23MAC260 Elliptic Curves: Week 6

Last updated: February 27, 2024

1 Reduction mod p

In Week 5 we saw how the Nagell-Lutz Theorem allows us to compute the torsion subgroup $T \subset E(\mathbb{Q})$ for an elliptic curve E defined over $\mathbb{Q}$. The main drawback of Nagell–Lutz is that for a given curve E, there may be lots of integers whose square divides the discriminant Δ of E. This week we will look at an alternative method for computing T, based on reduction modulo primes.

Notation: Recall that for a prime number p, the field $\mathbb{F}_p$ consists of the elements $\{0, 1, \ldots, p-1\}$ with the operations of addition and multiplication mod p.

Definition 1.1. *Let p be a prime number. We define the* **reduction mod p** *map*

$$r_p \colon \mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{F}_p}$$

as follows: for a point $q \in \mathbb{P}^2_{\mathbb{Q}}$, choose homogeneous coordinates $q = [x, y, z]$ where $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Then we define

$$r_p(q) = [\overline{x}, \overline{y}, \overline{z}]$$

where $\overline{x}$ denotes the reduction of x mod p and similarly for $\overline{y}$ and $\overline{z}$.

Example: Take $p = 2$. Consider the point

$$q = \left[2, \frac{2}{3}, \frac{2}{5}\right] \in \mathbb{P}^2_{\mathbb{Q}}.$$

To compute the reduction of q mod p, we first scale the homogeneous coordinates to make them integers, then scale to eliminate any common factors. This gives

$$\begin{aligned} q &= \left[2, \frac{2}{3}, \frac{2}{5}\right] \\ &= [30, 10, 6] \\ &= [15, 5, 3]. \end{aligned}$$

Now we can reduce mod 2:

$$\begin{aligned} r_2(q) &= [\overline{15}, \overline{5}, \overline{3}] \\ &= [1, 1, 1] \in \mathbb{P}^2_{\mathbb{F}_2}. \end{aligned}$$

Now let E be an elliptic curve over $\mathbb{Q}$ defined by an integral model

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

and let p be a prime number.

Definition 1.2. *The* **reduction mod** p *of* E *is the curve* $\overline{E}$ *over the field* $\mathbb{F}_p$ *defined by the equation*

$$\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}$$

where $\overline{a} = a \bmod p$ *and* $\overline{b} = b \bmod p$.

Lemma 1.3. *If* $q \in \mathbb{P}^2_{\mathbb{Q}}$ *is a point such that* $q \in E(\mathbb{Q})$, *then* $r_p(q) \in \overline{E}(\mathbb{F}_p)$.

In other words, r_p *maps points of* $E(\mathbb{Q})$ *to points of* $\overline{E}(\mathbb{F}_p)$.

Proof. Say $q = [x, y, z]$ with x, y, $z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Then $q \in E(\mathbb{Q})$ means that

$$y^2 z = x^3 + axz^2 + bz^3.$$

Reducing this equation mod p we get

$$\overline{y}^2\overline{z} = \overline{x}^3 + \overline{a}\,\overline{x}\,\overline{z}^2 + \overline{b}\overline{z}^3$$

which says exactly that the point $r_p(q) = [\overline{x}, \overline{y}, \overline{z}]$ is in the set $\overline{E}(\mathbb{F}_p)$. □

We need to take care when reducing mod p: even if E is a perfectly good elliptic curve over $\mathbb{Q}$, its reduction mod p might not be an elliptic curve any more. But we can easily find the "bad" primes p for which this happens:

Proposition 1.4. *Let* E *and* $\overline{E}$ *be as above. For any* **odd** *prime such that* $p \nmid \Delta$, *the reduction* $\overline{E}$ *is an elliptic curve over* $\mathbb{F}_p$.

Proof. Our proof from Week 3 that showed that $x^3 + ax + b$ has a multiple root if and only if $\Delta = 0$ works just as well in any field $\mathbb{F}_p$ with $p \neq 2$, 3.

For $\mathbb{F}_3$ we compute

$$\begin{aligned} \frac{d}{dx}(x^3 + ax + b) &= 3x^2 + a \\ &= a \end{aligned}$$

so our cubic has a multiple root if and only if $a = 0$. On the other hand

$$\begin{aligned} \Delta = -4a^3 - 27b^2 &= -a^3 \\ &= -a \end{aligned}$$

since $a^3 = a$ for any $a \in \mathbb{F}_3$. So again in this case, $\Delta \neq 0$ if and only our cubic does not have a multiple root.

Finally if E is an elliptic curve given by an integral model with discriminant Δ, then

$$\Delta \bmod p = -4\overline{a}^3 - 27\overline{b}^2$$

which is exactly the discriminant of $\overline{E}$. So $\overline{E}$ has discriminant 0 if and only if $\Delta = 0 \bmod p$, that is, if and only if p divides Δ. □

So as long as $p \nmid \Delta$ we know that $\overline{E}$ is an elliptic curve. We can use this to get information about the torsion subgroup, thanks to the following theorem:

Theorem 1.5 (Torsion Embedding)**.** *Let E be an elliptic curve over $\mathbb{Q}$ defined by an integral model*

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

Let p be an odd prime such that $p \nmid \Delta$, and let $\overline{E}$ be the elliptic curve over $\mathbb{F}_p$ given by

$$\overline{E} : \; y^2 = x^3 + \overline{a}x + \overline{b}.$$

Then:

(a) The reduction mod p map

$$r_p \colon E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$$

is a group homomorphism.

(b) If $T \subset E(\mathbb{Q})$ is the torsion subgroup, then

$$T \cap \ker(r_p) = \{O\}.$$

Hence r_p gives an embedding (that is, an injective homomorphism)

$$r_p \colon T \hookrightarrow \overline{E}(\mathbb{F}_p).$$

Proof. To prove (a), first note that for any point $S = (x, y)$ we have $O * S = (x, -y)$, so

$$\begin{aligned} r_P(O * S) &= r_P([x, -y, 1]) \\ &= [\overline{x}, -\overline{y}, 1] \\ &= O * r_P(S). \end{aligned}$$

Now suppose that P_1 and P_2 are points in $E(\mathbb{Q})$. Let $P_3 = P_1 * P_2$, so that $P_1 \oplus P_2 = O * P_3$. Then P_1, P_2, P_3 lie on a line L. Since L contains 3 points of $E(\mathbb{Q})$, it is defined by a linear equation with rational coefficients: clearing denominators and cancelling common factors as before, we can assume L is defined by

$$L : \; ax + by + cz = 0$$

where a, b, c are integers with $operatornamegcd(a, b, c) = 1$.

Now reduce mod p to get a line $\overline{L}$ in $\mathbb{P}^2_{\mathbb{F}_p}$ defined by

$$\overline{L} : \; \overline{a}x + \overline{b}y + \overline{c}z = 0$$

(noting that not all of $\overline{a}$, $\overline{b}$, $\overline{c}$ can be zero).

By Lemma 1.3 each of the points $r_p(P_i)$ lies on $\overline{E}$, and by the same argument, each of them lies on $\overline{L}$ also. By Week 2 Lemma 1.1 (which applies to any algebraically closed field), the intersection $\overline{E} \cap \overline{L}$ consists of at most 3 points. So we have shown

$$\overline{E} \cap \overline{L} = \{r_p(P_1),\ r_p(P_2),\ r_p(P_3)\}.$$

This means that

$$\begin{aligned} r_P(P_1 \oplus P_2) &= r_P(O * P_3) \\ &= O * r_P(P_3) \\ &= O * (r_P(P_1) * r_p(P_2)) \\ &= r_P(P_1) \oplus r_P(P_2). \end{aligned}$$

To prove (b), let $Q \in T$ be any point other than the identity O. By the Integrality Theorem, the point Q has affine coordinates $Q = (x, y)$ with x, $y \in \mathbb{Z}$. So in homogeneous coordinates we have

$$\begin{aligned} Q &= [x, y, 1] \quad \text{hence} \\ r_p(Q) &= [\overline{x}, \overline{y}, 1]. \end{aligned}$$

This shows $r_P(Q) \neq O$, so $Q \notin \ker(r_P)$. □

Corollary 1.6. *Let E be as above, p an odd prime such that $p \nmid \Delta$, and $\overline{E}$ the reduction of E mod p. Then the order of T divides the order of $\overline{E}(\mathbb{F}_p)$: that is,*

$$|T| \mid \left|\overline{E}(\mathbb{F}_p)\right|.$$

Proof. By Theorem 1.5, for $p \nmid \Delta$ the torsion subgroup $T \subset E(\mathbb{Q})$ is isomorphic to a subgroup of $\overline{E}(\mathbb{F}_p)$, so Lagrange's theorem says that the order of T must divide the order of $\overline{E}(\mathbb{F}_p)$. □

2 Examples

In this section we'll use the Torsion Embedding Theorem to compute the torsion subgroup in some examples.

Example 1. Consider the elliptic curve

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

First we calculate the discriminant of E: it is

$$\Delta = -27 \cdot 4^2 = -2^4 \cdot 3^3$$

Hence for any $p \neq 2$, 3, the reduction of E mod p is an elliptic curve.

So let's take $p = 5$, and let $\overline{E}$ be the reduction of E mod 5: it is given by the equation

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

We can find the number of points in $\overline{E}(\mathbb{F}_5)$ just by tabulation: we substitute each $x \in \mathbb{F}_5$ into the equation above, then find the solutions for y if any. Before we start it's useful to recall which elements of $\mathbb{F}_5$ are squares:

$$0^2 = 0,\ 1^2 = 1 = 4^2,\ 2^2 = 4 = 3^2.$$

So the squares are 0, 1, and 4.

Now we make our table:

x	0	1	2	3	4
x^3	0	1	3	2	4
$y^2 = x^3 + 4$	4	0	2	1	3
y	± 2	0	–	± 1	–

So we have

$$\overline{E}(\mathbb{F}_5) = \{O, (0, \pm 2), (1, 0), (3, \pm 1)\}.$$

This is a group with 6 elements, and so Theorem 1.5 tells us that $|T|$ divides 6. Which divisor of 6 is it?

To decide this, note that T does not contain an element of order 2. Any such element would be a point of T with y-coordinate equal to 0, in other words a point $(x, 0)$ where x is a **rational** solution of $x^3 + 4 = 0$. But this equation has no rational solutions. Any group of order 2 contains an element of order 2, and any abelian group of order 6 is isomorphic to $\mathbb{Z}_6$ which contains an element of order 2. So T cannot have order 2 or 6.

The only remaining possibilities are $|T| = 1$ or $|T| = 3$. Now, $E(\mathbb{Q})$ contains the point $P = (0, 2)$; computing the tangent line to E at P, we find it is given by the equation $y = 2$. When $y = 2$, our curve equation has the only solution $x = 0$. So the tangent line at P must meet E with multiplicity 3 at P, in other words $P * P = P$. So we have

$$\begin{aligned} P \oplus P &= O * P \\ &= -P \end{aligned}$$

hence $3P = O$. This shows that P is a point of order 3 on $E(\mathbb{Q})$. Hence the torsion subgroup contains an element of order 3. So we must have $|T| = 3$, and hence

$$T = \langle P \rangle \cong \mathbb{Z}_3.$$

Example 2. Let's see an example where the advantage of this method over Nagell–Lutz is very clear. Consider the elliptic curve

$$E\colon y^2 = x^3 + 18x + 72.$$

Here the discriminant is

$$\begin{aligned} \Delta &= -4(18)^3 - 27(72)^2 \\ &= -163296 \\ &= -2^5 \cdot 3^6 \cdot 7. \end{aligned}$$

To apply Nagell–Lutz here, we would have to consider $y = 0$ and $|y| = 2^a 3^b$ with $a \in \{0, 1, 2\}$, $b \in \{0, 1, 2, 3\}$. This would take a lot of work!

Instead we will reduce modulo 5 and 11, which are the 2 smallest primes not dividing Δ. Let's see what this tells us.

- $\overline{E}(\mathbb{F}_5)$: reducing our equation mod 5 we get

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

and tabulating the solutions we get

x	0	1	2	3	4
$y^2 = x^3 + 3x + 2$	2	1	1	3	3
y	$-$	± 1	± 1	$-$	$-$

So

$$\overline{E}(\mathbb{F}_5) = \{O, (1, \pm 1), (2, \pm 1)\}$$

which tells us that $|T|$ divides 5.

- $\overline{E}(\mathbb{F}_{11})$ reducing our equation mod 11 we get

$$y^2 = x^3 + 7x + 6.$$

To tabulate the solutions, let's first list the squares in $\mathbb{F}_{11}$:

$$0^2 = 0,\ 1^2 = 10^2 = 1,\ 2^2 = 9^2 = 4,\ 3^2 = 8^2 = 9,\ 4^2 = 7^2 = 5,\ 5^2 = 6^2 = 3.$$

Now we can make our table:

x	0	1	2	3	4	5	6	7	8	9	10
$y^2 = x^3 + 7x + 6$	6	3	6	10	10	1	0	2	2	6	9
y	$-$	± 5	$-$	$-$	$-$	± 1	0	$-$	$-$	$-$	± 3

So

$$\overline{E}(\mathbb{F}_{11}) = \{O, (1, \pm 5), (5, \pm 1), (6, 0), (10, \pm 3)\}$$

which tells us that $|T|$ divides 8.

Putting these two results together, we see that $|T|$ divides both 5 and 8, hence divides $\gcd(5, 8) = 1$. This means $|T| = 1$, that is,

$$T = \{O\}.$$

3 Bounds on the number of points (Non-examinable)

In this final section, we mention some contrasting results about the numbers of points of finite order on elliptic curves over $\mathbb{Q}$ and over $\mathbb{F}_p$.

3.1 Torsion over $\mathbb{Q}$

Surprisingly, for elliptic curves over the rational numbers, there is a small finite list of possible torsion subgroups:

Theorem 3.1 (Mazur, 1977)**.** *Let* E *be an elliptic curve over* $\mathbb{Q}$ *and* $T \subset E(\mathbb{Q})$ *its torsion subgroup. Then* T *is isomorphic to one of the following groups:*

$$\begin{array}{ll} \{O\} & \textit{(the trivial group)} \\ \mathbb{Z}_n & \textit{for } n \in \{2,3,4,5,6,7,8,9,10,12\} \\ \mathbb{Z}_2 \oplus \mathbb{Z}_{2n} & \textit{for } n \in \{1,2,3,4\}. \end{array}$$

In particular we always have $|T| \leq 16$.

It was known long before Mazur's theorem that, for each group G on the list above, there is an elliptic curve E defined over $\mathbb{Q}$ such that the torsion subgroup $T \subset E(\mathbb{Q})$ is isomorphic to G. But some of these are hard to find:

Example: The biggest possible torsion subgroup is $\mathbb{Z}_2 \oplus \mathbb{Z}_8$ with order 16. The simplest (!) curve E with torsion subgroup T isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_8$ is given by the following minimal integral model:

$$E\colon y^2 = x^3 - 1386747x + 368636886.$$

3.2 Finite fields

For elliptic curves over finite fields, the picture is quite different. Since there are only finitely many points altogether in the projective plane $\mathbb{P}^2_{\mathbb{F}_p}$, in this case **every** point on an elliptic curve has finite order. The number of points on such a curve cannot be too far away from p:

Theorem 3.2 (Hasse)**.** *Let* E *be an elliptic curve over* $\mathbb{F}_p$*. Then*

$$|E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

We won't prove Hasse's theorem, but let's give an intuitive argument for why we expect the number of points to be close to $p+1$.

Let E be defined by an equation $y^2 = f(x)$. Then

$$|E(\mathbb{F}_p)| = 1 + \#\{x \mid f(x) = 0\} + 2\#\{x \mid f(x) \text{ is a nonzero square in } \mathbb{F}_p\}.$$

Now **assume** that the values of $f(x)$ are distributed identically to the values of x: that is, $x \mapsto f(x)$ is a bjection on $\mathbb{F}_p$. Then:

$$\#\{x \mid f(x) = 0\} = 1$$
$$\#\{x \mid f(x) \text{ is a nonzero square in } \mathbb{F}_p\} = \#\text{ nonzero squares in } \mathbb{F}_p.$$

The nonzero squares in $\mathbb{F}_p$ are the image of the 2-to-1 map

$$\begin{aligned} \mathbb{F}_p \setminus \{0\} &\to \mathbb{F}_p \setminus \{0\} \\ x &\mapsto x^2. \end{aligned}$$

So the number of points in the image is $\frac{1}{2}(p-1)$. Therefore, under our assumpotion we get

$$\begin{aligned} |E(\mathbb{F}_p)| &= 1 + 1 + 2 \cdot \frac{1}{2}(p-1) \\ &= p + 1. \end{aligned}$$

In practice the assumption above does not hold, but Hasse proved that the error is of order $\sqrt{p}$.

Example: Take $p = 97$. For any elliptic curve E over $\mathbb{F}_p$, Hasse's theorem tells us that the number of $\mathbb{F}_p$-points on E satisfies

$$98 - 2\sqrt{97} \leq |E(\mathbb{F}_p)| \leq 98 + 2\sqrt{97}$$

The upper bound is approximately 117.69, so $|E(\mathbb{F}_p)|$ is at most 117.

Now consider the curve

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

A computer calculation (which you can check!) shows that the $\mathbb{F}_p$-points on E are exactly those points of $\mathbb{P}^2_{\mathbb{F}_p}$ with the following homogeneous coordinates:

$[0,1,0]$	$[0,14,1]$	$[0,83,1]$	$[1,10,1]$	$[1,87,1]$	$[4,39,1]$
$[4,58,1]$	$[6,11,1]$	$[6,86,1]$	$[7,32,1]$	$[7,65,1]$	$[10,41,1]$
$[10,56,1]$	$[11,13,1]$	$[11,84,1]$	$[12,9,1]$	$[12,88,1]$	$[13,29,1]$
$[13,68,1]$	$[15,46,1]$	$[15,51,1]$	$[16,11,1]$	$[16,86,1]$	$[17,29,1]$
$[17,68,1]$	$[20,40,1]$	$[20,57,1]$	$[21,40,1]$	$[21,57,1]$	$[23,23,1]$
$[23,74,1]$	$[27,24,1]$	$[27,73,1]$	$[28,41,1]$	$[28,56,1]$	$[29,23,1]$
$[29,74,1]$	$[30,6,1]$	$[30,91,1]$	$[32,9,1]$	$[32,88,1]$	$[33,7,1]$
$[33,90,1]$	$[35,10,1]$	$[35,87,1]$	$[36,1,1]$	$[36,96,1]$	$[39,32,1]$
$[39,65,1]$	$[40,46,1]$	$[40,51,1]$	$[41,21,1]$	$[41,76,1]$	$[42,46,1]$
$[42,51,1]$	$[43,39,1]$	$[43,58,1]$	$[45,23,1]$	$[45,74,1]$	$[46,12,1]$
$[46,85,1]$	$[47,36,1]$	$[47,61,1]$	$[50,39,1]$	$[50,58,1]$	$[51,32,1]$
$[51,65,1]$	$[53,9,1]$	$[53,88,1]$	$[54,36,1]$	$[54,61,1]$	$[55,33,1]$
$[55,64,1]$	$[56,40,1]$	$[56,57,1]$	$[57,33,1]$	$[57,64,1]$	$[58,12,1]$
$[58,85,1]$	$[59,41,1]$	$[59,56,1]$	$[61,10,1]$	$[61,87,1]$	$[62,1,1]$
$[62,96,1]$	$[67,29,1]$	$[67,68,1]$	$[72,24,1]$	$[72,73,1]$	$[73,7,1]$
$[73,90,1]$	$[75,11,1]$	$[75,86,1]$	$[76,21,1]$	$[76,76,1]$	$[77,21,1]$
$[77,76,1]$	$[80,6,1]$	$[80,91,1]$	$[82,33,1]$	$[82,64,1]$	$[84,6,1]$
$[84,91,1]$	$[88,7,1]$	$[88,90,1]$	$[89,13,1]$	$[89,84,1]$	$[90,12,1]$
$[90,85,1]$	$[93,36,1]$	$[93,61,1]$	$[94,13,1]$	$[94,84,1]$	$[95,24,1]$
$[95,73,1]$	$[96,1,1]$	$[96,96,1]$			

In particular we obtain $|E(\mathbb{F}_p)| = 117$, showing that the Hasse bound is optimal at least for $p = 97$.