Ασκήσεις Φυλλάδιο #4

1) Να λυθούν οι Διοφαντικές εξισώσεις: 2/12/2016

β) $5x+7y+14z=2$

$(5,7,14)=(5,(7,14))=(5,7)=1/2$

Θέταμε $7y+14z=(7,14)w=7w$

Επομένως, θα έχαμε $5x+7w=2$

Μια λύση $(-1,1)$

$x=-1+7t$, $t\in\mathbb{Z}$

$w=1-5t$

$7y+14z=7$ $\quad y=-w+14s \Rightarrow y=-1+5t+14s$ $\quad t,s\in\mathbb{Z}$

$(-1,1)$ $\quad z=w-7s \quad z=1-5t-7s$

$5(-1+7t)+7(-1+5t+14s)+14(1-5t-7s)=$

$-5+35t-7+35t+98s+14-70t-98s=2$

a) $256x+337y=179$

$(256,337)=1$,

Από τον αλγόριθμο του Ευκλείδη $x_0=179\cdot104$ $\quad y_0=-79\cdot179$

$256\cdot104-337\cdot79=1$

Γεν. λύση : $x=179\cdot104+337t$ $\quad t\in\mathbb{Z}$

$y=-79\cdot179-256t$

γ) $5x + 7y + 14z = 44$

$(5,7,14) = 1 \mid 44$

$5x + 7y = (5,7)w = w$

$14z + w = 44$

$(3,2)$ λύση

$\left.\begin{array}{l} w = 2 - 14t \\ z = 3 + t \end{array}\right\}$ Πρέπει $w > 0$, $w \in \mathbb{Z}$ αφού $w = 5x + 7y$

$x, y > 0 \Rightarrow w > 0 \Rightarrow$

$2 - 14t > 0 \Rightarrow 14t < 2 \Rightarrow 7t < 1 \Rightarrow t \leq 0$

$z > 0 \Rightarrow t > -3$, $t = \{-2, -1, 0\}$

$\left.\begin{array}{l} w = \{30, 16, 2\} \\ z = \{1, 2, 3\} \end{array}\right\}$ για $w = 30 \Rightarrow 14z + 30 = 44 \Rightarrow z = 1$

$5x + 7y = 30$ → για $y = 1$: $7y = 7 \Rightarrow 5x = 23$ αδύνατη
για $y = 2$: $7y = 14 \Rightarrow 5x = 16$ αδύνατη
για $y = 3$: $7y = 21 \Rightarrow 5x = 9$ αδύνατη
για $y \geq 4 \Rightarrow 7y \geq 28 \Rightarrow 5x = 2$ αδύνατη

$5x + 7y = 16 \Rightarrow x \geq 1 \Rightarrow 5x \geq 5$, $y \geq 1 \Rightarrow 7y \geq 7 \Rightarrow 5x + 7y \geq 12$ (*)

$5x + 7y = 2 \Rightarrow$ αδύνατη γιατί $x, y > 0 \Rightarrow 5x > 0$ και $7y > 0$ τότε $5x + 7y > 2$

(*) για $x = 2$ ή $y = 2$ έχουμε $5x + 7y > 16$

4) Αν $a \equiv b \bmod m$ και $a \equiv \gamma \bmod n$, τότε $b \equiv \gamma \bmod (m,n)$

ακέραιος

$$\left.\begin{aligned} a-b &= \kappa \cdot m \\ a-\gamma &= \lambda \cdot n \end{aligned}\right\} \Rightarrow \gamma - b = \lambda n - \kappa \cdot m = (m,n) \cdot \left(\frac{\lambda n - \kappa m}{(m,n)} \right)$$

$$\Rightarrow \gamma - b = \delta \cdot (m,n) \Leftrightarrow \gamma \equiv b \bmod (m,n)$$

Άσκηση 9

$31x + 21y = 1770 \quad , \quad x, y \geq 0$

$(31, 21) = 1$

$(x_0, y_0) = (9, 71)$

$x = 9 - 21t$

$y = 71 + 31t$

$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases} \Rightarrow \begin{cases} 9 - 21t \geq 0 \\ 71 + 31t \geq 0 \end{cases} \Rightarrow \begin{cases} t \leq \frac{9}{21} \\ t \geq -\frac{71}{31} \end{cases} \Rightarrow \begin{cases} t \leq 0 \\ t \geq -2 \end{cases} \Rightarrow t = 0,\ t = -1$ και $t = -2$.

Αντικαθιστώντας, στις γενική λύση έχουμε το αποτέλεσμα

29/11/2016

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ
Ασκήσεις #5 ΤΜΗΜΑ ΠΕΡΙΤΤΩΝ

1) Να βρεθούν όλα τα ζεύγη φυσικών ώστε το άθροισμά τους να είναι 100, ο πρώτος να διαιρείται με το 7 και ο δεύτερος με το 11.

2) Να βρεθούν οι ακέραιες λύσεις του συστήματος, αν υπάρχουν:
$$3x+5y+7z=560$$
$$9x+25y+49z=2920$$

3) Να βρεθούν οι αντιστρέψιμες κλάσεις modulo 15 καθώς και οι αντίστροφοι αυτών.

4) Δείξτε ότι $\mathbb{Z}_{17}=\{[0],[3^0],[3^1],\dots,[3^{15}]\}$

5) Αν $\varphi(m)=\varphi(mn)$ και $n>1$, τότε $n=2$ και m περιττός.

6) Δείξτε ότι $2^{2n}\equiv 1 \bmod 3$, $2^{3n}\equiv 1 \bmod 7$, $2^{20}\equiv 1 \bmod 41$

7) Δείξτε ότι $\varphi(m^2)=m\varphi(m)$

8) Αν $(m,n)=d$, τότε $\varphi(mn)\varphi(d)=d\varphi(m)\varphi(n)$.

9) Να δείξετε ότι ο αριθμός $\frac{1}{5}a^5+\frac{1}{3}a^3+\frac{7}{15}a$ είναι πάντοτε ακέραιος για κάθε ακέραιο a

10) Βρείτε τα δύο τελευταία ψηφία του αριθμού 3^{1000}.

4) $\mathbb{Z}_{17}$ $\quad 3,\ 3^2=9,\ 3^3=27\equiv 10,\ 3^4\equiv 30\equiv -4,\ 3^5\equiv -19\equiv 5,$

$3^6\equiv 15\equiv -2,\ 3^7\equiv -6,\ 3^8\equiv -18\equiv -1$

$3^9\equiv -3,\ 3^{10}\equiv -9 \ \ldots\ 3^{16}\equiv 1 \bmod 17$

$Ord_{17}(3)=16=\varphi(17) \Leftrightarrow$ 3 ένα πρωταρχική ρίζα mod 17

$$\mathbb{Z}_{17}^{*}=\{\underset{3^{16}}{\overset{\shortparallel}{1}},\underset{3^{12}}{\overset{\shortparallel}{2}},\underset{3}{\overset{\shortparallel}{3}},\underset{3^{3}}{\overset{\shortparallel}{4}},\underset{3^{5}}{\overset{\shortparallel}{5}},\underset{3^{14}}{\overset{\shortparallel}{6}},\ \ldots,\ 15,\underset{3^{8}}{\overset{\shortparallel}{16}}\}$$

6) $2^{2n}\equiv 1 \bmod 3$

$(2^2)^n$

$(2^2)^n\equiv (1)^n \bmod n$

$\phi(3)=2$

$2^{3n}\equiv 1 \bmod 7$

$2^{\varphi(7)}\equiv 1 \bmod 7$

$2^6\equiv 1 \bmod 7$

$(8)^n=(2^3)^n=(1)^n \bmod 7$

$2^{20}\equiv 1 \bmod 41$

$\phi(41)=40$

$2^{40}\equiv 1 \bmod 41$, $ord_{(41)}(2)=1,2,4,5,8,$
$10,20,40$

$ord_n(a) \nmid \varphi(n)$

$2,\ 2^2=4,\ 2^4=4^2\equiv 16,\ 2^5\equiv 16\cdot 2\equiv 32\equiv -9 \bmod 41$

$(2^4)^2=2^8\equiv (16)^2=256$

$$\begin{array}{r} 16 \\ \times 16 \\ \hline 256 \end{array} \quad 256 \div 41 = 6,\ \text{remainder } 10$$

$2^8\cdot 2^2=10\cdot 4=40 \bmod 41 \Rightarrow$

$\Rightarrow (2^{10})^2\equiv 1 \bmod 41$

$Ord_{(41)}2=20 \Rightarrow 2^{20}\equiv 1 \bmod 41$

Ασκήσεις Φυλλάδιο #5 2/12/2016

Άσκηση 1

Έστω $n, k \in \mathbb{N}$ με $7n + 11k = 100$

$(7,11) = 1 \mid 100$. Άρα, υπάρχει λύση

$7(-3) + 11 \cdot 2 = 1$

$\Rightarrow 7(-300) + 11 \cdot 200 = 100$

άρα $(x_0, y_0) = (-300, 200)$

Γενική λύση: $x = -300 + 11t$

$y = 200 - 7t, \quad t \in \mathbb{Z}$

Πρέπει $x, y \geq 0$ αφού $x, y \in \mathbb{N}$

$x \geq 0$

$11t \geq 300$

$t \geq \frac{300}{11} = 27,27 \Rightarrow t \geq 28$ (1)

$y \geq 0$

$200 - 7t \geq 0 \Rightarrow 7t \leq 200$

$\Rightarrow t \leq 28$ (2)

Άρα, από (1), (2) $t = 28$

$x = -300 + 11 \cdot 28 = 56$

$y = 200 - 7 \cdot 28 = 44$

2) $\left.\begin{array}{l} 3x + 5y + 7z = 560 \\ 9x + 25y + 49z = 2920 \end{array}\right\} \Rightarrow$

$\Rightarrow \begin{cases} -9x - 15y - 21z = -1680 \\ 9x + 25y + 49z = 2920 \end{cases} \Rightarrow$ $10y + 28z = 1240 \Rightarrow 5y + 14z = 620$ $(5,14) = 1 \mid 620$

$3x + 5y + 7z = 560$

$3 \cdot 620 + \cancel{2} \cdot 620$

$\boxed{\begin{array}{l} y = 3 \cdot 620 + 14t \\ z = -620 - 5t \end{array}}$: λύση διοφαντικής

$3x + 15 \cdot 620 + 70t - 7 \cdot 620 - 35t = 560$

$3x + 35t = 8 \cdot 260 + 560 = A$

$12A \quad -1A$

$\boxed{x = 12A + 35s} \leftarrow$

$t = -A - 3s \rightarrow$ $\boxed{y = 3\,620 + 14(-A - 3s)}$

$\boxed{z = -620 - 5(-A - 3s)}$

3) mod15

$(a, 15) = 1$

$[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}$ — <u>8 κλάσεις</u>

$[1]^{-1}$ $[8]$ $[4]$ $[13]$ $[11]$ $[14]^{-1}$

<u>Επαλήθευση: $\phi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$ κλάσεις</u>

$ord_{15}(2) = 5$ $\quad 2^5 = 1 \bmod 15$ $\quad$ 5 έλαχιστο

$2^{\phi(15)} \equiv 1 \bmod 15$ $\quad 2^8 \equiv 1 \bmod 15$

$ord_{15}(2) = 4$ $\quad 2^4 \equiv 1 \bmod 15$ και $2^3, 2^2, 2 \not\equiv 1 \bmod 15$