5. feladatsor: Számelmélet

Pozitív osztók száma, legnagyobb közös osztó és legkisebb közös többszörös kiszámítása a kanonikus alakból

1. Írjuk fel a következő számokat kanonikus alakban, majd határozzuk meg pozitív osztóik számát:

a) 9 b) 7 c) 45 d) 360 e) 13882 f) 355218

2. Az alábbi példákban határozzuk meg (a, b) és $[a, b]$ értékét a *kanonikus alak* segítségével:

a) $a = 245$, $b = -378$ b) $a = -147$, $b = 514$ c) $a = 713$, $b = 276$

Euler-féle φ-függvény, Euler-Fermat tétel és alkalmazásai

3. Számoljuk ki $\varphi(n)$ értékét $n = 1, 2, 3, 4, 10, 24, 96, 100$ esetén!

4. Bizonyítsuk be, hogy

a) $n^6 - 1$ osztható 7-tel, ha $(n, 7) = 1$;
b) $n^{12} - 1$ osztható 7-tel, ha $(n, 7) = 1$;
c) $n^{6k} - 1$ osztható 7-tel ha $(n, 7) = 1$.

5. Bizonyítsuk be, hogy bármely egész x-re $x^7 \equiv x \mod 42$.

6. Határozzuk meg 3^{1003} utolsó három számjegyét.

7. Állapítsuk meg, hogy 173^{163} milyen maradékot ad 17-tel osztva.

8. Határozzuk meg (a tizes számrendszerben felírt) 143^{143} utolsó három jegyét hármas alapú számrendszerben.

9. Milyen maradékot ad 103-mal osztva a következő szám: $205^{206^{207}}$?

10. Határozzuk meg a $37^{39^{42}}$ szám utolsó két számjegyét.

11. Mi lesz $17^{3^{2013}}$ utolsó két számjegye nyolcas számrendszerben?

12. Mi a $11^{2013^{26}}$ utolsó két jegye 10-es számrendszerben?

13. Milyen maradékot ad

a) 323^{149}-nek a 63-mal;
b) 423^{173}-nak az 52-vel;
c) 495^{173}-nak a 98-cal;
d) 457^{101}-nek a 90-nel való osztáskor?

14. Bizonyítsuk be, hogy $n^{13} - n$ minden n egészre osztható a 2, 3, 5, 7 és 13 számokkal.

15. Oldjuk meg az alábbi kongruenciákat az Euler-Fermat tétel segítségével:

a) $21x \equiv 14 \mod 35$; b) $172x \equiv 6 \mod 62$; c) $3x \equiv 8 \mod 13$; d) $12x \equiv 9 \mod 18$

való osztáskor?

16. Mutassuk meg, hogy $a^{1729} \equiv a \mod 1729$, habár az 1729 mégsem prím.

További feladatok

17. Legyenek $p = 29$ és $q = 31$ és legyen most $n = pq =$ az RSA-eljárásban használt modulus (a nyilvános kulcs modolusa).

a) Válasszunk egy alkalmas e értéket a nyilvános kulcs kitevőjéül.

b) A fenti (n, e) (nyilvános) kulcsot alkalmazva titkosítsuk a 134 üzenetet az RSA-algoritmussal.

c) Határozzuk meg a d (titkos) kulcs (egy megfelelő) értékét.

d) Fejtsük meg a 219 üzenetet.

18. Írjunk programot, mely egy adott p prím esetén keres egy generátort modulo p, továbbá mely legenerálja az adott generátorhoz tartozó diszkrét logaritmus táblázatot!