Věta (Lutz-Nagell)
Buď E eliptická křivka daná rovnicí $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. Nechť $P = (x, y) \in E(\mathbb{Q})$ je bod konečného řádu. Pak $x, y \in \mathbb{Z}$. Pokud $y \neq 0$, pak

$$y^2 \mid 4A^3 + 27B^2.$$

$x \in \mathbb{Q} \setminus \mathbb{Z}$. Pak existuje prvočíslo p takové, že $v_p(x) < 0$.
Buď p libovolné pevně zvolené prvočíslo.
Budeme studovat body $(x, y) \in E(\mathbb{Q})$ splňující $v_p(x) < 0$.

Pro libovolné $n \in \mathbb{N}$ definujme

$$E_n = \{(x, y) \in E(\mathbb{Q}) ; v_p(x) < 0, v_p(x/y) \geq n\} \cup \{\infty\}$$

Ukážeme, že E_n je podgrupa grupy $E(\mathbb{Q})$.

$$v_p\left(-\frac{x}{y}\right) = v_p\left(\frac{x}{y}\right)$$

$$(x, y) \in E_n \Rightarrow (x, -y) \in E_n$$

Buďte $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E_n$ libovolné body.
Nechť

$$ax + by + c = 0$$

je rovnice přímky procházející body P_1 a P_2. Pokud $P_1 = P_2$, uvažme touhu procházející tímto bodem. Označme P_3 třetí bod ležící na této přímce a předpokládejme, že $P_3 \neq \infty$, tj. $P_3 = (x_3, y_3)$ pro vhodná $x_3, y_3 \in \mathbb{Q}$. A pokusme se odhadnout hodnotu $v_p\left(\frac{x_3}{y_3}\right)$.

Zavedeme substituci $t = \frac{x}{y}$ a $s = \frac{1}{y}$. Po vydělení rovnice $y^2 = x^3 + Ax + B$ číslem y^3

$$s = t^3 + At s^2 + B s^3$$

a po vydělení rovnice $ax + by + c = 0$ číslem y dostaneme

$$at + b + cs = 0.$$

Označme $t_i = \frac{x_i}{y_i}$ pro $i = 1, 2, 3$.

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

Chceme ukázat, že $c \neq 0$. Dokažme to sporem. Předpokládejme, že je nulové. Pak rovnice přímky procházející body P_1 a P_2 je tvaru

$$y = kx, \text{ kde } k = \frac{y_1}{x_1} \quad v_p(k) \leq -n$$

$$v_p(x_1) = -2r, \ r \in \mathbb{N} \Rightarrow v_p(y_1) = -3r \qquad r \geq n$$
$$\Rightarrow v_p(k) = -r$$

$$k^2 x^2 = x^3 + Ax + B$$
$$x^3 - k^2 x^2 + Ax + B = 0$$

Lemma Nechť $f = x^3 + ux^2 + vx + w \in \mathbb{Q}[x]$ je polynom splňující $v_p(w) \geq 0$, $v_p(v) \geq 0$ a $v_p(u) < 0$. Dále předpokládejme, že f se v $\mathbb{Q}[x]$ rozkládá na lin. činitele, tj. existují $x_1, x_2, x_3 \in \mathbb{Q}$ taková, že $f = (x - x_1)(x - x_2)(x - x_3)$. Pokud $v_p(x_1) = v_p(u)$, pak $v_p(x_2) \geq 0$ a $v_p(x_3) \geq 0$.

$$v_p(x_1) < 0$$

Platí

$$-W = x_1 x_2 x_3$$
$$V = x_1 x_2 + x_1 x_3 + x_2 x_3$$
$$-U = x_1 + x_2 + x_3.$$

Předpokládejme, že $v_p(x_2) < 0$. Pak $v_p(x_3) = v_p\left(\frac{-W}{x_1 x_2}\right) = v_p(W) - v_p(x_1) - v_p(x_2) > 0$.

Platí

$$v_p(x_1 x_2) = v_p(x_1) + v_p(x_2) < v_p(x_1) + v_p(x_3) = v_p(x_1 x_3)$$
$$v_p(x_1 x_2) = v_p(x_1) + v_p(x_2) < v_p(x_3) + v_p(x_2) = v_p(x_2 x_3).$$

Pak $v_p(V) = v_p(x_1 x_2) < 0$.

Zavedeme substituci $t = \frac{x}{y}$ a $s = \frac{1}{y}$. Po vydělení rovnice $y^2 = x^3 + Ax + B$ číslem y^3

$$s = t^3 + At s^2 + Bs^3$$

a po vydělení rovnice $ax + by + c = 0$ číslem y dostaneme

$$at + b + cs = 0.$$

Označme $t_i = \frac{x_i}{y_i}$ pro $i = 1, 2, 3$.

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

BÚNO můžeme předpokládat, že $c = -1$. Pak přímka určená body P_1 a P_2 je tvaru

$$s = at + b.$$

Spočtěme směrnici a. Pokud $t_1 \neq t_2$, pak

$$a = \frac{s_1 - s_2}{t_1 - t_2}$$

$$s_1 = t_1^3 + A t_1 s_1^2 + B s_1^3$$
$$s_2 = t_2^3 + A t_2 s_2^2 + B s_2^3$$

$$s_1 - s_2 = t_1^3 - t_2^3 + A t_1 s_1^2 - A t_2 s_2^2 + B s_1^3 - B s_2^3$$

$$= t_1^3 - t_2^3 + A t_1 s_1^2 - A t_1 s_2^2 + A t_1 s_2^2 - A t_2 s_2^2 + B s_1^3 - B s_2^3$$

$$s_1 - s_2 - A t_1 s_1^2 + A t_1 s_2^2 - B s_1^3 + B s_2^3 = (t_1 - t_2)(t_1^2 + t_1 t_2 + t_2^2 + A s_2^2)$$
$$(s_1 - s_2)(1 - A t_1 s_1 - A t_1 s_2 - B s_1^2 - B s_1 s_2 - B s_2^2) = (t_1 - t_2)(t_1^2 + t_1 t_2 + t_2^2 + A s_2^2)$$

$$\frac{s_1 - s_2}{t_1 - t_2} = \frac{t_1^2 + t_1 t_2 + t_2^2 + A s_2^2}{1 - A t_1 (s_1 + s_2) - B(s_1^2 + s_1 s_2 + s_2^2)} \quad |$$

Pokud $t_1 = t_2$, pak $s_1 = a t_1 + b = a t_2 + b = s_2$

$$s = t^3 + A t s^2 + B s^3$$
$$s'(t) = 3t^2 + 2A s' s t + A s^2 + 3B s^2 \cdot s'$$

$$s'(1 - 2Ast - 3Bs^2) = 3t^2 + As^2$$
$$s' = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2}$$

$$s'(t_1) = \frac{3t_1^2 + A s_1^2}{1 - 2A s_1 t_1 - 3B s_1^2}$$

$$v_p(t_i) \geq n \quad a \quad v_p(s_i) = v_p\left(\frac{1}{y_i}\right) = -v_p(y_i) \geq 3n \quad | \; n \in \mathbb{N}$$

$$v_p(y_i) \leq -3n$$

pro $i = 1, 2.$

platí i pro $t_1 = t_2$

$$a = \frac{t_2^2 + t_1 t_2 + t_1^2 + A s_2^2}{1 - A(s_1+s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)}$$

$$v_p\left(1 - A(s_1+s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)\right) = 0$$

$$v_p(1) = 0 < v_p\left(A(s_1+s_2)t_1\right)$$
$$v_p(1) < v_p\left(B(s_2^2 + s_1 s_2 + s_1^2)\right)$$

$$v_p\left(t_2^2 + t_1 t_2 + t_1^2 + A s_2^2\right) \geq 2n$$

$$\Rightarrow v_p(a) \geq 2n$$

$$v_p(b) = v_p(s_1 - a t_1) \geq \min\{\underbrace{v_p(s_1)}_{\geq 3n}, \underbrace{v_p(a)}_{\geq 2n} + \underbrace{v_p(t_1)}_{\geq n}\} \geq 3n$$

Dosadíme $s = at + b$ do rovnice $s = t^3 + A t s^2 + B s^3$

$$at + b = t^3 + At(at+b)^2 + B(at+b)^3$$

$$t^3 + Aa^2t^3 + 2Aabt^2 + Ab^2t + Ba^3t^3 + 3a^2bBt^2 + 3ab^2Bt + Bb^3 - at - b = 0$$

$$t^3(1 + Aa^2 + Ba^3) + t^2(2Aab + 3a^2bB) + t(Ab^2 + 3ab^2B - a) + Bb^3 - b = 0$$

$$t_1 + t_2 + t_3 = -\frac{2Aab + 3a^2bB}{1 + Aa^2 + Ba^3}$$

$$v_p(t_1 + t_2 + t_3) = v_p(2Aab + 3a^2bB) - \underbrace{v_p(1 + Aa^2 + Ba^3)}_{0}$$

$$v_p(2Aab + 3a^2bB) \geq \min\{\underbrace{v_p(2Aab)}_{\geq 5n}, \underbrace{v_p(3a^2bB)}_{\geq 7n}\} \geq 5n$$

Důsledek Platí $P_3 \in \bar{E}_n$.

Snadno se vidí, $v_p(t_3) \geq n$. Kdyby $v_p(t_3) < n$, $v_p(t_3) < v_p(t_1)$ a $v_p(t_3) < v_p(t_2)$, a tedy $v_p(t_1 t_2 + t_3) = v_p(t_3) < n$, spor.

Z důkazu předchozího tvrzení plyne, že

$$v_p(s_3) = v_p(at_3 + b) > 0, \text{ tedy}$$
$$v_p(y_3) = -v_p(s_3) < 0, \text{ proto } v_p(x_3) < 0, \text{ tedy } (x_3, y_3) \in E_n,$$

Nechť

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

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

$$\lambda_n : E_n \longrightarrow \mathfrak{p}^n/\mathfrak{p}^{\delta_n} \quad \text{dané předpisem}$$
$$(x, y) \longmapsto \frac{x}{y} \pmod{\mathfrak{p}^{\delta_n}}$$
$$\infty \longmapsto 0 \pmod{\mathfrak{p}^{\delta_n}}$$

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