23MAC260 Elliptic Curves: Week 7

Last updated: March 15, 2024

1 Heights on elliptic curves

Recall from Week 5 the statement of Mordell's Theorem:

Theorem 1.1 (Mordell)**.** *Let* E *be an elliptic curve over* $\mathbb{Q}$*. Then*

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

where $r \geq 0$ *is a natural number (the* **rank** *of* E*) and* T *is a finite group.*

This week we will say something about the proof. The very rough idea is to start by defining the "size" of a point on an elliptic curve, then show that multiplying a point by 2 increases its "size, and that the set of points with bounded "size" is finite. This is the motivation for the next definition:

Definition 1.2. *(A) Let* $t \in \mathbb{Q}$ *and write it as* $t = \frac{p}{q}$ *in lowest terms. The* **height** $H(t)$ *of* t *is defined as*

$$H(t) = \max\{|p|, |q|\}.$$

(B) Now let E *be an elliptic curve over* $\mathbb{Q}$ *given by an integral model*

$$y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z}).$$

The (logarithmic) **height** *on* $E(\mathbb{Q})$ *is the function*

$$h_x \colon E(\mathbb{Q}) \to \mathbb{R}$$

defined by

$$h_x(P) = \begin{cases} \ln H(x(P)) & \text{for } P \neq O \\ 0 & \text{for } P = O. \end{cases}$$

Note that $H(t) \geq 1$ for any rational number t, so h_x is always nonnegative.

Example: On the curve

$$E: \quad y^2 = x^3 + 3x + 5$$

consider the point $P = (1, 3)$. (As we will see, it has infinite order.)

The height of this point is

$$h_x(P) = \ln H(x(P)) = \ln H(1) = \ln 1 = 0.$$

What happens if we take higher and higher multiples of P? Using our formulas from Week 3, we can compute:

$$5P = \left(-\frac{11}{25}, \frac{237}{125}\right)$$

so

$$\begin{aligned} H(x(5P)) = H(-11/25) &= \max\{11, 25\} \\ &= 25 \\ \Rightarrow h_x(5P) &= \ln(25) \\ &= 3.2188\cdots \end{aligned}$$

Continuing:

$$\begin{aligned} 10P &= \left(\frac{276431}{156025}, ?\right) \\ \Rightarrow h_x(10P) &= \ln(276431) = 12.5927\cdots \\ &\vdots \\ h_x(20P) &= 50.595\cdots \\ &\vdots \\ h_x(40P) &= 204.8624\cdots \end{aligned}$$

So it seems that "in the long run", doubling a point multiplies its height by a factor of about 4.

To make this observation precise and explain part of the proof of Mordell's Theorem, we will need some properties of the height function. First we start with a lemma.

Lemma 1.3. *Let* E *be an elliptic curve defined by an integral model*

$$y^2 = x^3 + ax + b.$$

Then any point $(x, y) \in E(\mathbb{Q})$ *has the form*

$$x = \frac{m}{d^2}, \quad y = \frac{n}{d^3}$$

with $m, n, d \in \mathbb{Z}$ *and* $\gcd(m, d) = \gcd(n, d) = 1$.

Proof. See Problem Sheet 7. □

Now we can look at the key properties of the height function that we need to prove Mordell's Theorem.

Proposition 1.4. *Let* E *be an elliptic curve given by an integral model*

$$y^2 = x^3 + ax + b.$$

Let h_x *be the height function on* E*. Then:*

(a) Let $P_0 \in E(\mathbb{Q})$*. There is a constant* C_1 *depending on* a*,* b*, and* P_0 *such that*

$$h_x(P + P_0) \leq 2h_x(P) + C_1 \quad \forall P \in E(\mathbb{Q})$$

(b) There is a constant C_2 *depending on* a *and* b *such that*

$$h_x(2P) \geq 4h_x(P) - C_2 \quad \forall P \in E(\mathbb{Q})$$

(c) For any constant $C \in \mathbb{R}$*, the set*

$$\{P \in E(\mathbb{Q}) \mid h_x(P) \leq C\}$$

is finite.

Sketch of proof. (a) Let $P_0 = (x_0, y_0) \in E(\mathbb{Q})$ be a fixed point, and let $P = (x, y) \in E(\mathbb{Q})$ be any point. By the previous lemma, we know there exist integers α_0, β_0, d_0 and α, β, d such that

$$x_0 = \frac{\alpha_0}{d_0^2}, \quad y_0 = \frac{\beta_0}{d_0^3}$$
$$x = \frac{\alpha}{d^2}, \quad y = \frac{\beta}{d^3}$$

Our formula from Week 3 says

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0$$

We can simplify this expression by putting everything over a common denominator and multiplying out the squares. When we do this, we can replace y_0^2 by $x_0^3 + ax_0 + b$, and y^2 by $x^3 + ax + b$, since P_0 and P are points on the curve E. Substituting the above expressions for the coordinates x_0, y_0, x, y and simplifying, the formula above becomes (check it!)

$$x(P + P_0) = \frac{(\alpha\alpha_0 + ad^2d_0^2)(\alpha d_0^2 + \alpha_0 d^2) + 2bd^4d_0^4 - 2\beta d\beta_0 d_0}{(\alpha d_0^2 - \alpha_0 d^2)^2}$$

We want to find an **upper** bound for $h_x(P + P_0)$; any cancellation in the numerator and denominator of this fraction will only decrease the height, so we can neglect it.

We can estimate the height $H(x(P + P_0)$ from the above expression as follows. Consider the case when $|\alpha| > |d|^2$: then the term $(\alpha\alpha_0 + ad^2d_0^2)$ has absolute value at most $(|\alpha_0 + |a||d_0|)^2|\alpha|$. Here the coefficient of $|\alpha|$ is a constant that only depends on the "fixed" data of the curve E and the point P_0. We can

continue in this way to estimate the other terms in the above expression, and also to consider what happens when $|\alpha| < |d|^2$, and so on. In this way we get

$$H(x(P + P_0)) \leq C_1' \max\left\{|\alpha|^2, |d|^4, |\beta d|\right\} \qquad (*)$$

where C_1' is a constant that only depends on $a, b, \alpha_0, \beta_0, d_0$, in other words only on the curve and on P_0.

Note that

$$H(x(P))^2 = \max\left\{|\alpha|^2, |d|^4\right\}$$

so inequality $(*)$ almost gives

$$H(x(P + P_0)) \leq C_1' H(x(P))^2$$

except for the $|\beta d|$ term.

To deal with this, notice that since the point $P = \left(\frac{\alpha}{d^2}, \frac{\beta}{d^3}\right)$ lies on the curve, we have

$$\left(\frac{\beta}{d^3}\right)^2 = \left(\frac{\alpha}{d^2}\right)^3 + a\left(\frac{\alpha}{d^2}\right) + b \quad \text{so}$$
$$\beta^2 = \alpha^3 + a\alpha d^4 + b d^6.$$

This imples that there is a constant Γ_1 such that

$$|\beta| \leq \Gamma_1 \max\left\{|\alpha|^{3/2}, |d|^3\right\} \quad \text{so}$$
$$|\beta d| \leq \Gamma_1 \max\left\{|\alpha|^2, |d|^4\right\}.$$

So if $C_1'' = \max\{C_1', \Gamma_1\}$ then we finally get

$$\begin{aligned} H(x(P + P_0)) &\leq C_1'' \max\left\{|\alpha|^2, |d|^4\right\} \\ &= C_1'' H(x(P))^2 \end{aligned}$$

So taking logs we get

$$h_x(P + P_0) \leq 2h_x(P) + C_1$$

where $C_1 = \ln C_1''$.

(b) Similar to Part (a) but trickier: see Silverman pp. 221-224 for details.

(c) Let $C \in \mathbb{R}$ be any constant. Let P be a point of $E(\mathbb{Q})$ and write $x(P) = m/n$ as a fraction in lowest terms. Then

$$\begin{aligned} h_x(P) \leq C &\Leftrightarrow H(x(P)) \leq e^C \\ &\Leftrightarrow \max\{|m|, |n|\} \leq e^C \end{aligned}$$

There are only finitely many m and n which satisfy this condition, hence only finitely many possibilities for $x(P)$. For each possible value x of $x(P)$, there are at most 2 values of y such that $(x, y) \in E$. So altogeter there are finitely many possibilities for P.

□

2 Proof of Mordell's Theorem

We need one more ingredient to prove Mordell's Theorem:

Theorem 2.1 (Weak Mordell's Theorem)**.** *For an elliptic curve* E *over* $\mathbb{Q}$*, write* $2E(\mathbb{Q})$ *to denote the subgroup*

$$\{Q \in E(\mathbb{Q}) \mid \exists P \in E(\mathbb{Q}) \text{ such that } Q = 2P\} \subset E(\mathbb{Q}).$$

Then the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ *is finite.*

We will use this result without proof, together with the facts about heights from the last lecture, to prove Mordell's Theorem.

Proof of Mordell's Theorem. Let E be an elliptic curve over $\mathbb{Q}$. We want to prove that

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

for some natural number r and some finite group T. By the classification of finitely-generated abelian groups, this is equivalent to proving that $E(\mathbb{Q})$ is finitely generated: that is, there is a finite set of points $P_1, \ldots, P_n \in E(\mathbb{Q})$ such that

$$E(\mathbb{Q}) = \langle P_1, \ldots, P_n \rangle.$$

Start by choosing points $Q_1, \ldots, Q_r \in E(\mathbb{Q})$ which represent all the cosets of $E(\mathbb{Q})/2E(\mathbb{Q})$. (The Weak Mordell Theorem guarantees that there is such a finite set.)

Now let $P \in E(\mathbb{Q})$ be an arbitrary point. Then there exists i_1 such that $P - Q_{i_1} \in 2E(\mathbb{Q})$, in other words

$$P = Q_{i_1} + 2P_1 \quad \text{for some } P_1 \in E(\mathbb{Q})$$

We can repeat this process with P_1 in place of P, and so on:

$$\begin{aligned} P_1 &= Q_{i_2} + 2P_2 \quad \text{for some } P_2 \in E(\mathbb{Q}) \\ &\vdots \\ P_{n-1} &= Q_{i_n} + 2P_n \quad \text{for some } P_n \text{in} E(\mathbb{Q}). \end{aligned}$$

For any j, Proposition 1.4 (b) tells us that

$$\begin{aligned} h_x(P_j) &\le \frac{1}{4}\left(h_x(2P_j) + C_2\right) \\ &= \frac{1}{4}\left(h_x(P_{j-1} - Q_{i_j}) + C_2\right) \end{aligned}$$

Now let C_1' be the maximum of the constants found in Proposition 1.4 (a) for P_0 one the (finitely many) points $\{-Q_1, \ldots, -Q_r\}$. Then using Proposition 1.4 (a) the previous inequality becomes

$$\begin{aligned} h_x(P_j) &\le \frac{1}{4}\left(2h_x(P_{j-1}) + C_1' + C_2\right) \\ &= \frac{1}{2}h_x(P_{j-1}) + \frac{1}{4}(C_1' + C_2). \end{aligned}$$

Repeating this for P, $P_1, \ldots, P_n$ we end up with

$$h_x(P_n) \leq \left(\frac{1}{2}\right)^n h(P) + \Sigma_n(C_1' + C_2)$$

where $\Sigma_n = \sum_{i=1}^{n} \frac{1}{2^{i+1}}$. Note that for all n we have $\Sigma_n \leq \sum_{i=1}^{\infty} \frac{1}{2^{i+1}} = \frac{1}{2}$.

So for sufficiently large n, the previous inequality gives us

$$h_x(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2)$$

Letting $C_3 = 1 + \frac{1}{2}(C_1' + C_2)$, Proposition 1.4 (c) shows that the set

$$\{P \in E(\mathbb{Q}) \mid h_x(P) \leq C_3\}$$

is finite. Call this set $\{R_1, \ldots, R_s\}$. So for n sufficiently large, $P_n = R_k$ for some $k = 1, \ldots, s$.

Finally since

$$P = 2^n P_n + \sum_{j=1}^{n} 2^{j-1} Q_{i_j}$$

we see that P is in the subgroup of $E(\mathbb{Q})$ generated by the finite set

$$\{Q_1, \ldots, Q_r\} \cup \{R_1, \ldots, R_s\}.$$

□

3 Computing the rank (non-examinable)

We have seen that computing the torsion subgroup $T \subset E(\mathbb{Q})$ is not too difficult. Computing the rank r is much more difficult. One tool that can help in certain cases is the so-called *Kummer map*, which we will now introduce.

Before doing so let us fix some notation. Let $\mathbb{Q}^\times$ denote the set of nonzero elements of $\mathbb{Q}$: this is a group under multiplication. Let $(\mathbb{Q}^\times)^2$ denote the subset of elements of $\mathbb{Q}^\times$ which are of the form q^2: that is, the subset of squares of rational numbers. Then it is not hard to check that $(\mathbb{Q}^\times)^2$ is a subgroup of $\mathbb{Q}^\times$, and since $\mathbb{Q}^\times$ is abelian, we can form the quotient group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. For $q \in \mathbb{Q}$, we denote by $[q]$ its coset in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Note that for any $q_1, q_2 \in \mathbb{Q}$ we have $[q_1^2 q_2] = [q_1]$: in other words, we can cancel squares in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Definition 3.1. *Let E be an elliptic curve given in the form*

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

The **Kummer map** *or* **2-descent map**

$$\delta \colon E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

is defined as follows:

$$\delta(P) = \begin{cases} [1] & \text{for } P = O \\ [b] & \text{for } P = (0,0) \\ [x(P)] & \text{for } P \neq O,\ (0,0) \end{cases}$$

Proposition 3.2. *The Kummer map is a group homomorphism.*

Proof. See Problem Sheet 7. □

To use this to say something about the rank of a curve, the idea is the following. If points $\{P_1, \ldots, P_r\}$ are dependent in $E(\mathbb{Q})$, meaning that

$$n_1 P_1 \oplus \cdots \oplus n_r P_r = O$$

for some integers n_i, then applying the homomorphism δ we see that the images of the P_i under δ must satisfy the corresponding equation in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$:

$$\delta(P_1)^{n_1} \cdots \delta(P_r)^{n_r} = [1].$$

Turning this around, if the $\delta(P_i)$ are independent, then so too are the P_i.

In practice, there is a tricky point, namely that every element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ has order 2, so any element of the form $[q_1]^{n_1} \cdots [q_r]^{n_r}$ in which the exponents n_i are all even will always equal $[1]$. But with a bit more care we can still use the strategy described.

Let's see how this works in a specific example.

Example (Wiman, 1945) Let's show that the curve E given by

$$E : \ y^2 = x(x^2 - 210^2)$$

has rank at least 2.

To begin, we need to compute the torsion subgroup $T \subset E(\mathbb{Q})$. We will do this by reducing modulo appropriate primes. The discriminant of the equation above is

$$\begin{aligned} \Delta &= -4 \cdot (-210)^6 \\ &= -2^8 \cdot 3^6 \cdot 5^6 \cdot 7^6. \end{aligned}$$

So reducing modulo any prime $p \geq 11$, we get an elliptic curve $\overline{E}_p$, and the Torsion Embedding Theorem from Week 6 tells us that $|T|$ divides $|\overline{E}_p(\mathbb{F}_p)$. Reducing mod 11 and 13 we find

$$\begin{aligned} |\overline{E}_{11}(\mathbb{F}_{11})| &= 12 \\ |\overline{E}_{13}(\mathbb{F}_{13})| &= 20 \end{aligned}$$

so $|T|$ must divide $\gcd(12, 20) = 4$.

On the other hand, there are 4 obvious torsion points on E: we can write the equation of E as

$$y^2 = (x - 210)x(x + 210)$$

so we get 3 points of order 2 in T, namely

$$\begin{aligned} Q_1 &= (-210, 0) \\ Q_2 &= (0, 0) \\ Q_3 &= (210, 0). \end{aligned}$$

Since we have 3 nontrivial points in T, together with the identity O we have 4 torsion points, so this must be the whole torsion subgroup:

$$T = \{O, Q_1, Q_2, Q_3\}.$$

Let us compute the images of these points under the Kummer homomorphism: we get

$$\begin{aligned}
\delta(O) &= [1] \\
\delta(Q_1) &= [-210] \\
\delta(Q_2) &= [b] = [-210^2] = [-1] \\
\delta(Q_3) &= [210].
\end{aligned}$$

Now we will find 2 point of infinite order on E. We will use the fact that $210 = 5 \cdot 6 \cdot 7$. Therefore if we take $x = 6 \cdot 210$, we get

$$\begin{aligned}
(x - 210)x(x + 210) &= (5 \cdot 210) \cdot (6 \cdot 210) \cdot (7 \cdot 210) \\
&= 210^4.
\end{aligned}$$

Therefore

$$P_1 = (6 \cdot 210,\, 210^2) \in E(\mathbb{Q}).$$

Similarly, if we set $x = 525 = 5 \cdot \frac{210}{2}$, then

$$\begin{aligned}
(x - 210)x(x + 210) &= 3 \cdot 5 \cdot 7 \cdot \left(\frac{210}{2}\right)^3 \\
&= 5 \cdot 6 \cdot 7 \cdot \left(\frac{210^3}{2^4}\right) \\
&= \left(\frac{210}{2}\right)^4
\end{aligned}$$

Therefore

$$P_2 = \left(5 \cdot \frac{210}{2},\, \left(\frac{210}{2}\right)^2\right) \in E(\mathbb{Q}).$$

Neither P_1 nor P_2 is in T, so they both have infinite order. So the rank of E is at least 1. We will show that in fact the rank is at least 2.

If the rank of E was equal to 1, then we would have

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

and therefore we could find integers n_1, n_2 such that

$$n_1 P_1 \oplus n_2 P_2 = O.$$

If $\gcd(n_1, n_2) = d \neq 1$, then we can rewrite this equation as

$$d(m_1 P_1 \oplus m_2 P_2) = O$$

for some coprime integers m_1 and m_2. This means that the point $m_1P_1 \oplus m_2P_2$ is a torsion point, hence equal to one of the elements of T listed above. So we have

$$m_1P_1 \oplus m_2P_2 = \begin{cases} O & \text{if } d = 1 \\ Q_i \ (i = 1, 2, 3) & \text{if } d > 1. \end{cases}$$

Applying the Kummer homomorphism, this gives an equation

$$\delta(P_1)^{m_1} \cdot \delta(P_2)^{m_2} = \begin{cases} [1] & \text{or} \\ [-210] = [-5] \cdot [6] \cdot [7] & \text{or} \\ [-1] & \text{or} \\ [210] = [5] \cdot [6] \cdot [7]. \end{cases}$$

We will show that none of these equations can hold, proving that the rank of E is at least 2.

To show this, we compute

$$\begin{aligned} \delta(P_1) &= [6 \cdot 210] \\ &= [5 \cdot 6^2 \cdot 7] \\ &= [5] \cdot [7]; \\ \delta(P_2) &= [525] \\ &= [3 \cdot 5^2 \cdot 7] \\ &= [3] \cdot [7]. \end{aligned}$$

Therefore

$$\delta(P_1)^{m_1}\delta(P_2)^{m_2} = [3]^{m_2} \cdot [5]^{m_1} \cdot [7]^{m_1+m_2}$$

This can never equal $[\pm 5] \cdot [6] \cdot [7]$ since there is no factor of 2; it can never equal $[-1]$ since two representatives of the same element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ differ by a square, so have the same sign. Finally, it equals $[1]$ only if m_1 and m_2 are both even, but by assumption m_1 and m_2 are coprime, so this is impossible too.

Remark: It is still unknown whether r is bounded for all elliptic curves over $\mathbb{Q}$: in other words whether, given any natural number N, we can find an elliptic curve E whose rank $r(E)$ satisfies $r(E) \geq N$. The current world record holder is a curve discovered by Noam Elkies in 2006, whose rank satisfies $r(E) \geq 28$ (the exact value is not known). This curve is defined by the long Weierstrass form

$$y^2 + xy + y = x^3 - x^2 - ax - b$$

where the coefficients are

$a = -20067762415575526585033208209338542750930230312178956502$

$b =$

$344816117950305564670329856903907203748559443593191803612660082962919394487322434292$