

Finding points on elliptic curves: Very explicit methods

Álvaro Lozano Robledo

November 3, 2003

1 Introduction

Some number theorists would say that Number Theory is the study of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This is just a *fancy* way of saying that number theory is the study of solutions of polynomial equations in \mathbb{Z} (or \mathbb{Q}). How much is known? Let's see:

- *Polynomials in one variable*: If $\frac{p}{q} \in \mathbb{Q}$ is a solution of:

$$a_0X^n + a_1X^{n+1} + \dots + a_n = 0$$

then p divides a_n and q divides a_0 . So this case is easy.

- *Linear equations in two variables*: $ax + by = d$; this was solved two thousand years ago, by Euclid, etc. We just need to find the gcd of a and b .
- *Quadratic equations in two variables*: $ax^2 + bxy + cy^2 = d$; solvable by parametrization of the curve (this is, projection into $\mathbb{P}^1(\mathbb{Q})$).
- *Cubic equations in two variables*: *NO IDEA!*, no general procedure is known.

2 Elliptic Curves

Definition 1. *An elliptic curve over a field K is a non-singular projective scheme of dimension 1 (a curve) and genus 1, together with a point defined over K , the origin O .*

Having said this formal definition, we forget about it right away. For the following we consider a rather naive definition of elliptic curve. For us an elliptic curve over K will be any non-singular cubic curve

$$E: f(x, y, z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + jyz^2 + kz^3 = 0, \quad (1)$$

with coefficients in K , and we require the existence of (at least) a point in E , which we call the origin, or O .

Remark: A curve $C: f(x, y, z) = 0$ is singular at a point $P \in C$ if and only if

$$\partial f / \partial x(P) = \partial f / \partial y(P) = \partial f / \partial z(P) = 0$$

The equation in (1) is projective, given by a homogeneous polynomial. Most of the time we dehomogenize the equation, by doing the change of variables

$$x/z \mapsto X, \quad y/z \mapsto Y$$

and we obtain

$$E: f(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + jY + k = 0, \quad (2)$$

However we should not forget that there might be some points of E “at infinity”, i.e. points that had $z = 0$. The following proposition is a considerable simplification:

Proposition 1. *Let E be an elliptic curve defined over K , with $\text{char}(K) \neq 2, 3$. Then there exists a rational change of variables so that E has a **Weierstrass equation** of the form*

$$Y^2 = X^3 + AX + B, \quad A, B \in K$$

The origin O has (projective) coordinates $[0, 1, 0]$, and this is the unique point at infinity.

3 The Group Structure

Let E be an elliptic curve defined over \mathbb{Q} with Weierstrass equation

$$Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{Q}$$

Actually, using a suitable change of coordinates we can assume that $A, B \in \mathbb{Z}$. First, we try to find all solutions with integer coefficients. Siegel proved the following result:

Theorem 1. *Let E/\mathbb{Q} be an elliptic curve of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Then E has only finitely many solutions with integer coefficients.*

Moreover, Alan Baker gave an algorithm to find these integral solutions (we will not discuss his method here).

Next, we are interested in finding all points of E with rational coordinates. We denote this set by

$$E(\mathbb{Q}) = \{(x, y) \in E \mid x, y \in \mathbb{Q}\}$$

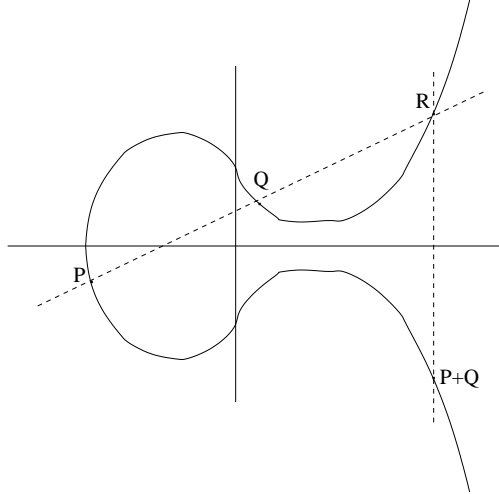
It turns out that this set has a beautiful structure and it forms a group. The (addition) group law is defined as follows. Given $P, Q \in E(\mathbb{Q})$, let \mathcal{L} be the line \overline{PQ} . Since E is given by a cubic equation, there is a unique third point of intersection in $\mathcal{L} \cap E$, which is also defined over \mathbb{Q} (why??)

$$\mathcal{L} \cap E = \{P, Q, R\}$$

We define

$$R = -(P + Q)$$

and $P + Q$ is then the second point of intersection of the vertical line through R with E .



Lo and behold! $(E, +)$ is a group. This is the greatest tool of all when we want to find points defined over \mathbb{Q} . Given any two points $P, Q \in E(\mathbb{Q})$ the addition in the group gives us a new point, also defined over \mathbb{Q} (notice that this follows from the construction of $P + Q$). Even if we just have a single point $P \in E(\mathbb{Q})$, we can find $2P, 3P, 4P, \dots$ (in order to construct $2P$ we take the tangent line to E at P , and look for the third point of intersection, which will be $-2P$).

Now we know $E(\mathbb{Q})$ is a group, so the natural question to ask is: *what is the structure of this group?* The answer is the following:

Theorem 2 (Mordell-Weil). $E(\mathbb{Q})$ is a finitely generated abelian group.

Proof. The proof of this theorem is fairly involved. The main two ingredients are the so called “weak Mordell-Weil theorem” (see below), the concept of height function for abelian groups and the “descent” theorem. See [2], Chapter VIII, page 189. \square

Remark: The Mordell-Weil theorem is true for elliptic curves over: \mathbb{Q} , any number field K , any finite field \mathbb{F}_q , for $F(T)$ (with F any of the fields mentioned before)...

Theorem 3 (Weak Mordell-Weil). $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite for all $m \geq 2$.

The Mordell-Weil theorem, together with the fundamental theorem of finitely generated abelian groups, implies that for any elliptic curve E/\mathbb{Q} the group of points has the following structure:

$$E(\mathbb{Q}) \simeq E_{torsion}(\mathbb{Q}) \oplus \mathbb{Z}^R$$

where $E_{torsion}(\mathbb{Q})$ denotes the set of points of finite order, and R is a non-negative integer which is called the *rank* of the elliptic curve. It is not known how big this number R can get for elliptic curves over \mathbb{Q} . The largest rank known for an elliptic curve over \mathbb{Q} is 24. However, conjecturally, we expect that there are elliptic curves with rank arbitrarily high. Some “hope” in this direction was given by the work of Shafarevich and Tate, who showed that this is true for curves over $\mathbb{F}_p(T)$ (see [8]).

Examples:

1. The elliptic curve $E_1/\mathbb{Q}: y^2 = x^3 + 6$ has rank 0 and $E_1(\mathbb{Q}) \simeq 0$.
2. Let $E_2/\mathbb{Q}: y^2 = x^3 + 1$, then $E_2(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. The torsion group is generated by the point $(2, 3)$.
3. Let $E_3/\mathbb{Q}: y^2 = x^3 + 109858299531561$, then $E_3(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}^5$ (see my website for details, math.bu.edu/people/alozano).
4. Let $E_4/\mathbb{Q}: y^2 + 1951/164xy - 3222367/40344y = x^3 + 3537/164x^2 - 40302641/121032x$, then $E_4(\mathbb{Q}) \simeq \mathbb{Z}^{10}$ (again, see my web).

4 Torsion Points

We start by analyzing the *torsion* part of E . These are the points:

$$E_{\text{torsion}}(\mathbb{Q}) = \{P \in E \mid \exists m \in \mathbb{N} \text{ such that } mP = O\}$$

Note that by the Mordell-Weil theorem $E_{\text{torsion}}(\mathbb{Q})$ is a finite abelian group. So the first question to ask is: *what finite abelian groups are possible?* The answer was given by Barry Mazur:

Theorem 4 (Mazur, [5], [6]). *Let E/\mathbb{Q} be an elliptic curve. Then the torsion subgroup $E_{\text{torsion}}(\mathbb{Q})$ is exactly one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} \quad \text{with } 1 \leq N \leq 10 \quad \text{or} \quad N = 12 \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \quad 1 \leq N \leq 4 \end{aligned}$$

Moreover, all these groups occur.

Remark: The theorem implies that if the order of a point $P \in E(\mathbb{Q})$ is greater than 12 then this point is actually not a torsion point (i.e. the point is of infinite order). Other than this, the theorem, even though very interesting, is not of great help when actually trying to compute the torsion of an elliptic curve E . The following theorem, proved independently by E. Lutz and T. Nagell, gives a very efficient method to compute the torsion subgroup of an elliptic curve defined over \mathbb{Q} .

Theorem 5 (Nagell-Lutz Theorem). *Let E/\mathbb{Q} be an elliptic curve with Weierstrass equation:*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

Then for all non-zero torsion points P we have:

1. *The coordinates of P are in \mathbb{Z} , i.e.*

$$x(P), y(P) \in \mathbb{Z}$$

2. *If P is of order greater than 2, then*

$$y(P)^2 \quad \text{divides} \quad 4A^3 + 27B^2$$

3. If P is of order 2 then

$$y(P) = 0 \quad \text{and} \quad x(P)^3 + Ax(P) + B = 0$$

Example: Let $p \in \mathbb{Z}$ be a prime and let $E_3/\mathbb{Q}: y^2 = x^3 + p^2$. Since $x^3 + p^2 = 0$ does not have solutions in \mathbb{Q} , there is no 2-torsion. Now,

$$4A^3 + 27B^2 = 27p^4$$

so if (x, y) is a torsion point then $x, y \in \mathbb{Z}$ and $y^2 \mid 27p^4$, thus

$$y = \pm 1, \pm p, \pm p^2, \pm 3p, \pm 3p^2$$

It is clear that $(0, \pm p) \in E$, and they can be checked to be points of order 3.

Definition 2. Let E be an elliptic curve over \mathbb{Q} given by a Weierstrass equation

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}$$

We define Δ , the discriminant of E , to be

$$\Delta = -16(4A^3 + 27B^2)$$

(compare with Theorem 4.2)

5 Elliptic Curves over Finite Fields

Let E/\mathbb{Q} be an elliptic curve. Assume that E has a (more general) Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients in \mathbb{Z} . Let p be a prime. By reducing each of the coefficients a_i modulo p we obtain the equation of a cubic curve \tilde{E} over the finite field \mathbb{F}_p (the field with p elements). Even though E was a non-singular curve, \tilde{E} might have singular points.

Definition 3. If \tilde{E} is a non-singular curve, we say that E has good reduction at p . Otherwise, we say that E has bad reduction at p .

Thus, for primes p of good reduction \tilde{E} is an elliptic curve defined over a finite field of p elements, $\mathbb{Z}/p\mathbb{Z}$. Of course, an elliptic curve defined over a finite field is much easier to work with than those defined over \mathbb{Q} . For example, we could just use *brute force* to find all possible solutions to the equation. By the way, the primes of bad reduction are easily found by looking at the discriminant of the curve:

Proposition 2. Let E be an elliptic curve and let Δ be the discriminant of E . Then if p is a prime of bad reduction then $p \mid \Delta$.

Let E be an elliptic curve defined over a finite field \mathbb{F}_q with $q = p^r$ elements ($p \in \mathbb{Z}$ is a prime). The following theorem gives a bound of the size of $E(\mathbb{F}_q)$, denoted by N_q , i.e. the number of points of E defined over \mathbb{F}_q . This was first conjectured by Emil Artin (in his thesis!) and proved by Helmut Hasse in the 1930's.

Theorem 6 (Hasse).

$$|N_q - q - 1| \leq 2\sqrt{q}$$

There are beautiful connections between the numbers N_p , the number of solutions modulo p , and the global group $E(\mathbb{Q})$. The most mysterious one is related to the Birch and Swinnerton-Dyer conjecture, which relates the growth of these numbers to the rank of the elliptic curve. In the following proposition we give an example of another interesting relationship.

Notation: Given a group G , we denote by $G[m]$ the m -torsion of G , i.e. the points of order m .

Proposition 3. *Let E/\mathbb{Q} be an elliptic curve (as above) and let m be a positive integer such that $\gcd(p, m) = 1$. If $\tilde{E}(\mathbb{F}_p)$ is a non-singular curve, then the map given by reduction modulo p (coordinate by coordinate)*

$$E(\mathbb{Q})[m] \longrightarrow \tilde{E}(\mathbb{F}_p)$$

is injective. Moreover this map is a homomorphism of abelian groups.

Remark: This proposition is quite useful when trying to compute the torsion subgroup of E/\mathbb{Q} . Note that this can be reinterpreted as follows: for all primes p which not divide m ,

$$E(\mathbb{Q})[m] \longrightarrow \tilde{E}(\mathbb{F}_p)$$

must be injective and therefore the number of m -torsion points divides the number of points defined over \mathbb{F}_p .

Example:

Let E/\mathbb{Q} be given by

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

The discriminant of this curve is $\Delta = -3888 = -2^4 3^5$. Recall that if p is a prime of bad reduction, then $p \mid \Delta$. Thus the only primes of bad reduction are 2, 3, so \tilde{E} is non-singular for all $p \geq 5$.

Let $p = 5$ and consider the reduction of E modulo 5, \tilde{E} . Then we have

$$\tilde{E}(\mathbb{Z}/5\mathbb{Z}) = \{\tilde{O}, (1, 2), (1, 3), (2, 1), (2, 4), (3, 0)\}$$

where all the coordinates are to be considered modulo 5 (remember the point at infinity!). Hence $N_5 = |\tilde{E}(\mathbb{Z}/5\mathbb{Z})| = 6$. Similarly, we can prove that $N_7 = 13$.

Now let $q \neq 5, 7$ be a prime number. Then we claim that $E(\mathbb{Q})[q]$ is trivial. Indeed, by the remark above we have

$$|E(\mathbb{Q})[q]| \text{ divides } N_5 = 6, N_7 = 13$$

so $|E(\mathbb{Q})[q]|$ must be 1.

For the case $q = 5$ we know that $|E(\mathbb{Q})[5]|$ divides $N_7 = 13$. But it is easy to see that if $E(\mathbb{Q})[p]$ is non-trivial, then p divides its order. Since 5 does not divide 13, we conclude that $E(\mathbb{Q})[5]$ must be trivial. Similarly $E(\mathbb{Q})[7]$ is trivial as well. Therefore $E(\mathbb{Q})$ has trivial torsion subgroup.

Notice that $(1, 2) \in E(\mathbb{Q})$ is an obvious point in the curve. Since we have proved that there is no non-trivial torsion, this point must be of infinite order! In fact

$$E(\mathbb{Q}) \cong \mathbb{Z}$$

and the group is generated by $(1, 2)$.

6 The Free Part

So far we have been successful to provide a number of efficient methods to compute the torsion part of $E(\mathbb{Q})$. Remember that Mordell-Weil says that

$$E(\mathbb{Q}) \cong E_{\text{torsion}} \oplus \mathbb{Z}^R$$

so it remains to show a way to find the points of infinite order, generators of the free part. This turns out to be a really hard question.

One could hope, via naive thinking, that if the coefficients of the elliptic curve are “small” then the generators should be “small” too, so we don’t have to look far. Unfortunately, this is far from the true story. Bremner and Cassels showed that the elliptic curve

$$y^2 = x^3 + 877x$$

has rank 1, and the x -coordinate of a generator P is given by

$$x = (612776083187947368101/7884153586063900210)^2$$

We would like to compute the full Mordell-Weil group for some elliptic curves, or at least a subgroup of finite index (this is, a set of points which generate a subgroup of rank R). Also, depending on our interests, we might just want to compute R , the rank of the elliptic curve. In both cases, it is enough to look at the *weak Mordell-Weil* group

$$E(\mathbb{Q})/2E(\mathbb{Q})$$

This is still hard to compute, but can be embedded in an easier (but bigger) cohomological group, the *Selmer group* $S^{(2)}(E/\mathbb{Q})$ (see Appendix A for group cohomology, see Appendix B for the Selmer group). There is an exact sequence:

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S^{(2)}(E/\mathbb{Q}) \longrightarrow TS(E/\mathbb{Q})[2] \longrightarrow 0$$

where $TS(E/\mathbb{Q})$ is the *Tate-Shafarevich* group (see Appendix B). So, if we could compute the Selmer group, we could give a bound of the weak Mordell-Weil group, or even compute it! This process, computing $S^{(2)}(E/\mathbb{Q})$ is usually known as *2-Descent*. The algorithm was first explained by Birch and Swinnerton-Dyer, who used it to provide evidence for their celebrated conjecture (see [9]). Later on J. Cremona implemented the algorithm in a much more efficient way, and a program can be found online, *mwrnk* (see [11]).

Note that the map “multiplication by 2” (denoted [2]) is an *isogeny* of any elliptic curve, this is, an endomorphism of the group $E(\mathbb{Q})$. If E' is another elliptic curve, and $\phi: E \rightarrow E'$ is any other 2-isogeny (group homomorphism together with another homomorphism $\hat{\phi}: E' \rightarrow E$ such that $\phi \circ \hat{\phi} = [2]$), then we can compute another Selmer group for ϕ , $S^\phi(E/\mathbb{Q})$, which fits in a similar exact sequence:

$$0 \longrightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \longrightarrow S^\phi(E/\mathbb{Q}) \longrightarrow TS(E/\mathbb{Q})[\phi] \longrightarrow 0$$

Moreover, putting $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ together, we may be able to reconstruct the weak Mordell-Weil group, by using the following exact sequence:

$$0 \longrightarrow \frac{E'(\mathbb{Q})[\hat{\phi}]}{\phi(E(\mathbb{Q})[2])} \longrightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \longrightarrow 0$$

7 2-Descent

Let E/\mathbb{Q} be an elliptic curve. We assume that E contains a 2-torsion point P ($2P = O$). The algorithm can be done in general but this case is much easier for the exposition. By a change of variables, we can assume $P = (0, 0)$ and E has Weierstrass equation:

$$E: y^2 = x^3 + ax^2 + bx = x(x^2 + ax + b)$$

Define also the auxiliar elliptic curve E' :

$$E': Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$$

Then there exists a 2 isogeny:

$$\phi: E \rightarrow E', \quad \phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

$$\hat{\phi}: E' \rightarrow E, \quad \hat{\phi}(X, Y) = \left(\frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2)}{8X^2} \right)$$

Let $S = \{\text{primes dividing } 2b(a^2 - 4b)\}$ and define

$$\mathbb{Q}(S, 2) = \{x \in \mathbb{Z} : \text{ord}_p(x) = 0 \ \forall p \text{ not in } S, \text{ord}_p(x) = 0 \text{ or } 1 \ \forall p \in S\} / \{\mathbb{Z}^2\}$$

For each $d \in \mathbb{Q}(S, 2)$ define the following *homogeneous spaces*:

$$C_d(w, z): dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4$$

$$C'_d(W, Z): dW^2 = d^2 + 4adZ^2 + 16bZ^4$$

There are maps:

$$\psi: C_d \rightarrow E', \psi(z, w) = (d/z^2, -dw/z^3)$$

$$\psi': C'_d \rightarrow E, \psi'(Z, W) = (d/Z^2, -dW/Z^3)$$

and injective maps:

$$\delta: E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \rightarrow \mathbb{Q}(S, 2), \quad \delta(O) = 1, \delta(0, 0) = a^2 - 4b, \delta(X, Y) = X$$

$$\delta': E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \rightarrow \mathbb{Q}(S, 2), \quad \delta'(O) = 1, \delta'(0, 0) = b, \delta'(x, y) = x$$

such that

$$\delta(\psi(P)) = d, \quad \delta'(\psi'(P')) = d, \quad \forall P \in C_d, \quad \forall P' \in C'_d$$

Theorem 7 (2-Descent). *With notation as above*

$$S^\phi(E/\mathbb{Q}) = \{d \in \mathbb{Q}(S, 2) : C_d(\mathbb{Q}_p) \neq \emptyset \forall p \in S, C_d(\mathbb{R}) \neq \emptyset\}$$

Moreover,

$$E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \cong \{d \in \mathbb{Q}(S, 2) : C_{d'} \text{ has a rational point}\}$$

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \cong \{d \in \mathbb{Q}(S, 2) : C_d \text{ has a rational point}\}$$

If we denote the order of these groups by n_1, n'_1 then the rank R of the elliptic curve E is

$$2^R = \frac{n_1 n'_1}{4}$$

As a summary, given E/\mathbb{Q} we construct the homogeneous spaces C_d and $C_{d'}$. These spaces have points over \mathbb{Q} if and only if E has points, and the points in the homogeneous spaces map to points on E via the maps ψ' and $\hat{\phi} \circ \psi$.

8 Appendix A: Group Cohomology

Let G be a group and let M be a (left) G -module. The 0^{th} cohomology group of the G -module M is

$$H^0(G, M) = \{m \in M : \forall \sigma \in G, \sigma m = m\}$$

which is the set of elements of M which are G -invariant, also denoted by M^G .

A map $\phi: G \rightarrow M$ is said to be a *crossed homomorphism* (or *1-cocycle*) if

$$\phi(\alpha\beta) = \phi(\alpha) + \alpha\phi(\beta)$$

for all $\alpha, \beta \in G$. If we fix $m \in M$, the map $\rho: G \rightarrow M$ defined by

$$\rho(\alpha) = \alpha m - m$$

is clearly a crossed homomorphism, said to be *principal* (or *1-coboundary*). We define the following groups:

$$Z^1(G, M) = \{\phi: G \rightarrow M : \phi \text{ is a 1-cocycle}\}$$

$$B^1(G, M) = \{\rho: G \rightarrow M : \rho \text{ is a 1-coboundary}\}$$

Finally, the 1^{st} cohomology group of the G -module M is defined to be the quotient group:

$$H^1(G, M) = Z^1(G, M)/B^1(G, M)$$

The following proposition is very useful when trying to compute cohomology groups:

Proposition 4. *Let G be a group and let A, B, C be G -modules related by an exact sequence:*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

Then there is a long exact sequence in cohomology:

$$0 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C)$$

9 Appendix B: The Selmer and Tate-Shafarevich groups

Given an elliptic curve E we can define two very interesting and important groups, the *Selmer group* and the *Tate-Shafarevich group*, which together provide a measure of the failure of the Hasse principle for elliptic curves, by measuring whether the curve is everywhere locally soluble. Here we present the construction of these groups.

Let E, E' be elliptic curves defined over \mathbb{Q} and let $\bar{\mathbb{Q}}$ be an algebraic closure of \mathbb{Q} . Let $\phi: E \rightarrow E'$ be a non-constant isogeny (for example, we can let $E = E'$ and think of ϕ as being the “multiplication by n ” map, $[n]: E \rightarrow E$). The following standard result asserts that ϕ is surjective over $\bar{\mathbb{Q}}$:

Theorem 8. *Let C_1, C_2 be curves defined over an algebraically closed field K and let*

$$\psi: C_1 \rightarrow C_2$$

be a morphism (or algebraic map) of curves. Then ψ is either constant or surjective.

Proof. See [7], Chapter II.6.8. □

Since $\phi: E(\bar{\mathbb{Q}}) \rightarrow E'(\bar{\mathbb{Q}})$ is non-constant, it must be surjective and we obtain the following exact sequence:

$$0 \rightarrow E(\bar{\mathbb{Q}})[\phi] \rightarrow E(\bar{\mathbb{Q}}) \rightarrow E'(\bar{\mathbb{Q}}) \rightarrow 0 \quad (1)$$

where $E(\bar{\mathbb{Q}})[\phi] = \text{Ker } \phi$. Let $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of \mathbb{Q} , and consider the i^{th} -cohomology group $H^i(G, E(\bar{\mathbb{Q}}))$ (we abbreviate by $H^i(G, E)$). Using equation (1) we obtain the following long exact sequence (see Proposition 1 in Appendix A: Group cohomology):

$$\begin{aligned} 0 &\rightarrow H^0(G, E(\bar{\mathbb{Q}})[\phi]) \rightarrow H^0(G, E) \rightarrow H^0(G, E') \rightarrow \\ &\rightarrow H^1(G, E(\bar{\mathbb{Q}})[\phi]) \rightarrow H^1(G, E) \rightarrow H^1(G, E') \end{aligned} \quad (2)$$

Note that

$$H^0(G, E(\bar{\mathbb{Q}})[\phi]) = (E(\bar{\mathbb{Q}})[\phi])^G = E(\mathbb{Q})[\phi]$$

and similarly

$$H^0(G, E) = E(\mathbb{Q}), \quad H^0(G, E') = E'(\mathbb{Q})$$

From (2) we can obtain an exact sequence:

$$0 \rightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \rightarrow H^1(G, E(\bar{\mathbb{Q}})[\phi]) \rightarrow H^1(G, E)[\phi] \rightarrow 0$$

We could repeat the same procedure but this time for E, E' defined over \mathbb{Q}_p , for some prime number p , and obtain a similar exact sequence but with coefficients in \mathbb{Q}_p which relates to the original in the following commutative diagram (here $G_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$):

$$\begin{array}{ccccccc} 0 & \rightarrow & E'(\mathbb{Q})/\phi(E(\mathbb{Q})) & \rightarrow & H^1(G, E(\bar{\mathbb{Q}})[\phi]) & \rightarrow & H^1(G, E)[\phi] \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) & \rightarrow & H^1(G_p, E(\bar{\mathbb{Q}}_p)[\phi]) & \rightarrow & H^1(G_p, E)[\phi] \rightarrow 0 \end{array}$$

The goal here is to find a **finite** group containing $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$. Unfortunately $H^1(G, E(\bar{\mathbb{Q}})[\phi])$ is not necessarily finite. With this purpose in mind, we define the ϕ -Selmer group:

$$S^\phi(E/\mathbb{Q}) = \text{Ker} \left(H^1(G, E(\bar{\mathbb{Q}})[\phi]) \rightarrow \prod_p H^1(G_p, E) \right)$$

Equivalently, the ϕ -Selmer group is the set of elements γ of $H^1(G, E(\bar{\mathbb{Q}})[\phi])$ which image γ_p in $H^1(G_p, E(\bar{\mathbb{Q}})[\phi])$ comes from some element in $E(\mathbb{Q}_p)$.

Finally, by imitation of the definition of the Selmer group, we define the *Tate-Shafarevich group*:

$$TS(E/\mathbb{Q}) = \text{Ker} \left(H^1(G, E) \rightarrow \prod_p H^1(G_p, E) \right)$$

The Tate-Shafarevich group is precisely the group that measures the Hasse principle in the elliptic curve E . It is unknown if this group is finite.

References

- [1] James Milne, *Elliptic Curves*, online course notes, <http://www.jmilne.org/math/CourseNotes/math679.html>
- [2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.
- [3] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.
- [4] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, New Jersey, 1971.
- [5] Barry Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. 47 (1977), 33-186.
- [6] Barry Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129-162.
- [7] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.
- [8] I. R. Shafarevich, J. Tate, *The rank of elliptic curves*, AMS Transl. 8 (1967), 917-920.
- [9] B. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves (I) and (II)*, J. Reine Angew. Math. 212 (1963), 7-25 and 218 (1965), 79-108.
- [10] J.P. Serre, *Galois Cohomology*, Springer-Verlag, New York.
- [11] John Cremona's website: <http://www.maths.nott.ac.uk/personal/jec/>