Tvrzení Platí $v_p(t_1+t_2+t_3) \geq 5n$.

$t_1 = t_2 \Rightarrow P_1 = P_2$ $\qquad$ $s = at + b$

$$ax + by - 1 = 0$$
$$by = 1 - ax$$
$$y = -\frac{a}{b}x + \frac{1}{b}$$

$$-\frac{ay_1}{1-ax_1} = -\frac{a}{b} = \frac{3x_1^2 + A}{2y_1}$$

$$t_1 = \frac{x_1}{y_1}$$

$$-2ay_1^2 = (3x_1^2 + A)\cdot(1 - ax_1)$$

$$s_1 = \frac{1}{y_1}$$

$$-2ay_1^2 + 3ax_1^3 + Aax_1 = 3x_1^2 + A$$
$$ax_1^3 - Aax_1 - 2aB = 3x_1^2 + A$$
$$a = \frac{3x_1^2 + A}{x_1^3 - Ax_1 - 2B} = \frac{3x_1^2 + A}{y_1^2 - 2Ax_1 - 3B} = \frac{3t_1^2 + As_1^2}{1 - 2At_1s_1 - 3Bs_1^2}$$

Nechť

$$\mathcal{O}_p = \{x \in \mathbb{Q};\ v_p(x) \geq 0\}$$
$$\mathfrak{p} = \{x \in \mathbb{Q};\ v_p(x) > 0\} = p\mathcal{O}_p$$

Důsledek

Buď $n \in \mathbb{N}$ libovolné. Zobrazení

$$\lambda_n : E_n \longrightarrow \mathfrak{p}^n / \mathfrak{p}^{5n}$$

dané předpisem

$$(x, y) \longmapsto \frac{x}{y} \pmod{\mathfrak{p}^{5n}}$$
$$\infty \longmapsto 0 \pmod{\mathfrak{p}^{5n}}$$

je homomorfismus grup a jeho jádrem je $\bar{E}_{5n}$.

Důkaz: Nechť $P_1, P_2 \in \bar{E}_n$ jsou libovolné body. Chceme ukázat

$$\lambda_n(P_1) + \lambda_n(P_2) = \lambda_n(P_1 + P_2). \qquad (*)$$

Je-li některý z bodů P_1, P_2, P_1+P_2 roven ∞, pak $(*)$ zřejmě platí. Předpokládejme, že existují $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{Q}$ tak, že $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ a $P_3 = (x_3, y_3)$, kde $-P_3 = P_1 + P_2$. Podle předchozího důsledku $P_3 \in \bar{E}_n$ a platí

$$\begin{aligned}\lambda_n(P_1) + \lambda_n(P_2) - \lambda_n(P_1+P_2) &= \lambda_n(P_1) + \lambda_n(P_2) - \lambda_n(-P_3) \\ &= \frac{x_1}{y_1} + \frac{x_2}{y_2} - \left(-\frac{x_3}{y_3}\right) \pmod{p^5} \\ &= \frac{x_1}{y_1} + \frac{x_2}{y_2} + \frac{x_3}{y_3} \pmod{p^{5n}} \\ &= 0 \pmod{p^{5n}},\end{aligned}$$

neboť $v_p\left(\frac{x_1}{y_1} + \frac{x_2}{y_2} + \frac{x_3}{y_3}\right) \geq 5n$ podle předchozího tvrzení.

Jádrem tohoto homomorfismu je pak

$$\begin{aligned}\ker \lambda_n &= \{P \in \bar{E}_n,\ \lambda_n(P) = 0 \pmod{p^{5n}}\} \\ &= \{\infty\} \cup \{(x,y) \in E(\mathbb{Q}),\ v_p(x) < 0,\ v_p\left(\tfrac{x}{y}\right) \geq 5n\} = \bar{E}_{5n}.\end{aligned}$$

Tvrzení: Grupa $\bar{E}_1$ nemá torzi.

Důkaz: Buď $P \in \bar{E}_1$, $P \neq \infty$, bod řádu $m \in \mathbb{N}$, $m > 1$. Buď q libovolné prvočíslo dělící m. Pak $Q = \frac{m}{q} P$ je bod řádu q. Nechť $Q = (x,y)$ a nechť $n \in \mathbb{N}$ je takové, že $Q \in \bar{E}_n$, $Q \notin \bar{E}_{n+1}$, tj. $v_p\left(\frac{x}{y}\right) = n$.

$$q \cdot \frac{x}{y} \pmod{p^{5n}} = q\,\lambda_n(Q) = \lambda_n(qQ) = \lambda_n(\infty) = 0 \pmod{p^{5n}},$$

tedy

$$v_p\left(\frac{x}{y}\right) \geq \begin{cases} 5n, & \text{pokud } q \neq p \\ 5n-1, & \text{pokud } q = p, \end{cases}$$

což není možné.

Důkaz věty Lutz-Nagell:

Buď $P = (x, y) \in E(\mathbb{Q})$ bod konečného řádu. Na chvíli předpokládejme, že x nebo y není celé číslo. Pak musí existovat prvočíslo p tak, že $v_p(x) < 0$, tedy $P \in E_1$. Podle předchozího tvrzení však grupa E_1 neobsahuje body konečného řádu, spor. Tedy $x, y \in \mathbb{Z}$.

Nyní předpokládejme, že $y \neq 0$. Pak $2P = (x_2, y_2) \neq \infty$ je také bod konečného řádu, tedy $x_2, y_2 \in \mathbb{Z}$, přičemž

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}, \text{ tedy } y^2 \mid x^4 - 2Ax^2 - 8Bx + A^2.$$

Platí

$$4A^3 + 27B^2 = (3x^2 + 4A)\cdot(x^4 - 2Ax^2 - 8Bx + A^2) - (3x^3 - 5Ax - 27B)\underbrace{(x^3 + Ax + B)}_{y^2}$$

Protože y^2 dělí pravou stranu, musí dělit také levou.

Tvrzení: Nechť E je eliptická křivka daná rovnicí $y^2 = x^3 + Ax + B$, kde $A, B \in \mathbb{Z}$. Buď p liché prvočíslo a předpokládejme, že $p \nmid 4A^3 + 27B^2$. Pak zobrazení

$$\varphi_p : E(\mathbb{Q}) \longrightarrow E(\mathbb{Z}_p)$$

dané předpisem

$$(x : y : z) \longmapsto ([x]_p : [y]_p : [z]_p), \quad x, y, z \in \mathbb{Z}, \gcd(x, y, z) = 1$$

je homomorfismus grup. Navíc, jestli $P \in E(\mathbb{Q})$ bod konečného řádu a $\varphi_p(P) \stackrel{!}{=} \infty$, pak $P \stackrel{!}{=} \infty$.

Př. $y^2 = x^3 + 8$ nad $\mathbb{Q}$

$$4A^3 + 27B^2 = 27 \cdot 8^2 = 3^3 \cdot 2^6$$

$p = 5$ $\quad |E(\mathbb{Z}_5)| = 6 \quad \Rightarrow |E(\mathbb{Q})_{tors}| \mid 6$

$p = 13$ $\quad |E(\mathbb{Z}_{13})| = 16$

$$\Rightarrow |E(\mathbb{Q})_{tors}| \mid 16$$

$$\Rightarrow |E(\mathbb{Q})_{tors}| \mid 2$$

$$\Rightarrow E(\mathbb{Q})_{tors} = \{\infty, (-2,0)\}.$$

Věta (Mazur)
Nechť E je eliptická křivka definovaná nad $\mathbb{Q}$. Pak torzní podgrupa grupy $E(\mathbb{Q})$ je jedna z následujících grup:

$\mathbb{Z}_n$, kde $1 \leq n \leq 10$ nebo $n = 12$,
$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$, kde $1 \leq n \leq 4$.

G konečně generovaná abelovská grupa
$m \in \mathbb{N}$

Pak G/mG je konečná grupa.

$G \cong T \oplus \mathbb{Z}^r$, $r \geq 0, r \in \mathbb{Z}$, T je konečná grupa

$G/mG \cong T/mT \oplus \mathbb{Z}_m^r$

$m \in \mathbb{N}$

$\mathbb{R}/m\mathbb{R} \cong \{0\}$, ale $\mathbb{R}$ není konečně generovaná ab. grupa

Věta

Buď G komutativní grupa a předpokládejme, že podgrupa $2G$ má konečný index v G. Dále předpokládejme, že existuje zobrazení

$$h: G \longrightarrow \mathbb{R}_0^+,$$

které splňuje následující podmínky:

1. Pro každé reálné číslo M je množina

$$\{P \in G;\ h(P) \leq M\}$$

konečná.

2. Pro každé $P_0 \in G$ existuje konstanta $c_0 \in \mathbb{R}$ taková, že

$$h(P + P_0) \leq 2h(P) + c_0 \quad \text{pro všechna } P \in G.$$

3. Existuje konstanta $c \in \mathbb{R}$ taková, že

$$h(2P) \geq 4h(P) - c \quad \text{pro všechna } P \in G.$$

Pak je G konečně generovaná.

Pozn. Zobrazení h se nazývá výška

Důkaz. V každé třídě rozkladu G podle $2G$ zvolme jednoho reprezentanta. Protože $G/2G$ je těchto reprezentantů konečně mnoho, označme je $Q_1, Q_2, \dots, Q_n$. To znamená, že pro libovolné $P_0 \in G$ existuje, a to jediné $i_0 \in \{1, 2, \dots, n\}$ tak, že

$$P_0 - Q_{i_0} \in 2G,$$

tedy

$$P_0 - Q_{i_0} = 2P_1$$

pro vhodné $P_1 \in G$. Pro každé $i \in \{1, 2, \dots, n\}$ existuje c_i takové, že

$$h(P - Q_i) \leq 2h(P) + c_i \quad \text{pro všechna } P \in G.$$

Označme c' největší z těchto konstant. Označme c konstantu z podmínky 3. Pak

$$4h(P_1) \leq h(2P_1) + c = h(P_0 - Q_{i_0}) + c \leq 2h(P_0) + c' + c$$

Odtud

$$h(P_1) \leq \frac{1}{2}h(P_0) + \frac{c'+c}{4} = \frac{3}{4}h(P_0) - \frac{1}{4}\left(h(P_0) - (c'+c)\right).$$

Pokud $h(P_0) \geq c'+c$, pak $h(P_1) \leq \frac{3}{4}h(P_0)$.

$$\{P \in G;\ h(P) \leq c'+c\} = \{R_1, R_2, \dots, R_m\}$$

Pak G je generovaná množinou $\{Q_1, Q_2, \dots, Q_n\} \cup \{R_1, \dots, R_m\}$