

Finding Rational Points on Elliptic Curves
(Over \mathbb{Q})

Alan Silvester

April 18, 2005

1 History

One substantial part of number theory is Diophantine equations. These are polynomial equations that we wish to solve in terms of integer or rational solutions. They are named after Diophantus of Alexandria, one of the greatest Greek mathematicians who posed many problems of this form. The questions usually asked are: Given a Diophantine equation

1. Are there any solutions in integers?
2. Are there any solutions in rational numbers?
3. How many integer solutions are there?
4. How many rational solutions are there?

For linear and quadratic equations, we already know the answers to these questions. For a linear equation $ax + by = c$, there are always infinitely many rational solutions. If $\gcd(a, b) \nmid c$, there are infinitely many integer solutions. Otherwise if $\gcd(a, b) \mid c$, then there are no integer solutions. For a quadratic equation, if one can find a rational solution then there are infinitely many rational solutions. But what about elliptic curves

$$y^2 = x^3 + ax^2 + bx + c?$$

The integer and rational number solutions to equations of this form are not completely understood. The description of these solutions usually involve an interesting mix of algebra, number theory, and geometry.

2 Integer and Rational Points

In the 1920's, Siegel showed that an elliptic curve has only finitely many integer solutions. Much later, in 1970, Baker and Coates gave an explicit upper bound on the largest solution, based on the coefficients of the elliptic curve polynomial. Unfortunately, this bound is quite large and generally impractical.

For rational points on elliptic curves, Poincaré conjectured in 1901 that there exists a finite set of points that would generate all of the (possibly infinite) rational points. This was later proven by Mordell in 1923. So far, Mordell's method *often* allows one to find such a finite generating set, but it has not been proven to always work – this is still just a conjecture. In this paper, we will build up the necessary framework needed to discuss Mordell's Theorem and some of the problems that arise.

Definition 1 Let E be an elliptic curve over \mathbb{Q} and let

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

where \mathcal{O} is the point at infinity, denote the additive group of rational points on E .

What can we say about this group, its size and its structure? We'll begin by considering points of finite order. For the remainder of this paper, we will make two assumptions: that our elliptic curve E can be rewritten in Weierstrass form $y^2 = x^3 + ax + b$ and that the point at infinity \mathcal{O} is a rational point.

3 Points of Finite Order

Recall the group law for point addition on an elliptic curve E over a field K . If our elliptic curve E is defined over \mathbb{Q} then adding two rational points will always result in another rational point since the formulas in the group law definition are rational functions.

Definition 2 Let $E[n] = \{P \in E(\mathbb{Q}) \mid [n]P = \mathcal{O}\}$ be the n -torsion subgroup of $E(\mathbb{Q})$.

We would like to begin classifying the possible structures for $E[n]$ for various values of n .

3.1 Points of Order 2

In $E(\mathbb{Q})$, which points satisfy $2P = \mathcal{O}$ and $P \neq \mathcal{O}$. It's easier to consider the equivalent condition that $P = -P$. Since our elliptic curve is in Weierstrass form, $-(x, y) = (x, -y)$ and points P satisfying $P = -P$ are just those with $y = 0$. In other words, the points

$$P_1 = (\alpha_1, 0) \quad P_2 = (\alpha_2, 0) \quad P_3 = (\alpha_3, 0)$$

where α_i is a root of the cubic $f(x)$.

Allowing only rational coordinates, we see that $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2,$ or $\{0\}$ depending on whether $f(x)$ has 3, 1, or 0 rational roots.

3.2 Explicit Duplication Formulas

From our group law, we know $[2]P = P + P$ is given by the following

$$[2]P = \left(\left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1, \frac{3x_1^2 + a}{2y_1} (x_1 - x_3) - y_1 \right)$$

Considering only the x coordinate, we see

$$\begin{aligned} \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 &= \frac{(3x_1^2 + a)^2}{4y_1^2} - 2x_1 = \frac{(3x_1^2 + a)^2}{4(x_1^3 + ax_1 + b)} - 2x_1 \\ &= \frac{(3x_1^2 + a)^2 - 8x_1(x_1^3 + ax_1 + b)}{4(x_1^3 + ax_1 + b)} \\ &= \frac{x_1^4 - 2ax_1^2 - 8x_1b + a^2}{4(x_1^3 + ax_1 + b)} \end{aligned}$$

We will need this formula in the next section.

3.3 Points of Order 3

As with the points of order 2, we will consider $2P = -P$ instead of $3P = \mathcal{O}$. Looking at just the coordinates, $[2](x, y) = -(x, y) = (x, -y)$. So

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} = x$$

Cross-multiplication and simplifying gives: $3x^4 + 6ax^2 + 12bx - a^2 = 0$. So a point has order 3 iff its x coordinate is a root of

$$3x^4 + 6ax^2 + 12bx - a^2 = 0 \tag{1}$$

Moreover, these four roots must be distinct since

$$\frac{d}{dx} 3x^4 + 6ax^2 + 12bx - a^2 = 12f(x)$$

and

$$3x^4 + 6ax^2 + 12bx - a^2 = 2f(x)f''(x) - f'(x)^2$$

So if (1) had a double root, then so do $f(x)$, $f'(x)$ which would contradict the non-singularity of our elliptic curve.

Each of these four roots gives rise to two possible y coordinate values, so we have eight possible points. Including \mathcal{O} , we see $|E[3]| = 9$ and since every point in $E[3]$ has order 3, we must have $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ or $\{0\}$.

3.4 Points of Other Orders

Theorem 1 *Let E be an elliptic curve over \mathbb{Q} and n be a positive integer. Then*

$$E[n] \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

This theorem can be generalized to an elliptic curve over an arbitrary field K , however problems arise if $\text{char}(K) \mid n$ (see [10], Theorem 3.2).

4 Discriminants and Integral Coordinates

Before we introduce our first two major results, we need to recall the discriminant of an elliptic curve.

Definition 3 *For an elliptic curve $E : y^2 = x^3 + ax + b$ over \mathbb{Q} , the discriminant is $\Delta = -4a^3 - 27b^2 \neq 0$.*

One very interesting part of the theorem we are building up to is that if (x, y) is a rational point with finite order on E , then $x, y \in \mathbb{Z}$. We will not prove this fact, though. See [9] (Chapter ii, Section 4) or [10] (Chapter 8, Section 1) for more details and a proof of this claim.

5 Theorems of Nagell-Lutz and Mazur

Using the concepts we have developed, we can now state the Nagell-Lutz theorem.

Theorem 2 (Nagell-Lutz) *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over \mathbb{Q} with $a, b \in \mathbb{Z}$. If $P = (x, y) \in E$ is a rational point of finite order then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y \mid \Delta$.*

Computationally, it's often useful to use a stronger version of the Nagell-Lutz theorem. More specifically, we can prove that if P is a point of finite order $m \neq 2$ then $y^2 \mid \Delta$.

We need to be careful in using the Nagell-Lutz theorem: it's not an "if and only if" theorem. It is possible to have points with integer coordinates and $y \mid \Delta$ but not to have finite order. The Nagell-Lutz theorem allows us to construct a list of points containing all points of finite order, but we can never use it to show a point has finite order. To do that, we need to find n such that $[n]P = \mathcal{O}$.

On the other hand, the Nagell-Lutz theorem can be used to show a point has infinite order. Taking a point P , we can compute the x coordinates

of $[2]P$, $[4]P$, $[8]P, \dots$ using the doubling formula. If the x coordinate of $[n]P$ is not an integer, then $[n]P$ and hence P are not points of finite order.

Another interesting corollary to the Nagell-Lutz theorem is that the torsion subgroup T of $E(\mathbb{Q})$ is finite. This follows since there are only finitely many divisors of the discriminant Δ .

So what finite orders are possible? We've seen that it is relatively easy to get points of orders 2 and 3. We can find points of even higher orders. For example, for every $t \neq 0, 1/4 \in \mathbb{Q}$ the point $P = (t, t)$ on

$$y^2 = x^3 - (2t - 1)x^2 + t^2x$$

is a point of order 4. So there are infinitely many elliptic curves with points of order 4.

Through the mid- to late-1800s, families of curves with points of orders 5, 6, 7, 8, 9, 10 and 12 were produced. But no one could produce a curve with a point of order 11 or order higher than 12. It wasn't until 1940 that Billing and Mahler [1] showed that no elliptic curve had a point of order 11. This work eventually resulted in Mazur's theorem, which characterises the possible finite orders.

Theorem 3 (Mazur) *Let E be an elliptic curve over \mathbb{Q} and suppose that P is a point of finite order m . Then $1 \leq m \leq 10$ or $m = 12$. Moreover, the torsion subgroup $T \subseteq E(\mathbb{Q})$ is isomorphic to one of the following:*

- \mathbb{Z}_n for $1 \leq n \leq 10$ or $n = 12$
- $\mathbb{Z}_2 \times \mathbb{Z}_{2n}$ for $1 \leq n \leq 4$.

6 Examples

In this section we consider two examples showing the computation of the torsion subgroup T .

Let $E : y^2 = x^3 + 4$. We see $\Delta = -432$. So suppose $P = (x, y)$ is a point of finite order. Since $0 = x^3 + 4$ has no rational solutions, we must have $y \neq 0$. So by the Nagell-Lutz theorem, we must have $y^2 \mid -432$. So the possibilities for y are

$$y \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

Checking all of these, only $y = \pm 2$ give rational values for x , namely $x = 0$. So the only possible torsion points are $(0, 2)$ and $(0, -2)$. A quick calculation shows that $[3](0, \pm 2) = \mathcal{O}$. So the torsion subgroup is $T \cong \mathbb{Z}/3\mathbb{Z}$.

Let $E : y^2 = x^3 + 8$. This time $\Delta = -1728$ and if $y = 0$ then $x = -2$. We know $(-2, 0)$ has order 2. So suppose $y \neq 0 \Rightarrow y^2 \mid -1728 \Rightarrow y \mid -24$. Checking all possibilities, only the points $(1, \pm 3)$ and $(2, \pm 4)$ satisfy E . However,

$$[2](1, 3) = \left(\frac{-7}{4}, \frac{-13}{8} \right) \quad [2](2, 4) = \left(\frac{-7}{4}, \frac{13}{8} \right)$$

Since these points don't have integer coordinates, they cannot have finite order. So $(1, \pm 3)$ and $(2, \pm 4)$ are not points of finite order either. Thus, the torsion subgroup of $E(\mathbb{Q})$ is $\{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$.

7 Descent

We have seen that the rational points of finite order have been completely characterised by the theorems of Nagell-Lutz and Mazur. But what about rational points of infinite order?

7.1 General Theory

Consider an elliptic curve of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ for distinct $e_i \in \mathbb{Z}$. If $y = 0$ then $x = e_1, e_2, e_3$ are the only rational points on E . So assume that $y \neq 0$. Notice that the right-hand side of E is a square. So, intuitively, each factor should be close to being a square. Write

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

for $a, b, c, u, v, w \in \mathbb{Q}$. Then

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad \Rightarrow \quad y^2 = au^2 \cdot bv^2 \cdot cw^2 = abc(uvw)^2$$

So abc must be a square. Moreover, by adjusting u, v, w we may assume that a, b, c are squarefree.

The key observation is expressed in the following lemma:

Lemma 1 *Let $S = \{p \mid p \text{ prime}, p \mid \sqrt{\Delta}\}$. If p is prime and $p \mid abc$ then $p \in S$.*

Since S is finite, there are only finitely many possibilities for (a, b, c) . This surprising fact holds for any elliptic curve over \mathbb{Q} ! The process we are describing is called a descent (specifically a 2-descent). Suppose x had at most N digits in its numerator and denominator. Then u, v, w should have at most $N/2$ digits. So instead of searching for the large points x , we can search for

the smaller u, v, w values. In the next section we will present a work-through example showing how 2-descent works in practice.

Next, we wish to show the finite number of combinations for (a, b, c) come from the points (x, y) that form a group mod squares.

Definition 4 Let $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ be the group of rational numbers mod squares. We say two numbers $x \neq y \in \mathbb{Q}$ are equivalent if they differ by a square. In other words

$$x \sim y \quad \Leftrightarrow \quad \exists t \in \mathbb{Q} \text{ s.t. } x = t^2 y.$$

Every element in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented by ± 1 times a product of distinct primes. This leads us to consider the following homomorphism:

Theorem 4 Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ be an elliptic curve with distinct $e_i \in \mathbb{Z}$. Then

$$\begin{aligned} \varphi : E(\mathbb{Q}) &\rightarrow \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \right) \oplus \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \right) \oplus \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \right) \\ (x, y) &\mapsto (x - e_1, x - e_2, x - e_3) \\ \mathcal{O} &\mapsto (1, 1, 1) \\ (e_1, 0) &\mapsto ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) \\ (e_2, 0) &\mapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) \\ (e_3, 0) &\mapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)) \end{aligned}$$

is a homomorphism with $\ker(\varphi) = 2E(\mathbb{Q})$.

Example 1 Consider the elliptic curve $E : y^2 = x(x + 2)(x - 2)$. We have

$$\begin{aligned} \varphi(\mathcal{O}) &= (1, 1, 1) & \varphi(0, 0) &= (-1, -2, 2) \\ \varphi(2, 0) &= (2, 2, 1) & \varphi(-2, 0) &= (-2, -1, 2) \end{aligned}$$

7.2 Illustrated Example

We now present a worked through example to show how 2-descent works in practice.

Example 2 Consider the following elliptic curve:

$$E = y^2 = x(x + 2)(x - 2)$$

If $y = 0$ then $x = 0, \pm 2$ are the only rational points on E . So assume that $y \neq 0$. As in the previous section, we write

$$x = au^2 \quad (x + 2) = bv^2 \quad (x - 2) = cw^2$$

for $a, b, c, u, v, w \in \mathbb{Q}$. Then

$$y^2 = x(x + 2)(x - 2) \quad \Rightarrow \quad y^2 = au^2 \cdot bv^2 \cdot cw^2 = abc(uvw)^2$$

and abc is square with a, b, c squarefree. We claim that $a, b, c \in \{\pm 1, \pm 2\}$. For a proof of this claim, see [10] (Chapter 8, Section 2).

Since abc is a square, a, b uniquely determine c . So we have four possible choices for both a and b . This gives 16 possibilities. We begin by eliminating some of these choices. Notice

$$x - 2 < x < x + 2 \quad \Rightarrow \quad bv^2 < au^2 < cw^2$$

If $a < 0$ then $b < 0$ and if $a > 0$ then $c > 0$, which implies that $abc > 0$ and so $b > 0$. Thus a, b must have the same sign. This leaves 8 possibilities. Consider the case $(a, b, c) = (1, 2, 2)$. Then

$$x = u^2 \quad x - 2 = 2v^2 \quad x + 2 = 2w^2$$

and so $u^2 - 2v^2 = 2$ and $u^2 - 2w^2 = -2$. If $2 \mid \text{denom}(v)$ then $2^l \parallel \text{denom}(2v^2)$ for some odd l . But the exact power of 2 in $\text{denom}(u)$ is even. So $u^2 - 2v^2 \notin \mathbb{Z}$ which is a contradiction. So u, v must have odd denominators. We now work mod powers of 2. Now $2 \mid u^2 \Rightarrow 2 \mid u \Rightarrow 4 \mid u^2$ so $-2v^2 \equiv 2 \pmod{4}$. Hence $2 \nmid v$. By symmetry, $-2w^2 \equiv -2 \pmod{4}$ and so $2 \nmid w$. So it follows that $v^2 \equiv w^2 \equiv 1 \pmod{8}$ and

$$2 = u^2 - 2v^2 \equiv u^2 - 2 \equiv u^2 - 2w^2 = -2 \pmod{8}$$

which is a contradiction. Hence $(a, b, c) = (1, 2, 2)$ is impossible. By similar arguments, we can eliminate $(-1, -1, 1), (2, 1, 2), (-2, 2, -1)$.

The only possibilities remaining are

$$(a, b, c) \in \{(1, 1, 1), (-1, -2, 2), (2, 2, 1), (-2, -1, 2)\}$$

but as seen in the previous example, these choices correspond to the points we already had, namely: $\mathcal{O}, (0, 0), (2, 0)$, and $(-2, 0)$. Using the Nagell-Lutz theorem, we see if P is a point of finite order then $y^2 \mid -256$. But the x coordinates corresponding to these values are not integral or even rational. So there are no non-trivial points of odd orders. Thus the group of rational points on E is $E(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (2, 0), (-2, 0)\}$.

8 Mordell-Weil Theorems

The homomorphism theorem stated in the previous section has a very important corollary.

Theorem 5 (Weak Mordell-Weil) *Let E be an elliptic curve defined over \mathbb{Q} . Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

We can actually generalize this theorem to say if E is an elliptic curve over K then $E(K)/2E(K)$ is finite. However, we will not need this for this paper.

Because we are considering $E(\mathbb{Q})/2E(\mathbb{Q})$, it is useful to note that the duplication map $[2] : E(\mathbb{Q}) \rightarrow 2E(\mathbb{Q})$ can actually be decomposed into the composition of two other maps. Looking at the x coordinate in the duplication map, we notice that it is of degree 4. This implies that we should be able to find two degree 2 maps. Assume that $f(x)$ has one rational root. Then E has a rational point of order 2 at, say, $(x_0, 0)$. Translating the curve, we can place $(x_0, 0)$ at the origin without affecting $E(\mathbb{Q})$. Our elliptic curve E then becomes $E : y^2 = f(x) = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Z}$ and rational point $\mathcal{T} = (0, 0)$ of order 2. The discriminant of this new curve is $\Delta = b^2(a^2 - 4b) \neq 0$.

Definition 5 *Let $E : y^2 = x^3 + ax^2 + bx$ be an elliptic curve over \mathbb{Q} . We define a related elliptic curve $\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$.*

To justify this definition, consider $\bar{E} : y^2 = x^3 + 4ax^2 + 16bx$. Using a change of variables $x \mapsto 4x$ and $y \mapsto 8y$, we see \bar{E} becomes $64y^2 = 64x^3 + 64x^2 + 64bx$, which is basically E . So the map sending $(x, y) \mapsto (x/4, y/8)$ gives that $\bar{E} \cong E$ and moreover that $\bar{E} \cong E(\mathbb{Q})$.

Lemma 2 *Let E, \bar{E} be an elliptic curve and its related curve as defined above. Let $P \in E$ and $\bar{P} \in \bar{E}$ be points with non-zero x coordinates and let $\mathcal{T} = (0, 0)$. We define two maps*

$$\begin{array}{lcl} \varphi : E & \rightarrow & \bar{E} \\ (x, y) & \mapsto & \left(\frac{y^2}{x^2}, y \left(\frac{x^2 - b}{x^2} \right) \right) \\ \mathcal{O}, \mathcal{T} & \mapsto & \bar{\mathcal{O}} \end{array} \quad \begin{array}{lcl} \psi : \bar{E} & \rightarrow & \bar{\bar{E}} \\ (\bar{x}, \bar{y}) & \mapsto & \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2 - \bar{b})}{8\bar{x}^2} \right) \\ \bar{\mathcal{O}}, \bar{\mathcal{T}} & \mapsto & \bar{\mathcal{O}} \end{array}$$

Then $\psi \circ \varphi = [2] : P \mapsto 2P$.

We will not go through the details of this proof, but it is not hard to check that both φ and ψ are well-defined homomorphisms and that their composition does result in the multiplication by two map [2]. This lemma then allows us to quickly prove that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

The most important thing to notice is that we can strengthen the Weak Mordell-Weil theorem:

Theorem 6 (Mordell-Weil) *Let E be an elliptic curve over \mathbb{Q} . Then $E(\mathbb{Q})$ is a finitely-generated abelian group.*

8.1 Heights

Definition 6 *Let $r = a/b \in \mathbb{Q}$ be in lowest terms. The logarithmic height function is $h(r) = \log \max \{|a|, |b|\}$.*

The height function is closely related to the number of digits needed to write a rational number. In other words, it is a measure of the “complexity” of a rational number. Consider $1/2$ and $5001/10000$. Both numbers have the same basic numerical value, but one is obvious much more “complicated”. An interesting property of this function is that for a given constant c , there are only finitely many rational numbers r such that $h(r) \leq c$.

8.2 The Descent Theorem

The descent theorem is a key component to the proof of the Mordell-Weil Theorem. In fact, the Mordell-Weil Theorem is a special case of the descent theorem.

Theorem 7 *Let Γ be a commutative group and suppose that there is a function $\lambda : \Gamma \rightarrow [0, \infty)$ with the following three properties:*

- *For every real number C , the set $\{P \in \Gamma \mid \lambda(P) \leq C\}$ is finite.*
- *For every $P_0 \in \Gamma$, there is a constant κ_0 such that $\lambda(P+P_0) \leq 2\lambda(P) + \kappa_0$ for all $P \in \Gamma$.*
- *There is a constant κ_1 such that $\lambda(2P) \geq 4\lambda(P) - \kappa_1$ for all $P \in \Gamma$.*

Suppose further that the subgroup 2Γ has finite index in Γ . Then Γ is finitely generated.

Letting $\Gamma = E(\mathbb{Q})$ and $\lambda = h$ we have a restatement of the Mordell-Weil theorem.

8.3 Sketch of the Mordell-Weil Theorem Proof

We know $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, but this isn't quite enough. It is the concept of heights that will allow us to prove the Mordell-Weil theorem. Let R_1, \dots, R_n represent the finitely many cosets in $E(\mathbb{Q})/2E(\mathbb{Q})$ and let $P \in E(\mathbb{Q})$ be an arbitrary point. We can write $P = R_i + 2P_1$ for some i and point P_1 . We can then write $P_1 = R_j + 2P_2$ for some j and P_2 and so on. If we can show that this process eventually terminates, we can use this to prove the theorem. The height function can be used to show that the points P_1, P_2, P_3, \dots are "getting smaller" and that eventually one of the points P_k will lay in a finite set of small points. This shows that any point of $E(\mathbb{Q})$ can be constructed by applying the group law to our finite set. Thus $E(\mathbb{Q})$ will be a finitely-generated abelian group. Of course, the devil is in the details and the actual proof of this theorem is much more complex.

By the Fundamental Theorem of Finitely Generated Abelian Groups, we know that $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$ where T is a finite group called the torsion subgroup and where $r \geq 0 \in \mathbb{Z}$ is call the rank of $E(\mathbb{Q})$.

9 Computing the Rank of an Elliptic Curve

As seen in earlier sections, the Nagell-Lutz theorem gives us a method for computing the torsion subgroup T of $E(\mathbb{Q})$. If the rank of an elliptic curve is zero, then all rational points on E have finite order. But if the rank is non-zero, then there are rational points of infinite order on E . Two questions naturally arise: how do we compute the rank of an elliptic curve and how do we find these rational points of infinite order?

To compute the rank of $E(\mathbb{Q})$, we will use a combination of 2-descent, the rational numbers mod squares, and our homomorphism φ . The method of 2-descent allows us to rewrite our elliptic curve E as $y^2 = abc(uvw)^2$. By lemma 1, we can find a list of possibilities for a, b , and c . By carefully choosing values for a, b , and c we can eliminate many combinations since φ is a homomorphism. Then

$$\left| \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \right| = |\varphi(E(\mathbb{Q}))| = |T| \cdot |\mathbb{Z}_2^r| = |T| \cdot 2^r$$

Using the Nagell-Lutz theorem, we can determine T and hence $|T|$. By eliminating possibilities for a, b, c we'll have computed $|\varphi(E(\mathbb{Q}))|$. Thus we can determine the rank of E .

10 Illustrated Example

We now present a worked through example showing how the algorithm presented in the previous section works. Consider the elliptic curve $E : y^2 = x^3 - 25x$. We begin by finding all of the torsion points in $E(\mathbb{Q})$. If $y = 0$ then

$$0 = x^3 - 25x = x(x - 5)(x + 5)$$

and the only 2-torsion points are $(0, 0)$ and $(\pm 5, 0)$. Supposing $y \neq 0$, we can show via the Nagell-Lutz theorem that there are no n -torsion points for $n \geq 3$. Thus $T \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Notice, however, that the point $(-4, 6)$ satisfies E and moreover

$$[2](-4, 6) = \left(\frac{41^2}{12^2}, \frac{-62279}{1728} \right)$$

So we have a rational point of infinite order on E . Recall our homomorphism $\varphi : (x, y) \mapsto (x, x - 5, x + 5)$. Under φ , we have

$$\begin{array}{llll} \varphi(\mathcal{O}) & = & (1, 1, 1) & \varphi(0, 0) & = & (-1, -5, 5) \\ \varphi(5, 0) & = & (5, 2, 10) & \varphi(-5, 0) & = & (-5, -10, 2) \\ & & \varphi(-4, 6) & = & & (-1, -1, 1) \end{array}$$

Since φ is a homomorphism, we can multiply these tuples to get other tuples that must be in $Im(\varphi)$. This implies that there are rational points on E such that

$$(1, 5, 5), (-5, -2, 10), (5, 10, 1) \in Im(\varphi)$$

Now we use the method of 2-descent. Write the linear factors of $x^3 - 25x$ as

$$x = au^2 \quad x - 5 = bv^2 \quad x + 5 = cw^2$$

for $a, b, c, u, v, w \in \mathbb{Q}$. From Lemma 1, we see that

$$a, b, c \in \{\pm 1, \pm 2, \pm 5, \pm 10\} \pmod{\mathbb{Q}^{\times 2}}$$

Since abc is a square, once we have chosen values for a and b , the value of c is automatically determined. There are 64 possible choices for (a, b) . We've found 8 so far.

Consider the following inequalities

$$x - 5 < x < x + 5 \quad \Rightarrow \quad bv^2 < au^2 < cw^2$$

Without too much work, we can show that a and b must have the same sign. So this reduces our 64 choices to 32. Consider a special case: $(a, b) = (2, 1)$. Substituting into our 2-descent gives

$$x = 2u^2 \quad x - 5 = v^2 \quad x + 5 = 2w^2$$

and rearranging gives

$$2u^2 - v^2 = 5 \quad 2w^2 - 2u^2 = 5$$

Due to space concerns, we will only outline the remainder of this example. For more details, see [10], Chapter 8, Section 4.

We can show that u, v must have odd denominators, which allows us to work modulo powers of 2. Some clever arguments then allow us to derive a contradiction. Thus, the choice $(a, b) = (2, 1)$ is impossible. If we consider two more special cases, namely $(a, b) = (5, 1)$ and $(a, b) = (10, 1)$, and work modulo powers of 5, we can derive two more contradictions. After eliminating these three cases, we can use the fact that φ is a homomorphism to eliminate a total of 24 cases: we have eight cases that work and three that don't, so multiplying these tuples together will give 24 cases that don't work. Thus of the remaining 32 possibilities, only 8 are left – the ones we have already found. So $|\varphi(E(\mathbb{Q}))| = 8$ and by our formula

$$\left| \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \right| = |\varphi(E(\mathbb{Q}))| = |T| \cdot |\mathbb{Z}_2^r| = |T| \cdot 2^r$$

we see

$$8 = |T| \cdot 2^r = 4 \cdot 2^r \quad \Rightarrow \quad r = 1$$

So the rank of E is one and thus $E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}$.

11 Birch and Swinnerton-Dyer Conjecture

Due to the complicated nature of the material in this section, we will only state the Birch and Swinnerton-Dyer conjecture and its implications in rational point finding without delving into too much of the reasoning and theory behind it.

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, $s \in \mathbb{C}$ and p be prime. We define $N_p = | \{ \text{solutions of } y^2 = x^3 + ax + b \pmod{p} \} |$ and $a_p = p - N_p$.

The incomplete¹ L -series of E is

$$L(E, s) = \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

which we consider as a function of the complex variable s . This is known to converge when $\Re(s) > 3/2$. A conjecture by Hasse, now proven (see [11]), predicted that $L(C, s)$ should have an analytic continuation to the entire complex plane. With this fact, we can now present the Birch and Swinnerton-Dyer conjecture:

Conjecture 1 *The Taylor expansion of $L(C, s)$ at $s = 1$ has the form $L(C, s) = c(s - 1)^r + \text{higher order terms}$ with $c \neq 0$ and $r = \text{rank}(E(\mathbb{Q}))$.*

The conjecture asserts that $L(E, s) = 0$ iff $E(\mathbb{Q})$ is infinite. This conjecture can actually be refined by considering the completed L -series of E , denoted $L^*(E, s)$. The refined conjecture then states that $L^*(E, s) \sim c^*(s - 1)^r$ where

$$c^* = |\text{III}(E)| R_\infty w_\infty \prod_{p \mid 2\Delta} \frac{w_p}{|T|^2}$$

See [11] for the definitions of these factors. Some mathematicians are hopeful that a proof of the Birch and Swinnerton-Dyer conjecture will also lead to a proof that the Shafarevich-Tate $\text{III}(E)$ is finite.

The important point to note is that a proof of the refined Birch and Swinnerton-Dyer conjecture will give an effective method of finding generators for $E(\mathbb{Q})$.

12 Concluding Remarks

As we have seen, computing the torsion subgroup of $E(\mathbb{Q})$ is a relatively simple process. We run into problems if the roots of our elliptic curve E become too large. If the roots are large, say $O(n)$ then the discriminant Δ is of size $O(n^3)$. This means that we have many possibilities (usually) for $y^2 \mid \Delta$ – so there are many more computations that need to be performed. However, the more fundamental problem is that we need to factor an integer of size $O(n^3)$ to determine the possibilities for $y^2 \mid \Delta$.

¹This L -series is incomplete because we omit the factors, known as Euler factors, for primes $p \mid 2\Delta$.

The problems of computing the rank of $E(\mathbb{Q})$ and a list of generators had not been resolved. We have presented an illustrative version of “descent”, a generalization of Fermat’s method of infinite descent. Descent usually works well (in practice) when a, b , the coefficients of the elliptic curve, are not too large. In general, though, the success of descent depends on a conjecture that a certain associated group to E is finite². It has been shown that this group is finite for infinitely many elliptic curves with a certain property (see [6]).

In general, it is difficult to predict the rank of an elliptic curve from its equation. Consider the rather innocent looking elliptic curve $y^2 = x^3 + 877x$. It has rank 1, but the group of rational points is generated by the points $(0, 0)$ and the point with x coordinate

$$x_0 = \left(\frac{612, 776, 083, 187, 947, 368, 101}{7, 884, 153, 586, 063, 900, 210} \right)^2$$

We have presented curves with ranks 0,1 and it is not too difficult to find curves with ranks 2, 3, and 4. However, it is very hard to find curves with larger ranks – in fact, it’s still an open problem as to whether there exists an elliptic curve with an arbitrary rank. In 2000, Martin-McMillen showed that for

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116$$

over \mathbb{Q} we have $E(\mathbb{Q}) \cong \{0\} \times \mathbb{Z}^{24}$ (see [2]). This is the highest known rank to date for an elliptic curve over \mathbb{Q} .

²The Shafarevich-Tate group $\text{III}(E)$.

References

- [1] G. Billing and K. Mahler. “On Exceptional Points on Cubic Curves”. London Journal of Mathematics, Vol. 15 (1940), pp. 32-43.
- [2] A. Dujella. “High Rank Elliptic Curves with Prescribed Torsion”. <<http://www.math.hr/~duje/tors/tors.html> >
- [3] I. Kiming. “Theorem of Nagell-Lutz: The Decisive Lemma”. <http://www.math.ku.dk/~kiming/courses/2003/intro.ell/nagell_lutz2.pdf >
- [4] F. Lemmermeyer. “General 2-Descent”. <<http://www.fen.bilkent.edu.tr/~franz/ta/ta-2d.pdf> >
- [5] J. S. Milne. *Elliptic Curves*. “Chapter 8: Torsion Points”. <<http://www.jmilne.org/math/CourseNotes/math679.pdf> >
- [6] B. Poonen. “Computing Rational Points on Curves”. <<http://math.berkeley.edu/~poonen/papers/millennial.pdf> >
- [7] Á. L. Robledo. “Finding Points on Elliptic Curves: Very Explicit Methods”. <<http://math.bu.edu/people/alozano/finding%20points.pdf> >
- [8] E. F. Schaefer and M. Stoll. “How to do a p -Descent on an Elliptic Curve”. Trans. Amer. Math. Soc. Vol. 356, No. 3. pp. 1209-1231.
- [9] J. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer: New York. 1992.
- [10] L. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC: New York. 2003.
- [11] A. Wiles. “The Birch and Swinnerton-Dyer Conjecture”. <http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/ >