Tate-Shafarevich and Selmer groups of abelian varieties

Stefan van der Lugt

March 12, 2016

1 Notation

In these notes, almost all fields are perfect. Some of the theory can be generalized to arbitrary fields but I've chosen not to do so as all the fields we'll be working with later on are either number fields or (algebraic extensions of) finite fields. Important to notice is that any variety V over a field k is identified with its set of $\bar{k}$-rational points in the context of Galois cohomology. So, for example, we define for an abelian variety A over a perfect field k:

$$H^1(k, A) = H^1(\mathrm{Gal}(\bar{k}/k), A(\bar{k})).$$

Let A and A' be two abelian varieties over a perfect field K that have the same dimension. A K-morphism $A \to A'$ is an *isogeny* if it is a group homomorphism and $A(\bar{K}) \to A'(\bar{K})$ is surjective. We define $A[\phi]$ to be the kernel of $\phi : A(\bar{K}) \to A'(\bar{K})$, and $A(K)[\phi]$ is the kernel of $A(K) \to A'(K)$.

2 The Mordell-Weil group

Let K be a number field, and let A be an Abelian variety over K. We are interested in the abelian group of K-rational points $A(K)$. The Mordell-Weil theorem tells us that the structure of this group is not too complicated.

Theorem 2.1 (Mordell-Weil theorem)**.** *The group $A(K)$ is finitely generated.*

The Mordell-Weil group therefore has a decomposition

$$A(K) \cong \mathbb{Z}^r \oplus A(K)_{\mathrm{tors}}$$

where $A(K)_{\mathrm{tors}}$ is the torsion subgroup of $A(K)$. We call r the *rank* of $A(K)$. The torsion subgroup $A(K)_{\mathrm{tors}}$ is computable; in the case of elliptic curves the Nagell-Lutz theorem is often used. However, there is no known algorithm that will always return the rank of $A(K)$. There is, however, a candidate algorithm, but it is not certain yet that this algorithm will terminate in every case. It is conjectured that the Tate-Shafarevich group is finite, and if this conjecture is true the algorithm will always terminate.

As we will see later, it is possible to find an upper bound for the rank of $A(K)$ using Selmer groups.

The Mordell-Weil theorem implies the Weak Mordell-Weil Theorem:

Theorem 2.2. *For all $m \geq 1$ the quotient $A(K)/mA(K)$ is finite.*

Usually one proves the Mordell-Weil theorem by first proving the Weak Mordell-Weil theorem.

3 Group cohomology

Let G be a profinite group, and let A be a (discrete, right) G-module. That is, G acts on the abelian group A, and the action $A \times G \to A$ is continuous. We denote the action of $\sigma \in G$ on A by $a \mapsto a^\sigma$.

Example 3.1. Let $K \subset L$ be a Galois extension. Then L and L^* are $\mathrm{Gal}(L/K)$-modules.

Example 3.2. Let A be an Abelian variety over K. Then $A(L)$ is a $\mathrm{Gal}(L/K)$-module.

For every G-module A we define A^G to be the group of G-invariant elements of A. We obtain a functor $(-)^G$ from the category of G-modules to the category of abelian groups. This functor is left exact; we denote its right derived functors by $H^i(G,-)$. So for every exact sequence of G-modules $0 \to A \to B \to C \to 0$ there are natural homomorphisms $\delta : H^i(G,C) \to H^{i+1}(G,A)$ such that the sequence

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \xrightarrow{\delta} H^2(G,A) \to \dots$$

is exact.

Given an abelian variety A over a perfect field k we define

$$H^1(k,A) := H^1(\mathrm{Gal}(\bar{k}/k), A(\bar{k})).$$

Example 3.3. Let $\phi : A \to A'$ be an isogeny of abelian varieties over a perfect field k. Then ϕ is surjective on $\bar{k}$-rational points, but not necessarily on k-rational points. Taking Galois cohomology of the exact sequence of $\mathrm{Gal}(\bar{k}/k)$-modules $0 \to A[\phi] \to A \xrightarrow{\phi} A' \to 0$ yields an exact sequence

$$0 \to A(k)[\phi] \to A(k) \xrightarrow{\phi} A'(k) \to H^1(k, A[\phi]) \to H^1(k,A) \xrightarrow{\phi} H^1(k,A') \to \dots.$$

The size of the kernel of $H^1(k,A[\phi]) \to H^1(k,A)$ measures the failure of $A(K) \to A'(K)$ to be surjective.

For our purposes it is useful to give an explicit definition for the first cohomology groups. If A is a G-module, we let $C^1(G,M)$ be the group of (continuous) maps $G \to A$. We then define the group of *1-cocycles* $Z^1(G,M) \subset C^1(G,M)$ to be the subgroup of maps $\xi : G \to A$ that satisfy

$$\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)$$

for all $\sigma, \tau \in G$. A *1-coboundary* is a map $G \to A$ of the form $\sigma \mapsto a^\sigma - a$ for some $a \in A$; they form a subgroup $B^1(G,A) \subset Z^1(G,A)$. We then have:

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

If the action of G on A is trivial, we have

$$H^1(G,A) = \mathrm{Hom}_{\mathrm{cont}}(G,A).$$

Let $H \subset G$ be a subgroup. If $\xi : G \to A$ is a 1-cocycle, then its restriction to H is a 1-cocycle, and we obtain a *restriction homomorphism*

$$\mathrm{Res} : H^1(G,M) \to H^1(H,M).$$

Suppose, moreover, that $H \subset G$ is normal. Then the G-module structure on H induces a G/H-module structure on A^H. Every 1-cocycle $\xi : G/H \to A^H$ induces a 1-cocycle $G \to G/H \to A^H \subset A$, and we obtain an *inflation homomorphism*

$$\mathrm{Inf} : H^1(G/H, A^H) \to H^1(G,A).$$

Proposition 3.4. *The sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A)$$

is exact.

Another useful theorem we will need later on is the following.

Theorem 3.5 (Hilbert's Theorem 90)**.** *Let L/K be a Galois extension with Galois group G. Then*

$$H^1(G, L^\times) = 1.$$

For our purposes, it is convenient to generalize the cohomology groups to the terrain of non-abelian G-modules. Unfortunately, as we're not working with abelian categories, we cannot use right derived functors to define the higher cohomology groups anymore. However, by simply generalizing the explicit description of the first cohomology group of (abelian) G-modules, it is still possible to define the first cohomology *set* of any group M on which G acts. A *1-cocycle* $\xi : G \to M$ is a (continuous) map that satisfies $\xi(\sigma\tau) = \xi(\sigma)^\tau \xi(\tau)$ for all $\sigma, \tau \in G$; they form a set $Z^1(G, M)$. Two 1-cocycles $\xi, \zeta \in Z^1(G, M)$ are *cohomologous* if there exists some $m \in M$ such that $m^\sigma \xi(\sigma) = \zeta(\sigma)m$ for all $\sigma \in G$. This defines an equivalence relation on $Z^1(G, M)$, and we define $H^1(G, M)$ to be the set of equivalence classes. This is a pointed set, of which the distinguished element is the class of the trivial 1-cocycle $\sigma \mapsto 1$.

3.1 Kummer theory

Another nice application of Galois cohomology is the following.

Let K be a field and n a positive integer that is not divisible by the characteristic of K. Suppose, moreover, that K contains a primitive nth root of unity (and therefore contains all nth roots of unity of $\bar{K}$). Let $\mu_n \subset K$ denote the cyclic group of nth roots of unity. Let L/K be a Galois extension, and let $G = \mathrm{Gal}(L/K)$ be its Galois group. We have an exact sequence of G-modules

$$1 \to \mu_n \to L^\times \xrightarrow{n} (L^\times)^n \to 1,$$

where $L^\times \xrightarrow{n} (L^\times)^n$ is the nth power map. Taking Galois cohomology then yields an exact sequence

$$1 \to \mu_n \to K^\times \xrightarrow{n} (L^\times)^n \cap K^\times \to H^1(G, \mu_n) \to H^1(G, L^\times) \to \dots$$

and by Hilbert 90 the group $H^1(G, L^\times)$ is trivial. Moreover the action of G on μ_n is trivial. We therefore obtain a natural isomorphism

$$\frac{(L^\times)^n \cap K^\times}{(K^\times)^n} \simeq \mathrm{Hom}_{\mathrm{cont}}(G, \mu_n).$$

Given an element $\phi \in \mathrm{Hom}_{\mathrm{cont}}(G, \mu_n)$, the kernel $\ker \phi$ is an open normal subgroup, and therefore defines a Galois extension K'/K in L with Galois group $\mathrm{Gal}(K'/K) \simeq \mathrm{im}\, \phi$. If ϕ and ϕ' generate the same cyclic subgroup of $\mathrm{Hom}_{\mathrm{cont}}(G, \mu_n)$ then their kernels agree, so they induce the same cyclic extension of K. We therefore obtain a well-defined map

$$\{\text{cyclic subgroups of } \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L/K), \mu_n)\} \to \{\text{cyclic extensions of degree } d \mid n \text{ of } K \text{ in } L\}.$$

This map has an inverse: given a cyclic extension K'/K in L of degree $d|n$, we fix an embedding $\mathrm{Gal}(K'/K) \to \mu_n$, which induces a homomorphism $\mathrm{Gal}(L/K) \to \mu_n$, and this generates a cyclic subgroup of $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L/K), \mu_n)$ that does not depend on any of the choices we've made.

4 Twists

Let k be a perfect field, and let V be a smooth projective variety over k. We denote by $\mathrm{Isom}(V)$ the group of $\bar{k}$-isomorphisms from V to itself, and by $\mathrm{Isom}_k(V)$ the subgroup of isomorphisms defined over k.[1] A *twist* of V/k is a smooth projective k-variety V' that is isomorphic to V over $\bar{k}$. Two twists of V/k are *equivalent* if they are isomorphic over k. We define $\mathrm{Twist}(V/k)$ to be the set of twists of V/k modulo equivalence. The set $\mathrm{Twist}(V/k)$ is a pointed set: its distinguished element is the class of V/k.

There exists a map of pointed sets

$$\mathrm{Twist}(V/k) \to H^1(k, \mathrm{Isom}(V))$$

defined as follows. Suppose that V' is a twist of V/k. Choose a $\bar{k}$-isomorphism $\phi : V' \to V$, and define a map $\xi : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Isom}(V)$ by setting $\xi(\sigma) = \phi^\sigma \phi^{-1}$. This is a 1-cocycle, and its cohomology class depends only on the k-isomorphism class of V', which implies that the above map is well-defined.

[1] Normally we would write $\mathrm{Aut}(V)$ for the group of automorphisms of a variety V. However, in the context of abelian varieties, the group $\mathrm{Aut}(A)$ has another meaning, namely the group of automorphisms of A that respect the group structure on A.

Theorem 4.1. *The map*

$$\mathrm{Twist}(V/k) \to H^1(k, \mathrm{Isom}(V))$$

is a bijection.

For a proof of this theorem, see [1, X.2.2]. The theorem given there assumes that V is a curve, but its proof carries over without issue to the more general case that was stated here.

5 Principal homogeneous spaces

Let A/k be an abelian variety. A *principal homogeneous space for* A/k is a smooth variety V/k together with a k-morphism $V \times A \to V$ that induces a transitive and free group action $V(\bar{k}) \times A(\bar{k}) \to V(\bar{k})$. Notice that A acts on itself and therefore is a principal homogeneous space for A/k. Two principal homogeneous V and V' are *equivalent* if there exists a k-isomorphism $V \to V'$ that is compatible with the A-action. The set of equivalence classes of principal homogeneous spaces is called the *Weil-Châtelet group for* A/k and denoted by $\mathrm{WC}(A/k)$. Notice that $\mathrm{WC}(A/k)$ is, a priori, just a pointed set and not a group. Its distinguished element, the *trivial class*, is the equivalence class of the trivial principal homogeneous space A.

Proposition 5.1. *Let V/k be a homogeneous space for A/k. Then V is in the trivial class if and only if $V(k) \neq \emptyset$.*

Proof. If V is in the trivial class then there exists a k-isomorphism $V \to A$. As A has a k-rational point we immediately find that V has a k-rational point. Conversely, suppose that $V(k) \neq \emptyset$. Let $p \in V(k)$ be a point, and consider the morphism $A \to V$ given by $P \mapsto p + P$. One can check that this is an isomorphism defined over k, and therefore V lies in the trivial class. □

The following theorem can be used to define a group structure on $\mathrm{WC}(A/k)$.

Theorem 5.2 ([1, X.3.2])**.** *Let A/k be an abelian variety. There is a natural bijection*

$$\mathrm{WC}(A/k) \to H^1(k, A) = H^1(\mathrm{Gal}(\bar{k}/k), A(\bar{k}))$$

defined as follows:

Let V/k be a principal homogeneous space for A/k, and let $p_0 \in V(\bar{k})$ be any point. Then

$$\{V/k\} \mapsto \{\sigma \mapsto p_0^\sigma - p_0\},$$

where for any two points p, q in $V(\bar{k})$ the difference $p - q$ is defined to be the unique $P \in A(\bar{k})$ such that $q + (p - q) = p$.

6 The Selmer group

Suppose that we have an abelian variety A over a number field K, and we wish to compute $A(K)/nA(K)$ for some integer $n \geq 1$. Or, more generally, we consider an isogeny $\phi : A \to A'$ of abelian varieties over K, and we want to compute $A'(K)/\phi(A(K))$.

We have an exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \to A[\phi] \to A \xrightarrow{\phi} A' \to 0.$$

From the long exact sequence of Galois cohomology

$$0 \to A(K)[\phi] \to A(K) \xrightarrow{\phi} A'(K) \to H^1(K, A[\phi]) \to H^1(K, A) \xrightarrow{\phi} H^1(K, A'),$$

we can extract a short exact sequence

$$0 \to A'(K)/\phi(A(K)) \to H^1(K, A[\phi]) \to H^1(K, A)[\phi] \to 0.$$

Unfortunately, the group $H^1(K, A[\phi])$ is not finite, in general. Moreover, there is no known effective method to decide for every element of $H^1(K, A[\phi])$ whether or not its image in $H^1(K, A)$ is trivial.

The first issue can be circumvented by replacing $H^1(K, A[\phi])$ with a finite and computable subgroup. For every place v of K, we fix an extension of v to $\bar{K}$, which fixes inclusions $\bar{K} \subset \bar{K}_v$ and $\mathrm{Gal}(\bar{K}_v/K_v) \subset \mathrm{Gal}(\bar{K}/K)$. By repeating the above argument we find exact sequences

$$0 \to A'(K_v)/\phi(A(K_v)) \to H^1(K_v, A[\phi]) \to H^1(K_v, A)[\phi] \to 0.$$

Moreover, the inclusions $\mathrm{Gal}(\bar{K}_v/K_v) \subset \mathrm{Gal}(\bar{K}/K)$ and $A(\bar{K}) \subset A(\bar{K}_v)$ give restriction maps res_v on cohomology (and they do not depend on any choices!), and we obtain a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A'(K)/\phi(A(K)) & \longrightarrow & H^1(K, A[\phi]) & \longrightarrow & H^1(K, A)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \\
0 & \longrightarrow & \prod_v A'(K_v)/\phi(A(K_v)) & \longrightarrow & \prod_v H^1(K_v, A[\phi]) & \longrightarrow & \prod_v H^1(K_v, A)[\phi] & \longrightarrow & 0.
\end{array}$$

We now define the *ϕ-Selmer group* of A/K by

$$\mathrm{Sel}^\phi(A/K) = \ker\left(H^1(K, A[\phi]) \to \prod_v H^1(K_v, A)\right).$$

The *Tate-Shafarevich group* of A/K is the group

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

The above diagram now induces a short exact sequence

$$0 \to A'(K)/\phi(A(K)) \to \mathrm{Sel}^\phi(A/K) \to Ш(A/K)[\phi] \to 0.$$

Theorem 6.1. *The Selmer group $\mathrm{Sel}^\phi(A/K)$ is finite and computable (in theory).*

An immediate consequence of this theorem is the weak Mordell-Weil theorem.

Corollary 6.2. *The group $A'(K)/\phi(A(K))$ is finite.*

Moreover, the following corollary shows that the m-torsion part of the Tate-Shafarevich group is finite for every integer $m \geq 1$.

Corollary 6.3. *The group $Ш(A/K)[\phi]$ is finite.*

The Tate-Shafarevich group $Ш(A/K)$ has the following interpretation. It is a subgroup of $H^1(K, A)$, so its elements are (equivalence classes of) principal homogeneous spaces for A/K. Such a principal homogeneous space V/K maps to zero in $\prod_v H^1(A, K_v)$ if and only if it has a K_v-rational point for every place v of K. So the non-trivial elements of $Ш(A/K)$ correspond to principal homogeneous spaces V for A/K such that $V(K)$ is empty, but $V(K_v)$ is non-empty for every place v of K. So the size of $Ш(A/K)$ measures the failure of the Hasse principle[2] for principal homogeneous spaces for A/K.

7 Computing a Selmer group

Let A be an abelian variety over a number field K, and suppose that the torsion subgroup of $A(K)$ is non-trivial. This section gives a method to compute a Selmer group for A in order to give an upper bound for the rank of A.

Fix a non-trivial subgroup $\Phi \subset A(K)_{\mathrm{tors}}$. Then there exists (up to a unique isomorphism) a unique abelian variety $A' = A/\Phi$ and a unique isogeny $A \to A'$ with kernel $A(K)$. Let S be the (smallest) set containing the following places of K:

[2]The *Hasse principle* for quadratic forms is the fact that a quadratic form over a number field K has a non-trivial K-rational solution if and only if it has a non-trivial K_v-rational solution for all places v of K.

- the infinite places;
- the finite places dividing $\deg \phi = \#\Phi$;
- the finite places where A (and/or A')[3] has bad reduction.

Let K_S be the maximal abelian extension of K having exponent dividing that of $A[\phi]$ that is unramified outside S. Then one can show that $\mathrm{Sel}^\phi(A/K)$ is contained in the image of the inflation map (equivalently, in the kernel of the restriction map) in the following exact sequence

$$0 \to H^1(\mathrm{Gal}(K_S/K), A[\phi]) \to H^1(\mathrm{Gal}(\bar{K}/K), A[\phi]) \to H^1(\mathrm{Gal}(\bar{K}/K_S), A[\phi]).$$

Moreover, as $A[\phi] \subset A(K)$ is trivial as a $\mathrm{Gal}(\bar{K}/K)$-module, the above H^1s can be replaced by Homs.

Now given an element

$$\xi \in \mathrm{Hom}(\mathrm{Gal}(K_S/K), A[\phi]) = H^1(\mathrm{Gal}(K_S/K), A[\phi]) \subset H^1(\mathrm{Gal}(\bar{K}/K), A[\phi]),$$

we can compute its image under the map

$$H^1(\mathrm{Gal}(\bar{K}/K), A[\phi]) \to H^1(\mathrm{Gal}(\bar{K}/K), A) = \mathrm{WC}(A/K).$$

The image of ξ in $\mathrm{WC}(A/K)$ is represented by a principal homogeneous space V_ξ for A over K. Now ξ lies in $\mathrm{Sel}^\phi(A/K)$ if and only if $V_\xi(K_v) \neq \emptyset$ for all $v \in S$. For finite primes this can be done by reducing modulo powers of these primes and using Hensel's lemma if a solution modulo these powers is found, and one can determine in a finite amount of time whether or not V_ξ has a K_v-rational point. This allows us to compute the Selmer group in a finite amount of time.

Now suppose that we have computed the Selmer group. Consider again the exact sequence

$$0 \to A'(K)/\phi(A(K)) \to \mathrm{Sel}^\phi(A/K) \to Ш(A/K)[\phi] \to 0.$$

In order to find generators for $A'(K)/\phi(A(K))$, we can try to find elements of the kernel of the map $\mathrm{Sel}^\phi(A/K) \to Ш(A/K)[\phi]$. An element $\xi \in \mathrm{Sel}^\phi(A/K)$ is in this kernel if and only if the corresponding principal homogeneous space V_ξ has a K-rational point. Unfortunately, there is no known general algorithm that determines for any principal homogeneous space V_ξ if $V_\xi(K)$ is non-empty. However, if we are able to determine the kernel somehow, then we can lift the elements in this kernel to elements of $A'(K)/\phi(A(K))$.

Suppose that we are able to use this method to compute generators for $A'(K)/\phi(A(K))$, and also generators for $A(K)/\hat{\phi}(A'(K))$ using the dual isogeny $\hat{\phi}$. Let $m = \deg \phi$. Then using the exact sequence

$$0 \to \frac{A'(K)[\hat{\phi}]}{\phi(A(K)[m])} \to \frac{A'(K)}{\phi(A(K))} \xrightarrow{\hat{\phi}} \frac{A(K)}{mA(K)} \to \frac{A(K)}{\hat{\phi}(A'(K))} \to 0$$

we can compute generators for $A(K)/mA(K)$.

8 Example: descent via 2-isogeny

Consider the following elliptic curve over $\mathbb{Q}$:

$$E : y^2 = x^3 + 17x.$$

One can compute (for example, by reducing modulo 3 and 5):

$$E(\mathbb{Q})_{\mathrm{tors}} = E(\mathbb{Q})[2] = \{O, T = (0,0)\}.$$

We therefore immediately see that O and T represent two distinct elements of $E(\mathbb{Q})/2E(\mathbb{Q})$.

Let $\phi : E \to E'$ be the isogeny with kernel $\{O, T\}$. The elliptic curve E' is given by

$$E' : y^2 = x^3 - 68x$$

[3] isogeneous abelian varieties have good reduction at the same primes

and the isogeny ϕ is given by

$$\phi(x,y) = \left(\frac{x^2+17}{x}, \frac{x^2y-17y}{x^2}\right).$$

We consider the exact sequence

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

Now let us compute the middle term of this exact sequence.

Step 1: computing S and $\mathbb{Q}_S$. The field $\mathbb{Q}$ has only one archimedean place, which we will denote by ∞. The degree of ϕ is 2. The discriminant of E is $314432 = -2^6 \cdot 17^3$, so E has bad reduction at 2 and 17 and good reduction at the other finite primes. We therefore set

$$S = \{2, 17, \infty\}.$$

Let $\mathbb{Q}_S/\mathbb{Q}$ be the maximal abelian extension of exponent 2 that is unramified outside S. Then this extension is the composite of a finite number of quadratic extensions, and we quickly find that

$$\mathbb{Q}_S = \mathbb{Q}(i, \sqrt{2}, \sqrt{17}).$$

Step 2: computing the cohomology group $H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), E[\phi])$. The group $E[\phi] = \{O, T\}$ is defined over $\mathbb{Q}$, so it is trivial as a $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$-module, and there is a natural isomorphism of $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$-modules $E[\phi] \cong \{\pm 1\}$, which induces a natural isomorphism

$$H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), E[\phi]) \cong H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), \{\pm 1\}).$$

Consider the exact sequence of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules

$$1 \to \{\pm 1\} \to \bar{\mathbb{Q}}^{\times} \xrightarrow{2} \bar{\mathbb{Q}}^{\times} \to 1.$$

Taking cohomology of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules, and restricting to cohomology of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_S)$-modules yields a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathbb{Q}^{\times} & \xrightarrow{2} & \mathbb{Q}^{\times} & \longrightarrow & H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \{\pm 1\}) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathbb{Q}_S^{\times} & \xrightarrow{2} & \mathbb{Q}_S^{\times} & \longrightarrow & H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_S), \{\pm 1\}) \longrightarrow 1
\end{array}$$

(here the rightmost terms are trivial by Hilbert's theorem 90). The kernel of the rightmost vertical map is $H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), \{\pm 1\})$ by inflation-restriction, and a diagram chase reveals a natural isomorphism

$$H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), \{\pm 1\}) \cong \ker(\mathbb{Q}^{\times}/\mathbb{Q}^{\times 2} \to \mathbb{Q}_S^{\times}/\mathbb{Q}_S^{\times 2}) = \langle -1, 2, 17\rangle \subset \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}.$$

So we find that $H^1(\mathrm{Gal}(\mathbb{Q}_S, \mathbb{Q}), E[\phi])$ has order 8.

Step 3: computing the Selmer group. To see which elements of $H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), E[\phi])$ lie in the Selmer group, we need to compute the corresponding principal homogeneous spaces in $\mathrm{WC}(E/\mathbb{Q})$ and check if they have a $\mathbb{Q}_v$-rational point for every $v \in S$.

Let $\xi_d \in H^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), E[\phi])$ correspond to $d \in \langle -1, 2, 17\rangle \subset \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ under the natural isomorphism we found earlier. One can compute that the class in $\mathrm{WC}(E/K)$ induced by ξ_d is represented by the curve $C_d \subset \mathbb{P}^3$ given by the equations

$$C_d : X_0X_3 = X_1^2 \quad \text{and} \quad d^2X_0^2 = dX_2^2 + 68X_3^2.$$

If $K/\mathbb{Q}$ is any extension, we easily verify that $C_d(K) \neq \emptyset$ if and only if

$$d^2 = du^2 + 68v^4 \text{ has a } K\text{-rational solution or } -17d \text{ is a square in } K.$$

One easily verifies that $-17d$ is a square in $\mathbb{Q}_2$, $\mathbb{Q}_{17}$ and in $\mathbb{R}$ if and only if $d = -17 \in \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$. In this case C_d even has a $\mathbb{Q}$-rational point. Let us consider some more cases.

- $d = -1$: $-17d = 17$ is a square in $\mathbb{Q}_2$ and $\mathbb{R}$, so $C_{-1}(\mathbb{Q}_2)$ and $C_{-1}(\mathbb{R})$ are non-empty, but 17 is not a square in $\mathbb{Q}_{17}$. We have to check whether or not the equation $1 = -u^2 + 68v^4$ has a solution in $\mathbb{Q}_{17}$. Setting $u = 4$ and $v = 0$ gives a solution modulo 17, and using Hensel's lemma we can lift this to a solution in $\mathbb{Q}_{17}$. So we conclude that $C_{-1}(\mathbb{Q}_v) \neq \emptyset$ for all $v \in S$.
- $d = -34$: $-17d = 2 \cdot 17^2$ is a square in $\mathbb{R}$ and in $\mathbb{Q}_{17}$ (2 is a quadratic residue modulo 17), so $C_{-34}(\mathbb{R})$ and $C_{-34}(\mathbb{Q}_{17})$ are non-empty. Let's try to solve the equation $(-34)^2 = -34u^2 + 68v^4$ in $\mathbb{Q}_2$. Using Hensel's lemma, one can show that the solution $v = 1$ to $v^4 \equiv 17 \bmod 8$ lifts to a solution of $v^4 = 17$ in $\mathbb{Q}_2$. Setting $u = 0$ and $v \in \mathbb{Q}_2$ with $v^4 = 17$ we obtain a $\mathbb{Q}_2$-rational point on C_{-34}.

The Selmer group $\mathrm{Sel}^\phi(E/\mathbb{Q}) \subset H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), E[\phi])$ corresponds to a subgroup of $\langle -1, 2, 17\rangle \subset \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ containing -17, -1 and -34, so it must correspond to the full subgroup $\langle -1, 2, 17\rangle$. We find that

$$\mathrm{Sel}^\phi(E/\mathbb{Q}) = H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), E[\phi]),$$

so the ϕ-Selmer group of $E/\mathbb{Q}$ has order 8.

Consider again the exact sequence

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathrm{Sel}^\phi(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

We wish to determine which part of $\mathrm{Sel}^\phi(E/\mathbb{Q}) \cong \langle -1, 2, 17\rangle$ comes from $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and which part comes from $Ш(E/\mathbb{Q})[\phi]$. We already know that C_{-17} has a rational point, so -17 comes from the left hand side. We claim that -17 is the only non-trivial element of $\mathrm{Sel}^\phi(E/\mathbb{Q})$ coming from $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$. We can prove this by showing that the principal homogeneous spaces corresponding to other elements of $\mathrm{Sel}^\phi(E/\mathbb{Q})$ have no $\mathbb{Q}$-rational points.

- $d = \pm 2$: clearly $-17d$ is not a square in $\mathbb{Q}$. Suppose that $4 = \mp 2u^2 + 68v^4$ has a $\mathbb{Q}$-rational solution. Write $u = r/t$ and $v = s/t$ with $r, s, t \in \mathbb{Z}$ and $\gcd(r, s, t) = 1$. Then we can rewrite the given equation to
$$\pm r^2 t^2 = 34s^4 - 2t^4.$$
Let q be a prime dividing t. Then also $q \mid s$, and therefore $q \nmid r$. Let v_q denote the q-adic valuation on $\mathbb{Z}$. Taking the q-adic valuation of the above equation and applying the triangle inequality yields
$$2v_q(t) = 2v_q(r) + 2v_q(t) \geq \min(v_q(34) + 4v_q(s), v_q(2) + 4v_q(t)),$$
with equality if $v_q(34) + 4v_q(s) \neq v_q(2) + 4v_q(t)$. As $2v_q(t) < v_q(2) + 4v_q(t)$, we find that
$$2v_q(t) = v_q(34) + 4v_q(s).$$
We therefore see that $q \neq 2, 17$, and that $v_q(t) = 2v_q(s)$. In particular we see that $v_q(t)$ is even for every prime q, and we may therefore assume that t is a square. Write $t = a^2$. Rewriting the above equation yields
$$\pm r^2 a^4 = 34s^4 - 2a^8,$$
and we have $\gcd(a, r, s) = 1$ and $17 \nmid a$. Let q be a prime dividing r. Then as $\gcd(a, r, s) = 1$ we see that a, s and 17 are nonzero modulo q, and $17s^4 \equiv a^8 \bmod q$. Therefore 17 is a quadratic residue modulo q, and by quadratic reciprocity we also find that q is a quadratic residue modulo 17. Also 2 is a quadratic residue modulo 17, so we see that r is a quadratic residue modulo 17. As we have
$$\pm r^2 a^4 \equiv -2a^8 \bmod 17$$
and ± 1, r^2 and a^4 are all non-zero quartic residues modulo 17, we find that 2 is a quartic residue modulo 17. But one can easily verify by hand that 2 is not a quartic residue modulo 17, so this yields a contradiction. We conclude that $C_{\pm 2}(\mathbb{Q}) = \emptyset$.
- $d = -1$: a proof for this case can be found in Silverman [1, X.6.5].

We therefore see that $-1, \pm 2 \in \langle -1, 2, 17\rangle \cong \mathrm{Sel}^\phi(E/\mathbb{Q})$ do not lie in the kernel of $\mathrm{Sel}^\phi(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi]$, and therefore we must conclude the following:

$$\begin{aligned} \#\mathrm{Sel}^\phi(E/\mathbb{Q}) &= 8 \\ \#E(\mathbb{Q})/2E(\mathbb{Q}) &= 2 \\ \#Ш(E/\mathbb{Q})[\phi] &= 4. \end{aligned}$$

Similarly, the dual isogeny $\hat{\phi} : E' \to E$ has kernel $\{O', T' = (0,0)\}$, and the group $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ has order 2 and is generated by T'. We consider the exact sequence

$$\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \xrightarrow{\hat{\phi}} E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0.$$

The first homomorphism is zero, and therefore the second one is an isomorphism, and we find that $E(\mathbb{Q})/2E(\mathbb{Q})$ has order 2 and is generated by T.

9 Computability of $A(K)/mA(K)$

We know that for every integer $m \geq 1$ the Selmer group $\mathrm{Sel}^m(A/K)$ is effectively computable. However, it is in general not easy to compute which part comes from the Mordell-Weil group and which part comes from the Tate-Shafarevich group. Still, for every $n \geq 1$ we can also effectively compute the m^n-Selmer group of A/K, and we get a commutative diagram

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/m^3A(K) & \longrightarrow & \mathrm{Sel}^{m^3}(A/K) & \longrightarrow & Ш(A/K)[m^3] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/m^2A(K) & \longrightarrow & \mathrm{Sel}^{m^2}(A/K) & \longrightarrow & Ш(A/K)[m^2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/mA(K) & \longrightarrow & \mathrm{Sel}^{m}(A/K) & \longrightarrow & Ш(A/K)[m] & \longrightarrow & 0.
\end{array}$$

For $n \geq 1$ we let the *relative Selmer groups* $\mathrm{Sel}^{(m,n)}(A/K)$ denote the image of $\mathrm{Sel}^{m^n}(A/K)$ in $\mathrm{Sel}^m(A/K)$. Chasing through the above diagram then yields an exact sequence

$$0 \to A(K)/mA(K) \to \mathrm{Sel}^{(m,n)}(A/K) \to m^{n-1}Ш(A/K)[m^n] \to 0.$$

The relative Selmer groups give rise to a decreasing sequence of subgroups of $\mathrm{Sel}^m(A/K)$, all containing $A(K)/mA(K)$:

$$\mathrm{Sel}^m(A/K) = \mathrm{Sel}^{(m,1)}(A/K) \supset \mathrm{Sel}^{(m,2)}(A/K) \supset \mathrm{Sel}^{(m,3)}(A/K) \supset \dots.$$

One might hope that for n large enough this sequence stabilizes at $A(K)/mA(K)$. This happens precisely when $m^{n-1}Ш(A/K)[m^n] = 0$, or, equivalently, when $Ш(A/K)[m^n] = Ш(A/K)[m^{n-1}]$. Unfortunately, this might never happen. More precisely, it could occur that $Ш(A/K)$ has an element that is infinitely m-divisible. There is, however, the following conjecture, which implies that such elements cannot exist.

Conjecture 9.1. The Tate-Shafarevich group $Ш(A/K)$ is finite.

Suppose, from now on, that this conjecture is true. Then the above sequence stabilizes at $A(K)/mA(K)$ at some point. However, while we can compute the elements in the sequence one at a time, we generally cannot tell yet if our sequence has stabilized at any given point, as we haven't been able to compute $A(K)/mA(K)$ and $Ш(A/K)$ yet.

On the other hand, we have an increasing sequence of subgroups of $\mathrm{Sel}^m(A/K)$ defined as follows. Given an integer $r \geq 0$ we can effectively compute the set of points in $A(K)$ that have *height* $\leq r$. We can then compute the subgroup of $A(K)/mA(K)$ they generate, and let the image of this subgroup in $\mathrm{Sel}^m(A/K)$ be denoted by $T_{(m,r)}$. We obtain an increasing sequence

$$T_{(m,1)} \subset T_{(m,2)} \subset T_{(m,3)} \subset \dots.$$

As $A(K)/mA(K)$ is finite, this sequence stabilizes at $A(K)/mA(K)$ too. So for r and n large enough, we find that

$$T_{(m,r)} = \mathrm{Sel}^{(m,n)}(A/K).$$

When this occurs we have finally found the group $A(K)/mA(K)$.

References

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2nd edition, 2009

[2] Bjorn Poonen, *The Selmer group, the Shafarevich-Tate group, and the Weak Mordell-Weil Theorem*, found at http://math.univ-lyon1.fr/~roblot/ihp/weakmw.pdf