Θεωρία αριθμών

Μαθηματικά των Υπολογιστών

2023-2024

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

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

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

Άσκηση 1

Να βρεθεί ο ΜΚΔ των 12075 *και* 4655.

Λύση.

Έχουμε ότι

$$\begin{aligned} 12075 &= 2 \cdot 4655 + 2765 \\ 4655 &= 1 \cdot 2765 + 1890 \\ 2765 &= 1 \cdot 1890 + 875 \\ 1890 &= 2 \cdot 875 + 140 \\ 875 &= 6 \cdot 140 + 35 \\ 140 &= 4 \cdot 35 + 0. \end{aligned}$$

Άρα, $\text{ΜΚΔ}(12075, 4655) = 35$. □

Η γραμμική διοφαντική εξίσωση

$$ax + by = c$$

έχει λύση, αν και μόνο αν $\gcd(a, b) \mid c$.
Επιπλέον, αν (x_0, y_0) είναι μια λύση της, τότε κάθε λύση της είναι της μορφής

$$(x, y) = (x_0 + \lambda \frac{b}{\gcd(a, b)}, y_0 - \lambda \frac{a}{\gcd(a, b)}), \text{όπου } \lambda \in \mathbb{Z}.$$

Επιπρόσθετα, η (απλούστερη) εξίσωση

$$\frac{a}{\gcd(a, b)} x + \frac{b}{\gcd(a, b)} y = \frac{c}{\gcd(a, b)}$$

έχει τις ίδιες ακέραιες λύσεις.

Άσκηση 2

Να λυθούν οι διοφαντικές εξισώσεις:

α) $12075x + 4655y = 105.$

β) $12075x - 4655y = 70.$

Άσκηση 3

Να βρεθούν όλες οι ακέραιες λύσεις της διοφαντικής εξίσωσης

$$500x + 68y + 30z = 18.$$

Παρατηρούμε ότι για κάθε $x, y \in \mathbb{Z}$ ισχύει ότι

$$500x + 68y = \gcd(500, 68) \cdot r_1 \text{ για κάποιο ακέραιο } r_1.$$

Επομένως, η εξίσωση $500x + 68y + 30z = 18$ είναι ισοδύναμη με το σύστημα εξισώσεων

$$\begin{cases} 500x + 68y = \gcd(500, 68) \cdot r_1 \\ \gcd(500, 68) \cdot r_1 + 30z = 18 \end{cases}$$

Με τον αλγόριθμο του Ευκλείδη υπολογίζουμε τον μκδ των 500 και 68:

$$\begin{aligned} 500 &= 7 \cdot 68 + 24 \\ 68 &= 2 \cdot 24 + 20 \\ 24 &= 1 \cdot 20 + 4 \\ 20 &= 5 \cdot 4 + 0 \end{aligned}$$

Άρα, $\gcd(500, 68) = 4$.
Άρα, η εξίσωση $500x + 68y + 30z = 18$ είναι ισοδύναμη με το σύστημα εξισώσεων

$$\begin{cases} 500x + 68y = 4r_1 \\ 4r_1 + 30z = 18 \end{cases}$$

Χρησιμοποιώντας τον επεκτεταμένο αλγόριθμο του Ευκλείδη βρίσκουμε τις λύσεις της πρώτης εξίσωσης του συστήματος:

$$\begin{aligned} 4 &= 1 \cdot 24 + (-1)20 = 1 \cdot 24 + (-1)(1 \cdot 68 + (-2) \cdot 24) \\ &= (-1) \cdot 68 + 3 \cdot 24 = (-1) \cdot 68 + 3 \cdot (1 \cdot 500 + (-7) \cdot 68) \\ &= 3 \cdot 500 + (-22) \cdot 68. \end{aligned}$$

Άρα, το ζεύγος $(x, y) = (3, -22)$ είναι λύση της εξίσωσης $500x + 68y = 4$. Πολλαπλασιάζοντας με r_1 προκύπτει ότι το ζεύγος $(x, y) = (3r_1, -22r_1)$ είναι λύση της εξίσωσης $500x + 68y = 4r_1$. Επομένως, οι λύσεις της εξίσωσης $500x + 68y = 4r_1$ είναι όλα τα ζεύγη (x, y) της μορφής

$$\begin{aligned} (x, y) &= (3r_1 - \frac{68}{4}\lambda_1, -22r_1 + \frac{500}{4}\lambda_1) \\ &= (3r_1 - 17\lambda_1, -22r_1 + 125\lambda_1), \text{ όπου } \lambda_1 \in \mathbb{Z}. \end{aligned}$$

Πάλι χρησιμοποιώντας τον επεκτεταμένο αλγόριθμο του Ευκλείδη βρίσκουμε τις λύσεις της δεύτερης εξίσωσης του συστήματος:

$$30 = 7 \cdot 4 + 2$$
$$4 = 2 \cdot 2 + 2.$$

Άρα, $\gcd(30, 4) = 2$ και $2 \mid 18$. Επίσης, άμεσα έχουμε ότι

$$2 = 1 \cdot 30 + (-7) \cdot 4.$$

Άρα, το ζεύγος $(r_1, z) = (-7, 1)$ είναι λύση της εξίσωσης $4r_1 + 30z = 2$. Πολλαπλασιάζοντας με 9 προκύπτει ότι το ζεύγος $(r_1, z) = (-63, 9)$ είναι λύση της εξίσωσης $4r_1 + 30z = 18$. Επομένως, οι λύσεις της εξίσωσης $4r_1 + 30z = 18$ είναι όλα τα ζεύγη (r_1, z) της μορφής

$$(r_1, z) = (-63 + \frac{30}{2}\lambda_2, 9 - \frac{4}{2}\lambda_2) = (-63 + 15\lambda_2, 9 - 2\lambda_2), \text{ όπου } \lambda_2 \in \mathbb{Z}.$$

Για να βρούμε τις λύσεις της αρχικής εξίσωσης $500x + 68y + 30z = 18$ αρκεί να απαλείψουμε την βοηθητική μεταβλητή r_1:

$$x = 3r_1 - 17\lambda_1 = 3(-63 + 15\lambda_2) - 17\lambda_1 = -189 + 45\lambda_2 - 17\lambda_1$$

$$y = -22r_1 + 125\lambda_1 = -22(-63 + 15\lambda_2) + 125\lambda_1 = 1386 - 330\lambda_2 + 125\lambda_1$$

$$z = 9 - 2\lambda_2$$

Τελικά, οι λύσεις τις εξίσωσης $500x + 68y + 30z = 18$ είναι οι τριάδες της μορφής

$(x, y, z) = (-189+45\lambda_2-17\lambda_1, 1386-330\lambda_2+125\lambda_1, 9-2\lambda_2)$ όπου $\lambda_1, \lambda_2 \in \mathbb{Z}$

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).
Ισοδύναμα, 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.

Αν n είναι ένας σταθερός φυσικός αριθμός και a, b, c, d ακέραιοι, τότε:

- Αν $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$, τότε

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

- Αν $a \equiv b \pmod{n}$, τότε

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

- Αν $a \equiv b \pmod{n}$, τότε

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

- 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

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

Άσκηση 4 (Έλεγχος εγκυρότητας 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*

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

Να εξετασθεί αν ο αριθμός 123456783 *ανήκει στους παραπάνω αριθμούς.*

Πράγματι,

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

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.

Θεώρημα Euler - Fermat

Αν a, m είναι φυσικοί αριθμοί και $\text{ΜΚΔ}(a, m) = 1$, τότε ισχύει ότι

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

όπου $\phi(n)$ είναι 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.

- 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 $\text{ΜΚΔ}(m, n) = 1$. Τότε $\phi(mn) = \phi(m)\phi(n)$.
- Αν $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ όπου $p_1, p_2, \ldots, p_k$ είναι πρώτοι αριθμοί και $a_1, a_2, \ldots, a_k$ είναι φυσικοί αριθμοί. Τότε

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

Άσκηση 5

Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση

$$x \equiv 17^{812} \pmod{110}.$$

Λύση.

Επειδή $\gcd(110, 17) = 1$, έπεται ότι

$$17^{\phi(110)} \equiv 1 \pmod{110}.$$

Επίσης, $\phi(110) = \phi(2 \cdot 5 \cdot 11) = 1 \cdot 4 \cdot 10 = 40$.
Επομένως, $17^{40} \equiv 1 \pmod{110}$, οπότε

$$\begin{aligned} x &\equiv 17^{812} \equiv 17^{20 \cdot 40 + 12} \equiv (17^{40})^{20} \cdot 17^{12} \equiv 1^{20} \cdot 17^{12} \\ &\equiv 17^{12} \equiv (17^2)^6 \equiv 289^6 \equiv 69^6 \equiv (69^2)^3 \equiv 4761^3 \\ &\equiv 31^3 \equiv 31 \cdot 31^2 \equiv 31 \cdot 961 \equiv 31 \cdot 81 \equiv 2511 \equiv 91 \pmod{110}. \end{aligned}$$

□

Άσκηση 6

Να δειχθεί ότι το 44 *διαιρεί τον* $19^{19} + 69^{69}$.

Έστω a, n δύο ακέραιοι αριθμοί με $n \geq 2$.

- Ο a έχει αντίστροφο modulo n αν και μόνο αν $\gcd(a, n) = 1$.
- Επιπλέον, αν s, t είναι ακέραιοι ώστε $as + tn = 1$ τότε ο s είναι ένας αντίστροφος του a modulo n.
- Επιπρόσθετα, $s = \pi n + \upsilon$, όπου $0 < \upsilon < n$ τότε ο υ είναι ο μοναδικός αντίστροφος του a modulo n στο διάστημα $[n - 1]$.

Άσκηση 7

α) Να βρεθεί, εφόσον υπάρχει, ο αντίστροφος του 7 modulo 18
β) Να λυθεί η εξίσωση $7x \equiv 5 \bmod 18$.

α) Επειδή $\gcd(7, 18) = 1$, ο αντίστροφος του 7 modulo 18 υπάρχει.
Για να τον υπολογίσουμε, αρχικά εκτελούμε τις διαιρέσεις των βημάτων του αλγορίθμου του Ευκλείδη.

$$\begin{aligned} 18 &= 2 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1, \end{aligned}$$

έπειτα λύνουμε τις ισότητες ως προς τα υπόλοιπα κάθε διαίρεσης

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ 3 &= 7 - 1 \cdot 4 \\ 4 &= 18 - 2 \cdot 7, \end{aligned}$$

και στη συνέχεια κάνουμε διαδοχικές αντικαταστάσεις των πηλίκων και υπολοίπων, όπως παρακάτω:

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) = -1 \cdot 7 + 2 \cdot 4 \\ &= -1 \cdot 7 + 2 \cdot (18 - 2 \cdot 7) \\ &= -5 \cdot 7 + 2 \cdot 18 \\ &= (13 - 18) \cdot 7 + 2 \cdot 18 \\ &= 13 \cdot 7 + 1 \cdot 18. \end{aligned}$$

Επομένως, ο αντίστροφος του 7 modulo 18 είναι το 13.
Πράγματι, $7 \cdot 13 = 91$ και $91 \equiv 1 \bmod 18$, αφού $91 - 1 = 5 \cdot 18$.
β) Πολλαπλασιάζοντας την εξίσωση κατά μέλη με το 13 έχουμε ότι

$$x \equiv 5 \cdot 13 \equiv 65 \equiv 11 \bmod 18.$$

Άρα, οι λύσεις της εξίσωσης είναι όλα τα $x = 11 + 18k$, $k \in \mathbb{Z}$.