

Számelmélet 2005/2006 ősz

11. gyakorlat: Kvadratikus maradékok

A feladatokban p páratlan prím.

1. Számítsuk ki az alábbi Legendre-szimbólumok értékét.

$$\left(\frac{37}{19}\right), \quad \left(\frac{-100}{19}\right), \quad \bullet \quad \left(\frac{26123}{65537}\right)$$

2. Legyen g primitív gyök modulo p . Számoljuk ki minden k -ra a $\left(\frac{g^k}{p}\right)$ Legendre-jelet.
3. Bizonyítsuk be, hogy ha $o_p(a)$ páratlan, akkor a kvadratikus maradék modulo p . Mely prímekre igaz az állítás megfordítása?
4. Tegyük fel, hogy $\left(\frac{a}{97}\right) = -1$ és a nem primitív gyök modulo 97. Számítsuk ki $o_{97}(a)$ értékét.
- 5. Igazoljuk, hogy az alábbi állítások ekvivalensek.
 - (i) ab , ac és bc is kvadratikus maradék.
 - (ii) Vagy a , b és c is kvadratikus maradék, vagy mindhárom kvadratikus nem-maradék.
6. Mutassuk meg, hogy egy $8c^2 - 1$ alakú számnak minden prímosztója $8k \pm 1$ alakú és $c \neq 0$ esetén van $8k - 1$ alakú prímosztója.
- 7. Mely p prímekre van az $x^2 + y^2 \equiv 0 \pmod{p}$ kongruenciának nemtriviális megoldása. (Triviális megoldás az $x \equiv 0 \pmod{p}$, $y \equiv 0 \pmod{p}$; minden egyéb megoldás nemtriviális.)
8. Mennyi az $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)$ Legendre-jelek összege és szorzata?