

Számelmélet 2004/2005 ősz

6. gyakorlat: Magasabb fokú kongruenciák, rend

- 1. (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.
- 2. Legyen p prím és jelölje az $f(x) \equiv 0 \pmod{p}$ kongruencia (modulo p páronként különböző) megoldásainak számát r . Lássuk be, hogy

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

- 3. Számoljuk ki az alábbi rendeket!

(a) $o_{21}(23)$

- (b) $o_{89}(86)$

- 4. Tegyük fel, hogy p prím és $o_p(a) = 3$.

(a) Bizonyítsuk be, hogy $1 + a + a^2 \equiv 0 \pmod{p}$.

(b) Számítsuk ki $o_p(1 + a)$ értékét.

- 5. Bizonyítsuk be, hogy amennyiben $o(a) = n$, akkor $o(a^k) = \frac{n}{(n,k)}$.

- 6. Tegyük fel, hogy egy 54 lapos kártyapakli keverésére a következő módszert alkalmazzuk: két egyenlő részre szedjük szét a paklit, majd egymásba pörgetjük a két kupac kártyát, úgy, hogy a felső fél alsó lapja kerül most legalulra, utána az alsó fél alsó lapja, majd a felső fél (alulról) második lapja, majd az alsó fél (alulról) második lapja, és így tovább. Ezt elismételjük néhányszor, hogy jól megkeveredjen a pakli. Valójában viszont csalni szeretnénk, addig akarjuk keverni a kártyákat, amíg vissza nem rendeződnek az eredeti sorrendjükbe. Hányszor kell legalább kevernünk?

(Útmutatás: Számozzuk be a kártyákat alulról az $1, 2, \dots, 54$ számokkal és írjuk fel, hogy az n sorszámú kártya egy keverés után hányadik helyre kerül.)

- 7. Mutassuk meg, hogy $(a^n - 1, a^k + 1) \leq 2$, amennyiben n páratlan.