DIOFANTOVE m-TORKE I ELIPTIČKE KRIVULJE

3. zadaća

1. Neka je E eliptička krivulja s jednadžbom
$$y^2 = x^3 + ax + b.$$
Neka je $P = (x_1, y_1)$ točka na E, te neka je $2P = (x_2, y_2)$. Dokažite da vrijedi
$$y_1^2(4x_2(3x_1^2 + 4a) - 3x_1^3 + 5ax_1 + 27b) = 4a^3 + 27b^2.$$

2. Nađite sve točke konačnog reda te odredite strukturu torzijske grupe za eliptičku krivulju
$$y^2 = \Big(\frac{12}{7}x + 1\Big)\Big(-\frac{15}{28}x + 1\Big)\Big(\frac{7}{4}x + 1\Big)$$
induciranu racionalnom Diofantovom trojkom $\{\frac{12}{7}, -\frac{15}{28}, \frac{7}{4}\}$. Odredite sve proste brojeve p za koje vrijedi $|E(\mathbb{Q})_{\mathrm{tors}}| = |E(\mathbb{F}_p)|$.

3. Izračunajte rang eliptičke krivulje nad $\mathbb{Q}$ zadane jednadžbom
$$y^2 = x^3 - 82x.$$
Koje od jednadžbi četvrtog stupnja koje je javljaju u algoritmu silaska s pomoću 2-izogenije imaju rješenja?

4. Neka su $a_1, a_2, a_3, a_4, a_5, a_6$ različiti prirodni brojevi. Neka je $p(x) = (x^2 - a_1^2)(x^2 - a_2^2)(x^2 - a_3^2)(x^2 - a_4^2)(x^2 - a_5^2)(x^2 - a_6^2)$, te neka su $q(x)$ i $r(x)$ polinomi s racionalnim koeficijentima takvi da je $p = q^2 - r$ i $\deg r \leq 4$. Odredite prirodne brojeve $a_1, a_2, a_3, a_4, a_5, a_6$ tako da vrijedi:
   - $\deg r = 4$,
   - r nema višestrukih korijena,
   - vodeći koeficijent od r je kvadrat racionalnog broja,
   - eliptička krivulja E ekvivalentna krivulji $y^2 = r(x)$ ima rang ≥ 6.

   Napomena: polinom $r(x)$ je paran, pa eliptička krivulja E ima točku reda 2.

5. Nađite jednu krivulju nad $\mathbb{Q}$ takvu da je
$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}^2.$$

Andrej Dujella