Rational points on abelian varieties

Karl Rubin

MSRI, January 17 2006

Abelian varieties

An *abelian variety* is a connected projective group variety.

One-dimensional abelian varieties are elliptic curves, which in characteristic different from 2 and 3 can be defined by Weierstrass equations

$$y^2 = x^3 + ax + b$$

with $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

Abelian varieties

The jacobian of a curve of genus g is an abelian variety of dimension g.

An abelian variety over $\mathbf{C}$ is a complex torus (but in dimension greater than one not every complex torus is an abelian variety).

Rational points on abelian varieties

If A is an abelian variety defined over a field k, the k-rational points $A(k)$ form a commutative group.

Basic Problem: *Given an abelian variety A over k, find $A(k)$.*

Mordell-Weil Theorem. *If k is a number field, then $A(k)$ is a finitely generated abelian group.*

Overview

We don't know how to compute $A(k)$ in general, so instead we study $A(k)/nA(k)$ for $n \in \mathbf{Z}^+$.

By the Mordell-Weil theorem,

$$A(k) \cong A(k)_{\text{tors}} \oplus \mathbf{Z}^r$$

for some $r \geq 0$. We call r the *rank* of $A(k)$. Then

$$A(k)/nA(k) \cong A(k)_{\text{tors}}/n(A(k)_{\text{tors}}) \oplus (\mathbf{Z}/n\mathbf{Z})^r.$$

Overview

$$A(k)/nA(k) \cong A(k)_{\mathsf{tors}}/n(A(k)_{\mathsf{tors}}) \oplus (\mathbf{Z}/n\mathbf{Z})^r.$$

In particular, if we know $A(k)/nA(k)$ and $A(k)_{\mathsf{tors}}$, then we can compute the rank r.

For example, if $n = p$ is prime then

$$\dim_{\mathbf{F}_p} A(k)/pA(k) = \dim_{\mathbf{F}_p} A(k)[p] + \mathsf{rank}(A(k)).$$

Overview

We don't know how to compute $A(k)/nA(k)$ in general either, so we will define an effectively computable *Selmer group* $S_n(A/k)$ containing $A(k)/nA(k)$.

The *Shafarevich-Tate group* $Ш(A/k)$ is the "error term" (so we hope it's small)

$$0 \to A(k)/nA(k) \to S_n(A/k) \to Ш(A/k)[n] \to 0$$

where $Ш(A/k)[n]$ is the n-torsion in $Ш(A/k)$. Unfortunately $Ш(A/k)$ is very mysterious. This is why computing $A(k)$, or $A(k)/nA(k)$, is so difficult.

Outline of talk

- Kummer theory on abelian varieties (first approximation to the Selmer group, and sketch of proof of the Mordell-Weil theorem)

- The Selmer group

- Principal homogeneous spaces and the Shafarevich-Tate group

Notation

Let k^{sep} be a separable closure of k and $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

If n is prime to the characteristic of k, let $A[n]$ denote the kernel of multiplication by n in $A(k^{\mathrm{sep}})$. Then $A[n] \cong (\mathbf{Z}/n\mathbf{Z})^{2\dim(A)}$.

We will abbreviate $H^1(k, A[n]) = H^1(G_k, A[n])$.

Kummer theory on abelian varieties

Suppose first that $A[n] \subset A(k)$. We define a Kummer map

$$A(k) \to \mathsf{Hom}(G_k, A[n])$$

as follows. For $x \in A(k)$,

- choose $y \in A(k^{\mathrm{sep}})$ such that $ny = x$,
- map $\sigma \in G_k$ to $y^\sigma - y \in A[n]$.

Since $A[n] \subset A(k)$, $y^\sigma - y$ is independent of the choice of y and the map $\sigma \mapsto y^\sigma - y$ is a homomorphism.

Kummer theory on abelian varieties

$$A(k) \to \mathrm{Hom}(G_k, A[n])$$

$$x \longmapsto (\sigma \mapsto (\tfrac{1}{n}x)^\sigma - \tfrac{1}{n}x)$$

This induces a well-defined injective homomorphism

$$A(k)/nA(k) \hookrightarrow \mathrm{Hom}(G_k, A[n])$$

that is *not* in general surjective.

If $A[n] \not\subset A(k)$ then the same map induces an injective Kummer map, which we denote by κ

$$A(k)/nA(k) \xrightarrow{\kappa} H^1(k, A[n]).$$

Kummer theory on abelian varieties

To prove the Mordell-Weil theorem, it is harmless to increase k. Thus without loss of generality we may assume that $A[n] \subset A(k)$. Then

$$\begin{array}{ccc} A(k)/nA(k) & \stackrel{\kappa}{\hookrightarrow} & \mathrm{Hom}(G_k, A[n]) \\ & & \downarrow \cong \\ & & \mathrm{Hom}(G_k, \mathbf{Z}/n\mathbf{Z})^{2\dim(A)}. \end{array}$$

But when k is a number field, $\mathrm{Hom}(G_k, \mathbf{Z}/n\mathbf{Z})$ is infinite, so this is still much too big. We will use "local constraints" to bound the image of κ.

Selmer groups: first approximation

From now on suppose that k is a number field, and let Σ be the finite set

$$\{\text{primes } v \text{ of } k : v \mid n \text{ or } A \text{ has bad reduction at } v\}.$$

Theorem. *If $x \in A(k)$, $y \in A(\bar{k})$, $ny = x$, and $v \notin \Sigma$, then $k(y)/k$ is unramified at v.*

Let k_Σ be the maximal extension of k unramified outside of Σ and archimedean primes.

Corollary. *If $x \in A(k)$, $y \in A(\bar{k})$, and $ny = x$, then $y \in A(k_\Sigma)$.*

Selmer groups: first approximation

$$\begin{array}{ccc} A(k)/nA(k) & \overset{\kappa}{\hookrightarrow} & \mathrm{Hom}(G_k, A[n]) \\ & \searrow & \uparrow \\ & & \mathrm{Hom}(\mathrm{Gal}(k_\Sigma/k), A[n]) \end{array}$$

By class field theory, $\mathrm{Hom}(\mathrm{Gal}(k_\Sigma/k), A[n])$ is finite. This proves:

Weak Mordell-Weil Theorem. *For every n, the group $A(k)/nA(k)$ is finite.*

$\mathrm{Hom}(\mathrm{Gal}(k_\Sigma/k), A[n])$ is our "first approximation" to the Selmer group.

Selmer groups: first approximation

Using the weak Mordell-Weil theorem for a single $n \geq 2$, and the canonical height, one deduces easily:

Mordell-Weil Theorem. *The group* $A(k)$ *is finitely generated.*

(If $x_1, \ldots, x_r \in A(k)$ generate $A(k)/nA(k)$, then the set of points in $A(k)$ of height at most max$\{\mathrm{ht}(x_i)\}$ generates $A(k)$.)

Example

Let $k = \mathbf{Q}$, and let A be the elliptic curve $y^2 = x^3 - x$. Take $n = 2$, so

$$A[2] = \{O, (0,0), (1,0), (-1,0)\} \subset A(\mathbf{Q}).$$

We have $\Sigma = \{2\}$, so the Kummer map gives an injection

$$\begin{aligned} A(\mathbf{Q})/2A(\mathbf{Q}) \hookrightarrow & \ \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}_\Sigma/\mathbf{Q}), A[2]) \\ & = \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}(i, \sqrt{2})/\mathbf{Q}), A[2]). \end{aligned}$$

Example

Since $A[2] \subset A(\mathbf{Q})$ and $\dim_{\mathbf{F}_2} A[2] = 2$, we have

$$\dim_{\mathbf{F}_2} A(\mathbf{Q})/2A(\mathbf{Q}) = \mathrm{rank}(A(\mathbf{Q})) + 2,$$
$$\dim_{\mathbf{F}_2} \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}(i,\sqrt{2})/\mathbf{Q}), A[2]) = 4.$$

Using

$$A(\mathbf{Q})/2A(\mathbf{Q}) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}(i,\sqrt{2})/\mathbf{Q}), A[2]).$$

we conclude that $\mathrm{rank}(A(\mathbf{Q})) \leq 2$.

In fact, $\mathrm{rank}(A(\mathbf{Q})) = 0$, so we would like to do better.

Selmer groups

For every place v of k we have

$$\begin{array}{ccccc} A(k)/nA(k) & \xrightarrow{\kappa} & H^1(k, A[n]) & & c \\ \downarrow & & \downarrow & & \downarrow \\ A(k_v)/nA(k_v) & \xrightarrow{\kappa_v} & H^1(k_v, A[n]) & & c_v \end{array}$$

Definition. The *Selmer group* $S_n = S_n(A/k)$ is the subgroup of $H^1(k, A[n])$

$$S_n := \{c \in H^1(k, A[n]) : c_v \in \mathrm{image}(\kappa_v) \text{ for every } v\}.$$

Then S_n contains the image of κ.

Selmer groups

S_n is finite, since

$$S_n \subset H^1(\mathsf{Gal}(k_\Sigma/k), A[n])$$

which is finite.

S_n is effectively computable.

"Effectively computable" is not the same as "easy."

Example

Back to our example $A : y^2 = x^3 - x$. We will now compute $S_2(A/\mathbf{Q})$.

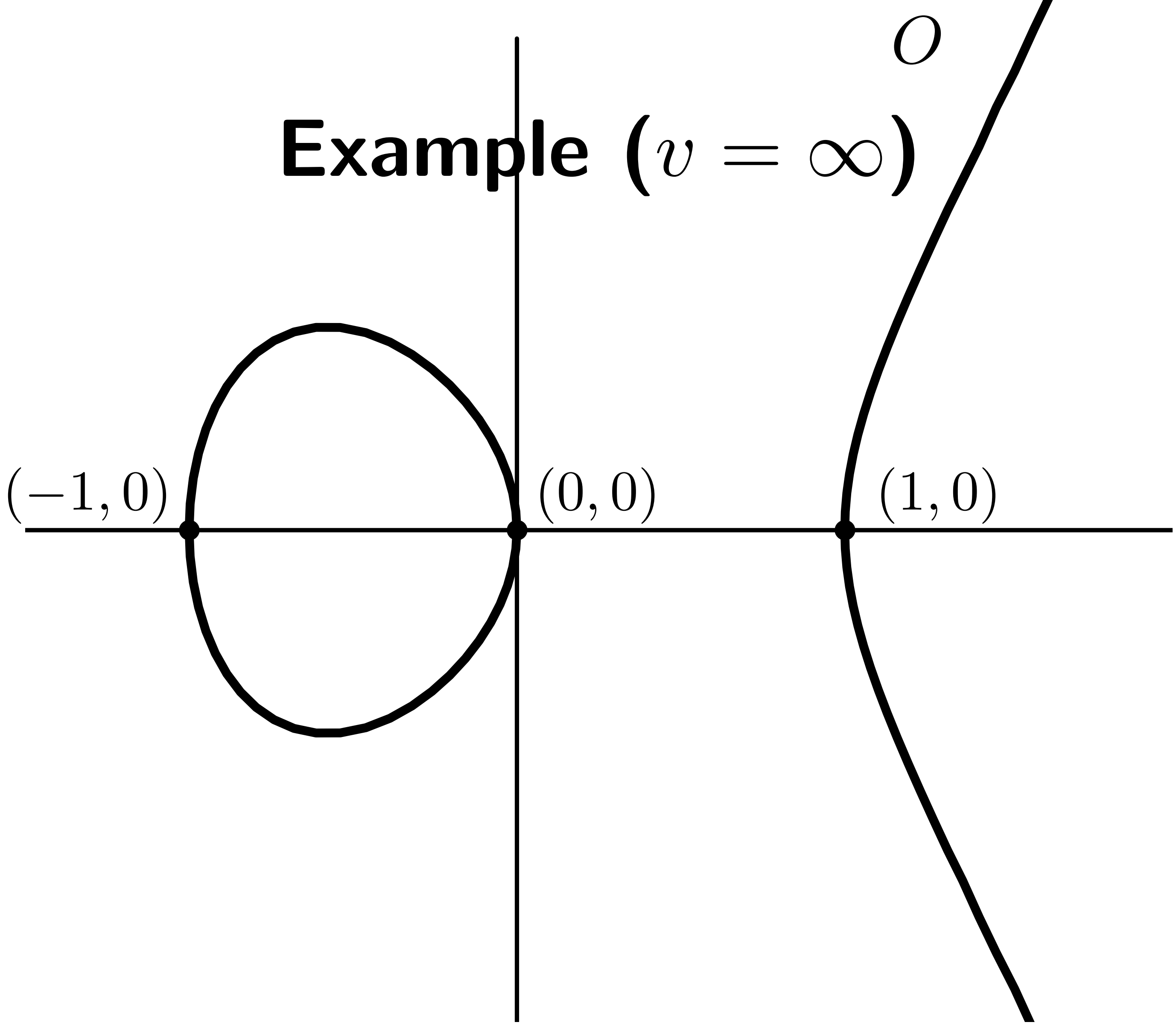
Suppose $c \in \mathrm{Hom}(G_k, A[2])$. If $c_v \in \mathrm{image}(\kappa_v)$ for every $v \neq 2, \infty$, then

$$c \in \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}(i, \sqrt{2})/\mathbf{Q}), A[2]).$$

Thus S_2 is contained in

$$\{c \in \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}(i, \sqrt{2})/\mathbf{Q}), A[2]) : \\ c_2 \in \mathrm{image}(\kappa_2), c_\infty \in \mathrm{image}(\kappa_\infty)\}.$$

Example ($v = \infty$)



$A(\mathbf{R})/2A(\mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z}$, and $(0, 0)$ represents the nontrivial coset.

Example ($v = \infty$)

$$A(\mathbf{R})/2A(\mathbf{R}) \xrightarrow{\kappa_\infty} \mathsf{Hom}(\mathsf{Gal}(\mathbf{C}/\mathbf{R}), A[2])$$

We need to compute $\kappa_\infty(x)$, where $x = (0,0)$.

Let $y = (i, i-1) \in A(\mathbf{Q}(i)) \subset A(\mathbf{C})$. Then $2y = x$, and if τ denotes complex conjugation

$$\kappa_\infty(x)(\tau) = y^\tau - y = (-1, 0).$$

Therefore if $c \in \mathsf{Hom}(G_{\mathbf{Q}}, A[2])$, then

$$c_\infty \in \mathrm{image}(\kappa_\infty) \Longrightarrow c(\tau) \in \langle(-1,0)\rangle.$$

Example ($v = 2$)

One can compute

$$A(\mathbf{Q}_2)/2A(\mathbf{Q}_2) \cong (\mathbf{Z}/2\mathbf{Z})^3$$

with generators

$$x_1 = (0,0), \quad x_2 = (1,0), \quad x_3 = (-4, 2\sqrt{-15}).$$

We compute $y_i \in \mathbf{Q}_2(\sqrt{-1}, \sqrt{2})$ with $2y_i = x_i$

$$y_1 = (\sqrt{-1}, 1 - \sqrt{-1}), \quad y_2 = (1 + \sqrt{2}, 2 + \sqrt{2}),$$
$$y_3 = \left(4\sqrt{-1} + \sqrt{-15}, 2(1 + \sqrt{-1})\sqrt{-31 - 8\sqrt{-1}\sqrt{-15}}\right).$$

Example ($v = 2$)

Let σ be the nontrivial element of $\mathrm{Gal}(\mathbf{Q}_2(\sqrt{-1}, \sqrt{2})/\mathbf{Q}_2(\sqrt{-1}))$.

Since $y_1, y_3 \in A(\mathbf{Q}_2(\sqrt{-1}))$, we have

$$\kappa_2(x_1)(\sigma) = y_1^\sigma - y_1 = O, \quad \kappa_2(x_3)(\sigma) = y_3^\sigma - y_3 = O.$$

On the other hand,

$$\kappa_2(x_2)(\sigma) = y_2^\sigma - y_2 = (0, 0).$$

Therefore if $c \in \mathrm{Hom}(G_{\mathbf{Q}}, A[2])$, then

$$c_2 \in \mathrm{image}(\kappa_2) \Longrightarrow c(\sigma) \in \langle (0, 0) \rangle.$$

Example

$$S_2 \subset \{c \in \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}(i,\sqrt{2})/\mathbf{Q}), A[2]) : \\ c(\sigma) \in \langle(0,0)\rangle, c(\tau) \in \langle(-1,0)\rangle\}.$$

Since $\mathrm{Gal}(\mathbf{Q}(i,\sqrt{2})/\mathbf{Q})$ is generated by σ and τ, this shows that $\dim_{\mathbf{F}_2} S_2 \le 2$.

We have

$$A(\mathbf{Q})_{\text{tors}}/2(A(\mathbf{Q})_{\text{tors}}) \subset A(\mathbf{Q})/2A(\mathbf{Q}) \subset S_2$$

and $\dim_{\mathbf{F}_2}(A(\mathbf{Q})_{\text{tors}}/2(A(\mathbf{Q})_{\text{tors}})) = 2$, so these inclusions are equalities and

$$A(\mathbf{Q}) = A(\mathbf{Q})_{\text{tors}} = A[2].$$

$S_n/\text{image}(\kappa)$

To understand $A(k)/nA(k)$, we need to understand both S_n and the cokernel of $A(k)/nA(k) \hookrightarrow S_n$.

Cohomology of the exact sequence

$$0 \longrightarrow A[n] \longrightarrow A(\bar{k}) \xrightarrow{\;n\;} A(\bar{k}) \longrightarrow 0$$

gives a short exact sequence

$$0 \to A(k)/nA(k) \to H^1(k, A[n]) \to H^1(k, A)[n] \to 0$$

where $H^1(k, A)$ is shorthand for $H^1(G_k, A(\bar{k}))$.

$S_n/\mathrm{image}(\kappa)$

$$
\begin{array}{ccccccccc}
0 & \to & A(k)/nA(k) & \longrightarrow & S_n & \longrightarrow & \lambda(S_n) & \longrightarrow & 0 \\
 & & \downarrow = & & \downarrow & & \downarrow & & \\
0 & \to & A(k)/nA(k) & \xrightarrow{\kappa} & H^1(k, A[n]) & \xrightarrow{\lambda} & H^1(k, A)[n] & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A(k_v)/nA(k_v) & \xrightarrow{\kappa_v} & H^1(k_v, A[n]) & \xrightarrow{\lambda_v} & H^1(k_v, A)[n] & \to & 0
\end{array}
$$

We have

$$S_n = \{c \in H^1(k, A[n]) : \lambda_v(c_v) = 0 \text{ for every } v\}$$

$S_n/\mathrm{image}(\kappa)$

$$\begin{array}{ccccccccc}
0 \to & A(k)/nA(k) & \longrightarrow & S_n & \longrightarrow & \lambda(S_n) & \longrightarrow & 0 \\
& \downarrow = & & \downarrow & & \downarrow & & \\
0 \to & A(k)/nA(k) & \xrightarrow{\kappa} & H^1(k, A[n]) & \xrightarrow{\lambda} & H^1(k, A)[n] & \to & 0 \\
& \downarrow & & \downarrow & & \downarrow & & \\
0 \to & A(k_v)/nA(k_v) & \xrightarrow{\kappa_v} & H^1(k_v, A[n]) & \xrightarrow{\lambda_v} & H^1(k_v, A)[n] & \to & 0
\end{array}$$

We have

$$S_n = \{c \in H^1(k, A[n]) : \lambda(c)_v = 0 \text{ for every } v\}$$

so

$$\lambda(S_n) = \{d \in H^1(k, A)[n] : d_v = 0 \text{ for every } v\}.$$

The Shafarevich-Tate group

Definition. The *Shafarevich-Tate group* $\text{Ш}(A/k) \subset H^1(k, A)$ is

$$\{d \in H^1(k, A) : d_v = 0 \text{ in } H^1(k_v, A) \text{ for every } v\}.$$

Then we have an exact sequence

$$0 \to A(k)/nA(k) \to S_n(A/k) \to \text{Ш}(A/k)[n] \to 0.$$

In particular $\text{Ш}(A/k)[n]$ is finite for every n.

Principal homogeneous spaces

Definition. A *principal homogeneous space* (or G_k-torsor) C for A/k is a variety C/k with a free transitive action of A. In other words, there are k-morphisms

$$A \times C \longrightarrow C, \qquad C \times C \longrightarrow A$$
$$(a, c) \longmapsto a \oplus c, \qquad (c, c') \longmapsto c \ominus c'$$

satisfying obvious properties like $(a \oplus c) \ominus c = a$, $(c \ominus c') \oplus c' = c$, etc.

Principal homogeneous spaces

Examples.

A is a principal homogeneous space for itself. We call this the trivial principal homogeneous space.

If C is a nonsingular curve of genus 1, then C is a PHS for its jacobian.

Principal homogeneous spaces

If C is a principal homogeneous space for A/k and C has a k-rational point x, then $a \mapsto a \oplus x$ is an isomorphism from A to C, defined over k.

Conversely, if C is isomorphic to A over k then C has k-rational points. Thus

$$C \cong_k A \iff C(k) \text{ is nonempty.}$$

A principal homogeneous space for A/k is *trivial* if it has k-rational points.

Principal homogeneous spaces

Theorem. *There is a natural bijection between $H^1(k, A)$ and the set of k-isomorphism classes of principal homogeneous spaces for A/k.*

Proof. If C is a principal homogeneous space and $x \in C(\bar{k})$, identify C with the cocycle

$$\sigma \mapsto x^\sigma \ominus x \in A(\bar{k}).$$

The isomorphism class of A itself is identified with $0 \in H^1(k, A)$.

Principal homogeneous spaces

Theorem. *There is a natural bijection between* $H^1(k, A)$ *and the set of* k*-isomorphism classes of principal homogeneous spaces for* A/k*.*

Recall that $Ш(A/k)$ is

$$\{d \in H^1(k, A) : d_v = 0 \text{ in } H^1(k_v, A) \text{ for every } v\}.$$

The theorem identifies $Ш(A/k)$ with the isomorphism classes of PHS's for A/k that are trivial as PHS's for A/k_v for every v (i.e., have rational points in every completion k_v).

Principal homogeneous spaces

The nonzero elements of $\text{Ш}(A/k)$ correspond to PHS's for A/k that have rational points in every completion k_v, but *no k-rational points*.

Thus $\text{Ш}(A/k)$ measures the failure of the Hasse principle for PHS's for A/k.

Examples

Let $A/\mathbf{Q}$ be the elliptic curve $y^2 = x^3 - x$. We showed that $S_2(A/\mathbf{Q}) = A(\mathbf{Q})/2A(\mathbf{Q})$, so $Ш(A/\mathbf{Q})[2] = 0$.

In fact, $Ш(A/\mathbf{Q}) = 0$.

Examples

Let C be the curve $3x^3 + 4y^3 + 5z^3 = 0$ over $\mathbf{Q}$. Then C is a PHS for its jacobian, which is the elliptic curve $A : x^3 + y^3 + 60z^3 = 0$. Selmer proved that C has no $\mathbf{Q}$-rational points and that C has $\mathbf{Q}_v$-rational points for every v, so C corresponds to a nonzero element of $Ш(A/\mathbf{Q})$.

Since C visibly has points over cubic extensions of $\mathbf{Q}$, it is not hard to show that C corresponds to an element of order 3 in $Ш(A/\mathbf{Q})$. In fact, in this case $Ш(A/\mathbf{Q}) \cong (\mathbf{Z}/3\mathbf{Z})^2$.

Shafarevich-Tate Conjecture

Shafarevich-Tate Conjecture. $Ш(A/k)$ *is finite.*

If $Ш(A/k)$ is finite, then there is an algorithm to compute $\mathrm{rank}(A(k))$:

- Compute S_2, S_3, S_5, S_7, ... This will give upper bounds for $\mathrm{rank}(A(k))$.
- While doing that, search for points in $A(k)$. This will give lower bounds for $\mathrm{rank}(A(k))$.

If the Shafarevich-Tate conjecture is true, then eventually these bounds will meet.

Shafarevich-Tate Conjecture

Suppose p is a prime, and define

$$S_{p^\infty}(A/k) = \varinjlim S_{p^m}(A/k) \subset H^1(k, A[p^\infty]).$$

Then

$$0 \to A(k) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to S_{p^\infty}(A/k) \to Ш(A/k)[p^\infty] \to 0.$$

If $Ш(A/k)$ is finite, then for every prime p,

$$\mathrm{corank}_{\mathbf{Z}_p} S_{p^\infty}(A/k) = \mathrm{rank}(A(k)).$$

Shafarevich-Tate Conjecture

The Shafarevich-Tate Conjecture is known for certain elliptic curves over $\mathbf{Q}$ with rank$(A(\mathbf{Q})) \leq 1$.

There are no elliptic curves over $\mathbf{Q}$ with rank$(A(\mathbf{Q})) > 1$ for which $Ш(A/\mathbf{Q})$ is known to be finite.

The Shafarevich-Tate Conjecture is known for certain abelian varieties over $\mathbf{Q}$ with rank$(A(\mathbf{Q})) \leq \dim(A)$. There are no abelian varieties over $\mathbf{Q}$ with rank$(A(\mathbf{Q})) > \dim(A)$ for which $Ш(A/\mathbf{Q})$ is known to be finite.