25/11/2016

Συνάρτηση Euler $\phi: \mathbb{N}^* \to \mathbb{N}$

$\phi(n)$ = πλήθος πρώτων προς τον n

$\phi(1)=1$, $\phi(2)=1$

$\phi(p)=p-1$, p πρώτος

$\phi(m \cdot n)=\phi(m)\cdot\phi(n)$, όταν $(m,n)=1$

$$\phi(p_1^{k_1}\cdots p_\ell^{k_\ell})=p_1^{k_1-1}\cdots p_\ell^{k_\ell-1}(p_1-1)\cdots(p_\ell-1)$$

Gauss $\quad n=\sum_{d|n}\phi(d)$

$(a,m)=1 \Rightarrow \{[a_1]_m, \dots, [a_{\phi(m)}]_m\} = \{[aa_1]_m, \dots, [a a_{\phi(m)}]_m\}$

<u>Wilson</u> : $(p-1)! \equiv -1 \bmod p \Leftrightarrow$ p πρώτος

Διαφορετικά $(m-1)! \equiv 0 \bmod m$, m σύνθετος

<u>Παράδειγμα</u>

$\phi(n)=4$, βρείτε το n

$4=p_1^{k}\cdots p_\ell^{k_\ell-1}(p_1-1)(p_\ell-1)$

$4=4=1\cdot 4=\cancel{2\cdot 2}=1\cdot 2\cdot 2=1\cdot \cancel{2\cdot 2}$

$p_1-1=4 \Rightarrow p_1=5=n$

$p_1 - 1 = 1 \Rightarrow p_1 = 2$ $\quad n = 10$

$p_2 - 1 = 4 \Rightarrow p_2 = 5$

$p_1 - 1 = 1 \Rightarrow p_1 = 2$ $\quad n = 8$

$k_1 = 3$

$p_1 - 1 = 1 \quad p_1 = 2 \quad k = 2$

$p_2 - 1 = 2 \quad p_2 = 3 \quad n = 2^3 \cdot 3 = 12$

$n = 5, 10, 8, 12 \qquad \phi(12) = 4 \qquad \phi(11) = 10$

Παράδειγμα

$$\frac{21!}{11!} \equiv -1 \bmod 11$$

$$\frac{21!}{11!} = 12 \cdot 13 \cdot \ldots \cdot 21$$

$1 \cdot 2 \cdot \ldots \cdot 10 = (11-1)! \equiv -1 \bmod 11$

$12 \equiv 13 \ldots 21 \bmod 11 \quad \{[0]_{11}, [1]_{11}, \ldots, [10]_{11}\}$

$12 = (11+1)$

$13 = (11+2) \qquad \{[a+0]_{11}, [a+1]_{11}, \ldots, [a+10]_{11}\}$

⇒ Θυμάμαι $\quad (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \ldots + \binom{n}{n-1} a b^{n-1} + b^n$

$n = p$ πρώτος $\quad \binom{p}{k} = \frac{p!}{k!(p-k)!}$ φυσικός

$$\frac{4!}{2!(4-2)!} = \frac{1 \cdot 2 \cdot 3 \cdot 4}{\cancel{1 \cdot 2 \cdot 1 \cdot 2}}$$

→ $p \mid m$ Δηλαδή το $\binom{p}{k}$ με $1 \le k \le p-1$

Είναι πολλ/σιο του p

$\binom{p}{k} \bmod p \equiv 0$

$\boxed{(a+b)^p \bmod p \equiv a^p + b^p}$ (+) όχι για n σύνθετο

ΘΕΩΡΗΜΑ

Έστω p πρώτος. Τότε $a^p \equiv a \bmod p$.
Αν $p \nmid a$, τότε $a^{p-1} \equiv 1 \bmod p$ $a \in \mathbb{Z}$

Απόδειξη

Με επαγωγή στο a για $a \geq 1$

$a=1 \Rightarrow 1^p = 1 \bmod p$
$a=2 \Rightarrow 2^p = (1+1)^p \overset{(+)}{\equiv} (1^p+1^p) \bmod p = 2 \bmod p$

Υποθέτουμε ότι ισχύει μέχρι k.
Θα αποδείξουμε για $k+1$.

$(k+1)^p \equiv (k+1) \bmod p$. Θέλουμε

$(k+1)^p \overset{(+)}{\equiv} (k^p + 1^p) \bmod p \overset{\text{επαγωγή}}{\equiv} (k+1) \bmod p$

Αν $p \nmid a \Leftrightarrow (p, a) = 1 \Leftrightarrow [a]_p$ αντιστρέφεται

Δηλαδή $\exists\, b$ με $a \cdot b \equiv 1 \bmod p$
$a^p \equiv a \bmod p \Rightarrow a^p \cdot b = ab \bmod p \Rightarrow$
$a^{p-1}(ab) \equiv 1 \bmod p \Rightarrow a^{p-1} \equiv 1 \bmod p$

ΘΕΩΡΗΜΑ Euler

Έστω $a, m \in \mathbb{N}^*$ με $(a,m)=1$
Τότε $a^{\phi(m)} \equiv 1 \bmod m$

Απόδειξη

$\phi(m)$ = το πλήθος των αντιστρέψιμων κλάσεων modm

$\{[a_1]_m, [a_2]_m, \dots, [a_{\phi(m)}]_m\}$

Αντιστρέψιμη : $\exists\ [a_1']_m$ με $[a_1]_m[a_1']_m = [1]_m$

$(a,m)=1 \Rightarrow [a]_m$ αντιστρέψιμη $\Rightarrow$
$[a] \in A$. Δηλαδή $\exists\ i$ με $[a]_m = [a_i]_m$

$A = \{[aa_1]_m, [a, a_2]_m, \dots, [a, a_{\phi(m)}]_m\}$

$(aa_1)(aa_2)\dots(aa_{\phi(m)}) \bmod m \equiv$
$a_1a_2\dots a_{\phi(m)} \bmod m$
$a^{\phi(m)} \cdot a_1 \cdot a_2 \dots \cdot a_{\phi(m)} \equiv a_1 a_2 \dots a_{\phi(m)} \bmod m$

Όλα τα a_i είναι αντιστρέψιμα.
Άρα, $\exists\ b_i$ με $a_ib_i \equiv 1 \bmod m$

$a^{\phi(m)} \cdot a_1a_2 \dots a_{\phi(m)} b_1b_2 \dots b_{\phi(m)} \equiv$
$a_1a_2\dots a_{\phi(m)} b_1b_2 \dots b_{\phi(m)} \bmod m$

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

Παράδειγμα

1) Να βρεθεί το $2^{50} \bmod 13$

Με το θεώρημα Euler έχουμε $2^{\phi(13)} = 1 \bmod 13$

$2^{12} \equiv 1 \bmod 13 \Rightarrow \underbrace{(2^{12})^2}_{2^{24}} \equiv 1^2 \bmod 13 \equiv 1 \bmod 13$

$50 = 4 \cdot 12 + 2$ $\qquad 2^{50} = 2^{4 \cdot 12 + 2} = 2^{4 \cdot 12} \cdot 2^2$

$= ((2^{12})^4 \cdot 2^2 \bmod 13)\ (2^2 \bmod 13)$

$= (1^4 \bmod 13)(4 \bmod 13)$

$2^{50} \bmod 13 \equiv 4$

2) Να βρεθεί το $(2^{50} + 3^{50}) \bmod 13$

$(2^{50} + 3^{50}) \bmod 13 = 2^{50} \bmod 13 + 3^{50} \bmod 13$

$= (4 + 9) \bmod 13 \equiv 0$

$3^{12} \equiv 1 \bmod 13$

$50 = 4 \cdot 12 + 2 \Rightarrow \ldots \Rightarrow 3^{50} \equiv ((3^{12})^4 \cdot 3^2) \bmod 13 =$

$\equiv (3^{12})^4 \bmod 13\ (9 \bmod 13) \equiv 9 \bmod 13$

3) $3^{372} \equiv a \bmod 37$. Να βρεθεί το a.

Euler $\Rightarrow$ $3^{\phi(37)} \equiv 1 \bmod 37$

$\phi(37) = 36$

$372 = 10 \cdot 36 + 12$

$3^{372} = (3^{36})^{10} \cdot 3^{12} \bmod 37 = 1 \cdot 3^{12} \bmod 37$

$3^3 = 27 \equiv 27 \bmod 37 \equiv (-10) \bmod 37$
$3^4 \equiv 3(-10) \bmod 37 \equiv (-30) \bmod 37 \equiv 7 \bmod 37$

$3^4 \equiv 7 \bmod 37$

$(3^4)^3 = 7^3 \bmod 37 \equiv 7^2 \cdot 7 \bmod 37 = 12 \cdot 7 \bmod 37$
$\equiv 84 \bmod 37 \equiv 10 \bmod 37$

4) Να δείξετε ότι $7 \nmid n^2+1$ για $n \geq 1$

Υποθέτουμε ότι $7 \mid n^2+1 \Leftrightarrow n^2+1 \equiv 0 \bmod 7$
$n^2 \equiv -1 \bmod 7$

Υποθέτουμε ότι 7 πρώτος $\mid n \Rightarrow 7 \mid n^2$
$7 \mid n^2+1-n^2 = 1$ Αδύνατο

$7 \nmid n \quad n^{\phi(7)} \equiv 1 \bmod 7$
$n^6 \equiv 1 \bmod 7$

$n^2 \equiv -1 \bmod 7 \Rightarrow (n^2)^2 \equiv 1^2 \bmod 7$
$n^6 = n^4 \cdot n^2 \equiv 1^2(-1) \bmod 7$
$\equiv$
$1 \bmod 7 \quad \neq$

άρα, δεν γίνεται $7 \mid n^2+1$

5) Να βρεθούν τα δύο τελευταία ψηφία του 7^{200}

$$\underbrace{a_n 10^n + a_{n-1}10^{n-1} + \dots + \underline{a_1}10 + \underline{a_0}}_{} = \overbrace{a_n a_{n-1} \dots a_0}^{\text{αριθμός}}$$

$a_n \neq 0 \quad , a_{n-1}, \dots, a_0 = 0, \dots, 9$

$$(a_n 10^n + a_{n-1}10^{n-1} + \dots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0) \bmod 100 \equiv \underline{a_1 10 + a_0}$$

$a_1 10 + a_0 < 100 \Rightarrow (a_1 10 + a_0) \bmod 100 \equiv a_1 10 + a_0$

$(a_n 10^n + \dots + a_2 10^2) = (a_n 10^{n-2} + \dots + a_3 10 + a_2)\, 100 \bmod 100 = 0$

$7^{200} \bmod 100$

$(7, 100) = 1 \quad \text{Euler} \Rightarrow 7^{\phi(100)} \equiv 1 \bmod 100$

$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2) \cdot \phi(5^2) = 2\phi(2) \cdot 5\phi(5) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$

$7^{40} \bmod 100 = 1 \Rightarrow (7^{40})^5 \equiv 1^5 \bmod 100 \equiv 1$

Άρα, $a_1 = 0$ και $a_0 = 1$

Άρα, τα δυο τελευταία ψηφία είναι **01**