Domácí úkol z 10. listopadu 2022

Nechť E je eliptická křivka nad $\mathbb{Q}$ daná rovnicí

$$y^2 = x^3 - 2x.$$

1. Najděte všechny body $(x, y) \in E(\mathbb{Q})$ splňující $x, y \in \mathbb{Z}$ a $y^2 \mid 4 \cdot (-2)^3$.
2. Spočtěte podgrupu $E(\mathbb{Q})_{tors}$ bodů konečného řádu grupy $E(\mathbb{Q})$.
3. Vysvětlete, proč je grupa $E(\mathbb{Q})$ nekonečná.

Označme $K = \mathbb{Q}(\sqrt{2})$. Dále označme $e_1, e_2, e_3 \in \mathbb{Z}[\sqrt{2}]$ kořeny polynomu $x^3 - 2x$. Okruh $\mathbb{Z}[\sqrt{2}]$ je okruh s jednoznačným rozkladem a platí

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm\varepsilon^k; k \in \mathbb{Z}\},$$

kde $\varepsilon = 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Označme $\pi = \sqrt{2}$ (π je ireducibilní prvek okruhu $\mathbb{Z}[\sqrt{2}]$). Podobně jako na semináři lze ukázat, že pro libovolné $x \in K, x \neq e_i$ existuje jediné bezčtvercové $a \in \mathbb{Z}[\sqrt{2}]$ takové, že

$$x - e_i = au^2$$

pro vhodné $u \in K$. Pokud navíc existuje $y \in K$ takové, že $(x, y) \in E(K)$, pak $a \in \big\{(-1)^r \cdot \pi^s \cdot \varepsilon^t; r, s, t \in \{0, 1\}\big\}$. Dále lze ukázat, že zobrazení

$$\phi\colon E(K) \to \big(K^\times/(K^\times)^2\big) \oplus \big(K^\times/(K^\times)^2\big) \oplus \big(K^\times/(K^\times)^2\big)$$

definované předpisem

$$\begin{aligned}
(x, y) &\mapsto (x - e_1, x - e_2, x - e_3) \qquad \text{pro } y \neq 0 \\
\infty &\mapsto (1, 1, 1) \\
(e_1, 0) &\mapsto ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) \\
(e_2, 0) &\mapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) \\
(e_3, 0) &\mapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2))
\end{aligned}$$

je homomorfismus grup, jehož jádrem je $2E(K)$. (Výše uvedené poznatky můžete využít při řešení následujících úloh, ale nemusíte je dokazovat.)

* 4. Označme $\mathfrak{o}_\pi = \{\alpha \in K; \operatorname{ord}_\pi(\alpha) \geq 0\}$, kde $\operatorname{ord}_\pi\colon K \to \mathbb{Z} \cup \{\infty\}$ je příslušná valuace. Dokažte, že pro libovolné $u \in \mathfrak{o}_\pi$ platí

$$\operatorname{ord}_\pi(u) = 0 \Rightarrow u^2 \equiv 1 \pmod{\pi^5} \quad \text{nebo} \quad u^2 \equiv \varepsilon^2 \pmod{\pi^5}.$$

(Nápověda: Můžete využít toho, že každý prvek α okruhu $\mathfrak{o}_\pi$ lze vyjádřit jako (případně nekonečný) součet $\alpha = \sum_{i=0}^{\infty} a_i \pi^i$, přičemž toto vyjádření je jednoznačné, předpokládáme-li, že koeficienty a_i jsou 0 nebo 1. Existenci a jednoznačnost takového vyjádření nemusíte dokazovat.)

5. Ukažte, že neexistují $u, v \in \mathfrak{o}_\pi^\times = \{\alpha \in K; \mathrm{ord}_\pi(\alpha) = 0\}$ tak, že
$$u^2 - v^2 = \pm 2.$$
(Nápověda: Řešte modulo π^5.)

6. Ukažte, že neexistují $u, v \in \mathfrak{o}_\pi^\times$ tak, že
$$u^2 - \varepsilon v^2 = \pm 2.$$
(Nápověda: Řešte modulo π^5.)

7. Označme $e_1 = 0$, $e_2 = \pi$, $e_3 = -\pi$. Ukažte, že žádná z trojic $(1, \pi, \pi)$, $(\varepsilon, \varepsilon\pi, \pi)$, $(\varepsilon, \pi, \varepsilon\pi)$ neleží v obraze ϕ. *(Nápověda: Můžete použít body 5 a 6.)*

8. Spočtěte $|\phi(E(K))|$. *(Nápověda: Nejprve využijte toho, že pro libovolné $(x, y) \in E(K)$ musí být $x - e$, kde e je nejmenší z čísel e_1, e_2, e_3, nezáporné. Pak využijte bod 7.)*

9. Určete, čemu je izomorfní $E(\mathbb{Q})$, víte-li, že grupa $E(K)$ je konečně generovaná. *(Nápověda: Využijte toho, že $E(\mathbb{Q})$ je podgrupa $E(K)$, a tedy $\mathbb{Z}$-rank grupy $E(\mathbb{Q})$ je menší roven $\mathbb{Z}$-ranku grupy $E(K)$.)*