Nechť E je eliptická křivka zadaná rovnicí

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

kde $e_1, e_2, e_3 \in \mathbb{Z}$.

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 celá čísla a, b, c a vhodná racionální čísla u, v, w.

Odtud dostaneme

$$au^2 - bv^2 = e_2 - e_1, \quad au^2 - cw^2 = e_3 - e_1.$$

Tyto rovnice zadávají křivku $C_{a,b,c}$ v neznámých u, v, w.

K tomu, abychom popsali $E(\mathbb{Q})/2E(\mathbb{Q})$ potřebujeme znát $\mathrm{Im}\,\phi$.

Platí

$$(a,b,c) \in \mathrm{Im}\,\phi \iff C_{a,b,c} \text{ má racionální bod.}$$

Nutnou podmínkou pro to, aby křivka $C_{a,b,c}$ měla racionální bod, je, že má bod ve všech zúplněních tělesa racionálních čísel, tj. v $\mathbb{R}$ a v $\mathbb{Q}_p$ pro každé prvočíslo p.

p prvočíslo, $a \in \mathbb{Q}$

$$|a|_p = \begin{cases} 0 & a = 0 \\ p^{-v_p(a)} & a \neq 0 \end{cases}$$

Tato podmínka není obecně postačující, nicméně nám to dává lepší odhad na velikost obrazu, neboť $\mathrm{Im}\,\phi$ je podgrupou grupy

$S_2 = \{(a,b,c);\ C_{a,b,c}$ má bod ve všech zúplněních tělesa $\mathbb{Q}\}$.
Grupa S_2 se nazývá 2-Selmerova grupa. Faktorgrupa

$$Ш_2 = S_2 / \mathrm{Im}\,\phi$$

je 2-torzní podgrupa tzv. Šafarevičovy-Tateovy grupy.

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

$$y^2 = x(x-2p)(x+2p),$$

kde p je prvočíslo

Tvrzení Jestliže $p \equiv 9\ (16)$, pak křivka

$$C_{1,p,p}: \quad u^2 - pv^2 = 2p, \qquad u^2 - pw^2 = -2p$$

má bod v každém zúplnění $\mathbb{Q}$, ale nemá žádný racionální bod.

Lemma Předpokládejme, že x,y,z jsou nesoudělná přirozená čísla taková, že

$$x^2 + y^2 = z^2.$$

Pak jedno z čísel x,y je sudé. Předpokládejme, že je to x.
V takovém případě existují $m,n \in \mathbb{N}$ tak, že

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

Navíc, platí $(m,n) = 1$ a $m \not\equiv n \pmod 2$.

Dk. Kdyby $2 \mid z$, pak $4 \mid z^2 = (x+iy)(x-iy)$, a tedy $2 \mid (x+iy)$ nebo $2 \mid (x-iy)$, což znamená, že $2 \mid \gcd(x,y,z)$, spor. Čísla $x+iy$ a $x-iy$ jsou nesoudělná, proto existují $\varepsilon \in \{1,-i\}$ a $m,n \in \mathbb{N}$ tak, že

$$x+iy = \varepsilon(m+ni)^2 = \varepsilon(m^2-n^2+2mni).$$

$d=(m,n) \Rightarrow d \mid x, d \mid y, d \mid z$. $\gcd(x,y,z)=1 \Rightarrow d=1$.

$m \not\equiv n \not\equiv 1 \pmod 2 \Rightarrow 2 \mid y, 2 \mid z, 2 \mid x$, spor.

$$C_{1,p,p}: \quad u^2 - pv^2 = 2p, \quad u^2 - pw^2 = -2p$$

Dk. Tvrzení.
Tvrzení dokážeme sporem. Předpokládejme, že $C_{1,p,p}$ má racionální bod (u,v,w). Můžeme předpokládat, že $u>0, v>0, w>0$. Protože $v_p(pv^2) \not\equiv 1 \pmod 2$ a $v_p(u^2) \not\equiv 0 \pmod 2$, platí

$$1 = v_p(2p) = v_p(u^2 - pv^2) = v_p(pv^2),$$

tedy $v_p(v)=0$. Podobně $v_p(w)=0$. Platí

$$v_p(u^2) = v_p(p(2+v^2)) = \underbrace{v_p(p)}_{=1} + \underbrace{v_p(2+v^2)}_{\geq 0} \geq 1,$$

tedy $v_p(u)>0$. Pro libovolné prvočíslo $q \neq p$ platí

$$v_q(u) < 0 \iff v_q(v) < 0$$
$$v_q(u) < 0 \iff v_q(w) < 0,$$

přičemž, pokud $v_q(u)<0$, pak $v_q(u) = v_q(v) = v_q(w)$.

Můžeme předpokládat, že existují čísla $r,s,t,e \in \mathbb{N}$ tak, že

$$u = \frac{pr}{e}, \quad v = \frac{s}{e}, \quad w = \frac{t}{e},$$

splňují $(r,e)=1$, $(s,e)=1$, $(t,e)=1$.

$$C_{1|p|p}: \quad u^2 - pv^2 = 2p, \quad u^2 - pw^2 = -2p$$

Pak platí

$$pr^2 - s^2 = 2e^2, \quad pr^2 - t^2 = -2e^2.$$

Odečtením dostaneme

$$s^2 - t^2 = -4e^2,$$

tedy

$$s^2 + 4e^2 = t^2.$$

Kdyby $2|s$, pak $2|e$, spor s tím $(s,e)=1$. Čísla s, $2e$ a t jsou nesoudělná, proto existují $m,n \in \mathbb{N}$ taková

$$2e = 2mn, \quad s = m^2 - n^2, \quad t = m^2 + n^2.$$

Pak

$$pr^2 = 2e^2 + s^2 = 2m^2n^2 + m^4 - 2m^2n^2 + n^4 = m^4 + n^4.$$

Protože $m \not\equiv n \pmod 2$, je pr^2 liché číslo. Buď q libovolné prvočíslo dělící r. Čísla m a n jsou nesoudělná, proto alespoň jedno z nich není dělitelné q. Protože $m^4 + n^4 \equiv 0 \pmod q$ dostaneme, že ani jedno z nich není dělitelné q.

$$m^4 + n^4 \equiv 0 \pmod q$$

$$\left(\frac{m}{n}\right)^4 \equiv -1 \pmod q$$

To znamená, že $\left[\frac{m}{n}\right]_q$ je prvek řádu 8 v grupě $\mathbb{F}_q^\times$, tedy $8 \mid q-1$, neboli $q \equiv 1 \ (8)$. Proto $r \equiv 1 \ (8)$.
Odtud

$$r^2 \equiv 1 \ (16).$$

Pak
$m^4+n^4 = pr^2 \equiv 9 \ (16)$. Ale pro libovolné $a \in \mathbb{Z}$ platí $a^4 \equiv 0, 1 \ (16)$. Proto $m^4+n^4 \equiv 0, 1, 2$, tedy $pr^2 \neq m^4+n^4$.