Elliptic Curves, n° 2

Lei Bichang

November 2, 2024

Exercise 1

(a) Let $\phi_{q,i}$ be the q^{th}-Frobenius on E_i, $i = 1, 2$. Then $\#E_i(\mathbb{F}_q) = \deg(1 - \phi_{q,i})$. Since ψ is an isogeny defined over $\mathbb{F}_q$, it is invariant under $\mathrm{Gal}(\bar{\mathbb{F}}_q|\mathbb{F}_q)$, so for every $P \in E_1$,

$$\psi(\phi_{q,1}(P)) = \psi(P^\sigma) = \psi^\sigma(P^\sigma) = \psi(P)^\sigma = \phi_{q,2}(\psi(P)),$$

where $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q|\mathbb{F}_q)$ denotes the q^{th}-Frobenius. Hence

$$\psi \circ (1 - \phi_{q,1}) = \psi - \psi \circ \phi_{q,1} = \psi - \phi_{q,2} \circ \psi = (1 - \phi_{q,2}) \circ \psi.$$

As ψ is nonzero, $\deg \psi \neq 0$. So taking degree on the above equation yields

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q).$$

(b) No. Let $q = 5$,

$$E_1 : y^2 = x^3 + x, \quad E_2 : y^2 = x^3 + 2x.$$

Then

$$(x, y) \mapsto (u^2 x, u^3 y), \quad u = \sqrt[4]{3}$$

is an isomorphism over $\bar{\mathbb{F}}_5$, but

$$\#E_1(\mathbb{F}_5) = 4, \ \#E_2(\mathbb{F}_5) = 2.$$

Exercise 2

(a) $E : y^2 = x^3 + 1$.

$\Delta = -16 \cdot 27 = -2^4 \cdot 3^3$, so the equation is minimal for every prime p, and the possible rational points (x, y) with finite order satisfy $x \in \mathbb{Z}$ and $y = 0, 1, 2, 3, 4, 6$. These points are

$$(-1, 0), \ (0, \pm 1), \ (2, \pm 3).$$

We compute the following points.

- $2 \cdot (0, \pm 1)$. Since $\lambda := \dfrac{3 \cdot 0^2}{2 \cdot \pm 1} = 0$, we have $x(2 \cdot (0, \pm 1)) = 0$, so $2 \cdot (0, \pm 1) = (0, \mp 1) = -(0, \pm 1)$. Therefore $(0, \pm 1)$ have order 3.
- $2 \cdot (2, 3)$. Since $\lambda := \dfrac{3 \cdot 2^2}{2 \cdot 3} = 2$, we have $x(2 \cdot (2, 3)) = \lambda^2 - 2 \cdot 2 = 0$, so $2 \cdot (2, 3) \in \{(0, \pm 1)\}$ have order 3, and thus $(2, 3)$ have order 3.

Hence all the five points are of fintie order, and $E(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/6\mathbb{Z}$.

(b) $E : y^2 = x(x - 1)(x + 2)$.

$\Delta = 16(0 - 1)^2(0 + 2)^2(1 + 2)^2 = 2^6 3^2$, so the equation is minimal for every prime.

- $E(\mathbb{Q})[2] = \{O, (0, 0), (1, 0), (-2, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- E has good reduction at 5, and

$$\tilde{E}(\mathbb{F}_5) = \{O, (0,0), (1,0), (-2,0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

If $5 \nmid m$, then $E(\mathbb{Q})[m] \hookrightarrow E(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So $\#E(\mathbb{Q})[m] \mid 4$. Hence $\#E(\mathbb{Q})[p^n] = 0$ for every prime $p \neq 2, 5$.

- E has good reduction at 7, and

$$\tilde{E}(\mathbb{F}_7) = \{O, (0,0), (1,0), (-1,\pm 3), (2,\pm 1), (-2,0), (3,\pm 3), (-3,\pm 3)\}.$$

This group has order 8 and four points of order 2, so $\tilde{E}(\mathbb{F}_7) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If $7 \nmid m$ and $E(\mathbb{Q})[m] \neq 0$, then $\#E(\mathbb{Q})[m] \mid 8$. Therefore $\#E(\mathbb{Q})[p^n] = 0$ for every prime $p \neq 2$

- Now suppose m is not a power of 2 and $P \in E[m]$. Then $\frac{m}{p^n} P \in E[p^n] = 0$ for every prime $p \neq 2$ and prime power $p^n \mid m$. Therefore $P \in E[2^n]$ for some $n \geq 0$, and $E(\mathbb{Q})_{\text{tor}} = E[2^\infty]$.
- Since $\#E(\mathbb{Q})[2] = \#\tilde{E}(\mathbb{F}_5)$ and $E(\mathbb{Q})[2] \subset E(\mathbb{Q})[2^n] \hookrightarrow \tilde{E}(\mathbb{F}_5)$ for all $n \geq 1$, we see that

$$E(\mathbb{Q})_{\text{tor}} = E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

1. $E : y^2 = x^3 - 43x + 166$.

$\Delta = -16(4 \cdot (-43)^3 + 27 \cdot 166^2) = -2^{19} \cdot 13$, so it is minimal for all primes $p \neq 2$.

- E has good reduction at 3 and 7, and

$$\tilde{E}(\mathbb{F}_3) = \{O, (0,\pm 1), (1,\pm 1), (-1,\pm 1)\} \simeq \mathbb{Z}/7\mathbb{Z},$$

$$\tilde{E}(\mathbb{F}_5) = \{O, (0,\pm 1), (1,\pm 2), (-2,\pm 2)\} \simeq \mathbb{Z}/7\mathbb{Z}.$$

So $E(\mathbb{Q})[p^n] = 0$ for all $p \neq 7$.

- Using a calculator, I found

$$(3,8) \in E(\mathbb{Q}).$$

Then using Sage, I found that the order of $(3,8)$ is 7. As $E(\mathbb{Q})[7] \hookrightarrow \tilde{E}(\mathbb{F}_3) \simeq \mathbb{Z}/7\mathbb{Z}$, we see that $E(\mathbb{Q})[7] \simeq \mathbb{Z}/7\mathbb{Z}$. By a similar argument as before,

$$E(\mathbb{Q})_{\text{tor}} = E(\mathbb{Q})[7] \simeq \mathbb{Z}/7\mathbb{Z}$$

and it is generated by $(3,8)$.