

Számelmélet 2005/2006 őszi 9. gyakorlat: Rend

1. Számoljuk ki az alábbi rendeket!
 - (a) $o_{21}(23)$
 - (b) $o_{89}(86)$
2. Ebben a feladatban megmutatjuk, hogy ha a és b rendje relatív prím, akkor $o(ab) = o(a)o(b)$.
 - (a) Először lássuk be, hogy $o(g) = o(g^{-1})$.
 - (b) Ezt felhasználva bizonyítsuk, hogy $(ab)^d = 1$ esetén $o(a^d) = o(b^d)$ osztja $(o(a), o(b))$ -t.
 - (c) Igazoljuk az állítást!
3. 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.
4. 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.)
- 5. Legyen p prím és $o_p(a) = 2000$. Mennyi lehet $o_p(a^2)$, $o_p(a^3)$ és $o_p(-a)$ értéke?
6. Tegyük fel, hogy $a^{33} \equiv -1 \pmod{71}$. Mennyi a^{22} modulo 71?
- 7. Mutassuk meg, hogy $(a^n - 1, a^k + 1) \leq 2$, amennyiben n páratlan.
(Útmutatás: Ha $d = (a^n - 1, a^k + 1)$, akkor vizsgáljuk $o_d(a)$ számot.)