός δακτύλιος $(R, +, \cdot)$ με μοναδιαίο στοιχείο που δεν έχει διαιρέτες του 0, λέγεται ***ακέραια περιοχή***.

Έτσι αν $(A, +, \cdot)$ είναι μια ακέραια περιοχή τότε ισχύει η συνεπαγωγή

$a \cdot b = 0 \Rightarrow a = 0$ ή $b = 0 \quad (a, b \in A)$

Βέβαια η αντίστροφη συνεπαγωγή ισχύει πάντα σε ένα δακτύλιο (βλ. παραπάνω, την ιδιότητα **1**).

Για παράδειγμα, η αλγεβρική δομή $(\boldsymbol{Z}, +, \cdot)$ είναι μια ακέραια περιοχή, γιατί είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο που δεν έχει διαιρέτες του 0 γιατί αν $a \cdot b = 0$ τότε $a = 0$ ή $b = 0$.

Επίσης να πούμε ότι στην ουσία, ένας δακτύλιος είναι ένα σύνολο στο οποίο μπορούμε να κάνουμε πρόσθεση, αφαίρεση $[a - b = a + (-b)]$ και πολλαπλασιασμό χωρίς να βγούμε από το σύνολο. Αν θέλουμε να κάνουμε και διαίρεση $[a / b = a \cdot (b^{-1})]$ χωρίς να βγούμε από το σύνολο, θα πρέπει να εμπλουτίσουμε τη δομή μας πηγαίνοντας από δακτύλιο σε σώμα (βλ. Ορισμό 2.10 παρακάτω).

ΠΑΡΑΔΕΙΓΜΑ 2.2 – Δακτύλιος $\boldsymbol{Z_8}$ ή αριθμητική modulo 8

Οι πίνακες για την πρόσθεση και τον πολλαπλασιασμό, modulo 8, είναι

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\cdot_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

για δε τους αντίθετους και αντίστροφους (όσοι υπάρχουν), modulo 8, έχουμε

a	0	1	2	3	4	5	6	7
$-a$	0	7	6	5	4	3	2	1
a^{-1}	-	1	-	3	-	5	-	7

Ο τελευταίος πίνακας επαληθεύει το γεγονός ότι ένας ακέραιος έχει αντίστροφο, modulo n, αν αυτός ο ακέραιος είναι σχετικά πρώτος με τον n. Οι ακέραιοι 1, 3, 5, 7 είναι σχετικά πρώτοι με τον 8 ενώ οι 0, 2, 4, 6 όχι.

[**] Δηλ. $R \neq \{0\}$.

Δύο βασικές έννοιες που αναφέρονται στην ‘‘ομοιότητα’’ δύο δακτυλίων είναι ο ***ομομορφισμός*** και ο ***ισομορφισμός*** δακτυλίων.

ΟΡΙΣΜΟΣ 2.8 – Μια απεικόνιση $f : R \to R'$ μεταξύ δακτυλίων με μοναδιαία στοιχεία e και e' λέγεται ομομορφισμός (δακτυλίων) αν

$f(e) = e'$ και
$\forall\, a, b \in R,\ \mathrm{f}(a + b) = \mathrm{f}(a) + \mathrm{f}(b),\ \mathrm{f}(a \cdot b) = \mathrm{f}(a) \cdot \mathrm{f}(b).$

Δηλαδή στην ουσία, ομομορφισμός σημαίνει ότι έχουμε μια απεικόνιση η οποία διατηρεί την προσθετική και την πολλαπλασιαστική δομή.

ΟΡΙΣΜΟΣ 2.9 – Μια απεικόνιση $f : R \to R'$ μεταξύ δακτυλίων με μοναδιαία στοιχεία λέγεται ισομορφισμός (δακτυλίων) αν η f είναι ένας ομομορφισμός και μια 1 – 1 αντιστοιχία μεταξύ των συνόλων R και R'.

Αν η f είναι ένας ισομορφισμός τότε η αντίστροφη απεικόνιση $g = f^{-1}$ είναι επίσης ένας ισομορφισμός. Για να το δούμε αυτό, αρκεί να δούμε ότι η g είναι ένας ομομορφισμός. Πράγματι, έστω $a', b' \in R'$. Τότε $a' = f(a)$ και $b' = f(b)$, και $g(a' \cdot b') = g(f(a) \cdot f(b)) = g(f(a \cdot b)) = f^{-1}(f(a \cdot b)) = a \cdot b = g(a') \cdot g(b')$ (Παρόμοια η περίπτωση της +).

Ο ισομορφισμός είναι ένα άκρως όμορφο χαρακτηριστικό μιας αντιστοιχίας μεταξύ δακτυλίων. Σημαίνει για παράδειγμα, ότι το a είναι ένα αντιστρέψιμο στοιχείο του R αν και μόνον αν το $f(a)$ είναι ένα αντιστρέψιμο στοιχείο του R'. (Πράγματι, $e' = f(e) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$, οπότε το $f(a^{-1})$ είναι ένα αντίστροφο του $f(a)$). Σημαίνει επίσης ότι οι ‘‘ίδιες’’ εξισώσεις ισχύουν στο πεδίο ορισμού και στο σύνολο τιμών. Για παράδειγμα, έχουμε $a^2 = b$ στο R αν και μόνον αν $f(a)^2 = f(b)$ (σημειωτέον ότι $f(a)^2 = f(a^2)$). Έτσι, το b είναι ένα τετράγωνο αν και μόνον αν το $f(b)$ είναι ένα τετράγωνο.

Ισομορφισμός σημαίνει γενικότερα ότι το πεδίο ορισμού και το σύνολο τιμών μπορούν να θεωρηθούν ίδια σε ότι αφορά την πρόσθεση και τον πολλαπλασιασμό.

ΟΡΙΣΜΟΣ 2.10 – Ένα σύνολο F εφοδιασμένο με τις πράξεις + και · λέγεται ***σώμα*** (field), όταν: (1) η δομή $(F, +, \cdot)$ είναι μη μηδενικός αντιμεταθετικός δακτύλιος, και (2) η δομή $(F^*, \cdot)$ με $F^* = F - \{0\}$ είναι ομάδα.

Ώστε η δομή $(F, +, \cdot)$ είναι σώμα όταν:

A.1. $\forall a, b, c \in F,\ \ (a + b) + c = a + (b + c)$

A.2. $\exists\, 0 \in F, \forall a \in F,\ \ a + 0 = 0 + a = a$

A.3. $\forall a \in F, \exists\, (-\alpha) \in F,\ \ a + (-\alpha) = (-\alpha) + a = 0$

A.4. $\forall a, b \in F,\ \ a + b = b + a$

A.5. $\forall a, b, c \in F,\ \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

A.6. $\forall a, b, c \in F,\ \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{cases}$

A.7. $\forall a, b \in F, \quad a \cdot b = b \cdot a$
A.8. $\exists\, 1 \in F, \forall a \in F, \quad a \cdot 1 = 1 \cdot a = a$
A.9. $\forall a \in F^*, \exists\, \alpha^{-1} \in F^*, \quad a \cdot \alpha^{-1} = \alpha^{-1} \cdot a = 1.$

Επειδή σε ένα σώμα η δομή $(F, +)$ είναι αντιμεταθετική προσθετική ομάδα και η $(F^*, \cdot)$ αντιμεταθετική πολλαπλασιαστική ομάδα:

- ► οι εξισώσεις $a + x = b$ και $a \cdot x = b$ με $a \neq 0$ έχουν μοναδική λύση
- ► ισχύουν οι νόμοι απλοποίησης ή διαγραφής:
  - $\forall a, b, c \in F, \quad a + b = a + c \Rightarrow b = c$
  - $\forall a, b, c \in F, \quad (a \cdot b = a \cdot c \ \wedge \ a \neq 0) \ \Rightarrow \ b = c$

Βασική ιδιότητα στα σώματα είναι και η ακόλουθη

Αν $(F, +, \cdot)$ είναι σώμα και $a, b \in F$ τότε ισχύει η συνεπαγωγή

$a \cdot b = 0 \ \Rightarrow \ (a = 0 \ \text{ή} \ b = 0)$

δηλαδή κάθε σώμα είναι ακέραια περιοχή. Πράγματι, αν $b \neq 0$ θα υπάρχει $b^{-1} \in F^*$ και τότε

$$a \cdot b = 0 \Rightarrow (a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1} \Rightarrow a \cdot (b \cdot b^{-1}) = 0 \Rightarrow a \cdot 1 = 0 \Rightarrow a = 0.$$

Για παράδειγμα, οι δομές $(\boldsymbol{Q}, +, \cdot)$, $(\boldsymbol{R}, +, \cdot)$ και $(\boldsymbol{C}, +, \cdot)$ των ρητών, πραγματικών και μιγαδικών αριθμών αντίστοιχα, είναι οι πλέον γνωστές περιπτώσεις σωμάτων, όπως επίσης και η $(B, +, \cdot)$ όπου B είναι το σύνολο $\{0, 1\}$ και οι πράξεις $+$ και $\cdot$ που ορίζονται στους πίνακες

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Τα παραπάνω τρία πρώτα σώματα δεν είναι πεπερασμένα ενώ το τέταρτο είναι πεπερασμένο. Ένα ***πεπερασμένο σώμα*** είναι ένα σώμα $(F, +, \cdot)$ όπου το F περιέχει ένα πεπερασμένο πλήθος στοιχείων. Το πλήθος των στοιχείων του F είναι η *τάξη* του σώματος. Τα πεπερασμένα σώματα παίζουν σημαντικό ρόλο σε πολλούς κρυπτογραφικούς αλγόριθμους, ενώ τα μη πεπερασμένα σώματα δεν παρουσιάζουν ιδιαίτερο ενδιαφέρον στην κρυπτογραφία. Θα δούμε ότι η τάξη ενός πεπερασμένου σώματος πρέπει να είναι μια δύναμη της μορφής p^n, όπου p είναι πρώτος και n ένας θετικός ακέραιος. Το πεπερασμένο σώμα τάξεως p^n συμβολίζεται συνήθως με $GF(p^n)$. Δύο ειδικές περιπτώσεις είναι ιδιαίτερου ενδιαφέροντος για τους

σκοπούς μας. Για $n = 1$, έχουμε το πεπερασμένο σώμα $GF(p)$ το οποίο έχει μια διαφορετική δομή από αυτήν των πεπερασμένων σωμάτων με $n > 1$.

2.5.1. Πεπερασμένα σώματα τάξεως p

Για δοθέντα πρώτο p, το πεπερασμένο σώμα τάξεως p, $GF(p)$ ορίζεται ως η αλγεβρική δομή $(\boldsymbol{Z_p}, +_p, \cdot_p)$, το σύνολο δηλαδή $\boldsymbol{Z_p} = \{0, 1, 2, \ldots, p-1\}$ εφοδιασμένο με τις αριθμητικές πράξεις, modulo p. Να υπενθυμίσουμε ότι το σύνολο $\boldsymbol{Z_n} = \{0, 1, 2, \ldots, n-1\}$, των ακεραίων, εφοδιασμένο με τις αριθμητικές πράξεις, modulo n, είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και ότι κάθε ακέραιος στο $\boldsymbol{Z_n}$ έχει αντίστροφο αν και μόνον αν ο ακέραιος αυτός είναι σχετικά πρώτος με τον n. Αν ο n είναι πρώτος, τότε όλοι οι μη μηδενικοί ακέραιοι στο $\boldsymbol{Z_n}$ είναι σχετικά πρώτοι με τον n και επομένως υπάρχει ένα (πολλαπλασιαστικό) αντίστροφο στοιχείο για κάθε ακέραιο στο $\boldsymbol{Z}_n^* = \boldsymbol{Z_n} - \{0\}$:

$$\forall a \in \boldsymbol{Z}_n^*, \exists z \in \boldsymbol{Z}_n^*, \quad a \cdot z \equiv 1 \pmod{p}.$$

Στο γεγονός αυτό εξ άλλου στηρίχθηκε, κυρίως, η απόδειξη του Θεωρήματος 2.10 που λέει ότι η δομή $(\boldsymbol{Z}_n^*, \cdot_n)$ είναι μια πεπερασμένη αβελιανή ομάδα τάξεως $\phi(n) = n - 1$ (όταν n πρώτος). Όλα τα παραπάνω πιστοποιούν ότι όντως το $GF(p)$ είναι ένα πεπερασμένο σώμα τάξεως p. Συνοψίζοντας σ' έναν πίνακα τις ιδιότητες που έχουμε σ' ένα σώμα, έχουμε τις παρακάτω ιδιότητες που συνιστούν την modular αριθμητική μέσα στο $GF(p)$:

Ιδιότητα	Παράσταση
Αντιμεταθετική	$(a + b) \bmod p = (b + a) \bmod p$ $(a \cdot b) \bmod p = (b \cdot a) \bmod p$
Προσεταιριστική	$[(a + b) + c] \bmod p = [a + (b + c)] \bmod p$ $[(a \cdot b) \cdot c] \bmod p = [a \cdot (b \cdot c)] \bmod p$
Επιμεριστική	$[a \cdot (b + c)] \bmod p = [(a \cdot b) + (a \cdot c)] \bmod p$ $[(a + b) \cdot c] \bmod p = [(a \cdot c) + (b \cdot c)] \bmod p$
Ουδέτερο στοιχείο	$(0 + a) \bmod p = a \bmod p$ $(a \cdot 1) \bmod p = a \bmod p$
Συμμετρικό στοιχείο	$(a + (-a)) \bmod p = 0 \bmod p$ $(a \cdot (a^{-1})) = 1 \bmod p$

Το απλούστερο πεπερασμένο σώμα είναι το $GF(2)$. Οι αριθμητικές του πράξεις συνοψίζονται εύκολα στους ακόλουθους πίνακες

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

a	$-a$	a^{-1}
0	0	–
1	1	1

Πρέπει να παρατηρήσουμε ότι η πρόσθεση είναι ισοδύναμη με την πράξη του Αποκλειστικού-Ή (*XOR*) και ο πολλαπλασιασμός είναι ισοδύναμος με την πράξη του λογικού ΚΑΙ (AND). Επίσης η πρόσθεση είναι ισοδύναμη με την αφαίρεση, αφού $\forall a, b \in GF(2)$, $b + a = b + (-a) = b - a$.

ΠΑΡΑΔΕΙΓΜΑ 2.3 – Το πεπερασμένο σώμα $GF(7)$ ή αριθμητική modulo 7

Οι πίνακες για την πρόσθεση και τον πολλαπλασιασμό, modulo 7, εύκολα βρίσκουμε ότι είναι

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Οι αντίθετοι και αντίστροφοι modulo 7, είναι

a	0	1	2	3	4	5	6
$-a$	0	6	5	4	3	2	1
a^{-1}	–	1	4	5	2	3	6

Πέρα από την αριθμητική ακεραίων έχουμε και την αριθμητική πολυωνύμων μιας μεταβλητής όπου μπορούμε να διακρίνουμε τρεις κατηγορίες:

- η γνωστή μας κανονική αριθμητική πολυωνύμων (χρήση των βασικών κανόνων της άλγεβρας)
- αριθμητική πολυωνύμων στην οποία η αριθμητική επί των συντελεστών εκτελείται modulo p, δηλαδή οι συντελεστές των πολυωνύμων θεωρούμε ότι είναι στοιχεία του $\boldsymbol{Z_p}$
- αριθμητική πολυωνύμων στην οποία οι συντελεστές των πολυωνύμων είναι στο $\boldsymbol{Z_p}$ και τα πολυώνυμα ορίζονται modulo ένα πολυώνυμο $q(x)$ του οποίου ο βαθμός είναι κάποιος ακέραιος n.

Ας κάνουμε μια σύντομη αναδρομή στη βασική θεωρία πολυωνύμων. Ένα πολυώνυμο βαθμού $n \geq 0$ είναι μια παράσταση της μορφής

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k$$

όπου οι συντελεστές a_k είναι στοιχεία ενός προκαθορισμένου συνόλου αριθμών A (σύνολο των συντελεστών) με $a_n \neq 0$. Με αυτήν την έννοια λέμε ότι το πολυώνυμο είναι ορισμένο επί του A. Το μηδενικού βαθμού πολυώνυμο λέγεται ότι είναι ένα ***σταθερό*** πολυώνυμο και είναι απλά ένα στοιχείο του συνόλου των συντελεστών. Αν όλοι οι συντελεστές του πολυωνύμου είναι 0 τότε το πολυώνυμο λέγεται ότι είναι το μηδενικό πολυώνυμο και εξ ορισμού ο βαθμός του είναι - ∞. Το πολυώνυμο $P(x)$ λέγεται ***μονοειδές*** (monic) αν ο συντελεστής του μεγιστοβάθμιου όρου του είναι 1. Σε ότι έχει να κάνει με την άλγεβρα των πολυωνύμων δεν μας ενδιαφέρει ο υπολογισμός ενός πολυωνύμου για κάποια συγκεκριμένη τιμή της μεταβλητής x και για να υπογραμμίσουμε το γεγονός αυτό η μεταβλητή x μερικές φορές αναφέρεται ως ***ακαθόριστη***.

Η αριθμητική αυτών των πολυωνύμων περιλαμβάνει τις πράξεις της πρόσθεσης, της αφαίρεσης και του πολλαπλασιασμού. Οι πράξεις αυτές ορίζονται κατά τον πλέον φυσικό τρόπο σαν να ήταν η μεταβλητή x στοιχείο του συνόλου A. Η διαίρεση ορίζεται παρόμοια, αλλά απαιτεί το A να είναι σώμα. Χαρακτηριστικές περιπτώσεις σωμάτων που χρησιμοποιούνται είναι αυτές των πραγματικών αριθμών, των ρητών και του $\boldsymbol{Z_p}$ όπου, p πρώτος. Το σύνολο όλων των ακεραίων δεν υποστηρίζει διαίρεση πολυωνύμων γιατί δεν είναι σώμα.

Η πρόσθεση και αφαίρεση εκτελούνται προσθέτοντας ή αφαιρώντας τους αντίστοιχους (ομοιόβαθμους) συντελεστές. Έτσι, αν

$$P(x) = \sum_{k=0}^{n} a_k x^k \ , \ \ Q(x) = \sum_{k=0}^{m} b_k x^k \ , \ m \leq n$$

τότε

$$P(x) + Q(x) = \sum_{k=0}^{m} (a_k + b_k) x^k + \sum_{k=m+1}^{n} a_k x^k \ .$$

Για τον πολλαπλασιασμό, ορίζουμε

$$P(x) \cdot Q(x) = \sum_{k=0}^{n+m} c_k x^k \ ,$$

όπου

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$$

με τη διευκρίνιση ότι στον τελευταίο τύπο θέτουμε $a_k = 0$ για $k > n$ και $b_k = 0$ για $k > m$.

Για παράδειγμα, αν $P(x) = 4x^3 + x - 1$ και $Q(x) = 2x^2 + x + 2$, τότε

$P(x) + Q(x) = 4x^3 + 2x^2 + 2x + 1$

$P(x) - Q(x) = 4x^3 - 2x^2 - 3$
$P(x) \cdot Q(x) = 8x^5 + 4x^4 + 10x^3 - x^2 + x - 2$

Στη συνέχεια, ας θεωρήσουμε πολυώνυμα των οποίων οι συντελεστές είναι στοιχεία κάποιου σώματος $(F, +, \cdot)$. Είναι εύκολο (και ανιαρό) να δείξουμε ότι το σύνολο όλων αυτών των πολυωνύμων, εφοδιασμένο με τις ίδιες πράξεις $(+, \cdot)$, είναι ένας δακτύλιος ο οποίος αναφέρεται ως ένας ***πολυωνυμικός δακτύλιος*** $F[x]$. Όταν κάνουμε αριθμητική με πολυώνυμα επί ενός σώματος, τότε είναι δυνατή η διαίρεση, χωρίς αυτό να σημαίνει ότι αυτή θα είναι τέλεια διαίρεση. Σε σώμα, δοθέντων δύο στοιχείων a και b, το πηλίκο a/b είναι ένα στοιχείο του σώματος. Σε ένα δακτύλιο όμως (που δεν είναι σώμα), μια διαίρεση, γενικά, θα έχει ως αποτέλεσμα ένα πηλίκο και ένα υπόλοιπο. Αν τώρα, προσπαθήσουμε να εκτελέσουμε διαίρεση πολυωνύμων επί συνόλου συντελεστών το οποίο δεν συνιστά σώμα, τότε διαπιστώνουμε ότι η διαίρεση δεν ορίζεται πάντοτε. Αν, για παράδειγμα, το σύνολο των συντελεστών είναι το σύνολο $\boldsymbol{Z}$ των ακεραίων, τότε η διαίρεση $(4x^2)/(3x)$ δεν ορίζεται γιατί θα απαιτούσε συντελεστή με τιμή 4/3 που δεν είναι στο σύνολο των συντελεστών μας. Η ίδια όμως διαίρεση είναι δυνατή επί του $\boldsymbol{Z}_7$ όπου έχουμε $(4x^2)/(3x) = 6x$, που είναι ένα έγκυρο πολυώνυμο επί του $\boldsymbol{Z}_7$.

Γενικά, όπως προαναφέραμε, ακόμα και αν το σύνολο των συντελεστών είναι σώμα, η διαίρεση πολυωνύμων δεν είναι αναγκαία τέλεια και θα παράγει ένα πηλίκο και ένα υπόλοιπο:

$$\frac{P(x)}{Q(x)} = q(x) + \frac{r(x)}{Q(x)} \qquad (2.23)$$
$$P(x) = q(x)Q(x) + r(x)$$

Αν οι βαθμοί των $P(x)$ και $Q(x)$ είναι n και m αντίστοιχα, με $m \le n$, τότε ο βαθμός του πηλίκου $q(x)$ είναι $n - m$ και ο βαθμός του υπόλοιπου $r(x)$ είναι το πολύ $m - 1$. Έχοντας κατά νου ότι επιτρέπονται υπόλοιπα, μπορούμε να πούμε ότι είναι δυνατή η διαίρεση πολυωνύμων αν το σύνολο των συντελεστών συνιστά ένα σώμα. Κατ' αναλογία με την αριθμητική ακεραίων, μπορούμε να γράφουμε $P(x) \bmod Q(x)$ για το υπόλοιπο $r(x)$ στην (2.22): $r(x) = P(x) \bmod Q(x)$. Αν $r(x) = 0$, τότε μπορούμε να πούμε ότι το $Q(x)$ ***διαιρεί*** το $P(x)$, συμβολικά $Q(x)|P(x)$, ή ισοδύναμα, μπορούμε να πούμε ότι το $Q(x)$ είναι ένας ***παράγοντας*** του $P(x)$, ή ότι το $Q(x)$ είναι ένας ***διαιρέτης*** του $P(x)$. Σε γενικές γραμμές, πολλές από τις ιδιότητες της διαιρετότητας πολυωνύμων είναι όμοιες με τις ιδιότητες της διαιρετότητας των ακέραιων αριθμών και δεν κρίνουμε σκόπιμο να τις αναφέρουμε εδώ.

Για παράδειγμα, αν $P(x) = x^3 - x^2 + 2$ και $Q(x) = x^2 + x + 1$, τότε εκτελώντας τη διαίρεση κατά τα γνωστά στο $\boldsymbol{R}[x]$, βρίσκουμε πηλίκο $q(x) = x - 2$ και υπόλοιπο $r(x) = x + 4$, γεγονός που μπορούμε να επαληθεύσουμε με την ταυτότητα της διαίρεσης

$q(x)Q(x) + r(x) = (x - 2)(x^2 + x + 1) + x + 4 = x^3 - x^2 + 2 = P(x)$.

Στα πλαίσια της κρυπτογραφίας, μας ενδιαφέρει η περίπτωση των πολυωνύμων επί του $GF(2)$. Είδαμε προηγούμενα ότι στο $GF(2)$, η πρόσθεση είναι ισοδύναμη με την πράξη *XOR* και ο πολλαπλασιασμός με την πράξη AND. Επιπλέον, η πρόσθεση και αφαίρεση είναι ισοδύναμες mod 2.

ΠΑΡΑΔΕΙΓΜΑ 2.4 – Αριθμητική πολυωνύμων επί του $GF(2)$.
Έστω $P(x) = x^6 + x^4 + x^3 + x + 1$ και $Q(x) = x^3 + x + 1$. Για τα πολυώνυμα $P(x) + Q(x)$, $P(x) \cdot Q(x)$ και $P(x) / Q(x)$ βρίσκουμε, αντίστοιχα

$$\begin{array}{r} x^6 + x^4 + x^3 + x + 1 \\ + \qquad\qquad x^3 + x + 1 \\ \hline x^6 + x^4 \end{array} \quad = P(x) + Q(x)$$

$$\begin{array}{r} \qquad\qquad x^6 \quad + x^4 + x^3 \quad + x + 1 \\ \cdot \qquad\qquad\qquad\quad x^3 \quad + x + 1 \\ \hline \qquad\qquad x^6 \quad + x^4 + x^3 \quad + x + 1 \\ \qquad x^7 \quad + x^5 + x^4 \quad + x^2 + \mathrm{x} \\ x^9 \quad + x^7 + x^6 \quad + x^4 + x^3 \\ \hline x^9 \qquad\quad + x^5 + x^4 \quad + x^2 \quad + 1 \end{array} \quad = P(x) \cdot Q(x)$$

$$\begin{array}{r|l} x^6 \quad + x^4 + x^3 \quad + x + 1 & x^3 + x + 1 \\ \cline{2-2} x^6 \quad + x^4 + x^3 & x^3 \qquad = q(x) \\ \cline{1-1} \qquad\qquad\qquad x + 1 & \qquad\quad = r(x) \end{array}$$

Ένα πολυώνυμο $P(x)$ επί ενός σώματος F λέγεται ***ανάγωγο*** (irreducible) ή ***πρώτο*** αν και μόνον αν δεν μπορεί να γραφτεί ως γινόμενο δύο πολυωνύμων τα οποία είναι βαθμού μικρότερου από τον βαθμό του $P(x)$ και είναι και τα δύο επί του F. Να τονίσουμε ότι το να είναι ένα πολυώνυμο ανάγωγο ή όχι εξαρτάται από το σώμα στο οποίο το θεωρούμε. Π. χ. το πολυώνυμο $x^2 + 1$ είναι ανάγωγο στο σώμα ($\boldsymbol{R}$, +, ·) των πραγματικών αριθμών αλλά δεν είναι ανάγωγο στο σώμα ($\boldsymbol{C}$, +, ·) των μιγαδικών, γιατί $x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$ στο $\boldsymbol{C}$. Επίσης το $x^4 + 1$ είναι ανάγωγο επί του $\boldsymbol{R}$ αλλά δεν είναι ανάγωγο επί του $GF(2)$, γιατί $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$, όπως μπορούμε εύκολα να διαπιστώσουμε.

Επεκτείνοντας την αναλογία μεταξύ της αριθμητικής πολυωνύμων επί ενός σώματος και της αριθμητικής ακεραίων, μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη δύο πολυωνύμων. Το μονοειδές πολυώνυμο $d(x)$ λέγεται ότι είναι ο μέγιστος κοινός διαιρέτης των $a(x)$ και $b(x)$, συμβολικά $\gcd[a(x), b(x)]$, αν το $d(x)$ διαιρεί το $a(x)$ και το $b(x)$ και επιπλέον, οποιοσδήποτε διαιρέτης των $a(x)$ και $b(x)$ είναι διαιρέτης του $d(x)$. Ισοδύναμος ορισμός: Ο $\gcd[a(x), b(x)]$ είναι το μονοειδές με το μεγαλύτερο βαθμό που είναι κοινός διαιρέτης των πολυωνύμων $a(x)$ και $b(x)$. Η διαδικασία υπολογισμού μέγιστων κοινών διαιρετών για πολυώνυμα βασί-

ζεται σε θεώρημα ανάλογο με το Θεώρημα 2.8 γράφοντας την εξίσωση (2.16) στη μορφή

$$\gcd[a(x), b(x)] = \gcd[b(x), a(x) \bmod b(x)]$$

όπου υποθέτουμε ότι ο βαθμός του $a(x)$ είναι μεγαλύτερος από το βαθμό του $b(x)$. Παρόμοια, ανάλογο προς το Θεώρημα 2.4 είναι και το ακόλουθο

ΘΕΩΡΗΜΑ 2.20 – Έστω τα μη μηδενικά πολυώνυμα $a(x)$ και $b(x)$ επί του σώματος F. Το μονοειδές

$$d(x) = s(x) \cdot a(x) + t(x) \cdot b(x), \;\; s(x), t(x) \in F[x]$$

ελάχιστου βαθμού, είναι ο $\gcd[a(x), b(x)]$.

2.5.2. Πεπερασμένα σώματα της μορφής $GF(2^n)$

Όπως προαναφέραμε, η τάξη ενός πεπερασμένου σώματος πρέπει να είναι της μορφής p^n, όπου p πρώτος και n θετικός ακέραιος. Επίσης είδαμε στην ειδική περίπτωση των πεπερασμένων σωμάτων τάξεως p ότι το $\boldsymbol{Z_p}$ εφοδιασμένο με τις αριθμητικές πράξεις modulo p αποκτά τη δομή πεπερασμένου σώματος. Πράξεις modulo p^n όπου $n > 1$, δεν δημιουργούν σώμα. Μένει να δούμε ποια δομή ικανοποιεί τις ιδιότητες ορισμού ενός σώματος σε ένα σύνολο με p^n στοιχεία και να επικεντρώσουμε την προσοχή μας στο $GF(2^n)$ γιατί έχει διαπιστωθεί ότι πεπερασμένα σώματα της μορφής αυτής προσφέρονται για κρυπτογραφικούς αλγόριθμους.

Ας θεωρήσουμε το σύνολο $\boldsymbol{Z_p}[x]$ όλων των πολυωνύμων βαθμού μικρότερου ή ίσου του $n - 1$ επί του σώματος $\boldsymbol{Z_p}$, δηλαδή των πολυωνύμων της μορφής

$$P(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots a_1 x \; + a_0 = \sum_{k=0}^{n-1} a_k x^k$$

όπου κάθε συντελεστής a_k παίρνει τιμές στο σύνολο $\{0, 1, 2, \ldots, p - 1\}$. Εύκολα βλέπουμε ότι το πλήθος των πολυωνύμων αυτής της μορφής (= πληθικός αριθμός του συνόλου $\boldsymbol{Z_p}[x]$) είναι p^n. Για παράδειγμα, για $p = 3$ και $n = 2$, τα πολυώνυμα του αντίστοιχου συνόλου $\boldsymbol{Z_p}[x]$ είναι

0	x	$2x$
1	$x + 1$	$2x + 1$
2	$x + 2$	$2x + 2$

Με κατάλληλους ορισμούς των αριθμητικών πράξεων, κάθε τέτοιο σύνολο $\boldsymbol{Z_p}[x]$ αποκτά τη δομή ενός πεπερασμένου σώματος. Τέτοιοι ορισμοί είναι απόρροια μιας αριθμητικής που ακολουθεί τους συνήθεις κανόνες της αριθμητικής πολυωνύμων χρησιμοποιώντας τους βασικούς κανόνες της άλγεβρας και που επιπλέον

- η αριθμητική επί των συντελεστών εκτελείται modulo p, ή με άλλα λόγια χρησιμοποιώντας τους κανόνες της αριθμητικής του σώματος $\boldsymbol{Z_p}$

- αν ο πολλαπλασιασμός έχει ως αποτέλεσμα ένα πολυώνυμο βαθμού μεγαλύτερου από $n - 1$, τότε γίνεται αναγωγή του πολυωνύμου, modulo κάποιο ανάγωγο πολυώνυμο $m(x)$ βαθμού n, δηλαδή γίνεται διαίρεση δια $m(x)$ και κρατάμε το υπόλοιπο. (Για το πολυώνυμο $P(x)$, το υπόλοιπο παριστάνεται με $P(x) \bmod m(x)$).

Για παράδειγμα, το πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard) χρησιμοποιεί αριθμητική στο $GF(2^8)$ modulo το ανάγωγο πολυώνυμο

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$

Θεωρώντας τα πολυώνυμα, $P(x) = x^6 + x^4 + x^2 + x + 1$ και $Q(x) = x^7 + x + 1$, βρίσκουμε εύκολα ότι

$$P(x) + Q(x) = x^7 + x^6 + x^4 + x^2$$

και

$$P(x) \cdot Q(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

οπότε εκτελώντας τη διαίρεση $P(x) \cdot Q(x) : m(x)$, έχουμε

$$\begin{array}{llllllll|l}
x^{13} & +x^{11} & +x^9+x^8 & +x^6+x^5+x^4+x^3 & & & & +1 & x^8+x^4+x^3+x+1 \\
\cline{9-9}
x^{13} & & +x^9+x^8 & +x^6+x^5 & & & & & x^5+x^3 \\
\cline{1-8}
 & x^{11} & & & & +x^4+x^3 & & +1 & \\
 & x^{11} & & +x^7+x^6 & & +x^4+x^3 & & & \\
\cline{1-8}
 & & & & x^7+x^6 & & & +1 &
\end{array}$$

Επομένως, $P(x) \cdot Q(x) \bmod m(x) = x^7 + x^6 + 1$.

Βλέπουμε λοιπόν ότι, όπως με την modular αριθμητική ακεραίων, έχουμε στη modular αριθμητική πολυωνύμων την έννοια του συνόλου κατάλοιπων. Το σύνολο των κατάλοιπων modulo $m(x)$, όπου $m(x)$ πολυώνυμο βαθμού n, περιέχει p^n στοιχεία, το καθένα εκ των οποίων αναπαριστάται με ένα από τα πλήθους p^n πολυώνυμα βαθμού $m < n$. Για παράδειγμα, η κλάση κατάλοιπου $[x + 1]$, modulo $m(x)$, αποτελείται από όλα τα πολυώνυμα $a(x)$ τέτοια ώστε $a(x) \equiv x + 1 \pmod{m(x)}$ ή ισοδύναμα, από όλα τα πολυώνυμα $a(x)$ που ικανοποιούν την ισότητα $a(x) \bmod m(x) = x + 1$. Αποδεικνύεται τελικά, ότι το σύνολο των πολυωνύμων modulo ένα ανάγωγο πολυώνυμο $m(x)$ βαθμού n συνιστά ένα πεπερασμένο σώμα. Επιπλέον είναι γνωστό ότι όλα τα πεπερασμένα σώματα της αυτής τάξης είναι ισόμορφα, που σημαίνει ότι δύο τέτοια σώματα έχουν την ίδια δομή και απλά η αναπαράσταση των στοιχείων μπορεί να είναι διαφορετική. Στο $GF(2^8)$ κάθε στοιχείο μπορεί να παρασταθεί μονοσήμαντα ως πολυώνυμο της μορφής

$$b_7x^7 + b_6x^6 + b_5x^5 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

όπου οι συντελεστές b_i παίρνουν τιμές 0 ή 1. Τα 8 bits παριστάνουν ένα byte, οπότε μπορούμε να αναπαριστάμε τα στοιχεία του $GF(2^8)$ ως 8-bit bytes. Για παράδειγμα, το πολυώνυμο $x^7 + x^6 + x^3 + x + 1$ γίνεται 11001011. Η πρόσθεση είναι η *XOR* των bits:

$$(x^7 + x^6 + x^3 + x + 1) + (x^4 + x^3 + 1) \Rightarrow 11001011 \oplus 00011001 = 11010010 \Rightarrow$$
$$\Rightarrow x^7 + x^6 + x^4 + x.$$

Ο πολλαπλασιασμός δεν είναι και τόσο προφανής. Αυτό οφείλεται στο γεγονός ότι δουλεύουμε modulo το πολυώνυμο $x^8 + x^4 + x^3 + x + 1$ το οποίο μπορούμε να αναπαραστήσουμε με τα 9 bits 100011011. Αρχικά ας πολλαπλασιάσουμε το $x^7 + x^6 + x^3 + x + 1$ με το x:

$$(x^7 + x^6 + x^3 + x + 1)\cdot x = x^8 + x^7 + x^4 + x^2 + x$$
$$= (x^7 + x^3 + x^2 + 1) + (x^8 + x^4 + x^3 + x + 1)$$
$$\equiv x^7 + x^3 + x^2 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}.$$

Η ίδια πράξη με bits γίνεται

$$11001011 \Rightarrow 110010110 \text{ (ολίσθηση (shift) αριστερά και προσθήκη ενός 0)}$$
$$\Rightarrow 110010110 + 100011011$$
$$= 010001101$$

που αντιστοιχεί στο προηγούμενο αποτέλεσμα. Γενικά, μπορούμε να πολλαπλασιάζουμε με το x με την ακόλουθη διαδικασία:

1. Ολίσθηση αριστερά και προσθήκη ενός 0 ως το τελευταίο bit
2. Αν το πρώτο bit είναι 0, στοπ
3. Αν το πρώτο bit είναι 1, *XOR* με 100011011.

Ο λόγος για το στοπ στο βήμα 2 είναι γιατί αν το πρώτο bit είναι 0 τότε το πολυώνυμο εξακολουθεί να έχει βαθμό μικρότερο του 8 παρότι πολλαπλασιάστηκε με το x, οπότε δεν υπάρχει λόγος να γίνει αναγωγή. Για τον πολλαπλασιασμό με μεγαλύτερες δυνάμεις του x, πολλαπλασιάζουμε διαδοχικά με x τόσες φορές όσες καθορίζει ο εκθέτης. Για παράδειγμα, ο πολλαπλασιασμός με το x^3 μπορεί να γίνει με τρεις μετατοπίσεις και τρεις το πολύ *XOR*. Ο πολλαπλασιασμός με ένα οποιοδήποτε πολυώνυμο μπορεί να επιτευχθεί πολλαπλασιάζοντας με τις διάφορες δυνάμεις του x που εμφανίζονται σ' αυτό το πολυώνυμο και στη συνέχεια προσθέτοντας (δηλ. *XOR*οντας) τα αποτελέσματα.

Συνοψίζοντας, βλέπουμε ότι οι πράξεις της πρόσθεσης και του πολλαπλασιασμού στο $GF(2^8)$ μπορούν να πραγματοποιηθούν πολύ αποτελεσματικά. Παρόμοια θεώρηση των πραγμάτων έχουμε σε οποιοδήποτε πεπερασμένο σώμα.

Η αναλογία μεταξύ των ακεραίων modulo έναν πρώτο και των πολυωνύμων modulo ένα ανάγωγο πολυώνυμο είναι αξιοσημείωτη και μπορούμε να την συνοψίσουμε ως ακολούθως

ακέραιοι	$\leftrightarrow \boldsymbol{Z_p}[x]$
πρώτος αριθμός p	$\leftrightarrow$ ανάγωγο πολυώνυμο $m(x)$ βαθμού n
$\boldsymbol{Z_p}$	$\leftrightarrow \boldsymbol{Z_p}[x] \pmod{m(x)}$
σώμα με p στοιχεία	$\leftrightarrow$ σώμα με p^n στοιχεία

Έστω $GF(p^n)^*$ το σύνολο των μη μηδενικών στοιχείων του $GF(p^n)$. Το σύνολο αυτό, το οποίο έχει $p^n - 1$ στοιχεία, είναι κλειστό ως προς τον πολλαπλασιασμό, όπως είναι το σύνολο των ακεραίων των μη ισοδύναμων με το 0 mod p κλειστό ως προς τον πολλαπλασιασμό. Αποδεικνύεται ότι υπάρχει ένα πολυώνυμο $g(x)$ τέτοιο ώστε κάθε στοιχείο του $GF(p^n)^*$ να μπορεί να εκφραστεί ως μια δύναμη του $g(x)$ (= πολυώνυμο γεννήτορας). Αυτό σημαίνει επίσης ότι ο μικρότερος εκθέτης k που είναι τέτοιος ώστε $g(x)^k \equiv 1$ είναι $p^n - 1$. Αυτό είναι το ανάλογο, όπως θα δούμε στην επόμενη ενότητα, της ***πρωτεύουσας ρίζας*** για πρώτους. Υπάρχουν $\phi(p^n - 1)$, το πλήθος, τέτοια πολυώνυμα γεννήτορες, όπου ϕ η συνάρτηση του Euler. Μια ενδιαφέρουσα περίπτωση είναι όταν $p = 2$ και ο $2^n - 1$ είναι πρώτος. Σ' αυτήν την περίπτωση, κάθε μη μηδενικό πολυώνυμο $f(x) \neq 1$ στο $GF(2^n)$ είναι ένα πολυώνυμο γεννήτορας γιατί το σύνολο $GF(2^n)^*$ είναι ομάδα της οποίας η τάξη είναι πρώτος, οπότε κάθε στοιχείο, εκτός του μοναδιαίου, είναι ένας γεννήτορας.

Ένα άλλο πρόβλημα των ακεραίων που θα δούμε στην επόμενη ενότητα και το οποίο έχει το ανάλογό του για πεπερασμένα σώματα, είναι το πρόβλημα του ***διακριτού λογάριθμου***: δοθέντος ενός πολυωνύμου $h(x)$, να βρεθεί ακέραιος k τέτοιος ώστε $h(x) = g(x)^k$ στο $GF(p^n)$. Η εύρεση ενός τέτοιου k φαίνεται να είναι πολύ δύσκολη υπόθεση στις περισσότερες των περιπτώσεων.

2.6. Κινέζικο θεώρημα υπολοίπων

Το γνωστό ως ***Κινέζικο θεώρημα υπολοίπων*** μας παρέχει μια αντιστοιχία μεταξύ ενός συστήματος εξισώσεων modulo ένα σύστημα ανά δύο σχετικά πρώτων moduli (όπως 3, 5, 7) και μιας εξίσωσης modulo το γινόμενό τους (όπως 105). Έχει δύο κύριες χρήσεις. Ας υποθέσουμε ότι ο ακέραιος n παραγοντοποιείται ως $n = n_1 n_2 \ldots n_k$, όπου οι παράγοντες n_i είναι ανά δύο σχετικά πρώτοι. Κατά πρώτον, το Κινέζικο θεώρημα υπολοίπων περιγράφει τη δομή του $\boldsymbol{Z_n}$ ως ταυτόσημη με τη δομή του Καρτεσιανού γινομένου $\boldsymbol{Z}_{n_1} \times \boldsymbol{Z}_{n_2} \times \cdots \times \boldsymbol{Z}_{n_k}$ με πρόσθεση και πολλαπλασιασμό modulo n_i στην i$^{\eta}$ συνιστώσα. Κατά δεύτερον, αυτή η περιγραφή μπορεί να χρησιμοποιηθεί προκειμένου να προκύψουν αποτελεσματικοί αλγόριθμοι, επειδή το να δουλεύει κανείς σε καθένα από τα αλγεβρικά συστήματα $\boldsymbol{Z}_{n_i}$ είναι δυνατό να είναι πιο αποτελεσματικό από το να δουλεύει modulo n.

ΘΕΩΡΗΜΑ 2.21 – Έστω $n = n_1 n_2 \ldots n_k$, όπου οι $n_1, n_2, \ldots, n_k \in \boldsymbol{N}^*$ είναι ανά δύο σχετικά πρώτοι, δηλαδή $\gcd(n_i, n_j) = 1$, για $i \neq j$. Τότε η απεικόνιση

$$f : \boldsymbol{Z_n} \to \boldsymbol{Z}_{n_1} \times \boldsymbol{Z}_{n_2} \times \cdots \times \boldsymbol{Z}_{n_k}, \; a \to (a \bmod n_1, a \bmod n_2, \ldots, a \bmod n_k) \quad (2.24)$$

είναι ένας ισομορφισμός δακτυλίων.

Πριν δώσουμε μια απόδειξη του θεωρήματος αυτού, κρίνουμε σκόπιμο να διευκρινίσουμε τι σημαίνει ότι η (2.24) είναι ένας ισομορφισμός δακτυλίων.
Έστω η αντιστοιχία

$$a \leftrightarrow (a_1, a_2, \ldots, a_k)$$

όπου $a \in \boldsymbol{Z_n}$, $a_i \in \boldsymbol{Z}_{n_i}$ και

$$a_i = a \bmod n_i$$

για $i = 1, 2, \ldots, k$. Η απεικόνιση (2.24) είναι μια 1 – 1 αντιστοιχία μεταξύ του $\boldsymbol{Z_n}$ και του $\boldsymbol{Z}_{n_1} \times \boldsymbol{Z}_{n_2} \times \cdots \times \boldsymbol{Z}_{n_k}$. Οι πράξεις που εκτελούνται στα στοιχεία του $\boldsymbol{Z_n}$ μπορούν ισοδύναμα να γίνουν στις αντίστοιχες διατεταγμένες k – αδες εκτελώντας τις πράξεις ανεξάρτητα σε κάθε συνιστώσα:

αν

$$a \leftrightarrow (a_1, a_2, \ldots, a_k),$$

$$b \leftrightarrow (b_1, b_2, \ldots, b_k),$$

τότε

$$(a + b) \bmod n \;\leftrightarrow\; ((a_1 + b_1) \bmod n_1, (a_2 + b_2) \bmod n_2, \ldots, (a_k + b_k) \bmod n_k) \quad (2.25)$$

$$(ab) \bmod n \;\leftrightarrow\; ((a_1 b_1) \bmod n_1, (a_2 b_2) \bmod n_2, \ldots, (a_k b_k) \bmod n_k) \quad (2.26)$$

Απόδειξη Αρχικά ορίζουμε

$$m_i = n/n_i = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k, \; i = 1, 2, \ldots, k. \quad (2.27)$$

Στη συνέχεια ορίζουμε

$$c_i = m_i \left(m_i^{-1} \bmod n_i \right), \quad i = 1, 2, \ldots, k \quad (2.28)$$

Από το Θεώρημα 2.5 έχουμε ότι οι m_i και n_i είναι σχετικά πρώτοι οπότε το Πόρισμα 2.9 μας εγγυάται ότι οι $\left(m_i^{-1} \bmod n_i \right)$, $i = 1, 2, \ldots, k$ υπάρχουν και επομένως η (2.28) είναι πάντοτε καλώς ορισμένη. Τελικά, μπορούμε να υπολογίσουμε τον a ως συνάρτηση των $a_1, a_2, \ldots, a_k$ με τον εξής τρόπο:

$$a \equiv a_1 c_1 + a_2 c_2 + \ldots + a_k c_k \pmod{n}. \quad (2.29)$$

Δείχνουμε τώρα ότι η (2.29) εξασφαλίζει τις $a \equiv a_i \pmod{n_i}$, $i = 1, 2, \ldots, k$. Να παρατηρήσουμε ότι αν $j \neq i$, τότε $m_j \equiv 0 \pmod{n_i}$, που συνεπάγεται ότι $c_j \equiv m_j \equiv 0$

(mod n_i). Επίσης, από την (2.28) έχουμε ότι $c_i \equiv 1 \pmod{n_i}$. Έχουμε έτσι τη χρήσιμη αντιστοιχία $c_i \leftrightarrow (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ όπου έχουμε ένα διάνυσμα με μηδενικά εκτός από την i συντεταγμένη στην οποία υπάρχει το 1. Για κάθε i έχουμε επομένως

$$a \equiv a_i c_i \pmod{n_i}$$
$$\equiv a_i m_i \left(m_i^{-1} \bmod n_i \right) \pmod{n_i}$$
$$\equiv a_i \pmod{n_i}$$

που είναι ότι ακριβώς θέλαμε να δείξουμε: η μέθοδος υπολογισμού του a από τους a_i παράγει ως αποτέλεσμα ένα a που ικανοποιεί τους περιορισμούς $a \equiv a_i \pmod{n_i}$ για $i = 1, 2, \ldots, k$. Φυσικά το να πάμε από τον a στους $(a_1, a_2, \ldots, a_k)$ γίνεται αρκετά εύκολα και άμεσα απαιτώντας μόνο k διαιρέσεις. Έτσι η αντιστοιχία είναι 1 – 1 επειδή ο μετασχηματισμός είναι αμφίδρομος. Τελικά, οι (2.25), (2.26) προκύπτουν από το γεγονός ότι, όπως αποδεικνύεται εύκολα, $b \bmod n_i \equiv (b \bmod n) \bmod n_i$ για κάθε b και $i = 1, 2, \ldots, k$._

Από το παραπάνω θεώρημα προκύπτουν τα παρακάτω δύο χρήσιμα πορίσματα.

ΠΟΡΙΣΜΑ 2.10 – Αν $n_1, n_2, \ldots, n_k$ είναι ανά δύο σχετικά πρώτοι και $n = n_1 n_2 \cdots n_k$, τότε για οποιουσδήποτε ακέραιους $a_1, a_2, \ldots, a_k$, το σύστημα των εξισώσεων (ισοτιμιών)

$$x \equiv a_i \pmod{n_i}, \quad i = 1, 2, \ldots, k$$

έχει μοναδική λύση, modulo n, για τον άγνωστο x.

ΠΟΡΙΣΜΑ 2.11 – Αν $n_1, n_2, \ldots, n_k$ είναι ανά δύο σχετικά πρώτοι και $n = n_1 n_2 \cdots n_k$, τότε για όλους τους ακέραιους x και a, είναι

$$x \equiv a \pmod{n_i}, \quad i = 1, 2, \ldots, k$$

αν και μόνον αν

$$x \equiv a \pmod{n}.$$

ΠΑΡΑΔΕΙΓΜΑ 2.5 – Έστω ότι δίνονται οι ισοτιμίες

$$x \equiv 2 \pmod{9}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 2 \pmod{4}$$

Είναι,

$$a_1 = 2, a_2 = 1, a_3 = 2,$$

$$n = 9 \cdot 5 \cdot 4 = 180,$$

$n_1 = 9$, $n_2 = 5$, $n_3 = 4$,

$m_1 = 5\cdot4 = 20$, $m_2 = 9\cdot4 = 36$, $m_3 = 9\cdot5 = 45$.

Θέλουμε να υπολογίσουμε τον a mod 180, γιατί $n = 180$. Υπολογίζουμε τους αντίστροφους (χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη ή με δοκιμές) των 20, 36 και 45, modulo 9, 5 και 4 αντίστοιχα: $20^{-1} \equiv 5 \pmod 9$, $36^{-1} \equiv 1 \pmod 5$ και $45^{-1} \equiv 1 \pmod 4$. Επομένως,

$c_1 = 20(5 \bmod 9) = 100$

$c_2 = 36(1 \bmod 5) = 36$

$c_3 = 45(1 \bmod 4) = 45$

και

$$a \equiv 2\cdot100 + 1\cdot36 + 2\cdot45 \pmod{180}$$
$$\equiv 146 \pmod{180}$$

είναι η μοναδική λύση του συστήματος.

2.6.1. Συστήματα γραμμικών ισοδυναμιών

Εφαρμόζοντας μεθόδους παρμένες από τη γραμμική άλγεβρα, μπορούμε να λύσουμε συστήματα n γραμμικών ισοδυναμιών με n άγνωστους ακέραιους. Τέτοια συστήματα προκύπτουν σε κρυπτογραφικές μελέτες και για να αντιμετωπίσουμε την περίπτωση που ο n είναι μεγάλος ακέραιος είναι σκόπιμο να χρησιμοποιήσουμε τη γλώσσα των πινάκων έτσι όπως τη συναντάει κανείς σε ένα βιβλίο γραμμικής άλγεβρας.

ΟΡΙΣΜΟΣ 2.11 – Έστω $\boldsymbol{A} = [a_{ij}]$ και $\boldsymbol{B} = [b_{ij}]$ δύο $l\times m$ πίνακες με στοιχεία ακέραιους. Λέμε ότι "$\boldsymbol{A}$ είναι ***ισότιμος*** ή ***ισοδύναμος*** με $\boldsymbol{B}$, modulo n", συμβολικά $\boldsymbol{A} \equiv \boldsymbol{B} \pmod n$, αν $a_{ij} \equiv b_{ij} \pmod n$ για όλα τα (i, j) με $1 \le i \le l$ και $1 \le j \le m$.

Στην ουσία πρόκειται για έναν συνοπτικό τρόπο να γράψει κανείς $l\cdot m$ ισοδυναμίες, modulo n. Για παράδειγμα, εύκολα μπορούμε να δούμε ότι

$$\begin{pmatrix} 15 & 3 \\ 8 & 12 \end{pmatrix} \equiv \begin{pmatrix} 4 & 3 \\ -3 & 1 \end{pmatrix} \pmod{11}$$

Βασιζόμενοι στον πολλαπλασιασμό πινάκων και τους κανόνες της modular αριθμητικής μπορούμε να αποδείξουμε (δίνεται ως άσκηση) το ακόλουθο θεώρημα.

ΘΕΩΡΗΜΑ 2.22 – Αν $\boldsymbol{A}$ και $\boldsymbol{B}$ είναι $l\times m$ πίνακες τέτοιοι ώστε $\boldsymbol{A} \equiv \boldsymbol{B} \pmod n$, $\boldsymbol{C}$ είναι ένας $k\times l$ πίνακας και $\boldsymbol{D}$ είναι ένας $m\times k$ πίνακας, όλοι τους με στοιχεία ακέραιους, τότε $\boldsymbol{CA} \equiv \boldsymbol{CB} \pmod n$ και $\boldsymbol{AD} \equiv \boldsymbol{BD} \pmod n$.

Έστω τώρα το σύστημα

$$\begin{aligned} a_{11}x_1 &+ a_{12}x_2 + \cdots + a_{1m}x_m \equiv b_1 \pmod n \\ a_{21}x_1 &+ a_{22}x_2 + \cdots + a_{2m}x_m \equiv b_2 \pmod n \\ &\vdots \\ a_{m1}x_1 &+ a_{m2}x_2 + \cdots + a_{mm}x_m \equiv b_m \pmod n \end{aligned}$$

Χρησιμοποιώντας πίνακες το σύστημα αυτό μπορεί να γραφεί στη μορφή

$\boldsymbol{AX} \equiv \boldsymbol{B} \pmod n$,

όπου

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ & & \ddots & \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix}, \quad \boldsymbol{X} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \quad \text{και} \quad \boldsymbol{B} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

Για παράδειγμα, το σύστημα

$$\begin{aligned} 2x &+ 5y \equiv 5 \pmod{11} \\ 3x &+ 4y \equiv 7 \pmod{11} \end{aligned}$$

γράφεται

$$\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 7 \end{pmatrix} \pmod{11}.$$

ΟΡΙΣΜΟΣ 2.12 – Αν για τον $m \times m$ πίνακα ακεραίων $\boldsymbol{A}$ υπάρχει πίνακας ακεραίων $\boldsymbol{X}$ τέτοιος ώστε να είναι $\boldsymbol{AX} \equiv \boldsymbol{XA} \equiv \boldsymbol{I} \pmod n$, όπου $\boldsymbol{I}$ είναι ο μοναδιαίος πίνακας τάξεως m, τότε λέμε ότι ο $\boldsymbol{A}$ είναι αντιστρέψιμος modulo n και καλούμε τον $\boldsymbol{X}$ αντίστροφο του $\boldsymbol{A}$ modulo n, συμβολίζοντας με $\boldsymbol{A}^{-1}$.

Για τους αντίστροφους πίνακες modulo n, αποδεικνύονται εύκολα οι εξής προτάσεις:

- Αν ο $\boldsymbol{A}^{-1}$ είναι ένας αντίστροφος του $\boldsymbol{A}$, modulo n και $\boldsymbol{B} \equiv \boldsymbol{A}^{-1} \pmod n$, τότε ο $\boldsymbol{B}$ είναι επίσης ένας αντίστροφος του $\boldsymbol{A}$, modulo n.
- Αν $\boldsymbol{B}_1$ και $\boldsymbol{B}_2$ είναι και οι δύο αντίστροφοι του $\boldsymbol{A}$, modulo n, τότε $\boldsymbol{B}_1 \equiv \boldsymbol{B}_2 \pmod n$.

ΠΑΡΑΔΕΙΓΜΑ 2.6 – Επειδή

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \equiv \begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

και

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \equiv \begin{pmatrix} 131 & 182 \\ 286 & 261 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

έχουμε ότι ο πίνακας $\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$ είναι ένας αντίστροφος του πίνακα $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, modulo 26.

Για την εύρεση του αντίστροφου ενός τετραγωνικού πίνακα $m \times m$ πρέπει να χρησιμοποιήσουμε την έννοια του προσαρτημένου πίνακα.

ΟΡΙΣΜΟΣ 2.13 – Αν $\boldsymbol{A} = [a_{ij}]$ είναι ένας $m \times m$ πίνακας, ο *προσαρτημένος* ή *adjoint* του $\boldsymbol{A}$, συμβολικά adj$\boldsymbol{A}$, είναι ο $m \times m$ πίνακας με στοιχείο A_{ji} στη θέση (i, j), όπου $A_{ij} = (-1)^{i+j} (\det \boldsymbol{A}^{c}_{ij})$.

Στον παραπάνω ορισμό χρησιμοποιήσαμε την έννοια της ορίζουσας τετραγωνικού πίνακα. Να θυμίσουμε ότι, ***ορίζουσα*** του $\boldsymbol{A}$ λέμε τον αριθμό

$$\det \boldsymbol{A} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{vmatrix} = \sum_{j=1}^{m} (-1)^{i+j} a_{ij} \left(\det \boldsymbol{A}_{ij}^{c} \right)$$

όπου $\boldsymbol{A}_{ij}^{c}$ είναι ένας $(m\text{-}1) \times (m\text{-}1)$ ελάσσων πίνακας που προκύπτει από τον πίνακα Α διαγράφοντας την i γραμμή και την j στήλη. Το άθροισμα στον τύπο υπολογίζεται *για οποιαδήποτε τιμή του i* και συχνά αναφέρεται ως το ανάπτυγμα της ορίζουσας ως προς τα στοιχεία της i γραμμής.

ΘΕΩΡΗΜΑ 2.23 – Αν $\boldsymbol{A}$ είναι ένας $m \times m$ πίνακας με $\det \boldsymbol{A} \neq 0$, τότε

$$\boldsymbol{A} \cdot \text{adj}\boldsymbol{A} = \text{adj}\boldsymbol{A} \cdot \boldsymbol{A} = (\det \boldsymbol{A})\boldsymbol{I}$$

Χρησιμοποιώντας αυτό το θεώρημα, μπορούμε να αποδείξουμε ότι ισχύει το ακόλουθο

ΘΕΩΡΗΜΑ 2.24 – Αν $\boldsymbol{A}$ είναι ένας $m \times m$ πίνακας με στοιχεία ακέραιους και n είναι θετικός ακέραιος τέτοιος ώστε $\gcd(\det \boldsymbol{A}, n) = 1$, τότε ο πίνακας

$$\boldsymbol{A}^{-1} = D^{-1} \text{adj}\boldsymbol{A}$$

είναι ένας αντίστροφος του $\boldsymbol{A}$ modulo n, όπου D^{-1} είναι ένας αντίστροφος του $D = \det \boldsymbol{A}$, modulo n.

Απόδειξη Χρησιμοποιώντας $D = \det\boldsymbol{A}$, αν $\gcd(D, n) = 1$, τότε είναι γνωστό ότι $D \neq 0$, οπότε από το Θεώρημα 2.23, έχουμε $\boldsymbol{A}\cdot\mathrm{adj}\boldsymbol{A} = D\boldsymbol{I}$. Επειδή $\gcd(D, n) = 1$, υπάρχει ένας αντίστροφος D^{-1} του D modulo n, οπότε

$$\boldsymbol{A}\cdot(D^{-1}\,\mathrm{adj}\boldsymbol{A}) \equiv D^{-1}\,\boldsymbol{A}\cdot\mathrm{adj}\boldsymbol{A} \equiv D^{-1}D\boldsymbol{I} \equiv \boldsymbol{I} \pmod{n}$$

και

$$(D^{-1}\,\mathrm{adj}\boldsymbol{A})\cdot\boldsymbol{A} \equiv D^{-1}\,\mathrm{adj}\boldsymbol{A}\cdot\boldsymbol{A} \equiv D^{-1}D\boldsymbol{I} \equiv \boldsymbol{I} \pmod{n}.\_$$

Μπορούμε τώρα να χρησιμοποιήσουμε έναν αντίστροφο του πίνακα $\boldsymbol{A}$ modulo n, προκειμένου να λύσουμε το σύστημα

$$\boldsymbol{AX} \equiv \boldsymbol{B} \pmod{n},$$

όπου $\gcd(\det\boldsymbol{A}, n) = 1$. Εφαρμόζοντας το Θεώρημα 2.22 παίρνουμε διαδοχικά,

$$\boldsymbol{A}^{-1}(\boldsymbol{AX}) \equiv \boldsymbol{A}^{-1}\boldsymbol{B} \pmod{n},$$

$$(\boldsymbol{A}^{-1}\boldsymbol{A})\boldsymbol{X} \equiv \boldsymbol{A}^{-1}\boldsymbol{B} \pmod{n},$$

$$\boldsymbol{IX} \equiv \boldsymbol{A}^{-1}\boldsymbol{B} \pmod{n},$$

$$\boldsymbol{X} \equiv \boldsymbol{A}^{-1}\boldsymbol{B} \pmod{n}.$$

Βρίσκουμε δηλαδή τη λύση $\boldsymbol{X}$ υπολογίζοντας τον πίνακα $\boldsymbol{A}^{-1}\boldsymbol{B}$ modulo n.

ΠΑΡΑΔΕΙΓΜΑ 2.7 – Έστω το σύστημα των τριών ισοδυναμιών

$$2x_1 + 5x_2 + 6x_3 \equiv 3 \pmod 7$$
$$2x_1 + x_3 \equiv 4 \pmod 7$$
$$x_1 + 2x_2 + 3x_3 \equiv 1 \pmod 7$$

το οποίο υπό μορφή πινάκων γράφεται

$$\begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} \pmod 7.$$

Υπολογίζουμε την ορίζουσα του πίνακα $\boldsymbol{A} = \begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ και βρίσκουμε $\det\boldsymbol{A} = -5$.

Επειδή $\gcd(\det\boldsymbol{A}, 7) = 1$ και $(-5)^{-1} \equiv 4 \pmod 7$, γιατί $(-5)4 = -20 \equiv 1 \pmod 7$, υπάρχει αντίστροφος του $\boldsymbol{A}$ modulo n, και βρίσκουμε ότι

$$\boldsymbol{A}^{-1} = 4\,\mathrm{adj}\boldsymbol{A} = 4\begin{pmatrix} -2 & -3 & 5 \\ -5 & 0 & 10 \\ 4 & 1 & -10 \end{pmatrix} = \begin{pmatrix} -8 & -12 & 20 \\ -20 & 0 & 40 \\ 16 & 4 & -40 \end{pmatrix} \equiv \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix} \pmod 7.$$

Έτσι, έχουμε

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix}\begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 32 \\ 8 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \pmod 7.$$

Τελειώνοντας, θα πρέπει να πούμε ότι πολλές από τις μεθόδους επίλυσης συστημάτων γραμμικών εξισώσεων μπορούν να προσαρμοστούν για τη λύση συστημάτων ισοτιμιών. Για παράδειγμα, η μέθοδος απαλοιφής Gauss μπορεί να προσαρμοστεί στην περίπτωση των γραμμικών ισοδυναμιών, όπου η διαίρεση πρέπει να αντικαθίσταται πάντα με πολλαπλασιασμό με αντίστροφους modulo n.

2.7. Δυνάμεις στο $\boldsymbol{Z}_n^*$

Συχνά έχουμε να κάνουμε με τις δυνάμεις ενός στοιχείου a, modulo n, όπου $a \in \boldsymbol{Z}_n^*$. Αν παρατηρήσουμε την ακολουθία δυνάμεων $a^k \bmod n$ θα διαπιστώσουμε ότι συχνά για κάποια τιμή, έστω m, του k έχουμε, $a^m \equiv 1 \pmod n$. Αυτό το γεγονός είναι αρκετά σημαντικό γιατί δηλώνει μια περιοδικότητα στη δομή της ακολουθίας, δηλαδή $a^{m+l} \equiv a^m a^l \equiv a^l \pmod n$. Για παράδειγμα, μερικοί όροι της ακολουθίας δυνάμεων $7^k \bmod 10$ είναι,

$7^0 \equiv 1 \pmod{10}$

$7^1 \equiv 7 \pmod{10}$

$7^2 = 49 \equiv 9 \pmod{10}$

$7^3 = 7^2 \cdot 7 \equiv 9 \cdot 7 \equiv 3 \pmod{10}$

$7^4 = 7^3 \cdot 7 \equiv 3 \cdot 7 \equiv 1 \pmod{10}$

$7^5 = 7^4 \cdot 7 \equiv 1 \cdot 7 \equiv 7 \pmod{10}$

$7^6 = 7^4 \cdot 7^2 \equiv 1 \cdot 49 \equiv 9 \pmod{10}$

$\vdots$

δηλαδή τα υπόλοιπα $7^k \bmod 10$ επαναλαμβάνονται με μια περίοδο ίση με 4, παίρνοντας τις τιμές 1, 7, 9 και 3. Αν τώρα αντί για δυνάμεις του 7 υπολογίζαμε τις δυνάμεις του $a = 2$, δεν θα βρίσκαμε ποτέ $2^k \equiv 1 \pmod{10}$ αφού ο 2^k είναι άρτιος. Παρ' όλα αυτά, αν μελετήσουμε τις τιμές του $2^k \bmod 10$, για $k \geq 1$ παρατηρούμε

ότι και εδώ τελικά τα υπόλοιπα επαναλαμβάνονται με μια περίοδο ίση με 4, παίρνοντας τις τιμές 2, 4, 8 και 6:

$2^1 \equiv 2 \pmod{10}$

$2^2 \equiv 4 \pmod{10}$

$2^3 \equiv 8 \pmod{10}$

$2^4 \equiv 6 \pmod{10}$

$2^5 \equiv 2 \pmod{10}$

$2^6 \equiv 4 \pmod{10}$

$\vdots$

Παρατηρούμε λοιπόν μια δομή στη μορφή του $a^k \bmod n$, η οποία όπως θα δούμε στη συνέχεια έχει να κάνει με τον αριθμό $\phi(n)$, όπου ϕ είναι η συνάρτηση του Euler.

Έστω $\langle a \rangle$ η υποομάδα της ομάδας $\boldsymbol{Z}_n^*$ που δημιουργείται από το a και $\mathrm{ord}_n(a)$ η τάξη του a, modulo n, στο $\boldsymbol{Z}_n^*$. Για παράδειγμα, $\langle 7 \rangle = \{1, 3, 7, 9\}$ και $\mathrm{ord}_{10}(7) = 4$, στο $\boldsymbol{Z}_{10}^*$. Χρησιμοποιώντας τον ορισμό της συνάρτησης ϕ του Euler (βλ. § 2.3) και τον συμβολισμό του $\boldsymbol{Z}_n^*$ μπορούμε να γράψουμε το θεώρημα του Euler ως άμεση συνέπεια του Πορίσματος 2.6 και να το εξειδικεύσουμε στο $\boldsymbol{Z}_p^*$, όπου p πρώτος, προκειμένου να καταλήξουμε στο θεώρημα του Fermat:

ΘΕΩΡΗΜΑ 2.25 (Euler) – Για οποιονδήποτε ακέραιο $n > 1$,

$a^{\phi(n)} \equiv 1 \pmod{n}, \ \forall\, a \in \boldsymbol{Z}_n^*$.

ΘΕΩΡΗΜΑ 2.26 (Fermat) – Αν p είναι πρώτος, τότε

$a^{p-1} \equiv 1 \pmod{p}, \ \forall\, a \in \boldsymbol{Z}_p^*$.

Το θεώρημα αυτό εφαρμόζεται σε κάθε στοιχείο του $\boldsymbol{Z_p}$ εκτός του 0, γιατί $0 \notin \boldsymbol{Z}_p^*$. Πάντως, αν p είναι πρώτος, τότε $a^p \equiv a \pmod{p}, \ \forall\, a \in \boldsymbol{Z_p}$.

Μια χρήσιμη εφαρμογή του Θεωρήματος του Euler (χρησιμοποιείται στην απόδειξη ορθότητας του αλγόριθμου RSA) είναι η ακόλουθη.

- Δοθέντων δύο πρώτων p και q και των ακεραίων $n = pq$ και m, με $0 < m < n$, ισχύει η ακόλουθη σχέση

$$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \pmod{n}.$$

Πράγματι, αν $\gcd(m, n) = 1$, τότε από το Θεώρημα 2.25 θα είναι $m^{\phi(n)} \equiv 1 \pmod{n}$ ή $m^{\phi(n)+1} \equiv m \pmod{n}$. Έστω τώρα, $\gcd(m, n) \neq 1$. Επειδή $n = pq$ αυτό σημαίνει ότι

ο m είναι πολλαπλάσιο του p ή πολλαπλάσιο του q. Ας θεωρήσουμε ότι $m = kp$ για κάποιο θετικό ακέραιο k. Σ' αυτήν την περίπτωση θα πρέπει να έχουμε $\gcd(m, q) = 1$ γιατί διαφορετικά θα έχουμε, m πολλαπλάσιο του p και m πολλαπλάσιο του q και επιπλέον $m < pq$. Αν λοιπόν $\gcd(m, q) = 1$, τότε εφαρμόζεται το Θεώρημα του Euler οπότε

$$m^{\phi(q)} \equiv 1 \pmod{q}$$

Αλλά τότε, με βάση τους κανόνες της modular αριθμητικής,

$$(m^{\phi(q)})^{\phi(p)} \equiv 1 \pmod{q}, \text{ ή}$$

$$m^{\phi(n)} \equiv 1 \pmod{q}.$$

Επομένως, υπάρχει ακέραιος l τέτοιος ώστε

$$m^{\phi(n)} = 1 + lq$$

οπότε πολλαπλασιάζοντας και τα δύο μέλη με $m = kp$, παίρνουμε

$$\begin{aligned} m^{\phi(n)+1} &= m + lkpq \\ &= m + lkn \end{aligned}$$

δηλαδή

$$m^{\phi(n)+1} \equiv m \pmod{n}.$$

Παρόμοια είναι η περίπτωση $m = kq$._

Στην περίπτωση που για κάποιο $g \in \boldsymbol{Z}_n^*$ είναι $\text{ord}_n(g) = |\boldsymbol{Z}_n^*|$, τότε κάθε στοιχείο του $\boldsymbol{Z}_n^*$ είναι μια δύναμη του g, modulo n και όπως ξέρουμε το g είναι ένας γεννήτορας του $\boldsymbol{Z}_n^*$. Επίσης σ' αυτήν την περίπτωση συνήθως λέμε ότι το g είναι μια ***πρωτεύουσα ρίζα*** (primitive root) του $\boldsymbol{Z}_n^*$.

ΠΑΡΑΔΕΙΓΜΑ 2.8 – Οι δυνάμεις του 3 modulo 7 είναι

k	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$3^k \bmod 7$	1	3	2	6	4	5	1	3	2	6	4	5	1	...

ενώ οι δυνάμεις του 2 modulo 7 είναι

k	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$2^k \bmod 7$	1	2	4	1	2	4	1	2	4	1	2	4	1	...

και είναι $\langle 3\rangle = \{1, 2, 3, 4, 5, 6\} = \boldsymbol{Z}_7^*$, $\langle 2\rangle = \{1, 2, 4\}$. Έτσι, ο 3 είναι μια πρωτεύουσα ρίζα, modulo 7, ενώ ο 2 δεν είναι πρωτεύουσα ρίζα, modulo 7.

Αν το $\boldsymbol{Z}_n^*$ περιέχει μια πρωτεύουσα ρίζα, τότε λέμε ότι η ομάδα $\boldsymbol{Z}_n^*$ είναι ***κυκλική*** και ισχύει το ακόλουθο θεώρημα, το οποίο απλά το αναφέρουμε.

ΘΕΩΡΗΜΑ 2.27 – Οι τιμές του $n > 1$ για τις οποίες το $\boldsymbol{Z}_n^*$ είναι κυκλική ομάδα είναι 2, 4, p^e και $2p^e$, για όλους τους πρώτους $p > 2$ και όλους τους θετικούς ακέραιους e.

Αν g είναι μια πρωτεύουσα ρίζα του $\boldsymbol{Z}_n^*$ και a ένα οποιοδήποτε στοιχείο του, τότε υπάρχει ένα z τέτοιο ώστε $g^z \equiv a \pmod n$. Αυτό το z λέγεται ***διακριτός λογάριθμος*** (discrete logarithm) ή ***δείκτης*** (index) του a, modulo n, ως προς τη βάση g, και το συμβολίζουμε ως $\text{ind}_{n,g}$. Για παράδειγμα, για την ισοδυναμία $2^z \equiv 3 \pmod{13}$ έχουμε την ακόλουθη ακολουθία:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10,$$

$$2^{11} \equiv 7,\ 2^{12} \equiv 1 \pmod{13}$$

οπότε $z = 4$.

Σχετικό είναι το ακόλουθο θεώρημα που είναι γνωστό ως το ***θεώρημα διακριτού λογάριθμου***.

ΘΕΩΡΗΜΑ 2.28 – Αν g είναι μια πρωτεύουσα ρίζα του $\boldsymbol{Z}_n^*$, τότε η σχέση $g^x \equiv g^y \pmod n$ ισχύει αν και μόνον αν ισχύει η σχέση $x \equiv y \pmod{\phi(n)}$.

Απόδειξη Έστω ότι $x \equiv y \pmod{\phi(n)}$. Τότε, $x = y + k\phi(n)$ όπου k ακέραιος. Επομένως,

$$\begin{aligned} g^x &\equiv g^{y+k\phi(n)} \pmod n \\ &\equiv g^y \cdot (g^{\phi(n)})^k \pmod n \\ &\equiv g^y \cdot (1)^k \pmod n \\ &\equiv g^y \pmod n. \end{aligned}$$

Έστω τώρα ότι $g^x \equiv g^y \pmod n$. Επειδή κάθε στοιχείο του $\langle g\rangle$ είναι μια δύναμη του g και $|\langle g\rangle| = \phi(n)$, από το Πόρισμα 2.5 συνεπάγεται ότι η ακολουθία δυνάμεων του g είναι περιοδική με περίοδο $\phi(n)$. Επομένως, αν $g^x \equiv g^y \pmod n$, τότε θα πρέπει να είναι $x \equiv y \pmod{\phi(n)}$. ∎

ΘΕΩΡΗΜΑ 2.29– Αν p είναι ένας περιττός πρώτος και $e \geq 1$, τότε η εξίσωση

$$x^2 \equiv 1 \pmod{p^e} \tag{2.30}$$

έχει δύο μόνο λύσεις, τις $x = 1$ και $x = -1$.

Απόδειξη Έστω $n = p^e$. Από το Θεώρημα 2.27 έχουμε ότι το $\boldsymbol{Z}_n^*$ έχει μια πρωτεύουσα ρίζα g η δε εξίσωση (2.30) μπορεί να γραφεί

$$\left(g^{\mathrm{ind}_{n,g}(x)}\right)^2 \equiv g^{\mathrm{ind}_{n,g}(1)} \pmod{n}. \tag{2.31}$$

Επειδή όμως $\mathrm{ind}_{n,g}(1) = 0$, από το θεώρημα διακριτού λογάριθμου έχουμε ότι η εξίσωση (2.31) είναι ισοδύναμη με την

$$2\cdot\mathrm{ind}_{n,g}(x) \equiv 0 \pmod{\phi(n)}. \tag{2.32}$$

Για να λύσουμε την εξίσωση (2.32) ως προς $\mathrm{ind}_{n,g}(x)$, εφαρμόζουμε τις μεθόδους της § 2.4. Από την (2.20) έχουμε $\phi(n) = p^e(1 - 1/p) = p^{e-1}(p - 1)$. Θέτοντας $d = \gcd(2, \phi(n)) = \gcd(2, p^{e-1}(p - 1)) = 2$ και σημειώνοντας ότι $d \mid 0$, από το Θεώρημα 2.19 βρίσκουμε ότι η (2.32) έχει ακριβώς $d = 2$ λύσεις. Επομένως, επειδή η εξίσωση (2.30) έχει προφανείς λύσεις τις $x = 1$ και $x = -1$, αυτές θα είναι και οι μοναδικές._

Από την παραπάνω απόδειξη μπορούμε να δούμε ότι το να παίρνουμε διακριτούς λογάριθμους μπορεί μερικές φορές να απλοποιεί τους συλλογισμούς μας κατά τη λύση modular εξισώσεων.

ΟΡΙΣΜΟΣ 2.14 – Ο αριθμός x είναι μια ***μη τετριμμένη τετραγωνική ρίζα του 1***, αν ικανοποιεί την εξίσωση $x^2 \equiv 1 \pmod{n}$ και δεν είναι ισοδύναμος με καμιά από τις δύο τετριμμένες τετραγωνικές ρίζες: 1 ή –1, modulo n.

Για παράδειγμα, ο 6 είναι μια μη τετριμμένη τετραγωνική ρίζα του 1, modulo 35. Σχετικό είναι και το ακόλουθο πόρισμα του τελευταίου θεωρήματος.

ΠΟΡΙΣΜΑ 2.12 – Αν υπάρχει μια μη τετριμμένη τετραγωνική ρίζα του 1, modulo n, τότε ο n είναι σύνθετος.

Πράγματι, με αντιθετοαντιστροφή στο Θεώρημα 2.29, αν υπάρχει μια μη τετριμμένη τετραγωνική ρίζα του 1, modulo n, τότε ο n δεν μπορεί να είναι ένας περιττός πρώτος ή μια δύναμη ενός περιττού πρώτου. Αν $x^2 \equiv 1 \pmod 2$, τότε $x \equiv 1 \pmod 2$ και έτσι όλες οι τετραγωνικές ρίζες του 1, modulo 2, είναι τετριμμένες. Επομένως, ο n δεν μπορεί να είναι πρώτος. Τελικά πρέπει να έχουμε $n > 1$ για να υπάρχει μια μη τετριμμένη τετραγωνική ρίζα του 1. Άρα, ο n πρέπει να είναι σύνθετος.

2.7.1. Modular εκθετοποίηση

Στην κρυπτογραφία (και όχι μόνον) συχνά έχουμε να υπολογίσουμε μια δύναμη a^e ή μια modular δύναμη $a^e \bmod n$. Πριν δούμε πως αντιμετωπίζεται αποτελεσματικά αυτό το πρόβλημα ας δούμε ορισμένα παραδείγματα. Πέστε ότι για κάποιο λόγο έχουμε να υπολογίσουμε το

$$5^{100000000000000} \bmod 12830603.$$

Αν ο 12830603 ήταν πρώτος, θα προσπαθούσαμε να χρησιμοποιήσουμε το Θεώρημα 2.26 (Fermat) και στην περίπτωση που δεν είναι πρώτος έχουμε στη διάθεσή μας το Θεώρημα2.25 (Euler). Όντως προκύπτει ότι

$$12830603 = 3571 \cdot 3593 \text{ και}$$

$$\phi(12830603) = \phi(3571)\phi(3593) = 3570 \cdot 3592 = 12823440.$$

Το Θεώρημα του Euler μας λέει ότι $a^{\phi(n)} \equiv 1 \pmod{n}$ για οποιουσδήποτε a και n με $\gcd(a, n) = 1$, οπότε μπορούμε να χρησιμοποιήσουμε το γεγονός ότι

$$100000000000000 = 7798219 \cdot 12823440 + 6546640$$

για να ‘‘απλοποιήσουμε’’ το πρόβλημά μας, γράφοντας

$$5^{100000000000000} = (5^{12823440})^{7798219} \cdot 5^{6546640}$$
$$\equiv 5^{6546640} \pmod{12830603}.$$

Μας μένει τώρα να υπολογίσουμε την 6546640^{η} δύναμη του 5 και στη συνέχεια να την κάνουμε αναγωγή modulo 12830603. Συμβαίνει όμως ο αριθμός $5^{6546640}$ να έχει περισσότερα από 4 εκατομμύρια ψηφία και θα ήταν δύσκολο να τον υπολογίσουμε και με τη χρήση ενός υπολογιστή. Και να λάβει κανείς υπόψη ότι θα θελήσουμε κάποια στιγμή να υπολογίσουμε δυνάμεις της μορφής $a^e \bmod n$ για ακέραιους a, e και n οι οποίοι έχουν εκατοντάδες ψηφία! Χρειαζόμαστε μια αποτελεσματικότερη μέθοδο. Πριν την περιγράψουμε στη γενική της μορφή, ας τη δούμε σε ένα παράδειγμα. Πέστε ότι θέλουμε να υπολογίσουμε το

$$7^{327} \bmod 853.$$

Το πρώτο που κάνουμε είναι να δημιουργήσουμε έναν πίνακα με τις τιμές 7, 7^2, 7^4, 7^8, 7^{16}, …, modulo 853. Να παρατηρήσουμε ότι για την επόμενη τιμή χρειάζεται απλά να τετραγωνίζουμε την προηγούμενη και επιπλέον, επειδή πάντα κάνουμε αναγωγή modulo 853 πριν τετραγωνίσουμε, ποτέ δεν θα χρειαστεί να δουλέψουμε με ακέραιους μεγαλύτερους από 852^2. Ο πίνακας των 2^k-δυνάμεων του 7 modulo 853, είναι

7^1			$\equiv 7$	$\equiv 7 \pmod{853}$
7^2	$\equiv (7^1)^2$	$\equiv 7^2$	$\equiv 49$	$\equiv 49 \pmod{853}$
7^4	$\equiv (7^2)^2$	$\equiv 49^2$	$\equiv 2401$	$\equiv 695 \pmod{853}$
7^8	$\equiv (7^4)^2$	$\equiv 695^2$	$\equiv 483025$	$\equiv 227 \pmod{853}$
7^{16}	$\equiv (7^8)^2$	$\equiv 227^2$	$\equiv 51529$	$\equiv 349 \pmod{853}$
7^{32}	$\equiv (7^{16})^2$	$\equiv 349^2$	$\equiv 121801$	$\equiv 675 \pmod{853}$
7^{64}	$\equiv (7^{32})^2$	$\equiv 675^2$	$\equiv 455625$	$\equiv 123 \pmod{853}$

$7^{128} \equiv (7^{64})^2 \equiv 123^2 \equiv 15129 \equiv 628 \pmod{853}$

$7^{256} \equiv (7^{128})^2 \equiv 628^2 \equiv 394384 \equiv 298 \pmod{853}$

Στη συνέχεια γράφουμε τον εκθέτη 327 ως άθροισμα δυνάμεων του 2 (δυαδικό ανάπτυγμα)

$327 = 256 + 64 + 4 + 2 + 1$

και υπολογίζουμε

$7^{327} = 7^{256+64+4+2+1} = 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7^1$

$\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \pmod{853}.$

Προκειμένου τώρα να πολλαπλασιάσουμε τους πέντε ακέραιους που προέκυψαν μπορούμε να πολλαπλασιάσουμε τους δύο πρώτους, να κάνουμε στη συνέχεια αναγωγή modulo 853, μετά να πολλαπλασιάσουμε με τον τρίτο, αναγωγή πάλι modulo 853 κτλ. Με αυτόν τον τρόπο πάλι δεν θα χρειαστεί να δουλέψουμε με ακέραιο μεγαλύτερο του 852^2. Έτσι

$$298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \equiv 828 \cdot 695 \cdot 49 \cdot 7 \equiv 538 \cdot 49 \cdot 7 \equiv 772 \cdot 7$$

$$\equiv 286 \pmod{853}.\_$$

Στη μελέτη αλγορίθμων με ακέραιους στην είσοδο και στην έξοδο, χρειαζόμαστε τις ***δυαδικές κωδικοποιήσεις*** (binary encodings) των ακεραίων (και των κατάλοιπων). Υποθέτουμε πάντοτε ότι οι ακέραιοι $n \geq 0$ κωδικοποιούνται στον στάνταρ τρόπο ως μη προσημασμένοι ακέραιοι:
Η ακολουθία $b_{k-1}b_{k-2}\ldots b_1b_0$ των bits $b_i \in \{0, 1\}$, $0 \leq i \leq k-1$, είναι η κωδικοποίηση του

$$n = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \ldots + b_{k-2} \cdot 2^{k-2} + b_{k-1} \cdot 2^{k-1} = \sum_{i=0}^{k-1} b_i \cdot 2^i \ .$$

Αν το πρώτο ψηφίο b_{k-1} δεν είναι μηδέν, δηλ. $b_{k-1} = 1$, καλούμε τον n ως k-bit ακέραιο και το k καλείται ***δυαδικό μήκος*** (bit length) του k, συμβολικά $|n|$ (αν δεν υπάρχει κίνδυνος σύγχυσης με την απόλυτη τιμή). Το δυαδικό μήκος του $n \in \boldsymbol{N}^*$ είναι, ως γνωστόν, $\lfloor \log_2 n \rfloor + 1$ και οι ακέραιοι δυαδικού μήκους k είναι οι αριθμοί $n \in \boldsymbol{N}^*$ με $2^{k-1} \leq n \leq 2^k - 1$.

Ο αποτελεσματικός υπολογισμός μιας δύναμης a^e ή μιας modular δύναμης $a^e \bmod n$, όπου a και e είναι μη αρνητικοί ακέραιοι και n θετικός ακέραιος, μπορεί να γίνει με τη μέθοδο του ***επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού***. Στηρίζεται στην εξής ιδέα. Αν ο εκθέτης e είναι μια δύναμη του 2, ας πούμε $e = 2^k$, τότε μπορούμε να ‘‘εκθετοποιήσουμε’’ με διαδοχικούς τετραγωνισμούς:

$$a^e = a^{2^k} = \left(\left(\left(\left(\ldots\left(a^2\right)^2\right)^2\ldots\right)^2\right)^2\right)^2.$$

Με αυτόν τον τρόπο υπολογίζουμε τον a^e, όπου $e = 2^k$, με k τετραγωνισμούς. Για παράδειγμα,

$$a^{16} = \left(\left(\left(a^2\right)^2\right)^2\right)^2.$$

Αν ο εκθέτης δεν είναι δύναμη του 2, τότε χρησιμοποιούμε τη δυαδική του αναπαράσταση. Έστω ότι ο e είναι ένας k-bit ακέραιος, $2^{k-1} \le e \le 2^k - 1$. Τότε

$$\begin{aligned} e &= 2^{k-1}e_{k-1} + 2^{k-2}e_{k-2} + \ldots + 2^1 e_1 + 2^0 e_0, \quad (\text{με } e_{k-1} = 1) \\ &= \left(2^{k-2}e_{k-1} + 2^{k-3}e_{k-2} + \ldots + e_1\right)\cdot 2 + e_0 \\ &= \left(\ldots\left(\left(2e_{k-1} + e_{k-2}\right)\cdot 2 + e_{k-3}\right)\cdot 2 + \ldots + e_1\right)\cdot 2 + e_0. \end{aligned}$$

Έτσι,

$$\begin{aligned} a^e &= a^{\left(\ldots\left(\left(2e_{k-1}+e_{k-2}\right)\cdot 2+e_{k-3}\right)\cdot 2+\ldots e_1\right)\cdot 2+e_0} \\ &= \left(a^{\left(\ldots\left(\left(2e_{k-1}+e_{k-2}\right)\cdot 2+e_{k-3}\right)\cdot 2+\ldots e_1\right)}\right)^2 \cdot a^{e_0} \\ &= \left(\ldots\left(\left(\left(a^2 \cdot a^{e_{k-2}}\right)^2 \cdot a^{e_{k-3}}\right)^2 \cdot \ldots\right)^2 \cdot a^{e_1}\right)^2 \cdot a^{e_0}. \end{aligned}$$

Βλέπουμε ότι ο a^e μπορεί να υπολογιστεί σε $k - 1$ βήματα, όπου κάθε βήμα συνίσταται σε τετραγωνισμό του ενδιάμεσου αποτελέσματος και, αν το αντίστοιχο ψηφίο e_i του e (= Bit(e, i)) είναι 1, σε έναν επιπλέον πολλαπλασιασμό με a. Αν τώρα θέλουμε να υπολογίσουμε την modular δύναμη $a^e \bmod n$, τότε παίρνουμε το υπόλοιπο modulo n μετά από κάθε τετραγωνισμό και πολλαπλασιασμό:

$$\begin{aligned} a^e \bmod n = \\ = \left(\ldots\left(\left(\left(a^2 \cdot a^{e_{k-2}} \bmod n\right)^2 \cdot a^{e_{k-3}} \bmod n\right)^2 \cdot \ldots\right)^2 \cdot a^{e_1} \bmod n\right)^2 \cdot a^{e_0} \bmod n. \end{aligned}$$

Σύμφωνα με τα παραπάνω, έχουμε τον ακόλουθο αλγόριθμο για αποτελεσματική modular εκθετοποίηση.

ModΔυναμη(a, e, n)

```
1  b ← a
2  for i ← BitLength(e) – 2 downto 0 do
3      b ← b^2 · a^Bit(e, i) mod n
4  return b
```

Τελειώνοντας να πούμε ότι επειδή το δυαδικό μήκος k του e είναι $\lfloor \log_2 e \rfloor + 1$, ο υπολογισμός του $a^e \bmod n$ μπορεί να γίνει με m τετραγωνισμούς, m πολλαπλασιασμούς και m διαιρέσεις, όπου $m = \lfloor \log_2 e \rfloor$.

Όροι-κλειδιά του κεφαλαίου

- πρώτος – σύνθετος
- κατάλοιπο
- αναγωγή modulo n
- κλάση κατάλοιπου modulo n
- μέγιστος κοινός διαιρέτης
- σχετικά πρώτοι
- αλγόριθμος του Ευκλείδη
- ομάδα, δακτύλιος, σώμα
- τάξη πεπερασμένης ομάδας
- συνάρτηση του Euler
- γεννήτορας υποομάδας
- τάξη στοιχείου ομάδας
- χαρακτηριστική δακτυλίου
- ομομορφισμός – ισομορφισμός
- πεπερασμένο σώμα
- ανάγωγο πολυώνυμο
- κυκλική ομάδα
- πρωτεύουσα ρίζα
- διακριτός λογάριθμος
- μέθοδος επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού

2.8. Ασκήσεις

1. Δείξτε ότι gcd(12345, 11111) = 1 και βρείτε τους ακέραιους x και y για τους οποίους είναι $12345x + 11111y = 1$. Ποιος είναι ο $11111^{-1} \pmod{12345}$;

2. Κάντε τους πίνακες για την πρόσθεση και τον πολλαπλασιασμό ακεραίων, modulo 6 και βρείτε τους αντίθετους και αντίστροφους (όσοι υπάρχουν), modulo 6.

3. Λύστε τις εξισώσεις:

i) $5x + 6 \equiv 13 \pmod{11}$

ii) $11111x \equiv 4 \pmod{12345}$

iii) $x^2 \equiv 1 \pmod{35}$

4. Βρείτε τον αντίστροφο, modulo 11, του πίνακα

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix}$$

5. Έστω ότι $x \equiv 17 \pmod{101}$, $x \equiv 18 \pmod{201}$και $x \equiv 19 \pmod{301}$. Βρείτε τον x.

6. i) Έστω $p = 7, 13$ ή 19. Δείξτε ότι $a^{1728} \equiv 1 \pmod{p}$ για όλους τους a με $p \nmid a$.

ii) Έστω $p = 7, 13$ ή 19. Δείξτε ότι $a^{1728} \equiv a \pmod{p}$ για όλους τους a.

iii) Δείξτε ότι $a^{1729} \equiv a \pmod{1729}$ για όλους τους a.

7. i) Δείξτε ότι τα μόνα ανάγωγα πολυώνυμα στο $\boldsymbol{Z}_2[x]$ βαθμού το πολύ 2, είναι τα x, $x + 1$ και $x^2 + x + 1$.

ii) Δείξτε ότι το $x^4 + x + 1$ είναι ανάγωγο στο $\boldsymbol{Z}_2[x]$

iii) Δείξτε ότι $x^4 \equiv x + 1$, $x^8 \equiv x^2 + 1$ και $x^{16} \equiv x \pmod{x^4 + x + 1}$.