Számelmélet 2006/2007 ősz
6. gyakorlat: Primitív gyök, index, Wilson-tétel

1. Oldjuk meg a $3x^5 \equiv 2 \ (13)$ és a $3x^{10} \equiv 4 \ (13)$ kongruenciákat!

- 2. Adjuk meg az $5x^{22} \equiv 6 \ (17)$ összes megoldását.

- 3. Tegyük fel, hogy az $x^k \equiv 1 \ (p)$ összes megoldása a b_1, b_2, ..., b_r (modulo p különböző) számok. Legyen $(a,p) = 1$ és $x^k \equiv a \ (p)$ egy megoldása c. Bizonyítsuk be, hogy ekkor $x^k \equiv a \ (p)$ összes (modulo p különböző) megoldása éppen cb_1, cb_2, ..., 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. (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 irreducíbilis polinomokra bontása.

7. Legyen p prím és jelölje az $f(x) \equiv 0 \ (p)$ kongruencia (modulo p páronként különböző) megoldásainak számát r. Lássuk be, hogy

$$r \equiv -\sum_{a=1}^{p} f(a)^{p-1} \quad (p)$$

8. Tegyük fel, hogy p egy $4k-1$ alakú prím. Bizonyítsuk be, hogy

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \quad (p).$$

9. Legyen $p \geq 3$ prím, $\{a_1, a_2, \ldots, a_p\}$ és $\{b_1, b_2, \ldots, b_p\}$ teljes maradékrendszerek modulo p. Igazoljuk, hogy $\{a_1b_1, a_2b_2, \ldots, a_pb_p\}$ nem lehet teljes maradékrendszer. (Útmutatás: Használjuk a Wilson-tételt.)