TEORIJA BROJEVA U KRIPTOGRAFIJI

4. zadaća

7. 4. 2004.

1. Za prirodan broj m, sa $s(m)$ označimo broj kvadrata u prstenu $\mathbb{Z}_m$, tj. broj elemenata a skupa $\{0, 1, \dots m-1\}$ za koje postoji cijeli broj x takav da je $x^2 \equiv a \pmod{m}$. Odredite sve prirodne brojeve $m \le 100$ sa svojstvom da je $\frac{s(m)}{m} < \frac{1}{3}$.

2. Neka su x_1, x_2, x_3 nultočke polinoma $f(x) = x^3 + ax + b$. Dokažite da vrijedi

$$(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -4a^3 - 27b^2.$$

3. Nađite sve točke konačnog reda, te odredite strukturu torzijske grupe za sljedeće eliptičke krivulje nad $\mathbb{Q}$:

   a) $y^2 = x^3 - x$, b) $y^2 = x^3 + 4$, c) $y^2 = x^3 + x + 2$, d) $y^2 = x^3 - 43x + 166$.

4. Za polinom

$$p(x) = (x-18)(x-16)(x-15)(x-13)(x-12)(x-11)(x-10)(x-9)(x+15)(x+16)(x+17)(x+18),$$

   odredite polinome $q(x), r(x) \in \mathbb{Q}[x]$ takve da vrijedi $p(x) = q^2(x) - r(x)$ i $\deg r \le 4$.

5. Za svaki od brojeva $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$, pronađite jednu eliptičku krivulju E_n nad $\mathbb{F}_5$ sa svojstvom da je red grupe $E_n(\mathbb{F}_5)$ jednak n.

6. Zadana je eliptička krivulja

$$E: \quad y^2 = x^3 + x + 4$$

   nad poljem $\mathbb{F}_{151}$. Odredite red grupe $E(\mathbb{F}_{151})$ Shanks-Mestreovom metodom, koristeći točku $P = (0, 2)$.

Rok za predaju zadaće je 12.5.2004.

Andrej Dujella