Szimultán kongruenciarendszerek, Euler–Fermat-tétel

Bevezetés a számításelméletbe 1
2. gyakorlat

Tétel

Az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, m) \mid b$. A kongruencia megoldáshalmaza (a, m) darab maradékosztály modulo m.

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.

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

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

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. (a) 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?

   (b) Egy másik százlábú is megirigyli ezt a módszert. Neki 16-osával számolva 5 marad ki, 20-asával számolva pedig 15 marad ki. Bizonyítsuk be, hogy elszámolta magát.

   (c) A százlábúak királyához is eljut a módszer. Neki 6-osával számolva 5 marad ki, 7-esével számolva 6, 8-asával számolva pedig 7. Neki hány lába van?

2. Határozzuk meg a $\varphi(60)$, $\varphi(100)$ és a $\varphi(11)$ értékeket.

3. Milyen maradékot ad

(a) 108^{182} 19-cel osztva;

(b) 5^{2017} 17-tel osztva;

(c) 59^{99} 101-gyel osztva;

(d) $46^{47^{48}}$ 25-tel osztva;

(e) $42^{41^{40}}$ 121-gyel osztva;

(f) $100^{3^{2011}}$ 3^{2011}-nel osztva?

4. Mutassuk meg, hogy

(a) $4^{24} - 3^{24}$ osztható 35-tel;

(b) $2002^{2002} + 1$ osztható 17-tel;

(c) $3^{931} + 5^{930} - 52$ osztható 2006-tal. (Segítségül: $2006 = 2 \cdot 17 \cdot 59$.)

5. Legyen a egy 2001-hez relatív prím egész szám. Bizonyítsuk be, hogy ekkor $(a^{28} - 1)(a^{24} - a^{22} - a^2 + 1)$ osztható 2001-gyel. (Segítségül: $2001 = 3 \cdot 23 \cdot 29$.)

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

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

8. Az n szám kettes számrendszerbeli alakja 11010010111011000011011. Határozzuk meg az n^n szám kettes számrendszerbeli alakjának utolsó négy jegyét.

9. Határozzuk meg az összes olyan n egész számot, melyre

(a) $n^7 - n$ osztható 9-cel;

(b) $n^{42} - n$ osztható 41-gyel.

10. Mutassuk meg, hogy végtelen sok olyan n pozitív egész szám létezik, amelyre $2011^n - 1$ osztható n-nel!

11. Bizonyítsuk be, hogy ha a egy 11-gyel nem osztható egész szám, akkor az $x^3 \equiv a \pmod{121}$ kongruencia megoldható.