ΠΑΡΑΤΗΡΗΣΗ: Έστω $\begin{cases} x = z_1 e + t\frac{b}{d} \\ y = z_2 e - t\frac{a}{d} \end{cases}$

Αφού $(a,b) \neq (0,0)$ έχουμε

Αν $b \neq 0$, τότε $t_1 \neq t_2 \Rightarrow z_1 e + t_1\frac{b}{d} \neq z_1 e + t_2\frac{b}{d}$

Αν $a \neq 0$, τότε $t_1 \neq t_2 \Rightarrow z_2 e - t_1\frac{a}{d} \neq z_2 e - t_2\frac{a}{d}$

Άρα αν $d|c$ η $(*)$ έχει άπειρες λύσεις.

ΠΑΡΑΤΗΡΗΣΗ: Έστω $d|c$. Τι χρειάζεται να κάνω για να υπολογίσω όλες τις λύσεις της $(*)$;

Πρέπει (με Ευκλείδειο Αλγόριθμο) να υπολογίσω το $d = ΜΚΔ(a,b)$ κ' $z_1, z_2 \in \mathbb{Z}$ με $d = z_1 a + z_2 b$

Π.χ. Βρείτε όλες τις λύσεις (αν υπάρχουν) της διοφαντικής $2x + 6y = 5$

Λύση Έχουμε $2|6$ άρα $ΜΚΔ(2,6) = 2$ κ' $2 \nmid 5$. Επομένως η διοφαντική εξίσωση ΔΕΝ έχει λύσεις στο $\mathbb{Z}^2$ από το θεώρημα.

Π.χ. Βρείτε όλες τις λύσεις (αν υπάρχουν) της διοφαντικής $1492x + 1066y = -4$

Λύση Έχουμε $a = 1492$, $b = 1066$. Θέτουμε $d = ΜΚΔ(1492, 1066)$

Υπολογίζουμε d με Ευκλείδειο Αλγόριθμο

$1492 = 1 \cdot 1066 + 426$

$1066 = 2 \cdot 426 + 214$

$426 = 1 \cdot 214 + 212$

$214 = 1 \cdot 212 + 2$

$212 = 2 \cdot 106 + 0$

Συνεπώς $d = 2$. Αφού $d | -4 = c$ η διοφαντική έχει λύσεις στο $\mathbb{Z}^2$

Βήμα 2ο: Υπολογίζει $z_1, z_2 \in \mathbb{Z}$ με $d = z_1 a + z_2 b$. Λύνει το γνωστό, διαιρεί το πρόβλημα $d = z_1 \cdot 1492 + z_2 \cdot 1066$ με $z_1 = -5$ κ' $z_2 = 7$.

Βήμα 3ο: Από το Θεώρημα, το σύνολο λύσεων της διοφαντικής είναι:

$$\left\{(x,y) = \left(\frac{c}{d} z_1 + t\frac{b}{d}, \frac{c}{d} z_2 - t\frac{a}{d}\right), t \in \mathbb{Z}\right\} =$$

$$= \{(x,y) = (10 + t \cdot 533, -14 - t \cdot 764) : t \in \mathbb{Z}\}$$

Υπενθύμιση: (*) $ax + by = c$ με $a, b, c \in \mathbb{Z}$ $(a,b) \neq (0,0)$ έχει λύση στο $\mathbb{Z}^2$ ως προς (x,y) ανν ΜΚΔ$(a,b) | c$

Πρόταση 6 από 2 1): Έστω (*) με $a, b, c \in \mathbb{N}$. Αναζητούμε θετικές λύσεις, δηλαδή λύσεις $(x,y) \in \mathbb{Z}^2$ με $x > 0, y > 0$. Έστω Ω σύνολο θετικών λύσεων της (*)

1) Δ.ο. για $31x + 43y = 5$. Έχουμε $\Omega = \emptyset$

2) Δ.ο. για την (*) το σύνολο Ω είναι πεπερασμένο

Απόδειξη

1) Έστω $(x,y) \in \mathbb{N} \times \mathbb{N}$ λύση της $31x + 43y = 5$ (θα βρούμε αντίφαση). Αφού $x, y \in \mathbb{N} \Rightarrow x \geq 1, y \geq 1$. Άρα $31x + 43y \geq 31 \cdot 1 + 43 \cdot 1 = 74 > 5$. Αλλά $31x + 43y = 5$, αντίφαση

2) ΙΣΧΥΡΙΣΜΟΣ: Έστω $(x,y) \in \mathbb{N} \times \mathbb{N}$ λύση της (*). Τότε $x \leq c$ κ' $y \leq c$. Άρα Ω πεπερασμένο κ' $\#\Omega \leq c^2$
πλήθος στοιχείων

Απόδειξη: Υποθέτουμε ότι $\exists (x,y) \in \Omega$ με $x > c$. Αφού $a \in \mathbb{N}, b \in \mathbb{N}, x > c, y \geq 1$ έχουμε $ax + by \geq ax \geq x > c$. Αλλά $(x,y) \in \Omega$, άρα $ax + by = c$, αντίφαση. Το ίδιο επιχείρημα δίνει αντίφαση αν $y > c$.

Άτοπο $\to$ Ω

3) Δ.ο. η διοφαντική εξίσωση $x - y = 1$ έχει άπειρο το πλήθος θετικές λύσεις

Απόδειξη. Πράγματι αν $z \in \mathbb{N}$, το $(z+1, z)$ είναι θετική λύση της $x - y = 1$. Αφού το $\mathbb{N}$ είναι άπειρο σύνολο, το αποτέλεσμα έπεται

Φυλ 5 ασκ 9. Να περιγραφούν όλοι οι φυσικοί αριθμοί που έχουν ακριβώς 1,2,3,4 θετικούς διαιρέτες.

ΥΠΕΝΘΥΜΙΣΗ: Αν $p_1, p_2, \dots, p_r$ πρώτοι με $p_i \neq p_j$ για $i \neq j$ κ' $p_1, p_2, \dots, p_r$ μη αρνητικοί ακέραιοι από πρόταση, ο αριθμός των θετικών διαιρετών του $p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ είναι ίσος με $(e_1+1)(e_2+1)\dots(e_r+1)$

Άρα αν $a \in \mathbb{N}$ ο a έχει ακριβώς ένα θετικό διαιρέτη αν $e_1 = e_2 = \dots = e_r = 0$, δηλ αν $a = 1$

Ισχυρισμός 1) Ο $a \in \mathbb{N}$ έχει ακριβώς δύο θετικούς διαιρέτες, αν ο a είναι πρώτος

Απόδειξη: Από τον ορισμό του πρώτου

Ισχυρισμός 2) Ο $a \in \mathbb{N}$ έχει ακριβώς τρεις θετικούς διαιρέτες αν $\exists$ πρώτος p με $a = p^2$. Συνεπώς $\exists e_i = 2$ κ' για $i \neq j$ $e_j = 0$. Ο ισχυρισμός 2 έπεται

$4 = (e_1+1)(e_2+1)\dots(e_r+1)$

Ισχυρισμός 3: Ο $a \in \mathbb{N}$ έχει ακριβώς 4 θετικούς διαιρέτες αν (i) $\exists$ πρώτος p με $a = p^3$ ή (ii) $\exists$ πρώτοι p_1, p_2 με $p_1 \neq p_2$ ώστε $a = p_1 p_2$

Απόδειξη: $4 = (e_1+1)(e_2+1)\dots(e_r+1)$ με $e_i \geq 0$ ακεραίους συνεπάγεται ότι ή $\exists e_i = 3$ κ' για $i \neq j$ $e_j = 0$ ή $\exists i_1 \neq i_2$ με $e_{i_1} = e_{i_2} = 1$ κ' $e_j = 0$ για $j \notin \{e_{i_1}, e_{i_2}\}$

π.χ του ισχυρισμό 3 $2^3 = 8$, $2 \cdot 3 = 6$

Φυλ 5 ασκ 10. Έστω $a \in \mathbb{N}$. Ν.δ.ο το πλήθος των θετικών διαιρετών του a είναι περιττός αριθμός αν $\exists b \in \mathbb{N}$ με $a = b^2$

Απόδειξη: $\exists$ $p_1, \dots, p_r$ πρώτοι με $p_i \neq p_j$ για $i \neq j$ κ' $e_1 \dots e_r \in 2/$ μη αρνητικοί ώστε $a = p_1^{e_1} \dots p_r^{e_r}$

Από υπόθεση ο αριθμός των θετικών διαιρετών του a είναι ίσος με $(e_1+1)(e_2+1)\dots(e_r+1)$

Επειδή γινόμενο άρτιου με περιττούς είναι άρτιος (αφού $(2k)(2l+1)=2(k(2l+1))$ άρτιος)
Έχουμε $(e_1+1)(e_2+1)\dots(e_r+1)$ περιττός αν $\forall i$, e_i+1 περιττός. Άρα $\forall i$, e_i άρτιος.
Άρα $\exists q_i\in\mathbb{N}$, $q_i\geq 0$ με $e_i=2q_i$. Συνεπώς $a=p_1^{e_1}\cdots p_r^{e_r}=p_1^{2q_1}p_2^{2q_2}\cdots p_r^{2q_r}=(p_1^{q_1}p_2^{q_2}\cdots p_r^{q_r})^2$

Φυλ 4 άσκ 5. Έστω $u\in\mathbb{Z}$. Νδο οι $6u-1, 6u+1, 6u+2, 6u+3, 6u+5$ είναι πρώτοι (ανά δύο) μεταξύ τους.
Απόδειξη: (Για $a=6u+2$ $b=6u+5$)
Υποθέτουμε $ΜΚΔ(a,b)\neq 1$. Άρα $\exists$ πρώτος p, με $p\mid ΜΚΔ(a,b)$
Έχουμε $ΜΚΔ(a,b)=ΜΚΔ(a,b-a)=ΜΚΔ(6u+2,3)$. Άρα $p\mid 3\Rightarrow p=3$. Συνεπώς $3\mid 6u+2$

Αφού $\left.\begin{array}{l}3\mid 6\\ \text{κ' } 3\mid 6u+2\end{array}\right\}\Rightarrow 3\mid (6u+2)+(-u)6\Rightarrow 3\mid 2$, αντίφαση

Παρόμοια απόδειξη για κάθε άλλο ζεύγος.

ΑΚΕΡΑΙΟΣ MODULO n (με $n\in\mathbb{N}$)

Συμβολισμός. Έστω $n\geq 1$ κ' $a\in\mathbb{Z}$. Θέτουμε $[a]_n=\{a+kn\mid k\in\mathbb{Z}\}$
(π.χ.) $[2019]_2$ = ΠΕΡΙΤΤΟΣ ΑΚΕΡΑΙΟΣ, $=[1]_2=\{\dots,-5,-3,-1,1,3,5\}$.
$[2020]_2=[0]_2$ = άρτιοι ακέραιοι $=\{\dots,-6,-4,-2,0,2,4,6\}$
$[3]_5$ = ακέραιοι "της μορφής $5k+3$" $=\{\dots,-7,-2,3,8,13\dots\}$

ΠΑΡΑΤΗΡΗΣΗ: Έστω $n\geq 1$. Ορίζουμε σχέση ισοδυναμίας στο $\mathbb{Z}$ $a\sim b$ αν $n\mid a-b$. Εύκολα βλέπουμε ότι το $[a]_n$ είναι μια κλάση ισοδυναμίας του $a\in\mathbb{Z}$. Με άλλα λόγια ότι:

Πρόταση Έστω $n\geq 1$ κ' $a,b\in\mathbb{Z}$. Τότε $[a]_n=[b]_n$ αν ν $n\mid b-a$

Απόδειξη Έστω $n\mid b-a$, τότε $\exists k\in\mathbb{Z}$ με $b-a=kn\Rightarrow b=kn+a$

Άρα για $t\in\mathbb{Z}$ ο $a+tn=b+(t-k)n$. Άρα $[a]_n\subseteq[b]_n$. Παρόμοια δείχνουμε $[b]_n\subseteq[a]_n$. Άρα $[a]_n=[b]_n$

Αντίστροφα υποθέτουμε $[a]_n = [b]_n$ (και επομένως τα $\mathbb{Z}$) τότε $a = b + cn \in [a]_n = [b]_n$. Άρα $\exists\, c \in \mathbb{Z}$ με $a - b = cn$ άρα $n \mid b - a$

<u>Πόρισμα</u> Έστω $n \geq 1$ κ' $a, b \in \mathbb{Z}$. Έστω r_a το υπόλοιπο της Ευκλείδειας Διαίρεσης του a με του n, κ' r_b το υπόλοιπο της Ευκλείδειας Διαίρεσης του b με το n. Τότε $[a]_n = [b]_n$ αν $r_a = r_b$

<u>Απόδειξη</u> Άμεσα από την πρόταση

π.χ. Ισχύει $[2017]_3 = [7102]_3$ ή όχι;

<u>Λύση</u> <u>α' τρόπος</u> $7102 - 2017 = 5085$

Έχουμε $5+0+8+5 = 18$

οπότε από κριτήριο $3 \mid 5085$

$$\begin{array}{r} 7102 \\ 2017 \\ \hline 5085 \end{array}$$

Συνεπώς $[2017]_3 = [7102]_3$

2017 modulo 3

<u>β' τρόπος</u> Ευκλείδεια Διαίρεση

$2017 = 672 \cdot 3 + 1$

$7102 = 2367 \cdot 3 + 1$

$$\begin{array}{r|l} 2017 & 3 \\ 21 & \overline{672} \\ 7 & \\ 1 & \end{array}$$

Αφού τα υπόλοιπα είναι ίσα έπεται $[2017]_3 = [7102]_3$

$$\begin{array}{r|l} 7102 & 3 \\ 110 & \overline{2367} \\ 20 & \\ 22 & \\ 1 & \end{array}$$

<u>Ορισμός</u> Έστω $n \geq 1$ θέτουμε $\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}$

<u>Πρόταση</u> Έχουμε $\# \mathbb{Z}_n = n$ κ' $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

π.χ. Από την πρόταση $\# \mathbb{Z}_1 = 1$ κ' $\mathbb{Z}_1 = \{[0]_1\}$

$\# \mathbb{Z}_2 = 2$ κ' $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$

$\# \mathbb{Z}_6 = 6$ κ' $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$

<u>Απόδειξη πρότασης</u> Θέτουμε $B = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\} \subseteq \mathbb{Z}_n$

<u>Ισχυρισμός 1</u> $B = \mathbb{Z}_n$

<u>Απόδειξη</u> Έστω $a \in \mathbb{Z}$ κ' r το υπόλοιπο της Ευκλείδειας Διαίρεσης του a με το n. Τότε $0 \leq r \leq n-1$ κ' από το πόρισμα $[a]_n = [r]_n$. Συνεπώς $[a]_n \in B$. Άρα $\mathbb{Z}_n \subseteq B$

κ' αφού $B \subseteq \mathbb{Z}/n$ έχουμε $B = \mathbb{Z}/n$

Ισχυρισμός 2: Εάν $r_1 \neq r_2$ με $0 \le r_1 \le n-1$ κ' $0 \le r_2 \le n-1$. Τότε $[r_1]_n \neq [r_2]_n$

Απόδειξη: Έχουμε $r_1 = 0 \cdot n + r_1$, συνεπώς το r_1 είναι το υπόλοιπο της Ευκλείδιας Διαίρεσης του r_1 με τον n. Ομοίως, r_2 είναι το υπόλοιπο της Ευκλείδιας Διαίρεσης του r_2 με τον n. Αφού $r_1 \neq r_2$ από το πόρισμα $[r_1]_n \neq [r_2]_n$

Από τους Ισχυρισμούς 1 κ' 2 έπεται η πρόταση

Ερώτηση: Ισχύει $\mathbb{Z}/4 = \{[0]_4, [2]_4, [4]_4, [8]_4\}$ ή όχι;

Απάντηση: Έχουμε $[0]_4 = [4]_4$, γιατί $4 \mid (4-0)$ κ' $[8]_4 = [0]_4$ γιατί $4 \mid (0-8)$. Συνεπώς $\{[0]_4, [2]_4, [4]_4, [8]_4\} = \{[0]_4, [2]_4\}$. Άρα έχει δύο στοιχεία κ' αφού με τον n το $\mathbb{Z}/4$ έχει 4 από την πρόταση δεν μπορεί να είναι ίσα.

Φανερά, $\mathbb{Z}/4 - \{[0]_4, [2]_4\} = \{[1]_4, [3]_4\}$.

Ερώτηση: Πόσα στοιχεία έχει το υποσύνολο $C = \{[5]_3, [6]_3, [7]_3, [8]_3\}$ του $\mathbb{Z}/3$; Ισχύει $C = \mathbb{Z}/3$ ή όχι;

Λύση: $[5]_3 = [2]_3$, $[6]_3 = [0]_3$, $[7]_3 = [1]_3$, $[8]_3 = [2]_3$.

Συνεπώς, $C = \{[2]_3, [0]_3, [1]_3\} = \mathbb{Z}/3$ κ' $\# C = \# \mathbb{Z}/3 = 3$

Υπενθύμιση: Για $n \ge 1$ κ' $a \in \mathbb{Z}$, ορίσαμε το $[a]_n \in \mathbb{Z}/n$
Ισχύει $[a]_n = [b]_n$ ανν $n \mid b-a$

Ορισμός: Έστω $n \ge 1$ κ' $a, b \in \mathbb{Z}$. Γράφουμε $a \equiv b \bmod n$ (α ισότιμος b κατά μέτρο n) αν $n \mid b-a$

Παρατήρηση: Προφανώς $a \equiv b \bmod n$ ανν $[a]_n = [b]_n$

Υπενθύμιση: Από πρόταση, $\# \mathbb{Z}/n = n$ κ' $\mathbb{Z}/n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

Παρατήρηση: Θα ορίσουμε πρόσθεση κ' πολλαπλασιασμό στο $\mathbb{Z}/n$