Miniproject - Elliptic Curves

Simon Pohmann

March 18, 2022

1 Question 1

Example 1.1 (1(i))**.** Have

$$|162^2 + 6|_5 = |26250|_5 = |5^4 \cdot 7 \cdot 2 \cdot 3|_5 = 5^{-4} < 5^{-3}$$

Example 1.2 (1(ii))**.** Let

$$\alpha = 5^{-1} + 2 \cdot 5^0 + 5(1 + 4 \cdot 5) \sum_{n \geq 0} 5^{2n} \in \mathbb{Q}_5$$

Note that in $\mathbb{Q}_5$ we have

$$\sum_{n \geq 0} 5^{2n} = \sum_{n \geq 0} 25^n = \frac{1}{1 - 25} = -\frac{1}{24}$$

So

$$\alpha = \frac{1}{5} + 2 + 5(21)\frac{1}{24} = \frac{263}{40}$$

For the next exercises, we will slightly abuse notation and write

$$E(R) := \{(x, y) \in E(\bar{k}) \mid x, y \in R\} \cup \{\mathcal{O}\}$$

for an Elliptic Curve E defined over k and any ring R contained in the algebraic closure $\bar{k}$. Note that this is usually not a group anymore, and does not have a lot of nice structure.

Proposition 1.3 (1(iii))**.** Consider the Elliptic Curve $E : y^2 = x^3 + 2x + 2$ defined over $\mathbb{Z}$. Then $E(\mathbb{Z}) = \{\mathcal{O}\}$ and

$$E(\mathbb{Z}_p) \neq \{\mathcal{O}\} \iff p \neq 3$$

Proof. First show that there exists some $(x, y) \in \tilde{E}(\mathbb{F}_p)$ with $y \neq 0$ for all primes $p \neq 3$.

If $p \equiv 1, 5 \mod 8$, then -1 is a square in $\mathbb{F}_p$, thus there is $\alpha \in \mathbb{F}_p$ with $\alpha^2 = -1$ and so $(-1, \alpha) \in \tilde{E}(\mathbb{F}_p)$. If $p \equiv 7 \mod 8$, then (by Quadratic Reciprocity) it follows that 2 is a square in $\mathbb{F}_p$. Thus there is $\alpha \in \mathbb{F}_p$ with $\alpha^2 = 2$ and so $(0, \alpha) \in \tilde{E}(\mathbb{F}_p)$.

Hence, consider now the case $p \equiv 3 \mod 8$. Note that

$$\Delta(E) = 4 \cdot 2^3 + 27 \cdot 2^2 = 140 = 2^2 \cdot 5 \cdot 7$$

Hence we see that $p \nmid \Delta(E)$ and so $\tilde{E}$ is an Elliptic Curve defined over $\mathbb{F}_p$. Now the Hasse bound shows that

$$\#\tilde{E}(\mathbb{F}_p) \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$

Note that for $p > 9$ have $\sqrt{p} < p/3$ and thus

$$p + 1 - 2\sqrt{p} > 4$$

Thus $\tilde{E}(\mathbb{F}_p) \geq 5$ and so there must be $(x, y) \in \tilde{E}(\mathbb{F}_p)$ with $y \neq 0$, as there are at most four points on $\tilde{E}(\mathbb{F}_p)$ that do not satisfy this ($\mathcal{O}$ and possibly $(\alpha_i, 0)$ with α_i a root of $x^3 + 2x + 2$).

Now consider any prime $p \neq 2, 3$ and $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p), x, y \in \mathbb{Z}$. Let $f(t) := t^2 - x^3 - 2x - 2$. Then

$$|f(y)|_p \leq p^{-1} \quad \text{and} \quad |f'(y)|_p = |y|_p = 1$$

Thus $|f(y)|_p < |f'(y)|_p^2$ and Hensel's Lemma yields a root $\gamma \in \mathbb{Z}_p$ with $(x, \gamma) \in E(\mathbb{Z}_p)$.

In the case $p = 2$, note that $f(t) := t^2 - 5^3 - 2 \cdot 5 - 2 = t^2 - 137$ satisfies

$$|f(1)|_2 = |-136|_2 = |-17 \cdot 2^3|_2 = 2^{-3} < \left(2^{-1}\right)^2 = |2|_2^2 = |f'(1)|_2^2$$

and so Hensel's Lemma yields a point $(5, \gamma) \in E(\mathbb{Z}_2)$.

The only remaining case is $p = 3$, and a trying all 9 points in $\mathbb{F}_3^2$ shows that $\tilde{E}(\mathbb{F}_3) = \{\mathcal{O}\}$. This clearly shows that $E(\mathbb{Z}_3) = \{\mathcal{O}\}$ and so $E(\mathbb{Z}) = \{\mathcal{O}\}$. □

For the next exercise, we first summarize the techniques we have used above.

Proposition 1.4. Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an Elliptic Curve defined over $\mathbb{Z}$. Let p be a prime. Then

- If $E(\mathbb{Z}_p) \neq \{\mathcal{O}\}$ then $\tilde{E}(\mathbb{F}_p) \neq \{\mathcal{O}\}$.
- Suppose $p \neq 2$. There is $(x, y) \in \tilde{E}(\mathbb{F}_p)$ with $y \neq 0$ if and only if there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$.
- Suppose $p \neq 2$. If $\#\tilde{E}(\mathbb{F}_p) \geq 5$ then there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$.
- Suppose $p \geq 11$ and $p \nmid \Delta(E)$. Then there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$.

Proof. The first part is trivial and follows from the fact that any $(x, y) \in E(\mathbb{Z}_p)$ yields $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p)$.

For the second part, note that by assumption, there is $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p), x, y \in \mathbb{Z}$ with $|y|_p = 1$ and so

$$|y^2 - x^3 - a_2x^2 - a_4x - a_6|_p \leq p^{-1} < 1 = 1^2 = |2y|_p$$

Hensel's Lemma now shows that there is $\gamma \in \mathbb{Z}_p$ such that $\gamma^2 = x^3 + a_2x^2 + a_4x + a_6$ and so $(x, \gamma) \in E(\mathbb{Z}_p)$. Since $|y|_p = 1$ clearly also $|\gamma|_p = 1$. The other direction is obvious and follows directly by taking the reduction modulo p.

For the third part, notice that there are at most three different points $(x, y) \in \tilde{E}(\mathbb{F}_p)$ with $y = 0$, as in this case x is a root of the cubic $t^3+a_2t^2+a_4t+a_6$. Thus, if $\#\tilde{E}(\mathbb{F}_p) \geq 5$, there must be $(x, y) \in \tilde{E}(\mathbb{F}_p)$ with $y \neq 0$ and so the claim follows by the second part.

For the fourth part, note that as above, $p > 9$ implies $\sqrt{p} < p/3$ and so the Hasse bound yields (since $\tilde{E}$ is an Elliptic Curve by assumption, as $p \nmid \Delta(E)$)

$$\#\tilde{E}(\mathbb{F}_p) \geq p + 1 - 2\sqrt{p} > 4$$

thus $\#\tilde{E}(\mathbb{F}_p) \geq 5$. The claim now follows by the third part. □

This already shows that we do not have to worry to much about the condition $E(\mathbb{Z}_p) \neq \{\mathcal{O}\}$ for $p \neq 2, 3, 5, 7$ prime, as we expect that it is fulfilled quite often. This gives the following condition.

Proposition 1.5. Let $f_0, f_1, f_2 \in \mathbb{Z}$ and consider the Elliptic Curve $E : y^2 = x^3+f_2x^2+f_1x+f_0$. Let $p \in \{3, 5, 7\}$. Then there is no $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$ if and only if

$$\begin{aligned} p = 3 &\Rightarrow n^3 + f_2n^2 + f_1n + f_0 \equiv 0, 2 \mod 3 \\ p = 5 &\Rightarrow n^3 + f_2n^2 + f_1n + f_0 \equiv 0, 2, 3 \mod 5 \\ p = 7 &\Rightarrow n^3 + f_2n^2 + f_1n + f_0 \equiv 0, 3, 5, 6 \mod 7 \end{aligned}$$

for all $n \in \mathbb{Z}$.

In particular, this is necessary for E to satisfy the desired properties, i.e. there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$ if and only if $p \neq 3, 5, 7$ [1].

Proof. Let $p \in \{3, 5, 7\}$. Assume there is some $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p), x, y \in \mathbb{Z}$ with $\tilde{y} \neq 0$. Then have

$$y^2 \equiv x^3 + f_2x^2 + f_1x + f_0 \mod p$$

and so $x^3 + f_2x^2 + f_1x + f_0$ is a quadratic residue modulo p.

By checking all elements in $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$, one finds

$$\begin{aligned} n \text{ quadratic residue modulo } 3 &\Leftrightarrow n \equiv 0, 1 \mod 3 \\ n \text{ quadratic residue modulo } 5 &\Leftrightarrow n \equiv 0, 1, 4 \mod 5 \\ n \text{ quadratic residue modulo } 7 &\Leftrightarrow n \equiv 0, 1, 4, 2 \mod 7 \end{aligned}$$

Except for $n \equiv 0 \mod p$, these cases have been excluded by assumption. However we assumed that $y \not\equiv 0 \mod p$, so $y^2 \not\equiv 0 \mod p$ and the claim follows.

The other direction follows by reversing the above computation. The claim now follows from Proposition 1.4. □

[1] I understood the task here to be "if and only if". As mentioned later, this interpretation is probably wrong, and I will discuss the other case next.

However, there is one problem here. Using a computer, one can easily find (e.g. by trying all possibilities) that there are no $f_0, f_1, f_2 \in \mathbb{Z}$ such that the above conditions are (simultaneously) fulfilled for 3, 5 and 7. This seems to indicate that I have indeed misunderstood the task, and we only look for Elliptic Curves $E : y^2 = x^3 + f_2x^2 + f_1x + f_0$ such that there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$ for every $p \neq 3, 5, 7$, and do not require further properties for $E(\mathbb{Z}_3), E(\mathbb{Z}_5)$ and $E(\mathbb{Z}_7)$.

So instead consider a strengthening of the last part of Proposition 1.4.

Proposition 1.6. Let $p \geq 11$ be a prime and $E : y^2 = x^3 + f_2x^2 + f_1x + f_0$ an Elliptic Curve with $f_0, f_1, f_2 \in \mathbb{Z}$. Then there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$.

Proof. If $p \geq 11$ and $p \nmid \Delta(E)$ then $\tilde{E}$ is an Elliptic Curve over $\mathbb{F}_p$ and the claim follows from Proposition 1.4.

So assume now that $p \mid \Delta(E)$, hence $x^3 + f_2x^2 + f_1x + f_0$ factors as

$$x^3 + \tilde{f}_2x^2 + \tilde{f}_1x + \tilde{f}_0 \equiv (x - \alpha)^2(x - \beta)$$

with $\alpha, \beta \in \bar{\mathbb{F}}_p$. However, note that $\mathbb{F}_p$ is perfect, so $(x-\alpha)^2(x-\beta)$ cannot be irreducible over $\mathbb{F}_p$, otherwise $\mathbb{F}_p[x]/\langle(x - \alpha)^2(x - \beta)\rangle$ would be a non-separable field extension of $\mathbb{F}_p$. Thus, either $\alpha \in \mathbb{F}_p$ or $\beta \in \mathbb{F}_p$. If $\alpha \in \mathbb{F}_p$, then clearly also $\beta = -2\alpha - \tilde{f}_2 \in \mathbb{F}_p$. If $\beta \in \mathbb{F}_p$, then also $(x - \alpha)^2 \in \mathbb{F}_p[x]$ and again by perfectness of $\mathbb{F}_p$, note that $\alpha \in \mathbb{F}_p$. So $\alpha, \beta \in \mathbb{F}_p$.

Now note that for $t \in \mathbb{F}_p$ have

$$\Big(t^2 + \beta,\ t(t^2 + \beta - \alpha)\Big) \in \tilde{E}$$

Hence, we find a function

$$\phi : \mathbb{F}_p \to \tilde{E}(\mathbb{F}_p) \setminus \{\mathcal{O}\}, \quad t \mapsto \Big(t^2 + \beta,\ t(t^2 + \beta - \alpha)\Big)$$

If there is $\gamma \in \mathbb{F}_p$ with $\gamma^2 = \alpha - \beta$, then

$$\phi|_{\mathbb{F}_p \setminus \{-\gamma\}} : \mathbb{F}_p \setminus \{-\gamma\} \to \tilde{E}(\mathbb{F}_p)$$

is injective, otherwise ϕ is injective. Hence, we see that $\#(\tilde{E}(\mathbb{F}_p) \setminus \{\mathcal{O}\}) \geq \#\mathbb{F}_p - 1 \geq 4$ and so $\#\tilde{E}(\mathbb{F}_p) \geq 5$. It follows that there is $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p)$ with $\tilde{y} \neq 0$. By a Hensel-lifting argument as in Proposition 1.4, we now see that there is $\gamma \in \mathbb{Z}_p$ with $(x, \gamma) \in E(\mathbb{Z}_p)$ and $|\gamma|_p = 1$. □

The above proposition shows that constructing Elliptic Curves $E : y^2 = x^3 + f_2x^2 + f_1x + f_0$ such that there is $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$ for all primes $p \neq 3, 5, 7$ is indeed quite simple, as almost all curves satisfy this. This only case that can fail is $p = 2$, but here, the condition is fulfilled quite often, so we can just try different choices.

Example 1.7. Let

$$E_1 : y^2 = x^3 + 2x$$
$$E_2 : y^2 = x^3 + 2x^2 + 6x + 5$$
$$E_3 : y^2 = x^3 + 6x + 1$$

Note that

$$1^2 \equiv 3^3 + 2 \cdot 3 = 33 \mod 8$$
$$1^2 \equiv 2^3 + 2 \cdot 2^2 + 6 \cdot 2 + 5 = 33 \mod 8$$
$$1^2 \equiv 4^3 + 6 \cdot 4 + 1 = 89 \mod 8$$

so Hensel's Lemma yields points $(x, y) \in E_i(\mathbb{Z}_2)$ with $|y|_2 = 1$ for $i \in \{1, 2, 3\}$. By Proposition 1.6, we have points $(x, y) \in E(\mathbb{Z}_p)$ with $|y|_p = 1$ for all $p \geq 11$.

Finally, note that trying all points shows

$$\tilde{E}_1(\mathbb{F}_3) = \{(0, 0), (1, 0), (2, 0), \mathcal{O}\}$$
$$\tilde{E}_1(\mathbb{F}_5) = \{(0, 0), \mathcal{O}\}$$
$$\tilde{E}_2(\mathbb{F}_7) = \{(1, 0), (5, 0), (6, 0), \mathcal{O}\}$$

so there is no point $(x, y) \in E_i(\mathbb{Z}_p)$ with $|y|_p = 1$ for $p \in \{3, 5, 7\}$ and a suitable i.

2 Question 2

Example 2.1 (2(i))**.** Consider the Elliptic Curve $E : y^2 = x(x + 1)(x + 4)$ defined over $\mathbb{Q}$. Have

$$x(x + 1)(x + 4) = x^3 + 5x^2 + 4x = \left(x + \frac{5}{3}\right)^3 - \frac{13}{3}\left(x + \frac{5}{3}\right) + \frac{70}{27}$$

So E is isomorphic to $E' : y^2 = x^3 - \frac{13}{3}x + \frac{70}{27}$ via

$$\psi : E \to E', \quad (x, y) \mapsto \left(x + \frac{5}{3}, y\right)$$

This isomorphism preserves the group structure[2], and so $E'_{\text{tors}} \cong E_{\text{tors}}$. Have

$$\Delta(E') = 4\left(-\frac{13}{3}\right)^3 + 27\left(\frac{70}{27}\right)^2 = -144 = \Delta(E)$$

Consider now any prime $p \neq 2, 3$. Then the isomorphism $\psi : E \to E'$ induces an isomorphism $\tilde{\psi} : \tilde{E} \to \tilde{E}'$ between the reductions modulo p. Note that $\tilde{E}, \tilde{E}'$ are still Elliptic Curves.

[2]It is a general result that all isogenies are group homomorphisms, but in this case, it is also directly obvious as the isomorphism is linear, hence maps lines to lines.

Hence, we can use results from the lecture on the reduction modulo $p \neq 2, 3$ for the curve E, even though it is not given by an equation of the form $y^2 = x^3 + Ax + B$, as all these statements are preserved under isomorphism. In particular, we see that the kernel of reduction $E_1(\mathbb{Q}_5)$ has no torsion and so there is an embedding

$$E_{\text{tors}}(\mathbb{Q}) \hookrightarrow \tilde{E}(\mathbb{F}_5)$$

Note that

$$\tilde{E}(\mathbb{F}_5) = \{(0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0), \mathcal{O}\}$$

has order 8. Clearly

$$(0,0), (-1,0), (-4,0), \mathcal{O} \in E_{\text{tors}}(\mathbb{Q})$$

So the only remaining question is whether this is all the torsion (i.e. $\#E_{\text{tors}}(\mathbb{Q}) = 4$) or there are more points (i.e. $\#E_{\text{tors}}(\mathbb{Q}) = 8$).

Consider now $P = (-2, 2) \in E$. The tangent at P is given by $y = -x$ and the third point of intersection with E is thus $(0, 0)$. Hence $P + P = (0, 0)$ and so $[4]P = \mathcal{O}$. It follows that $\#E_{\text{tors}}(\mathbb{Q}) = 8$ and furthermore that

$$E_{\text{tors}}(E) = \langle P, (-1, 0)\rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Example 2.2 (2(ii))**.** Consider the Elliptic Curve $E : y^2 = x(x + 1)(x - 8)$. Note that we have an isomorphism

$$\psi : E \to E', \quad (x, y) \mapsto \left(x - \frac{7}{3}, y\right)$$

to the Elliptic Curve $E' : y^2 = x^3 - \frac{73}{3}x - \frac{1190}{27}$ defined over $\mathbb{Q}$. Have that

$$\Delta(E) = -72^2 = -5184 = \Delta(E')$$

Note that this has only the prime factors 2 and 3. As before, this shows that all the results from the lecture on the reduction modulo $p \neq 2, 3$ are also valid for the curve E, even though it is not defined by an equation of the form $y^2 = x^3 + Ax + B$. We see that

$$\tilde{E}(\mathbb{F}_7) = \{(0,0), (1,0), (4,2), (4,5), (5,1), (5,6), (6,0), \mathcal{O}\}$$

and thus has order 8. As before, we this only leaves two possible cases, either the obvious 2-torsion points are all torsion points (i.e. $\#E_{\text{tors}}(\mathbb{Q}) = 4$) or each of the points $\tilde{E}(\mathbb{F}_5)$ lifts to a torsion point (i.e. $\#E_{\text{tors}}(\mathbb{Q}) = 8$).

Unlike the previous example however, this time the former is the case. To see this, we use the Nagell-Lutz theorem. Assume $(x, y) \in E_{\text{tors}}(\mathbb{Q})$ with $y \neq 0$. Then it yields that $y^2 \mid \Delta(E) = -72^2$ and so $y \mid 72$. So

$$y \in \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 3 \pm 6, \pm 12, \pm 24, \pm 9, \pm 18, \pm 36, \pm 72\}$$

Furthermore $y \not\equiv 0 \mod 7$ and since $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_7)$, it follows that

$$(\tilde{x}, \tilde{y}) \in \{(4, \pm 2), (5, \pm 1)\} \Rightarrow \tilde{y} \in \{\pm 1, \pm 2\}$$

Thus we only have the possibilities

$$y \in \{\pm 1, \pm 2, \pm 8, \pm 6, \pm 12, \pm 9, \pm 36, \pm 72\}$$

Furthermore, observe that

$$\tilde{E}(\mathbb{F}_{11}) = \{(0,0), (5,3), (5,8), (6,2), (6,9), (8,0), (10,0), \mathcal{O}\}$$

and so it follows by the same argument that

$$\tilde{y} \in \{\pm 2, \pm 3\}$$

This further restricts the possibilities to

$$y \in \{\pm 2, \pm 8, \pm 12, \pm 9\}$$

Finally, observe that none of the equations

$$\begin{aligned} 4 &= x^3 - 7x^2 - 8x \\ 64 &= x^3 - 7x^2 - 8x \\ 144 &= x^3 - 7x^2 - 8x \\ 81 &= x^3 - 7x^2 - 8x \end{aligned}$$

has a solution in $\mathbb{Q}$. To see this, use e.g. the rational root theorem and some computation:

The only factors of 4 are $\pm 1, \pm 2, \pm 4$ and none solves $4 = x^3 + 7x^2 - 8x$. The only factors of 64 are $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32, \pm 64$ and none solves $64 = x^3 - 7x^2 - 8x$. The only factors of 144 are $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 3, \pm 6, \pm 12, \pm 24, \pm 48, \pm 9, \pm 18, \pm 36, \pm 72, \pm 144$ and none solves $144 = x^3 - 7x^2 - 8x$. The only factors of 81 are $\pm 1, \pm 3, \pm 9, \pm 27, \pm 81$ and none solves $81 = x^3 - 7x^2 - 8x$.

Note that the usual approach to bound the size of $E_{\text{tors}}(\mathbb{Q})$ is use to the theorem that this embeds into $\tilde{E}(\mathbb{F}_p)$ whenever $\tilde{E}$ is an Elliptic Curve. However, for this example, this was not sufficient, as we could not find a prime such that the group $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ does not embed into $\tilde{E}(\mathbb{F}_p)$. In the next part, we want to study this phenomenon more carefully and indeed see that there is no such prime, i.e. it is impossible to show that $\#E_{\text{tors}}(\mathbb{Q}) \neq 8$ by just considering the reductions modulo p.

First, it is convenient to have a closed formula for the x-coordinate of $[2]P$ for a point P on an Elliptic Curve.

Proposition 2.3 (Duplication Formula)**.** Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an Elliptic Curve over a field k. For a point $P \in E$ with $P \neq \mathcal{O}$ denote by $x(P)$ its (affine) x-coordinate. Then have for all $P \in E$ with $P \neq -P$ that

$$x([2]P) = \frac{x(P)^4 - 2a_4x(P)^2 - 8a_6x(P) + a_4^2 - 4a_2a_6}{4(x(P)^3 + a_2x(P)^2 + a_4x(P) + a_6)}$$

Proposition 2.4. Let $E : y^2 = x(x+1)(x-8)$ be the Elliptic Curve from the previous example. The for each prime $p \geq 5$, have that $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is a subgroup of $\tilde{E}(\mathbb{F}_p)$.

Proof. First of all, note that the duplication formula from Proposition 2.3 has the form

$$x([2]P) = \frac{x(P)^4 + 16x(P) + 64}{4x(P)^3 - 28x(P)^2 - 32x(P)}$$

Consider any prime $p \geq 5$.

Case 1 If -1 is a quadratic residue modulo p, then there is $\beta \in \mathbb{F}_p$ with $\beta^2 = -36$. Have then that $(2, \beta) \in \tilde{E}(\mathbb{F}_p)$ and

$$x([2](2,\beta)) = \frac{2^4 + 16 \cdot 2^2 + 64}{4 \cdot 2^3 - 28 \cdot 2^2 - 32 \cdot 2} = \frac{144}{-144} = -1$$

and so $[2](2, \beta) = (-1, 0)$ is a 2-torsion point. Thus $(2, \beta)$ has order 4 and we see that

$$\langle (2,\beta), (0,0) \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Case 2 If -2 is a quadratic residue modulo p, then there is $\alpha \in \mathbb{F}_p$ with $\alpha^2 = -8$. Then

$$(\alpha - 8)^2 = (\alpha^2 + \alpha)(\alpha - 8) = \alpha(\alpha + 1)(\alpha - 8)$$

With $\beta := \alpha - 8$ we now find $(\alpha, \beta) \in \tilde{E}(\mathbb{F}_p)$ and

$$x([2](\alpha,\beta)) = \frac{\alpha^4 + 16\alpha^2 + 64}{4\alpha^3 - 28\alpha^2 - 32\alpha} = \frac{(\alpha^2 + 8)^2}{4\alpha^3 - 28\alpha^2 - 32\alpha} = 0$$

and so $[2](\alpha, \beta) = (0, 0)$ is a 2-torsion point. Hence, (α, β) has order 4 and thus

$$\langle (\alpha,\beta), (-1,0) \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Case 3 If 2 is a quadratic residue modulo p, then there is $\alpha' \in \mathbb{F}_p$ with $(\alpha')^2 = 72$ and so there is $\alpha = \alpha' + 8$ with $\alpha^2 - 16\alpha - 8 = 0$. Note that $\alpha^2 = 16\alpha + 8$ and thus

$$(9\alpha - 24)^2 = 81 \cdot 16\alpha + 81 \cdot 8 - 432\alpha + 576 = 1224 + 864\alpha = \alpha^3 - 7\alpha^2 - 8\alpha = \alpha(\alpha+1)(\alpha-8)$$

With $\beta := 9\alpha - 24$ we now find $(\alpha, \beta) \in \tilde{E}(\mathbb{F}_p)$ and

$$\begin{aligned} x([2](\alpha,\beta)) =& \frac{\alpha^4 + 16\alpha^2 + 64}{4\alpha^3 - 28\alpha^2 - 32\alpha} = \frac{(\alpha^2 + 8)^2}{4\alpha(\alpha+1)(\alpha-8)} \\ =& \frac{16^2(\alpha+1)^2}{4\alpha(\alpha+1)(\alpha-8)} = \frac{64(\alpha+1)}{(\alpha^2 - 8\alpha)} = \frac{64(\alpha+1)}{16\alpha + 8 - 8\alpha} = 8 \end{aligned}$$

and so $[2](\alpha, \beta) = (8, 0)$ is a 2-torsion point. Hence (α, β) has order 4 and thus

$$\langle (\alpha,\beta), (0,0) \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Since the Legendre symbol is multiplicative and $(-2)(-1) = 2$, these cases are exhaustive. □

To find more examples, it might be a good idea to use the structure from the previous theorem, but take another set of exhaustive cases. So consider an Elliptic Curve

$$E : y^2 = x(x-\alpha)(x-\beta) = x^3 - (\alpha+\beta)x^2 + \alpha\beta x$$

with 3 nontrivial torsion points $(\alpha, 0), (\beta, 0), (0, 0)$ over $\mathbb{Q}$. We study in which cases there is some $P \in \tilde{E}(\mathbb{F}_p)$ of order 4.

Lemma 2.5. Let $E : y^2 = x(x-\alpha)(x-\beta)$ be an Elliptic Curve over a field k of characteristic $\neq 2$. Then there exists $P \in E(k)$ of order 4 if and only if k has a root of the polynomial $F(T)$ given by

$$\left(T^4 + 2(\alpha+\beta)T^2 + (\alpha-\beta)^2\right)\left(T^4 + (2\beta-4\alpha)T^2 + \beta^2\right)\left(T^4 + (2\alpha-4\beta)T^2 + \alpha^2\right)$$

Proof. The duplication formula for E gives with $x = x(P)$ that

$$x([2]P) = d(x) := \frac{x^4 - 2\alpha\beta x^2 + \alpha^2\beta^2}{4x^3 - 4(\alpha+\beta)x^2 + 4\alpha\beta x}$$

Case 1 If there is $\mu \in \mathbb{F}_p$ with $\mu^4 + 2(\alpha+\beta)\mu^2 + (\alpha-\beta)^2 = 0$.
Then note that there is $\gamma := \frac{1}{2}(\mu^2 - \alpha - \beta)$ such that $\gamma^2 = \alpha\beta$. Thus

$$d(\gamma) = \frac{\gamma^4 - 2\alpha\beta\gamma^2 + \alpha^2\beta^2}{4\gamma^3 - 4(\alpha+\beta)\gamma^2 + 4\alpha\beta\gamma} = \frac{0}{4\gamma^3 - 4(\alpha+\beta)\gamma^2 + 4\alpha\beta\gamma} = 0$$

Note further that

$$\gamma^3 - (\alpha+\beta)\gamma^2 + \alpha\beta\gamma = 2\alpha\beta\gamma - \alpha\beta(\alpha+\beta) = \alpha\beta(2\gamma - \alpha - \beta) = \gamma^2\mu^2$$

since $\mu^2 = 2\gamma - \alpha - \beta$. So there is a point $(\gamma, \gamma\mu) \in E(k)$ with $[2](\gamma, \mu) = (0, 0)$.

Case 2 If there is $\mu \in k$ with $\mu^4 + (2\beta - 4\alpha)\mu^2 + \beta^2 = 0$.
Then note that there is $\gamma := \frac{1}{2}(\mu^2 + \beta)$ such that $\gamma^2 - 2\alpha\gamma + \alpha\beta = 0$. Thus

$$\begin{aligned}
&\gamma^4 - 2\alpha\beta\gamma^2 + \alpha^2\beta^2 = 4\alpha\gamma^3 - 4\alpha(\alpha+\beta)\gamma^2 + 4\alpha^2\beta\gamma \\
=&\gamma^4 - 4\alpha\gamma^3 + (4\alpha^2 + 4\alpha\beta - 2\alpha\beta)\gamma^2 - 4\alpha^2\beta\gamma + \alpha^2\beta^2 \\
=&\gamma^4 - 4\alpha\gamma^3 + 2\alpha(2\alpha+\beta)\gamma^2 - 4\alpha^2\beta\gamma + \alpha^2\beta^2 \\
=&(\gamma^2 - 2\alpha\gamma + \alpha\beta)^2 = 0^2 = 0
\end{aligned}$$

and so

$$\gamma^4 - 2\alpha\beta\gamma^2 + \alpha^2\beta^2 = \alpha(4\gamma^3 - 4(\alpha+\beta)\gamma^2 + 4\alpha\beta\gamma)$$

It follows that

$$d(\gamma) = \frac{\gamma^4 - 2\alpha\beta\gamma^2 + \alpha^2\beta^2}{4\gamma^3 - 4(\alpha+\beta)\gamma^2 + 4\alpha\beta\gamma} = \alpha$$

Furthermore note that

$$\begin{aligned}\gamma^3 - (\alpha+\beta)\gamma^2 + \alpha\beta\gamma =& \gamma(2\alpha\gamma - \alpha\beta) - (2\alpha\gamma - \alpha\beta)(\alpha+\beta) + \alpha\beta\gamma \\ =& 2\alpha(2\alpha\gamma - \alpha\beta) - 2\alpha^2\gamma - 2\alpha\beta\gamma + \alpha^2\beta + \alpha\beta^2 \\ =& \gamma(4\alpha^2 - 2\alpha^2 - 2\alpha\beta) + \alpha^2\beta + \alpha\beta^2 - 2\alpha^2\beta \\ =& 2\alpha\gamma(\alpha-\beta) + \alpha\beta(\beta-\alpha) \\ =& \alpha(\alpha-\beta)(2\gamma-\beta) \\ =& (\gamma-\alpha)^2\mu^2\end{aligned}$$

as $\mu^2 = 2\gamma - \beta$ and $(\gamma-\alpha)^2 = 2\alpha\gamma - \alpha\beta - 2\gamma\alpha + \alpha^2 = \alpha(\alpha-\beta)$. So there is a point $(\gamma, (\gamma-\alpha)\mu) \in E(k)$ with $[2](\gamma, (\gamma-\alpha)\mu) = (\alpha, 0)$.

Case 3 Similarly, if there is $\mu \in k$ with $\mu^4 + (2\alpha - 4\beta)\mu^2 + \alpha^2 = 0$, then there is a point $P \in E(k)$ with $[2]P = (\beta, 0)$ □

Hence, we just have to find $\alpha, \beta \in \mathbb{Q}$ such that the polynomial F has no root in $\mathbb{Q}$ and a root in every $\mathbb{F}_p$ (where p is a prime of good reduction). First, note that $F(T) = G(T^2)$ where

$$G(T) = \left(T^2 + 2(\alpha+\beta)T + (\alpha-\beta)^2\right)\left(T^2 + (2\beta-4\alpha)T + \beta^2\right)\left(T^2 + (2\alpha-\beta)T + \alpha^2\right)$$

Since the cases where this has a root in $\mathbb{Q}$ are clearly a Zariski-closed condition on (α, β), we see that "most" value of α, β will result in no root of $F(T)$. Hence, we focus on finding $\alpha, \beta \in \mathbb{Z}$ such that $F(T)$ has a root modulo any prime p (of good reduction). A necessary condition for that is that $G(T)$ has a root modulo any prime p, which in turn is equivalent that any of the discriminants (scaled by squares)

$$\alpha\beta,\ (\alpha-3\beta)(\alpha-\beta),\ (\beta-3\alpha)(\beta-\alpha)$$

is a quadratic residue modulo p, for any prime p.

3 Question 3

Lemma 3.1. Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an Elliptic Curve defined over k. Suppose that E has a nontrivial 5-torsion point $P = (\alpha_1, \beta_1) \in E(k)$. wlog $\alpha_1 = 0$. Let further $(\alpha_2, \beta_2) = [2](0, \beta)$. Then

$$\alpha_2^3 = -4\beta\beta_2$$

Proof. Consider the following SAGE script:

```
# (a, b, c) = (a_2, a_4, a_6),
# y = beta,
# (u, v) = (alpha_2, beta_2)
R.<a,b,c,y,u,v> = PolynomialRing(QQ, 6)
```

```
# slope of the tangent at (0,y)
l1_num = b
l1_den = 2 * y
# slope of the tangent at (u,v)
l2_num = 3 * u^2 + 2 * a * u + b
l2_den = 2 * v

I = ideal(
    y^2 - c, # (0,y) in E
    v^2 - u^3 - a * u^2 - b * u - c, # (u,v) in E

    u * l1_den^2 + a * l1_den^2 - l1_num^2,
    v * l1_den + y * l1_den + u * l1_num, # [2](0,y) = (u,v)

    2 * u * l2_den^2 + a * l2_den^2 - l2_num^2,
    -y * l2_den + v * l2_den - u * l2_num, # [2](u,v) = (0,-y)
)

# the next statement prints:
# Ideal (u^3 + 4*y*v) of Multivariate Polynomial Ring ...
print(I.elimination_ideal([a, b, c]))
```

The output shows that $\alpha_2^3 = -4\beta\beta_2$ already follows from the facts

$$(0, \beta) \in E,$$
$$(\alpha_2, \beta_2) \in E,$$
$$[2](0, \beta) = (\alpha_2, \beta_2),$$
$$[2](\alpha_2, \beta_2) = (0, -\beta)$$

which hold by assumption that $(0, \beta)$ has order 5. The claim follows. □

Lemma 3.2. Let

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and

$$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

be Elliptic Curves. If there are five distinct points $P_1, ..., P_5 \in E \cap E'$ in "sufficiently independent position", then $E = E'$ (meaning $a_i = a'_i$).

To be completely precise, there is a fixed 1-dimensional algebraic curve $C \subseteq \mathbb{A}^{10}$ (that does not depend on E, E' or $P_1, ..., P_5$) of degree 6 such that if there are five points $P_1 = (x_1, y_1), ..., P_5 = (x_5, y_5) \in E \cap E'$ with

$$(x_1, ..., x_5, y_1, ..., y_5) \notin C$$

then $E = E'$.

Proof. Consider the matrix $A = (a_{ij}) \in k[x_1, ..., x_5, y_1, ..., y_5]^{5\times 5}$ given by

$$a_{ij} = \begin{cases} x_i^{j-1} & \text{if } j \leq 3 \\ -x_i y_i & \text{if } j = 4 \\ -y_i & \text{if } j = 5 \end{cases}$$

Let $C = \mathbb{V}(\det(A))$ and assume there are five points $P_1 = (x_1, y_1), ..., P_5(x_5, y_5) \in E \cap E'$. Then the matrix $A_P := A(x_1, ..., x_5, y_1, ..., y_5) \in k^{5\times 5}$ is regular. Since $P_1, ..., P_5 \in E \cap E'$, see that

$$A_P(a_6 \;\; a_4 \;\; a_2 \;\; a_1 \;\; a_3)^T = (y_1^2 x_1^3 \;\; ... \;\; y_5^2 x_5^3)^T$$

and

$$A_P(a_6' \;\; a_4' \;\; a_2' \;\; a_1' \;\; a_3')^T = (y_1^2 x_1^3 \;\; ... \;\; y_5^2 x_5^3)^T$$

Thus by linear algebra, find that $E = E'$. □

Proposition 3.3. Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an Elliptic Curve defined over k. Suppose that E has a nontrivial 5-torsion point $P = (0, \beta) \in E(k)$. Let further $[2]P = (\alpha_2, \beta_2)$ and note that $0 \neq \alpha_2$. Then there exists a birational equivalence $E \to E'$ where $E' : y^2 + (1 + v)xy + vy = x^3 + vx^2$ given by

$$\psi : E \to E', \quad (x, y) \mapsto (u^2x, u^3y + u^2sx + t)$$

with

$$v = \frac{\beta_2}{\beta}, \quad t = -\frac{\beta_2}{2\beta}, \quad u = -\frac{\alpha_2}{2\beta}, \quad s = \frac{u}{\alpha_2}(\beta_2 + \beta)$$

Proof. Clearly ψ maps E to an Elliptic Curve E''. Note that by assumption, we have

$$[1](0, \beta) = (0, \beta), \quad [2](0, \beta) = (\alpha_2, \beta_2),$$
$$[3](0, \beta) = -[2](0, \beta) = (\alpha_2, -\beta_2), \quad [4](0, \beta) = -[1](0, \beta) = (0, -\beta)$$

By Lemma 3.1 we have that $\alpha_2^3 = -4\beta\beta_2$ and so

$$u^3 = \left(-\frac{\alpha_2}{2\beta}\right)^3 = -\frac{\alpha_2^3}{8\beta^3} = \frac{4\beta\beta_2}{8\beta^3} = \frac{\beta_2}{2\beta^2}$$

Under ψ, we now see that

$$(0,\ \beta) \mapsto (0, u^3\beta + t) = \left(0,\ \frac{\beta}{2\beta_2} - \frac{\beta}{2\beta_2}\right) = (0, 0) \in E'$$

and

$$\begin{aligned}(\alpha_2,\ \beta_2) \mapsto (u^2\alpha_2,\ u^3\beta_2 + u^2s\alpha_2 + t) &= \left(\frac{\alpha_2^3}{4\beta^2},\ \frac{\beta_2^2}{2\beta^2} + \frac{\beta_2}{2\beta}\left(\frac{\beta_2}{\beta} + 1\right) - \frac{\beta_2}{2\beta}\right) \\ &= \left(-\frac{\beta_2}{\beta},\ \frac{\beta_2^2}{\beta^2}\right) = (-v,\ v^2) \in E'\end{aligned}$$

and

$$(\alpha_2, \beta_2) \mapsto (u^2\alpha_2,\ -u^3\beta_2 + u^2 s\alpha_2 + t) = \left(\frac{\alpha_2^3}{4\beta^2},\ -\frac{\beta_2^2}{2\beta^2} + \frac{\beta_2}{2\beta}\left(\frac{\beta_2}{\beta} + 1\right) - \frac{\beta_2}{2\beta}\right)$$
$$= (-\frac{\beta_2}{\beta},\ 0) = (-v,\ 0) \in E'$$

and

$$(0,\ -\beta) \mapsto (0, -u^3\beta + t) = \left(0,\ -\frac{\beta_2}{2\beta} - \frac{\beta_2}{2\beta}\right) = (0,\ -v) \in E'$$

and of course $\mathcal{O} \mapsto \mathcal{O}$. Hence we have $\#(E' \cap E'') \geq 5$ and by the previous proposition we see that $E' = E''$. □

Corollary 3.4 (3(i))**.** Let E be an Elliptic Curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ has a nontrivial 5-torsion point if and only if E is isomorphic (over $\mathbb{Q}$) to an Elliptic Curve given by an equation of the form

$$y^2 + (v+1)xy + vy = x^3 + vx^2$$

Proof. Note that E is isomorphic (over $\mathbb{Q}$) to an Elliptic Curve defined by a Weierstraß equation, so assume wlog

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

Now let $P = (\alpha, \beta)$ be a nontrivial 5-torsion point. Then E is isomorphic via $(x, y) \mapsto (x - \alpha, \beta)$ to an Elliptic Curve

$$E' : y^2 = x^3 + a_2'x^2 + a_4'x$$

and $(0, \beta)$ is a nontrivial 5-torsion point of E'. The claim follows now by Proposition 3.3.

Conversely, assume that

$$E : y^2 + (v+1)xy + vy = x^3 + vx^2$$

For example by the duplication formula 2.3 find that

$$[2](0,0) = (-v, v^2), \quad [2](-v, v^2) = (0, -v)$$

and thus $[4](0,0) + (0,0) = \mathcal{O}$, hence $(0,0)$ has order 5. □

In the lecture, it was mentioned that a theorem of Mazur states that the torsion group of an Elliptic Curve E defined over $\mathbb{Q}$ has one of the following forms

- $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{1, ..., 10, 12\}$
- $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for $n \in \{2, 4, 6, 8\}$

Hence, we are quite limited for N a similar idea can work. First, note that the case $N = 2$ is easy.

Proposition 3.5 (3(ii))**.** Let E be an Elliptic Curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ has a nontrivial 2-torsion point if and only if E is isomorphic (over $\mathbb{Q}$) to an Elliptic Curve given by an equation of the form

$$y^2 = x^3 + a_2x^2 + a_4x$$

Proof. Assume $E : y^2 = x^3 + a_2x^2 + a_4x$ is an Elliptic Curve. Then clearly $(0, 0) \in E(\mathbb{Q})$ and $(0, 0) = -(0, 0)$, so $(0, 0)$ is nontrival 2-torsion point. Hence, there is a nontrivial 2-torsion point in $E'(\mathbb{Q})$ for all Elliptic Curves E' that are isomorphic (over $\mathbb{Q}$) to E.

Conversely, let E be an Elliptic Curve with a nontrivial 2-torsion point in $E(\mathbb{Q})$. Note that E is isomorphic to an Elliptic Curve

$$E' : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

as this holds for every Elliptic Curve. Now let $(\alpha, \beta) \in E'(\mathbb{Q})$ be a nontrival 2-torsion point. Thus $-(\alpha, \beta) = (\alpha, \beta)$, so $\beta = 0$ and $\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6 = 0$. Now consider the isomorphism

$$E' \to E'', \quad (x, y) \mapsto (x - \alpha, y)$$

where

$$E'' : y^2 = x^3 + (3\alpha + a_2)x^2 + (3\alpha^2 + 2\alpha a_2 + a_4)x + \underbrace{\alpha^3 + \alpha^2 a_2 + \alpha a_4 + a_6}_{=0}$$

Observe that E'' is of the described form, and the claim follows. □

The case $N = 3$ is slightly more interesting. For this, we first look at some basic transformations we can do to Weierstraß equations.

Proposition 3.6. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an Elliptic Curve defined over k. There are three nice types of transformations

Translation Let $P = (s, t) \in E(k)$ be a point. Then the isomorphism

$$E \to E', \quad (x, y) \mapsto (x - s, y - t)$$

maps P to $(0, 0)$ and the curve E to an Elliptic Curve

$$E' : y^2 + a_1xy + (a_3 + 2t + a_1s)y = x^3 + (a_2 + 3s)x^2 + (a_4 - 3s^2 + 2a_2s - a_1t)x$$

This is very useful to clear a_6 and continue working with the point $(0, 0)$.

Shearing Let $r \in k$. Then the isomorphism

$$E \to E', \quad (x, y) \mapsto (x, y - rx)$$

preserves $(0, 0)$ and maps E to an Elliptic Curve

$$E' : y^2 + (a_1 + 2r)xy + a_3y = x^3 + (a_2 + r^2 - a_1r)x^2 + (a_4 - ra_3)x + a_6$$

This is very useful, as it does not change a_3 and a_6.

Scaling Let $u \in k^*$. Then the isomorphism

$$E \to E', \quad (x, y) \mapsto (u^2 x, y^3 y)$$

preserves $(0, 0)$ and maps E to an Elliptic Curve

$$E' : y^2 + \frac{a_1}{u}xy + \frac{a_3}{u^3} = x^3 + \frac{a_2}{u^2}x^2 + \frac{a_4}{u^4}x + \frac{a_6}{u^6}$$

This is very useful, as it does not change which of the $a_1, ..., a_4, a_6$ are zero.

Now we can find a nice form for Elliptic Curves with a (nontrivial) 3-torsion point by the following step:

- Apply a translation to get an isomorphic curve whose (nontrivial) 3-torsion point is $(0, 0)$.
- Observe that $(0, 0)$ being a 3-torsion point is equivalent to the fact that the tangent at E through $(0, 0)$ meets E at $(0, 0)$ with multiplicity three.
- Apply clever shearing and scaling to get a nice form. Note that this does not destroy the fact $a_6 = 0$.

Now we get

Proposition 3.7. Let E be an Elliptic Curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ has a nontrivial 3-torsion point if and only if E is isomorphic (over $\mathbb{Q}$) to an Elliptic Curve given by an equation of the form

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

Proof. By Proposition 3.6 we can assume wlog that

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$

and $(0, 0) \in E(\mathbb{Q})$ is a nontrivial 3-torsion point. Now a shearing with $r = a_4/a_3$ transforms E into an Elliptic Curve

$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2$$

Observe that $(0, 0)$ is still a nontrivial 3-torsion point of $E'(\mathbb{Q})$.

Now note that the tangent at $(0, 0)$ has slope $m = a_4'/a_3' = 0$. Hence, since $-[2](0, 0) = (0, 0)$ is the third point of intersection of E' and the tangent, we see that the tangent meets E' at $(0, 0)$ with multiplicity three. Thus

$$x^3 + a_2'x^2$$

must already be x^3 and thus have $a_2' = 0$. Finally, apply a scaling with $u = a_1'$ (note that $a_1' \neq 0$, otherwise the curve would be singular) and find that E is isomorphic to the curve

$$E'' : y^2 + xy + vy = x^3$$

where $v = a_3'/(a_1')^3$.

Conversely, assume that E is isomorphic to an Elliptic Curve of the above form, so wlog

$$E : y^2 + xy + vy = x^3$$

We show that $(0,0) \in E(\mathbb{Q})$ has order 3. The tangent at $(0,0)$ has slope 0, so is given by the line $y = 0$. Plugging this in yields $x^3 = 0$, and so the third point of intersection with E is $(0,0)$.

Now consider the line through $\mathcal{O}$ and $(0,0)$, which is given by $x = 0$. Plugging this in yields $y^2 + vy = 0$ and so the third point of intersection is $(0, -v)$. Now note that $(0,0)$, $(0,-v)$ and $\mathcal{O}$ are colinear, so $(0,0) + (0,-v) + \mathcal{O} = \mathcal{O}$, hence $(0,0) = -[2](0,0)$ has order 3. □

4 Question 4

Let $S = \{x^2 \mid x \in \mathbb{Q}^2\}$.

Example 4.1 (4(i))**.** The Elliptic Curve $E : y^2 = x(x + 6 + 1)$ has rank 0.

Proof. As in the lecture, consider

$$\begin{aligned}
&E' : y^2 = x(x^2 - 12x + 32) \\
&\phi : E \to E', \quad (u,v) \mapsto \left(\frac{y^2}{x^2},\ y\frac{x^2-1}{x^2}\right) \\
&\hat{\phi} : E' \to E, \quad (u,v) \mapsto \left(\frac{y^2}{4x^2},\ y\frac{x^2-1}{8x^2}\right) \\
&q : E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathbb{Q}^*/S, \quad \overline{(u,v)} \mapsto \begin{cases} \overline{u} & \text{if } u \neq 0 \\ \overline{32} & \text{if } u = 0 \end{cases} \\
&\hat{q} : E(\mathbb{Q})/\phi(E'(\mathbb{Q})) \to \mathbb{Q}^*/S, \quad \overline{(u,v)} \mapsto \begin{cases} \overline{u} & \text{if } u \neq 0 \\ \overline{1} & \text{if } u = 0 \end{cases}
\end{aligned}$$

Find $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ As in the lecture, consider $r \mid 32$ square-free, i.e. $r \in \{\pm 1, \pm 2\}$.

For $r = 2$, have that $(l,m,n) = (2,1,0)$ solves

$$2l^4 - 12l^2m^2 + 16m^4 = n^2$$

and indeed we find $(8,0) \in E'(\mathbb{Q})$.

For $r = -1$, note that

$$-l^4 - 12l^2m^2 - 32m^4 = n^2$$

has no nontrivial solutions in $\mathbb{Q}$, as the left-hand side is always ≤ 0 and the right-hand side is ≥ 0.

Since $-2 = -1 \cdot 2$, we see that $\mathrm{im}(q) = \langle 2 \rangle$ and $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) = \langle (8,0) \rangle$.

Find $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ Consider $r \mid 1$, i.e. $r \in \{\pm 1\}$.
For $r = -1$, have that $(l, m, n) = (1, 1, 2)$ solves

$$-l^4 + 6l^2m^2 - m^2 = n^2$$

and indeed find $(-1, 2) \in E(\mathbb{Q})$.
Thus find $\mathrm{im}(\hat{q}) = \langle -1 \rangle$ and $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) = \langle (-1, 2) \rangle$.

Find the rank of E By the above two steps, we see that

$$E(\mathbb{Q})/[2]E(\mathbb{Q}) = \langle (-1, 2), \hat{\phi}((8, 0)) \rangle = \langle (-1, 2), (0, 0) \rangle$$

Now observe that $[2](-1, 2) = (0, 0)$ and $[2](0, 0) = \mathcal{O}$. Hence $E(\mathbb{Q}) = E_{\mathrm{tors}}(\mathbb{Q})$ and the rank is 0 as claimed. □

To find an example with rank two, it seems like a good way to take a curve with many rational points. Further requiring those points to be non-integral increases our chance, as that way, they cannot be torsion points.

For rank one, this is perfectly rigorous: If we find a curve with integral coefficients and at least one non-integral point, its rank must be ≥ 1. Such a curve is easy to find by guessing a point and using linear algebra. Furthermore, if we have two points P, Q with distinct x-coordinates ($\neq 1$), then we already see that $\overline{P} \neq \overline{Q} \in E(\mathbb{Q})/\hat{q}(E'(\mathbb{Q}))$ and since both are non-torsion (they have non-integral coordinates), it follows that the rank is at least 2.

Example 4.2. Guess the points

$$P_1 = \left(-1, \frac{1}{2}\right), \quad P_2 = \left(-2, \frac{1}{2}\right)$$

and consider an Elliptic Curve given by

$$y^2 = x^3 + a_2x^2 + a_4x$$

If $P_1, P_2, P_3 \in E$, we must have

$$\begin{aligned} -1 + a_2 - a_4 &= \frac{1}{4} \\ -8 + 4a_2 - 2a_4 &= \frac{1}{4} \end{aligned}$$

This has the solution $(a_2, a_4) = (23/8, 13/8)$. Hence, we consider the curve given by

$$y^2 = x^3 + \frac{23}{8}x^2 + \frac{13/8}{x}$$

Putting it into standard form yields

$$E : y^2 = x(x^2 + 46x + 104)$$

Now we would like to compute the rank of this curve, however the standard method fails here. The reason is that some of the equations, like

$$13l^4 + 65l^2m^2 + 8m^4 = n^2$$

(resulting from $r = 13 \mid 104$) seem to have no integer solutions, but seem have one modulo any prime.

Note however that we find

$$-l^4 + 46l^2m^2 - 104m^4 = n^2 \quad \text{has solution } (l, m, n) = (2, 1, 8)$$

and

$$104l^4 + 46l^2m^2 + 1m^4 = n^2 \quad \text{has solution } (l, m, n) = (0, 1, 1)$$

and

$$2l^4 + 46l^2m^2 + 52m^4 = n^2 \quad \text{has solution } (l, m, n) = (1, 1, 10)$$

corresponding to the points P_1, P_2 and $(0, 0)$.

So we find that $(\mathbb{Z}/2\mathbb{Z})^3 \hookrightarrow E(\mathbb{Q})/[2]E(\mathbb{Q})$ and since $x^2+46x+104$ has no rational roots (the discriminant 1700 is not a perfect square), observe that $E_{\text{tors}}(\mathbb{Q})/[2]E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Thus

$$(\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow E_{\text{torsion-free}}(\mathbb{Q})/[2]E(\mathbb{Q})$$

and E has rank at least 2.

A lot of trying around shows that most curves that are generated in a "clever" way to satisfy nice properties (like high rank, or only few square-free $r \mid b$ resp. $r \mid b_1$) cause problems when computing the rank, due to resulting in hard-to-solve equations as above. So it would be good to find a method that generates "nice" curves, i.e. curves where each of the equations

$$rl^4 + al^2m^2 + \frac{b}{r}m^4 = n^4 \quad \text{resp} \quad rl^4 + a_1l^2m^2 + \frac{b_1}{r}m^4 = n^4$$

obviously has or hasn't a nontrivial solution. At the moment, I fail to see any elegant method to generate "nice" curves with desired properties. So lets fall back to brute force, which works quite well here as this condition is very easy to test via a computer.

Example 4.3 (4(ii))**.** Consider the curve

$$E : y^2 = x(x^2 + 47x + 30)$$

Clearly $30 = 2 \cdot 3 \cdot 5$ has at least 3 different prime factors. We want to compute the rank of E. As always, have

$$E' : y^2 = x(x^2 - 92x + 2089)$$

Find $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ Have $b_1 = 2089$ is prime, so consider $r \in \{\pm 1, \pm 2098\}$. First note that for $r < 0$, the equation

$$rl^4 - 92l^2m^2 + \frac{2089}{r}m^4 = n^2$$

has no real nontrivial solutions, as the left-hand side is < 0 and the right-hand side is ≥ 0. Hence, it is left to consider $r = 1$ and $r = 2089$. Notice that the equations

$$l^4 - 92l^2m^2 + 2089m^4 = n^2 \quad \text{and} \quad 2089l^4 - 92l^2m^2 + 1m^4 = n^2$$

are symmetric w.r.t. swapping l, m.

Hence we only have the obvious solutions $(l, m, n) = (1, 0, 1)$ and $(l, m, n) = (0, 1, 1)$ that give the points $(0, 0)$ and $\mathcal{O}$. So $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) = \langle (0, 0) \rangle$.

Find $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ Have $b = 30 = 2 \cdot 3 \cdot 5$, so consider

$$r \in \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15\}$$

The equation

$$-l^4 + 47l^2m^2 - 30m^4 = n^2$$

has the solution $(l, m, n) = (1, 1, 4)$ which gives a point $(-1, 4) \in E(\mathbb{Q})$.

The equation

$$2l^4 + 47l^2m^2 + 15m^4 = n^2$$

has the solution $(l, m, n) = (1, 1, 8)$ which gives a point $(2, 8) \in E(\mathbb{Q})$.

The equation

$$3l^4 + 47l^2m^2 + 10m^4 = n^2$$

has the solution $(l, m, n) = (3, 1, 26)$ which gives a point $(27, 234) \in E(\mathbb{Q})$.

The equation

$$5l^4 + 47l^2m^2 + 6m^4 = n^2$$

has the solution $(l, m, n) = (1, 2, 17)$ which gives a point $(\frac{5}{4}, \frac{85}{8})$.

Since $\mathrm{im}(\hat{q})$ is a group and $-1, 2, 3, 5$ clearly generate

$$\{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15\} \subseteq \mathbb{Q}^*/S$$

we already see that $\mathrm{im}(\hat{q}) = \langle -1, 2, 3, 5 \rangle$.

Find the rank of E Combining the above, we see that

$$E(\mathbb{Q})/[2]E(\mathbb{Q}) = \langle (-1, 4), (2, 8), (27, 234), (\frac{5}{4}, \frac{85}{8}) \rangle$$

since $\hat{\phi}((0, 0)) = \mathcal{O}$. This further shows that $E(\mathbb{Q})/[2]E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$. Note that $x^2 + 47x + 30$ has no rational root, so $(0, 0)$ is the only nontrivial 2-torsion points and thus

$$E_{\mathrm{tors}}(\mathbb{Q})/[2]E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$$

Hence we see that the rank of E is $4 - 1 = 3 \geq 2$.

Note that the computer also found other, similarly special curves, given by equations[3]

$$E_1 : y^2 = x(x^2 + 59x^2 + 42)$$
$$E_2 : y^2 = x(x^2 + 83x^2 + 78)$$

[3] I should have guessed that there is a solution involving 42.