

Számelmélet 2009/2010 ősz
5. gyakorlat: Lineáris kongruenciák, rend

1. Keressük meg az alábbi kongruenciák megoldásait!

- (a) $5x \equiv 2 \pmod{17}$;
- (b) $-6x \equiv 10 \pmod{27}$;
- (c) $32x \equiv 8 \pmod{34}$;
- (d) $18x \equiv 99 \pmod{323}$;
- (e) $555x \equiv 5555 \pmod{55555}$.

2. Oldjuk meg a következő kongruenciarendszereket!

- (a) $3x \equiv 4 \pmod{11}$, $11x \equiv 3 \pmod{15}$;
- (b) $3x \equiv 4 \pmod{16}$, $11x \equiv 3 \pmod{14}$.

3. Mi a következő (nem lineáris) kongruenciák megoldása?

- (a) $2x^{20} + 3x + 4 \equiv 0 \pmod{176}$;
- (b) $2x^{91} + 5x + 1 \equiv 0 \pmod{297}$.

4. Számoljuk ki az alábbi rendeket!

- (a) $o_{21}(23)$
- (b) $o_{89}(86)$

5. 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.

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

7. 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.)

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