Ασκήσεις (6)

Άσκηση 1

Βρείτε τον gcd(12453, 2347) και τους ακεραίους x και y για τους οποίους είναι

$$12453\,x + 2347y = \gcd(12453, 2347)$$

Λύση

Στην αριστερή στήλη είναι ο αλγόριθμος του Ευκλείδη για τους ακέραιους $a = 12453$, $b = 2347$, και στη δεξιά στήλη η λύση της εξίσωσης $a\,x + by = \gcd(a, b)$:

$a = 5 \times b + 718$	$718 = a - 5b$
$b = 3 \times 718 + 193$	$193 = b - 3 \times 718 = b - 3 \times (a - 5b)$
	$= -3a + 16b$
$718 = 3 \times 193 + 139$	$139 = 718 - 3 \times 193 = (a - 5b) - 3 \times (-3a + 16\,b)$
	$= 10a - 53b$
$193 = 1 \times 139 + 54$	$54 = 193 - 139 = (-3a + 16b) - (10a - 53b)$
	$= -13a + 69b$
$139 = 2 \times 54 + 31$	$31 = 139 - 2 \times 54 = (10a - 53b) - 2 \times (-13a + 69b)$
	$= 36a - 191b$
$54 = 1 \times 31 + 23$	$23 = 54 - 31 = -13a + 69b - (36a - 191b)$
	$= -49a + 260b$
$31 = 1 \times 23 + 8$	$8 = 31 - 23 = 36a - 191b - (49a + 260b)$
	$= 85a - 451b$
$23 = 2 \times 8 + 7$	$7 = 23 - 2 \times 8 = (49a + 260b) - 2 \times (85a - 451b)$
	$= -219a + 1162b$
$8 = 1 \times 7 + 1$	$1 = 8 - 7 = 85a - 451b - (-219a + 1162b)$
	$= 304a - 1613b$
$7 = 7 \times 1 + 0$	

Οπότε, gcd(12453, 2347) = 1 και η εξίσωση $12453x + 2347y = 1$ έχει τη λύση

$$(x, y) = (304, -1613).$$

2ος τρόπος:

Μπορούμε να εκτελέσουμε τον διευρυμένο Ευκλείδειο αλγόριθμο χρησιμοποιώντας τις γνωστές σχέσεις

$r_{i+1} = r_{i-1} - r_i q_i$, με $r_0 = 12453$, $r_1 = 2347$,
$s_{i+1} = s_{i-1} - s_i q_i$, με $s_0 = 1$, $s_1 = 0$,
$t_{i+1} = t_{i-1} - t_i q_i$, με $t_0 = 0$, $t_1 = 1$

και τον σχετικό πίνακα καταγραφής των βημάτων του αλγορίθμου, οπότε βρίσκουμε

i	0	1	2	3	4	5	6	7	8	9	10	
r_i	12453	2347	718	193	139	54	31	23	8	7	1	0
q_i		5	3	3	1	2	1	1	2	1	7	1
s_i	1	0	1	–3	10	–13	36	–49	85	–219	304	
t_i	0	1	–5	16	–53	69	–191	260	–451	1162	–1613	

Είναι,

gcd(12453, 2347) = 1 και $(x, y) = (s_{10}, t_{10}) = (304, -1613)$.

Άσκηση 2

Δείξτε ότι αν $a \equiv b \pmod{n_1}$ και $a \equiv c \pmod{n_2}$, τότε $b \equiv c \pmod{n}$, όπου $n = \gcd(n_1, n_2)$.

Λύση

Έχουμε:

$$a \equiv b \pmod{n_1} \Rightarrow n_1 \mid (a - b)$$

$$n = \gcd(n_1, n_2). \Rightarrow n \mid n_1$$

επομένως

$$n \mid (a - b).$$

Ομοίως

$$n \mid (a - c).$$

Συνεπώς

$$n \mid (a - b) - (a - c) \text{ ή } n \mid (c - b) \text{ δηλαδή, } c \equiv b \pmod{n} \text{ ή } b \equiv c \pmod{n}.$$

Άσκηση 3

Έστω $x, y, n \in \mathbb{Z}$, με $n > 0$ και $x \equiv y \pmod{n}$. Επίσης, έστω $a_0, a_1, \ldots, a_k \in \mathbb{Z}$. Δείξτε ότι $a_0 + a_1x + \cdots + a_kx^k \equiv a_0 + a_1y + \cdots + a_ky^k \pmod{n}$.

Λύση

Από την $x \equiv y \pmod{n}$ συνεπάγεται ότι

$$x^2 \equiv y^2 \pmod{n}, x^3 \equiv y^3 \pmod{n}, \ldots, x^k \equiv y^k \pmod{n} \quad \text{(βλ. και Άσκηση 5.4(ii))}$$

και

$$a_1x \equiv a_1y \pmod{n}, a_2x^2 \equiv a_2y^2 \pmod{n}, a_3x^3 \equiv a_3y^3 \pmod{n}, \ldots, a_kx^k \equiv a_ky^k \pmod{n},$$

οπότε θα είναι και

$$a_0 + a_1x + \cdots + a_kx^k \equiv a_0 + a_1y + \cdots + a_ky^k \pmod{n}.$$

Άσκηση 4

i) Αν για τους ακέραιους a, b και c ισχύει

$$c \equiv 0 \pmod{a}, c \equiv 0 \pmod{b} \text{ και } \gcd(a, b) = 1, \text{ τότε } c \equiv 0 \pmod{ab}.$$

ii) Αν a, b, k και n είναι ακέραιοι τέτοιοι, ώστε $k > 0$, $n > 0$ και $a \equiv b \pmod{n}$, τότε

$$a^k \equiv b^k \pmod{n}.$$

iii) Δείξτε ότι για κάθε φυσικό αριθμό n ο αριθμός $5^{2n+1} + 11^{2n+1} + 17^{2n+1}$ είναι πολ/σιο του 33.

Λύση

i)

Έχουμε:

$$c \equiv 0 \pmod{a} \Rightarrow c = ak, \ k \in \mathbb{Z}$$
$$c \equiv 0 \pmod{b} \Rightarrow c = bm, \ m \in \mathbb{Z}$$
$$\gcd(a, b) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z} : ax + by = 1$$

Επομένως,

$$c = cax + cby = bmax + akby = ab(mx + ky) = abn,\ n = (mx + ky) \in \mathbb{Z}.$$

Συνεπώς,

$$c \equiv 0 \pmod{ab}.$$

ii)

Έχουμε:

$$a \equiv b \pmod{n} \ \Rightarrow\ n \mid (a - b) \qquad (1)$$

και επειδή

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1})$$

έχουμε ότι

$$(a - b) \mid (a^k - b^k) \qquad (2)$$

Από (1) και (2) συνεπάγεται ότι

$$n \mid (a^k - b^k).$$

iii)

Έχουμε:

- $33 = 3 \times 11$ και $\gcd(3, 11) = 1$ (3)
- $5 \equiv 2 \pmod{3} \ \Rightarrow\ 5^{2n+1} \equiv 2^{2n+1} \pmod{3}$

  $11 \equiv 2 \pmod{3} \ \Rightarrow\ 11^{2n+1} \equiv 2^{2n+1} \pmod{3}$

  $17 \equiv 2 \pmod{3} \ \Rightarrow\ 17^{2n+1} \equiv 2^{2n+1} \pmod{3}$

  Επομένως

  $$5^{2n+1} + 11^{2n+1} + 17^{2n+1} \equiv 3 \times 2^{2n+1} \pmod{3} \equiv 0 \pmod{3} \qquad (4)$$

- $5 \equiv -6 \pmod{11} \ \Rightarrow\ 5^{2n+1} \equiv (-6)^{2n+1} \pmod{11}$

  $11 \equiv 0 \pmod{11} \ \Rightarrow\ 11^{2n+1} \equiv 0 \pmod{11}$

  $17 \equiv 6 \pmod{11} \ \Rightarrow\ 17^{2n+1} \equiv 6^{2n+1} \pmod{11}$

  Επομένως

  $$5^{2n+1} + 11^{2n+1} + 17^{2n+1} \equiv [(-6)^{2n+1} + 6^{2n+1}] \pmod{11} \equiv 0 \pmod{11} \qquad (5)$$

Από τις (3), (4), (5) και το (i), προκύπτει το ζητούμενο.

Άσκηση 5

Έστω $a, b, n, n' \in \mathbb{Z}$ με $n > 0$ και $n' \mid n$. Δείξτε ότι αν $a \equiv b \pmod{n}$, τότε $a \equiv b \pmod{n'}$.

Λύση

Επειδή $a \equiv b \pmod{n}$ συνεπάγεται ότι υπάρχει ακέραιος k_1 τέτοιος ώστε $a = b + k_1 n$. Επειδή $n' \mid n$, υπάρχει ακέραιος k_2 τέτοιος ώστε $n = k_2 n'$. Άρα $a = b + k_1 k_2 n'$, ή $a - b = kn'$, όπου $k = k_1 k_2 \in \mathbb{Z}$, δηλαδή $a \equiv b \pmod{n'}$.

Άσκηση 6

Έστω $a, b, n, n' \in \mathbb{Z}$ με $n > 0$, $n' > 0$ και $\gcd(n, n') = 1$. Δείξτε ότι αν $a \equiv b \pmod{n}$ και $a \equiv b \pmod{n'}$, τότε $a \equiv b \pmod{nn'}$.

Λύση

Αν $a \equiv b \pmod{n}$ τότε $a - b = k_1 n$, $k_1, \in \mathbb{Z}$, και
αν $a \equiv b \pmod{n'}$ τότε $a - b = k_2 n'$, $k_2 \in \mathbb{Z}$
οπότε, $k_1 n = a - b = k_2 n'$, απ' όπου συνεπάγεται ότι $n' \mid k_1 n$.
Τώρα, $\gcd(n, n') = 1 \Rightarrow nx + n'y = 1$, όπου $x, y \in \mathbb{Z}$. Συνεπώς, $k_1 = k_1 nx + k_1 n'y$ και αφού $n' \mid k_1 nx$ (επειδή $n' \mid k_1 n$) και $n' \mid k_1 n'y$ έχουμε ότι $n' \mid k_1$. Επομένως, $k_1 = n'm$, όπου $m \in \mathbb{Z}$, και $a - b = k_1 n = n'mn = m(n'n)$. Άρα τελικά, $a \equiv b \pmod{nn'}$.

Άσκηση 7

Έστω $a, b, n \in \mathbb{Z}$, τέτοιοι, ώστε $n > 0$ και $a \equiv b \pmod{n}$. Δείξτε ότι $\gcd(a, n) = \gcd(b, n)$.

Λύση

Έστω $\gcd(a, n) = g$ και $\gcd(b, n) = h$. Τότε $a \equiv b \pmod{n} \Rightarrow a = b + kn$, $k \in \mathbb{Z}$. Επομένως $g \mid b$ και $h \mid a$. Αφού τώρα $g \mid b$ και $g \mid n \Rightarrow g \mid h$. Επίσης αφού $h \mid a$ και $h \mid n \Rightarrow h \mid g$. Άρα τελικά $g = h$.

Άσκηση 8

Έστω a ένας θετικός ακέραιος του οποίου η αναπαράσταση στο δεκαδικό σύστημα είναι $a = (a_k\, a_{k-1} \ldots a_1 a_0)_{10}$. Έστω b το άθροισμα των δεκαδικών ψηφίων του a· δηλαδή, έστω $b := a_0 + a_1 + \ldots + a_k + a_{k-1}$. Δείξτε ότι $a \equiv b \pmod{9}$. Από αυτό, δικαιολογήστε τους γνωστούς κανόνες μνημοτεχνικής με τους οποίους προσδιορίζουμε τη διαιρετότητα με 9 και 3: ο a διαιρείται με το 9 (αντίστοιχα, 3), αν και μόνο αν το άθροισμα των δεκαδικών ψηφίων του a διαιρείται με το 9 (αντίστοιχα, 3).

Λύση

Έστω a ένας ακέραιος και $a = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10^1 + a_0 10^0$ $[= (a_k a_{k-1} \cdots a_1 a_0)_{10}]$ η αναπαράστασή του ως προς βάση το 10.
Επειδή

$$10 \equiv 1 \pmod{9} \Rightarrow 10^r \equiv 1^r \equiv 1 \pmod{9}, \text{ για } r = 1, 2, \ldots, k$$

συνεπάγεται ότι

$$a \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod{9}.$$

Επομένως

$$a \equiv 0 \pmod{9}, \text{ αν και μόνο αν } a_k + a_{k-1} + \cdots + a_1 + a_0 \equiv 0 \pmod{9}.$$

Με λόγια: ένας ακέραιος διαιρείται με το 9, αν και μόνο αν το άθροισμα των ψηφίων του διαιρείται με το 9.

Επειδή $10 \equiv 1 \pmod{3}$, καταλήγουμε παρόμοια στο κριτήριο:
Ένας ακέραιος διαιρείται με το 3, αν και μόνο αν το άθροισμα των ψηφίων του διαιρείται με το 3.

Άσκηση 9

Δείξτε ότι αν a και b είναι ακέραιοι τέτοιοι, ώστε $a \mid b$ και $b > 0$, τότε

$$(x \bmod b) \bmod a = x \bmod a$$

για κάθε $x \in \mathbb{Z}$. Δείξτε ότι κάτω από τις ίδιες προϋποθέσεις

$$x \equiv y \pmod{b} \Rightarrow x \equiv y \pmod{a}$$

για οποιουσδήποτε ακεραίους x και y.

Λύση

Κατ' αρχήν να παρατηρήσουμε ότι για κάθε $x \in \mathbb{Z}$ είναι

$$x \bmod a = (x + ka) \bmod a,\ k \in \mathbb{Z}$$

αφού $ka \bmod a = 0$.
Τώρα για κάθε $x \in \mathbb{Z}$, έχουμε

$x = bq + r$, με $q \in \mathbb{Z}$, $r = x \bmod b \Rightarrow r = x - bq = x - kaq = x - aq_1$, (αφού $a \mid b \Rightarrow b = ka$, $k \in \mathbb{Z}$)

Επομένως,

$$r \bmod a = (x \bmod b) \bmod a = (x - q_1 a) \bmod a = x \bmod a,$$

δηλαδή

$$(x \bmod b) \bmod a = x \bmod a.$$

Παρόμοια, έχουμε

$x \equiv y \pmod{b} \Rightarrow x = y + mb$, $m \in \mathbb{Z} \Rightarrow x = y + mka = y + (mk)a = y + na$, όπου $n\ (= mk) \in \mathbb{Z}$

$$\Rightarrow x - y = na \Rightarrow x \equiv y \pmod{a}.$$

Άσκηση 10

Έστω οι a, n, b ακέραιοι με $n > 0$ και έστω $d := \gcd(a, n)$. Δείξτε ότι η εξίσωση ισοτιμίας

$$az \equiv b \pmod{n}$$

έχει λύση ως προς z, αν και μόνο αν $d \mid b$;

Λύση

Έστω z ακέραιος τέτοιος, ώστε $az \equiv b \pmod{n}$. Τότε $n \mid az - b$ και επομένως υπάρχει $c \in \mathbb{Z}$ έτσι, ώστε $az - b = cn$ ή $b = az + cn$. Καθώς $d \mid a$ και $d \mid n$, προκύπτει ότι $d \mid b$.

Αντίστροφα, έστω ότι $d \mid b$. Τότε υπάρχει $k \in \mathbb{Z}$ τέτοιος, ώστε $b = kd$. Επειδή όμως $d := \gcd(a, n)$ συνεπάγεται ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι, ώστε $d = ax + ny$, οπότε $b = k(ax + ny) = kax + kny$, ή $kax - b = -kny$. Συνεπώς υπάρχει $z\ (= kx) \in \mathbb{Z}$ τέτοιος, ώστε $az - b = (ky)n$ ή $az \equiv b \pmod{n}$.

Άσκηση 11

Δείξτε ότι ο αριθμός $2222^{5555} + 5555^{2222}$ είναι πολλαπλάσιο του 7.

Λύση

Έχουμε

- $2222 \equiv 3 \pmod{7}$ και $5555 \equiv 4 \pmod{7}$
- $3^6 = 720 \equiv 1 \pmod{7}$ και $4^3 = 64 \equiv 1 \pmod{7}$

Επομένως

$$\begin{aligned} 2222^{5555} + 5555^{2222} &\equiv 3^{5555} + 4^{2222} \pmod 7 \\ &\equiv 3^5\times(3^6)^{925} + 4^2\times(4^3)^{740} \pmod 7 \\ &\equiv 3^5 + 4^2 \pmod 7 \\ &\equiv 243 + 16 \pmod 7 \\ &\equiv 259 \pmod 7 \\ &\equiv 0 \pmod 7. \end{aligned}$$

Άσκηση 12

Βρείτε τον 12453^{-1} mod 2347.

Λύση

Πρέπει να λύσουμε την εξίσωση $12453x \equiv 1 \pmod{2347}$. Είναι,

$$\begin{aligned} &12453x \equiv 1 \pmod{2347} \quad \Leftrightarrow \\ &12453x = 1 + 2347k \quad \Leftrightarrow \\ &12453x - 2347k = 1 \quad \Leftrightarrow \\ &12453x + 2347(-k) = 1 \quad \Leftrightarrow \\ &12453x + 2347y = 1. \end{aligned}$$

Από τη διαδικασία της λύσης της Άσκησης 5.1 έχουμε

$$x = 304$$

δηλαδή

$$12453^{-1} \bmod 2347 = 304.$$

(Για επαλήθευση, $12453 \times 304 = 3785712$ και το υπόλοιπο της διαίρεσης $3785712 : 2347$ είναι 1).

Άσκηση 13

Να λυθεί η εξίσωση ισοτιμίας,

i) $140x \equiv 133 \pmod{301}$.

ii) $63x \equiv 20 \pmod 7$.

Λύση

i)

Η εξίσωση είναι της μορφής $ax \equiv b \pmod n$, με $a = 140$, $n = 301$ και $b = 133$.

Αρχικά, με τον διευρυμένο αλγόριθμο του Ευκλείδη, βρίσκουμε την τριάδα ακεραίων (d, x', y') που είναι τέτοιοι, ώστε $d = ax' + ny'$, όπου $d = \gcd(a, n) = \gcd(n, a)$:

Χρησιμοποιώντας τις γνωστές σχέσεις

$r_{i+1} = r_{i-1} - r_i q_i$, με $r_0 = 301$, $r_1 = 140$,

$s_{i+1} = s_{i-1} - s_i q_i$, με $s_0 = 1$, $s_1 = 0$,
$t_{i+1} = t_{i-1} - t_i q_i$, με $t_0 = 0$, $t_1 = 1$

όπου $q_i = \lfloor r_{i-1}/r_i \rfloor$, $i = 1, 2, \ldots$, βρίσκουμε

i	0	1	2	3	4	5
r_i	301	140	21	14	7	0
q_i		2	6	1	2	
s_i	1	0	1	– 6	7	
t_i	0	1	– 2	13	– 15	

Είναι,

$$\gcd(140, 301) = \gcd(301, 140) = 7 \Rightarrow 301s + 140t = 7.$$

Άρα,

$$d = 7 \text{ και } x' = -15.$$

Επειδή 7 | 133 (δηλ. $d \mid b$), η εξίσωση δεν είναι αδύνατη και οι λύσεις της δίνονται από τον τύπο

$$x_k = (x_0 + kn/d) \bmod n, \;\; k = 0, 1, 2, \ldots, (d-1)$$

όπου x_0 μια λύση της που δίνεται από τον τύπο

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

Έτσι, αντικαθιστώντας βρίσκουμε

$$x_0 = -15(133/7) \bmod 301 = 16$$

και για

$k = 0 \Rightarrow x_0 = 16$

$k = 1 \Rightarrow x_1 = (16 + 301/7) \bmod 301 = 59$

$k = 2 \Rightarrow x_2 = (16 + 2\times301/7) \bmod 301 = 102$

$k = 3 \Rightarrow x_3 = (16 + 3\times301/7) \bmod 301 = 145$

$k = 4 \Rightarrow x_4 = (16 + 4\times301/7) \bmod 301 = 188$

$k = 5 \Rightarrow x_5 = (16 + 5\times301/7) \bmod 301 = 231$

$k = 6 \Rightarrow x_6 = (16 + 6\times301/7) \bmod 301 = 274.$

ii)

Λύση

Επειδή $\gcd(63, 7) = 7 \nmid 20$, η εξίσωση αυτή δεν έχει λύση.

Άσκηση 14

Να βρεθούν, αν υπάρχουν, οι ακέραιες λύσεις της εξίσωσης

i) $12x + 27y = 30$.

ii) $35x + 49y = 427$.

Λύση

i)

Έχουμε, για $x, y \in \mathbb{Z}$,

$$12x + 27y = 30 \Leftrightarrow 12x = 30 - 27y \Leftrightarrow 12x = 30 + 27(-y) \Leftrightarrow 12x = 30 + 27k,\ k = -y \in \mathbb{Z}$$

$$\Leftrightarrow 12x \equiv 30 \pmod{27} \qquad (1)$$

Δηλαδή αρκεί να λύσουμε τη γραμμική ισοτιμία (1) για να βρούμε, αν υπάρχουν, τους ακεραίους x και στη συνέχεια θα βρούμε τους ακεραίους y από την

$$27y = 30 - 12x.$$

Η ισοτιμία (1) είναι της μορφής $ax \equiv b \pmod{n}$, με $a = 12$, $n = 27$ και $b = 30$.

Αρχικά, με τον διευρυμένο αλγόριθμο του Ευκλείδη, βρίσκουμε την τριάδα ακεραίων (d, x', y') που είναι τέτοιοι, ώστε $d = ax' + ny'$, όπου $d = \gcd(a, n) = \gcd(n, a)$:

Χρησιμοποιώντας τις γνωστές σχέσεις

$r_{i+1} = r_{i-1} - r_i q_i$, με $r_0 = 27$, $r_1 = 12$,
$s_{i+1} = s_{i-1} - s_i q_i$, με $s_0 = 1$, $s_1 = 0$,
$t_{i+1} = t_{i-1} - t_i q_i$, με $t_0 = 0$, $t_1 = 1$

όπου $q_i = \lfloor r_{i-1}/r_i \rfloor$, $i = 1, 2, \ldots$, βρίσκουμε

i	0	1	2	3
r_i	27	12	3	0
q_i		2	4	
s_i	1	0	1	
t_i	0	1	– 2	

Είναι,

$$\gcd(12, 27) = \gcd(27, 12) = 3 \Rightarrow 27s + 12t = 3.$$

Άρα,

$$d = 3 \text{ και } x' = -2.$$

Επειδή $3 \mid 30$ (δηλ. $d \mid b$), η εξίσωση δεν είναι αδύνατη και οι λύσεις της δίνονται από τον τύπο

$$x = x_0 + m(n/d),\ \ m \in \mathbb{Z}$$

όπου x_0 μια λύση της που δίνεται από τον τύπο

$$x_0 = x'(b/d)$$

Έτσι, αντικαθιστώντας βρίσκουμε

$$x = -2(30/3) + m(27/3) \Rightarrow\ x = -20 + 9m,\ \ m \in \mathbb{Z}$$

και για τον y,

$$27y = 30 - 12x = 30 - 12(-20 + 9m) = 270 - 108m \Rightarrow y = 10 - 4m,\ m \in \mathbb{Z}.$$

ii)

Λύση

Αφήνεται στον αναγνώστη για εξάσκηση.

(απ. $x = 183 + 7m$, $y = -122 - 5m$, $m \in \mathbb{Z}$)

Άσκηση 15

Να εξετάσετε αν οι ακόλουθες ομάδες είναι κυκλικές

i) $\mathbb{Z}_{10}^*$

ii) $\mathbb{Z}_{15}^*$

Λύση

i)

Αρχικά βρίσκουμε τα στοιχεία του δοθέντος συνόλου

$$\mathbb{Z}_{10}^* = \{x \in \mathbb{Z}_{10} : \gcd(x, 10) = 1\} = \{1, 3, 7, 9\}$$

Στη συνέχεια, για να εξακριβώσουμε αν η ομάδα ($\mathbb{Z}_{10}^*$, ·), (που έχουμε συμφωνήσει να τη συμβολίζουμε απλά ως $\mathbb{Z}_{10}^*$) είναι κυκλική, βρίσκουμε αν κάποιος από τους ακέραιους $x = 3$, 7 και 9 έχει τάξη 4, όπου $4 = |\mathbb{Z}_{10}^*|$ η τάξη της ομάδας. Για λόγους εξάσκησης και εξοικείωσης με τους υπολογισμούς modulo, υπολογίζουμε τις δυνάμεις και των τριών ακεραίων ως προς την πράξη της ομάδας, που στην περίπτωσή μας είναι ο πολλαπλασιασμός modulo 10:

k	1	2	3	4
3^k mod 10	3	9	7	1
7^k mod 10	7	9	3	1
9^k mod 10	9	1	9	1

ή αν κάνουμε τους υπολογισμούς μας στο $\mathbb{Z}_{10}^*$:

k	1	2	3	4
3^k	3	9	7	1
7^k	7	9	3	1
9^k	9	1	9	1

Παρατηρούμε ότι σε δύο περιπτώσεις η τάξη του στοιχείου είναι 4: για $x = 3$, και για $x = 7$. Παρατηρούμε επίσης ότι στις δύο πρώτες γραμμές του πίνακα εμφανίζονται και τα τέσσερα στοιχεία του συνόλου $\mathbb{Z}_{10}^*$. Συνεπώς η ομάδα $\mathbb{Z}_{10}^*$ είναι κυκλική και τα στοιχεία 3 και 7 είναι γεννήτορές της.

ii)

Δουλεύουμε όπως και πριν. Το δοθέν σύνολο βρίσκουμε ότι είναι το

$$\mathbb{Z}_{15}^* = \{x \in \mathbb{Z}_{15} : \gcd(x, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

Στη συνέχεια, υπολογίζουμε τις δυνάμεις και των οκτώ ακεραίων ως προς την πράξη της ομάδας, που στην περίπτωσή μας είναι ο πολλαπλασιασμός modulo 15:

k	1	2	3	4	5	6	7	8
2^k mod 15	2	4	8	1	2	4	8	1

4^k mod 15	4	1	4	1	4	1	4	1
7^k mod 15	7	4	13	1	7	4	13	1
8^k mod 15	8	4	2	1	8	4	2	1
11^k mod 15	11	1	11	1	11	1	11	1
13^k mod 15	13	4	7	1	13	4	7	1
14^k mod 15	14	1	14	1	14	1	14	1

Παρατηρούμε ότι δεν υπάρχει γραμμή του πίνακα στην οποία να εμφανίζονται και τα οκτώ στοιχεία, που σημαίνει ότι κανένα από αυτά δεν είναι γεννήτορας της ομάδας η οποία βέβαια δεν είναι κυκλική.

Άσκηση 16

Στην ομάδα $\mathbb{Z}_{45}^*$ βρείτε

1) Ένα στοιχείο τάξης 3
2) Μια υποομάδα τάξης 6.

Λύση

1)

Ένα στοιχείο $a \in \mathbb{Z}_n^*$ είναι τάξης t αν a^t mod n = 1, αλλά a^k mod $n \neq 1$, για όλους τους k = 1, 2, …, t – 1.

Για να προσδιορίσουμε στην ομάδα $\mathbb{Z}_{45}^*$ ένα στοιχείο τάξης 3 προσδιορίζουμε πρώτα το σύνολο

$\mathbb{Z}_{45}^* = \{x \in \mathbb{Z}_{45} \mid \gcd(x, 45) = 1\}$

$= \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44\}$

Στη συνέχεια υπολογίζουμε δυνάμεις ως προς την πράξη του πολλαπλασιασμού modulo 45:

k	1	2	3
2^k mod 45	2	4	8
4^k mod 45	4	16	19
7^k mod 45	7	4	28
8^k mod 45	8	19	17
11^k mod 45	11	31	26
13^k mod 45	13	34	37
14^k mod 45	14	16	44
16^k mod 45	16	31	1

Από τον παραπάνω πίνακα διαπιστώνουμε ότι 16^3 mod 45 = 1, αλλά 16^k mod 45 $\neq$ 1 για k = 1, 2. Συνεπώς το 16 είναι ένα στοιχείο τάξης 3 στην ομάδα $\mathbb{Z}_{45}^*$.

2)

Βρίσκουμε πρώτα ένα στοιχείο τάξης 6 υπολογίζοντας αυτή τη φορά δυνάμεις με εκθέτες μέχρι το 6:

k	1	2	3	4	5	6
2^k mod 45	2	4	8	16	32	19
4^k mod 45	4	16	19	31	34	1

Παρατηρούμε ότι το 4 είναι τάξης 6 στην ομάδα $\mathbb{Z}_{45}^*$. Να υπενθυμίσουμε ότι για οποιοδήποτε στοιχείο a μιας ομάδας το σύνολο $\langle a \rangle$ αποτελεί μια υποομάδα της οποίας η τάξη είναι η τάξη του a. Συνεπώς, μια υποομάδα τάξης 6, στην ομάδα $\mathbb{Z}_{45}^*$, είναι

$$\langle 4 \rangle = \{1, 4, 16, 19, 31, 34\}.$$

Άσκηση 17

1) Στην ομάδα $(\mathbb{Z}_{40}, +)$ βρείτε όλα τα στοιχεία τάξης 10.

2) Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης 40. Ποια στοιχεία του G έχουν τάξη 10;

Λύση

Αφήνεται στον αναγνώστη για εξάσκηση.

(απ. 1) τα στοιχεία τάξης 10 είναι 4, 12, 28, και 36. 2) τα στοιχεία τάξης 10 είναι $a^{(4)}$, $a^{(12)}$, $a^{(28)}$ και $a^{(36)}$)

Άσκηση 18

Βρείτε όλους τους γεννήτορες της πολλαπλασιαστικής ομάδας $\mathbb{Z}_{10}^*$.

Λύση

Το σύνολο της ομάδας $\mathbb{Z}_{10}^*$ είναι

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

και η τάξη της είναι $m = \left|\mathbb{Z}_{10}^*\right| = \phi(10) = 4.$ Η ανάλυση του 4 σε γινόμενο πρώτων παραγόντων είναι 2^2. Επομένως, ο έλεγχος του κατά πόσο ένα δεδομένο στοιχείο $a \in \mathbb{Z}_{10}^*$ είναι γεννήτορας, είναι εάν $a^2 \not\equiv 1 \pmod{10}$. Υπολογίζουμε λοιπόν το $a^2 \bmod 10$ για κάθε $a \in \mathbb{Z}_{10}^*$:

a	1	3	7	9
$a^2 \bmod 10$	1	9	9	1

Οι γεννήτορες είναι εκείνα τα a για τα οποία η αντίστοιχη στήλη δεν έχει καταχώριση ίση με 1. Έτσι, το σύνολο των γεννητόρων της ομάδας είναι

$$\mathrm{Gen}\left(\mathbb{Z}_{10}^*\right) = \{3, 7\}.$$

Μπορούμε να εργαστούμε και ως εξής. Είναι εύλογο να δοκιμάσουμε ως υποψήφιο γεννήτορα το $a = 3$. Είναι

i	1	2	3	4
$3^i \bmod 10$	3	9	7	1

οπότε διαπιστώνουμε ότι το 3 είναι ένας γεννήτορας της $\mathbb{Z}_{10}^*$. Επομένως το σύνολο των γεννητόρων είναι

$$\mathrm{Gen}\left(\mathbb{Z}_{10}^{*}\right)=\{3^{i} \bmod 10 : i \in \mathbb{Z}_{4}^{*}\}$$

διότι η τάξη της ομάδας είναι 4. Τώρα, αφού $\mathbb{Z}_4^* = \{1,3\}$, βρίσκουμε ότι

$$\{3^{i} \bmod 10 : i \in \mathbb{Z}_{4}^{*}\}=\{3^{1} \bmod 10,\ 3^{3} \bmod 10\}=\{3,7\}.$$

Πρόκειται φυσικά για το ίδιο σύνολο που βρήκαμε παραπάνω.

Άσκηση 19

1) Θεωρήστε την ομάδα $\mathbb{Z}_{23}^*$. Βρείτε τους γεννήτορές της.

2) Βρείτε όλους τους γεννήτορες των κυκλικών ομάδων ($\mathbb{Z}_{12}$, +), ($\mathbb{Z}_{16}$, +) και ($\mathbb{Z}_{24}$, +).

Λύση

Αφήνεται στον αναγνώστη για εξάσκηση.

(απ. 1) Gen($\mathbb{Z}_{23}^*$) = {5, 7, 10, 11, 14, 15, 17, 19, 20, 21}.

2) Gen($\mathbb{Z}_{12}$) = {1,5,7,11}, Gen($\mathbb{Z}_{16}$) = {1,3,5,7,9,11,13,15}, Gen($\mathbb{Z}_{24}$) = {1,5,7,11,13,17,19,23})

Άσκηση 20

Θεωρήστε την ομάδα $\mathbb{Z}_{19}^*$.

1) Δείξτε ότι η ομάδα αυτή είναι κυκλική.

2) Βρείτε τις υποομάδες της και τους γεννήτορές τους.

Λύση

1)

Επειδή ο 19 είναι πρώτος το σύνολο $\mathbb{Z}_{19}^*$ περιέχει όλους τους ακεραίους από τον 1 μέχρι και τον 18

$$\mathbb{Z}_{19}^* = \{1, 2, \ldots, 18\}$$

Υπολογίζοντας δυνάμεις ως προς την πράξη του πολλαπλασιασμού modulo 19 βρίσκουμε

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^k \bmod 19$	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

οπότε παρατηρούμε ότι στις δυνάμεις του 2 εμφανίζονται όλα τα στοιχεία του $\mathbb{Z}_{19}^*$ (ή ότι η τάξη του στοιχείου 2 είναι 18 = $|\mathbb{Z}_{19}^*|$ = τάξη της ομάδας). Έτσι η ομάδα $\mathbb{Z}_{19}^*$ είναι κυκλική και το 2 είναι ένας γεννήτοράς της.

2)

Ο αναγνώστης μπορεί, για εξάσκηση, να επαληθεύσει ότι οι υποομάδες της $\mathbb{Z}_{19}^*$ με τους γεννήτορές τους, είναι όπως φαίνεται στον ακόλουθο πίνακα:

Υποομάδα	Γεννήτορες	Τάξη
{1}	1	1
{1, 18}	18	2
{1, 7, 11}	7, 11	3
{1, 7, 8, 11, 12, 18}	8, 12	6
{1, 4, 5, 6, 7, 9, 11, 16, 17}	4, 5, 6, 9, 16, 17	9
{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18}	2, 3, 10, 13, 14, 15	18

Στην άσκηση αυτή βλέπουμε να επαληθεύεται το θεώρημα που λέει ότι αν p είναι ένας πρώτος, τότε το $\mathbb{Z}_p^*$ είναι κυκλική ομάδα και το πλήθος των γεννητόρων της είναι $\phi(p-1)$. Πράγματι, για $p = 19$, επειδή $p - 1 = 18 = 2\cdot 3^2$, έχουμε

$$\phi(p-1) = \phi(18) = 18\prod_{i=1}^{2}(1-\frac{1}{p_i}) = 18(1-\frac{1}{2})(1-\frac{1}{3}) = 6$$

όπου χρησιμοποιήσαμε το γεγονός ότι, αν $n \in \mathbb{N}$ και $n = p_1^{e_1}\cdots p_r^{e_r}$ είναι η παραγοντοποίηση του n σε πρώτους, τότε η συνάρτηση ϕ του Euler δίνεται από τον τύπο

$$\phi(n) = n\prod_{i=1}^{r}(1-\frac{1}{p_i}).$$

Άσκηση 21

Υπολογίστε το a^{17}

i) με τον από αριστερά στα δεξιά αλγόριθμο εκθετοποίησης

ii) με τον από δεξιά στα αριστερά αλγόριθμο εκθετοποίησης.

Λύση

Είναι $n = 17 = 10001_2$.

i)

Έχουμε τον ακόλουθο πίνακα που συμπληρώνουμε από αριστερά στα δεξιά:

i	4	3	2	1	0
b_i	1	0	0	0	1
	a	a^2	$(a^2)^2 = a^4$	$(a^4)^2 = a^8$	$(a^8)^2\cdot a = a^{17}$

ii)

Με τον από δεξιά στα αριστερά αλγόριθμο εκθετοποίησης έχουμε τον ακόλουθο πίνακα που συμπληρώνουμε από δεξιά στα αριστερά:

4	3	2	1	0	i
1	0	0	0	1	b_i
a^{16}	a^8	a^4	a^2	a	a^{2^i}
$a\cdot a^{16} = a^{17}$				a	

Άσκηση 22

1) Υπολογίστε το 2^{644} mod 645

2) Υπολογίστε το 7^{327} mod 853.

Λύση

1)

Είναι 644 = 1010000100_2 οπότε έχουμε τον από αριστερά στα δεξιά αλγόριθμο εκθετοποίησης (δηλ. με τον αλγόριθμο εκθετοποίησης που βασίζεται στο σχήμα του Horner) τον ακόλουθο πίνακα στον οποίο πλέον για λόγους συντομίας (και απλότητας!) κάνουμε τους υπολογισμούς μας στο $\mathbb{Z}_{645}$:

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	1	0	0	0	0	1	0	0
	2	2^2 = 4	$4^2 \cdot 2$ = 32	32^2 = 379	379^2 = 451	451^2 = 226	226^2 = 121	$121^2 \cdot 2$ = $451 \cdot 2$ = 257	257^2 = 259	259^2 = 1

Άρα, 2^{644} mod 645 = 1.

Να τονίσουμε το γεγονός ότι οι υπολογισμοί έγιναν στο $\mathbb{Z}_{645}$ (δηλαδή modulo 645, στο $\mathbb{Z}$). Έτσι, για παράδειγμα, η ισότητα

$$32^2 = 379$$

σημαίνει

$$32^2 \equiv 379 \pmod{645}$$

ή ότι

$$32^2 \bmod 645 = 379.$$

Πράγματι, είναι

$$32^2 = 1024$$

και

$$1024 \bmod 645 = 379$$

διότι το υπόλοιπο της διαίρεσης 1024 : 645 είναι 379.

2)

Αφήνεται στον αναγνώστη για εξάσκηση.

Άσκηση 23

Γράψτε πρόγραμμα, σε μια γλώσσα προγραμματισμού της αρεσκείας σας, που να υπολογίζει το a^k mod n για μη αρνητικούς ακεραίους. Στη συνέχεια χρησιμοποιήστε το πρόγραμμά σας για τον υπολογισμό των

i) 2^{1000} mod 2379

ii) 567^{1234} mod 4321

iii) 47^{258008} (mod 1315171).

Άσκηση 24

Να λυθεί το σύστημα ισοτιμιών $\begin{cases} x \equiv 14 \pmod{31} \\ x \equiv 16 \pmod{32} \\ x \equiv 18 \pmod{33} \end{cases}$

Λύση

Είναι

$$\begin{cases} a_1 = 14 \\ a_2 \equiv 16 \\ a_3 = 18 \end{cases}, \quad \begin{cases} m_1 = 31 \\ m_2 \equiv 32 \\ m_3 = 33 \end{cases}, \quad M = m_1\, m_2\, m_3 = 32736 \quad \text{και} \quad \begin{cases} M_1 = M/m_1 = 1056 \\ M_2 = M/m_2 = 1023 \\ M_3 = M/m_3 = 992 \end{cases}$$

Με τον διευρυμένο αλγόριθμο Ευκλείδη (όπου χρειάζεται):

$$y_1 = M_1^{-1} \bmod m_1 = 1056^{-1} \bmod 31 = (34\cdot 31+2)^{-1} \bmod 31 = 2^{-1} \bmod 31 = 16$$
$$y_2 = M_2^{-1} \bmod m_2 = 1023^{-1} \bmod 32 = (31\cdot 32+31)^{-1} \bmod 32 = 31^{-1} \bmod 32 = 31$$
$$y_3 = M_3^{-1} \bmod m_3 = 992^{-1} \bmod 33 = (30\cdot 33+2)^{-1} \bmod 33 = 2^{-1} \bmod 33 = 17$$

Επομένως,

$$\begin{aligned} x &\equiv 14\cdot 1056\cdot 16 + 16\cdot 1023\cdot 31 + 18\cdot 992\cdot 17 \pmod{32736} \\ &\equiv 1047504 \pmod{32736} \equiv 31\cdot 32736 + 32688 \pmod{32736} \\ &\equiv 32688 \pmod{32736}. \end{aligned}$$

Άσκηση 25

Βρείτε τα δύο τελευταία ψηφία των

1) 123^{456}

2) 8765^{4321}

3) 2554^{3333}.

Λύση

Για να βρούμε τα δύο τελευταία ψηφία ενός ακεραίου πρέπει να υπολογίσουμε το υπόλοιπό του modulo 100.

Το Θεώρημα Euler μας λέει ότι αν gcd(a, 100) = 1, τότε $a^{\phi(100)} \equiv 1 \pmod{100}$.

1)

Στην περίπτωση που είναι $a = 123$, είναι gcd(123, 100) = 1, οπότε $123^{\phi(100)} \equiv 1 \pmod{100}$.

Είναι τώρα,

$$\phi(100) = \phi(2^2\cdot 5^2) = 100(1 - 1/2)(1 - 1/5) = 40,$$

οπότε

$$123^{40} \equiv 1 \pmod{100}.$$

Επειδή $456 \equiv 16 \pmod{40} \Rightarrow 123^{456} \equiv 123^{456 \bmod 40} \equiv 123^{16} \pmod{100}$.

Επίσης είναι $123 \equiv 23 \pmod{100} \Rightarrow 123^{16} \equiv 23^{16} \pmod{100}$.

Για τον υπολογισμό της δύναμης αυτής χρησιμοποιούμε τη μέθοδο των επανειλημμένων τετραγωνισμών (από αριστερά στα δεξιά εκθετοποίηση):

Είναι $16 = 10000_2$ και με τους υπολογισμούς να γίνονται στο $\mathbb{Z}_{100}$, βρίσκουμε

i	4	3	2	1	0
b_i	1	0	0	0	0
	23	$23^2 = 29$	$29^2 = 41$	$41^2 = 81$	$81^2 = 61$

Άρα, $23^{16} \equiv 61 \pmod{100}$ και τελικά

$$123^{456} \equiv 61 \pmod{100}.$$

Συνεπώς τα δύο τελευταία ψηφία είναι 61.

2)

Στην περίπτωση που $a = 8765 =$ πολ 5, είναι $\gcd(\alpha, 100) \neq 1$. Μπορούμε όμως να επιταχύνουμε τους υπολογισμούς μας με το Κινέζικο θεώρημα υπολοίπων.

Είναι $100 = 4\cdot 25$ και $\gcd(4, 25) = 1$. Επομένως η ισοτιμία

$$x \equiv 8765^{4321} \pmod{100}$$

είναι ισοδύναμη με το σύστημα ισοτιμιών

$$\begin{cases} x \equiv 8765^{4321} \pmod{4}, & (1) \\ x \equiv 8765^{4321} \pmod{25}, & (2) \end{cases}$$

Επειδή $8765 \equiv 1 \pmod{4} \Rightarrow 8765^{4321} \equiv 1 \pmod{4}$, οπότε

$$(1) \Leftrightarrow x \equiv 1 \pmod{4}.$$

Επίσης, επειδή $8765 \equiv 15 \pmod{25} \Rightarrow 8765^2 \equiv 15^2 \equiv 225 \equiv 0 \pmod{25} \Rightarrow$

$$\forall\, k \geq 2,\ 8765^k \equiv 0 \pmod{25},$$

οπότε,

$$8765^{4321} \equiv 0 \pmod{25}$$

και

$$(2) \Leftrightarrow x \equiv 0 \pmod{25}.$$

Τελικά η ισοτιμία

$$x \equiv 8765^{4321} \pmod{100}$$

είναι ισοδύναμη με το σύστημα ισοτιμιών

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{25} \end{cases}$$

Είναι

$$\begin{cases} a_1 = 1 \\ a_2 = 0 \end{cases}, \quad \begin{cases} m_1 = 4 \\ m_2 = 25 \end{cases} \text{ (ανά δύο σχετικώς πρώτοι) και } M = m_1 m_2 = 100.$$

Βρίσκουμε

$$\begin{cases} M_1 = M/m_1 = 25 \\ M_2 = M/m_2 = 4 \end{cases} \text{ και } \begin{cases} b_1 = M_1 \bmod m_1 = 25 \bmod 4 = 1 \\ b_2 = M_2 \bmod m_2 = 4 \bmod 25 = 4 \end{cases}$$

Επίσης βρίσκουμε

$$\begin{cases} t_1 = b_1^{-1} \bmod m_1 = 1^{-1} \bmod 4 = 1 \\ t_2 = b_2^{-1} \bmod m_2 = 4^{-1} \bmod 25 = 19 \end{cases} \text{ και } \begin{cases} e_1 = M_1 t_1 = 25 \cdot 1 = 25 \\ e_2 = M_2 t_2 = 4 \cdot 19 = 76 \end{cases}$$

οπότε

$$x = (a_1e_1 + a_2e_2) \bmod M = (1\cdot 25 + 0\cdot 76) \bmod 100 = 25 \bmod 100 = 25.$$

Άρα, $x \equiv 25 \pmod{100}$ και συνεπώς τα δύο τελευταία ψηφία του 8765^{4321} είναι 25.

3)

Αφήνεται στον αναγνώστη για εξάσκηση.

Άσκηση 26

Να υπολογίσετε το $263790^{216491} \bmod 265651$ γνωρίζοντας ότι $265651 = 631\cdot 421$, όπου οι ακέραιοι 631, 421 είναι πρώτοι.

Λύση

Είναι

$$x \equiv 263790^{216491} \pmod{265651} \Leftrightarrow \begin{cases} x \equiv 263790^{216491} \pmod{631}, & (1) \\ x \equiv 263790^{216491} \pmod{421}, & (2) \end{cases}$$

Είναι

$$263790 \equiv 32 \pmod{631} \Rightarrow 263790^{216491} \pmod{631} \equiv 32^{216491} \pmod{631}.$$

Επειδή ο 631 είναι πρώτος, από το θεώρημα Fermat έχουμε

$$32^{630} \equiv 1 \pmod{631} \Rightarrow 32^{216491} \equiv 32^{216491 \bmod 630} \equiv 32^{401} \pmod{631}.$$

Για τον υπολογισμό της δύναμης αυτής χρησιμοποιούμε τη μέθοδο των επανειλημμένων τετραγωνισμών (από αριστερά στα δεξιά εκθετοποίηση):

Είναι $401 = 110010001_2$ και με τους υπολογισμούς να γίνονται στο $\mathbb{Z}_{631}$, βρίσκουμε

i	8	7	6	5	4	3	2	1	0
b_i	1	1	0	0	1	0	0	0	1
	32	$32^2\cdot 32$	587^2	43^2	$587^2\cdot 32$	114^2	376^2	32^2	$393^2\cdot 32$
		$= 587$	$= 43$	$= 587$	$= 114$	$= 376$	$= 32$	$= 393$	$= 376$

Άρα, $(1) \Leftrightarrow x \equiv 376 \pmod{631}$.

Παρόμοια, επειδή $263790 \equiv 244 \pmod{421}$ και $216491 \equiv 191 \pmod{420}$, έχουμε

$$263790^{216491} \equiv 244^{191} \pmod{421}$$

$$\equiv 102 \pmod{421}$$

οπότε

$(2) \Leftrightarrow x \equiv 102 \pmod{421}$.

Έτσι έχουμε καταλήξει στο εξής σύστημα ισοτιμιών

$$\begin{cases} x \equiv 376 \pmod{631} \\ x \equiv 102 \pmod{421} \end{cases}$$

Σύμφωνα με τη μέθοδο (αλγόριθμο) του Κινέζικου θεωρήματος υπολοίπων είναι:

$$\begin{cases} a_1 = 376 \\ a_2 = 102 \end{cases}, \quad \begin{cases} m_1 = 631 \\ m_2 = 421 \end{cases} \text{ (ανά δύο σχετικώς πρώτοι) και } M = m_1 m_2 = 265651.$$

Βρίσκουμε

$$\begin{cases} M_1 = M/m_1 = 421 \\ M_2 = M/m_2 = 631 \end{cases} \text{ και } \begin{cases} b_1 = M_1 \bmod m_1 = 421 \bmod 631 = 421 \\ b_2 = M_2 \bmod m_2 = 631 \bmod 421 = 210 \end{cases}$$

Επίσης βρίσκουμε

$$\begin{cases} t_1 = b_1^{-1} \bmod m_1 = 421^{-1} \bmod 631 = 3 \\ t_2 = b_2^{-1} \bmod m_2 = 210^{-1} \bmod 421 = 419 \end{cases} \text{ και } \begin{cases} e_1 = M_1 t_1 = 421 \cdot 3 = 1263 \\ e_2 = M_2 t_2 = 631 \cdot 419 = 264389 \end{cases}$$

[στους υπολογισμούς για τους αντίστροφους χρησιμοποιήσαμε τον διευρυμένο αλγόριθμο του Ευκλείδη:

i	0	1	2	3	4
r_i	631	421	210	1	0
q_i		1	2	210	
s_i	1	0	1	–2	
t_i	0	1	–1	3	

$\Rightarrow$ gcd(631, 421) = 1, $t = 3 \Rightarrow 421^{-1} \bmod 631 = 3$

και

i	0	1	2	3
r_i	421	210	1	0
q_i		2	210	
s_i	1	0	1	
t_i	0	1	–2	

$\Rightarrow$ gcd(421, 210) = 1, $t = -2 \equiv 419 \pmod{421} \Rightarrow 210^{-1} \bmod 421 = 419$.]

οπότε

$$x = (a_1 e_1 + a_2 e_2) \bmod M = (376 \cdot 1263 + 102 \cdot 264389) \bmod 265651 = 80513.$$

Άρα, $263790^{216491} \bmod 265651 = 80513$.

Άσκηση 27

Βρείτε το υπόλοιπο της διαίρεσης του $2^{2^{405}}$ με το 23.

Λύση

Αφήνεται στον αναγνώστη για εξάσκηση.