23MAC260 Elliptic Curves: Week 5

Last updated: February 27, 2024

1 Mordell's Theorem

In this part of the module, we will be studying the properties of elliptic curves E given by an equation

$$E : \; Y^2Z = G(X, Z) \tag{1}$$

in which all the coefficients of G are in the rational numbers $\mathbb{Q}$. We say that such a curve is **defined over** $\mathbb{Q}$, or just **over** $\mathbb{Q}$.

Main Question: Can we describe the group

$$E(\mathbb{Q}) = \left\{[a, b, c] \in \mathbb{P}^2 \mid a, b, c \in \mathbb{Q},\ [a, b, c] \in E\right\}$$

of **rational points** on E? (We saw in Week 3 that $E(\mathbb{Q})$ is a subgroup of E.)

To describe this subgroup, we need the following definition.

Definition 1.1. *Let A and B be abelian groups. The* **direct sum** *of A and B, denoted by $A \oplus B$, is the abelian group whose elements are pairs (a, b) with $a \in A$ and $b \in B$, and with operation*

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$

Exercise: Prove this definition of $A \oplus B$ actually satisfies the group axioms.

Notation: If A is an abelian group and $r \geq 0$ a natural number, we write A^r to mean $A \oplus \cdots \oplus A$ (r times). So an element of A^r is a tuple of the form

$$(a_1, \ldots, a_n) \quad \text{with } a_i \in A \forall\, i.$$

Our main result about the structure of $E(\mathbb{Q})$ is the following:

Theorem 1.2 (Mordell's Theorem)**.** *Let E be an elliptic curve defined by an equation of the form (1) with all coefficients in $\mathbb{Q}$. Then*

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

where $r \geq 0$ is a natural number and T is a finite group.

We will explain part of the proof in Week 7. For now we make the following remarks.

Remarks:

1. Since the subgroup T is finite, every element of T has finite order; conversely, an element

$$(a_1, \dots, a_n, t) \in \mathbb{Z}^r \oplus T$$

has finite order if and only if $a_1 = \cdots = a_n = 0$. So T is exactly the subgroup of $E(\mathbb{Q})$ of elements of finite order, also known as the **torsion subgroup** of $E(\mathbb{Q})$.

2. The theorem says that there is a finite set of points $P_1, \dots, P_r \in E(\mathbb{Q})$, each of infinite order, such that any point $P \in E(\mathbb{Q})$ can be written uniquely in the form

$$P = n_1 P_1 \oplus \cdots \oplus n_r P_r \oplus Q \quad \text{with } n_i \in \mathbb{Z},\ Q \in T.$$

So $E(\mathbb{Q})$ is a **finitely generated** abelian group.

3. In practice the torsion subgroup T is not hard to determine, as we will see, whereas the number r, called the **rank** of the curve, is hard to find. There are many unsettled questions in this area, such as

Given a natural number N, does there exists an elliptic curve over $\mathbb{Q}$ with rank $\geq N$?

For the rest of this week and next week, we will focus on the problem of computing the torsion subgroup T. For clarity, let's state the precise definition of T here:

Definition 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$. The* **torsion subgroup** *$T \subset E(\mathbb{Q})$ means the subgroup of $E(\mathbb{Q})$ consisting of points of finite order.*

2 Integral Models of Elliptic Curves

To work with elliptic curves over $\mathbb{Q}$, it is convenient to work with equations that are "as simple as possible".

Definition 2.1. *Let E be an elliptic curve*

$$E : y^2 = x^3 + ax + b \quad \textit{with } a, b \in \mathbb{Q}.$$

An **integral model** *of E is an elliptic curve*

$$E' : y^2 = x^3 + Ax + B \quad \textit{with } A, B \in \mathbb{Z}$$

such that $E \simeq_{\mathbb{Q}} E'$: that is, the curves are isomorphic over $\mathbb{Q}$.

The integral model E' is called **minimal** *if*

$$\left(d^4 \mid A \text{ and } d^6 \mid B\right) \Rightarrow d = \pm 1.$$

Proposition 2.2. *Every elliptic curve over $\mathbb{Q}$ has a minimal integral model.*

Proof. Given an elliptic curve E over $\mathbb{Q}$ defined by

$$E : y^2 = x^3 + ax + b \quad (a, \in \mathbb{Q})$$

we know that for any nonzero $\mu \in \mathbb{Q}$, the curve

$$E' : y^2 = x^3 + (\mu^4 a)x + (\mu^6 b)$$

is isomorphic to E. Choosing μ such that both $\mu^4 a$ and $\mu^6 b$ are in $\mathbb{Z}$, we get an integral model of E.

Now if p is any prime such that $p^4 \mid \mu^4 a$ and $p^6 \mid \mu^6 b$, we can replace μ with μ/p to get another integral model. Repeating this for all appropriate primes p, we end up with a minimal integral model. $\square$

3 The Torsion Subgroup

Recall that $T \subset E(\mathbb{Q})$ denotes the **torsion subgroup** of $E(\mathbb{Q})$, meaning the subgroup consisting of points of finite order. We want to understand the group T for a given curve E.

If we replace E by an integral model E', then as explained in Week 3 we get an isomorphism $E(\mathbb{Q}) \cong E'(\mathbb{Q})$. So to answer our question, it is enough to consider the case when E is given by

$$y^2 = x^3 + ax + b \quad \text{with } a,\ b \in \mathbb{Z}.$$

In this case, the key result about points of finite order is the following:

Theorem 3.1 (Integrality Theorem)**.** *Let E be an elliptic curve given by an equation*

$$y^2 = x^3 + ax + b \quad \textit{where } a, b \in \mathbb{Z}.$$

If $(x, y) \in E(\mathbb{Q})$ is a point of finite order, then x and y are integers.

Remarks:

1. We are not going to prove this theorem. The idea of the proof is to show rigorously what we already observed empirically: if $P = (x, y)$ is a point with rational coordinates which are **not** integers, then the coordinates of the multiples nP will have numerators and denominators which get larger and larger. (Compare Problem Sheet 3 Question 3.) For more details of the proof, consult Silverman, "The Arithmetic of Elliptic Curves", p.240.

2. The converse of the statement above is not true: a point $(x, y) \in E(\mathbb{Q})$ with coordinates in $\mathbb{Z}$ may have infinite order. (Again see Problem Sheet 3 Question 3.)

We will use the Integrality Theorem to deduce the following bound for the coordinates of torsion points.

Theorem 3.2 (Nagell-Lutz Theorem). *Let* E *be an elliptic curve given by an equation*

$$y^2 = x^3 + ax + b \quad \textit{where } a, b \in \mathbb{Z}.$$

Let $\Delta = -4a^3 - 27b^2$ *denote the discriminant of* E.

Let $(x, y) \in E(\mathbb{Q})$ *be a point of finite order. (So in particular* x, $y \in \mathbb{Z}$.*) Then either*

- $y = 0$, *or*
- $y^2 \mid \Delta$.

Proof. Let $P = (x, y)$ be a point of finite order in $E(\mathbb{Q})$. Let n denote the order of P.

First note that since $-P = (x, -y)$, we have $2P = O$ if and only if $y = 0$. So $n = 2$ if and only if $y = 0$.

So we can restrict to the case $y \neq 0$. In this case, the formulas for point addition from Week 3 Theorem 3.1 show that

$$\begin{aligned} x(2P) &= \left(\frac{3x^2 + a}{2y}\right)^2 - 2x \\ &= \frac{(3x^2 + a)^2 - 8xy^2}{4y^2} \\ &= \frac{(3x^2 + a)^2 - 8x(x^3 + ax + b)}{4y^2}. \end{aligned}$$

Now if P has finite order, then so does $2P$. By the Integrality Theorem, we therefore must have $x(2P) \in \mathbb{Z}$. So the previous equation implies

$$y^2 \mid (3x^2 + a)^2 - 8x(x^2 + ax + b). \tag{2}$$

We want to show that $y^2 \mid \Delta$, so we need to combine the right-hand side of Equation 2 with something to get Δ. A direct calculation shows that

$$\begin{aligned} &-(3x^2 + 4a)\left((3x^2 + a)^2 - 8x(x^3 + ax + b)\right) + (3x^3 - 5ax - 27b)(x^3 + ax + b) \\ &= -4a^3 - 27b^2 \\ &= \Delta. \end{aligned}$$

Since

$$\begin{aligned} &y^2 \mid (3x^2 + a)^2 - 8x(x^3 + ax + b) \quad \text{and} \\ &y^2 = x^3 + ax + b \end{aligned}$$

this shows $y^2 \mid \Delta$ as required. □

Corollary 3.3. *For any elliptic curve* E *defined over* $\mathbb{Q}$, *the torsion subgroup* $T \subset E(\mathbb{Q})$ *is finite.*

Proof. The subgroup T consists of the identity element O together with points of finite order of the form $P = (x, y)$. There are finitely many integers which either equal 0 or divide Δ, so Nagell–Lutz shows there are finitely many possibilities for y. For any given value of y, there are at most 3 values of x such that $x^3 + ax + b = y^2$, so altogether there are finitely many possibilities for (x, y). □

4 Computing the torsion subgroup: examples

Example 1

Consider the curve

$$E: \ y^2 = x^3 + 4.$$

We want to compute the torsion subgroup $T \subset E(\mathbb{Q})$.

For this curve we have $\Delta = -27(4^2) = -3 \cdot 12^2$. So Nagell–Lutz implies that if $P = (x, y)$ has finite order, then $y = 0$ or $y^2 \mid 3 \cdot 12^2$, which implies that $|y|$ divides 12. We can make a table of the possibilities for $|y|$ and x:

$\lvert y\rvert$	0	1	2	3	4	6	12
$x^3 = y^2 - 4$	-4	-3	0	5	12	32	140
x	–	–	0	–	–	–	–

So, besides the identity O, the only **candidates** for torsion points on our curve are $P = (0, 2)$ and $-P = (0, -2)$.

WARNING: Nagell–Lutz gives a *necessary* but not *sufficient* condition for a point to be a torsion point. Any candidate point we find must be checked!

So let us compute $2P$: from Week 3 Theorem 3.1 we get

$$x(2P) = \left(\frac{3x^2}{2y}\right)^2_{|P} - 2x(P) = 0.$$

So $2P$ has x-coordinate 0, therefore $2P = \pm P$. But if $2P = P$ then we would have $P = O$, which is false. So we must in fact have $2P = -P$, hence $3P = 0$.

So our point P is a point of order 3, and so we have

$$T = \{O, P, -P\} \cong \mathbb{Z}_3.$$

Example 2

Next consider

$$E: \ y^2 = x^3 + 8.$$

In this case the warning from the previous example becomes relevant: we compute $\Delta = -27 \cdot 8^2 = -3 \cdot 24^2$. So Nagell–Lutz implies that if $P = (x, y)$ is a torsion point, then $y = 0$ or $|y|$ divides 24.

Let's take for example $|y| = 3$: the equation

$$x^3 + 8 = 3^2$$

has the integer solution $x = 1$, so we get a candidate torsion point $P = (1, 3) \in E(\mathbb{Q})$. This point satisfies the conditions of the Integrality Theorem ($x, y \in \mathbb{Z}$) and Nagell–Lutz ($y^2 \mid \Delta$). However, P is **not** a point of finite order!

To see this, let's compute the x-coordinate of $2P$ as before:

$$\begin{aligned} x(2P) &= \left(\frac{3x^2}{2y}\right)^2_{|P} - 2x(P) \\ &= \left(\frac{3}{6}\right)^2 - 2\cdot(1) = -\frac{7}{4}. \end{aligned}$$

So $x(2P) \notin \mathbb{Z}$, and therefore by the Integrality Theorem, $2P$ is not a point of finite order. This implies that P is not a point of finite order.

Example 3

Finally we return to the curve discussed in Week 2:

$$E : \; y^2 = x^3 + 1.$$

We already know some points on E, namely

$$P = (2,3), \quad Q = (-1,0), \quad 2P = (0,1), \quad R = P \oplus Q = (0,-1).$$

Since Q has y-coordinate equal to O, we know $2Q = O$, or equivalently $Q = -Q$. We can also see that $2P = -R = -(P \oplus Q)$, so $3P = -Q = Q$, and hence $6P = O$. So the subgroup of E generated by the point P is

$$\begin{aligned} \langle P \rangle &= \{O, P, \ldots, 5P\} \\ &\cong \mathbb{Z}_6. \end{aligned}$$

Let's show that the torsion subgroup T is exactly the subgroup $\langle P \rangle$.

In this case we have $\Delta = -27 = -3 \cdot 3^2$, so Nagell–Lutz tells us that any point (x, y) of finite order must have $y = 0$ or $|y| = 1$ or $|y| = 3$. Let's examine each possibility:

- If $y = 0$ then $x^3 + 1 = 0$ so $x = -1$. So we get the point $(-1, 0) = 3P$.
- If $|y| = 1$ then $x^3 + 1 = 1$ so $x = 0$. So we get the points $(0,1) = 2P$ and $(0,-1) = R = P \oplus Q = 4P$.
- If $|y| = 3$ then $x^3 + 1 = 9$ so $x = 2$. So we get the points $(2,3) = P$ and $(2,-3) = -P = 5P$.

So all the candidate torsion points we found are multiples of P, therefore they are actual torsion points. So we have

$$T = \langle P \rangle \cong \mathbb{Z}_6.$$