

Számelmélet 2005/2006 ősz

10. gyakorlat: Primitív gyök

1. Keressük meg az összes primitív gyököt modulo 13, 10 és 18.
2. Oldjuk meg a $3x^5 \equiv 2 \pmod{13}$ és a $3x^{10} \equiv 4 \pmod{13}$ kongruenciákat.
- 3. Keressük meg az $x^{10} \equiv 7 \pmod{17}$ és a $11x^{15} \equiv 17 \pmod{23}$ kongruenciák összes megoldását.
4. Tegyük fel, hogy az $x^k \equiv 1 \pmod{p}$ összes megoldása a $b_1, b_2, \dots, b_r$ (modulo p különböző) számok. Legyen $(a, p) = 1$ és $x^k \equiv a \pmod{p}$ egy megoldása c . Bizonyítsuk be, hogy ekkor $x^k \equiv a \pmod{p}$ összes (modulo p különböző) megoldása éppen $cb_1, cb_2, \dots, cb_r$.
5. Legyen p prím, k egész. Mivel kongruens

$$\sum_{a=1}^{p-1} a^k$$

modulo p ?

- 6. Adjunk új bizonyítást a Wilson-tételre $((p-1)! \equiv -1 \pmod{p})$ primitív gyökök segítségével.
- 7. Legyen p prím, $d \mid p-1$, g primitív gyök modulo p és $(a, p) = 1$. Mutassuk meg, hogy

$$o_p(a) = d \iff \exists t, \text{ amelyre } (t, d) = 1 \text{ és } \text{ind}_g a = t \cdot \frac{(p-1)}{d}$$

8. Mutassuk meg, hogy ha $m \neq 2$, akkor két modulo m primitív gyök szorzata nem lehet primitív gyök.