ΠΜΣ ‘‘ΠΛΗΡΟΦΟΡΙΚΗ’’
(ΠΛΗ2, $6^{ος}$ κύκλος, $1^{ο}$ εξάμηνο, 2023)

ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ

Κ. ΜΑΝΕΣ - Ι. ΤΑΣΟΥΛΑΣ

Σημειώσεις διαλέξεων 5

Κεφάλαιο 3

Στοιχεία θεωρίας αριθμών

3.1 Διαιρετότητα

Έστω $a, b \in \mathbb{Z}$. Λέμε ότι ο b **διαιρεί** τον a αν υπάρχει ακέραιος αριθμός $\pi \in \mathbb{Z}$ τέτοιος $a = \pi b$. Στην περίπτωση αυτή γράφουμε $\mathbf{b \mid a}$ και λέμε ότι ο b είναι **διαιρέτης** του a, ενώ ο a είναι **πολλαπλάσιο** του b. (Ο συμβολισμός $a \mid b$ δεν πρέπει να συγχέεται με τον συμβολισμό a/b που εκφράζει το κλάσμα με αριθμητή τον a και παρανομαστή τον b.) Στη περίπτωση όπου $b \neq a$, ο b ονομάζεται **γνήσιος διαιρέτης** του a. Στην περίπτωση που δεν υπάρχει ακέραιος αριθμός π που επαληθεύει την εξίσωση $a = \pi b$ λέμε ότι ο b **δεν διαιρεί** τον a και γράφουμε $\mathbf{b \nmid a}$.

Για παράδειγμα, $13 \mid 26$ διότι $26 = 2 \cdot 13$ και $13 \nmid 17$ διότι δεν υπάρχει ακέραιος π ώστε $17 = \pi \cdot 13$.

Γενικότερα ισχύει η επόμενη πρόταση.

Πρόταση 2. *Αν a είναι ακέραιος και b είναι μη μηδενικός ακέραιος, τότε υπάρχουν μοναδικοί ακέραιοι π και υ ώστε*

$$a = \pi b + \upsilon, \text{ όπου } 0 \leq \upsilon < |b|.$$

Για παράδειγμα, έστω $b = 13$.

Αν $a = 26$, έχουμε

$$26 = 2 \cdot 13 + 0,$$

οπότε $\pi = 2$ και $\upsilon = 0$. Επίσης, $13 \mid 26$.

Αν $a = 17$, έχουμε

$$17 = 1 \cdot 13 + 4,$$

οπότε $\pi = 1$ και $\upsilon = 4$. Επίσης, $13 \nmid 17$.

Αν $a = 8$, έχουμε

$$8 = 0 \cdot 13 + 8,$$

οπότε $\pi = 0$ και $\upsilon = 8$. Επίσης, $13 \nmid 8$.

Αν $a = -39$, έχουμε

$$-39 = (-3) \cdot 13 + 0,$$

οπότε $\pi = -3$ και $\upsilon = 0$. Επίσης, $13 \mid (-39)$.

Τέλος, αν $a = -20$, έχουμε

$$-20 = (-2) \cdot 13 + 6,$$

οπότε $\pi = -2$ και $\upsilon = 6$. Επίσης, $13 \nmid -20$.

Παρατηρήσεις:

1. Η πρόταση αυτή αντιστοιχεί στην γνωστή διαίρεση του αριθμού a από τον αριθμό b. Ο αριθμός π ονομάζεται **πηλίκο** και ο αριθμός υ ονομάζεται **υπόλοιπο** της διαίρεσης του a από τον b. Στην περίπτωση που $\upsilon = 0$ η διαίρεση ονομάζεται **τέλεια**, ενώ αν $\upsilon \neq 0$ τότε η διαίρεση ονομάζεται **ατελής**.

2. **Προσοχή!** Το υπόλοιπο της διαίρεσης υ είναι πάντα μη αρνητικός αριθμός φραγμένος από το 0 και το $|b| - 1$.

3.1.1 Μέγιστος κοινός διαιρέτης

Έστω a, b φυσικοί αριθμοί. Ο **μέγιστος κοινός διαιρέτης** (ΜΚΔ) των a και b είναι ο μεγαλύτερος φυσικός αριθμός ο οποίος διαιρεί και τους δύο αριθμούς και συμβολίζεται με $\text{ΜΚΔ}(a, b)$, ή $\gcd(a, b)$.

Για παράδειγμα, ο μέγιστος κοινός διαιρέτης των $12, 18$ είναι το 6, διότι οι διαιρέτες του 12 είναι οι 1, 2, 3, 4, 6, 12, ενώ οι διαιρέτες του 18 είναι οι 1, 2, 3, 6, 9, 18, οι κοινοί διαιρέτες τους είναι το 1, 2, 3, 6, και ο μέγιστος από αυτούς είναι το 6, συμβολικά $\text{ΜΚΔ}(12, 18) = 6$. Επίσης, ο μέγιστος κοινός διαιρέτης των $12, 7$ είναι το 1, συμβολικά $\text{ΜΚΔ}(12, 7) = 1$. Τέλος, ο μέγιστος κοινός διαιρέτης των $12, 4$ είναι το 4, συμβολικά $\text{ΜΚΔ}(12, 4) = 4$.

Παρατηρήσεις:

1. Ο μέγιστος κοινός διαιρέτης των a και b είναι ο μέγιστος θετικός ακέραιος d που ικανοποιεί τις παρακάτω δύο ιδιότητες:

i) $d \mid a$ και $d \mid b$, και

ii) Αν $c \mid a$ και $c \mid b$, τότε $c \mid d$.

2. Αν $d \mid a$, τότε $\text{ΜΚΔ}(a, d) = d$.

3. Όταν $\text{ΜΚΔ}(a, b) = 1$, λέμε ότι οι a και b είναι **πρώτοι προς αλλήλους** ή (**σχετικά**) **πρώτοι μεταξύ τους**.

4. Αν $a = \pi b + \upsilon$ τότε $\text{ΜΚΔ}(a, b) \mid \upsilon$ και $\text{ΜΚΔ}(b, \upsilon) \mid a$. Η ιδιότητα αυτή είναι η βάση του αλγόριθμου του Ευκλείδη, που παρουσιάζεται στην επόμενη ενότητα.

3.1.2 Ο αλγόριθμος του Ευκλείδη

Ο απλοϊκός τρόπος υπολογισμού του ΜΚΔ δύο αριθμών a και b είναι η εύρεση όλων των διαιρετών των a και b και στη συνέχεια η επιλογή του μεγαλύτερου από αυτούς. Η διαδικασία αυτή απαιτεί πολλούς υπολογισμούς. Μια αποτελεσματικότερη μέθοδος είναι ο **αλγόριθμος του Ευκλείδη**.

Πρόταση 3. *Έστω $a, b \in \mathbb{N}^*$ με $a = \pi b + \upsilon$, όπου $0 \leq \upsilon < b$. Τότε ισχύει ότι*

$$\textit{ΜΚΔ}(a, b) = \textit{ΜΚΔ}(b, \upsilon).$$

Επιπλέον, αν $\upsilon = 0$, τότε $\textit{ΜΚΔ}(a, b) = b$.

Για παράδειγμα, ο υπολογισμός του ΜΚΔ των 168 και 25 προκύπτει με τη βοήθεια των παρακάτω ισοτήτων που περιγράφουν τις διαιρέσεις κάθε βήματος:

$$\begin{aligned} 168 &= 6 \cdot 25 + 18, \\ 25 &= 1 \cdot 18 + 7, \\ 18 &= 2 \cdot 7 + 4, \\ 7 &= 1 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Άρα, $\text{ΜΚΔ}(168, 25) = 1$.

Ο υπολογισμός του ΜΚΔ των 2520 και 154 προκύπτει ως εξής:

$$\begin{aligned} 2520 &= 16 \cdot 154 + 56, \\ 154 &= 2 \cdot 56 + 42, \\ 56 &= 1 \cdot 42 + 14, \\ 42 &= 3 \cdot 14 + 0. \end{aligned}$$

Άρα, $\text{ΜΚΔ}(2520, 154) = 14$.

Πολυπλοκότητα του αλγορίθμου του Ευκλείδη: Το κόστος εκτέλεσης του αλγορίθμου του Ευκλείδη είναι ανάλογο του αριθμού των διαιρέσεων που απαιτούνται για την εύρεση των υπολοίπων κάθε ενδιαμέσου ζεύγους. Ένα φράγμα για το κόστος του αλγορίθμου του Ευκλείδη δίδεται στην Πρόταση 4.

Πρόταση 4 (Πολυπλοκότητα του αλγορίθμου του Ευκλείδη). *Έστω $a, b \in \mathbb{N}^*$ με $a > b$. Ο αριθμός των διαιρέσεων $c(a, b)$ που απαιτούνται για τον υπολογισμό του μέγιστου κοινού διαιρέτη των a, b είναι μικρότερος από $5 \log_{10} a \simeq 1.50515 \log_2 a$.*

Παρατήρηση: Η πρόταση αυτή αποδείχθηκε από το Γάλλο μαθηματικό Gabriel Lamé και θεωρείται **το πρώτο αποτέλεσμα σχετικά με τον υπολογισμό της πολυπλοκότητας ενός αλγορίθμου**.

3.1.3 Πρώτοι αριθμοί

Ένας φυσικός αριθμός p ονομάζεται **πρώτος αριθμός** αν ο p διαιρείται μόνο από το 1 και τον p. Στην περίπτωση που υπάρχουν και άλλοι διαιρέτες ο αριθμός p ονομάζεται **σύνθετος**. Για λόγους που θα εξηγήσουμε παρακάτω, ο αριθμός 1 δεν θεωρείται ούτε πρώτος ούτε σύνθετος.

Στον επόμενο πίνακα σημειώνονται με έντονα στοιχεία οι πρώτοι αριθμοί από το 1 έως το 100, (συνολικά υπάρχουν 25 πρώτοι αριθμοί στο διάστημα 1 έως 100).

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Οι πρώτοι αριθμοί βρίσκονται στην καρδιά της έρευνας στην Θεωρία Αριθμών. Στην ενότητα αυτή θα δούμε ορισμένα προκαταρκτικά αποτελέσματα σχετικά με τους πρώτους αριθμούς.

Πρόταση 5. *Κάθε φυσικός αριθμός $n \geq 2$ είναι πρώτος, ή γινόμενο πρώτων αριθμών.*

Άραγε υπάρχουν άπειροι πρώτοι αριθμοί; Η απάντηση είναι καταφατική. Ο Ευκλείδης στο βιβλίο του Στοιχεία δίνει την επόμενη πρόταση.

Πρόταση 6. *Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.*

Όπως φαίνεται στην επόμενη πρόταση οι πρώτοι αριθμοί μπορούν να θεωρηθούν ως οι ''δομικοί λίθοι'' των φυσικών αριθμών.

Πρόταση 7 (Θεμελιώδες Θεώρημα της Αριθμητικής). *Κάθε φυσικός αριθμός $n \geq 2$ εκφράζεται κατά μοναδικό τρόπο ως γινόμενο πρώτων (χωρίς να μας ενδιαφέρει η σειρά με την οποία εμφανίζονται στο γινόμενο οι παράγοντες).*

Παρατήρηση: Από την προηγούμενη πρόταση προκύπτει ότι κάθε φυσικός αριθμός $n \geq 2$ παριστάνεται μονοσήμαντα ως

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

όπου p_1, p_2, ..., p_k είναι πρώτοι αριθμοί (διαφορετικοί ανά δύο) και a_1, a_2, ..., a_k είναι φυσικοί αριθμοί. Αυτή η ανάλυση ονομάζεται **κανονική παραγοντοποίηση** του αριθμού n.

Για παράδειγμα, ο αριθμός 84 αναλύεται ως γινόμενο

$$84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3 \cdot 7.$$

Ο αριθμός 2 εισέρχεται στην παραγοντοποίηση του 84 υψωμένος στο τετράγωνο, ενώ το 3 και το 7 στην πρώτη. Μπορούμε να υποθέσουμε ότι και το 5 εισέρχεται στην παραγοντοποίηση του 84 αλλά υψωμένο στην μηδενική δύναμη και γενικά ότι όλοι οι πρώτοι αριθμοί εισέρχονται σε μια παραγοντοποίηση αλλά μερικοί υψωμένοι στην μηδενική δύναμη. Καταλαβαίνουμε τώρα γιατί δεν είναι βολικό να θεωρούμε το 1 πρώτο αριθμό. Αυτός ο αριθμός μπορεί να περιληφθεί σε κάθε παραγοντοποίηση υψωμένος σε οποιαδήποτε δύναμη. Για παράδειγμα,

$$84 = 1^2 \cdot 2^2 \cdot 3 \cdot 7 = 1^{200} \cdot 2^2 \cdot 3 \cdot 7,$$

γεγονός που αναιρεί το μονοσήμαντο.

3.2 Ισοτιμίες

Έστω n ένας σταθερός φυσικός αριθμός. Οι ακέραιοι a, b καλούνται **ισότιμοι** (**modulo** n), ή **ισότιμοι κατά μέτρο** n, ή **ισοϋπόλοιποι modulo** n και γράφουμε $\mathbf{a \equiv b} \pmod{\mathbf{n}}$ αν και μόνο αν η διαφορά $a - b$ διαιρείται από τον n, δηλαδή

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Αν $n \nmid (a - b)$, γράφουμε $a \not\equiv b \pmod{n}$ και λέμε ότι ο a είναι **ανισότιμος προς τον** b (**modulo** n).

Για παράδειγμα, έχουμε

$$\begin{aligned}
15 &\equiv 10 \pmod{5} \text{ αφού ισχύει ότι } 5 \mid (15 - 10),\\
27 &\equiv 7 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (27 - 7),\\
7 &\equiv 27 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (7 - 27),\\
27 &\equiv 3 \pmod{3} \text{ αφού ισχύει ότι } 3 \mid (27 - 3),\\
7 &\equiv 3 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (7 - 3),\\
27 &\equiv -1 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (27 - (-1)),\\
21 &\equiv 0 \pmod{3} \text{ αφού ισχύει ότι } 3 \mid (21 - 0),\\
25 &\not\equiv 12 \pmod{7} \text{ αφού ισχύει ότι } 7 \nmid (25 - 12).
\end{aligned}$$

Παρατήρηση: Είναι πολύ συνηθισμένο το σύμβολο $a \bmod n$ να χρησιμοποιείται όχι μόνο ως σύμβολο της ισοτιμίας αλλά να συμβολίζει και το υπόλοιπο της διαίρεσης του a από το n. Στην περίπτωση αυτή χρησιμοποιείται συνήθως η γραφή $a \bmod n = b$ ή $b = a \bmod n$ αντί του συμβόλου $\equiv$. Όπως θα δούμε στην συνέχεια, αυτή η διπλή χρήση είναι δικαιολογημένη.

Πρόταση 8. *Δύο ακέραιοι a, b είναι ισότιμοι modulo n, δηλαδή ισχύει $a \equiv b \pmod{n}$ αν και μόνο αν διαιρούμενοι με τον n έχουν το ίδιο υπόλοιπο.*

Απόδειξη. Έστω δύο ακέραιοι a, b οι οποίοι διαιρούμενοι με το n έχουν υπόλοιπο υ, δηλαδή ισχύει ότι

$$a = \pi_1 n + \upsilon \text{ και } b = \pi_2 n + \upsilon \text{ όπου } 0 \leq \upsilon < n.$$

Τότε

$$a - b = (\pi_1 - \pi_2)n,$$

δηλαδή $n|(a-b)$, επομένως $a \equiv b \pmod{n}$.

Αντίστροφα, έστω ότι $a \equiv b \bmod n$ τότε $n|(a-b)$ δηλαδή ότι $a - b = \pi n$ όπου $\pi \in \mathbb{Z}$. Άρα

$$a = b + \pi n.$$

Αν διαιρέσουμε τον b με τον n προκύπτει ότι

$$b = \pi' n + \upsilon \text{ όπου } 0 \leq \upsilon < n$$

οπότε

$$a = \pi n + \pi' n + \upsilon = (\pi + \pi')n + \upsilon \text{ όπου } 0 \leq \upsilon \leq n.$$

Επομένως, οι ακέραιοι a, b διαιρουμένοι δια του n αφήνουν το ίδιο υπόλοιπο. □

Παρατήρηση: Οι ακέραιοι a οι οποίοι είναι ισότιμοι με b modulo n, δίνονται από τον τύπο

$$a = b + kn$$

όπου $k = 0, \pm 1, \pm 2, \ldots$.

Για παράδειγμα, οι ακέραιοι x οι οποίοι είναι ισότιμοι με 1 modulo 10, δηλαδή είναι λύσεις της εξίσωσης

$$x \equiv 1 \pmod{10}$$

είναι της μορφής

$$x = 10 \cdot k + 1, \text{ όπου } k = 0, \pm 1, \pm 2, \ldots.$$

Για $k = 0, 1, 2, 3, \ldots$ προκύπτει ότι

$$x = 1, 11, 21, 31, \ldots$$

και για $k = -1, -2, -3, \ldots$ προκύπτει ότι

$$x = -9, -19, -29, \ldots$$

Επομένως, οι ακέραιοι που είναι ισότιμοι με 1 modulo 10 είναι οι εξής:

$$x = \ldots, -29, -19, -9, 1, 11, 21, 31, \ldots.$$

Πρόταση 9. *Η σχέση ισοτιμίας* mod$n$ *είναι μια σχέση ισοδυναμίας στο σύνολο* $\mathbb{Z}$.

Απόδειξη. Αρκεί να αποδειχθεί ότι ισχύει η ανακλαστική, η συμμετρική και η μεταβατική ιδιότητα.

Πράγματι, για κάθε $a \in \mathbb{Z}$ ισχύει ότι $n \mid (a-a)$ επομένως $a \equiv a \pmod{n}$, δηλαδή ισχύει η ανακλαστική ιδιότητα.

Αν $a \equiv b \pmod{n}$ τότε $n \mid (a-b)$, επομένως ισχύει ότι $n \mid -(a-b)$ δηλαδή $n \mid (b-a)$, οπότε $b \equiv a \pmod{n}$, δηλαδή ισχύει η συμμετρική ιδιότητα.

Αν $a \equiv b \pmod{n}$ και $b \equiv c \pmod{n}$, τότε $n \mid (a-b)$ και $n \mid b-c$ οπότε $n \mid (a-b)+(b-c) = a-c$. Επομένως $a \equiv c \pmod{n}$, δηλαδή ισχύει η μεταβατική ιδιότητα. □

Παρατηρήσεις:

1. Με τη βοήθεια της σχέσης ισοτιμίας modulo n, όλοι οι ακέραιοι αριθμοί μπορούν να διαμεριστούν σε κλάσεις οι οποίες ονομάζονται **κλάσεις υπολοίπων** mod$n$. Οι κλάσεις αυτές έχουν την ιδιότητα ότι όλα τα στοιχεία που είναι στην ίδια κλάση είναι ανά δύο ισότιμα modulo n. Για κάθε $a \in \mathbb{Z}$ ορίζουμε την κλάση

$$\{x \in \mathbb{Z} : x \equiv a \pmod{n}\},$$

και την συμβολίζουμε με $\overline{a}$ ή με $[a]_n$.

2. Κάθε ακέραιος αριθμός είναι ισοϋπόλοιπος mod$n$ με έναν ακριβώς από τους αριθμούς: $0, 1, 2, \ldots, n-1$. Επομένως το σύνολο των ακεραίων χωρίζεται σε n κλάσεις mod$n$ τέτοιες ώστε:

$$\begin{aligned}
\overline{0} &= \{\ldots, -2\cdot n, -n, \ 0, \ n, \ 2\cdot n, \ \ldots\},\\
\overline{1} &= \{\ldots, -2\cdot n+1, -n+1, \ 1, \ n+1, \ 2\cdot n+1, \ \ldots\},\\
\overline{2} &= \{\ldots, -2\cdot n+2, -n+2, \ 2, \ n+2, \ 2\cdot n+2, \ \ldots\},\\
&\vdots\\
\overline{n-1} &= \{\ldots, -n-1, \ -1, \ n-1, \ 2\cdot n-1, \ 3\cdot n-1, \ \ldots\}.
\end{aligned}$$

Άρα

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}\\
&= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}.
\end{aligned}$$

Με $\mathbb{Z}_n$ συμβολίζουμε το **σύνολο κλάσεων** modulo n

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

Οι βασικές ιδιότητες της ισοτιμίας modulo n δίνονται στην επόμενη πρόταση.

Πρόταση 10. *Αν n είναι ένας σταθερός φυσικός αριθμός και a, b, c, d ακέραιοι, ισχύουν τα ακόλουθα:*

1. *Αν $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$, τότε*

$$a + c \equiv b + d \pmod{n} \text{ και } a \cdot c \equiv b \cdot d \pmod{n}.$$

2. *Αν $a \equiv b \pmod{n}$, τότε*

$$a + c \equiv b + c \pmod{n} \text{ και } a \cdot c \equiv b \cdot c \pmod{n}.$$

3. *Αν $a \equiv b \pmod{n}$, τότε*

$$a^k \equiv b^k \pmod{n} \text{ για κάθε } k \in \mathbb{N}.$$

4. *Αν $p(x) = c_0 + c_1 x + \ldots + c_k x^k$ είναι ένα πολυωνύμο με ακέραιους συντελεστές και $a \equiv b \pmod{n}$, τότε*

$$p(a) \equiv p(b) \pmod{n}.$$

Εφαρμογές

Με τη βοήθεια των προηγούμενων ιδιοτήτων των ισοτιμιών μπορούμε να μειώσουμε σημαντικά το κόστος υπολογισμού που απαιτείται κατά τις πράξεις αριθμών modulo n. Στη συνέχεια δίδονται ορισμένα χαρακτηριστικά παραδείγματα εφαρμογής των ιδιοτήτων των ισοτιμιών, κυρίως για τον υπολογισμό δυνάμεων ακεραίων modulo n.

Εφαρμογή 3.1. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$2^{100} \equiv x \pmod 7.$$

Λύση. Παρατηρούμε ότι $2^3 \equiv 8 \equiv 1 \pmod 7$ επομένως

$$2^{100} \equiv 2^{3\cdot 33+1} \equiv (2^3)^{33} \cdot 2 \equiv 1^{33} \cdot 2 \equiv 2 \pmod 7.$$

Άρα, $x = 2$. Δηλαδή, το υπόλοιπο της διαίρεσης του 2^{100} με το 7 ισούται με 2. □

Εφαρμογή 3.2. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$2^{100} \equiv x \pmod 9.$$

Λύση. Παρατηρούμε ότι $2^3 \equiv 8 \equiv -1 \pmod 9$ επομένως

$$2^{100} \equiv 2^{3\cdot 33+1} \equiv (2^3)^{33} \cdot 2 \equiv (-1)^{33} \cdot 2 \equiv -2 \equiv 7 \pmod 9.$$

Άρα, $x = 7$. Δηλαδή, το υπόλοιπο της διαίρεσης του 2^{100} με το 9 ισούται με 7. □

Εφαρμογή 3.3. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$3^{100} \equiv x \pmod{11}.$$

Λύση. Ισχύει ότι

$$3^{100} \equiv (3^2)^{50} \equiv 9^{50} \equiv (9^2)^{25} \equiv 81^{25} \pmod{11}.$$

Επειδή $81 \equiv 4 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 4^{25} \equiv (4^2)^{12} \cdot 4 \equiv 16^{12} \cdot 4 \pmod{11}.$$

Επειδή $16 \equiv 5 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 5^{12} \cdot 4 \equiv (5^2)^6 \cdot 4 \equiv 25^6 \cdot 4.$$

Επειδή $25 \equiv 3 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 3^6 \cdot 4 \equiv (3^2)^3 \cdot 4 \equiv 9^3 \cdot 4 \pmod{11} \equiv 9^2 \cdot 9 \cdot 4 \equiv 81 \cdot 36 \pmod{11}.$$

Επειδή $81 \equiv 4 \pmod{11}$ και $36 \equiv 3 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 4 \cdot 3 \equiv 12 \equiv 1 \pmod{11}.$$

Άρα, $x = 1$. Δηλαδή, το υπόλοιπο της διαίρεσης του 3^{100} με το 11 ισούται με 1. □

Εφαρμογή 3.4. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$7^{1000} \equiv x \pmod{13}.$$

Λύση. Ισχύει ότι

$$7^{1000} \equiv (7^2)^{500} \equiv 49^{500} \pmod{13}.$$

Επειδή $49 \equiv 10 \pmod{13}$, προκύπτει ότι

$$7^{1000} \equiv 10^{500} \equiv (10^2)^{250} \equiv 100^{250} \pmod{13}.$$

Επειδή $100 \equiv 9 \pmod{13}$, προκύπτει ότι

$$7^{1000} \equiv 9^{250} \equiv (9^2)^{125} \equiv 81^{125} \pmod{13}.$$

Επειδή $81 \equiv 3 \pmod{13}$, προκύπτει ότι

$$7^{1000} \equiv 3^{125} \pmod{13}.$$

Παρατηρούμε ότι $3^3 \equiv 27 \equiv 1 \pmod{13}$ και επομένως

$$7^{1000} \equiv 3^{125} \equiv 3^{3 \cdot 41 + 2} \equiv (3^3)^{41} \cdot 9 \equiv 1^{41} \cdot 9 \equiv 9 \pmod{13}.$$

Άρα, $x = 9$. Δηλαδή, το υπόλοιπο της διαίρεσης του 7^{1000} με το 13 ισούται με 9. □

3.2.1 Η συνάρτηση ϕ του Euler

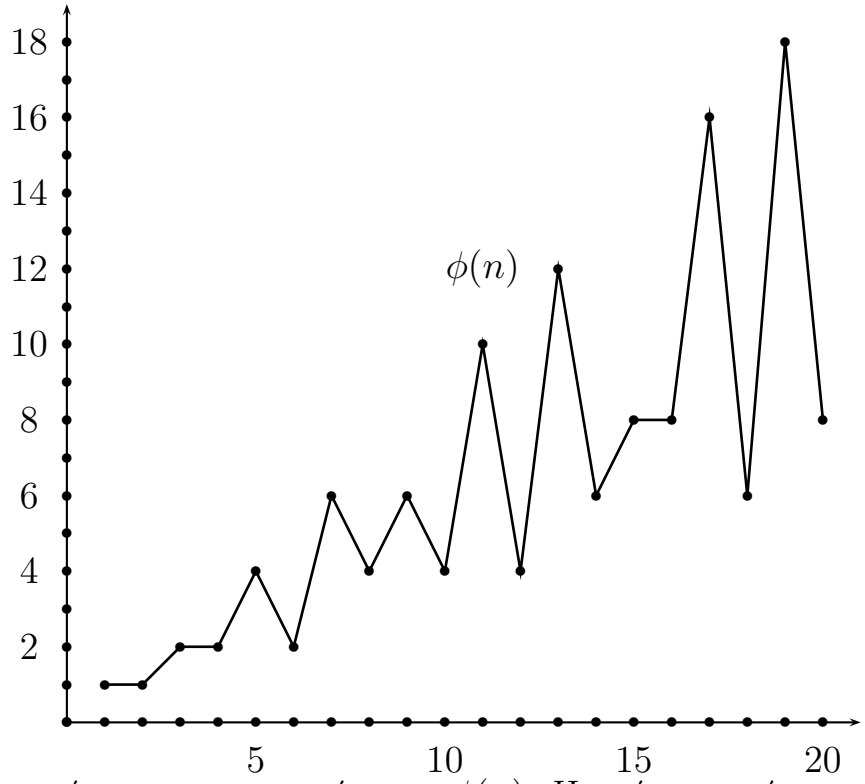
Στην ενότητα αυτή θα μελετήσουμε το ερώτημα πόσοι είναι οι αριθμοί που είναι μικρότεροι από κάποιο αριθμό και είναι σχετικά πρώτοι με αυτόν;

Έστω $\phi(n)$ το πλήθος των αριθμών m που είναι μικρότεροι ή ίσοι από το n και ισχύει ότι $\text{ΜΚΔ}(n, m) = 1$, δηλαδή τα n και m είναι σχετικά πρώτοι μεταξύ τους.

Για παράδειγμα, $\phi(12) = 4$, διότι από τους αριθμούς $1, 2, \ldots, 12$ το 12 είναι σχετικά πρώτο με τους αριθμούς 1, 5, 7, 11 (δεν είναι με το 8 διότι αν και το 8 δεν διαιρεί το 12 εν τούτοις ισχύει ότι $\text{ΜΚΔ}(12, 8) = 4$).

Οι τιμές της $\phi(n)$ για κάθε n μικρότερο ή ίσο του 20 δίνονται στον επόμενο πίνακα.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8



Υπάρχει τύπος για την συνάρτηση $\phi(n)$; Η απάντηση είναι καταφατική.

Πρόταση 11. *Αν p είναι πρώτος αριθμός και $k \in \mathbb{N}^*$. Τότε $\phi(p^k) = p^k - p^{k-1}$.*

Αν m, n φυσικοί αριθμοί με ΜΚΔ$(m, n) = 1$. Τότε $\phi(mn) = \phi(m)\phi(n)$.

Από την προηγούμενη πρόταση άμεσα προκύπτει μια έκφραση για τον υπολογισμό της τιμής $\phi(n)$ όταν γνωρίζουμε την κανονική παραγοντοποίηση του n.

Πρόταση 12. *Έστω n ένας φυσικός αριθμός με κανονική παραγοντοποίηση*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

όπου $p_1, p_2, \ldots, p_k$ είναι πρώτοι αριθμοί και $a_1, a_2, \ldots, a_k$ είναι φυσικοί αριθμοί. Τότε

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}).$$

Παράδειγμα: Να βρεθούν οι παρακάτω τιμές του $\phi(n)$.

- Για $n = 120$ είναι $120 = 2^3 \cdot 3 \cdot 5$, οπότε

  $$\phi(120) = \phi(2^3)\phi(3)\phi(5) = (2^3 - 2^2)(3-1)(5-1) = 4 \cdot 2 \cdot 4 = 32.$$

  Επομένως, υπάρχουν 32 αριθμοί μικρότεροι από το 120 που είναι σχετικά πρώτοι με αυτό.

- Για $n = 6!$ είναι $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 = 2^4 \cdot 3^2 \cdot 5$, οπότε

  $$\phi(6!) = \phi(2^4)\phi(3^2)\phi(5) = (2^4 - 2^3)(3^2 - 3^1)(5-1) = 8 \cdot 6 \cdot 4 = 192.$$

  Επομένως, υπάρχουν 192 αριθμοί μικρότεροι από το $6! = 720$ που είναι σχετικά πρώτοι με αυτό.

3.2.2 Θεώρημα Euler-Fermat

Πρόταση 13 (Θεώρημα του Euler). *Αν a, m είναι φυσικοί αριθμοί και $ΜΚΔ(a, m) = 1$, τότε ισχύει ότι*

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

Με τη βοήθεια του θεωρήματος του Euler προκύπτει η επόμενη πρόταση.

Πρόταση 14 (Μικρό θεώρημα του Fermat). *Αν p είναι πρώτος αριθμός και n φυσικός αριθμός, τότε*

$$n^p \equiv n \pmod{p}.$$

Εφαρμογές

Εφαρμογή 3.5. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$3^{1000} \equiv x \pmod{41}.$$

Λύση. Επειδή $\text{ΜΚΔ}(41, 3) = 1$, έπεται ότι

$$3^{\phi(41)} = 1 \pmod{41}.$$

Ο 41 είναι πρώτος, οπότε $\phi(41) = 41 - 1 = 40$.
Επομένως, $3^{40} \equiv 1 \pmod{41}$, οπότε

$$3^{1000} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1 \pmod{41}. \qquad \square$$

Εφαρμογή 3.6. *Να αποδειχθεί ότι $7 \mid a^{55} - a$, για κάθε ακέραιο a.*

Λύση. Αρκεί να αποδειχθεί ότι

$$a^{55} \equiv a \pmod{7}.$$

Πράγματι

$$7 \mid a^{55} - a \text{ ανν } a^{55} - a \equiv 0 \pmod{7}.$$

Επειδή το 7 είναι πρώτος αριθμός, από το μικρό θεώρημα του Fermat, προκύπτει ότι

$$a^7 \equiv a \pmod 7.$$

Επομένως

$$a^{55} \equiv (a^7)^7 \cdot a^6 \equiv a^7 \cdot a^6 \equiv a \cdot a^6 \equiv a^7 \equiv a \pmod 7.$$

Για παράδειγμα, ισχύει ότι $7 \mid 2^{55} - 2$. □

Εφαρμογή 3.7. *Να αποδειχθεί ότι* $30 \mid a^{25} - a$*, για κάθε ακέραιο* a*.*

Λύση. Παρατηρούμε ότι $30 = 2 \cdot 3 \cdot 5$, οπότε αρκεί να αποδειχθεί ότι

$$2 \mid a^{25} - a, \qquad 3 \mid a^{25} - a, \qquad 5 \mid a^{25} - a$$

ή ισοδύναμα ότι

$$a^{25} \equiv a \pmod 2,$$
$$a^{25} \equiv a \pmod 3,$$
$$a^{25} \equiv a \pmod 5.$$

Πράγματι, επειδή $2, 3, 5$ είναι πρώτοι, από το μικρό θεώρημα του Fermat, προκύπτει ότι

$$a^2 \equiv a \pmod 2,$$
$$a^3 \equiv a \pmod 3,$$
$$a^5 \equiv a \pmod 5,$$

οπότε

$$a^{25} \equiv (a^2)^{12} \cdot a \equiv a^{12} \cdot a \equiv (a^2)^6 \cdot a \equiv a^6 \cdot a \equiv (a^2)^3 \cdot a \equiv a^3 \cdot a \equiv a^4$$
$$\equiv (a^2)^2 \equiv a^2 \equiv a \pmod 2$$

$$a^{25} \equiv (a^3)^8 \cdot a \equiv a^8 \cdot a \equiv a^9 \equiv (a^3)^3 \equiv a^3 \equiv a \pmod 3$$

$$a^{25} \equiv (a^5)^5 \equiv a^5 \equiv a \pmod 5.$$

Επομένως, $30 \mid a^{25} - a$ για κάθε ακέραιο a. □

3.2.3 Ασκήσεις προς επίλυση

1. Για ποιους φυσικούς αριθμούς m ισχύουν οι ισοδυναμίες

   i. $35 \equiv 2 \pmod{m}$.
   ii. $1000 \equiv 1 \pmod{m}$.
   iii. $347 \equiv 0 \pmod{m}$.

2. Να βρεθεί η τιμή της συνάρτησης ϕ για τους φυσικούς αριθμούς

   i. 31, 125, 55, 124, 650, 7!, 10!, $\binom{10}{6}$.
   ii. 2^m, 30^m, 20^{10m}, $2^m 3^n$, $10^m 20^n$, όπου $m, n \in \mathbb{N}^*$.

3. Να βρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί τις εξισώσεις

   i. $x \equiv 2^{303} \pmod{7}$.
   ii. $x \equiv 15^{101} \pmod{8}$.
   iii. $x \equiv 15^{2011} \pmod{3}$.
   iv. $x \equiv 20^{640} \pmod{17}$.
   v. $x \equiv 20^{322} \pmod{17}$.
   vi. $x \equiv 11^{481} \pmod{45}$.
   vii. $x \equiv 13^{802} \pmod{55}$.

4. Να δειχθεί ότι ο 13 διαιρεί τον $2^{70} + 3^{70}$.

5. Να δειχθεί ότι ο 44 διαιρεί τον $19^{19} + 69^{69}$.

6. Να δειχθεί ότι ο $11 \cdot 31 \cdot 61$ διαιρεί τον $20^{15} - 1$.

3.2.4 Εφαρμογές των ισοτιμιών

Η έννοια της ισοτιμίας έχει πολλές εφαρμογές τόσο σε μαθηματικές όσο και σε καθημερινές χρήσεις.

1. **Έλεγχος εγκυρότητας ISBN.** Μια καθημερινή χρήση της ιδέας της ισοτιμίας είναι στην κατασκευή των αριθμών ISBN (International System Book Number) οι οποίοι είναι μοναδικοί για κάθε βιβλίο. Οι αριθμοί ISBN πριν το 2007 ήταν 10ψήφιοι αριθμοί (ISBN–10), ενώ μετά την 1η Ιανουαρίου 2007, έχουν γίνει 13ψήφιοι (ISBN–13). Τα ψηφία των αριθμών ISBN–10 χωρίζονται σε 4 ομάδες μεταβλητού μήκους, οι οποίες διαχωρίζονται από παύλες $-$. Για παράδειγμα, ένας αριθμός ISBN-10 είναι ο επόμενος:

   $$0 - 486 - 27709 - 7,$$

   ενώ τα ψηφία των αριθμών ISBN-13 χωρίζονται σε 5 ομάδες[1], για παράδειγμα

   $$978 - 960 - 7996 - 33 - 6.$$

   Στους αριθμούς ISBN–10 τα ψηφία της πρώτης ομάδας κωδικοποιούν την χώρα ή την περιοχή ή τις περιοχές που ομιλείται μια συγκεκριμένη γλώσσα στην οποία ανήκει ο εκδότης του βιβλίου. Για παράδειγμα, το 0 κωδικοποιεί τις χώρες με γλώσσα τα Αγγλικά, ενώ το 960 κωδικοποιεί τις Ελληνικές εκδόσεις.

   Τα ψηφία της δεύτερης ομάδας κωδικοποιούν τον εκδότη αυτής της περιοχής.

   Τα ψηφία της τρίτης ομάδας κωδικοποιούν ένα συγκεκριμένο βιβλίο.

   Τέλος, στην τέταρτη ομάδα περιέχεται μόνο ένα ψηφίο, το οποίο είναι ψηφίο ελέγχου, και υπολογίζεται από τα υπόλοιπα ψηφία. Στο ISBN–10 το τελευταίο ψηφίο υπολογίζεται ώστε το άθροισμα των ψηφίων του αριθμού ISBN–10 πολλαπλασιασμένα με κατάλληλους αριθμούς να είναι ισότιμο 0 mod 11. Συγκεκριμένα, για τον αριθμό ISBN–10

   $$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$$

   ισχύει ότι

   $$10x_1+9x_2+8x_3+7x_4+6x_5+5x_6+4x_7+3x_8+2x_9+1\cdot x_{10} \equiv 0 \bmod 11.$$

[1] Η πρώτη ομάδα προστέθηκε επειδή θα εξαντληθούν οι αριθμοί ISBN–10· μέχρι σήμερα η πρώτη ομάδα του ISBN–13 περιέχει τα ψηφία 978.

Πράγματι, για τον αριθμό ISBN–10 0-486-27709-7 ισχύει ότι

$$10{\cdot}0{+}4{\cdot}9{+}8{\cdot}8{+}7{\cdot}6{+}6{\cdot}2{+}5{\cdot}7{+}4{\cdot}7{+}3{\cdot}0{+}2{\cdot}9{+}1{\cdot}7 = 242 \equiv 0 \pmod{11},$$

αφού $242 = 22 \cdot 11$.

Χρησιμοποιώντας τις ιδιότητες των υπολοίπων μπορούμε να δείξουμε ότι το δέκατο ψηφίο x_{10} μπορεί να υπολογισθεί από τον τύπο

$$x_{10} = (1{\cdot}x_1{+}2{\cdot}x_2{+}3{\cdot}x_3{+}4{\cdot}x_4{+}5{\cdot}x_5{+}6{\cdot}x_6{+}7{\cdot}x_7{+}8{\cdot}x_8{+}9{\cdot}x_9) \bmod 11.$$

Επειδή τα δυνατά υπόλοιπα της διαίρεσης ενός αριθμού με το 11 είναι 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 στην περίπτωση που $x_{10} = 10$ χρησιμοποιείται αντ᾽ αυτού το γράμμα X.

Αποδεικνύεται ότι ο κώδικας αυτός αναγνωρίζει όχι μόνο σφάλματα σε κάποιο ψηφίο αλλά και σφάλματα αντιμετάθεσης, όπως για παράδειγμα να γράψουμε 14 αντί για 41.

Στον ISBN–13 το τελευταίο ψηφίο δίνεται με διαφορετικό τρόπο. Συγκεκριμένα για τον αριθμό ISBN–13

$$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}$$

ισχύει ότι

$$\begin{aligned} x_{13} = (10 - (x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 \\ +3x_{10} + x_{11} + 3x_{12}) \bmod 10) \bmod 10. \end{aligned}$$

Ο κώδικας αυτός, σε αντίθεση με τον ISBN–10 δεν εντοπίζει πάντα σφάλματα αντιμετάθεσης.

2. **Έλεγχος εγκυρότητας ΑΦΜ.** Η ίδια ιδέα με τον αριθμό ISBN βρίσκεται στην κατασκευή των αριθμών φορολογικού μητρώου (ΑΦΜ). Οι ΑΦΜ είναι 9 ψήφιοι αριθμοί στους οποίους το τελευταίο ψηφίο είναι ψηφίο ελέγχου.

Συγκεκριμένα, σε κάθε ΑΦΜ $x_1x_2x_3x_4x_5x_6x_7x_8x_9$ ισχύει ότι

$$x_9 = ((x_8{\cdot}2^1{+}x_7{\cdot}2^2{+}x_6{\cdot}2^3{+}x_5{\cdot}2^4{+}x_4{\cdot}2^5{+}x_3{\cdot}2^6{+}x_2{\cdot}2^7{+}x_1{\cdot}2^8) \bmod 11) \bmod 10.$$

Για παράδειγμα, ο αριθμός 123456783 ανήκει στους παραπάνω αριθμούς αφού

$$8 \cdot 2^1 + 7 \cdot 2^2 + 6 \cdot 2^3 + 5 \cdot 2^4 + 4 \cdot 2^5 + 3 \cdot 2^6 + 4 \cdot 2^7 + 1 \cdot 2^8 = 1004.$$

Ισχύει ότι $1004 = 91 \cdot 11 + 3$ άρα $1004 \bmod 11 = 3$ και $3 \bmod 10 = 3 = x_9$.

Φυσικά, ο παραπάνω έλεγχος είναι έλεγχος ορθότητας και δεν ελέγχει αν αυτός ο αριθμός είναι σε χρήση ή όχι.

3. Το σύστημα κρυπτογράφησης RSA

Το σύστημα κρυπτογράφησης RSA επινοήθηκε το 1976 από τους Ronald **R**ivest, Adi **S**hamir και Leonard **A**dleman. Βασίζεται στην εξής ιδέα:

Έστω p, q δύο πρώτοι αριθμοί και $n = pq$.

Επίσης, έστω e ένας αριθμός έτσι ώστε $\text{ΜΚΔ}((p-1)(q-1), e) = 1$. Τότε υπάρχει αριθμός d έτσι ώστε $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Για παράδειγμα, αν $p = 43$ και $q = 47$, τότε $n = 2021$.

Επίσης, για $e = 13$ ισχύει ότι $\text{ΜΚΔ}((43-1)(47-1), 13) = 1$. Τότε, ο αντίστροφος του $e = 13$ modulo (43-1)(47-1) = 1932 είναι το $d = 1189$.

Από το θεώρημα του Euler, για κάθε φυσικό αριθμό M με $\text{ΜΚΔ}(M, n) = 1$ ισχύει η ιδιότητα

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

Όμως

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1),$$

και επομένως

$$M^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

Η παραπάνω ισοτιμία είναι η κεντρική ιδέα του αλγορίθμου RSA.

Ο παραλήπτης Π του κρυφού μηνύματος επιλέγει δύο πρώτους αριθμούς p, q και υπολογίζει το γινόμενο $n = pq$, καθώς και την τιμή $\phi(n) = (p-1)(q-1)$. Επιπλέον, επιλέγει έναν αριθμό e, τέτοιον ώστε $\gcd(e, \phi(n)) = 1$ και υπολογίζει τον αντίστροφο d του e modulo $\phi(n)$, δηλαδή $ed \equiv 1 \pmod{\phi(n)}$. Τέλος, στέλνει τους αριθμούς n, e σε αυτόν που πρόκειται να στείλει το μήνυμα. Ο αποστολέας Α επιλέγει το μήνυμα M που θα

στείλει στον Π, τέτοιο ώστε $\gcd(M, n) = 1$. Αυτή η συνθήκη προφανώς ισχύει πάντα, εκτός αν το M είναι πολλαπλάσιο του p ή του q. Επειδή ως p, q επιλέγονται μεγάλοι πρώτοι, μπορεί να υποτεθεί ότι το M είναι πάντα μικρότερο από αυτούς.

Στη συνέχεια υπολογίζει το κρυπτογραφημένο μήνυμα C από τη σχέση

$$C \equiv M^e \pmod{n},$$

το οποίο και στέλνει.

Ο Π αποκωδικοποιεί το C με τη βοήθεια του d, το οποίο γνωρίζει μόνο αυτός, βάσει της σχέσης

$$M \equiv C^d \pmod{n}.$$

Πράγματι, βάσει του Θεωρήματος Euler-Fermat δεδομένου ότι υπάρχει ακέραιος k τέτοιος ώστε $ed = k\phi(n) + 1$, είναι

$$C^d \equiv M^{ed} \equiv M^{k\phi(n)+1} \equiv M \pmod{n}.$$

Για το προηγούμενο παράδειγμα, για να στείλει με ασφάλεια ο Α το μήνυμα $M = 501$ στον Π, αρκεί να στείλει το αποτέλεσμα

$$C = 501^{13} \pmod{2021} = 77.$$

Ο Π για να διαβάσει το μήνυμα M, αρκεί να υπολογίσει το αποτέλεσμα

$$77^{1189} \pmod{2021} = 501.$$

Η ασφάλεια του συστήματος RSA βασίζεται στην δυσκολία παραγοντοποίησης ενός αριθμού n της μορφής $n = pq$, όταν οι p, q έχουν εκατοντάδες ψηφία. Ακόμη και αν κάποιος υποκλέψει το κρυπτογραφημένο μήνυμα C είναι επίσης δύσκολο να λυθεί το πρόβλημα υπολογισμού κάποιου X έτσι ώστε $X^e = C \pmod{n}$.

Πώς όμως υπολογίζεται ο d ώστε $ed \equiv 1 \pmod{\varphi(n)}$; Με τη βοήθεια του εκτεταμένου αλγορίθμου του Ευκλείδη. Ο αλγόριθμος του Ευκλείδη, προκειμένου να υπολογίσει τον ΜΚΔ(a, b), θέτει αρχικά $r_0 =$

$\max\{|a|,|b|\}$ και $r_1 = \min\{|a|,|b|\}$ και εκτελεί ℓ σε πλήθος διαιρέσεις

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{\ell-2} &= r_{\ell-1} q_{\ell-1} + r_\ell \\ r_{\ell-1} &= r_\ell q_\ell + r_{\ell+1} \end{aligned}$$

υπολογίζοντας κατά την i-οστή διαίρεση, $i = 0, 1, \ldots, \ell-1$, το πηλίκο q_i και το νέο υπόλοιπο r_{i+1}. Το τελευταίο υπόλοιπο $r_{\ell+1}$ ισούται με 0, ενώ το r_ℓ ισούται με τον $\text{ΜΚΔ}(a,b)$.

Αν κατά την i-οστή διαίρεση υπολογίζουμε επιπλέον τους αριθμούς s_{i+1}, t_{i+1}, βάσει των τύπων

$$s_{i+1} = s_{i-1} - s_i q_i, \qquad t_{i+1} = t_{i-1} - t_i q_i, \qquad i \geq 1$$

και με αρχικές τιμές

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

τότε μπορούμε να δείξουμε με επαγωγή (άσκηση) ότι για κάθε i ισχύει $r_i = s_i a + t_i b$. Τότε όμως είναι

$$\text{ΜΚΔ}(a,b) = r_\ell = s_\ell a + t_\ell b$$

δηλαδή για $a = e$ και $b = \varphi(n)$, έχουμε

$$1 = \text{ΜΚΔ}(e, \varphi(n)) = s_\ell e + t_\ell \varphi(n)$$

οπότε $s_\ell e \equiv 1 \pmod{\varphi(n)}$, δηλαδή το ζητούμενο d ισούται με το s_ℓ.

Ασκήσεις προς επίλυση

1. Να βρεθεί ποιο είναι το ψηφίο ελέγχου για τους επόμενους αριθμούς ISBN–10: $960-351-034-?$, $960-7510-22-?$, $960-524-225-?$. και να ελεγχθεί αν οι επόμενοι αριθμοί ISBN–10 είναι έγκυροι: $0-486-65537-7$, $960-7778-74-8$.

2. Να γραφεί πρόγραμμα που υπολογίζει το τελευταίο ψηφίο των αριθμών ISBN–10 και ISBN–13.

3. Να γραφεί πρόγραμμα που να ελέγχει την εγκυρότητα ενός αριθμού ΑΦΜ.