ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ
ΤΜΗΜΑ Α
Ασκήσεις # 7

1) Έστω ότι τα υπόλοιπα της ηλικίας του η είναι v_1, v_2 και v_3 από τη διαίρεση με το 3, 5 και 7 αντιστοίχα. Τότε η ηλικία του είναι

$$n \equiv (-35v_1 + 21v_2 + 15v_3) \bmod 105$$

Υπ. Δείξουμε ότι η είναι δεκτός και μικρότερος του 105.

2) Να λυθούν, αν γίνεται, οι επόμενες ισοτιμίες:

α) $7x \equiv 3 \bmod 19$

β) $12x \equiv 16 \bmod 39$

γ) $69x \equiv 21 \bmod 99$

3) Να λυθούν τα συστήματα:

α) $x \equiv 10 \bmod 13$, $x \equiv 16 \bmod 17$

β) $16x \equiv 27 \bmod 41$, $23x \equiv 16 \bmod 43$

γ) $x \equiv 4 \bmod 7$, $x \equiv 9 \bmod 11$, $x \equiv 4 \bmod 13$

4) Να λυθεί η $x^2 \equiv 47 \bmod 11^3$

5) Να λυθεί η $x^2 \equiv 410 \bmod 847 = 7 \cdot 11^2$

6) Να λυθεί το σύστημα

$$2x \equiv 4 \bmod 12$$
$$2x \equiv 8 \bmod 20$$

7) $7x^2 + 28x \equiv \quad \bmod 45$

8) Έστω ότι ο n γράφεται σαν γινόμενο δύο διαφορετικών πρώτων $n = pq$. Αν γνωρίζουμε το n και το $\varphi(n)$ μπορούμε να βρούμε τους p και q;

Φυλλάδιο #7

13/01/2017

Άσκηση 2

$(7, 19) = 1$

α) $7X \equiv 3 \bmod 19 \Rightarrow 11 \cdot 7X \equiv 3 \cdot 11 \bmod 19$

$\exists ??? \; 7^{-1} \bmod 19 \qquad X \equiv 33 \bmod 19$

$7 \cdot 3 \equiv 2 \bmod 19 \qquad X \equiv -5 \bmod 19$

$10 \cdot 7 \cdot 3 \equiv 20 \bmod 19$

$\equiv 1 \bmod 19$

$7^{-1} \equiv 30 \bmod 19 \equiv 11 \bmod 19$

β) $12X \equiv 16 \bmod 39$

Αν $(12, 39) \mid 16$???

$3 \mid 16$ Δεν έχει λύση

γ) $69X \equiv 21 \bmod 99$

$(69, 99) = (3 \cdot 23, 9 \cdot 11) = 3 \mid 21$ έχει λύση

$\frac{69X}{3} \equiv \frac{21}{3} \bmod \frac{99}{3}$

$23X \equiv 7 \bmod 33$ θέλουμε $(23)^{-1} \bmod 33$

$23 \equiv -10 \bmod 33$

$23 \cdot (-10) = 10^2 \bmod 33 \equiv 1 \bmod 33$

$(-10) \cdot 23X \equiv (-10) \cdot 7 \bmod 33$

$X \equiv -70 \bmod 33$

$X \equiv -4 \bmod 33$

Λύση στο mod 99

Λύσεις : 29 $29 + \frac{99}{3} = 62$ και $29 + \frac{2 \cdot 99}{3} = 95$

Άσκηση 3

α) $x \equiv 10 \bmod 13$
$x \equiv 16 \bmod 17$

$(3,17)=1$ Κινέζικο θεώρημα

β) $16x \equiv 27 \bmod 41 \Rightarrow 18 \cdot 16x \equiv 18 \cdot 27 \bmod 41 \Rightarrow x \equiv 18 \cdot 27 \bmod 41$
$23x \equiv 16 \bmod 43 \Rightarrow 15 \cdot 23x \equiv 15 \cdot 16 \bmod 43 \Rightarrow x \equiv 15 \cdot 16 \bmod 43$
Κινέζικο θεώρημα

$(16^{-1}) \bmod 41$
$6 \cdot 3 \cdot 16 \equiv 6 \cdot 7 \equiv 1 \bmod 41$

$2 \cdot 23 \equiv 46 \equiv 3 \bmod 43$
69

$(42 \cdot 14 \cdot 2) 23 \equiv 1 \bmod 43$
-98
15

$14(3) \equiv 42 \bmod 43$

$2 \cdot 23 \equiv 46 \equiv 3 \bmod 43$
$14 \cdot 2 \cdot 23 \equiv 14 \cdot 3 \bmod 43 \equiv -1$
$(42 \cdot 98) \cdot 23 \equiv 1 \bmod 43 \Rightarrow$
$-1 \quad -15$
$\Rightarrow (23)^{-1} \equiv 15 \bmod 43$

γ) $x \equiv 4 \bmod 7$
$x \equiv 9 \bmod 11$
$x \equiv 4 \bmod 13$

$(7, 11, 13) = 1$
Κινέζικο θεώρημα

Άσκηση 6

$2x \equiv 4 \bmod 12$
$2x \equiv 8 \bmod 20$

$\Rightarrow \frac{2x}{2} \equiv \frac{4}{2} \bmod \frac{12}{2}$

$x \equiv 2 \bmod 6$

Λύσεις της $2x \equiv 4 \bmod 12$

$x \equiv 2 \bmod 12$

$x \equiv (2 + \frac{12}{2}) \equiv 8 \bmod 12$

$2x \equiv 8 \bmod 20$

$\frac{2x}{2} \equiv \frac{8}{2} \bmod \frac{20}{2} \Rightarrow x \equiv 4 \bmod 10$

Λύσεις $x \equiv 4 \bmod 20$

$x \equiv (4 + \frac{20}{2}) \equiv 14 \bmod 20$

Το αρχικό σύστημα γίνεται

$x \equiv 2 \bmod 12$ · $x \equiv 4 \bmod 20$

$x \equiv 8 \bmod 12$ $x \equiv 14 \bmod 20$

Αυτές είναι 4 συστήματα

$x \equiv 2 \bmod 12$
$x \equiv 4 \bmod 20$ Έχει λύση αν $(12, 20) \mid 4 - 2$

$4 \nmid 2$

$x \equiv 2 \bmod 12$
$x \equiv 14 \bmod 20$

$(12, 20) = 4 \mid 14 - 2$ Ναι
Έχει λύση

$x \equiv 2 + 12k$ ⊕ να βρεθεί το $k \in \mathbb{Z}$
$2 + 12k \equiv 14 \bmod 20 \Rightarrow 12k \equiv 12 \bmod 20$
$k \equiv 1 \bmod 20 \Rightarrow k = 1 + 20\lambda$ ⊕⇒
$\Rightarrow x = 2 + 12(1 + 20\lambda) = 14 + 240\lambda$ $\lambda \in \mathbb{Z}$

Επαλήθευση:
$(14 + 240\lambda) \equiv 2 \bmod 12$ ✓
$(14 + 240\lambda) \equiv 14 \bmod 20$ ✓

$x \equiv 8 \bmod 12$
$x \equiv 4 \bmod 20$

$(12, 20) = 4 \mid 8 - 4$
Έχει λύση

} λύνεται όπως το προηγούμενο

$x \equiv 8 \bmod 12$
$x \equiv 14 \bmod 20$

$(12, 20) = 4 \nmid 14 - 8 = 6$
Δεν έχει λύση.

Άσκηση 1

$0 < n$ πλήθος < 105

$n \equiv u_1 \bmod 3$

$n \equiv u_2 \bmod 5$

$n \equiv u_3 \bmod 7$

$n \equiv (-35u_1 + 21u_2 + 15u_3) \bmod 105$

$n \equiv (a_1u_1 + a_2u_2 + a_3u_3) \bmod 3 \cdot 5 \cdot 7$

$a_1 \cdot 5 \cdot 7 \equiv 1 \bmod 3$

$a_1 \equiv (5 \cdot 7)^{-1} \bmod 3$

$35 \bmod 3 \equiv 2$, $2 \cdot 2 \equiv 2 \bmod 3$

$2 \equiv -1 \bmod 3$

$35 \equiv 2 \bmod 3$

$-35 \equiv 1 \bmod 3$

Άσκηση 4

$x^2 \equiv 47 \bmod 11^2$

$x^2 \equiv 47 \bmod 11 \equiv 3 \bmod 11$

$11 = 4k+3 = 4 \cdot 2 + 3$

$x \equiv 3^{2+1} \bmod 11$

$\equiv 5 \bmod 11$

$5^2 \equiv 25 \bmod 11 \equiv 3$

Λύσεις: $x \equiv 5 \bmod 11$

$x \equiv -5 \bmod 11 \equiv 6 \bmod 11$

$x \equiv 5 \bmod 11$

$(5+11k)^2 \equiv 47 \bmod 11^2$ Να υπολογιστεί το $k \bmod 11^2$

$25 + 2 \cdot 5 \cdot 11k + 11^2 k^2 \equiv 47 \bmod 11^2$

$2 \cdot 5 \cdot 11 \cdot k \equiv 22 \bmod 11^2$

$5 \cdot 11k \equiv 11 \bmod 11^2$

$5k \equiv 1 \bmod 11$

Θέλουμε $(5^{-1}) \bmod 11 \equiv 9$

$2 \cdot 5 \equiv -1$

$20 \cdot 5 \equiv 1 \bmod 11$

9

$k \equiv 9 \bmod 11$

$x \equiv (5+11 \cdot 9) \bmod 11^2$

$\equiv 104 \bmod 11^2$

Με τον ίδιο τρόπο και η άλλη

Άσκηση 5

$x^2 \equiv 410 \bmod 847 = 410 \bmod (7 \cdot 11^2)$ $\quad (7, 11) = 1$

Ισοδυναμία με $x^2 \equiv 410 \bmod 7 \equiv 4 \bmod 7 \Rightarrow \begin{cases} x \equiv 2 \bmod 7 \\ x \equiv 5 \bmod 7 \end{cases}$

$x^2 \equiv 410 \bmod 11^2 \Rightarrow$

$\Rightarrow x^2 \equiv 47 \bmod 11^2$

$\Rightarrow$ από άσκηση 4

$x \equiv 105 \bmod 11^2$ και η άλλη ⊕

$$\begin{array}{r} 121 \\ \times\ 3 \\ \hline 303 \\ 410 \\ \hline 47 \end{array}$$

Τώρα το σύστημα γίνεται

$$\left.\begin{array}{l} x \equiv 2 \bmod 7 \\ x \equiv 104 \bmod 11^2 \\ (7, 11)^2 = 1 \end{array}\right\} \Rightarrow$$

Κινέζος

$(11^2)^{-1} \bmod 7 = (121)^{-1} \bmod 7 \equiv (2)^{-1} \bmod 7$

$\equiv 4$

$121 \mid 7$
$31 \quad 17$
2

$x = 4 \cdot 2 +$ → $x \equiv (4 \cdot 2 + 52 \cdot 104) \bmod 7 \cdot 11^2$

$(7)^{-1} \bmod 121$

$18 \cdot 7 = 126$

$121 = 7 \cdot 17 + 2$

$7 = 2 \cdot 3 + 1$

$1 = 7 - 2 \cdot 3$

$1 = 7 - (121 - 7 \cdot 17) 3$

$1 = 7 - 3 \cdot 121 + 7 \cdot 51$

$1 = 7 \cdot 52 - 3 \cdot 121$

$\ldots$

$(7)^{-1} \equiv 52 \bmod 121$

Άσκηση 7

$7x^2 + 28x \equiv 0 \bmod (45 = 5 \cdot 9 = 5 \cdot 3^2)$

$7(x^2 + 4x + 2^2) - 7 \cdot 2^2 \equiv 0 \bmod (5 \cdot 3^2)$

2 ② x

Θέτουμε $y = (x+2) \overset{+}{\equiv} 92 \bmod 45 \Rightarrow x \equiv 90 \bmod 45 \equiv 0 \bmod 45$

$7y^2 \equiv 7 \cdot 4 \bmod (5 \cdot 3^2)$

$(7)^{-1} \bmod 45 \equiv 13$

$7y^2 \equiv 7 \cdot 4 \bmod (5 \cdot 3^2)$

$13 \cdot 7 \cdot y^2 \equiv 13 \cdot 7 \cdot 4 \bmod (5 \cdot 3^2)$

$y^2 \equiv 13 \cdot 7 \cdot 4 \bmod 5 \cdot 3^2 \equiv 4 \bmod 5 \cdot 3^2$

$\begin{pmatrix} y^2 \equiv 4 \bmod 5 \\ y^2 \equiv 4 \bmod 9 \end{pmatrix}$ Ζυγότητα $\rightarrow y \equiv \pm 2 \bmod 5$

$\longrightarrow y^2 \equiv 4 \bmod 3 \rightarrow y \equiv 2 \bmod 3$

$y \equiv -2 \bmod 3$

$(2+3k)^2 \equiv 4 \bmod 9$

$4 + 2 \cdot 2 \cdot 3k + 3^2 k^2 \equiv 4 \bmod 9$

$3k \equiv 0 \bmod 9$

$k = 3 \Rightarrow y \equiv (2 + 3 \cdot 3) \bmod 9 \equiv 2$

$y \equiv 2 \bmod 5 \quad (5,9) = 1$ Κινέζικο Θεώρημα

$y \equiv 2 \bmod 9$

$y \equiv (2 \cdot 4^9 + 2 \cdot 2^5) \bmod (45)$

$y \equiv 92 \bmod 45$ ⊕