

Παράδειγμα (Θ. Euler).

$$\mathbb{Z}_5^* = \{ [1]_5, [2]_5, [3]_5, [4]_5 \}$$

$$[2]_5 \odot [2]_5 = [2]_5^2 = [4]_5 = [1]_5$$

$$[2]_5^3 = [4]_5 \odot [2]_5 = [8]_5 = [3]_5.$$

$$[2]_5^4 = [2]_5^{\varphi(5)} \stackrel{\text{Euler}}{=}_{(2,5)=1} [1]_5$$

$$\mathbb{Z}_5^* = \{ [2]_5, [2]_5^2, [2]_5^3, [2]_5^4 \}$$

Γενικά για κάθε πρώτο p υπάρχει μια υλίσου $[a]_p$ ώστε:

$$\mathbb{Z}_p^* = \{ [1]_p, [2]_p, \dots, [p-1]_p \} = \{ [a]_p, [a]_p^2, \dots, [a]_p^{p-1} \}$$

Αυτό το a , ονομάζεται πρωταρχική ρίζα modulo p

Η ρίζα χρησιμοποιείται για τη λύση μιας πολυωνυμικής εξίσωσης.

$$x^{p-1} - 1 = 0 \quad \text{Λύσεις μέσα από το } \{1, 2, \dots, p-1\}$$

$$x^4 - 1 = 0 \rightarrow 2 \text{ πραγματικές}$$

$$\rightarrow 2 \text{ φανταστικές}$$

$$x^k - 1 = 0 \rightarrow k \text{ μιγαδικές}$$

ΙΔΙΟΤΗΤΕΣ ΣΥΝΑΡΤΗΣΗΣ EULER:

- 1) Πολλαπλασιαστική αν $(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- 2) p πρώτος $\Rightarrow \varphi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$
- 3) Αν $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_l^{k_l} \Rightarrow$
$$\Rightarrow \varphi(n) = \prod_{i=1}^l \varphi(p_i^{k_i}) = p_1^{k_1-1} \cdot p_2^{k_2-1} \cdot \dots \cdot p_l^{k_l-1} (p_1-1)(p_2-1) \cdot \dots (p_l-1)$$
$$= n \prod_{i=1}^l (1 - \frac{1}{p_i})$$

$$[\varphi(4) = \varphi(2^2) = 2^2(1 - \frac{1}{2}) = 2 \rightarrow 4 \neq \varphi(4)]$$

4) Τύπος Gauss:

$$1(n) = n = \sum_{d|n} \varphi(d)$$

5) Τύπος Wilson:

$$(p-1)! \equiv -1 \pmod{p} \equiv (p-1) \pmod{p}$$

Πρόταση: Εάν $m \geq 4$ και σωθής, τότε $(m-1)! \equiv 0 \pmod{m}$

6) Τύπος Euler:

$$\text{Εάν } (a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$a^p \equiv a \pmod{p}, \quad p: \text{πρώτος}$$

$$a^p + b^p = (a+b)^p \pmod{p}$$

ΑΣΚΗΣΕΙΣ / ΕΦΑΡΜΟΓΕΣ

1) Να βρεθεί το n με $\varphi(n) = 6$

Λύση

1^{ου}: Εάν n πρώτος $\varphi(n) = n-1 = 6 \Rightarrow n = 7$

2^{ου}: Εάν n σωθής (δηλ $n = p \cdot q$, p, q πρώτοι) τότε

$$\varphi(n) = \varphi(p) \cdot \varphi(q) = 6$$

- $\varphi(p) = 1$ και $\varphi(q) = 6 \Rightarrow p = 2$ και $q = 7$
 - $\varphi(p) = 2$ και $\varphi(q) = 3 \Rightarrow p = 3$ και $q = 4$ (Αλλά $\varphi(4) = 2$)
- Αδύνατο

3^{ov}: Ο n συνθετός ώστε $n = pqr$, p, q, r πρώτοι διακεκομμένοι
Αλλά, $6 = \varphi(p)\varphi(q)\varphi(r)$ Αδύνατον.

4^{ov}: Ο $n = p^2 \Rightarrow \varphi(n) = p(p-1) \Rightarrow 6 = 3 \cdot 2 = p(p-1) \Rightarrow p = 3 \leadsto n = 9$

5^{ov}: Ο $n = p^2 \cdot q \Rightarrow \varphi(n) = \varphi(p^2)\varphi(q) = p(p-1)(q-1) = 6 \Rightarrow$
 $\Rightarrow p = 3$ και $q = 2 \leadsto n = 18$.

6^{ov}: Ο $n = p^2 \cdot q^2 \Rightarrow \varphi(n) = \varphi(p^2) \cdot \varphi(q^2) = p(p-1)q(q-1)$ Αδύνατον

7^{ov}: Ο $n = p^3$, p πρώτος $\Rightarrow \varphi(n) = \varphi(p^3) = p^2(p-1) = 6$ Αδύνατον

Πλ (Για το σπίτι)

Να υπολογιστεί το $5^{38} \bmod 17 \equiv$

2) Εάν p πρώτος, τότε:

α. $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv (p-1) \bmod p$

β. $1^p + 2^p + \dots + (p-1)^p \equiv 0 \bmod p$

ΛΥΣΗ

α. Από Euler:

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv \overbrace{(1 + 1 + \dots + 1)}^{p-1} \bmod p \equiv (p-1) \bmod p$$

β. $1^p + 2^p + \dots + (p-1)^p \equiv (1 + 2 + \dots + p-1) \bmod p \equiv$
 $\equiv \left(\frac{1+p-1}{2} \right)^{p-1} \bmod p \equiv p^{\frac{p-1}{2}} \bmod p \equiv 0 \bmod p$

3) Εάν p πρώτος τότε: $\sqrt{p}$:

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

ΛΥΣΗ

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \dots \cdot (p-2)(p-1) \equiv (p-1)! \equiv (-1) \bmod p \Rightarrow [(p-1)!]^2 \equiv 1 \bmod p$$

$$\begin{array}{l} -2 \equiv p-2 \\ -4 \equiv p-4 \\ \vdots \\ -(p-1) \equiv 1 \end{array} \left\{ \begin{array}{l} \text{mod } p \end{array} \right. \quad (-1)^{p-1/2} \cdot 2 \cdot 4 \cdot 6 \dots (p-1) \equiv \\ \equiv ((p-2) \cdot (p-4) \dots 3 \cdot 1) \text{ mod } p$$

Αρα, $(-1)^{\frac{p-1}{2}} \cdot 2 \cdot 4 \cdot 6 \dots (p-1) \cdot (p-2) \cdot (p-4) \dots 3 \cdot 1 \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \text{ mod } p$

Αρα, $1^2 \cdot 3^2 \dots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \text{ mod } p$

4) Να δείξετε ότι:

$$1! + 2! + 3! + \dots + 100! \equiv 9 \text{ mod } 12$$

Λύση

$$12 = 4 \cdot 3$$

$$4! = 1 \cdot 2 \cdot \underbrace{3 \cdot 4}$$

Αν $k \geq 4 \Rightarrow k! \equiv 0 \text{ mod } 12$

$$1! + 2! + 3! + \dots + 100! \equiv (1 + 2 + 6 + 0 + \dots + 0) \text{ mod } 12 \equiv 9 \text{ mod } 12$$

5) Εάν $d | n \stackrel{\text{NBO}}{\Rightarrow} \varphi(d) | \varphi(n)$

Λύση

Εστω $n = p_1^{k_1} \dots p_l^{k_l} \Rightarrow d = p_1^{\varepsilon_1} \dots p_l^{\varepsilon_l}, 0 \leq \varepsilon_i \leq k_i$

$$\varphi(n) = n \prod_{i=1}^l \left(1 - \frac{1}{p_i}\right) \text{ και } \varphi(d) = d \prod_{i=1}^l \left(1 - \frac{1}{p_i}\right)^{\alpha_i}$$

Οπου α_i είναι:

α. 0 όταν ο p_i δεν υπάρχει στο d

β. 1 όταν ο p_i υπάρχει στο d

$$\prod_{i=1}^l \left(1 - \frac{1}{p_i}\right)^{\alpha_i} \mid \prod_{i=1}^l \left(1 - \frac{1}{p_i}\right) \Rightarrow \varphi(d) \mid \varphi(n)$$