Φυλ 5 άσκ 11: Δ.ο. αν $\kappa \in \mathbb{Z}$ με $\kappa > 11$, τότε το κ είναι άθροισμα δύο σύνθετων ακεραίων.

Λύση: (Υπενθύμιση: Το $a \in \mathbb{Z}$ σύνθετος αν $a \geq 2$ κ' a όχι πρώτος π.χ. 4, 6, 8, 9, 10, 12, ...)

Περίπτωση 1η: κ άρτιος. Τότε $\kappa = (\kappa - 4) + 4$ (*)
Αφού $\kappa \geq 12 \Rightarrow \kappa - 4 \geq 8$ κ' $\kappa - 4$ άρτιος. Άρα (*) γράφει του κ σαν άθροισμα 2 σύνθετων.

Περίπτωση 2η: κ περιττός. Θέτουμε $a = 9$, $b = \kappa - 9$
Φανερά $\kappa = a + b$

Φανερά 9 σύνθετος. Έχουμε b άρτιος κ' $b \geq 9$, γιατί $\kappa \geq 13$ (αφού $\kappa \geq 12$ περιττός). Άρα b άρτιος με $b \geq 4$, συνεπώς b σύνθετος

Φυλ 5 ασκ 4: Έστω $p, a, b \in \mathbb{N}$ με p πρώτο κ' $pb = a^2$. Δ.ο. $p|b$

Απόδειξη: Αφού $p|a^2$ κ' πρώτος $\Rightarrow p|a$. Άρα $\exists k \in \mathbb{Z}$ με $a = kp \Rightarrow a^2 = k^2p^2$
$\Rightarrow pb = k^2p^2 \overset{p \neq 0}{\Rightarrow} b = k^2 p \Rightarrow p|b$.

Φυλ 5 Ασκ 7: Έστω $a, b, n, m \in \mathbb{N}$ με $n \geq m$. Υποθέτουμε ότι το a^n διαιρεί το b^m. Δ.ο. το a διαιρεί το b.

Λύση: $\exists$ πρώτοι $p_1, p_2, \ldots, p_r$ με $p_i \neq p_j$ για $i \neq j$ κ' ακέραιοι d_i, e_i με $d_i \geq 0, e_i \geq 0$, ώστε
$a = p_1^{d_1} p_2^{d_2} \ldots p_r^{d_r}$ κ' $b = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$

Έχουμε $a^n = (p_1^{d_1} \ldots p_r^{d_r})^n = p_1^{d_1 n} \ldots p_r^{d_r n}$ κ'
$b^m = (p_1^{e_1} \ldots p_r^{e_r})^m = p_1^{e_1 m} \ldots p_r^{e_r m}$

Αφού $a^n | b^m \Rightarrow d_i n \leq e_i m$ $\forall i = 1 \ldots r$
Αφού $n \geq m \geq 1$ κ' $e_i \geq 0$ έχουμε $e_i m \leq e_i n \Rightarrow d_i n \leq e_i n \underset{n \geq 1}{\Rightarrow} d_i \leq e_i$ $\forall i \Rightarrow a|b$.

Φυλ 4 ασκ 6: Έστω $a, b \in \mathbb{N}$ με ΜΚΔ$(a,b) = 1$
Δ.ο. ΜΚΔ$(a+b, a-b) = 1$ ή 2.
Βρείτε πότε είναι 1 κ' πότε 2.

Λύση: Θέτουμε $d =$ ΜΚΔ$(a+b, a-b)$. Τότε $d =$ ΜΚΔ$(a-b, (a+b) + 1(a+b)) =$
ΜΚΔ$(a+b, 2a)$

· Περίπτωση 1η: a άρτιος, b άρτιος. Δεν συμβαίνει, γιατί ΜΚΔ$(a,b) = 1$.

· Περίπτωση 2η: a άρτιος, b περιττός. Τότε $\exists k, l \in \mathbb{N}$ με $a = 2k$ κ' $b = 2l+1$
Επομένως $d =$ ΜΚΔ$(2k+2l+1, 4k)$ αλλά $2 \nmid (2k+2l+1)$, άρα
$d =$ ΜΚΔ$(2k+2l+1, k) =$ ΜΚΔ$(2k+2l+1, 2l) =$ ΜΚΔ$(a+b, a) =$ ΜΚΔ$(a+b-a, a) =$
ΜΚΔ$(a, b) = 1$

Παρατήρηση 3η α περιττός, b άρτιος. Τα ίδια επιχειρήματα δίνουν $d=1$

Παρατήρηση 4η Έστω α κ' b περιττοί. Τότε $\exists \kappa, \lambda \in \mathbb{N}$ με $\alpha = 2\kappa+1$ κ' $b = 2\lambda+1$

Ισχυρισμός: $ΜΚΔ(\alpha+b, \alpha-b) = 2$. Πράγματι, $d = ΜΚΔ(\alpha+b, 2\alpha) = ΜΚΔ(2\kappa+2\lambda+2, 2(2\kappa+1)) = ΜΚΔ(2(\kappa+\lambda+1), 2(2\kappa+1))$

Συνεπώς $2|d$. Έστω p περιττός πρώτος κ' $p|d$. Τότε $p|2\alpha \Rightarrow p|\alpha$ κ' $p|\alpha+b \Rightarrow p|(\alpha+b)-\alpha = b$. Άρα $p|ΜΚΔ(\alpha,b)=1$, αντίφαση.

Άρα $\exists \mu \geq 1$ ώστε $d = 2^{\mu}$

Αν $\mu \geq 2$, τότε $4|d$. Αφού $d = ΜΚΔ(\alpha+b, 2\alpha) \Rightarrow 4|2\alpha \Rightarrow 2|\alpha$, αντίφαση αφού α περιττός

Συνεπώς $\mu = 1$ κ' $d = 2$

– Σαν συμπέρασμα: Αν (α άρτιος, b περιττός) ή (α περιττός, b άρτιος) τότε $ΜΚΔ(\alpha+b, \alpha-b) = 1$.

Ενώ αν (α κ' b περιττοί), τότε $ΜΚΔ(\alpha+b, \alpha-b) = 2$

ΔΙΟΦΑΝΤΙΚΗ ΕΞΙΣΩΣΗ $\alpha x + by = c$

Έστω $\alpha, b, c \in \mathbb{Z}$ με $(\alpha, b) \neq (0,0)$ διοφαντική εξίσωση $\alpha x + by = c$ (*)

Ψάχνουμε λύσεις $(x,y) \in \mathbb{Z}^2$

πχ Για $\alpha = 3, b = 2, c = 7$: $3x + 2y = 7$

Θεώρημα Έστω $\alpha, b, c \in \mathbb{Z}$ με $(\alpha, b) \neq (0,0)$. Θεωρούμε τη διοφαντική εξίσωση $\alpha x + by = c$ (*)

(i) Η (*) έχει ακέραιες λύσεις $(x,y) \in \mathbb{Z}^2$ ανν $d|c$ όπου $d = ΜΚΔ(\alpha, b)$.

(ii) Έστω $d|c$. Υπολογίζουμε (πχ με Ευκλείδειο Αλγόριθμο) $z_1, z_2 \in \mathbb{Z}$ ώστε $d = \alpha z_1 + b z_2$.

Τότε το σύνολο λύσεων της (*) είναι το εξής:

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

<u>Απόδειξη</u> - <u>Ισχυρισμός (1)</u>. Αν $d \nmid c$, τότε η (*) αδύνατη στο $\mathbb{Z}^2$

<u>Απόδειξη</u>: Έστω ότι $d\nmid c$ κ' $(x,y)\in\mathbb{Z}^2$ ακέραια λύση της (*)
Τότε $c = ax+by$. Αφού $d = \text{ΜΚΔ}(a,b)$ έχουμε $d\mid a$ κ' $d\mid b \Rightarrow d\mid ax+by$
$\Rightarrow d\mid c$, άτοπο

- <u>Ισχυρισμός (2)</u> Έστω $d\mid c$ κ' $(x,y)\in A$. Τότε (x,y) λύση της (*)
<u>Απόδειξη</u>: Έχουμε ότι $\exists t\in\mathbb{Z}$ ώστε $\begin{cases} x = z_1\frac{c}{d}+t\frac{b}{d} \\ y = z_2\frac{c}{d} - t\frac{a}{d} \end{cases}$

Συνεπώς, $ax+by = az_1\frac{c}{d} + t\frac{ab}{d} + bz_2\frac{c}{d} - t\frac{ab}{d} = c(\frac{a}{d}z_1 + \frac{b}{d}z_2) =$
$= \frac{c}{d}(az_1+bz_2) = \frac{c}{d}\, d = c$

- <u>Ισχυρισμός (3)</u>: Έστω $(x,y)\in\mathbb{Z}^2$ λύση της (*), τότε $(x,y)\in A$
<u>Απόδειξη</u>. Θέτουμε $e = \frac{c}{d} \in \mathbb{Z}$. Αφού (x,y) λύση

$$\left.\begin{array}{l} ax+by=c \\ \text{Επίσης } az_1e+bz_2e=c \end{array}\right\} \Rightarrow a(x-z_1e)+b(y-z_2e)=0$$

$$\Rightarrow \frac{a}{d}(x-z_1e) = -\frac{b}{d}(y-z_2e) \quad (**)$$

Ισχυρισμός 1. Αν $d \nmid c$, τότε η (*) αδύνατη στο $\mathbb{Z}^2$

Απόδειξη: Έστω ότι $d \nmid c$ και $(x,y) \in \mathbb{Z}^2$ ακέραια λύση της (*).
Τότε $c = xa + by$. Αφού $d = \text{ΜΚΔ}(a,b)$ έχουμε $d \mid a$ και $d \mid b \Rightarrow$
$d \mid ax + by \Rightarrow d \mid c$. αντίφαση

Ισχυρισμός 2. Έστω $d \mid c$ και $(x,y) \in A$. Τότε (x,y) λύση της (*).

Απόδειξη: Έχουμε ότι $\exists t \in \mathbb{Z}$ ώστε $\begin{cases} x = z_1 \frac{c}{d} + t\frac{b}{d} \\ y = z_2 \frac{c}{d} - t\frac{a}{d} \end{cases}$

Συνεπώς $ax + by = a z_1 \frac{c}{d} + t\frac{ab}{d} + b z_2 \frac{c}{d} - t\frac{ab}{d} =$

$= c\left(\frac{a}{d} z_1 + \frac{b}{d} z_2\right) = \frac{c}{d}(a z_1 + b z_2) = \frac{c}{d} \cdot d = c$

Ισχυρισμός 3. Έστω $(x,y) \in \mathbb{Z}^2$ λύση της (*). Τότε $(x,y) \in A$

Απόδειξη: Θέτουμε $e = \frac{c}{d} \in \mathbb{Z}$. Αφού (x,y) λύση

$$\left.\begin{array}{l} ax + by = c \\ \text{Επίσης } a z_1 e + b z_2 e = c \end{array}\right\} \Rightarrow a(x - z_1 e) + b(y - z_2 e) = 0$$

$$\Rightarrow \frac{a}{d}(x - z_1 e) = -\frac{b}{d}(y - z_2 e) \quad (**)$$

Αλλά $d = \text{ΜΚΔ}(a,b)$ άρα από πρόταση $\text{ΜΚΔ}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
Συνεπώς (**)

$$\left.\begin{array}{l} \frac{b}{d} \mid \left(\frac{a}{d}(x - z_1 e)\right) \\ \text{ΜΚΔ}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \end{array}\right\} \Rightarrow \frac{b}{d} \mid (x - z_1 e)$$

άρα $\exists t \in \mathbb{Z}$ με $x - z_1 e = t\frac{b}{d}$

Τώρα $(**) \Rightarrow \frac{a}{d} \cdot t\frac{b}{d} = -\frac{b}{d}(y - z_2 e) \overset{b \neq 0}{\Rightarrow} y = z_2 e - t\frac{a}{d})$

Άρα $(x,y) \in A$

(Υποθέτουμε $b \neq 0$. Παρόμοια απόδειξη αν $a \neq 0$)