ALGORITMI ZA ELIPTIČKE KRIVULJE

3. zadaća

27. 5. 2009.

1. 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 $\deg r \leq 4$.

2. Izračunajte Mazurovu ogradu M_3 za rang eliptičke krivulje

   $$E : \; y^2 + xy + y = x^3 - 4213613959455x + 3328416232976793662$$

   s torzijskom grupom $\mathbb{Z}_3$.

3. Dokažite da jednadžba $y^2 = x^3 + 7$ nema cjelobrojnih rješenja.

4. 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.

5. 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 $P = (0, 2)$.

6. Pronađite barem jednu anomalnu i barem jednu supersingularnu eliptičku krivulju nad $\mathbb{F}_{23}$.

Rok za predaju zadaće je 10.6.2009.

Andrej Dujella