# ODABRANE TEME IZ TEORIJE BROJEVA: SEDMA ZADAĆA

## 1. Točke definirane nad kubnim poljima

Neka je $f(x) \in \mathbb{Q}[x]$ normirani polinom trećeg stupnja (s različitim nultočkama) i $E : y^2 = f(x)$ eliptička krivulja nad $\mathbb{Q}$, $K$ polje stupnja tri nad $\mathbb{Q}$ i $(x_0, y_0) \in E(K)$. Tada postoji polinom $h(x) = ax^2 + bx + c \in \mathbb{Q}[x]$, takav da je $y_0 = h(x_0)$. Neka je $g(x) \in \mathbb{Z}[x]$ minimalni polinom od $x_0$. Ako je $a \neq 0$ tada postoji linearni polinom $k(x) \in \mathbb{Q}[x]$ s nultočkom $x_1$ takav da vrijedi

$$h(x)^2 - f(x) = g(x)k(x),$$

tj. točka $(x_1, h(x_1))$ je iz $E(\mathbb{Q})$.

Cilj ove zadaće je istražiti gore definirano preslikavanje $E(K) \to E(\mathbb{Q})$, $(x_0, y_0) \mapsto (x_1, h(x_1))$ (slučaju $a = 0$ "odgovara" točka u beskonačnosti). Pitanje je kako "bolje" opisati to preslikavanja.

Probajte prvo eksperimentiranjem naslutiti odgovor, a zatim ga dokazati. Za računanje Mordell-Weilove grupe nad kubnim poljima možete koristiti Magmu (`http://magma.maths.usyd.edu.au/calc/`). Dosta informacija o kubnim poljima možete naći na `http://www.lmfdb.org/`. Npr. možda nije loše eksperimentirati malo s cikličkim poljima. Ako je $K$ jedno takvo polje i ako je $\sigma \in \mathrm{Gal(K/\mathbb{Q})}$ generator Galoisove grupe, tada za $P \in E(K)$ imamo definirano prirodno preslikavanje, trag, $E(K) \to E(\mathbb{Q})$ formulom $P \mapsto P + P^{\sigma} + P^{\sigma^2}$. Postoji li veza između našeg preslikavanja i traga?