

Primitív gyök, négyzetes maradék

p végig páratlan prímszámot jelöl, a, b, c pedig olyan egészeket, amelyeknek p nem osztója.

1. Hány (inkongruens) megoldása van az alábbi kongruenciáknak?

- (a) $x^2 \equiv 88 \pmod{163}$;
- (b) $6x^{25} + x^5 + 5x \equiv 0 \pmod{23}$;
- (c) $x^{10} - x^5 - 4 \equiv 0 \pmod{11}$.

2. Határozza meg a következő Legendre-szimbólumok értékét (minél egyszerűbben):

(a) $\left(\frac{97}{101}\right)$, (b) $\left(\frac{32}{67}\right)$, (c) $\left(\frac{106}{211}\right)$, (d) $\left(\frac{105}{307}\right)$.

3. Milyen maradékot ad 211-gyel osztva 106^{106} ?

4. Mutassa meg, hogy ha ab, bc, ac mindegyike négyzetes maradék modulo p , akkor vagy a, b, c is mind négyzetes maradék modulo p , vagy a, b, c mind négyzetes nemmaradék modulo p .

5. Igazolja, hogy ha p egy $12n^2 + 1$ alakú egész szám prímosztója, akkor

- (a) -3 négyzetes maradék modulo p , és így
- (b) p $6k + 1$ alakú.

6. Mutassa meg, hogy

- (a) ha p $8k \pm 1$ alakú, akkor $p \mid 2^{\frac{p-1}{2}} - 1$.
- (b) ha p $4k + 3$ alakú és a négyzetes maradék modulo p , akkor az $x^2 \equiv a \pmod{p}$ kongruencia megoldása $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$.

7. Döntse el, igazak-e az alábbi állítások; az igazakat bizonyítsa be, a hamisakra adjon ellenpéldát:

- (a) ha b négyzetes maradék modulo p , akkor b inverze modulo p szintén négyzetes maradék modulo p ;
- (b) ha $o_p(b)$ páratlan, akkor b négyzetes maradék modulo p ;
- (c) ha b négyzetes maradék modulo p , akkor $o_p(b)$ páratlan;
- (d) ha b primitív gyök modulo p , akkor b négyzetes maradék modulo p .

8. Legyenek $a_1, \dots, a_{\frac{p-1}{2}}$ egy modulo p redukált maradékrendszerben a négyzetes maradékok modulo p . Számítsa ki az $a_1 \cdots a_{\frac{p-1}{2}}$ szorzat maradékát modulo p .