23MAC260 Problem Sheet 7: Solutions

Week 7 Lectures
Last updated April 16, 2024

1. Prove that if E is an elliptic curve given by an integral model

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

then the coordinates of any point $(x, y) \in E(\mathbb{Q})$ must be of the form

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

for some integers $m,\ n,\ d$ with $\gcd(m, d) = \gcd(n, d) = 1$.

Solution: Suppose $(x, y) \in E(\mathbb{Q})$. We will prove the claim by looking individually at all the primes that divide the denominator of x.

Let p be any prime number. We can write x in the form

$$x = p^k \frac{r}{s}$$

where $k \in \mathbb{Z}$ and p doesn't divide either of r or s. Cubing this, we get

$$x^3 = p^{3k} \frac{r^3}{s^3}$$

Observe that p still doesn't divide either of r^3 or s^3.

Now let's look at the right-hand side of our elliptic curve equation: we get

$$\begin{aligned} x^3 + ax + b &= p^{3k} \frac{r^3}{s^3} + ap^k \frac{r}{s} + b \\ &= p^{3k} \left(\frac{r^3 + ap^{-2k} rs^2 + bp^{-3k} s^3}{s^3} \right) \\ &= p^{3k} \frac{t}{s^3} \qquad \text{where} \\ t &= r^3 + ap^{-2k} rs^2 + bp^{-3k} s^3. \end{aligned}$$

Now suppose that the prime p actually divides the denominator of x. That means the integer k appearing in our expression for x is negative: $k < 0$. That means the powers p^{-2k} and p^{-3k} appearing in t are integers. Also, since we started with an integral model, both a and b are integers. So t is an **integer**.

Moreover, looking at

$$t = r^3 + ap^{-2k}rs^2 + bp^{-3k}s^3$$

the last two terms on the right-hand side are divisible by p, but the first one r^3 isn't. That means t is not divisible by p. So we have

$$x^3 + ax + b = p^{3k}\frac{t}{s^3} \tag{A}$$

where p does not divide either t or s^3.

Now we look at the left-hand side of our elliptic curve equation. Again we can write

$$y = p^l \frac{u}{v}$$

where l is some integer and p doesn't divide either of u or v. So we get

$$y^2 = p^{2l}\frac{u^2}{v^2}. \tag{B}$$

Now we put everything together: returning to our elliptic curve equation

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

and substituting the expressions (A) and (B) we get

$$p^{2l}\frac{u^2}{v^2} = p^{3k}\frac{t}{s^3}$$

We can rearrange this to give

$$p^{2l-3k} = \frac{tv^2}{s^3u^2}$$

The left-hand side is a power of p, while everything on the right-hand side is coprime to p. This is only possible if both sides equal 1: in particular

$$2l = 3k$$

so k is even, say $k = 2j$, and hence $l = \frac{3}{2}k = 3j$.

So we get

$$x = p^{2j}\frac{t}{s},\ y = p^{3j}\frac{u}{v}$$

where $j < 0$ and s, t, u, v are all coprime to p.

Finally, we repeat the same argument for all the primes $p_1, \ldots, p_r$ dividing the denominator of x, find corresponding negative integers $j_1, \ldots, j_r$. If we set $d = p_1^{-j_1} \cdots p_r^{-j_r}$ then we have

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

where $\gcd(m, d) = \gcd(n, d) = 1$. Since all the primes dividing the denominator of x are factors of d, this imples that m and n are integers, as required.

2. On the elliptic curve E given by

$$y^2 = x^3 - x + 1$$

find:

(a) a point P with $h_x(P) > 0$;

(b) a point Q with $h_x(Q) > 1$;

(c) a point R with $h_x(R) > 10$.

(Hint: keep doubling!)

Solution: Let's start with the definitions. For a rational number t written in lowest terms as $t = p/q$ we define

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

For a point $P \in E(\mathbb{Q})$ with coordinates $P = (x, y)$ we define

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

Now, on the given curve E there is a fairly easy-to-spot rational point, namely $P = (1, 1)$. But

$$h_x(P) = \ln 1 = 0$$

so we have to keep looking. As the hint suggest, we can try repeatedly doubling the point P and see what happens.

In Week 3 we wrote down a formula (valid for curves in short Weierstrass form) for the x-coordinate of $2P$ in terms of the x-coordinate of P: it was

$$x(2P) = m^2 - 2x(P)$$

where m denotes the slope of the tangent line to the curve at P. In our case this gives

$$x(2P) = \left(\frac{3x^2 - 1}{2y}\right)\Bigg|_P^2 - 2x(P)$$

An important thing to note is that since $y^2 = x^3 - x + 1$, we can actually write everything in this formula just in terms of $x(P)$:

$$x(2P) = \left(\frac{(3x^2-1)^2}{4(x^3-x+1)} \right) \Bigg|_P - 2x(P)$$

In practice this is useful because it means that to compute the heghts of $2P, 4P, \ldots$ we only nee to calculate the x-coordinates, and can forget about the y-coordinates.

Plugging in $x(P) = 1$ into the above, we get

$$x(2P) = \left(\frac{(3(1)^2-1)^2}{4(1^3-1+1)} \right) - 2 \cdot 1 = -1.$$

So $h_x(2P) = 0$ still. That's disappointing, but let's keep doubling. We can compute $x(4P)$ by applying the doubling formula to $2P$, to get

$$x(4P) = \left(\frac{(3x^2-1)^2}{4(x^3-x+1)} \right) \Bigg|_{2P} - 2x(2P) = 3$$

So $h_x(4P) = \ln 3 > 1$. This answers Part (a) and Part (b).

Finally, what about Part (c)? We keep doubling to find

$$\begin{aligned} x(8P) &= \left(\frac{(3x^2-1)^2}{4(x^3-x+1)} \right) \Bigg|_{4P} - 2x(4P) \\ &= \frac{19}{25} \end{aligned}$$

so $h_x(8P) = \ln 25 \approx 3.22$. We're looking for a point of height larger than 10, so we need to go further: with the help of a calculator we compute

$$\begin{aligned} x(16P) &= \left(\frac{(3x^2-1)^2}{4(x^3-x+1)} \right) \Bigg|_{8P} - 2x(8P) \\ &= -\frac{350701}{265225} \end{aligned}$$

so $h_x(16P) = \ln(350701) \approx 12.77$.

3. (Non-examinable) Prove that for an elliptic curve E given by an equation

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

the Kummer map

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

is a group homomorphism. (Remember that the group operation on the right-hand side is multiplication.)

Solution: We want to prove that for $P, Q \in E(\mathbb{Q})$ we have

$$\delta(P \oplus Q) = \delta(P)\delta(Q).$$

The definition of δ was as follows: if $P \in E(\mathbb{Q})$ then

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

Here $[x]$ denotes the coset in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ containing the number x.

Before we start, observe that every element of the group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is its own multiplicative inverse: to see this, note that for any $q \in \mathbb{Q}^\times$ we can write

$$\begin{aligned} [q] &= \left[\frac{q}{q^2}\right] \qquad \text{(since } q^2 \text{ is a square)} \\ &= \left[\frac{1}{q}\right]. \end{aligned}$$

Now let's consider the case when P, Q, and $P \oplus Q$ are points in $E(\mathbb{Q})$ none of which equals O or $(0,0)$. We know that the x-coordinate $x(P \oplus Q)$ is the third root (besides $x(P)$ and $x(Q)$ of the equation

$$(mx + c)^2 = x(x^2 + ax + b) \tag{*}$$

where m is the slope of the line $\overline{PQ}$. We can rearrange equation $(*)$ to read

$$x^3 + (a - m^2)x^2 + (b - 2mc)x - c^2 = 0.$$

The product of the roots equals the negative of the constant term, so we get

$$x(P) \cdot x(Q) \cdot x(P \oplus Q) = c^2$$

hence

$$x(P \oplus Q) = c^2 \cdot \frac{1}{x(P)} \frac{1}{x(Q)}.$$

Since c^2 is a square, passing to the quotient group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ we get the equation of cosets

$$\begin{aligned} [x(P \oplus Q)] &= \left[\frac{1}{x(P)}\right] \cdot \left[\frac{1}{x(Q)}\right] \\ &= [x(P)] \cdot [x(Q)] \qquad \text{(as explained above);} \end{aligned}$$

in other words

$$\delta(P \oplus Q) = \delta(P)\delta(Q)$$

as required.

The remaining cases where one of P, Q, or $P \oplus Q$ equals $(0, 0)$ are similar; the cases where one of them equals O are straightforward.