

Számelmélet 2009/2010 ősz

7. gyakorlat: Primitív gyök, index

1. Oldjuk meg a $3x^5 \equiv 2 \pmod{13}$ és a $3x^{10} \equiv 4 \pmod{13}$ kongruenciákat!
- 2. Adjuk meg az $5x^{22} \equiv 6 \pmod{17}$ összes megoldását.
- 3. 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 $cb_1, cb_2, \dots, cb_r$.
4. Igazoljuk, hogy amennyiben g primitív gyök modulo m , akkor
 - (a) g^k primitív gyök $\iff (k, \varphi(m)) = 1$ és
 - (b) modulo m pontosan $\varphi(\varphi(m))$ (páronként inkongruens) primitív gyök van.
5. Legyen p prím, k egész. Mivel kongruens

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

modulo p ?

6. Legyen $p > 2$ prím. Milyen maradékot ad p -vel osztva az összes (páronként inkongruens) primitív gyök szorzata?
7.
 - (a) Mutassunk példát olyan 1 főegyütthatós, egész együtthatós f polinomra, aminek f fokszámánál több gyöke van modulo 15.
 - (b) Lássuk be (az előbbi f segítségével), hogy $\mathbb{Z}_{15}[x]$ polinomgyűrűben nem egyértelmű minden polinom irreducibilis polinomokra bontása.