Eliptické křivky definované nad $\mathbb{C}$ odpovídají mřížkám, přičemž mřížkou rozumíme podgrupu grupy $(\mathbb{C},+)$ tvaru

$$L = \{kw_1 + lw_2 ; k,l \in \mathbb{Z}\},$$

kde $w_1, w_2 \in \mathbb{C}$ lineárně nezávislá nad $\mathbb{R}$. Snadno se vidí, že tato čísla nejsou určena jednoznačně. V případě, že je daná křivka definovaná nad $\mathbb{R}$ lze tato čísla zvolit tak, aby jedno z nich bylo reálné. Toto reálné číslo je určeno jednoznačně až na znaménko.

Buď E eliptická křivka definovaná nad $\mathbb{R}$. Nechť

$$L = \{kw_1 + lw_2 ; k,l \in \mathbb{Z}\}$$

je příslušná mřížka, kde $w_1 \in \mathbb{R}$. Označme c počet komponent souvislosti křivky E. Pak

$$\Omega = c \cdot |w_1| = \begin{cases} 2|w_1|, & \text{pokud } E[2] \subseteq E(\mathbb{R}) \\ |w_1|, & \text{jinak.} \end{cases}$$

Šafarevičova - Tatova grupa

Máme následující exaktní posloupnost

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S_2 \longrightarrow Ш[2] \longrightarrow 0,$$

kde S_2 je 2-Selmerova grupa. Lze ukázat, že pro libovolné $n \in \mathbb{N}$ máme posloupnost

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S_n \longrightarrow Ш[n] \longrightarrow 0,$$

kde S_n je n-Selmerova grupa, kterou lze poměrně snadno spočítat.

Předpokládá se, že grupa Ш je vždy konečná (pro každou eliptickou křivku definovanou nad $\mathbb{Q}$), což znamená, že $Ш = Ш[n]$ pro vhodné n.

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

$$h(P) = h(x), \quad h(\infty) = 0,$$

kde

$$h\left(\frac{a}{b}\right) = \log \max\{|a|,|b|\} \quad \text{pro } (a,b)=1.$$

Definujeme zobrazení

$$\hat{h}: E(\mathbb{Q}) \longrightarrow \mathbb{R}_0^+ \quad \text{předpisem}$$

$$\hat{h}(P) = \frac{1}{2}\lim_{n\to\infty} \frac{1}{4^n} h(2^n P).$$

Lze ukázat, že existuje konstanta $c\in\mathbb{R}$ taková, že pro libovolný bod $P\in E(\mathbb{Q})$ platí

$$|h(2P) - 4h(P)| < c.$$

Platí

$$\sum_{i=1}^{n} \frac{1}{4^i}\left(h(2^i P) - 4h(2^{i-1}P)\right) = \frac{1}{4^n} h(2^n P) - h(P).$$

$$\lim_{n\to\infty} \frac{1}{4^n} h(2^n P) = h(P) + \sum_{i=1}^{\infty} \frac{1}{4^i}\left(h(2^i P) - 4h(2^{i-1}P)\right).$$

Řada konverguje absolutně, neboť

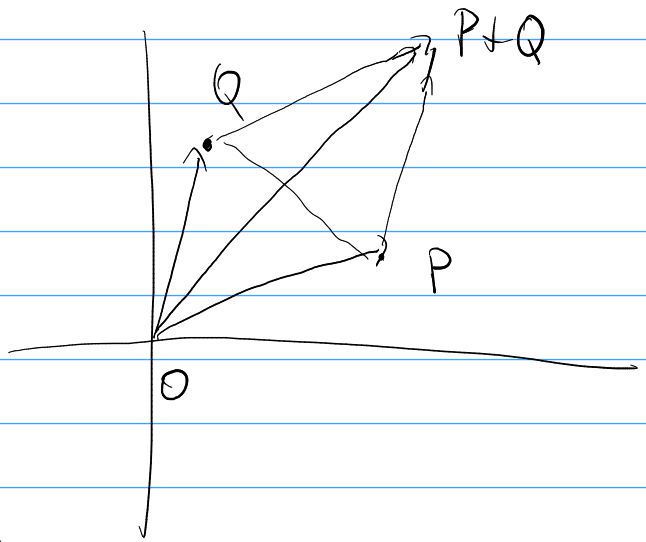
$$\sum_{i=1}^{\infty} \frac{1}{4^i} \left| h(2^i P) - 4h(2^{i-1}P) \right| \leq \sum_{i=1}^{\infty} \frac{c}{4^i} = \frac{c}{3}$$

Zobrazení $\hat{h}$ se nazývá kanonická (Néronova-Tateova) výška.

Tvrzení: Kanonická výška $\hat{h}$ má následující vlastnosti:

1. $\hat{h}(P) \geq 0$ pro každé $P \in E(\mathbb{Q})$.
2. Existuje konstanta c_0 taková, že $\left| \frac{1}{2} h(P) - \hat{h}(P) \right| \leq c_0$.
3. Pro libovolné c existuje pouze konečně mnoho bodů P splňujících $\hat{h}(P) \leq c$.
4. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ pro každé $P, Q \in E(\mathbb{Q})$.

$$\|P+Q\|^2 + \|P-Q\|^2 = 2\|P\|^2 + 2\|Q\|^2$$



5. $\hat{h}(mP) = m^2 \hat{h}(P)$ pro libovolné $m \in \mathbb{N}$
6. $\hat{h}(P) = 0$ právě tehdy, když P je bod konečného řádu.

$$\langle P, P \rangle = \hat{h}(2P) - 2\hat{h}(P) = 2\hat{h}(P)$$

$$\hat{h}(2P) + h_v(\infty) = 4\hat{h}(P)$$
$$\hat{h}(2P) = 4\hat{h}(P)$$

Nechť $P_1, P_2, \dots, P_r$ je báze $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

Definujme

$$Reg_E = \det(\langle P_i, P_j \rangle) \in \mathbb{R}.$$

Tato definice je zřejmě nezávislá na volbě báze.

$$E(\mathbb{Q}) \otimes \mathbb{R}$$