Szimultán kongruenciarendszerek, Euler–Fermat-tétel

Bevezetés a számításelméletbe 1
2020
2. gyakorlat

Tétel. Az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, m) \mid b$; és ha megoldható, akkor (a, m) darab megoldás van modulo m.

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 $n > 1$ egész 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. 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.

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

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.

   (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?

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: $2006 = 2 \cdot 17 \cdot 59$);

   (c) $1010^{1343} - 2$ osztható 2019-cel (segítségül: $2019 = 3 \cdot 673$).

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. Legyen $n = 200704261601$. Határozzuk meg n^n utolsó három számjegyét.

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

14. Jumurdzsák először örült a tiszti kinevezésnek, de hamarosan elment a kedve az egésztől. Mindjárt az első összecsapásban jópáran elestek a rábízott 50 fős csapatból, amit még elviselt volna, csakhogy köztük volt a pénztáros is, így már a második héten Jumurdzsáknak kellett kiosztania a zsoldot, ami cseppet sem volt egyszerű feladat. Minden alárendeltjének 26 akcse járt hetente (neki magának pedig 2 arany), de a főnökség persze nem bajlódott akcsékkal, aranyban adta át Jumurdzsáknak a csapat heti zsoldját (1 arany = 60 akcse). Fel kellett tehát váltania az aranyakat a zsold kiosztása előtt, ráadásul még a visszamaradó nyamvadt 2 akcsét sem tarthatta meg. – Így jár, aki elveszti a talizmánját – sóhajtott keserűen. Hányan estek el (a második hétig) Jumurdzsák alárendeltjei közül?

15. Létezik-e olyan n egész szám, amelyre $n^4 + 1$ osztható 101-gyel?