

$$x^k \equiv b \pmod{n} \quad \text{!} \quad \text{פונקציה} \quad \text{פולינום}$$

$$p(x) \equiv 0 \pmod{n}$$

החומר הזה, כיצד $\mathbb{Z}_n$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

$$|\mathbb{Z}_n^*| = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}| = \phi(n)$$

למשל $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2$$

אם p ראשוני, $\phi(p) = p-1$

אם $n = p^k$, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

$$\phi(p^k) = |\{1 \leq a \leq p^k : \gcd(a, p^k) = 1\}| = p^k - p^{k-1} = p^{k-1}(p-1)$$

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \dots \phi(p_r^{k_r})$$

$$\phi(n) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \dots \phi(p_r^{k_r}) = p_1^{k_1-1} (p_1-1) \dots p_r^{k_r-1} (p_r-1)$$

$$= n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

הפונקציה ϕ היא פונקציה מרובת ערכים

$$\phi(p \cdot m) = \phi(p) \phi(m) \quad \text{אם } p \nmid m$$

5K, 0K a 0K

$$gcd(a, p \cdot m) > 1 \Leftrightarrow gcd(a, m) > 1$$

$$\phi(p \cdot m) = |\{1 \leq a \leq p \cdot m : gcd(a, p \cdot m) = 1\}| =$$

$$= p \cdot \phi(m)$$

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$ ו- a מתחלק ב- m ...

$$gcd(a, m) = 1 \Leftrightarrow gcd(a, p \cdot m) = 1$$

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$

$$gcd(a, p \cdot m) = 1 \Leftrightarrow gcd(a, m) = 1 \wedge p \nmid a$$

$$\phi(p \cdot m) = |\{1 \leq a \leq p \cdot m : gcd(a, p \cdot m) = 1\}| =$$

$$= |\{1 \leq a \leq p \cdot m : gcd(a, m) = 1 \wedge p \nmid a\}| =$$

$$= |\{1 \leq a \leq p \cdot m : gcd(a, m) = 1\}| - |\{1 \leq a \leq p \cdot m : gcd(a, m) = 1 \wedge p \mid a\}| =$$

$$= I - II$$

$$I = p \cdot \phi(m)$$

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$

$$gcd(a, m) = 1 \Leftrightarrow gcd(a, p \cdot m) = 1 - a$$

$$gcd(a, m) = 1 \Leftrightarrow gcd(a, p \cdot m) = 1$$

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$ ו- a מתחלק ב- m

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$ ו- a מתחלק ב- m

$$\phi(p \cdot m) = p \cdot \phi(m) - \phi(m) = (p-1) \cdot \phi(m)$$

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$

אם a מתחלק ב- p אז a מתחלק ב- $p \cdot m$ ו- a מתחלק ב- m

$$\phi(p_1 \cdot p_2 \cdot \dots \cdot p_k) = \phi(p_1) \cdot \phi(p_2) \cdot \dots \cdot \phi(p_k)$$

$$= p_1 \cdot (p_1 - 1) \cdot p_2 \cdot (p_2 - 1) \cdot \dots \cdot p_k \cdot (p_k - 1)$$

$$= \dots = p_1^{k_1-1} \phi(p_1, \frac{n}{p_1^{k_1}})$$

$$= p_1^{k_1-1} (p_1-1) \cdot \phi(\frac{n}{p_1^{k_1}}) =$$

$$= \cancel{p_1^{k_1-1}} p_1^{k_1-1} (p_1-1) \cdot \dots \cdot p_{k_2}^{k_{k_2}-1} (p_{k_2}-1) =$$

$$= n \prod_{i=1}^k (1 - \frac{1}{p_i})$$

הנושא בסיסית

$$F(n) = \sum_{\substack{d|n \\ d \geq 1}} \phi(d) = \phi * 1$$

אם נסתכל על $F(n)$ כפונקציה של n אזי $F(n)$ היא פונקציה מרובעת. כלומר $F(n)$ היא פונקציה מרובעת.

הפונקציה $F(n)$ היא פונקציה מרובעת. כלומר $F(n)$ היא פונקציה מרובעת. $F(n)$ היא פונקציה מרובעת.

$$F(p^k) = \sum_{\substack{d|p^k \\ d \geq 1}} \phi(d) = \phi(p) + \phi(p^2) + \dots + \phi(p^k)$$

$$= 1 + (p-1)p + \dots + p^{k-1}(p-1) = 1 + (p-1)[p + p^2 + \dots + p^{k-1}]$$

$$= 1 + (p-1) \left[\frac{p^k - p}{p-1} \right] = p^k$$

כלומר $F(n) = n$

$a^{p-1} \equiv 1 \pmod{p}$ כאשר p ראשוני ו- a אינו מתחלק ב- p .
 $a^{\phi(n)} \equiv 1 \pmod{n}$ כאשר a אינו מתחלק ב- n .

כלומר $a^{\phi(n)} \equiv 1 \pmod{n}$ כאשר a אינו מתחלק ב- n .

הפונקציה $\phi(n)$ היא פונקציה מרובעת. כלומר $\phi(n)$ היא פונקציה מרובעת.

$$g_1, g_2, \dots, g_{\phi(n)}$$

$$g_i \equiv a g_j \pmod{n} \quad \text{כאשר } i \neq j$$

$$g_i \equiv g_j \pmod{n}$$

$$Z_n^*$$

$$a g_1, a g_2, \dots, a g_{\phi(n)}$$

הפונקציה $\phi(n)$ היא פונקציה מרובעת.

כלומר $a g_i \equiv a g_j \pmod{n}$ כאשר $i \neq j$.

12/ נ יבנת (א' ג' י' מ' 2 קה, ג' 3 ז' 1 סק, 1/1 מ' 1/1/1 -

$$g_1 g_2 \dots g_n \equiv a g_1 a g_2 - g g g_n \pmod{n}$$

$$a^n \underbrace{g_1 g_2 \dots g_n}_{\text{mod } n}$$

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