The Tate-Shafarevich group of elliptic curves

Mia Lam

12 March 2026

1 Galois cohomology

Let G be a group and let A be a G-module. Define

$$H^0(G, A) = A^G = \{a \in A : \sigma(a) = a \text{ for all } \sigma \in G\}.$$

The 1-*cochains*, 1-*cocycles* and 1-*coboundaries* of A in G are

$$\begin{aligned} C^1(G, A) &= \{\text{maps } G \to A\} = \{(a_\sigma \in A)_{\sigma \in G}\}, \\ Z^1(G, A) &= \{(a_\sigma)_{\sigma \in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma \text{ for all } \sigma, \tau \in G\}, \\ B^1(G, A) &= \{(\sigma(b) - b)_{\sigma \in G} : b \in A\}. \end{aligned}$$

The *first Galois cohomology* of A in G is

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}.$$

Lemma. *A short exact sequence of* G*-modules*

$$0 \to A \to B \to C \to 0$$

gives rise to a long exact sequence of abelian groups

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to \cdots.$$

Proposition (Inflation-restriction sequence)**.** *Let* A *be a* G*-module and let* $H \lhd G$ *be a normal subgroup. There exists an exact sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A).$$

Let K be a perfect field. $G = \text{Gal}(\bar{K}/K)$ has the structure of a profinite (topological) group, and $\text{Gal}(\bar{K}/L)$ for L/K finite Galois is a basis for open subgroups of G. For $H^1(G, A)$ to be well-defined, we modify its definition by insisting that:

(1) All cochains $G \to A$ are continuous with respect to the discrete topology on A,

(2) The stabiliser of each $a \in A$ is an open subgroup of G.

In other words, A must be a *discrete* G*-module*. Then we have

$$H^1(\text{Gal}(\bar{K}/K), A) \cong \varinjlim_{L/K \text{ finite Galois}} H^1(\text{Gal}(L/K), A^{\text{Gal}(\bar{K}/L)}),$$

where the direct limit is with respect to the inflation maps.

Theorem (Hilbert's theorem 90). *Let* L/K *be a finite Galois extension. Then*

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0.$$

Proof. Let $G = \mathrm{Gal}(L/K)$, and let $(a_\sigma)_{\sigma\in G} \in Z^1(G, L^\times)$. Distinct automorphisms are linearly independent, so there exists $y \in L$ such that $x = \sum_{\tau\in G} a_\tau^{-1}\tau(y) \neq 0$. Then

$$\sigma(x) = \sum_{\tau\in G} \sigma(a_\tau)^{-1}(\sigma\tau)(y) = a_\sigma \sum_{\tau\in G} a_{\sigma\tau}^{-1}(\sigma\tau)(y) = a_\sigma x.$$

Then $a_\sigma = \sigma(x)/x$ for all $\sigma \in G$, and $(a_\sigma)_{\sigma\in G} \in B^1(G, L^\times)$. Thus $H^1(G, L^\times) = 0$. □

Corollary. $H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^\times) = 0$.

For $\mathrm{char}\, K \nmid n$, there is a short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \to \mu_n \to \bar{K}^\times \xrightarrow{x\mapsto x^n} \bar{K}^\times \to 0$$

and an induced long exact sequence

$$\bar{K}^\times \xrightarrow{x\mapsto x^n} \bar{K}^\times \to H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \to H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^\times) = 0,$$

so $H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^\times/(K^\times)^n$.

Notation. Hereon, write $H^1(K, -)$ to denote $H^1(\mathrm{Gal}(\bar{K}/K), -)$.

Let $\phi : E \to E'$ be an isogeny of elliptic curves over K. The short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

induces a long exact sequence

$$E(K) \xrightarrow{\phi} E'(K) \to H^1(K, E[\phi]) \to H^1(K, E) \xrightarrow{\phi_*} H^1(K, E').$$

We get a short exact sequence

$$0 \to \frac{E'(K)}{\phi E(K)} \to H^1(K, E[\phi]) \to H^1(K, E)[\phi_*] \to 0.$$

2 Homogeneous spaces

We now give a description of $H^1(K, E)$.

Definition (Principal homogeneous spaces)**.** Let E be an elliptic curve over K. A *torsor* or *principal homogeneous space* under E is a smooth projective curve C of genus one over K, equipped with a simply transitive action $C \times E \to E, (p, P) \mapsto p + P$.

Proposition. *Let* E/K *be an elliptic curve and let* C/K *be a homogeneous space under* E/K. *Fix* $p_0 \in C$ *and define* $\theta : E \to C$ *by* $\theta(P) = p_0 + P$. *Then* θ *is an isomorphism defined over* $K(p_0)$, *and* C/K *is a twist of* E/K.

An isomorphism between two E-torsors C and C' is a K-isomorphism of curves $\theta : C \to C'$ which is equivariant with respect to the action of E, i.e.

$$\theta(p + P) = \theta(p) + P$$

for all $p \in C$ and $P \in E$.

Definition (Weil-Châtelet group)**.** The *Weil-Châtelet group* $WC(E/K)$ is the set of isomorphism classes of homogeneous spaces under E/K.

The trivial class of $WC(E/K)$ is the isomorphism class containing E itself.

Proposition. *Let* C/K *be a homogeneous space for* E/K. *Then* C/K *is in the trivial class if and only if* $C(K)$ *is not the empty set.*

The Weil-Châtelet group has the structure of an abelian group: for any two E_0-torsors E_1 and E_2, there exists an E_0-torsor E_3 and a morphism $\phi : E_1 \times E_2 \to E_3$ defined over K such that $\phi(p + x_1, q + x_2) = \phi(x_1, x_2) + p + q$ whenever $x_1 \in E_1$, $x_2 \in E_2$ and $p, q \in E$. E_3 is unique up to isomorphism of E_0-torsors, and $[E_3] = [E_1] + [E_2]$ in $WC(E_0)$.

Theorem. *There is a natural bijection*

$$WC(E) \to H^1(K, E)$$

defined by $[C] \mapsto [(\sigma \mapsto \sigma \cdot x - x)]$, *where* x *is any point in* $C(\bar{K})$.

Proof. We first check that the map is well-defined. $\sigma \mapsto x^\sigma - x$ is a 1-cocycle since

$$(\sigma\tau) \cdot x - x = ((\sigma\tau) \cdot x - \tau \cdot x) + (\tau \cdot x - x) = \tau \cdot (\sigma \cdot x - x) + (\tau \cdot x - x).$$

Suppose $\theta : C \to C'$ is an isomorphism of E-torsors, and let $y \in C'(\bar{K})$. For $\sigma \in G = \mathrm{Gal}(\bar{K}/K)$,

$$\begin{aligned} \theta(\sigma \cdot x) - \theta(x) &= ((\theta(\sigma \cdot x) + (x - \sigma \cdot x)) - \theta(x)) + (\sigma \cdot x - x) \\ &= (\theta(\sigma \cdot x + (x - \sigma \cdot x)) - \theta(x)) + (\sigma \cdot x - x) \\ &= \sigma \cdot x - x. \end{aligned}$$

On the other hand, we also have

$$\theta(\sigma \cdot x) - \theta(x) = (\sigma \cdot y - y) + (\sigma \cdot (\theta(x) - y) - (\theta(x) - y)).$$

The 1-cocycles $(\sigma \mapsto \sigma \cdot y - y)$ and $(\sigma \mapsto \sigma \cdot x - x)$ differ by the 1-coboundary generated by the point $\theta(x) - y \in E(\bar{K})$ and they give the same cohomology class in $H^1(G, E(\bar{K}))$.

For injectivity, let C, C' be E-torsors with $x_0 \in C(\bar{K})$ and $y_0 \in C'(\bar{K})$ such that $(\sigma \mapsto \sigma \cdot x_0 - x_0)$ and $(\sigma \mapsto \sigma \cdot y_0 - y_0)$ are cohomologous in $H^1(G, E(\bar{K}))$, i.e. there is some

$p_0 \in E(\bar{K})$ such that for all $\sigma \in G$,

$$\sigma \cdot x_0 - x_0 = \sigma \cdot y_0 - y_0 + (\sigma \cdot p_0 - p_0).$$

Now consider the map

$$\begin{aligned} \theta : C &\to C', \\ x &\mapsto y_0 + (x - x_0) + p_0. \end{aligned}$$

Clearly, θ is a $\bar{K}$-isomorphism which is equivariant with respect to the action of E, and θ is defined over K since

$$\begin{aligned} \sigma \cdot \theta(x) &= \sigma \cdot y_0 + \sigma \cdot (x - x_0) + \sigma \cdot p_0 \\ &= y_0 + (\sigma \cdot x - x_0) + p_0 + ((\sigma \cdot y_0 - y_0) + \sigma \cdot p_0 - p_0 - (\sigma \cdot x_0 - x_0)) \\ &= \theta(\sigma \cdot x) \end{aligned}$$

and hence $\sigma \cdot \theta(x) = \theta(x) \in C'(\bar{K})$ for all $x \in C(K)$. Thus $[C] = [C']$ in $WC(E)$.

Finally, for surjectivity, let $(p_\sigma)_{\sigma \in G} \in Z^1(G, E(\bar{K}))$ be a 1-cocycle. The translation-by-p_σ maps T_σ for $\sigma \in G$ are $\bar{K}$-isomorphisms $E \times_K \bar{K} \to E \times_K \bar{K}$ satisfying the cocycle condition: with G acting on the isomorphism group of $E \times_K \bar{K}$ via conjugation, for $p \in E(\bar{K})$,

$$T_{\sigma\tau}(p) = p + p_{\sigma\tau} = p + \tau \cdot p_\sigma + p_\tau = \tau \cdot (T_\sigma(\tau^{-1} \cdot p)) + p_\tau = (T_\tau \circ (\tau \cdot T_\sigma))(p).$$

$(T_\sigma)_{\sigma \in G}$ gives a *descent datum* on $E \times_K \bar{K}$ and $E \times_K \bar{K} = C \times_K \bar{K}$ for some smooth projective curve C over K of genus one. In particular, there is a $\bar{K}$-isomorphism $\phi : E \to C$ such that

$$T_\sigma = \phi^{-1} \circ (\sigma \cdot \phi)$$

for all $\sigma \in G$. Hence define an action

$$\begin{aligned} E \times C &\to C, \\ (p, x) &\mapsto \phi(\phi^{-1}(x) + p). \end{aligned}$$

We claim that C is an E-torsor over K with its associated cohomology class in $H^1(G, E(\bar{K}))$ being $[(p_\sigma)_{\sigma \in G}]$. Indeed, we check the following:

- The action of E on C is simply transitive. For $x, y \in C$,

$$p + x = \phi(\phi^{-1}(x) + p) = y \iff p = \phi^{-1}(y) - \phi^{-1}(x).$$

- The action of E on C is defined over K. For $\sigma \in G$, $p \in E$, $x \in C$, $\phi \circ T_\sigma = \sigma \cdot \phi$ and

$$T_\sigma((\sigma \cdot \phi^{-1})(\sigma \cdot x))) = \phi^{-1}(\sigma \cdot x),$$

so we have

$$\begin{aligned} \sigma \cdot (p + x) &= \sigma \cdot (\phi(\phi^{-1}(x) + p)) \\ &= (\sigma \cdot \phi)((\sigma \cdot \phi^{-1})(\sigma \cdot x) + \sigma \cdot p) \\ &= (\phi \circ T_\sigma)((T_\sigma^{-1} \circ \phi^{-1})(\sigma \cdot x) + \sigma \cdot p) \\ &= (\sigma \cdot p) + (\sigma \cdot x). \end{aligned}$$

- C maps to the correct cohomology class. Let $x_0 = \phi(O_E) \in C$. Then

$$\sigma \cdot x_0 - x_0 = \sigma \cdot (\phi(O_E)) - \phi(O_E) = \phi(O_E + p_\sigma) - \phi(O_E) = p_\sigma$$

for all $\sigma \in G$.

□

3 Selmer and Tate-Shafarevich groups

Let K be a number field. For each place $v \in M_K$, fix an embedding $\bar{K} \subset \bar{K}_v$. Then $\mathrm{Gal}(\bar{K}_v, K_v) \subset \mathrm{Gal}(\bar{K}/K)$. We have the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{E'(K)}{\phi E(K)} & \longrightarrow & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi_*] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \dfrac{E'(K_v)}{\phi E(K_v)} & \longrightarrow & H^1(K_v, E[\phi]) & \longrightarrow & H^1(K_v, E)[\phi_*] & \longrightarrow & 0 \end{array}$$

Definition (Selmer and Tate-Shafarevich groups)**.** The ϕ-*Selmer group* $S^{(\phi)}(E/K)$ of E/K is the kernel of the map along the dashed line in the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{E'(K)}{\phi E(K)} & \longrightarrow & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi_*] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \searrow & \downarrow & & \\ 0 & \longrightarrow & \displaystyle\prod_v \dfrac{E'(K_v)}{\phi E(K_v)} & \longrightarrow & \displaystyle\prod_v H^1(K_v, E[\phi]) & \longrightarrow & \displaystyle\prod_v H^1(K_v, E)[\phi_*] & \longrightarrow & 0 \end{array}$$

The *Tate-Shafarevich group* of E/K is

$$Ш(E/K) = \ker\left(H^1(K, E) \to \prod_v H^1(K_v, E)\right).$$

$Ш(E/K)$ is the group of isomorphism classes of homogeneous spaces for E/K that are everywhere locally trivially, i.e. they possess a K_v-rational point for every $v \in M_K$. Non-trivial elements of $Ш(E/K)$ fail Hasse's *local-to-global principle*.

Theorem. *Let $\phi : E/K \to E'/K$ be an isogeny of elliptic curves. Then:*

(a) There is a short exact sequence

$$0 \to \frac{E'(K)}{\phi E(K)} \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi_*] \to 0.$$

(b) The Selmer group $S^{(\phi)}(E/K)$ is finite.

Remark. The Selmer group is effectively computable. It is conjectured that $|Ш(E/K)| < \infty$.

4 Descent by 2-isogeny

Let E/K and E'/K be elliptic curves given by $E : y^2 = x(x^2+ax+b)$ and $E' : y^2 = x(x^2+a'x+b')$ with $b(a^2-4b) \neq 0$ and $a' = -2a$, $b' = a^2 - 4b$. We have a pair of dual isogenies

$$\begin{aligned} \phi : E &\longrightarrow E' \\ (x,y) &\longmapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2} \right), \end{aligned}$$

and

$$\begin{aligned} \hat{\phi} : E' &\longrightarrow E \\ (x,y) &\longmapsto \left(\frac{1}{4}\left(\frac{y}{x}\right)^2, \frac{y(x^2-b')}{8x^2} \right). \end{aligned}$$

Then $E[\phi] = \{0, T\}$ for $T = (0,0) \in E(K)$, and $E'[\hat{\phi}] = \{0, T'\}$ for $T' = (0,0) \in E'(K)$.

Proposition. *There is a group homomorphism*

$$\begin{aligned} E'(K) &\longrightarrow K^*/(K^*)^2 \\ (x,y) &\longmapsto \begin{cases} x \mod (K^*)^2 & \text{if } x \neq 0 \\ b' \mod (K^*)^2 & \text{if } x = 0 \end{cases} \end{aligned}$$

with kernel $\phi E(K)$.

Lemma. $2^{\operatorname{rank} E(K)} = |\operatorname{Im} \alpha_E| \cdot |\operatorname{Im} \alpha_{E'}|/4$.

Proof. If $A \xrightarrow{f} B \xrightarrow{g} C$ are homomorphisms of abelian groups, there is an exact sequence

$$0 \to \ker(f) \to \ker(gf) \xrightarrow{f} \ker(g) \to \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(gf) \to \operatorname{coker}(g) \to 0.$$

Since $\hat{\phi}\phi = [2]_E$, we get an exact sequence

$$0 \to \underbrace{E(K)[\phi]}_{\cong \mathbb{Z}/2\mathbb{Z}} \to E(K)[2] \xrightarrow{\phi} \underbrace{E'(K)[\hat{\phi}]}_{\cong \mathbb{Z}/2\mathbb{Z}} \to \underbrace{\frac{E'(K)}{\phi E(K)}}_{\cong \operatorname{Im}(\alpha_{E'})} \xrightarrow{\hat{\phi}} \frac{E(K)}{2E(K)} \to \underbrace{\frac{E'(K)}{\hat{\phi}E'(K)}}_{\cong \operatorname{Im}(\alpha_E)} \to 0.$$

Then we have

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{Im} \alpha_E||\operatorname{Im} \alpha_{E'}|}{4}. \tag{1}$$

By Mordell-Weil, $E(K) \cong \Delta \times \mathbb{Z}^r$ for Δ a finite group and $r = \operatorname{rank} E(K)$. Then $E(K)/2E(K) \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r$ and $E(K)[2] \cong \Delta[2]$, where $\Delta/2\Delta$ and $\Delta[2]$ have the same order since Δ is finite. Thus

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r. \tag{2}$$

Combining (1) and (2) completes the proof. □

Lemma. *If* K *is a number field and* $a, b \in \mathcal{O}_K$, *then* $\operatorname{Im}(\alpha_E) \subset K(S,2)$, *where* $S = \{\mathfrak{p} : \mathfrak{p} \mid b\}$.

Lemma. *If* $b_1 b_2 = b$, *then* $b_1(K^*)^2 \in \mathrm{Im}(\alpha_E)$ *if and only if*

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$$

is soluble for $u, v, w \in K$ *not all zero.*

Examples. 1. Let $E : y^2 = x^3 - x$, so that $a = 0$ and $b = -1$. $\mathrm{Im}(\alpha_E) = \langle -1 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. For $E' : y^2 = x^3 + 4x$, $\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Check the solubility of the following equations:

$$\begin{aligned} b_1 = -1 &: \qquad w^2 = -u^4 - 4v^4 \\ b_1 = 2 &: \qquad w^2 = 2u^4 + 2v^4 \\ b_1 = -2 &: \qquad w^2 = -2u^4 - 2v^4. \end{aligned}$$

The first and the third are insoluble over $\mathbb{R}$ and the second has solution $(u, v, w) = (1, 1, 2)$, so $\mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. So $2^{\operatorname{rank} E(\mathbb{Q})} = 2 \cdot 2/4 = 1$ and $\operatorname{rank} E(\mathbb{Q}) = 0$.

2. Let $E : y^2 = x^3 + px$ for p prime with $p \equiv 5 \pmod 8$. For $b_1 = -1$, $w^2 = -u^4 - pv^4$ is insoluble over $\mathbb{R}$. Thus $\mathrm{Im}(\alpha_E) = \langle p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. For $E' : y^2 = x^3 - 4px$, $\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Note that $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^*)^2 = (-p)(\mathbb{Q}^*)^2$, so it suffices to check:

$$\begin{aligned} b_1 = 2 &: \qquad w^2 = 2u^4 - 2pv^4 \\ b_1 = -2 &: \qquad w^2 = -2u^4 + 2pv^4 \\ b_1 = p &: \qquad w^2 = pu^4 - 4v^4. \end{aligned}$$

Suppose the first is soluble, and wlog $u, v, w \in \mathbb{Z}$ with $\gcd(u, v) = 1$. If $p \mid u$, then $p \mid w$ and $p \mid v$, a contradiction. Thus $w^2 \equiv 2u^4 \not\equiv 0 \pmod p$, and

$$\left(\frac{2}{p}\right) = +1,$$

a contradiction since $p \equiv 5 \pmod 8$.

Likewise, the second has no solutions since

$$\left(\frac{-2}{p}\right) = -1.$$

The third equation we consider is

$$w^2 = pu^4 - 4v^4. \tag{$*$}$$

$$\operatorname{rank} E(\mathbb{Q}) = \begin{cases} 0 & (*) \text{ is insoluble over } \mathbb{Q} \\ 1 & (*) \text{ is soluble over } \mathbb{Q}. \end{cases}$$

$(*)$ is soluble over $\mathbb{Q}_p$ since

$$\left(\frac{-1}{p}\right) = +1,$$

which implies by Hensel's lemma that $-1 \in (\mathbb{Z}_p^*)^2$. $(*)$ is soluble over $\mathbb{Q}_2$ since $p-4 \equiv 1 \pmod 8$ (so by Hensel's lemma, $p-4 \in (\mathbb{Z}_2)^*$), and $(*)$ is soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$. We check solubility for $p \equiv 5 \pmod 8$:

p	u	v	w
5	1	1	1
13	1	1	3
29	1	1	5
37	5	3	151
53	1	1	7

It is conjectured that $\operatorname{rank} E(\mathbb{Q}) = 1$ for all $p \equiv 5 \pmod 8$.

Example. Let $E : y^2 = x^3 + 17x$. $\operatorname{Im}(\alpha_E) = \langle 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. For $E' : y^2 = x^3 - 68x$, $\operatorname{Im}(\alpha_{E'}) \subset \langle -1, 2, 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. For $b_1 = 2$, consider the equation

$$w^2 = 2u^4 - 34v^4.$$

Replacing w by $2w$ and dividing by 2 gives

$$C : 2w^2 = u^4 - 17v^4. \qquad (*)$$

Write

$$C(K) = \{(u, v, w) \in K^3 \setminus \{0\} \text{ satisfying } (*)\}/\sim,$$

where $(u, v, w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for all $\lambda \in K^*$.

$C(\mathbb{Q}_2) \neq \varnothing$ since $17 \in (\mathbb{Z}_2^*)^4$, $C(\mathbb{Q}_{17}) \neq \varnothing$ since $2 \in (\mathbb{Z}_{17}^*)^2$, and $C(\mathbb{R}) \neq \varnothing$ since $\sqrt{2} \in \mathbb{R}$. Thus $C(\mathbb{Q}_v) \neq \varnothing$ for all places v of $\mathbb{Q}$.

Suppose $(u, v, w) \in C(\mathbb{Q})$, and wlog $u, v, w \in \mathbb{Z}$ with $\gcd(u, v) = 1$ and $w > 0$. If $17 \mid w$, then $17 \mid u$ and $17 \mid v$, a contradiction. So if $p \mid w$, then $p \neq 17$ and

$$\left(\frac{17}{p}\right) = +1,$$

then if p is odd, by quadratic reciprocity,

$$\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right) = 1,$$

and for $p = 2$,

$$\left(\frac{2}{17}\right) = +1.$$

Thus

$$\left(\frac{w}{17}\right) = +1.$$

But $2w^2 \equiv u^4 \pmod{17}$ and thus $2 \in (\mathbb{F}_{17}^*)^4 = \{\pm 1, \pm 4\}$, a contradiction. Thus $C(\mathbb{Q}) = \varnothing$, i.e. C is a counterexample to the Hasse principle.