Miniproject - Elliptic Curves

Simon Pohmann

March 12, 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

$$E(R) := \{(x, y) \in E \mid x, y \in R\}$$

for an Elliptic Curve E defined over k and any ring R contained in some extension field of k.

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. $\square$

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*

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

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

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

These cases have been excluded by assumption.

The other direction follows by reversing the above computation. The claim now follows from Proposition 4. $\square$

[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, it is easy to see that the linear equations

$$\forall n \in \mathbb{F}_7 : \ f_0 + f_1 n + f_2 n^2 + n^3 \equiv 3, 5, 6 \mod 7$$

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 Proposition 4 part four.

Proposition 6. *Let $p \geq 5$ 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. Using a computer, it is easy to check that the claim holds for $p = 5$ and $p = 7$ (there are only 5^5 resp. 7^7 different combinations of $f_0, f_1, f_2, x, y \in \mathbb{F}_5$ resp. $\mathbb{F}_7$).

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

$$x^3 + f_2x^2 + f_1x + f_0 \equiv (x - \alpha)^2(x - \beta) \mod p$$

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

$$\phi|_{\mathbb{F}_p \setminus \{-\gamma\}}$$

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 $|\gamma|_p = 1$. □