

ΔΙΟΦΑΝΤΙΚΕΣ ΕΞΙΣΩΣΕΙΣ:

$ax + by = \gamma$ Γεωμετρική ερμεία
Εξίσωση δύο αγνώστων με $a, b, \gamma \in \mathbb{Z}$

ΠΡΟΒΛΗΜΑ:

Ένας αγρότης έχει 1770 νομίσματα και θέλει να αγοράσει άλογα και αγελάδες. Αν το άλογο στοιχίζει 31 νομίσματα και η αγελάδα 21, πόσα άλογα και πόσες αγελάδες μπορεί να αγοράσει;

Αν:

Έστω x άλογα και y αγελάδες

Άρα, $31x + 21y = 1770$, $x, y \in \mathbb{N} \Leftrightarrow ax + by = \gamma, x, y \in \mathbb{R}$

Πχ

$6x + 2y = 7$ Εξίσωση με άκρες λύσεις στο $\mathbb{R}$

αλλά δεν έχει λύση στο $\mathbb{Z}$

ΟΡΙΣΜΟΣ:

Διοφαντικές εξισώσεις είναι πολυώνυμα $f(x_1, \dots, x_k)$

k μεταβλητών με ακέραιους συντελεστές. Η εξίσωση

$f(x_1, \dots, x_k) = 0$ καλείται Διοφαντική και λύνεται

ακέραιες λύσεις

Πχ1

Έστω $f(x, y) = x^2 - 2y^2 = 0 \Rightarrow x^2 - 2y^2 = 0 \Rightarrow$

$\Rightarrow (x - \sqrt{2}y)(x + \sqrt{2}y) = 0 \Rightarrow x = \sqrt{2}y \vee x = -\sqrt{2}y$

Λύσεις Γεωγ. Ευκλ. ν.

Ποιες είναι οι ακέραιες ρίζες της $x^2 = 2y^2$;

Αν: Το $(0, 0)$ προφανώς αποτελεί ρίζα

Καί εστιν αριθμός ακεραίων θετικής ή μη δύναμις: $2^k (2\lambda + 1)$
για $k \geq 0$ και $\lambda \in \mathbb{Z}$

$$x = 2^k(2\lambda+1) \Rightarrow x^2 = 2^{2k}(2\lambda+1)^2$$

$$y = 2^M(2v+1) \Rightarrow y^2 = 2^{2M}(2v+1)^2$$

$$2^{2k} (2v+1)^2 = 2 \cdot 2^{24} \cdot (2v+1)^2$$

• $k \geq 4$: $2^{2k}(2\lambda+1)^2 = 2 \cdot 2^{2k} \cdot (2v+1)^2$

$$2^{(k+1)} \cdot (2v+1)^2 = 2 \cdot (2v+1)^2$$

$$k = M$$

$$(21+1)^2 = 2 \cdot (2V_H)^2$$

Αδύνατη (δισύ το 2 δυν
μπορεί να διαιρεθεί τον
αριθμό (27+1) δισύ
πέντετος)

~~$K > 4$~~

$$(2v+1)^2 2^{2(k-v)-1} = (2v+1)^2$$

Αδυναμία για τον ίδιο λόγο
(όμως το $2^{2(k-1)-1}$ αρπάζει)

Αρρ, η συν $(0,0)$ είναι μοναδική στο $\mathbb{Z}$

$$\underline{n \times 2}$$

Εστω $f(x,y) = x + 2y - 1$, $(-3,1)$ αυστ. $\Rightarrow$ έχει άκρες

Εστω $g(x,y) = \underbrace{4x+6y-11}$, δεν έχει λύσεις στο $\mathbb{Z}$

διαρ. του 2

$\searrow$
 δεν διαρ. του 2

OEOPANA:

Η εξίσωση $\alpha x + \beta y = \gamma$, $\alpha, \beta, \gamma \in \mathbb{Z}$ έχει απέραιτες λύσεις αν $\nu(\alpha, \beta) \mid \gamma$. Αν (x_0, y_0) είναι λύση της εξίσωσης τότε όλες οι λύσεις δίνονται από

$$x = x_0 + \frac{\beta}{(a, \beta)} t \quad \text{u.a.} \quad y = y_0 - \frac{a}{(a, \beta)} t, \quad t \in \mathbb{Z}$$

ANAGLITH

$\Rightarrow$ Es sei (x_0, y_0) eine Lösung zur $ax + by = \delta$, $a, b, \delta \in \mathbb{Z}$

$\leadsto ax_0 + by_0 = \gamma$. Τότε, επειδή ο ΗΚΑ (a, b) διαιρεί τον
αριθμό $ax_0 + by_0 \leadsto 0$ (a, b) θα διαιρεί και τον $\gamma \in \mathbb{Z}$

⇐) Έστω $(\alpha, \beta) \mid \delta$. Έστω $\delta = (\alpha, \beta)$

$$\gamma = \delta \cdot \gamma', \quad \alpha = \delta \cdot \alpha', \quad \beta = \delta \cdot \beta'$$

Από το δ του Ευκλείδη $(\exists x_0, y_0 \in \mathbb{Z})$:

$$\delta = \alpha x_0 + \beta y_0 \Rightarrow \gamma' \delta = \alpha \gamma' x_0 + \beta \gamma' y_0 \Rightarrow$$

$$\Rightarrow \gamma = \alpha \gamma' x_0 + \beta \gamma' y_0$$

Άρα, αυτές είναι $\sim (\gamma' x_0, \gamma' y_0)$

Το ελάχιστο αλγεβρικό ζυγό

Έστω (x', y') ένα άλλο ζεύγος λύσεων

$$\alpha \gamma' x_0 + \beta \gamma' y_0 = \gamma \quad \Rightarrow \quad \alpha (x' - \gamma' x_0) + \beta (y' - \gamma' y_0) = 0$$

$$\alpha x' + \beta y' = \gamma$$

$$\frac{\alpha}{\delta} (x' - \gamma' x_0) + \frac{\beta}{\delta} (y' - \gamma' y_0) = 0 \Rightarrow \left[\frac{\alpha}{\delta}, \frac{\beta}{\delta} \right] = 1$$

$$\Rightarrow \frac{\alpha}{\delta} (x' - \gamma' x_0) = -\frac{\beta}{\delta} (y' - \gamma' y_0) \Rightarrow$$

$$\Rightarrow \left(\frac{\alpha}{\delta} \right) (x' - \gamma' x_0) = \left(\frac{\beta}{\delta} \right) (\gamma' y_0 - y') \Rightarrow$$

$\swarrow$ Διαμ. $\nwarrow$ Διαμ.

$$\Rightarrow \frac{\alpha}{\delta} \mid \gamma' y_0 - y' \quad \text{και} \quad \frac{\beta}{\delta} \mid x' - \gamma' x_0$$

για $(\exists t \in \mathbb{Z})$ με:

$$\frac{\alpha}{\delta} t = \gamma' y_0 - y' \rightarrow y' = \gamma' y_0 - \frac{\alpha}{\delta} t \mid t \in \mathbb{Z}$$

$$\text{ομοίως} \rightarrow x' = \gamma' x_0 + \frac{\beta}{\delta} t$$

Η λύση αυτή δίνεται

από τους 2 προηγούμενους τύπους

Πχ

Να λυθεί η διαφανική εξίσωση

$$1876x + 365y = 13$$

Λύση

Θα πρίνει ο ΜΕΑΘ $(1876, 365) | 13 \leadsto$ πρώτος

$$1876 = 365 \cdot 5 + 51$$

$$365 = 51 \cdot 7 + 8$$

$$51 = 8 \cdot 6 + 3$$

$$8 = 3 \cdot 2 + 2$$

$$3 = 2 \cdot 1 + \boxed{1} \quad , \text{ Άρα } (1876, 365) = 1 | 13 \quad \text{Άρα υπάρχει}$$

Πρίνει, να βρούμε μια λύση

και μετά να τις βρούμε όλες με τον ίδιο.

$$(1876, 365) = 1 = 3 - 2 \cdot 1 = 3 - (3 \cdot 2 + 8) = 3 - 8 + 3 \cdot 2 =$$

$$= -8 + 3 \cdot 3 = -8 + (51 - 8 \cdot 6) \cdot 3 =$$

$$= 51 \cdot 3 - 8 - 8 \cdot 18 = 51 \cdot 3 - 8 \cdot 19 =$$

$$= 51 \cdot 3 - (365 - 51 \cdot 7) \cdot 19 =$$

$$= 51 \cdot 3 - 19 \cdot 365 + 51 \cdot 142 =$$

$$= 51 \cdot 145 - 365 \cdot 19 =$$

$$= -365 \cdot 19 + 145 (1876 - 365 \cdot 5) =$$

$$= -365 \cdot 19 + 145 \cdot 1876 - 145 \cdot 5 \cdot 365 =$$

$$= 1876 \cdot 145 - 365 \cdot 744$$

πολλίω με το 13.

$$13 \cdot 1 = 1876 \cdot 145 \cdot 13 + 365 \cdot (744 \cdot (-13))$$

Αρχική λύση $x_0 = 145 \cdot 13$ και $y_0 = -744 \cdot 13$

Γενική λύση:

$$x = x_0 + \frac{q}{(q, \beta)} t = 145 \cdot 13 + 1876 \cdot t$$

$$y = y_0 - \frac{\beta}{(q, \beta)} t = -744 \cdot 13 - 365 \cdot t$$

ΠΟΡΙΣΜΑ: Έστω $a_1, \dots, a_k, c \in \mathbb{Z}$ και $d = (a_1, \dots, a_k)$. Η γραμμική Διαφορική Εξίσωση $a_1 x_1 + a_2 x_2 + \dots + a_k x_k = c$ έχει απείρως λύση αν $d \mid c$.

Οι τίνες είναι δίνουν οι λύση εξαρτώνται από το d και είναι πολύντομα.

Πχ

1) $6x + 8y + 10z = 1$

Δεν έχει απείρως λύση δόση $(6, 8, 10) = 2$
δεν διαιρεί το 1. Αλλά στον χώρο $(\mathbb{R}^3)$ έχει
λύσεις διότι αποτελεί ένα επίπεδο

2) $6x + 4y + 8z = 2 \Leftrightarrow 3x + 2y + 4z = 1$

Αφού $(6, 4, 8) = 2 \mid 2$ τότε επιδέχεται λύση
στον $\mathbb{Z}$. Αρκεί να βρούμε τις λύσεις της εξίσωσης

Έστω $w = 3x + 2y$ και θέλουμε να λύσει
την εξίσωση $w + 4z = 1$

Έχει λύση γιατί $(4, 1) = 1 \mid 1$

• Μια λύση της είναι $(5, -1)$

• Γενική λύση $w = 5 + 4t$

$$z = -1 - t$$

Αλλά $3x + 2y = 1 \cdot w$

$$3x + 2y = 1 \rightarrow \text{λύση } (1, -1)$$

$$\begin{cases} x = 1 \cdot w = 1 \cdot (5 + 4t) \\ y = -1 \cdot w = -1 \cdot (5 + 4t) \\ z = -1 - t \end{cases}$$

ΤΙΠΟΛΟΓΙΑ:

Πολλές φορές απαιτούνται θετικές λύσεις (και συγκεκριμένα φυσικούς). Οπότε το t δεν παίρνει οποιαδήποτε τιμή.

Π.Χ.

Να βρεθεί το πλήθος των θετικών ακεραίων λύσεων της εξίσωσης:

$$392x + 21y = 14 \quad (\text{Ανέχει λύση})$$

ΛΥΣΗ

$$\begin{aligned} (392, 21) &= 7 \\ \text{όπου } 392 &= 21 \cdot 18 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 \end{aligned}$$

$$\begin{aligned} 7 &= 21 - 14 = 21 - (392 - 21 \cdot 18) = \\ &= 21 - 392 + 21 \cdot 18 = \\ &= -392 + 21 \cdot 19 \end{aligned}$$

Πολ/Λω με 2: $14 = -2 \cdot 392 + 38 \cdot 21$

Λύσεις: $x = x_0 + \frac{b}{(a,b)} t = -2 + 3t$

$$y = y_0 + \frac{a}{(a,b)} t = 38 - 56t$$

$$x = -2 + 3t \quad | \quad x > 0$$

$$y = 38 - 56t \quad | \quad y > 0$$

$$\begin{cases} -2 + 3t > 0 \Rightarrow 3t > 2 \Rightarrow t > \frac{2}{3} \\ 38 - 56t > 0 \Rightarrow t < \frac{38}{56} \end{cases}$$

$$\forall t \in \mathbb{Z}$$

δεν υπάρχει

πλήθος ακεραίων

Αρα, δεν έχει ακεραίες θετικές λύσεις.

ΠΛΗΘΟΣ ΜΗ ΑΡΝΗΤΙΚΩΝ ΛΥΣΕΩΝ ΤΗΣ $ax + by = d$ (1)

Έστω (x_0, y_0) μια λύση της (1).

Τότε ορίζουμε ότι οι ευχάριστες λύσεις δίνονται

$$x = x_0 + \frac{b}{(a,b)} t \quad \text{και} \quad y = y_0 - \frac{a}{(a,b)} t$$

Έχουμε, όπως τούτ περιορισμούς $0 \leq x, y \Leftrightarrow$

$$\Leftrightarrow 0 \leq x_0 + \frac{b}{(a,b)} t \quad \text{και} \quad 0 \leq y_0 - \frac{a}{(a,b)} t$$

$$-x_0 \leq \frac{b}{(a,b)} \quad t \Rightarrow \frac{-x_0(a,b)}{b} \leq t \quad \text{και}$$

$$\frac{a}{(a,b)} t \leq x_0 \Leftrightarrow t \leq \frac{y_0(a,b)}{a}$$

$$\text{Άρα, } \frac{-x_0(a,b)}{b} \leq t \leq \frac{y_0(a,b)}{a}, \quad t \in \mathbb{Z}$$

ΙΣΟΤΙΜΙΕΣ - ΙΣΟΥΠΟΛΟΙΠΑ :

κάθε φυσικός είναι:

$$\text{άρτιος} = 2v + 0 \rightarrow \text{Υπολ. } 0$$

$$\text{περιττός} = 2v + 1 \rightarrow \text{Υπολ. } 1$$

κάθε φυσικός όταν διαιρείται με το 3 έχει

υπόλοιπο 0, 1, 2

$$\text{Άρα } k \in \mathbb{N} : k = 3v + 0 \quad \text{ή} \quad k = 3v + 1 \quad \text{ή} \quad k = 3v + 2$$

ΟΡΙΣΜΟΣ:

Έστω m φυσικός και μεγαλύτερος του 1

Δύο αμέτρητοι a και b λέγεται ότι είναι ισοτιμιοί ή ισοδυναμιοί ή ισουπόλοιποι modulo m , αν

$$a - b = km \Leftrightarrow m \mid a - b$$

Γράφουμε $a = b \pmod{m}$

Πχ

$$\text{Έστω } m=7, a=13 \text{ τότε } b=6 \text{ ή } b=-1$$

Άρα βάσει του $b=6$ άλλο μπορεί να είναι το

$$b = 6 + 1 \cdot 7 \quad \text{ή} \quad b = 6 + 2 \cdot 7 \quad \text{ή} \quad b = 6 + 3 \cdot 7, \text{ πολλαπλά του } 7$$

αλλά και σε σχέση με το $b=-1$ θα μπορεί

$$\text{να είναι το } b = 6 - 7 \quad \text{ή} \quad \text{πολλαπλά του } 7$$

Άρα, θα είναι ισοδυναμιοί $\pmod{7}$ η διαφορά τους

διαιρείται με το m (αλλά θα πρέπει να έχω

το ίδιο υπόλοιπο). Επειδή ο a έχει υπόλοιπο 6

θα είναι πολλαπλός με τον $13 \bmod 7$.

ΠΡΟΤΑΣΗ

- 1) $a \equiv b \bmod m \Leftrightarrow$ α και β έχουν το ίδιο υπόλοιπο ως προς m
- 2) Για κάθε αριθμό α υπάρχει μοναδικός αριθμός u με $a \equiv u \bmod m$ και $0 \leq u < m-1$

ΑΠΟΔΕΙΞΗ

1) $a \equiv b \bmod m \Leftrightarrow a - b = m \cdot \lambda$ (*)

Διαιρούμε τους α & b δια m : $a = m\pi_1 + u_1$ | (**)
 $b = m\pi_2 + u_2$

$a - b \stackrel{(*)}{=} m \cdot \lambda \Leftrightarrow m \cdot \pi_1 + u_1 - m\pi_2 - u_2 = m \cdot \lambda$

$m(\pi_1 - \pi_2 - \lambda) = u_2 - u_1 \sim u_2 - u_1$ πολλαπλό του m (***)

$0 \leq u_2 \leq m-1$

$0 \leq u_1 \leq m-1 \sim 0 \geq -u_1 \geq 1-m \Rightarrow -m+1 \leq -u_1 \leq 0$

$0 \leq u_2 \leq m-1$

$\sim -(m-1) \leq u_2 - u_1 \leq m-1$ (****)

Έχουμε, ότι $u_2 - u_1 = 0 \Leftrightarrow u_2 = u_1$

Αντιστροφή,

$a = m\pi_1 + u$ | $a - b = m(\pi_1 - \pi_2)$
 $b = m\pi_2 + u$ | $a \equiv b \bmod m$

- 2) Κάθε αριθμός όταν διαιρείται με τον m, έχει μοναδικό ηγτικό και υπόλοιπο

$a = m\pi + u$, $0 \leq u \leq m-1$ Μοναδικά

Αρα, $a \equiv u \bmod m$

πχ-

Να βρεθούν όλοι οι ρότιμοι mod 4

ΜΕΤ

Αυτοί θα χωρίζονται σε 4 κατηγορίες

Υπολοιπο 0: $\{ \underbrace{4\lambda}_{\in 0 \pmod 4} \mid \lambda \in \mathbb{Z} \} \sim \left\{ \begin{array}{l} \text{κάθε } 2 \text{ στοιχεία αυτού του} \\ \text{υποσυνόλου είναι ρότιμοι μετὰ 4} \end{array} \right.$

Υπολοιπο 1: $\{ \underbrace{4\lambda'+1}_{\in 1 \pmod 4} \mid \lambda' \in \mathbb{Z} \} \sim \left\{ \begin{array}{l} \text{ομοίως} \end{array} \right.$

Υπολοιπο 2: $\{ \underbrace{4\lambda''+2}_{\in 2 \pmod 4} \mid \lambda'' \in \mathbb{Z} \} \sim \left\{ \begin{array}{l} \text{ομοίως} \end{array} \right.$

Υπολοιπο 3: $\{ \underbrace{4\lambda''' + 3}_{\in 3 \pmod 4} \mid \lambda''' \in \mathbb{Z} \} \sim \left\{ \begin{array}{l} \text{ομοίως} \end{array} \right.$

$$\mathbb{Z} \subseteq [0]_4 \cup [1]_4 \cup [2]_4 \cup [3]_4 = \mathbb{Z}, \quad \cup : \text{είναι ένωση}$$

$[a]_4$: συμβολίζει όλους τους ακεραίους που
αν τους διατρέψεις με το 4 θα σου
δίνει υπολοιπο a .

ΠΡΟΤΑΣΗ: 1) Η ρωσικία $a = b \pmod m$ αποτελεί σχέση
ζωσθενάκτας

2) Για κάθε υπολοιπο (u) με $0 \leq u \leq m-1$
συμβολίζεται με $[u]_m = \{u + km \mid k \in \mathbb{Z}\}$
δηλ. το υποσύνολο του $\mathbb{Z}$ που περιέχει όλους τους
ακεραίους με υπολοιπο u όταν διαιρούνται με το m .

Τότε:

$$\text{Αν } u \neq u' \text{ τότε } [u]_m \cap [u']_m = \emptyset$$

$$\text{και } \mathbb{Z} = \bigcup_{0 \leq u \leq m-1} [u]_m \quad (\text{ζενι ένωση})$$

ΑΠΟΔΕΙΞΗ

1) Πρόταση (Αριστοβίς - Ευκλείδει - Μεταβατική)

2) Έστω $U \neq U'$ και $0 \leq U, U' \leq m-1$

Αν $[U]_m \cap [U']_m \neq \emptyset$ τότε υπάρχει κοινός αριθμός αντίθετος και στα δύο υποσύνολα. Δηλ. έχει δύο διαφορετικά υποσύνολα! Άρα, $[U]_m \cap [U']_m = \emptyset$

Σίγουρα ισχύει: $\mathbb{Z} \supseteq \bigsqcup_{0 \leq U \leq m-1} [U]_m$ πράγματι αυτός το κάθεται στο αντίστοιχο υποσύνολό του.

Έστω $a \in \mathbb{Z}$. Ψάχνω Αν το διαιρέσαμε με m θα έχει μοναδικό υποσύνολο U . Άρα, $a \in [U]_m$
Δηλ. $\forall a \in \mathbb{Z} \Rightarrow a \in \bigsqcup_{0 \leq U \leq m-1} [U]_m \Rightarrow$

$$\Rightarrow \mathbb{Z} \subseteq \bigsqcup_{0 \leq U \leq m-1} [U]_m \Rightarrow \mathbb{Z} = \bigsqcup_{0 \leq U \leq m-1} [U]_m$$