3/12/2018

**Θεώρημα Euler** : Αν $\text{μκδ}(a,n)=1$, τότε:

$$a^{\phi(n)} \equiv 1 \bmod n$$

**Θεώρημα Fermat**: Αν $\text{μκδ}(a,p)=1$, $p$: πρώτος, τότε:

$$a^{p-1} \equiv 1 \bmod p$$

**Πόρισμα** Για κάθε $a$ ισχύει:

$$a^p \equiv a \bmod p$$

Άσκηση Βρείτε το υπόλοιπο της διαίρεσης του $11^{241}$ με το 35

Λύση Euler με $\delta(11,35)=1$

$$11^{\phi(35)} \equiv 1 \bmod 35$$

$$\phi(35)=\phi(5\cdot 7)=5^{1-1}(5-1)\,7^{1-1}(7-1)=24$$

$$*\ \phi(p_1^{a_1}p_2^{a_2}\dots p_s^{a_s})=p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\dots p_s^{a_s-1}(p_s-1)$$

$$11^{24}\equiv 1 \bmod 35$$

$$11^{241}\equiv 11^{24\cdot 10+1} \bmod 35$$
$$\equiv 11^{24\cdot 10}\cdot 11 \bmod 35$$
$$\equiv (11^{24})^{10}\cdot 11 \bmod 35$$
$$\equiv 1^{10}\cdot 11 \bmod 35$$
$$\equiv 11 \bmod 35,\ 0\le 11<35$$

Άρα, το υπόλοιπο της διαίρεσης είναι ίσο με 11

Άσκηση Βρείτε το υπόλοιπο της διαίρεσης του $5^{24}$ με το 35

Λύση $\mu\kappa\delta(5,35)=5\neq 1$ (Άρα δεν μπορώ να χρησιμοποιήσω το θεώρημα του Euler)

$5^1\equiv 5 \bmod 35$

$5^2\equiv 25 \bmod 35$
$\equiv -10 \bmod 35$

$5^3\equiv 5^2\cdot 5 \bmod 35$
$\equiv (-10)\cdot 5 \bmod 35$
$\equiv -50 \bmod 35$
$\equiv 20 \bmod 35$

$5^4\equiv 5^3\cdot 5 \bmod 35$
$\equiv 20\cdot 5 \bmod 35$
$\equiv 100 \bmod 35$
$\equiv -5 \bmod 35$

$5^5\equiv 5^4\cdot 5 \bmod 35$
$\equiv -5\cdot 5 \bmod 35$
$\equiv -25 \bmod 35$
$\equiv 10 \bmod 35$

$5^6\equiv 5^5\cdot 5 \bmod 35$
$\equiv 10\cdot 5 \bmod 35$
$\equiv 50 \bmod 35$
$\equiv 15 \bmod 35$

$5^7\equiv 5^6\cdot 5 \bmod 35$
$\equiv 15\cdot 5 \bmod 35$
$\equiv 75 \bmod 35$
$\equiv 5 \bmod 35$
$5^7\equiv 5 \bmod 35$

(Μετά επαναλαμβάνονται οι ίδιες δυνάμεις)

$5^7\equiv 5 \bmod 35$

$(5^7)^3\equiv 5^3 \bmod 35$

$5^{21} \equiv 5^3 \bmod 35$

$5^{24} \equiv 5^3 \cdot 5^3 \bmod 35$

$5^{24} \equiv 5^6 \bmod 35$

$\equiv 15 \bmod 35$

Άρα, το υπόλοιπο του $5^{24}$ δια του 35 είναι 15.

**Παράδειγμα:**

$10! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \pmod{11}$

(όλοι αυτοί είναι πρώτοι με το 11 επειδή όλοι μικρότεροι του 11 και έχουν αντίστροφο.)

(2 και 6 είναι αντίστροφα ($2 \cdot 6 = 1$))

$\equiv 1 \cdot 10 \bmod 11$ Το 1 και το 10 έχουν αντίστροφο τον εαυτό τους.

$\equiv 10 \bmod 11$

$\equiv -1 \bmod 11$ (2,6), (3,4), (5,9), (7,8) αντίστροφα, άρα απλοποιούνται από το γινόμενο

**Θεώρημα Wilson** Αν $p$: πρώτος αριθμός, τότε:

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

Στο γινόμενο $1 \cdot 2 \cdot 3 \cdots (p-1)$ όλα τα στοιχεία είναι αντίστροφα και κάθενα από αυτά έχει στο γινόμενο το αντίστροφό του, οπότε απλοποιείται εκτός από αυτά που έχουν αντίστροφο τον εαυτό τους.
Έστω $a$ ένα τέτοιο στοιχείο, τότε:

$a a \equiv 1 \bmod p \Leftrightarrow a^2 \equiv 1 \bmod p \overset{\text{ορισμός}}{\Rightarrow} p \mid a^2 - 1 \Rightarrow$

$\Rightarrow p \mid (a-1)(a+1) \Rightarrow p \mid a-1$ ή $p \mid a+1 \Rightarrow$

($p$ πρώτος)

$\Rightarrow a \equiv 1 \bmod p$ ή $a \equiv -1 \bmod p$

$\equiv p-1 \bmod p$

Άρα $(p-1)! \equiv 1 \cdot (p-1) \bmod p$

$\equiv p-1 \bmod p$

$\equiv -1 \bmod p$

Παράδειγμα Υπολογίστε: $12! \equiv (\ ) \bmod 13$

$12! \equiv (\ ) \bmod 11$

Λύση $12! \equiv (\ ) \bmod 13 \Rightarrow (13-1)! \equiv -1 \bmod 13$ (Wilson)

$\equiv 12 \bmod 13$

$12! \equiv (\ ) \bmod 11 \Rightarrow 12! \equiv 0 \bmod 11$

$12! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \bmod 11$

↳ ισούται με 11 είναι το 0

$\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 0 \cdot 12 \bmod 11$

$\equiv 0 \bmod 11$

## Γραμμικές Ισοτιμίες

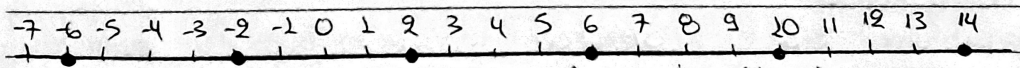
Ορισμός> Ονομάζουμε γραμμική ισοτιμία κάθε ισοτιμία της μορφής $ax \equiv b \bmod n$, όπου $a, b \in \mathbb{Z}$ και $n \in \mathbb{N}$.

Ορισμός> Λέμε ότι το $x_0 \in \mathbb{Z}$ είναι λύση της ισοτιμίας αν $ax_0 \equiv b \bmod n$

Παράδειγμα $3x \equiv 2 \bmod 4$. Το 6 είναι λύση της ισοτιμίας

$3 \cdot 6 \equiv 2 \bmod 4$

Το 7 δεν είναι λύση της ισοτιμίας $3 \cdot 7 \not\equiv 2 \bmod 4$

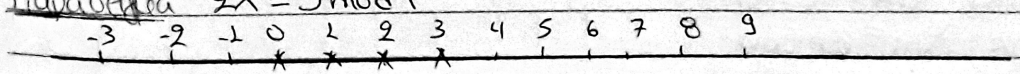



Αν έχει μία λύση, έχει άπειρες

$x \equiv 2 \bmod 4$, $2 \bmod 4$

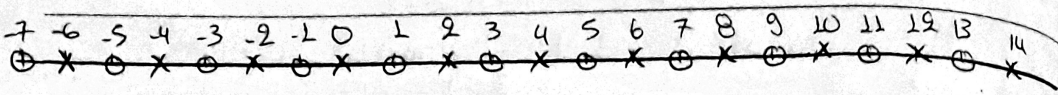
Αν το $x_0$ είναι λύση της $ax \equiv b \bmod n$, τότε κάθε $x_1 \equiv x_0 \bmod n$ είναι λύση της $ax \equiv b \bmod n$.

Παράδειγμα $2x \equiv 3 \bmod 4$




Η $2x \equiv 3 \bmod 4$ δεν έχει λύση.

Παράδειγμα $2x \equiv 2 \bmod 4$




$2x \equiv 2 \bmod 4$

$x \equiv 1 \bmod 4$ ή $x \equiv 3 \bmod 4$

$x \equiv 1 \bmod 2$

Θεώρημα Η γραμμική ισοτιμία $ax \equiv b \bmod n$ έχει λύση αν και μόνο αν $\delta = \mu\kappa\delta(a,n) \mid b$. Αν $\delta \mid b$, τότε υπάρχουν ακριβώς $\delta$ λύσεις modulo $n$, οι $x_0 \bmod n$, $x_0 + \frac{n}{\delta} \bmod n$, $x_0 + (\delta-1)\frac{n}{\delta} \bmod n$

και ακριβώς μία modulo $\frac{n}{\delta}$

Παράδειγμα $2x \equiv 3 \bmod 4$

$\mu\kappa\delta(2,4) = 2 \times 3$, άρα δεν έχει λύση.

Απόδειξη ($\Rightarrow$) Η $ax \equiv b \bmod n$ έχει λύση. Άρα υπάρχει $x_0 \in \mathbb{Z}$, τέτοιο ώστε $ax_0 \equiv b \bmod n \Rightarrow n \mid ax_0 - b \Rightarrow ax_0 - b = kn \Rightarrow$

$\Rightarrow ax_0 - kn = b$

$\left.\begin{matrix} \delta = \mu\kappa\delta(a,n) \\ \delta \mid a \\ \delta \mid n \end{matrix}\right\} \Rightarrow \delta \mid \overline{x_0}\, a + \overline{-k}\, n = b \Rightarrow \delta \mid b$

($\Leftarrow$) $\delta \mid b \Rightarrow \delta = \mu\kappa\delta(a,n) \mid b$

$b = \lambda\delta \overset{\text{ευκλείδης}}{\Rightarrow} \delta = \kappa a + \mu n$

$\delta = \mu\kappa\delta(a,n)$

$ak + \mu n = \delta$

$a\lambda k + \lambda\mu n = \lambda\delta = b$

$a\lambda k + \lambda\mu n \equiv b \bmod n$

$a\overline{\lambda k} \mid \equiv b \bmod n$. Άρα $x_0 = \lambda k$ είναι λύση.

Έστω $\delta \mid b$ και $x_0$ λύση της $ax \equiv b \bmod n$. Άρα $ax_0 \equiv b \bmod n$

Οι $x_0 \bmod n$, $x_0 + \frac{n}{\delta} \bmod n$ και $x_0 + (\delta-1)\frac{n}{\delta} \bmod n$ είναι λύσεις

αν $ax \equiv b \bmod n$

Έστω $x_1 = x_0 + \lambda\frac{n}{\delta} + \mu n$ μια από αυτές

$ax_1 \equiv a(x_0 + \lambda\frac{n}{\delta} + \mu n) \bmod n$

$\equiv ax_0 + a\lambda\frac{n}{\delta} \bmod n$

$\delta = \mu\kappa\delta(a,n)$, $\delta | a \Rightarrow a = a'\delta$

$ax \equiv ax_0 + a'\delta\frac{n}{\delta} \bmod n$

$\equiv b \bmod n$

Έστω $x_1$ λύση της $ax \equiv b \bmod n$

$ax_1 \equiv b \bmod n$

$ax_0 \equiv b \bmod n$

$ax_1 - ax_0 \equiv b - b \bmod n$

$a(x_1 - x_0) \equiv 0 \bmod n \Rightarrow n | a(x_1 - x_0)$

$\delta = \mu\kappa\delta(a,n) \Rightarrow a = \delta a'$

$n = \delta n'$

$\delta = \mu\kappa\delta(a,n) = \mu\kappa\delta(\delta a', \delta n') = \delta\mu\kappa\delta(a', n') \Rightarrow \mu\kappa\delta(a', n') = 1$

$n | a(x_1 - x_0) \Rightarrow \delta n' | \delta a'(x_1 - x_0) \Rightarrow n' | a'(x_1 - x_0)$

$\mu\kappa\delta(a', n') = 1$

$\Rightarrow n' = \frac{n}{\delta} \Big/ x_1 - x_0$

$\frac{n}{\delta} \Big/ x_1 - x_0 \Rightarrow x_1 \equiv x_0 \bmod \frac{n}{\delta}$

---

$\frac{n}{\delta} \Big/ x_1 - x_0 \Rightarrow x_1 - x_0 = \kappa\frac{n}{\delta}$

$x_1 - x_0 = (q\delta + r)\frac{n}{\delta}$

$\kappa = q\delta + r, \quad 0 \le r < \delta$

$x_1 - x_0 \equiv q\delta\frac{n}{\delta} + r\frac{n}{\delta} \bmod n$

$x_1 \equiv x_0 + r\frac{n}{\delta} \bmod n, \quad 0 \le r \le \delta - 1$