Θεωρία αριθμών

Μαθηματικά των Υπολογιστών

Σήμερα: • Αλγόριθμος Ευκλείδη & την επέκταση του

2024–2025

- Γραμμικές Διοφαντικές Εξισώσεις
- Θεώρημα Euler-Fermat
- Αντιστροφή modulo n

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

α) *Να βρεθεί ο ΜΚΔ των* 12075 *και* 4655.

Λύση.

Έχουμε ότι

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

Άρα, $\mathrm{MK\Delta}(12075, 4655) = 35$. □

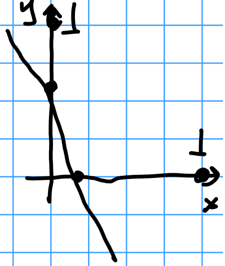
β) Να εκφραστεί ο ΜΚΔ(12075, 4655) ως γραμμικός συνδυασμός των 12075, 4655

$$
\begin{aligned}
35 &= 1\cdot 875 + (-6)\cdot 140 \\
&= 1\cdot 875 + (-6)\cdot\left(1\cdot 1890 + (-2)\cdot 875\right) \\
&= (-6)\cdot 1890 + 13\cdot 875 \\
&= (-6)\cdot 1890 + 13\cdot\left(1\cdot 2765 + (-1)\cdot 1890\right) \\
&= 13\cdot 2765 + (-19)\cdot 1890 \\
&= 13\cdot 2765 + (-19)\cdot\left(1\cdot 4655 + (-1)\cdot 2765\right) \\
&= (-19)\cdot 4655 + 32\cdot 2765 \\
&= (-19)\cdot 4655 + 32\cdot\left(1\cdot 12075 + (-2)\cdot 4655\right) \\
&= 32\cdot 12075 + (-83)\cdot 4655
\end{aligned}
$$

Άρα, $\boxed{32\cdot 12075 + (-83)\cdot 4655 = 35}$

γ) Να λυθούν οι γραμμικές διοφαντικές εξισώσεις

$$12075x + 4655y = 105 \quad (*)$$



Από το α) υπολογίσαμε ότι

$$\gcd(12075, 4655) = 35$$

Επειδή $35 \mid 105$ η εξίσωση έχει λύσεις.

Από το β) υπολογίσαμε ακεραίους s, t ώστε

$$12075s + 4655t = 35$$

και βρήκαμε

$$12075\cdot 32 + 4655\cdot(-83) = 35$$

$\lambda=1$

$\boxed{(-37, 96)}$

Άρα πολλαπλασιάζοντας επί 3 έχουμε

$$12075\cdot 96 + 4655\cdot(-249) = 105$$

Άρα, μία λύση της εξίσωσης $(*)$ είναι το ζευγάρι

$$(x_0, y_0) = (96, -249)$$

Άρα, οι λύσεις της εξίσωσης $(*)$ είναι τα ζεύγη $\lambda \in \mathbb{Z}$

$$(x,y) = \left(96 - \lambda\frac{4655}{35}, -249 + \lambda\frac{12075}{35}\right) = (96 - 133\lambda, -249 + 345\lambda)$$

Η γραμμική διοφαντική εξίσωση

$$\alpha x_0 + b y_0 = \gcd(\alpha, b)$$

$$\Rightarrow \alpha(kx_0) + b(ky_0) = c$$

$$ax + by = c$$

$$\frac{c}{\gcd(\alpha, b)} = k \in \mathbb{Z}$$

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

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

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) $\boxed{12075x - 4655y = 70.}$

Θέτουμε $\boxed{-y = z}$. Λύνουμε την εξίσωση

$$12075x + 4655z = 70 \qquad \ast$$

Στο τέλος τα ζεύγη (x, z) γίνονται $(x, -y)$

Άρα, οι λύσεις (x, y) είναι $(x, -z)$.

$$(x, y) = (x, -z) = \ldots$$

Μια λύση της (*) είναι

$$12075 \cdot (2 \cdot 32) + 4655 \cdot (2 \cdot (-83)) = 2 \cdot 35$$
$$12075 \cdot 64 + 4655 \cdot (-166) = 70$$

Το ζευγάρι $\boxed{(x_0, z_0) = (64, -166)}$

Άρα, οι λύσεις της (*) είναι

$$(x, z) = \left(64 + \lambda \frac{4655}{35}, -166 - \lambda \frac{12075}{35}\right)$$
$$= (64 + 133\lambda, \boxed{-166 - 345\lambda}) \quad \lambda \in \mathbb{Z}$$

Άρα οι λύσεις της $12075x - 4655y = 70$ είναι τα ζεύγη

$$(x, y) = (x, -z) = (64 + 133\lambda, \boxed{166 + 345\lambda}) \quad \lambda \in \mathbb{Z}.$$

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

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

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

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

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

$$\begin{aligned} 30 &= 7 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 2. \end{aligned}$$

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

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

$n = 2k + 1, \; k \in \mathbb{Z}$

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

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

Andrew Wiles 1992

Τελευταια εικασια του Fermat

Αν $n \geq 3$ η $x^n + y^n = z^n$ δεν εχει ακεραιες μη μηδενικες λυσεις

$x^2 + y^2 = z^2$

$x^3 + y^3 = z^3$ $\quad 0^3 + 0^3 = 0^3$

$x^4 + y^4 = z^4$ $\quad 1^3 + 0^3 = 1^3$

Gauss

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

43432234X

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 Να βρεθεί ο ελάχιστος φυσικός αριθμός x ο οποίος είναι λύση της εξίσωσης

$$x \equiv 11^{2023} \mod 200$$

Αρχικά θα υπολογίσουμε τον ΜΚΔ(200, 11)

$$200 = 18 \cdot 11 + 2$$
$$11 = 5 \cdot 2 + 1$$

Άρα, ΜΚΔ(200, 11) = 1

Άρα, από το Θεώρημα Euler-Fermat ισχύει ότι

$$\boxed{11^{\varphi(200)} \equiv 1 \mod 200}$$

Θα υπολογίσουμε το φ(200). Θα βρούμε τους πρώτους παράγοντες του 200

$$200 = 2 \cdot 100 = 2^2 \cdot 50 = 2^3 \cdot 25 = 2^3 \cdot 5^2$$

2, 5 πρώτοι

Άρα $\varphi(200)=\varphi(2^3)\cdot\varphi(5^2)=(2^3-2^2)(5^2-5^1)$

$=(8-4)\cdot(25-5)$

$=4\cdot 20=80$

Επομένως $\boxed{11^{80}\equiv 1 \bmod 200}$

$11^{40}\equiv 1 \bmod 200$

$11^{20}\equiv 1 \bmod 200$

$11^{10}\equiv 1 \bmod 200$

Βάσει αυτών:

$x\equiv 11^{2023}\equiv (11^{80})^{25}\cdot 11^{23} \pmod{200}$

$\equiv 1^{25}\cdot 11^{23}\equiv (11^2)^{11}\cdot 11$

Θ. Lagrange

$\boxed{11^{10}\equiv 1 \bmod 200}$

$11^{23}\equiv (11^{10})^2\cdot 11^3 \bmod 200$

$\equiv 1\cdot 11^3\equiv 121\cdot 11\equiv 1331$

$\equiv 1200+131$

$\equiv 0+131\equiv 131$

$\bmod 200$

$\equiv (121)^{11}\cdot 11\equiv (121^2)^5\cdot 121\cdot 11$

$\equiv 14641^5\cdot 1331\equiv 41^5\cdot 131\equiv 41^2\cdot 41^2\cdot 41\cdot 131$

$\equiv 1681\cdot 1681\cdot 5371\equiv$

$\equiv 81\cdot 81\cdot 171\equiv 1121931\equiv 131$

Άρα $\boxed{x=131}$

Σχόλιο Αν $\gcd(\alpha, m) = 1$ τότε

$$\alpha^{\varphi(m)} \equiv 1 \mod m$$

Γενικότερα, αν $\gcd(\alpha, m) = 1$ τότε υπαρχει $k \in \mathbb{N}^*$ ωστε

$$\alpha^k \equiv 1 \mod m$$

και το $\varphi(m)$ ειναι ενα τέτοιο k

Μας ενδιαφερει το μικροτερο δυνατο $k \in \mathbb{N}^*$ ωστε

$$\alpha^k \equiv 1 \mod m$$

Θεώρημα Lagrange Το μικρότερο $k \in \mathbb{N}^*$ ωστε $\alpha^k \equiv 1 \mod m$ ειναι διαιρετης του $\varphi(m)$

Άσκηση 5

Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση

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

Λύση.

n=110

Μέθοδος του υποτετραγωνισμού

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

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

Άσκηση 6

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

Αρκεί να δειχθεί ότι $19^{19} + 69^{69} \equiv 0 \mod 44$

Θα υπολογίσουμε ανεξάρτητα x_1, x_2 ώστε

$$x_1 \equiv 19^{19} \mod 44 \quad \text{και} \quad x_2 \equiv 69^{69} \mod 44$$

ΜΚΔ$(19, 44)$ = ΜΚΔ$(19, 69) = 1$ και

$$\varphi(44) = \varphi(2^2 \cdot 11^1) = (2^2 - 2^1)(11^1 - 11^0) = 2 \cdot 10 = 20$$

Άρα

$$\boxed{19^{20} \equiv 1 \mod 44}$$

και

$$69^{20} \equiv 1 \mod 44$$

Άρα

$$x_2 \equiv 69^{69} \equiv \left(69^{20}\right)^3 \cdot 69^9 \mod 44$$

$$\equiv 1^3 \cdot 69^9 \equiv 69^9 \equiv 25^9 \mod 44$$

$$\equiv (25^2)^4 \cdot 25 \equiv (225)^4 \cdot 25 \equiv 5^4 \cdot 25$$

$$\equiv 255 \cdot 25 \equiv 5 \cdot 25 \equiv 125 \equiv 37 \mod 44$$

$$x_1 \equiv 19^{19} \equiv (19^2)^9 \cdot 19 \equiv 361^9 \cdot 19$$

$$\circledast \quad \equiv 9^9 \cdot 19 \equiv (9^2)^4 \cdot 9 \cdot 19 \equiv 81^4 \cdot 171 \equiv 37^4 \cdot 39$$

$$\equiv (-7)^4 \cdot (-5) \equiv (-7)^2 (-7)^2 \cdot (-5) \equiv 49 \cdot 49 \cdot (-5)$$

$$\equiv 5 \cdot 5 \cdot (-5) \equiv 25 \cdot (-5) \equiv -125 \mod 44$$

Οπότε

$$x_1 + x_2 \equiv -125 + 37 \equiv -88 \equiv 0 \mod 44$$

δηλαδή ισχύει το ζητούμενο

(*) Υπαρχει αλλος ενας γρηγοροτερος τροπος για την ευρεση του x_1 χρησιμοποιωντας τον αντιστροφο του 19 modulo 44

$$44 = 2\cdot 19 + 6$$
$$19 = 3\cdot 6 + 1$$

Άρα

$$1 = 1\cdot 19 + (-3)\cdot 6 = 1\cdot 19 + (-3)\cdot(1\cdot 44 + (-2)\cdot 19)$$
$$= (-3)\cdot 44 + 7\cdot 19$$

δηλαδη $7\cdot 19 + (-3)\cdot 44 = 1$

οποτε $(7\cdot 19 + (-3)\cdot 44) \equiv 1 \mod 44 \iff$

$(7\cdot 19 + 0) \equiv 1 \mod 44 \iff$

$$\boxed{7\cdot 19 \equiv 1 \mod 44}$$

Θ. Euler-Fermat

Άρα, εχουμε

$$x_1 \equiv 19^{19} \pmod{44} \equiv 19^{19}\cdot 1^{1} \equiv 19^{19}(7\cdot 19) \equiv 19^{20}\cdot 7 \equiv 1\cdot 7 \equiv 7$$

Άρα $x_1 \equiv 7 \mod 44$

οποτε

$$x_1 + x_2 \equiv 7 + 37 \equiv 44 \equiv 0 \mod 44$$

δηλαδη ισχυει το ζητουμενο

Έστω n σταθερός φυσικός αριθμός με $n \geq 2$. Οι ακέραιοι αριθμοί a, b ονομάζονται **αντίστροφοι modulo** n αν και μόνο αν $ab \equiv 1 \pmod{n}$.

Για παράδειγμα, οι αριθμοί $5, 3$ είναι αντίστροφοι modulo 7 διότι

$$5 \cdot 3 \equiv 15 \equiv 1 \pmod{7}.$$

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

- Ο a έχει αντίστροφο modulo n αν και μόνο αν $\boxed{\gcd(a, n) = 1.}$
- 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 $\boxed{0 < \upsilon < n}$ τότε ο υ είναι ο μοναδικός αντίστροφος του a modulo n στο διάστημα $[n-1]$.

Άσκηση α) Να λυθεί η εξίσωση

$$x \equiv 15 \bmod 37$$

Από τον ορισμό της ισοτιμίας ισχύει ότι

$$37 \mid x - 15 \iff$$

Υπάρχει $\lambda \in \mathbb{Z}$ ώστε $x - 15 = 37\lambda \iff$

$$x = 15 + 37\lambda, \quad \lambda \in \mathbb{Z}$$

β) Να λυθεί η εξίσωση $x \equiv 83 \bmod 257$

Οι λύσεις είναι όλα τα x της μορφής:

$$x = 83 + 257\lambda, \quad \lambda \in \mathbb{Z}$$

γ) Να λυθεί η ετίσωση $3x \equiv 17 \mod 20$

<u>1ος τρόπος λύσης</u>

$$3x \equiv 17 \mod 20 \iff 20 \mid 3x-17 \iff 3x-17 = 20y$$
$$\iff 3x - 20y = 17 \quad (*)$$

$$20 = 6\cdot 3 + 2$$
$$3 = 1\cdot 2 + 1$$

Άρα $\gcd(20,30) = 1$

$$1 = 1\cdot 3 + (-1)\cdot 2$$
$$= 1\cdot 3 + (-1)\cdot(1\cdot 20 + (-6)\cdot 3)$$
$$= (-1)\cdot 20 + 7\cdot 3$$

οπότε $3\cdot 7 - 20\cdot 1 = 1$

πολ/ζουμε επί 17 $3\cdot 119 - 20\cdot 17 = 17$

Άρα, μια λύση είναι το ζευγάρι $(x_0, y_0) = (119, 17)$, άρα οι λύσεως της ~~(*)~~ (*) είναι $(x,y) = \left(119 - \lambda\frac{-20}{1}, 17 + \frac{3}{1}\lambda\right)$.

Μας ενδιαφέρουν μόνο τα x, επειδή $\boxed{x = 119 + 20\lambda,\ \lambda \in \mathbb{Z}}$

2ος τρόπος λύσης της $3x \equiv 17 \mod 20$

Θα υπολογίσουμε τον αντίστροφο του 3 modulo 20

$$20 = 6 \cdot 3 + 2 \qquad 1 = 1 \cdot 3 + (-1) \cdot 2$$
$$3 = 1 \cdot 2 + 1 \qquad = 1 \cdot 3 + (-1) \cdot (1 \cdot 20 + (-6) \cdot 3)$$
$$= -1 \cdot 20 + 7 \cdot 3$$

Άρα, ο αντίστροφος του 3 modulo 20 είναι το 7

δηλαδή $3 \cdot 7 \equiv 1 \mod 20$

Επομένως

$$3x \equiv 17 \mod 20 \xrightarrow[\text{επί } 7]{\text{πολ/ζουμε}} \quad \left(\begin{array}{c}\text{Δεν αλλάζουν}\\ \text{οι λύσεις}\end{array}\right)$$

$$3 \cdot 7 x \equiv 17 \cdot 7 \mod 20$$

$$x \equiv 119 \mod 20$$

δηλαδή οι λύσεις είναι τα x της μορφής

$$x = 119 + 20\lambda, \quad \lambda \in \mathbb{Z}$$

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

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

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

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

Επειδή $-5 = (-1) \cdot 18 + 13$ όπου $0 < 13 < 18$ έπεται ότι 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 $x = 11 + 18k$, $k \in \mathbb{Z}$.

Άσκηση Να βρεθεί ο ελάχιστος φυσικός x ο οποίος είναι λύση της εξίσωσης

$$x \equiv 19^{19} \mod 44$$

Λύση

$\text{ΜΚΔ}(19,44)=1$ και $\varphi(44)=\varphi(2^2\cdot 11^1)=2\cdot 10=20$

Από το Θ. Euler-Fermat $\quad 19^{20}\equiv 1 \mod 44 \quad (*)$

Για να αξιοποιήσουμε την ισότητα $(*)$ θα υπολογίσουμε τον αντίστροφο του 19 modulo 44.

$$44 = 2\cdot 19 + 6$$
$$19 = 3\cdot 6 + 1$$

$$\begin{aligned} 1 &= 1\cdot 19 + (-3)\cdot 6 \\ &= 1\cdot 19 + (-3)\cdot(1\cdot 44 + (-2)\cdot 19) \\ &= (-3)\cdot 44 + 7\cdot 19 \end{aligned}$$

Άρα, $7\cdot 19 \equiv 1 \mod 44$

$$x \equiv 19^{19} \equiv 19^{19}\cdot 1^1 \equiv 19^{19}\cdot 7\cdot 19 \equiv 19^{20}\cdot 7 \equiv 1\cdot 7 \equiv 7 \mod 44$$