Számelmélet

Bevezetés a számításelméletbe 1
12. gyakorlat
2015. december 1.

Tétel

Az $ax + by = c$ egyenletnek akkor és csak akkor létezik egész megoldása, ha $(a, b) \mid c$.

Tétel

Az $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ kongruenciarendszer akkor és csak akkor oldható meg, ha $(m_1, m_2) \mid a_1 - a_2$. A megoldás egy *modulo* $[m_1, m_2]$ maradékrendszer.

Kínai maradéktétel

Legyenek $m_1, \ldots, m_k$ páronként relatív prímek. Ekkor az

$$x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_k \pmod{m_k}$$

kongruenciarendszer megoldható, és a megoldás egy *modulo* $m_1 \cdot \ldots \cdot m_k$ maradékrendszer.

Az Euler-féle φ-függvény

Ha $n \geq 2$ egész szám, akkor az 1 és n közé eső, n-hez relatív prímek számát $\varphi(n)$ jelöli.

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

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right).$$

Euler–Fermat-tétel

Legyenek a és $m \geq 2$ egész számok. Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A kis Fermat-tétel

Legyen p egy prím és a egész szám. Ha $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

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) $7x + 11y = 118$

2. Egy százlábú meg akarja számolni a lábait. Azt tudja biológiából, hogy minden százlábúnak legfeljebb 344 lába van. Ha 13-asával számolja a lábait, akkor 3 marad ki, ha 17-esével számolja, akkor viszont 10 marad ki. Hánylábú a százlábú?

3. Egy n egész szám 3 maradékot ad 82-vel osztva. Milyen maradékot adhat az n szám 182-vel osztva?

4. Egy n egész szám 3 maradékot ad 72-vel osztva. Milyen maradékot adhat 102-vel osztva a $2n + 7$ szám?

5. Határozzuk meg a $\varphi(60)$ és a $\varphi(11)$ értékeket.

6. Oldjuk meg az alábbi kongruenciákat!

   (a) $x \equiv 108^{182} \pmod{19}$

   (b) $x \equiv 5^{1997} \pmod{17}$

7. Mutassuk meg, hogy $35 \mid 4^{24} - 3^{24}$.

8. Tekintsük azt a számtani sorozatot, amelynek első tagja 32, differenciája 51. Milyen maradékot ad a sorozat első 32 tagjának szorzata 51-gyel osztva?

9. Milyen maradékot ad $46^{47^{48}}$ 25-tel osztva?

10. Bizonyítsuk be, hogy tetszőleges p prímre $(a + b)^p \equiv a^p + b^p \pmod{p}$.

11. Az n szám kettes számrendszerbeli alakja 110100101101100011011. Határozzuk meg az n^n szám kettes számrendszerbeli alakjának utolsó négy jegyét.