MATH70064: Elliptic Curves

Coursework 2

CID: 02034074

December 6, 2024

Question 1

1. We can simply check all $x \in \mathbb{F}_5$ and see if there are any corresponding $y \in \mathbb{F}_5$ such that $y^2 = x^3 + x$.

x	0	1	2	3	4
y	0	-	0	-	-

   Seeing as there are exactly three points—namely, $(0, 0)$, $(2, 0)$, and $\mathcal{O}$, the point at infinity—that satisfy the relation, the group $E(k)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, the cyclic group with three elements.

2. We can simply check all $x \in \mathbb{F}_5$ and see if there are any corresponding $y \in \mathbb{F}_5$ such that $y^2 = x^3 + 2x$.

x	0	1	2	3	4
y	0	-	-	0	-

   Seeing as there are exactly three points—namely, $(0, 0)$, $(3, 0)$, and $\mathcal{O}$, the point at infinity—that satisfy the relation, the group $E(k)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, the cyclic group with three elements.

3. We can simply check all $x \in \mathbb{F}_3$ and see if there are any corresponding $y \in \mathbb{F}_3$ such that $y^2 = x^3 + x$.

x	0	1	2
y	0	-	± 1

Seeing as there are four points—namely, $(0,0)$, $(2,1)$, $(2,-1)=(2,2)$, and $\mathcal{O}$, the point at infinity—that satisfy the relation, the group $E(k)$ is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since there is only one point of order two—namely, $(0,0)$—this group cannot be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Therefore, $E(k) \cong \mathbb{Z}/4\mathbb{Z}$.

4. We can simply check all $x \in \mathbb{F}_2$ and see if there are any corresponding $y \in \mathbb{F}_2$ such that $y^2 + y = x^3 + x^2$.

x	0	1
y	0, 1	0, 1

Seeing as there are exactly five points—namely, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, and $\mathcal{O}$, the point at infinity—that satisfy the relation, the group $E(k)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$, the cyclic group with five elements.

Question 2

The idea would be to determine the torsion points using the Nagell-Lutz Theorem. However, in order to do that, we have to put the curves in question in to Weierstrass Form.

1. Observe that

$$y^2 - y = \left(y - \frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2$$
$$x^3 - x^2 = \left(x - \frac{1}{3}\right)^3 - \frac{1}{3}\left(x - \frac{1}{3}\right) - \frac{2}{27}$$

Define $s := y - \frac{1}{2}$ and $t := x - \frac{1}{3}$. Transforming our equation into (s,t)-coordinates via this rational change of variables, we get

$$\begin{aligned} s^2 &= t^3 - \frac{1}{3}t + \frac{1}{4} - \frac{2}{27} \\ &= t^3 - \frac{36}{108}t + \frac{19}{108} \\ \iff \qquad 2^6 3^6 \cdot s^2 &= 2^6 3^6 \cdot t^3 - 36 \cdot \frac{2^6 3^6}{2^2 3^3} \cdot t + 19 \cdot \frac{2^6 3^6}{2^2 3^3} \end{aligned}$$

$$\iff \quad \left(2^3 3^3 \cdot s\right)^2 = \left(2^2 3^2 \cdot t\right)^3 - 36 \cdot 2^2 3 \cdot \left(2^2 3^2 \cdot t\right) + 19 \cdot 2^4 3^3$$
$$\iff \quad (216s)^2 = (36t)^3 - 432\,(36t) + 8208$$

Define $u := 216s = 216\left(y - \frac{1}{2}\right)$ and $v = 36t = 36\left(x - \frac{1}{3}\right)$. Transforming our equation into (u, c)-coordinates via this rational change of variables, we get the equation

$$E : u^2 = v^3 - 432v + 8208 \tag{1}$$

whose group of rational points is isomorphic to that of the original curve. If we can compute the torsion points of this group, we can simply push it back through this change of coordinates to recover the required points.

We aim to apply Corollary 5.31 in the notes. To that end, we compute the value D for the curve (1) to be $2\left(27 \cdot 8208^2 - 4 \cdot 432^3\right) = 2993075712 = 2^9 \times 3^{12} \times 11$. Since 5 does not divide this quantity, we have that $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \overline{E}(\mathbb{F}_5)$. Indeed, we have

$$\overline{E} : u^2 = v^3 - 2v + 3$$

We can now enumerate all possible solutions over $\mathbb{F}_5$ of this reduced curve.

v	0	1	2	3	4
u	-	-	-	± 1	± 2

This means that $\overline{E}(\mathbb{F}_5) = \{\mathcal{O}, (3, \pm 1), (4, \pm 2)\} \cong \mathbb{Z}/5\mathbb{Z}$. Therefore, $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/5\mathbb{Z}$. It must hence either be trivial or isomorphic to $\mathbb{Z}/5\mathbb{Z}$ itself. It therefore suffices to identify a nontrivial torsion point. Indeed, we can find such a point in $(v, u) = (-12, -108)$. See Figure 1.

2. We begin by putting the equation into Weierstrass form. We have

$$y^2 + xy = y^2 + xy + \frac{x^2}{4} - \frac{x^2}{4} = \left(y + \frac{x}{2}\right)^2 - \frac{x^2}{4}$$

Define $\tilde{y} = y + \frac{x}{2}$. The equation of E is then given by

$$\tilde{y}^2 - \frac{x^2}{4} - 5\left(\tilde{y} - \frac{x}{2}\right) = x^3 - 5x^2$$
$$\iff \quad 4\tilde{y}^2 - 20\tilde{y} = 4x^3 - 19x^2 - 10x$$

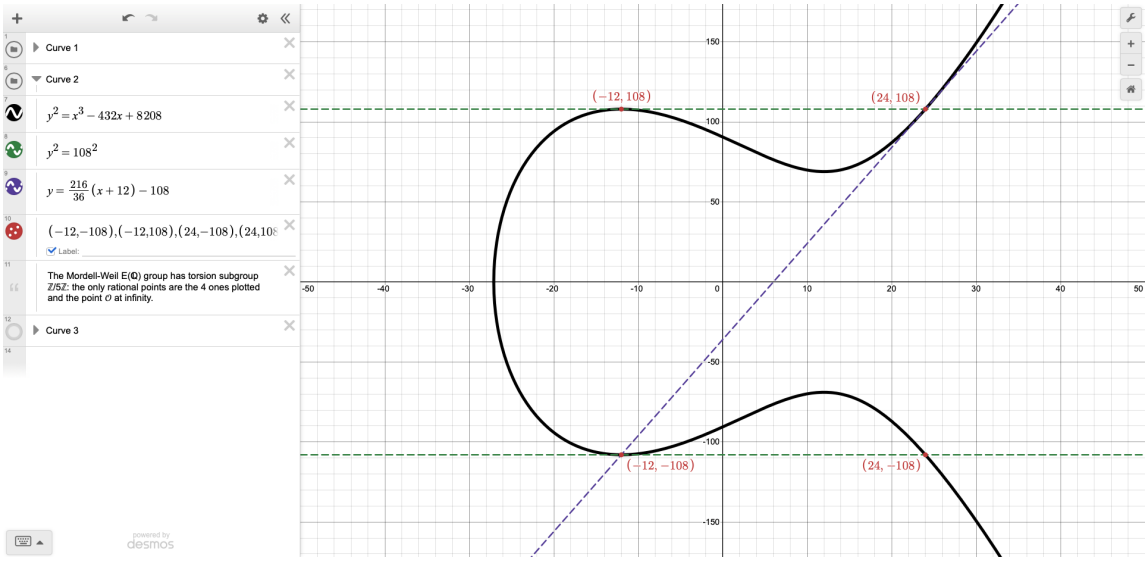

Figure 1: The non-$\mathcal{O}$ points in $E(\mathbb{Q})_{\text{tors}}$.

$$\iff \qquad 4\left(\tilde{y} - \frac{5}{2}\right)^2 - 25 = 4\left(x - \frac{19}{12}\right)^3 - \frac{481}{12}\left(x - \frac{19}{12}\right) - \frac{10,279}{216}$$

Define $s := 2\left(\tilde{y} - \frac{5}{2}\right)$ and $t := \left(x - \frac{19}{12}\right)$. Then, the equation of E in (t, s)-coordinates is

$$s^2 = 4t^3 - \frac{481}{12}t - \frac{4879}{216}$$

$$\iff \qquad 3^6 2^4 \cdot s^2 = 3^6 2^4 \cdot 2^2 \cdot t^3 - 481 \cdot \frac{3^6 2^4}{3^1 2^2} \cdot t - 4879 \cdot \frac{3^6 2^4}{3^3 2^3}$$

$$\iff \qquad \left(3^3 2^2 \cdot s\right)^2 = \left(3^2 2^2 \cdot t\right)^3 - 481 \cdot 3^3 \left(3^2 2^2 \cdot t\right) - 4879 \cdot 3^3 \cdot 2$$

Define $u := 108s$ and $v := 36t$. We then get an equation for E in (v, u)-coordinates that is in Weierstrass Form:

$$u^2 = v^3 - 12,987v - 263,466 \tag{2}$$

To determine a prime p modulo which to reduce, we first compute the quantity

$$D = 2\left(27 \times 263,466^2 - 4 \times 12,987^3\right) = -13,774,950,720,000 = -2^9 \times 3^{16} \times 5^4$$

We can therefore pick $p = 7$. We then know that $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \overline{E}(\mathbb{F}_7)$. We begin by computing the mod 7 reduction $\overline{E}$ of E:

$$u^2 = v^3 - 2v = v^3 + 5v$$

We can now enumerate all possible solutions over $\mathbb{F}_7$ of this reduced curve.

v	0	1	2	3	4	5	6
u	0	-	± 2	0	0	-	± 1

Clearly, $\overline{E}(\mathbb{F}_7)$ is of order 8, making it isomorphic to one of the following:

$$\mathbb{Z}/8\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Lagrange's Theorem then tells us that $|E(\mathbb{Q})_{\text{tors}}| \in \{1, 2, 4, 8\}$.

We can use the observation that

$$v^3 - 12,987v - 263,466 = (v + 21)(v + 102)(v - 123)$$

to conclude that $E(\mathbb{Q})_{\text{tors}}$ must contain at least three nontrivial points, making it a subgroup of order 4 or 8 of $\overline{E}(\mathbb{F}_7)$.

Now, the fact that these points are of order 2 also eliminates $\mathbb{Z}/8\mathbb{Z}$ as a candidate for $\overline{E}(\mathbb{F}_7)$. Furthermore, since we have exactly three points of order two in $\overline{E}(\mathbb{F}_7)$ (and cannot have any more, because we are looking at roots of a degree 3 polynomial in v) eliminates $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as a candidate for $\overline{E}(\mathbb{F}_7)$. We can therefore conclude that $E(\mathbb{Q})_{\text{tors}}$ is a subgroup of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Given this piece of information, we can conclude that the points of order 2 in $E(\mathbb{Q})_{\text{tors}}$ must be mapped to the elements $(1,0), (0,2), (1,2) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, as these are the *only* elements of order 2 in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Seeing as the set $\{(0,0), (1,0), (0,2), (1,2)\} \subset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ is not closed under the group operation, it is not a subgroup, and the smallest (and only) subgroup containing it must be all of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. We can therefore conclude that the injection is, in fact, an isomorphism, ie, we have

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

See Figure 2.

3. Let E denote our elliptic curve. We begin by expressing E in Weierstrass Form. We

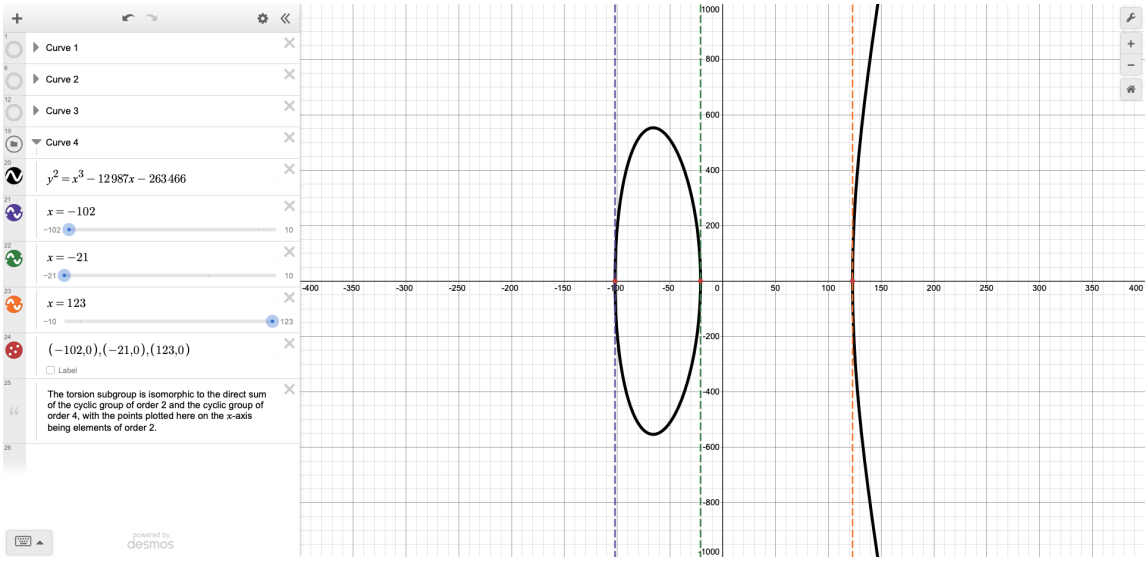

Figure 2: Points of order 2 in $E(\mathbb{Q})_{\text{tors}}$.

have

$$y^2 + xy = y^2 + xy + \frac{x^2}{4} - \frac{x^2}{4} = \left(y + \frac{x}{2}\right)^2 - \frac{x^2}{4}$$

Define $s := y + \frac{x}{2}$. We then get the equation of E to be

$$\begin{aligned} s^2 &= x^3 - \frac{1}{4}x^2 - 45x + 81 \\ &= \left(x - \frac{1}{12}\right)^3 - \frac{2161}{48}\left(x - \frac{1}{12}\right) + \frac{66743}{864} \end{aligned}$$

Define $t := x - \frac{1}{12}$. We then get the equation of E to be

$$\begin{aligned} & 2^6 3^3 \cdot s^2 = 2^6 3^6 \cdot t^3 - 2161 \cdot \frac{2^6 3^6}{2^4 3^1} \cdot t + 66743 \cdot \frac{2^6 3^6}{2^5 3^3} \\ \iff \quad & \left(2^3 3^3 \cdot s\right)^2 = \left(2^2 3^2 \cdot t\right)^3 - 2161 \cdot 3^3 \cdot \left(2^2 3^2 \cdot t\right) + 66743 \cdot 2 \cdot 3^3 \end{aligned}$$

Define $u := 2^3 3^3 \cdot s$ and $v := 2^2 3^2 \cdot t$. Then, the equation of E in (v, u)-coordinates, and in Weierstrass Form, is

$$u^2 = v^3 - 58347v + 3954150 \tag{3}$$

To determine a prime p modulo which to reduce, we first compute the quantity

$$D = 2\left(27 \times 3954150^2 - 4 \times 58347^3\right) = -744,773,015,568,384 = -2^{19} \times 3^{17} \times 11$$

We can therefore pick $p = 5$. We then know that $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \overline{E}(\mathbb{F}_5)$, where the curve $\overline{E}$

is given by the equation

$$y^2 = v^3 - 2v = v^3 + 3v$$

We can compute $\overline{E}(\mathbb{F}_5)$ by manually considering all possible solutions.

v	0	1	2	3	4
u	0	± 2	± 2	± 1	± 1

We have that $\overline{E}(\mathbb{F}_5)$ is of order 10, making it isomorphic to either $\mathbb{Z}/10\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. However, by the Chinese Remainder Theorem, these two groups are isomorphic to each other. Hence, we know what $\overline{E}(\mathbb{F}_5)$ looks like. We must therefore have $|E(\mathbb{Q})_{\text{tors}}| \in \{1, 2, 5, 10\}$.

First, note that

$$v^3 - 58347v + 3954150 = (v - 75)\left(v^2 + 75v - 52722\right)$$

with the quadratic part being irreducible over $\mathbb{Q}$. This means that we have one (and exactly one) element of order 2, meaning that $E(\mathbb{Q})_{\text{tors}}$ is isomorphic either to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/10\mathbb{Z}$.

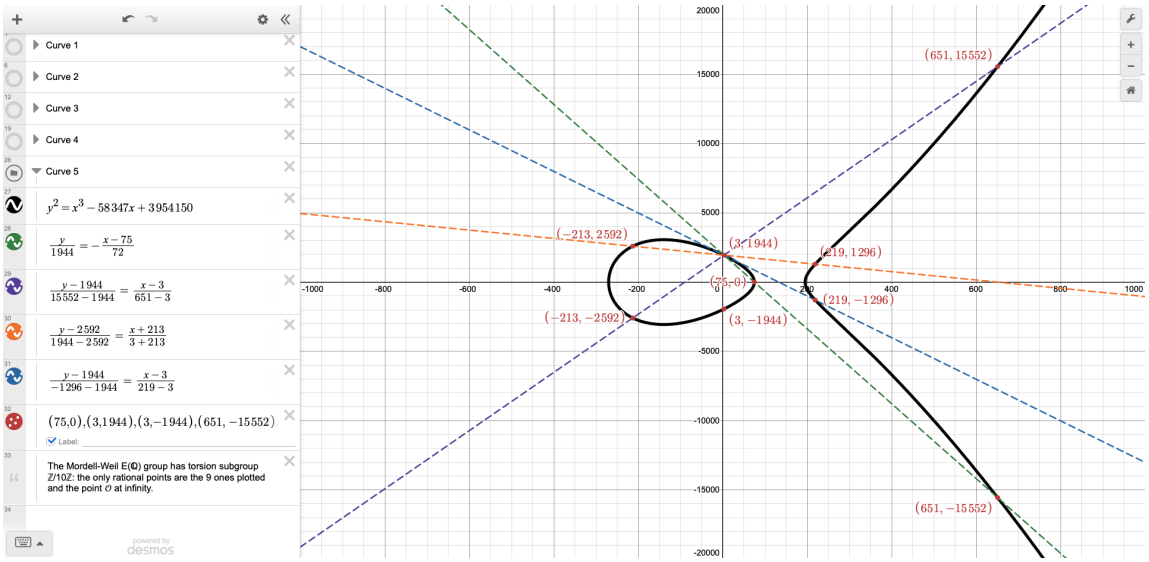

Figure 3: The non-$\mathcal{O}$ points in $E(\mathbb{Q})_{\text{tors}}$.

With some trial and error, we can find other rational points of finite order. In particular, the point $(3, 1944)$ acts as a generator, and the point $(219, -1296)$ is of order 5. These

are plotted in Figure 3. As such, we can conclude that

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/10\mathbb{Z}$$

Question 3

The Elliptic Curve we are working with is E, given by

$$y^2 = x^3 - 73x + 72 \tag{4}$$

Let $b = -73$ and $c = 72$. We have $y^2 = x^3 + bx + c$. Indeed, we have

$$4b^3 + 27c^2 = -1,416,100$$

We therefore have $D = 2\left(4b^3 + 27c^2\right) = -2832200 = -2^3 \times 5^2 \times 7^2 \times 17^2$.

(i) We apply the reduction mod 3 approach because 3 does not divide D (cf. Corollary 5.31). We have that $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \overline{E}(\mathbb{F}_3)$, where the mod 3-reduced curve $\overline{E}$ is given by

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

We can now enumerate all possible solutions over $\mathbb{F}_3$ of this reduced curve.

x	0	1	2
y	0	0	0

We therefore have that $\overline{E}(\mathbb{F}_3) = \{\mathcal{O}, (0,0), (1,0), (2,0)\}$. As an abelian group of order 4, we know that $\overline{E}(\mathbb{F}_3)$ is isomorphic either to the cyclic group or the Klein group.

We don't quite have enough to deduce what $E(\mathbb{Q})_{\text{tors}}$ is, but it turns out that the Nagell-Lutz Theorem gives us the information we need. Specifically, we can apply the fact that elements of order 2 must be precisely those with y-coordinate 0. If $y = 0$, we have that $x^3 - 73x + 72 = 0$. Indeed, we can write

$$x^3 - 73x + 72 = (x-1)(x-8)(x+9)$$

meaning that the points $(1,0)$, $(8,0)$, and $(-9,0)$ are of order 2. This tells us that

$4 \leq |E(\mathbb{Q})_{\text{tors}}|$, whereas the injection into $\overline{E}(\mathbb{F}_3)$ tells us that $|E(\mathbb{Q})_{\text{tors}}| \leq 4$. This means that $|E(\mathbb{Q})_{\text{tors}}| = 4$. Furthermore, since there are clearly three elements of order 2, we can conclude that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, ie, $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to the Klein group. See Figure 4.

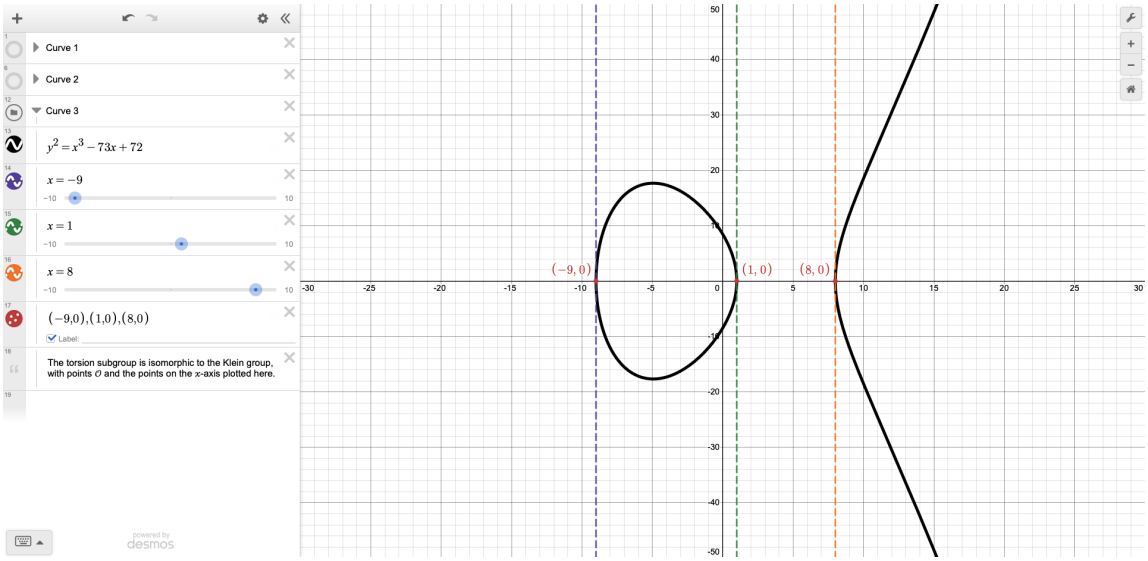

Figure 4: The non-$\mathcal{O}$ points in $E(\mathbb{Q})_{\text{tors}}$.

(ii) We show the rank is ≥ 2 by showing that there exist at least 2 free generators of $E(\mathbb{Q})$.

By trial-and-error, we can obtain the rational points $(-1, 12)$ and $(9, 12)$—see Figure 5. These must lie in the free subgroup because they are not torsion points (we already know all the torsion points). All we need to show is that $(9, 12)$ is not a multiple of $(-1, 12)$.

We do this by showing that it is neither an even multiple nor an odd multiple. We do this using the 2-descent homomorphism δ. Observe that

$$\delta(9, 12) = (9 - 1, 9 - 8, 9 + 9) = (2, 1, 2) \neq 0$$
$$\delta(-1, 12) = (-1 - 1, -1 - 8, -1 + 9) = (-2, -1, 2) \neq 0$$

Since neither point lies in $\ker(\delta)$, they are not even multiples of *any* point in $E(\mathbb{Q})$, let alone each other. Furthermore, if there existed some k such that $(9, 12) = (2k + 1)(-1, 12)$,

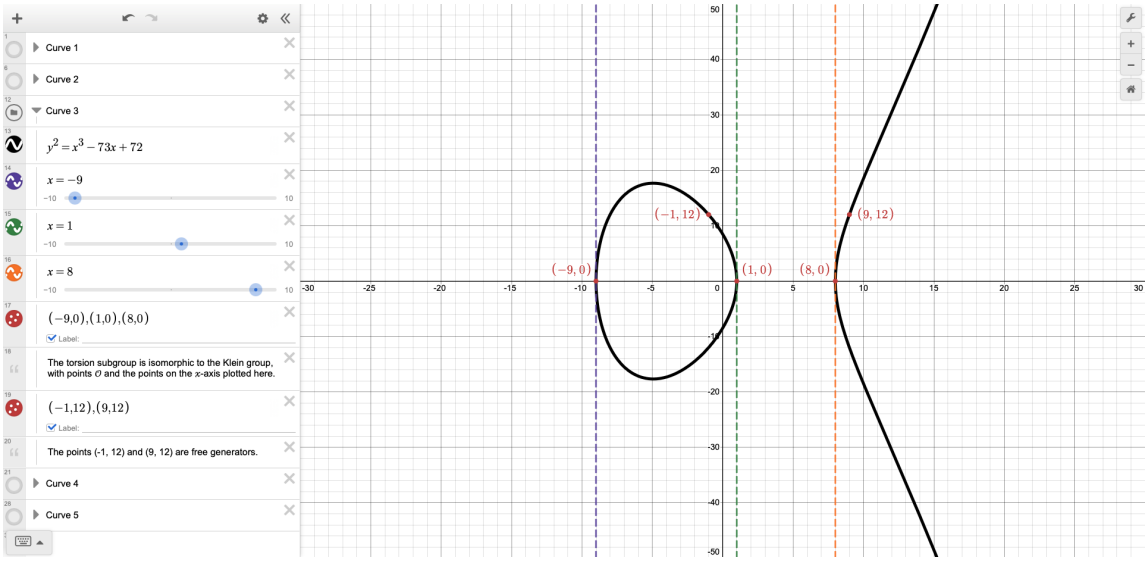

Figure 5: The non-$\mathcal{O}$ points in $E(\mathbb{Q})_{\text{tors}}$ along with two free points, which we can show to be $\mathbb{Z}$-linearly independent.

then we would have

$$\begin{aligned}\delta(9,12) &= \delta((2k+1)(-1,12)) \\ &= \delta(-1,12)^{2k+1} \\ &= \left(\delta(-1,12)^k\right)^2 \cdot \delta(-1,12) \\ &= \delta(-1,12)\end{aligned}$$

However, we can clearly see that this is not the case: we cannot multiply $(2,1,2)$ by any square to obtain $(-2,-1,2)$. Therefore, $(9,12)$ and $(-1,12)$ are not odd multiples of each other either. Therefore, they are simply not multiples of each other, making them $\mathbb{Z}$-linearly independent. Hence, the rank of E must be at least 2.

Question 5