Szimultán kongruenciarendszerek, Euler–Fermat-tétel

Bevezetés a számításelméletbe 1

2019

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

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

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. Egy egész szám 109-cel vett osztási maradéka 5-tel kisebb, mint a szám 18-szorosának a 109-cel vett osztási maradéka. Milyen maradékot adhat ez a szám 109-cel osztva?

2. Hány olyan x egész szám létezik 1 és 2017 között, amelyre teljesül, hogy $92x - 1$ x-szel azonos maradékot ad 399-cel osztva?

3. Adjuk meg az összes olyan négyjegyű pozitív egész számot, amelyre teljesül, hogy 51-gyel osztva 3 maradékot ad, továbbá a szám 17-szeresének utolsó két számjegye 15.

4. (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.

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

6. Milyen maradékot ad

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

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

   (c) $73^{37} + 37^{73}$ 108-cal osztva;

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

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

   (f) $169^{181^{194}}$ 392-vel osztva;

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

7. Mutassuk meg, hogy

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

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

8. 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: $2001 = 3 \cdot 23 \cdot 29$.)

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

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

11. Legyen p egy 3-tól különböző, pozitív prímszám, a pedig egy olyan egész szám, amely sem 3-mal, sem p-vel nem osztható. Mutassuk meg, hogy ekkor

$$a^{6p-6} \equiv 1 \pmod{9p}.$$

12. Határozzuk meg az összes olyan háromjegyű, pozitív egész számot, amelynek a 7-es és 8-as számrendszerbeli alakjának az utolsó két számjegye is 11.

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

14. Bizonyítsuk be, hogy ha a egy 11-gyel nem osztható egész szám, akkor az

$$x^3 \equiv a \pmod{121}$$

   kongruencia megoldható.

15. Határozzuk meg a 630-nál kisebb, 630-hoz relatív prím pozitív egész számok összegét.