8. gyakorlat

1. Oldjuk meg az alábbi kongruenciákat:

   (a) $3x^2 + 5x + 5 \equiv 0 \pmod{13}$;

   (b) $7x^2 + 8x \equiv 5 \pmod{17}$;

   (c) $6x^{25} + x^5 + 5x \equiv 0 \pmod{23}$;

   (d) $2x^{17} + 5x + 1 \equiv 0 \pmod{19}$.

2. Számítsuk ki az
$$\left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right),\ \ldots,\left(\frac{p-1}{p}\right)$$
Legendre-szimbólumok összegét és szorzatát.

3. Jelöljük $n(p)$ azt a legkisebb pozitív egész számot, ami kvadratikus nemmaradék modulo p prím. Bizonyítsuk be, hogy

   (a) $n(p)$ mindig prímszám.

   (b)* $n(p) < 1 + \sqrt{p}$.

4. Bizonyítsuk be, hogy ha $1999 \mid a^2 + 2b^2$, akkor $1999 \mid a$ és $1999 \mid b$.

5. Számítsuk ki az alábbi Jacobi-szimbólumokat:
$$a)\ \left(\tfrac{1234567}{225}\right);\quad b)\ \left(\tfrac{31}{95}\right);\quad c)\ \left(\tfrac{589}{1999}\right);\quad d)\ \left(\tfrac{1113}{11131}\right).$$

6. Legyen $n > 1$ páratlan, $n \nmid a$ és tekintsük az
$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$
kongruenciát, ahol $\left(\frac{a}{n}\right)$ a Jacobi-szimbólum. Ha n prím, akkor ez minden $n \nmid a$-ra teljesül. Igazoljuk, hogy ha n összetett, akkor viszont a fenti kongruencia egy teljes maradékrendszer kevesebb, mint a felére teljesül. Tehát ha 1000 db a-ra elvégezzük a tesztet és mindig teljesült a kongruencia, akkor 2^{-1000}-nél kisebb a valószínűsége, hogy az n összetett.

7. Igazoljuk, hogy ha a és b mindkettő előáll $x^2 - 2y^2$ alakban ($x, y \in \mathbb{Z}$), akkor ab is előáll.

8.* Legyen ε egy primitív p-edik egységgyök és u egy p-vel nem osztható pozitív egész szám, továbbá $S_u := \sum_{j=0}^{p-1} \varepsilon^{uj^2}$. Igazoljuk, hogy $S_u = \left(\frac{u}{p}\right) S_1$ és $S_1^2 = \left(\frac{-1}{p}\right) p$. **Hogy jön ki ebből a kvadratikus reciprocitási tétel?

9.* Adjunk meg olyan f egész együtthatós polinomot, aminek nincs racionális gyöke, de az $f(x) \equiv 0 \pmod{m}$ kongruencia minden m-re megoldható.