Lecture Notes on Rational Points on Elliptic Curves

Shiyue Li

Mathcamp 2018

Acknowledgment: Over the course of Rational Points on Elliptic Curves class (Week 4) in Canada/USA Mathcamp 2018, these notes are improved and completed via conversations with Mira, Aaron, students in the class, and other Mathcamp staff. The notes are based on a very nice treatment of rational points on elliptic curves in [ST15].

Contents

1 Cubic Curves

1.1 Diophantine Equations

The theory of Diophantine equations is a branch of number theory that finds integral or rational solution of polynomial equations.

Some natural questions that mathematicians want to ask are:

- Are there integral solutions to these equations? If so, how many are there?
- Are there rational solutions to these equations? If so, how many are there?
- If any integral or rational solution exists, can we express it in terms of the coefficients of the equation?

Example 1.1. The vanilla flavor of Diophantine equations are in the form of

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

where a_i's are integers. By Rational Root Theorem, if $\frac{p}{q}$ is a rational solution of the equation above, we have q divides a_n and p divides a_0. This gives us list of candidates to plug in and check.

For Diophantine equations in two variables, things can be more complicated.

Example 1.2. Consider the linear equation in two variables $ax + by = c$ for $a, b, c \in \mathbb{Z}$. If $\gcd(a, b)$ divides c. We consider the set of all positive numbers of the form

$$S = \{ax + by : x, y \in \mathbb{Z}\}$$

which by well-ordering principle, has a smallest element d. We can show by Euclidean Algorithm that d is the $\gcd(a, b)$ and d divides all $s \in S$. Therefore, we have infinitely many integral solutions if $\gcd(a, b)$ divides c; otherwise, we have no integral solutions.

There are infinitely many rational solutions to this equation once we see the equation as

$$y = -\frac{ax}{b} + c,$$

since every rational number x will give a rational y.

What about Diophantine equations of degree 2?

Example 1.3. Let us find all rational solutions to the equation $x^2 + y^2 = 1$.

We need to convince ourselves that if a line ℓ passes through a rational point P on the circle C and has rational slope t, then ℓ must meet the circle C again at another rational point Q.

Pick a point $P = (1, 0)$ and let $t \in \mathbb{Q}$ be the slope of the line $\ell : y = tx + 1$ that passes through P. Solving the system of equations

$$\begin{cases} y = tx + 1, \\ x^2 + y^2 = 1, \end{cases}$$

we get $x = \frac{-2t}{1+t^2}$, and $y = \frac{1-t^2}{1+t^2}$. As t varies over different rational numbers, x, y will take in different rational values.

Definition 1.4. The set of all real solutions to an equation $f(x, y) = 0$ gives a curve C in $\mathbb{R}^2$ called **algebraic curve**. Algebraic curves of degree 2 are called **conics** and algebraic curves of degree 3 are called **cubics** or **cubic curves**.

Remark 1.5.

- Now algebraic expressions $f(x, y)$ and geometric objects in the plane are in correspondence. Throughout the course, we will use the language – "let C be a curve $f(x, y)$" or "we have a curve $C : f(x, y)$" – to indicate that C contains the set of real points in $\mathbb{R}^2$ whose coordinates (x, y) satisfies the equation $f(x, y) = 0$.
- Elliptic curves do not have much to do with ellipses (a family of conic sections that are given by quadratic equations). They are named so because of their first appearance in calculation of arc length of ellipses.

This course will walk you through this beautiful subject of cubic curves, and we will primarily focus on finding the rational points on cubic curves. In the Example above, we see that given a rational point P on a cubic curve, we can draw the tangent line at P, and take the third point of the intersection of the line with the cubic, thereby finding more rational points. This "geometric operation" later on gives an abelian group structure to the set of all rational points on a cubic curve, which is the substance of the celebrated Mordell's Theorem.

1.2 The Weierstrass Normal Form, Singular and Non-Singular Curves

For every cubic curve:

$$C : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

for all $a, b, c, d, e, f, g, h, i, j$ in $\mathbb{Q}$. we can use projective geometry to show that there is a simpler-looking curve in **Weierstrass normal form**:

$$C' : y^2 = f(x) = x^3 + a_1x^2 + a_2x + a_3$$

such that C and C' are **birationally equivalent**. We won't elaborate what birational equivalence means, but we know that it is an equivalence relation on the set of all cubic curves. So we only need to study representatives of each equivalence class that look as simple as Weierstrass normal form. Another nice thing about the normal form is that, the curve is symmetric around x-axis.

Question 1.6. What do we know about real roots of $f(x)$?

Analyzing the roots of $f(x)$, we have the following situations:

(1) If $f(x)$ has one real root α, $C : f(x) = (x-\alpha)(x^2+\beta x+\gamma) = 0$ for some real number $\alpha, \beta, \gamma \in \mathbb{R}$. C has one component.

(2) If $f(x)$ has three real roots, $C = f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ for $\alpha, \beta, \gamma \in \mathbb{R}$.

- If all three of the real roots are distinct, C has two components.
- If two of the real roots are the same, say $\alpha = \beta$ without loss of generality, then in order to fully understand the geometry of C, we inspect the tangent line of C at each point of C. Let us rewrite $y^2 - f(x) = F(x,y)$ and the partial derivatives with respect to x, y are

$$\frac{\partial F(x,y)}{\partial x} = -f'(x) \text{ and } \frac{\partial F(x,y)}{\partial y} = 2y.$$

  Since $f(x) = (x-\alpha)^2(x-\gamma) = y^2$, then $y = 0$ at $x = \alpha$ and $-f'(\alpha) = -(\alpha-\alpha)^2 - 2(\alpha-\alpha)(\alpha-\gamma) = 0$, which implies that the partial derivatives are 0. This means that C has an **singularity** at $(\alpha, 0)$ and we say that C is a singular curve with **distinct tangent directions** or **a self-intersection**.
- If all three roots are the same, then by the same reasoning as above, C is a singular curve with **a cusp**.

Mordell's Theorem will not hold for these singular curves, and it is not a pity since finding rational points on a singular curve is in fact easy. To find rational points on a singular curve is the same as conics. We can project the curve to a line from the singular point, and a projecting line will only path through one other point on the curve. Hence we have a one-to-one correspondence from rational points on a singular curve to a rational points on a line; see Exercises for Day 1 for examples.

Thus we are only interested in non-singular cubic curves and they have a special name.

Definition 1.7. If a cubic curve $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ has distinct complex roots, then we call this curve an **elliptic curve**.

1.3 The Group Law on Elliptic Curves

In fact, all the points on an elliptic curve form an abelian group. Before we do this, let us admit a few facts from projective geometry that we won't elaborate here (talk to me at TAU if you are interested).

Assumption 1.8. (1) The point at infinity O is a rational point.

(2) Our non-singular curve C contains all the points on the xy-plane and the point at infinity O.

(3) Every line meets the cubic in three points:

- The line at infinity meets the cubic at O three times.
- A vertical line meets the cubic at two points in the xy plane and also at the point O.
- Any non-vertical line meets the cubic in three points in the xy plane. But we have to be careful here.

Now we can define the group structure.

- Addition: for any $P, Q \in C$, draw a line through P and Q. The line will intersect with the cubic at a third intersection. Denote the third intersection $P * Q$. Draw another line through $P * Q$ and O and the line will intersect with the cubic at the point $O * (P * Q)$. This is $P + Q$; or more precisely, we have

$$P + Q = O * (P * Q).$$

- From this formula, we see that for any $P \in C$,

$$O + P = P + O = O * (O * P) = O * (P * O) = P.$$

  So O is the identity of the group.

- What is the negative of a point P on C?

- Associativity of this group law will also hold.
- Addition is abelian.

Therefore, we have obtained a group structure on the points on an elliptic curve.

1.4 Exercises for Day 1

The projection of a singular cubic curve onto a line is one-to-one. Hence the rational points on a singular cubic can be put in a one-to-one correspondence with rationals on the line. The following two exercises are two examples.

Exercise 1.9. Find all the rational points of the singular cubic curve $C(y^2 = x^3)$ by parametrizing all rational x and y using a rational t.

Exercise 1.10. Find all the rational points on the singular cubic curve $C(y^2 = x^2(x+1))$ by letting $r = \frac{y}{x}$ for $(y, x) \neq (0, 0)$.

The following exercises help you understand the group law on elliptic curves!

Exercise 1.11. Show that the group law is associative: for any $P, Q, R \in C$, $(P + Q) + R = P + (Q + R)$.

Exercise 1.12. If P and Q are distinct rational points in the xy-plane, prove that the line conncecting them is a rational line.

Exercise 1.13. Let C be a non-singular cubic curve. Let $C(\mathbb{Q}), C(\mathbb{R}), C(\mathbb{C})$ be the rational points, real points, complex points on C. Show that each of $C(\mathbb{Q}), C(\mathbb{R}), C(\mathbb{C})$ is an additive group under the addition defined in the group law.

This exercise will give you a formula called "Duplication Formula", which will be an important tool later.

Exercise 1.14. Compute an explicit expression for the coordinates of $2P$ in terms of the coordinates for P on $C : y^2 = x^3 + ax^2 + bx + c$.

Exercise 1.15. Let $C : y^2 = x^3 + ax^2 + bx + c$ be a non-singular cubic curve. Let $P = (x, y)$ be a point on C. Find a polynomial in x whose roots are the x coordinates of the points $Q = (x, y)$ satisfying $3Q = O$. [1]

Exercise 1.16. Consider the point $P = (3, 8)$ on the cubic curve $y^2 = x^3 - 43x + 166$. Compute $P, 2P, 3P, 4P$ and $8P$. What do you find?

This exercise shows you an example of birational transformation.

Exercise 1.17. If u, v satisfies the relation $u^3 + v^3 = \alpha$, then the quantities $x = \frac{12\alpha}{u+v}$, $y = 36\alpha\frac{u-v}{u+v}$ satisfies $y^2 = x^3 - 432\alpha^2$. This gives a birational transformation from the curve $u^3 + v^3 = \alpha$ to the curve $y^2 = x^3 - 432\alpha^2$

[1] Hint: The relation $3Q = O$ can be translated into $2Q = -Q$.

2 A Hike to Mordell's Theorem

> Let's wander where the WiFi is weak
>
> Anonymous

Throughout, we assume our non-singular cubic curve C is given by a Weierstrass form:

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

where a, b, c are rationals. Recall that the "non-singularity" condition translates into the case that the elliptic curve $C : y^2 = f(x)$ crosses x-axis at exactly one or three distinct points; in other words, $f(x)$ has three distinct roots (real or complex). Recall that the points on C have a group structure and O is the identity element of the group.

Yesterday, we have seen that $C \cup \{O\}$ is an abelian group.

Definition 2.1. An element P of any group element is said to have order n if

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}} = O$$

and $mP \neq O$ for all $1 \leq m < n$. If $n < \infty$, we say that P has **finite** order; if $n = \infty$, P has **infinite** order.

To study furthermore about the structure of points on C, we can ask ourselves the following questions.

- Are there points of finite orders?
- Are there points of order 2?
- Are there points of order 3?

To answer the first question, we want to find $P \in C$ such that $2P = O$ and $P \neq O$, which is the same as $P = -P$. These are the points on C that are lying on the x-axis or floating in the vast space of $\mathbb{C}$ that we cannot draw on xy-plane. But if we include these complex roots, we get 4 points of order 2:

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

where $\alpha_1, \alpha_2, \alpha_3$ are real or complex.

Question 2.2. What is the relation between the three points plus the point O at infinity?

Proposition 2.3. *The set of points π_2 of order 2 on $C : y^2 = f(x)$ can be described as follows.*

(i) If we consider $\pi_2 \subseteq C(\mathbb{C})$, then $\pi_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, the Klein Four Group.

(ii) If we consider $\pi_2 \subseteq C(\mathbb{R})$, then $\pi_2 \cong \mathbb{Z}_2$ (if $f(x)$ has 1 real root) or $\pi_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (if $f(x)$ has 3 real roots).

(iii) If we consider $\pi_2 \subseteq C(\mathbb{Q})$, then $\pi_2 \cong \mathbb{Z}_2$ (if $f(x)$ has 1 real root) or $\pi_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (if $f(x)$ has 3 real roots), or $\pi_2 = \{O\}$ is trivial.

To answer the second question (cf. Exercises for Day 1), we want to find points P such that $3P = O$ but $P \neq O$ and $2P \neq O$. If such point $P = (x, y)$ exists, then $2P = (x', y') = -P$ implies that $x = x'$.

Using the "Duplication Formula" that you found out in Exercises in Day 1

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4bc}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Then x is a root of the polynomial

$$p(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

From these calculation you can see that the computation of the Mordell-Weil group could be a total mess.

2.1 Mordell's Theorem for Curves with a Rational Point of Order Two

In this class, we state Mordell's Theorem for non-singular curves with a rational point of order two and see a bunch of examples that will illustrate the ideas.

Theorem 2.4. *Let C be a non-singular cubic curve given by an equation*

$$C : y^2 = x^3 + ax^2 + bx,$$

where a and b are integers and C has a rational point of order two. Then the group of rational points, or Mordell-Weil group, $C(\mathbb{Q})$ is a finitely generated abelian group.

Theorem 2.5 (Structure Theorem for Finitely Generatedy Abelian Groups)**.** *A finitely generated abelian group G is isomorphic to*

$$\underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ is called rank}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

where each p_i is a prime and each α_i is a positive integer.

Mordell's Theorem gives us some hope in fully describing the rational points on elliptic curves.

Example 2.6. For $C : y^2 = x^3 - 5x$, $C(\mathbb{Q})$ has rank 1.

Example 2.7. For $C : y^2 = x^3 + x$ and $C : y^2 + 4x$, $C(\mathbb{Q})$ are finite.

Example 2.8. For $C : y^2 = x^3 + px$ where $p \equiv 7, 11 \pmod{16}$, $C(\mathbb{Q})$ is finite.

In this section, we prove Mordell's Theorem that the group of rational points on a non-singular cubic is finitely generated for curves that have a rational points of order 2 to start with. To do this, we need to define some useful tools to help us understand rational points on this cubics.

Throughout, we work with non-singular cubic curves $C : y^2 = x^3 + ax^2 + bx + c$ for $a, b, c \in \mathbb{Z}$.

2.2 Heights

Some rational points are complicated, some of them are not.

Definition 2.9. Let $x = \frac{p}{q}$ be a rational number written in reduced terms. Then the **height** $H(x)$ is the maximum of the absolute values of the numerator and the denominator. That is,

$$H(x) = H\left(\frac{p}{q}\right) = \max\{|p|, |q|\}.$$

Question 2.10. Given positive integer m, how many rationals x are there such that $H(x) \leq m$?

Definition 2.11. For a rational point $P = (x, y)$ on a curve C, we define the **height** of P to be the height of its x-coordinate. For calculation convenience, we define "small height" $h(P)$ to be $\log(H(P))$.

Note that $h(P)$ is a non-negative real number, so we are really on a hike.

Lemma 2.12. *Given a non-negative real number m, the set*

$$\{P \in C(\mathbb{Q}) : h(P) \leq m\}$$

is finite.

Lemma 2.13. *Fix P_0 on C. For all $P \in C(\mathbb{Q})$, there exists a constant k_0 that only depends on P_0, a, b, c such that*

$$h(P + P_0) \leq 2h(P) + k_0.$$

Lemma 2.14. *For all $P \in C(\mathbb{Q})$, there exists a constant k, that only depends on a, b, c such that*

$$h(2P) \geq 4h(P) - k.$$

Remark 2.15. The lemmas give us a tool to connect group law and height, which is a number theoretic tool. Lemma 2.13 tells us, if you start at a rational point and add another rational point, the height of the result is under control. Lemma 2.14 tells us, if you keeps doubling a point, the height will blow up eventually.

Lemma 2.16. *The index $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite.*

2.3 Descent

In this section, we will outline the proof of Mordell's Theorem using the four lemmas that we presented.

Lemma 4 told us that the index of $2C(\mathbb{Q})$ as a subgroup of $C(\mathbb{Q})$ is finite. Take a representative for each of the finitely many cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$, and call them $Q_1, \ldots, Q_n$.

For each element $P \in C(\mathbb{Q})$, P is in the coset of some Q_{i_1}. That is,

$$P - Q_{i_1} \in 2\Gamma \iff P - Q_{i_1} = 2P_1.$$

Iteratively, we have

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ P_3 - Q_{i_4} &= 2P_4 \\ \cdots . \end{aligned}$$

For each P_j in the sequence $P_1, P_2, P_3 \ldots$, we have that

$$h(P_j - Q_i) \leq 2h(P_j) + k_i$$

for all $1 \leq i \leq n$. We can let k be the maximum of all k_i's such that

$$h(P_j - Q_i) \leq 2h(P_j) + k_i.$$

Using Lemma 3, we have

$$4h(P_j) \leq h(2P_j) + k' = h(P_{j-1} - Q_{i_j}) + k' \leq 2h(P_{j-1}) + k + k'.$$

Thus we know that

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{1}{4}(k + k').$$

There exists some integer m such that

$$\frac{1}{2}h(P_{m-1}) \leq \frac{3}{4}(k + k'),$$

which gives

$$h(P_m) \leq k + k'.$$

Therefore, $P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m$. Since $h(P_m)$ is bounded and n is finite, P is generated by $\{Q_1, \ldots, Q_n\}$ and points $R \in C(\mathbb{Q})$ such that $h(R) \leq k + k'$, whose union is a finite set.

This method is called the method of infinite descent, originated from Fermat. He used this to show that $x^4 + y^4 = 1$ has no rational solutions with $xy \neq 0$. Maybe this was his idea to show that $x^n + y^n = 1$ for any $n \geq 3$. But the margin was apparently too small for an infinite descent. Who knows.

2.4 Exercises for Day 2

The exercises today will walk you through proving some key steps of the lemmas that we used in class. Throughout, let $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ where a, b, c are integers.

Exercise 2.17. Convince yourself that Lemma 2.12 is true.

Exercise 2.18. To prove Lemma 2.13, we want to study the relationship between P, P_0, and $P + P_0$ for $P, P_0 \in C(\mathbb{Q})$. First we notice that the lemma is trivial if $P_0 = O$, and so we let $P_0 = (x_0, y_0) \neq O$. Let $P = (x, y) \in C(\mathbb{Q})$, and we can write

$$x = \frac{m}{M} \text{ and } y = \frac{n}{N}$$

such that they are in reduced form with $M > 0$ and $N > 0$. We will show that $M^3 = N^2$.

(i) Use the fact that $P \in C$ to deduce that N^2 divides M^3.

(ii) Show that M divides $N^2 m^3$ and deduce that M divides N^2.

(iii) Show that M^2 must divides $N^2 m^3$, and deduce that M must divide N.

(iv) Show that M^3 divides $N^2 m^3$, so M^3 must divide N^2.

(v) Now we have $N^2 | M^3$ and $M^3 | N^2$ so $M^3 = N^2$. Since we showed that $M | N$, we can let $r = \frac{N}{M}$. Deduce the following equations.

$$r^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M$$

and

$$r^3 = \frac{N^3}{M^3}$$

Therefore, we can have

$$x = \frac{m}{r^2} \text{ and } y = \frac{n}{r^3}.$$

(vi) Substitute the new expressions for x and y back into $C : y^2 = f(x)$ and clear the denominator. Use triangle inequality to show that

$$|n| \leq \sqrt{1 + |a| + |b| + |c|}H(P).$$

That is, we have bounded the numerator of the y-coordinate of P in terms of $H(P)$.

(vii) Now we are ready to prove the lemma statement. Let $P + P_0 = (s, t)$, Express s in terms of coordinates of P, P_0 and a, b, c and when you get some term involving $y^2 - x^3$, replace it with $ax^2 + bx + c$. Eventually you get something like

$$s = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

where all the coefficients are integers and are in terms of a, b, c, x_0, y_0 (that's good!)

(viii) Substituting $x = \frac{m}{r^2}$, and $y = \frac{n}{r^3}$ into the equation and clearing the denominator, conclude that

$$H(P + P_0) = H(s) \leq \max(|AK| + |B| + |C| + |D|, |E| + |F| + |G|)H(P)^2.$$

(ix) Taking the log will give us the desired result.

2.5 Homomorphisms of Mordell Weil Groups

> The definition of a good mathematical problem is the mathematics it generates rather than the problem itself.
>
> Andrew Wiles

In Exercises for Day 2, we proved Lemma 2.12 and Lemma 2.13. The proofs of Lemma 2.14 use similar ideas as Lemma 2.13 and are rather too technical to be fun. Today we will outline a proof of Lemma 2.16, which states: The index $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite.

To study $2C(\mathbb{Q})$, we want to see how any point $P \in C$ as mapped to $2P$. Recall the "Duplication Formula" that you found out in Exercises in Day 1

$$\begin{aligned} P = (x,y) &\mapsto 2P \\ x &\mapsto \frac{x^4 - 2bx^2 - 8cx + b^2 - 4bc}{4x^3 + 4ax^2 + 4bx + 4c}. \end{aligned}$$

This map has degree 4. The strategy of the proof is the following.

(i) We construct a degree-2 map ϕ from C to $\overline{C}$ and a degree -2 map $\overline{\phi}$ from $\overline{C}$ to $\overline{\overline{C}}$.

(ii) We show that C and $\overline{\overline{C}}$ are isomorphic as cubic curves, hence having the isomorphic $C(\mathbb{Q})$.

(iii) The composition of $\overline{\phi} \circ \phi$ is a degree 4 map and induces a group homomorphism $C(\mathbb{Q}) \to 2C(\mathbb{Q})$.

(iv) Use a lemma to show Lemma 4.

Lemma 2.19. *Let A and B be abelian groups, and consider two homomorphisms $\phi : A \to B$ and $\overline{\phi} : B \to A$. Suppose that for all $a \in A$, and $b \in B$*

$$\overline{\phi} \circ \phi(a) = 2a \text{ and } \phi \circ \overline{\phi}(b) = 2b.$$

Suppose that $[B : \phi(A)]$ is finite, $[A : \overline{\phi}(B)]$ is finite, then

$$[A : 2A] \leq [A : \overline{\phi}(B)][B : \phi(A)].$$

Example 2.20. Let $A = \mathbb{Z} \times \mathbb{Z}$ and $B = \mathbb{Z} \times 2\mathbb{Z}$. Let $\phi : A \to B$ be $(a,b) \to (a,2b)$ and $\overline{\phi} : B \to A$ be $(a,2b) \mapsto (2a,2b)$. Then

$$\overline{\phi} \circ \phi((a,b)) = (2a,2b) \text{ and } \phi \circ \overline{\phi}((a,2b)) \mapsto (2a,4b).$$

Notice that

$$[\mathbb{Z} \times 2\mathbb{Z} : \mathbb{Z} \times 2\mathbb{Z}] = 1 \text{ and } [\mathbb{Z} \times \mathbb{Z} : 2\mathbb{Z} \times 2\mathbb{Z}] = 4,$$

and we can check that

$$4 = [\mathbb{Z} \times 2\mathbb{Z} : 2\mathbb{Z} \times 2\mathbb{Z}] \leq [\mathbb{Z} \times \mathbb{Z} : 2\mathbb{Z} \times 2\mathbb{Z}][\mathbb{Z} \times \mathbb{Z} : 2\mathbb{Z} \times 2\mathbb{Z}] = 4.$$

Proof. Similar to the proof of Mordell's Theorem, we will take advantage of the fact that $[A : \overline{\phi}(B)]$ and $[B : \phi(A)]$ are finite.

Since $\overline{\phi}(B)$ has finite index in A, we can find elements $a_1, \ldots, a_n$ representing the finitely many cosets of $\overline{\phi}(B)$ in A. Since $\phi(A)$ has finite index in B, we can find elements $b_1, \ldots, b_m$ to represent the finitely many cosets of $\phi(A)$ in B.

Recall our goal is to show that the number of cosets of $2A$ in A is finite. This amounts to showing that for any arbitrary $a \in A$, a can be written as the sum of some element that can be chosen from only finitely many elements in A and some element in $2A$.

Since $\overline{\phi}(B)$ is finite-index subgroup of A, there exists a coset representative a_i such that

$$a - a_i \in \overline{\phi}(B) \iff a - a_i = \overline{\phi}(b),$$

for some $b \in B$. Since $\phi(A)$ has finite index in B, there exists a coset representative b_j such that $b - b_j \in \phi(A) \iff b - b_j = \phi(a')$. Therefore,

$$a = a_i + \overline{\phi}(b) = a_i + \overline{\phi}(\phi(a') + b_j) = a_i + \overline{\phi}(b_j) + 2a'.$$

Since the options for the combination of a_i and $\overline{\phi}(b_j)$ are finite, $2A$ is indeed a finite index subgroup in A. □

To use this Lemma 2.19, we need to construct $\phi : C(\mathbb{Q}) \to \overline{C}(\mathbb{Q})$ and $\overline{\phi} : \overline{C}(\mathbb{Q}) \to C(\mathbb{Q})$ such that

(1) $\overline{\phi} \circ \phi$ and $\phi \circ \overline{\phi}$ are duplication maps.

(2) $[C(\mathbb{Q}) : \overline{\phi}(\overline{C}(\mathbb{Q}))]$ is finite.

(3) $[\overline{C}(\mathbb{Q}) : \phi(C(\mathbb{Q}))]$ is finite.

Now we start our really long journey of proving the last statements. First we recall that our $C : y^2 = f(x) = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}$ is a non-singular curve with a rational point of order 2. This means that $f(x)$ have a rational root α. Since $f(x)$ is a polynomial with integer coefficients and leading coefficient 1, α must be an integer, by Rational Root Theorem. Making a change of coordinates, we can move $(\alpha, 0)$ to origin, and the curve of interst is now in the form of

$$C : y^2 = f(x) = x^3 + ax^2 + bx$$

where $a, b \in \mathbb{Z}$.

For Step (1), we define a map between curves first. For $C : y^2 = x^3 + ax^2 + bx$, define a "conjugate curve"

$$\overline{C} : y^2 = x^3 + (-2a)x^2 + (a^2 - 4b)x.$$

Let $\phi : C \to \overline{C}$ be defined by

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & P \neq O, (0,0), \\ O & P = O \text{ or } (0,0). \end{cases}$$

The kernel of ϕ is $\{O, (0,0)\}$. Let $\overline{\phi} : \overline{C} \to C$ be defined by

$$\overline{\phi}(P) = \begin{cases} \left(\frac{y^2}{4x^2}, \frac{y(x^2-b)}{8x^2}\right), & P \neq O, (0,0), \\ O & P = O \text{ or } (0,0). \end{cases}$$

The kernel of ϕ is $\{O, (0,0)\}$. One can check that

(i) $\phi, \overline{\phi}$ are group homomorphisms.

(ii) $\phi \circ \overline{\phi}$ ande $\overline{\phi} \circ \phi$ are duplication maps.

(iii) $\phi_{C(\mathbb{Q})}$ and $\overline{\phi}_{\overline{C}(\mathbb{Q})}$ is a homomorphism between $C(\mathbb{Q})$ and $\overline{C}(\mathbb{Q})$.

To prove Lemma 2.16, we need to show that

- $[\overline{C}(\mathbb{Q}) : \phi(C(\mathbb{Q}))]$ is finite.
- $[C(\mathbb{Q}) : \overline{\phi}(\overline{C}(\mathbb{Q}))]$ is finite.

It suffices to show one of these since the other is given by the same map.

We proceed by proving the second one:

$$[C(\mathbb{Q}) : \overline{\phi}(\overline{C}(\mathbb{Q}))] < \infty.$$

Showing this amounts to showing that there is an injective homomorphism from the quotient group $C(\mathbb{Q})/\overline{\phi}(\overline{C}(\mathbb{Q}))$ into a finite group.

Recall our notation from last time,

$$\mathbb{Q}^* = \{\text{multiplicative group of } \mathbb{Q}\}, \text{ and } (\mathbb{Q}^*)^2 = \{x^2 : x \in \mathbb{Q}^*\}.$$

Define the map

$$\alpha : C(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$$

by

$$\begin{aligned} \alpha(O) &= 1 \pmod{\mathbb{Q}^{*2}} \\ \alpha(\xi) &= b \pmod{\mathbb{Q}^{*2}} \\ \alpha(x,y) &= x \pmod{\mathbb{Q}^{*2}}, x \neq 0. \end{aligned}$$

It is not obvious that α is a group homomorphism, but you will show this in the homework.

Proposition 2.21. *The kernel of α is image of $\overline{\phi}(\overline{C}(\mathbb{Q}))$.*

Proof. The kernel of α is the set of elements in $C(\mathbb{Q})$ that get sent to $\mathbb{Q}^{*2}$. The definition of α is as follows.

$$\begin{aligned}\alpha(O) &= 1 \pmod{\mathbb{Q}^{*2}}\\ \alpha(\xi) &= b \pmod{\mathbb{Q}^{*2}}\\ \alpha(x,y) &= x \pmod{\mathbb{Q}^{*2}}, x \neq 0.\end{aligned}$$

We describe points in the image of ϕ.

(i) $O \in \overline{\phi}(\overline{C}(\mathbb{Q}))$ by definition of $\overline{\phi}$.

(ii) $\xi = (0,0) = (\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}) \in \overline{\phi}(\overline{C}(\mathbb{Q}))$ if and only if the polynomial $\overline{f}(x)$ has a nonzero rational solution. This implies that in the factorization of $f(x) = x(x^2 + \overline{a}x + \overline{b})$, $x^2 + \overline{a}x + \overline{b}$ has a rational solution, and thus

$$\frac{-\overline{a} \pm \sqrt{\overline{a}^2 - 4\overline{b}}}{2}$$

is rational. This holds if and only if $\overline{a}^2 - 4\overline{b}$ is a square of a rational number if and only if

$$4a^2 - 4(a^2 - 4b) = 16b \in \mathbb{Q}^{*2} \iff b \in \mathbb{Q}^{*2}.$$

(iii) $P = (x,y) \in \overline{\phi}(\overline{C}(\mathbb{Q}))$ with $x \neq 0$ if and only if x is a square square of a rational number.

□

Proposition 2.22. *The image of α is contained in the subgroup $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements*

$$\{\pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} : \beta_i = 0 \text{ or } 1, p_i \text{ divides } b\},$$

Proof. Recall in Exercises for Day 1, we know that for every point $P = (x,y) \in C(\mathbb{Q})$ with $x \neq 0$, we can write

$$x = \frac{m}{r^2}, \text{ and } y = \frac{n}{r^3}$$

in their reduced form where $r = \frac{N}{M}$ in reduced form and where M, N are the original denominators for x, y in reduced form. You also remember in Exercises in Day 1 that if you plug in the point (x,y) in the polynomial equation of C and clear the denominator, you get

$$n^2 = m^3 + am^2r^2 + bmr^4 = m(m^2 + amr^2 + br^4).$$

Consider the divisors of m, they either divide $m^2 + amr^2 + br^4$ or don't divide $m^2 + amr^2 + br^4$. Those divisors of m that divide $m^2 + amr^2 + br^4$ must divide b since m and

r are coprime. Those divisors of m that do not divide $m^2 + amr^2 + br^4$ must have even power in the factorization of m. Therefore,

$$\alpha(P) = x = \frac{m}{r^2} \equiv m \equiv \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} \pmod{\mathbb{Q}^{*2}}$$

where p_i are divisors of b, and $\beta_i = 0$ or 1 for all i.

If $P = (0,0)$, then $\alpha(T) = b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} \pmod{\mathbb{Q}^{*2}}$ where p_i are divisors of b, and $\beta_i = 0$ or 1 for all i. □

Since Lemma 2.16 is true, we have completed the proof of Mordell's Theorem!!

2.6 Exercises for Day 4

Exercise 2.23.

These exercises will walk you through the proof of α is a group homomorphism from $C(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Exercise 2.24. Show that for any point $P = (x, y) \in C(\mathbb{Q})$,

$$\alpha(-P) = \alpha(P)^{-1} \pmod{\mathbb{Q}^{*2}}.$$

Exercise 2.25. Show that if $y = rx + s$ is a line that passes through C in three general points (not including the infinity P), the x-coordinate of the three points x_1, x_2, x_3 satisfy a cubic equation:

$$x^3 + Ax^2 + Bx + C = 0$$

. What are A, B, C in terms of r, s, a, b, c?

Exercise 2.26. Using the last exercise, what can you say about $x_1x_2x_3$? Deduce that if $P_1 + P_2 + P_3 = O$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \pmod{\mathbb{Q}^{*2}}$. This combines with the first exercise shows you that α is indeed a group homomorphism.

Before we compute a concrete example, let us think about an algorithm to compute the rank of Mordell-Weil group.

Exercise 2.27. Recall that the structure theorem for finitely generated abelian group and Mordell's Theorem combined tell us that

$$C(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}_{{p_1}^{\alpha_1}} \oplus \mathbb{Z}_{{p_2}^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_n}^{\alpha_n}}$$

where p_i are primes, α_i are positive integers. Write out $C(\mathbb{Q})/2C(\mathbb{Q})$. What is $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ (a number), depending on p_i for all i?

Exercise 2.28. Consider the set of elements P such that $2P = O$ in $C(\mathbb{Q})$ (Caution! These are not just elements of order 2). Denote this group as H. How would you describe it using $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ and the rank r of $C(\mathbb{Q})$?

Exercise 2.29. What is the cardinality of H from last exercise, depending on a, b in the polynomial of the curve C?

Exercise 2.30. Assuming the condition for H to have the largest cardinality holds, we can obtain the following formula

$$2^r = \frac{|\alpha(C(\mathbb{Q}))||\overline{\alpha}(\overline{C}(\mathbb{Q}))|}{4}.$$

In this formula, $\overline{\alpha} : \overline{C}(\mathbb{Q})$ is defined similarly as α but takes input from $\overline{C}(\mathbb{Q})$. You don't have to deduce this formula. This is just for you to read for your own sanity and for the next exercises. You are welcome to think about why this formula is true and talk to Shiyue about it.

This exercise will walk you through an example of computing the rank of a Mordell-Weil group $C(\mathbb{Q})$ and $C(\mathbb{Q})$ for $C : y^2 = x^3 - x$ and $\overline{C} : y^2 = x^3 + 4x$. This exercise will also help you understand the consequence of Mordell's Theorem.

Exercise 2.31. The above exercises tell us that we need to calculate cardinality of $\alpha(C(\mathbb{Q}))$ and $\overline{a}(\overline{C}(\mathbb{Q}))$ to get a hold of the rank. The cardinality of $\alpha(C(\mathbb{Q}))$ and $\overline{a}(C(\mathbb{Q}))$ depends on factors of $b, \overline{b}$, by Proposition 2.22.

- What is $a, b, \overline{a}, \overline{b}$ in this case?
- How many ways of factorization that satisfies Proposition 2.22 does $b, \overline{b}$ have?
- What are the points in $C(\mathbb{Q})$ that get sent to these factorizations?

Exercise 2.32. Do the same thing for $\overline{\alpha}(\overline{C}(\mathbb{Q}))$.

Exercise 2.33. Deduce that $C(\mathbb{Q})$ and $\overline{C}(\mathbb{Q})$ is finite.

3 Torsions

Given Mordell's Theorem and the structure theorem of finitely generated abelian groups, we have

$$C(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ is called rank}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}}.$$

The rank r of a general $C(\mathbb{Q})$ can be incredibly hard to compute, despite existence of ways to compute for specific curves. This section we study the finite part or the torsion part of $C(\mathbb{Q})$.

Theorem 3.1. *Let $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ where $a, b, c \in Z$ be a non-singular cubic curve. Recall that the discriminant of the cubic polynomial $f(x)$*

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

When $c = 0$ for Mordell's Theorem for curves with a rational point of order two, $D = b^2(a^2 - 4b)$. If $P = (x, y)$ is a rational point of finite order, then

- *x, y are integers;*
- *$y = 0$ and P has order 2; or y divides D.*

Example 3.2. Consider the curve $y^2 = x^3 - x^2 + x$, and we try to find all of its rational points of finite order. Notice that $(0, 0)$ is a rational point of order two. Since $D = b^2(a^2 - 4b) = -3$, the possible y values are $\pm 1, \pm 3$.

$$\begin{aligned} y = \pm 1 &\iff x = 1 \iff P = (1, \pm 1), \quad \text{☺} \\ y = \pm 3 &\iff x^3 - x^2 + x - 9 = 0. \quad \text{☹} \end{aligned}$$

Example 3.3. Consider the curve $C : y^2 = x^3 - x = x(x^2 - 1)$, which we knew from Exercises for Day 4 that the rank of $C(\mathbb{Q})$ is 0. We try to find all of its rational points of finite order. Notice that $(0, 0), (\pm 1, 0)$ are a rational points of order two. Since $D = b^2(a^2 - 4b) = 4$, the possible y values are $\pm 1, \pm 2, \pm 4$.

$$\begin{aligned} y = \pm 1 &\iff x^3 - x - 1 = 0. \quad \text{☹} \\ y = \pm 2 &\iff x^3 - x - 4 = 0. \quad \text{☹} \\ y = \pm 4 &\iff x^3 - x - 16 = 0. \quad \text{☹} \end{aligned}$$

So $C(\mathbb{Q}) \cong \mathbb{Z}_4$.

Recall that one technique that we have seen to prove that a rational number is integer, is to show that the denominator is 1; for example, we used this to show that non-zero rational points of order two for $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ are integers, which allowed us to move one of the integer point on x-axis to the origin. We adopt the same strategy and try to show that if $P = (x, y)$ is a rational point, then the denominators of x, y are 1; in other words, no primes divide the denominators.

To systematically study how primes divide denominators of a rational number, we define the p-order of a rational number as follows.

Definition 3.4. For a prime p, every non-zero rational number q can be written as $\frac{m}{np^\alpha}$, where m, n are coprime, and p does not divide n or m. Then the p**-order** of q is

$$\text{ord}\,(q) = \text{ord}\left(\frac{m}{np^\alpha}\right) = \alpha.$$

Assume we have a rational point $P = (x, y) \in C(\mathbb{Q})$ and some p divides the denominator of x. Then we have

$$x = \frac{m}{np^\alpha} \text{ and } y = \frac{u}{vp^\beta}$$

for some $\alpha > 0$. Since $P \in C(\mathbb{Q})$, we can plug in C to get

$$\frac{u^2}{v^2p^{2\beta}} = \frac{m^3 + am^2np^\alpha + bmn^2p^{2\alpha} + cn^3p^{3\alpha}}{n^3p^3\alpha}.$$

Since p does not divide u^2 and v^2, and $\alpha > 0$ and p does not divide m we have

$$p \not| (m^3 + am^2np^\alpha + bmn^2p^{2\alpha} + cn^3p^{3\alpha}).$$

Therefore,

$$-2\beta = \text{ord}\left(\frac{u^2}{v^2p^{2\beta}}\right) = \text{ord}\left(\frac{m^3 + am^2np^\alpha + bmn^2p^{2\alpha} + cn^3p^{3\alpha}}{n^3p^3\alpha}\right) = -3\alpha.$$

Similarly, if we assume that p divides the denominator of y, then we find the same result. So there exists some $\xi > 0$ such that if p divides either one of the denominators of x, y,

$$\alpha = 2\xi \text{ and } \beta = 3\xi.$$

Define

$$C(p^\xi) = \{(x, y) \in C(\mathbb{Q}) : \text{ord}\,(x) \leq -2\xi \text{ and ord}\,(y) \leq -3\xi\}.$$

The important part of the proof lies in the proof that $C(p^\alpha)$ is a subgroup of $C(\mathbb{Q})$. To show this we perform a change of coordinates and

$$t = \frac{x}{y} \text{ and } s = \frac{1}{y}.$$

The curve becomes

$$s = t^3 + at^2s + bts^2 + cs^3.$$

Notice that things have shifed in the following ways:

- O becomes the origin.
- The origin becomes O.
- A line $\ell : y = ux + v$ is $\ell' : s = -\frac{u}{v}t + \frac{1}{v}$.
- Group law almost changed but to get the inverse you connect with the infinity which is the origin now.

Now we can see how this new coordinate system will help us to show things we want. Let p be any prime. Let $P = (x, y)$ be our rational point such that p^α divides the denominator of y or x. That is

$$x = \frac{m}{np^{2(\alpha+i)}} \text{ and } y = \frac{u}{vp^3(\alpha+i)}$$

for $i \geq 0$. After changing coordinates, we have

$$t = \frac{x}{y} = \frac{mw}{nu}p^{v+i} \text{ and } s = \frac{1}{y} = \frac{w}{u}p^{3(v+i)}.$$

Now let us give ourselves more language. Let R be the set of all non-zero rational numbers x such that $\operatorname{ord}(x) \geq 0$. R has the following properties:

- R has unique factorization.
- R has only one prime p.
- The units of R are rational numbers of p-order 0.
- If $(t, s) \in C(p^\alpha)$, then $t \in p^\alpha R$ and $s \in p^{3\alpha}R$.

To show that $C(p^\alpha)$ is a subgroup of $C(\mathbb{Q})$, we add two points and show that if p^α divides the t-coordinate of each numerator of the two rational points, then p^α divides the t-coordinate of their sum. Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$. To ease your life, I calculated the followings. If $t_1 = t_2$, then $P_1 = -P_2$ and $P_1 + P_2 = O \in C(p^\alpha)$. If $t_1 \neq t_2$, then the line passing $s = \gamma t + \theta$ through P_1 and P_2 will have slope

$$\gamma = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1s_2 + s_1^2)}.$$

Let $P_3 = (t_3, s_3)$ be $-(P_1 + P_2)$. Substituting $s = \gamma t + \theta$ into the curve, we get that

$$t_1 + t_2 + t_3 = -\frac{a\theta + 2b\alpha\theta + 3c\gamma^2\theta}{1 + a\gamma + b\gamma^2 + c\gamma^3}.$$

Another thing we need is

$$\theta = s_1 - \gamma t_1.$$

We have all the information we need.

- The numerator of γ is in $p^{2\alpha}R$ since all $t_1, s_1, t_2, s_2 \in p^{2\alpha}R$.
- The denominator of γ disregarding 1 is in $p^{2\alpha}R$.
- $\theta \in p^{3\alpha}R$ since $s_1 \in p^{3\alpha}R$ and $\alpha \in p^{2\alpha}R$ and $t_1 \in p^{\alpha}R$.
- $t_1 + t_2 + t_3 \in p^{3\alpha}R$.
- $t_3 \in p^{\alpha}R$ since $t_1, t_2 \in p^{\alpha}R$.

Hence $C(p^{\alpha})$ is a subgroup of $C(\mathbb{Q})$ and

$$t_1 + t_2 + t_3 \in p^{3\alpha}R.$$

This means that

$$t_3 \equiv t_1 + t_2 \pmod{p^{3v}R}.$$

The map $P = (t,s) \mapsto t$ is a map from $C(p^{\alpha})$ to additive group of rational numbers under mod out the subgrougp $p^{3\alpha}R$. The kernel of this map is $C(p^{3\alpha})$. Therefore, we have an injective homomorphism

$$\frac{C(p^{\alpha})}{C(p^{3\alpha})} \to \frac{p^{\alpha}R}{p^{3\alpha}R}.$$

We now want to show that $P \in C(\mathbb{Q})$ of finite order and $P \neq O$ does not live in any $C(p)$ for all p.

Proof. Let P have order m and p be any prime. Since $P \neq O$, $m \neq 1$. Suppose for contradiction that $P = (t,s)$ such that $P \in C(p^{\alpha})$, but since P is not infinity, so there exists a $\mu > 0$ such that

$$P \in C(p^{\mu}) \text{ but } P \notin C(p^{\mu+1}).$$

If p does not divide m, we have that

$$0 \equiv t(mP) \equiv mt(P) \pmod{p^{3\mu}R}.$$

Since m is coprime to p, $P \in C(p^{3\alpha})$.

If p divides m. We have $m = pn$ for some n. Consider $P' = nP$. Then P' has order p. Using the same reasoning: Suppose $P \in C(p)$, then since $C(p)$ is a subgroup of $C(\mathbb{Q})$, $P' \in C(p)$. There exists a $\mu > 0$ such that

$$P \in C(p^{\mu}) \text{ but } P \notin C(p^{\mu+1}).$$

Then

$$0 = t(pP') \equiv pt(P') \pmod{p^{3\mu}R}.$$

Therefore, $P \in p^{3\mu-1}R$, a contradiction.

Therefore, P has integer coordinates.

Let $P = (x, y)$ such that P has finite order. Then $2P$ also has finite order and both P and $2P$ have integer coordinates. Let $2P = (z, w)$. The "Duplication Formula",

$$2x + z = \left(\frac{f'(x)}{2y}\right)^2 - a.$$

Since x, z are integers, $\frac{f'(x)}{2y}$ are integers, so $2y|f'(x)$ and $y|f(x)$ since

$$D = r(x)f(x) + s(x)f'(x).$$

Hence $y|D$. □

References

[ST15] Joseph Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, 2015.