Miniproject - Elliptic Curves

Simon Pohmann

March 13, 2022

1 Question 1

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

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

Example 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 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*

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

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 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 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 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 4.

Proposition 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 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 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 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 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 8 (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 9 (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. just considering reduction modulo p is not sufficient to compute the torsion group of E.

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 10. *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 11. *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 10 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. □