Buď $\frac{a}{b}$ zlomek ve zkráceném tvaru, tj. $\gcd(a,b)=1$. Definujeme

$$H\left(\frac{a}{b}\right) = \max\{|a|, |b|\}$$

a

$$h\left(\frac{a}{b}\right) = \log H\left(\frac{a}{b}\right).$$

Nechť E je eliptická křivka definovaná nad $\mathbb{Q}$ a nechť $(x,y) \in E(\mathbb{Q})$ je libovolný. Pak definujeme

$$h(x,y) = h(x), \qquad h(\infty) = 0.$$

Snadno se vidí, že pro libovolné $M \in \mathbb{R}$ je množina

$$\{P \in E(\mathbb{Q});\ h(P) \leq M\}$$

konečná.

Věta
Grupa $E(\mathbb{Q}) / 2E(\mathbb{Q})$ je konečná.

Buď E eliptická křivka zadaná rovnicí

$$y^2 = x^3 + Ax + B = (x-e_1)(x-e_2)(x-e_3)$$

a předpokládejme, že $e_1, e_2, e_3 \in \mathbb{Z}$.

Lemma Pro libovolné nenulové racionální x existuje jediné bezčtvercové celé číslo a takové, že $x = au^2$ pro vhodné $u \in \mathbb{Q}$.

Dk. Pro libovolné prvočíslo p definujme $v_p(a)$ jako zbytek po dělení čísla $v_p(x)$ dvěma, tj. $v_p(a) \in \{0,1\}$ a $v_p(a) \equiv v_p(x) \pmod 2$.
Pak

$$a = (-1)^{\operatorname{sgn}(x)} \cdot \prod_p p^{v_p(a)}$$

je hledané číslo.

Pozn. Pro $x=0$ platí

$$0 = a \cdot 0^2$$ pro libovolné a bezčtvercové.

Nechť $P = (x_0, y_0) \in E(\mathbb{Q})$, $y_0 \neq 0$ je libovolný bod eliptické křivky E. Pak

$$x_0 - e_1 = au^2$$
$$x_0 - e_2 = bv^2$$
$$x_0 - e_3 = cw^2$$

pro vhodná bezčtvercová čísla a, b, c a vhodná $u, v, w \in \mathbb{Q}$. Protože

$$y_0^2 = (x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = abc \cdot (uvw)^2,$$

platí, že abc je čtverec.

Tvrzení Buď

$$S = \{p \text{ prvočíslo} \mid p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

Pokud prvočíslo p dělí abc, pak $p \in S$.

Dk.

Nechť p je prvočíslo a předpokládejme, že $p \mid a$, tedy $v_p(a) = 1$. Označme $k = v_p(x_0 - e_1)$. Pak

$$k = v_p(x_0 - e_1) = v_p(au^2) = v_p(a) + 2v_p(u) = 1 + 2v_p(u)$$

je číslo liché. Pokud $k < 0$, pak

$$v_p(x_0) = v_p(x_0 - e_1 + e_1) = \min\{v_p(x_0 - e_1), v_p(e_1)\} = k$$

pak

$$v_p(x_0 - e_1) = v_p(x_0 - e_2) = k, \text{ proto}$$

$$2v_p(y_0) = v_p(y_0^2) = v_p((x_0 - e_1)(x_0 - e_2)(x_0 - e_3)) = 3k, \text{ spor.}$$

Předpokládejme, že $k > 0$. Pak $v_p(x_0) \geq 0$, $v_p(x_0 - e_2) \geq 0$ a $v_p(x_0 - e_3) \geq 0$. Kdyby $p \notin S$, pak $v_p(e_1 - e_3) = v_p(e_1 - e_2) = 0$.

$$v_p(x_0 - e_2) = v_p(x_0 - e_1 + e_1 - e_2) = 0$$

a podobně

$$v_p(x_0 - e_3) = v_p(x_0 - e_1 + e_1 - e_3) = 0.$$

Pak

$$2v_p(y_0) = v_p(y_0^2) = v_p(x_0 - e_1) + v_p(x_0 - e_2) + v_p(x_0 - e_3) = k,$$

Spor.

Věta Zobrazení

$$\phi : E(\mathbb{Q}) \longrightarrow (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \oplus (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \oplus (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)$$

definované předpisem

$$\begin{aligned}
(x,y) &\longmapsto (x-e_1,\ x-e_2,\ x-e_3) \quad \text{pro } y \neq 0 \\
\mathcal{O} &\longmapsto (1,\ 1,\ 1) \\
(e_1,0) &\longmapsto ((e_1-e_2)(e_1-e_3),\ e_1-e_2,\ e_1-e_3) \\
(e_2,0) &\longmapsto (e_2-e_1,\ (e_2-e_1)(e_2-e_3),\ e_2-e_3) \\
(e_3,0) &\longmapsto (e_3-e_1,\ e_3-e_2,\ (e_3-e_1)(e_3-e_2))
\end{aligned}$$

je homomorfismus grup. Jádro ϕ je $2E(\mathbb{Q})$.

$P_i = (x_i, y_i) \qquad y_i \neq 0 \quad \text{pro } i = 1, 2, 3$

$$\phi(P_i) = (x_i - e_1,\ x_i - e_2,\ x_i - e_3)$$

$\in (\mathbb{Q}^\times)^2$ $\qquad$ $\in (\mathbb{Q}^\times)^2$

$$\phi(P_1) \cdot \phi(P_2) \cdot \phi(P_3) = \big((x_1-e_1)\cdot(x_2-e_1)\cdot(x_3-e_1),\ (x_1-e_2)(x_2-e_2)(x_3-e_2),$$
$$(x_1-e_3)(x_2-e_3)(x_3-e_3)\big) = (1,1,1)$$

$\in (\mathbb{Q}^\times)^2$

4) $\phi(P_1)\cdot\phi(P_2)\cdot\phi(P_3)^{-1} = \phi(P_3)\cdot\phi(-P_3) = \phi(P_1+P_2)$

$$\phi_1(P_1+P_2)\,\phi_2(P_1+P_2)\,\phi_3(P_1+P_2) = 1$$

$$\phi_1(P_1+P_2) = \phi_2(P_1+P_2)\,\phi_3(P_1+P_2) = \phi_2(P_1)\,\phi_2(P_2)\,\phi_3(P_1)\,\phi_3(P_2)$$

$$\phi_2(P_1)\,\phi_3(P_1) = \phi_1(P_1) \qquad \phi_1(P_1)\cdot\phi_1(P_2)$$

$$\phi_2(P_2)\,\phi_3(P_2) = \phi_1(P_2)$$

$$x_1 = \frac{u_1}{u_2}$$

$$y_1 = \frac{1}{u_2}$$

$$0 = u_1^2 + 2u_0u_2 - Au_2^2$$

$$u_0 = \frac{Au_2^2 - u_1^2}{2u_2}\cdot\frac{\left(\frac{1}{u_2}\right)^2}{\left(\frac{1}{u_2}\right)^2} = \frac{A - x_1^2}{2y_1}$$

$$x = u_0^2 - 2Bu_1u_2 \qquad u_1u_2 = \frac{x_1}{y_1^2}$$

$$x = \frac{(A-x_1^2)^2}{4y_1^2} - \frac{2Bx_1}{y_1^2} = \frac{A^2 - 2Ax_1^2 + x_1^4 - 8Bx_1}{4y_1^2}$$

$e_1 = -2,\ e_2 = 0,\ e_3 = 2$ $\qquad \infty \longmapsto (1,1,1)$

$(e_1, 0) \longmapsto (2, -2, -1)$

$(e_2, 0) \longmapsto (2, -1, -2)$ $\qquad E(\mathbb{Q})/2E(\mathbb{Q})$

$(e_3, 0) \longmapsto (1, 2, 2)$ $\qquad E(\mathbb{Q}) = T \oplus \mathbb{Z}^r$

$E(\mathbb{Q})/2E(\mathbb{Q}) = T/2T \oplus \mathbb{Z}_2^r$