Euler–Fermat-tétel

Bevezetés a számításelméletbe 1

3. gyakorlat

2022.

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 $m \geq 2$ és a 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. Határozzuk meg a $\varphi(60)$, $\varphi(100)$ és a $\varphi(11)$ értékeket.
2. Milyen maradékot ad
   - (a) 5^{2017} 17-tel osztva;
   - (b) 108^{182} 19-cel osztva;
   - (c) $3^{147} + 70^{147}$ 73-mal osztva;
   - (d) 2020^{2021} 1011-gyel osztva;
   - (e) 7^{3234} 80-nal osztva;
   - (f) $73^{37} + 37^{73}$ 108-cal osztva;
   - (g) $46^{47^{48}}$ 25-tel osztva;
   - (h) $42^{41^{40}}$ 121-gyel osztva;
   - (i) $100^{3^{2011}}$ 3^{2011}-nel osztva?
3. Mutassuk meg, hogy
   - (a) $4^{24} - 3^{24}$ osztható 35-tel;
   - (b) $1010^{1343} - 2$ osztható 2019-cel (segítségül: $2019 = 3 \cdot 673$);
   - (c) $38^{59} + 2$ osztható 77-tel;
   - (d) $3^{931} + 5^{930} - 52$ osztható 2006-tal (segítségül: $2006 = 2 \cdot 17 \cdot 59$).

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

5. Tekintsük azt a mértani sorozatot, amelynek első tagja 41, kvóciense 7. Mi az utolsó három számjegye a sorozat első 800 tagjának a szorzatának?

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

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

8. Hány olyan 504-nél nemnagyobb, pozitív egész szám van, amelynek van 504-gyel osztva 1 maradékot adó többszöröse?

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

10. 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
$$a^{6p-6} \equiv 1 \pmod{9p}.$$

11. 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: $2001 = 3 \cdot 23 \cdot 29$.)

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

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

14. Határozzuk meg az összes olyan 1 és 100 közötti a egész számot, melyre $a^{21} \equiv 1 \pmod{100}$.

15. Igaz-e, hogy ha az a és b egész számokra $a^{40} \not\equiv b^{40} \pmod{100}$, akkor $a^{40}b^{40} \not\equiv 1 \pmod{100}$?