29/11/2016

Wilson $(p-1)! \equiv -1 \bmod p$, p πρώτος

Π.χ. p πρώτος $>2$

$(1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2))^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$

p πρώτος $>2$ $\Rightarrow$ p περιττός $\Rightarrow$ $(p-2)$ περιττός

$2 \cdot 1 \quad 2 \cdot 2 \quad 2 \cdot 3 \quad \ldots \quad 2 \cdot \frac{p-1}{2}$ άρτιος

$2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)$

$(-(p-2)) \cdot \ldots \cdot (-1) \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdots (p-2)$

$\cdot (-(p-4))$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot (p-2)(p-1) \equiv -1 \bmod p$

$1 \cdot 3 \cdot 5 \cdot (p-2) \cdot 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv -1 \bmod p \Rightarrow$

$\Rightarrow (1 \cdot 3 \cdot 5 \cdots (p-2))^2 (-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$

$(1 \cdot 3 \cdot 5 \cdots (p-2))^2 (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \equiv (-1)(-1)^{\frac{p-1}{2}} \bmod p$

$(1 \cdot 3 \cdot 5 \cdots (p-2))^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$

$a^2 \equiv -1 \bmod p$

Όταν $\frac{p+1}{2} = 2k+1 \Rightarrow p = 4k+1$

$x^2 \equiv -1 \bmod p$

**Θεώρημα**

Έστω $p$ περιττός πρώτος. Η εξίσωση $x^2 \equiv -1 \bmod p$ έχει λύση $\bmod p$ αν και μόνο αν $p = 4k+1$

**Παράδειγμα**

1) $p=13$. Να βρεθεί η λύση της $x^2 \equiv -1 \bmod p$, αν υπάρχει.

Για με $1 \le a \le p-1 = 12$ ώστε $a^2 \equiv -1 \bmod p$

**Λύση**

$p=13$

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 3 \bmod 13$

$5^2 = 25 \equiv -1 \bmod 13$

Η $x^2 \equiv -1 \bmod p$ έχει λύση το $5 \bmod 13$

και $p-5 = 13-5 = 8 \bmod 13$

2) Να ~~βρεθεί~~ αν η $x^2 \equiv -1 \bmod 11$ αν λύνεται

**Λύση**

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 5 \bmod 11$

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

$6 = -(11-6) \equiv -5 \bmod 11$

$7 = -(11-7) = -4 \bmod 11$

Δεν έχει λύσεις.

# Γραμμικές Ισοδυναμίες

Παράδειγμα

1) Να λυθεί η $5X \equiv 3 \bmod 24$

Λύση

$\exists$ ο αντίστροφος του 5 $\equiv$
Είναι η κλάση $[5]_{24}$ αντιστρέψιμη,
Επειδή $(5,24)=1 \Leftrightarrow \exists\ [5]^{-1}_{24} = [5]_{24}$

$5X \equiv 3 \bmod 24 \Rightarrow 5 \cdot 5X \equiv 5 \cdot 3 \bmod 24 \Rightarrow X \equiv 15 \bmod 24$

Μοναδική λύση

2) $90X \equiv 3 \bmod 37$

Λύση

$16X \equiv 3 \bmod 37$

$(16,37)=1 \Leftrightarrow \exists\ [16]^{-1}_{37}$

1ος τρόπος:

Ιδιότητα: $37 = 2 \cdot 16 + 5 \Rightarrow 5 = 37 - 2 \cdot 16$

$16 = 3 \cdot 5 + 1 \Rightarrow 1 = 16 - 3 \cdot 5 = 16 - 3(37 - 2 \cdot 16)$

$= -3 \cdot 37 + 7 \cdot 16$

άρα $[16]^{-1}_{37} = [7]_{37}$

2ος τρόπος:

Euler $\Rightarrow 16^{\phi(37)} \equiv 1 \bmod 37$

$16^{37} \equiv 1 \bmod 37$

$16 \cdot (16^{35}) \equiv 1 \bmod 37$

↑ αντίστροφος του 16

3) Να λυθεί $540x \equiv 18 \bmod 462$, αν λύνεται

Λύση

$348x \equiv 18 \bmod 462$

$(348, 462) = 6$

$462 = 5 \cdot 348 + 252$

$348 = 1 \cdot 252 + 96$

$\Rightarrow$ Αν $\frac{348x}{6} + \frac{462\beta}{6} = \boxed{\frac{18}{6}}$ ← από αυτό εξαρτάται αν έχει λύση
αν το διαιρεί έχει λύση
αν δεν το διαιρεί δεν έχει λύση

$\Rightarrow 58x + 77\beta = 3$

$58x \equiv 3 \bmod 77$

$(58, 77) = 1 \Leftrightarrow \exists\ [58]^{-1}_{\bmod 77}$

$[58]^{-1}_{77} = [6]_{77}$

$6 \cdot 58x \equiv 6 \cdot 3 \bmod 77$

$x \equiv 18 \bmod 77$

Επαλήθευση

$348 \cdot 18 = 1404 \bmod 462 \equiv 18$

$18 + 77 = 95$

$95 \cdot 348 \mid 462$

$18$

## Θεώρημα

Η εξίσωση $ax \equiv b \bmod n$ έχει λύση στους ακέραιους αν $(a,n) = \delta \mid b$.

Αν έχει λύσεις και $x_0$ είναι μια λύση, τότε όλες οι λύσεις $\bmod n$ δίνονται από $x_0, x_0 + \frac{n}{\delta}, x_0 + 2\frac{n}{\delta}, \dots, x_0 + (\delta-1)\frac{n}{\delta}$

## Απόδειξη

"$\Rightarrow$" Αν $x_0$ είναι μια λύση, τότε $ax \equiv b \bmod n \Leftrightarrow$
$ax_0 - b = kn$

Επειδή $\delta \mid a$, $n \Rightarrow \delta \mid ax_0$,
$kn \Rightarrow \delta \mid ax_0 - kn = b$

"$\Leftarrow$" Έστω ότι $\delta = (a,n) \mid b$

Η εξίσωση $ax \equiv b \bmod n$ γράφεται

$$ax - b = kn \Leftrightarrow \frac{a}{\delta}x - \frac{b}{\delta} = k\frac{n}{\delta} \Rightarrow$$

$$\Rightarrow \frac{a}{\delta}x = \frac{b}{\delta} \bmod \left(\frac{n}{\delta}\right)$$

$$\left(\frac{a}{\delta}, \frac{n}{\delta}\right) = 1 \Leftrightarrow \exists \left[\frac{a}{\delta}\right]^{-1}_{\frac{n}{\delta}}$$

$\frac{a}{\delta}x \equiv \frac{b}{\delta} \bmod \frac{n}{\delta}$ έχει μοναδική λύση

$$\left(\frac{a}{\delta}\right)^{-1} \frac{a}{\delta}x \equiv \left(\frac{a}{\delta}\right)^{-1} \frac{b}{\delta} \bmod \left(\frac{n}{\delta}\right) \Rightarrow \quad x \equiv \left(\frac{a}{\delta}\right)^{-1} \frac{b}{\delta} \bmod \left(\frac{n}{\delta}\right)$$

Υποθέσαμε ότι υπάρχουν δύο λύσεις $x_0$ και $y_0$ $\bmod n$

$$\left.\begin{array}{l} ax_0 \equiv b \bmod n \\ ay_0 \equiv b \bmod n \end{array}\right\} \Rightarrow a(x_0 - y_0) \equiv 0 \bmod n \Rightarrow$$

$\Rightarrow \frac{a}{\delta}(x_0 - y_0) \equiv 0 \bmod \left(\frac{n}{\delta}\right)$

Επειδή $\left(\frac{a}{\delta}, \frac{n}{\delta}\right) = 1 \Rightarrow x_0 - y_0 \equiv 0 \bmod \frac{n}{\delta}$

Άρα, $y_0 = x_0 \bmod \frac{n}{\delta} \Leftrightarrow$

$y_0 = x_0 + k\frac{n}{\delta}$

Θέλαμε τη λύση $\bmod n$.
Οι διακεκριμένες λύσεις βρίσκονται για $0 \le k \le \delta - 1$

Παράδειγμα

$6x \equiv 12 \bmod 36$ $\quad (6, 36) = 6 \mid 12$

$\frac{6}{6}x \equiv \frac{12}{6} \bmod \frac{36}{6}$

$x = 2 \bmod 6$

$x_0 = 2$ $\quad x_1 = 2 + \frac{36}{6} = 8$ $\quad x_4 = 2 + 4 \cdot 6 = 26$

$x_2 = 2 + 2 \cdot 6 = 14$

Πόρισμα
Αν $(a, n) = 1$, τότε η $ax \equiv b \bmod n$ έχει μοναδική λύση η οποία δίνεται από
$x \equiv a^{\varphi(n)-1} b \bmod n$

Παράδειγμα

1) Να βρείτε το $2^n \bmod 17$ για όλα τα $n$.

Λύση

$2^0=1,\ 2^1=2,\ 2^2=4,\ 2^3=8,\ 2^4=16\equiv -1 \bmod 17$

$2^5\equiv -2,\ 2^6\equiv -4,\ 2^7\equiv -8,\ 2^8=-16\equiv 1 \bmod 17$

$2^9=2$

$\{1, 2, 4, 8, -1, -2, -4, -8\}$

2) Να βρεθεί το $3^n \bmod 17$ για όλα τα $n$

Λύση

$3^0=1,\ 3^1=3,\ 3^2=9,\ 3^3=10\equiv -7 \bmod 17$

$3^4=-21\equiv -4,\ 3^5\equiv -12,\ 3^6\equiv -36\equiv -2$

$3^7=-6,\ 3^8\equiv -1,\ 3^9\equiv -3,\ 3^{10}\equiv -9$

$3^{11}\equiv 7,\ 3^{12}\equiv 4,\ 3^{13}\equiv 12,\ 3^{14}=2,\ 3^{15}\equiv 6,\ 3^{16}\equiv 1$

Γνωρίζουμε ότι αν $(a,n)=1$ τότε $a^{\varphi(n)}\equiv 1 \bmod n$

Π.χ. $2^{\varphi(17)}=2^{16}\equiv 1 \bmod 17$

αλλά $2^8\equiv 1 \bmod 17$

Αλλά για το 3 έχουμε

$3^{\varphi(17)}\equiv 1 \bmod 17$ και

δεν υπάρχει $1\le k<\phi(17)$ ώστε $3^k\equiv 1 \bmod 17$

**Ορισμός**

Έστω $n > 1$ και $a \in \mathbb{Z}^*$ με $(a,n)=1$. Ονομάζουμε τάξη του $a$ mod $n$ τον ελάχιστο φυσικό αριθμό $k$ ώστε $a^k \equiv 1 \bmod n$.

Γράφουμε $k = \text{ord}_n(a)$

**Πχ** $\text{ord}_{11}(2)=8$ , $\text{ord}_{17}(3)=16$.

$\text{ord}_{55}(12) = ? = 4$

$(12,55) = (2^2 \cdot 3, 5 \cdot 11) = 1$

Μέγιστη δύναμη $\phi(55) = \varphi(5)\cdot\varphi(11) = 4 \cdot 10 = 40$

$12^2 = 144 \equiv 34 \bmod 55$

$\equiv -21 \bmod 55$

$12^4 \equiv 21^2 \bmod 55 = 1$

$21 \times 21 = 441$