ALGORITMI ZA ELIPTIČKE KRIVULJE

2. zadaća

18. 3. 2008.

1. Zadana je familija eliptičkih krivulja

$$E_t \,:\, y^2 = x(x+t)(x+t+27).$$

Nađite racionalne brojeve t_1, t_2 sa svojstvom da je $E_{t_1}(\mathbb{Q})_{\text{tors}} = \mathbb{Z}_2 \times \mathbb{Z}_4$, $E_{t_2}(\mathbb{Q})_{\text{tors}} = \mathbb{Z}_2 \times \mathbb{Z}_6$.

2. Neka je $P \in E(\mathbb{Q})$ točka za koju vrijedi da je $< P, Q >= 0$ za svaki $Q \in E(\mathbb{Q})$. Dokažite da je tada P torzijska točka.

3. Na krivulji

$$E \,:\, y^2 = x^3 - x^2 - 3225667994796x + 2205916672708538820$$

nađite sve cjelobrojne točke $P = (x, y)$ takve da je $|x| < 10000000$. Među tim točkama nađite što veći skup točaka koje su nezavisne mod $E(\mathbb{Q})_{\text{tors}}$, tj. nađite što bolju donju ogradu za rang od E.

4. Zadana je eliptička krivulja

$$E \,:\, y^2 + xy = x^3 - 838180107375202300215 60x + 933440210183596939568163615814 5600$$

i njezina Mordell-Weilova baza

$$\begin{aligned}
P_1 &= [1618359630510240/10201, -5632981219622609708760/1030301],\\
P_2 &= [823553205878880/121, 2361296899738756023228 0/1331],\\
P_3 &= [7286328253584/49, -4320493144544323944/343],\\
P_4 &= [1473540358480/9, -7849844178883720/27],\\
P_5 &= [29034296357468/169, 5004336579041355704/2197],\\
P_6 &= [10477596585780/49, -11824951209336208980/343].
\end{aligned}$$

Nađite Mordell-Weilovu bazu za $E(\mathbb{Q})$ koja se sastoji od točaka s cjelobrojnim koordinatama.

5. Izračunajte rang eliptičke krivulje

$$E \,:\, y^2 = (x+1)(3x+1)(8x+1).$$

6. Nađite tri racionalna broja x_1, x_2, x_3 sa svojstvom da su brojevi $x_i + 1$, $3x_i + 1$ i $8x_i + 1$ kvadrati racionalnih brojeva ($i = 1, 2, 3$).

Rok za predaju zadaće je 8.4.2009.

Andrej Dujella