6/12/2018

Άσκηση Να λυθεί η ισοτιμία $3X \equiv 5 \bmod 7$

$\mu\kappa\delta(3,7) = 1$

$3X \equiv 5 \bmod 7$

$5 \cdot 3X \equiv 5 \cdot 5 \bmod 7$

$15X \equiv 25 \bmod 7$

$X \equiv 4 \bmod 7$

Άσκηση Να λυθεί η ισοτιμία $6X \equiv 5 \bmod 8$

$\mu\kappa\delta(6,8) = 2 \not| 5$. Άρα η ισοτιμία δεν έχει λύση

Άσκηση Να λυθεί η ισοτιμία $6X \equiv 2 \bmod 8$

$\mu\kappa\delta(6,8) = 2 | 2$ Άρα η ισοτιμία έχει λύση

(δύο λύσεις σε μόδιο 8, όσες είναι ο μκδ μεταξύ)

$6X \equiv 2 \bmod 8$ $\quad \left(\begin{array}{l} 8 | 6-2 \\ 2 \cdot 4 | 2 | 3x-1 \\ 4 | 3x-1 \end{array} \right)$

$3X \equiv 1 \bmod 4$

$33X \equiv 3 \bmod 4$

$9X \equiv 3 \bmod 4$

$X \equiv 3 \bmod 4 \longrightarrow \begin{cases} X \equiv 3 \bmod 8 \\ X \equiv 3+4 \bmod 8 \Rightarrow X \equiv 7 \bmod 8 \end{cases}$

Άσκηση Να λυθεί η ισοτιμία $1204X \equiv 47 \bmod 1453$

$(1453, 1204) = 1 | 47$, συνεπώς η ισοτιμία έχει λύση (μια λύση)

$1453 = 1 \cdot 1204 + 249$

$1204 = 4 \cdot 249 + 208$

$249 = 1 \cdot 208 + 41$

$208 = 5 \cdot 41 + 3$

$41 = 13 \cdot 3 + 2$

$3 = 1 \cdot 2 + \boxed{1}$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 2\cdot 1 = 3 - (41 - 13\cdot 3) =$
$= 14\cdot 3 - 41 = 14\cdot(208 - 5\cdot 41) - 41 =$
$= 14\cdot 208 - 71\cdot 41$
$= 14\cdot 208 - 71(249 - 208)$
$= 85\cdot 208 - 71\cdot 249$
$= 85(1204 - 4\cdot 249) - 71\cdot 249$
$= 85\cdot 1204 - 411\cdot 249$
$= 85\cdot 1204 - 411(1453 - 1204)$
$= \boxed{496}\,1204 - 411\cdot 1453$

πάντα το ένα θα είναι θετικό και το άλλο αρνητικό

$1 = 496\cdot 1204 - 411\cdot 1453$
$1 \equiv 496\cdot 1204 - 411\cdot 1453^{0} \bmod 1453$
$1 \equiv \boxed{496}\cdot 1204 \bmod 1453$
↳ αντίστροφο του 1204

$1204X \equiv 47 \bmod 1453$
$496\cdot 1204\,X \equiv 496\cdot 47 \bmod 1453$
1
$1X \equiv 496\cdot 47 \bmod 1453$
$496\cdot 47 = 23312 / 1453 = 16$
$X \equiv 16 \bmod 1453$

Άσκηση Να λυθεί η ισοτιμία $30X \equiv 12 \bmod 42$
$\mu\kappa\delta(30,42) = 6 \mid 12$ Άρα η ισοτιμία έχει λύση (6 λύσεις modulo 42; 1 λύση modulo 42 διά 16)

$42 = 1\cdot 30 + 12$
$30 = 2\cdot 12 + 6$
$12 = 2\cdot 6 + 0$

$30X \equiv 12 \bmod 42$
$6\cdot 5X \equiv 6\cdot 2 \bmod 67$
$5X \equiv 2 \bmod 7$
$3\cdot 5X \equiv 3\cdot 2 \bmod 7$
$15X \equiv 6 \bmod 7 \Rightarrow X \equiv 6 \bmod 7$

$X \equiv 6 + 0\cdot 7 \bmod 42$
$X \equiv 6 + 1\cdot 7 \bmod 42$
$X \equiv 6 + 2\cdot 7 \bmod 42$
$X \equiv 6 + 3\cdot 7 \bmod 42$
$X \equiv 6 + 4\cdot 7 \bmod 42$
$X \equiv 6 + 5\cdot 7 \bmod 42$

Άσκηση Να βρεθεί το υπόλοιπο του $44!$ με το 47.

$44! \equiv x \bmod 47$, $0 \le x < 47$

Wilson. Το 47 είναι πρώτος αριθμός / Αν όχι τότε ο 47 είναι σύνθετος, συνεπώς έχει ένα πρώτο διαιρέτη $p \le \sqrt{47} \simeq 6\ldots$, δηλαδή έναν από τους $2, 3, 5$)

$2 \nmid 47$ αφού 47 περιττός

$3 \nmid 47$ αφού $3 \nmid 4+7=11$ αφού $3 \nmid 1+1=2$

$5 \nmid 47$ αφού $5 \nmid 7$

Άρα 47 πρώτος αριθμός

$(p-1)! \equiv -1 \bmod p$ αν p πρώτος

$46! \equiv -1 \bmod 47$

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot 43 \cdot 44 \cdot 45 \cdot 46 \equiv -1 \bmod 47$

($1 \cdot 2 \cdot 3 \cdot \ldots \cdot 43 \cdot 44 = 44!$)

Αν ένας αριθμός διαιρείται από το 3 αν το 3 διαιρεί το άθροισμα των ψηφίων του

$x \cdot 45 \cdot 46 \equiv -1 \bmod 47$

$x \cdot 45 \cdot (-1) \equiv -1 \bmod 47$

$x \cdot (-2+1)(-1) \equiv -1 \bmod 47$

$-2x \equiv 1 \bmod 47$

$2x \equiv -1 \bmod 47$

$24 \cdot 2 \cdot x \equiv -24 \cdot 1 \bmod 47$

$48x \equiv -24 \bmod 47$

$(47+1)x \equiv -24 \bmod 47$

$1x \equiv 23 \bmod 47$

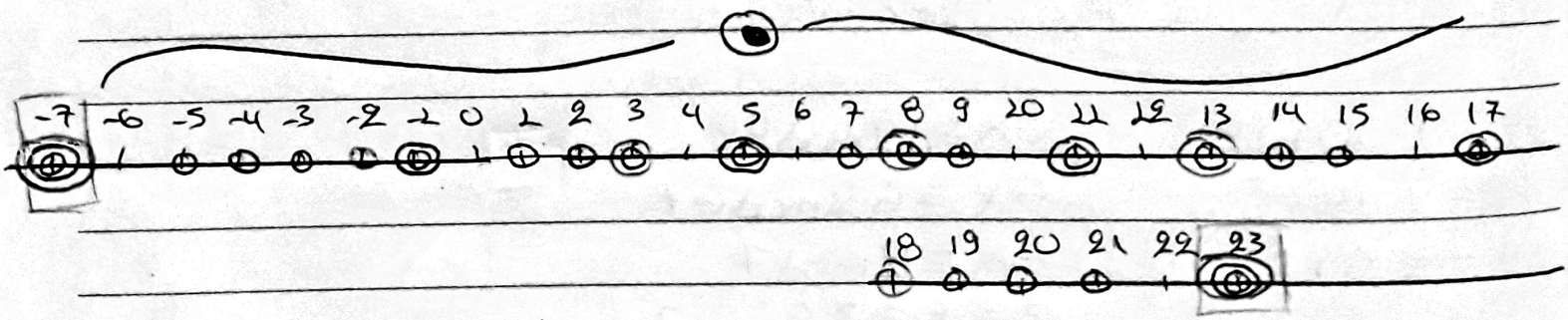
ή

$2x \equiv 46 \bmod 47$

$2x \equiv 2 \cdot 23 \bmod 47$

$\mu\kappa\delta(2, 47) = 1$

$x \equiv 23 \bmod 47$



Σύστημα

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \end{cases}$$

$x \equiv 23 \bmod 30$

Κινέζικο Θεώρημα

Έστω $m_1, m_2, \ldots, m_r$ φυσικοί αριθμοί πρώτοι μεταξύ τους ανά δύο, δηλαδή $\text{μκδ}(m_i, m_j) = 1$ αν $i \neq j$. Τότε το σύστημα των γραμμικών ισοτιμιών

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_r \bmod m_r \end{cases}$$

έχει μοναδική λύση $\bmod M$, όπου $M = m_1 m_2 \ldots m_r$

$M = m_1 m_2 \ldots m_r$, $M_i = \frac{M}{m_i}$, $b_i M_i \equiv 1 \bmod m_i$

$x \equiv a_1 b_1 M_1 + a_2 b_2 M_2 + \ldots + a_r b_r M_r \bmod M$, η λύση του συστήματος

$x_0 = a_1 b_1 M_1 + a_2 b_2 M_2 + \ldots + a_r b_r M_r + \lambda M$

$x_0 \equiv a_1 \bmod m_1$

$x_0 \equiv a_r \bmod m_r$

Παράδειγμα

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 6 \\ x \equiv 2 \bmod 11 \end{cases}$$

$\text{μκδ}(7,6) = 1$, $\text{μκδ}(6,11) = 1$, $\text{μκδ}(11,7) = 1$

Άρα εφαρμόζεται το κινέζικο Θεώρημα.

	a_i	M_i	b_i
	3	6·11	5
	5	7·11	-1
	2	7·6	5

$M = 7 \cdot 6 \cdot 11$

$M_1 = 6 \cdot 11$

$M_2 = 7 \cdot 11$

$M_3 = 7 \cdot 6$

$b_i M_i \equiv 1 \bmod m_i$

$b_1 M_1 \equiv 1 \bmod m_1$

$b_1 \cdot 6 \cdot 11 \equiv 1 \bmod 7$

$b_1 \cdot 66 \equiv 1 \bmod 7$

$b_1 \cdot 3 \equiv 1 \bmod 7$

$b_1 \equiv 5 \bmod 7$

$b_2 M_2 \equiv 1 \bmod m_2$

$b_2 7 \cdot 11 \equiv 1 \bmod 6$

$b_2 (4(-2) \equiv 1 \bmod 6$

$-b_2 \equiv 1 \bmod 6$

$b_2 \equiv -1 \bmod 6$

$b_3 M_3 \equiv 1 \bmod m_3$

$b_3 7 \cdot 6 \equiv 1 \bmod 11$

$b_3 \cdot 42 \equiv 1 \bmod 11$

$b_3 \cdot 9 \equiv 1 \bmod 11$

$b_3 \equiv 5 \bmod 11$

$x \equiv 3 \cdot 6 \cdot 11 \cdot 5 + 5 \cdot 7 \cdot 11 \cdot (-1) + 2 \cdot 7 \cdot 6 \cdot 5 \bmod 7 \cdot 6 \cdot 11$

$x \equiv 15 \cdot 6 \cdot 11 - 5 \cdot 7 \cdot 11 + 10 \cdot 7 \cdot 6 \bmod 7 \cdot 6 \cdot 11$

$x \equiv (2 \cdot 7 + 1) 6 \cdot 11 - (6-1) \cdot 7 \cdot 11 + (11-1) \cdot 7 \cdot 6 \bmod 7 \cdot 6 \cdot 11$

$x \equiv 2 \cdot \cancel{7 \cdot 6 \cdot 11}^{0} + 1 \cdot 6 \cdot 11 - \cancel{6 \cdot 7 \cdot 11}^{0} + 7 \cdot 11 + \cancel{11 \cdot 7 \cdot 6}^{0} - 7 \cdot 6 \bmod 6 \cdot 7 \cdot 11$

$x \equiv 66 + 77 - 42 \bmod 6 \cdot 7 \cdot 11$

$x \equiv 143 - 42 \bmod 6 \cdot 7 \cdot 11$

$x \equiv 101 \bmod 6 \cdot 7 \cdot 11$

Παράδειγμα

$$\begin{cases} x \equiv 7 \bmod 11 \\ x \equiv 7 \bmod 23 \\ x \equiv 7 \bmod 37 \end{cases}$$

$\mu\kappa\delta(11,23) = 1$

$\mu\kappa\delta(11,37) = 1$

$\mu\kappa\delta(23,37) = 1$

Άρα εφαρμόζω το κινέζικο θεώρημα. Το σύστημα έχει μοναδική λύση modulo $M = 11 \cdot 23 \cdot 37$

$x \equiv 7 \bmod 11 \cdot 23 \cdot 37$

Παράδειγμα

$$\begin{cases} x \equiv 9 \bmod 11 \\ x \equiv 21 \bmod 23 \\ x \equiv 35 \bmod 37 \end{cases}$$

$\mu\kappa\delta(11,23) = 1$

$\mu\kappa\delta(11,37) = 1$

$\mu\kappa\delta(23,37) = 1$

Άρα εφαρμόζω το κινέζικο θεώρημα. Το σύστημα έχει μοναδική λύση modulo $M = 11 \cdot 23 \cdot 37$

$x \equiv -2 \bmod 11 \cdot 23 \cdot 37$