22/11/2018.

ΔΙΟΦΑΝΤΙΚΕΣ ΕΞΙΣΩΣΕΙΣ.

ΠΑΡΑΔΕΙΓΜΑ - 1: Βρείτε όλα τα $(x,y) \in \mathbb{Z}^2$ ώστε $1492x + 10664 = -4$.

ΠΑΡΑΔΕΙΓΜΑ - 2: Βρείτε όλα τα $(x,y,z) \in \mathbb{Z}^3$ ώστε $x^2 + y^2 = z^2$

Λύσεις: $(x,y,z) = (0,0,0)$
$(x,y,z) = (1,0,1)$
$(x,y,z) = (3,4,5)$

Έστω $a,b,c \in \mathbb{Z}$ με τουλάχιστον ένα από τα a,b διάφορο του 0 και $ax+by=c$ (*)
(γραμμική) Διοφαντική εξίσωση στα x,y. Ψάχνουμε λύσεις $(x,y) \in \mathbb{Z}^2$.

ΠΑΡΑΔΕΙΓΜΑ: Η $2x+2y=5$ δεν έχει λύσεις $(x,y) \in \mathbb{Z}^2$, γιατί για κάθε $(x,y) \in \mathbb{Z}^2$, $2x+2y$ άρτιος, αλλά 5 περιττός.

ΘΕΩΡΗΜΑ: Θεωρούμε την (*) και θέτουμε $d = \text{ΜΚΔ}(a,b)$.
(i) Η (*) έχει ακέραιες λύσεις $(x,y) \in \mathbb{Z}^2$ αν-ν $d|c$
(ii) Υποθέτουμε $d|c$. Υπάρχουν $z_1, z_2 \in \mathbb{Z}$ ώστε $d = z_1 a + z_2 b$
Θέτουμε $e = \frac{c}{b} \in \mathbb{Z}$. Τότε το σύνολο λύσεων της (*) είναι το σύνολο A, όπου

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

Παράδειγμα - 1: Η διοφαντική εξίσωση $\underset{=}{2}x + \underset{=}{6}y = 5$ δεν έχει λύση στο $\mathbb{Z}^2$, γιατί $d = \text{ΜΚΔ}(2,6) = 2$ και 2×5.

Παράδειγμα - 2: Θα λύσουμε την διοφαντική εξίσωση $ax+by=c$ με $a=1492$, $b=1066$, $c=-4$. με χρήση του θεωρήματος.

Βήμα - 1°: Υπολογίζουμε το $d = \text{ΜΚΔ}(a,b)$ και $z_1, z_2 \in \mathbb{Z}$ με $d = z_1 a + z_2 b$. Υπολογίζουμε τον ευκλ. αλγόριθμο d, z_1, z_2.

$$1492 = 1 \cdot 1066 + 426$$
$$1066 = 2 \cdot 426 + 214$$
$$426 = 1 \cdot 214 + 212$$
$$214 = 1 \cdot 212 + 2$$
$$212 = 2 \cdot 106 + 0$$

Συνεπώς, $d=2$. Επίσης, οι εξισώσεις (*) δίνουν $d = z_1 \cdot 1492 + z_2 \cdot 1066$, όπου $z_1 = -5$, $z_2 = 7$ οπότε $d = \text{ΜΚΔ}(a,b) = 2 \mid c = -4$.
Επιπλέον, από το θεωρητικό η (*) έχει απείρως λύσεις, με σύνολο απείρων λύσεων

$$A = \{(x,y) : (z_1 e + t\frac{b}{d}, z_2 e - t\frac{a}{d}) \; t \in \mathbb{Z}\} \text{ όπου}$$
$$e = \frac{c}{d} = -\frac{4}{2} = -2.$$

Συνεπώς, $A = \{(x,y) = (10 + 533t, -14 - t \cdot 746) : t \in \mathbb{Z}\}$

Παρατήρηση: Το A είναι απείρο σύνολο. Αυτό ισχύει πάντα όταν $d \mid c$, γιατί $a \neq 0$ ή $b \neq 0$, άρα για διαφορετικές τιμές του t το $z_2 e - t\frac{a}{d}$ ή το $z_1 e + t\frac{b}{d}$ είναι διαφορετικές τιμές, καθώς το t μεταβάλλεται στο $\mathbb{Z}$.
Με άλλα λόγια η εξίσωση (*) του θεωρήματος ή δεν έχει καμία λύση στο $\mathbb{Z}^2$ ή υπάρχουν άπειρα το πλήθος ζεύγη $(x,y) \in \mathbb{Z}^2$ που την ικανοποιούν.

Απόδειξη Θεωρήματος: Έστω $a \neq 0$ και $b \neq 0$. Υποθέτουμε $b \neq 0$. Η ίδια απόδειξη δουλεύει αν $a \neq 0$.

Ισχυρισμός -1: Αν $d \nmid c$, τότε το σύστημα (*) δεν έχει λύση στο $\mathbb{Z}^2$.

Απόδειξη: Έστω $d = \text{ΜΚΔ}(a,b) \nmid c$ και όταν υπάρχει λύση $(x,y) \in \mathbb{Z}^2$ του συστήματος. Τότε $c = ax + by$. Αφού $d \mid a$ και $d \mid b$ και $c = ax + by$, έπεται $d \mid c$ αντίφαση.

Τώρα, υποθέτουμε $d \mid c$. Θα δείξουμε ότι το A είναι το σύνολο λύσεων της (*).

Ισχυρισμός -2: Αν $(x,y) \in A$, τότε (x,y) λύση του (*).

Απόδειξη: Έστω $t \in \mathbb{Z}$. Τότε $a(z_1 e + t\frac{b}{d}) + b(z_2 e - t\frac{a}{d}) =$
$= az_1 e + bz_2 e + tab - t\frac{ab}{d} = az_1 e + bz_2 e =$
$= e(az_1 + bz_2) = ed = \frac{c}{d} d = c.$

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

Απόδειξη: Αφού (x,y) λύση $ax + by = c$, επίσης $az_1 e + bz_2 e = c$ } αφαιρούμενοι ⟹

$$a(x - z_1 e) + b(y - z_2 e) = 0 \Rightarrow \frac{a}{d}(x - z_1 e) = -\frac{b}{d}(y - z_2 e) \quad (**)$$

Άρα $d = \text{ΜΚΔ}(a,b) \xrightarrow{\text{πρόταση}} \text{ΜΚΔ}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

Από (**) $\frac{b}{d} \mid \frac{a}{d}(x - z_1 e) \Rightarrow \frac{b}{d} \mid x - zy - e.$

Συνεπώς, υπάρχει $t \in \mathbb{Z}$ με $x - z_1 e = t\frac{b}{d} \Rightarrow$

$$x = z_1 e + t\frac{b}{d}.$$

Αρα $n \mid (**) \Rightarrow \frac{a}{d} + \frac{b}{d} = -\frac{b}{d}(y - z_2 e) \xrightarrow[d \neq 0]{}$

$\frac{at}{d} = -y + z_2 e \Rightarrow y = z_2 e - t\frac{a}{d}$

Αρα $(x, y) \in A$.

ΙΔΙΟΤΗΤΕΣ - ΑΚΕΡΑΙΟΙ mod n

ΟΡΙΣΜΟΣ: Έστω $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Λέμε ότι ο a είναι ισοϋπόλοιπος με το b modulon, συμβολίζουμε $a \equiv b \bmod n$, αν $n \mid (a-b)$. Αλλιώς γράφουμε $a \not\equiv b \bmod n$.

ΠΑΡΑΤΗΡΗΣΗ: Από την μοναδικότητα του υπολοίπου της ευκλ. διαίρεσης έπεται ότι $a \equiv b \bmod n$ αν-ν το υπόλοιπο της ευκλ. διαίρεσης του a με το n είναι ίδιο με το υπόλοιπο της ευκλ. διαίρεσης του b με το n.

ΠΑΡΑΔΕΙΓΜΑ:

$15 \equiv -5 \bmod 10$, γιατί $10 \mid 20 = 15 - (-5)$

$7 \equiv -3 \bmod 10$, γιατί $10 \mid 10 = 7 - (-3)$

$7 \not\equiv 3 \bmod 10$, γιατί $10 \nmid 7 - 3 = 4$

ΠΑΡΑΤΗΡΗΣΗ: Αν $a, b \in \mathbb{Z}$ $a \equiv b \bmod 1$, γιατί $1 \mid a - b$.

ΠΑΡΑΤΗΡΗΣΗ: Έστω $a \in \mathbb{Z}$. Τότε $a \equiv 0 \bmod 2$ αν-ν ο αριθμός $a \equiv 1 \bmod 2$ αν-ν ο περιττός.

Πρόταση: Έστω $n \in \mathbb{Z}$. Η σχέση $a \equiv b \bmod n$ είναι σχέση ισοδυναμίας στο $\mathbb{Z}^2$.

Απόδειξη:

- **Ανακλαστική ιδιότητα:** Έστω $a \in \mathbb{Z}$. Τότε $a \equiv a \bmod n$ γιατί $a - a = 0$ και $n \mid 0$.

- **Συμμετρική ιδιότητα:** Έστω $a, b \in \mathbb{Z}$ με $a \equiv b \bmod n$. Τότε $n \mid a-b \Rightarrow n \mid -(a-b) \Rightarrow n \mid b-a \Rightarrow b \equiv a \bmod n$.

- **Μεταβατική ιδιότητα:** Έστω $a, b, c \in \mathbb{Z}$ με $a \equiv b \bmod n$ και $b \equiv c$. Τότε $\left.\begin{matrix} n \mid a-b \\ n \mid b-c \end{matrix}\right\} \overset{\text{Πρόταση}}{\Rightarrow} n \mid a-c \Rightarrow a \equiv c \bmod n$.

Ορισμός: Έστω $n \in \mathbb{N}$. Δείξαμε ότι η σχέση mod n είναι σχέση ισοδυναμίας. Συμβολίζεται με $\mathbb{Z}_n$ το σύνολο πηλίκο του $\mathbb{Z}$ ως προς αυτή τη σχέση και για $a \in \mathbb{Z}$, συμβολίζουμε $[a]_n \in \mathbb{Z}_n$ την αντίστοιχη κλάση ισοδυναμίας.

Πρόταση: Τα στοιχεία $[0]_n, [1]_n, \dots [n-1]_n$ του $\mathbb{Z}_n$ είναι διαφορετικά ανά δύο και $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots [n-1]_n\}$. Συνεπώς, $\#\mathbb{Z}_n = n$ (δηλ. το σύνολο $\mathbb{Z}_n$ είναι πεπερ. με ακριβώς n στοιχεία).

*** **Παρατήρηση:** Έστω $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Πότε τα στοιχεία $[a]_n, [b]_n$ του $\mathbb{Z}_n$ είναι ίσα;

Απόδειξη: Από τους ορισμούς $[a]_n = [b]_n$ αν-ν $a \equiv b \bmod n$, δηλ. αν-ν $n \mid a-b$.

Παράδειγμα: Έστω $n=2$. Τότε

$[-10]_2 = [-8]_2 = [-6]_2 = [-4]_2 = [-2]_2 = [0]_2 = [2]_2 = [4]_2 = [6]_2 = \dots$

και

$[-9]_2 = [-7]_2 = [-5]_2 = [-3]_2 = [-1]_2 = [1]_2 = \dots$

και

$\mathbb{Z}_n = \{[0]_2, [1]_2\}$.

Επίσης, αν a άρτιος, b περιττός $[a]_2 \neq [b]_2$ γιατί a άρτιος b περιττός $\Rightarrow 2 \nmid b-a$.