Euler–Fermat-tétel

Bevezetés a számításelméletbe 1

3. gyakorlat

2023.

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. Egész szám-e az alábbi?
$$\frac{5 \cdot 279^{961} + 5}{1400}$$

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

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

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

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

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

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

13. Egy algoritmus bemenete egy tízes számrendszerben megadott n pozitív egész szám. Az algoritmus egy ciklusból áll, aminek a magja $2n$-szer fut le, és a ciklusmag minden végrehajtásakor kiírunk egy 1-est a képernyőre.
    (a) Határozzuk meg a bemenet méretét.
    (b) Hányszor fut le a ciklusmag?
    (c) Döntsük el, hogy a ciklusmag lefutásainak száma a bemenet méretében polinomiális-e.
    (d) Határozzuk meg a ciklusmagon belül végrehajtott műveletek lépésszámát.
    (e) Határozzuk meg a teljes algoritmus lépésszámát és döntsük el, hogy ez a bemenet méretében polinomiális-e.

14. Az alábbi két C kód közül az első a bemenetként (10-es számrendszerben) kapott n pozitív egész szám négyzetét, a második pedig az n számjegyeinek az összegét számítja ki. Tegyük fel, hogy a kódok végrehajtásakor a gép az alapműveleteket az (alsó tagozatban tanult) „írásbeli" összeadás, szorzás, stb. segítségével végzi el. Döntsük el, hogy az eljárások polinomiálisak-e. (A `floor(n/10.0)` az $n/10$ alsó egészrészét adja vissza.)

(a)
```
x = n; y = 0;
while (x > 0) {
    x = x-1;
    y = y+n;
}
printf("Eredmény: %d", y);
```

(b)
```
x = 0; y = 0;
while (n > 0) {
    x = floor(n/10.0);
    y = y+n-10*x;
    n = x;
}
printf("Összeg: %d", y);
```