Számelmélet

A számítástudomány alapjai
10. gyakorlat

2014. november 28.

Tétel. Az $ax \equiv b \pmod{m}$ kongruenciának akkor és csak akkor létezik megoldása, ha $(a, m)|b$.

Tétel. Ha az $ax \equiv b \pmod{m}$ kongruencia megoldható, akkor a megoldásszáma (a, m).

Def. Rögzített $m > 1$ egész esetén a $T \subseteq \mathbb{Z}$ halmaz teljes maradékrendszer modulo m, ha T minden m szerinti maradékosztályból pontosan egy elemet tartalmaz.

Def. Rögzített $m > 1$ egész esetén az $R \subseteq \mathbb{Z}$ halmaz redukált maradékrendszer modulo m, ha R minden m-hez relatív prím m szerinti maradékosztályból pontosan egy elemet tartalmaz.

Def. Tetszőleges $n \in \mathbb{Z}^+$ esetén $\varphi(n)$ jelöli az $\{1, \ldots, n\}$ számok közül az n-hez relatív prímek számát.

Tétel. Ha az $n \in \mathbb{Z}^+$ szám kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, akkor

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Tétel. Euler–Fermat-tétel $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$.

Tétel. A kis Fermat-tétel Ha p prím és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Tétel. A kis Fermat-tétel másik alakja Ha p prím, akkor bármely a egész számra $a^p \equiv a \pmod{p}$.

1. Oldjuk meg az alábbi lineáris diofantikus egyenleteket:
   (a) $43x + 25y = 98$
   (b) $7x + 11y = 118$
   (c) $64x + 26y = 4$
2. Határozzuk meg a $\varphi(60)$ és a $\varphi(11)$ értékeket.
3. Oldjuk meg az alábbi kongruenciákat!
   (a) $x \equiv 108^{182} \pmod{19}$
   (b) $x \equiv 5^{1997} \pmod{17}$
4. Bizonyítsuk be, hogy tetszőleges n természetes számra $\varphi(n^2) = n\varphi(n)$ teljesül.
5. Mutassuk meg, hogy $35 | \ 4^{24} - 3^{24}$.
6. Bizonyítsuk be, hogy $11 \mid n^{11} + 10n$ és $42 \mid n^7 - n$ teljesül tetszőleges $n \in \mathbb{N}$ esetén.
7. Határozzuk meg 253^{683} utolsó két számjegyét.
8. Bizonyítsuk be, hogy tetszőleges p prímre $(a + b)^p \equiv a^p + b^p \pmod{p}$.
9. Mely n természetes számokra igaz, hogy $\varphi(5n) + \varphi(3n) = 7\varphi(n)$?
10. Mely n számokra lesz $\varphi(n)$ prímszám? Mikor lesz $\varphi(n)$ páratlan?