Elliptic Curves

Lei Bichang

November 22, 2024

Exercise 1

(a) For a finitely generated abelian group G, denote by $\operatorname{rank} G$ the rank of G.

Let $\phi : E_1 \to E_2$ be a non-constant isogeny over K. Then ϕ induces a map

$$\phi_K : E_1(K) \to E_2(K),$$

which is clearly a group homomorphism. This gives an injection

$$E_1(K)/\ker \phi_K \hookrightarrow E_2(K)$$

of abelian groups of finite type. So $\operatorname{rank}(E_1(K)/\ker \phi_K) \leq \operatorname{rank} E_2(K)$. Since $\ker \phi_K \subset \ker \phi$ is finite, we have

$$\operatorname{rank} E_1(K) = \operatorname{rank}(E_1(K)/\ker \phi_K).$$

Hence $\operatorname{rank} E_1(K) \leq \operatorname{rank} E_2(K)$. Doing the same thing to a non-constant isogeny $E_2 \to E_1$ over K, say $\hat{\phi}$[1], we get $\operatorname{rank} E_2(K) \leq \operatorname{rank} E_1(K)$. So the ranks of E_1 and E_2 are equal.

(b) No. I checked on LMFDB that $E_1 : y^2 = x^3 + x$ has rank 0, and $E_2 : y^2 = x^3 + 3x$ has rank 1. But E_1 and E_2 are isogenous via

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

over $\mathbb{Q}(u)$.

Exercise 2

(a) $E : y^2 = x(x^2 + 3x + 5)$.

$a = 3,\ b = 5,\ a_1 = -2a = -6,\ b_1 = a^2 - 4b = -11.$

- **Determine** $\psi(E'(\mathbb{Q})/\phi(E(\mathbb{Q})))$.

  The integers $r \mid b_1$ are

  $$r = \pm 1, \pm 11.$$

  Write

  $$\begin{cases} u = rt^2, \\ u^2 + a_1 u + b_1 = \dfrac{v^2}{u} = rs^2, \end{cases} \qquad t = \frac{l}{m},\ (l, m) = 1, \quad s = \frac{n}{m^2}.$$

[1] I don't recall if we have shown in class that: if ϕ is defined over K, then $\hat{\phi}$ is defined over K. This can be proved by checking directly that: all the three maps in

$$E_2 \to \operatorname{Div}_0(E_2) \xrightarrow{\phi^*} \operatorname{Div}_0(E_1) \to E_1$$

are G_K-invariant.

which gives the equation

$$r^2l^4 + a_1rl^2m^2 + b_1m^4 = rn^2, \tag{1}$$

i.e, $r^2l^4 - 6rl^2m^2 - 11m^4 = rn^2$. The value $r = -11 = b_1 = a^2 - 4b$ corresponds to $(0, 0)$. Since $\operatorname{im} q$ is a group, it must be $\{[1], [-11]\}$ or $\{[1], [-11], [-1], [11]\}$.
Substitute $r = -1$ in Eq. (1) gives

$$l^4 + 6l^2m^2 - 11m^4 = -n^2, \tag{2}$$

which has a solution $(l, m, n) = (1, 1, 2)$, corresponding to

$$(u, v) = \left(\frac{rl^2}{m^2}, \frac{rnl}{m^3}\right) = (-1, -2) \in E'(\mathbb{Q}).$$

The image of $(-1, -2)$ in $E''(\mathbb{Q})$ is

$$\psi(u, v) = \left(u + a_1 + \frac{b_1}{u}, v - \frac{b_1v}{u^2}\right) = (4, -24).$$

The isomorphism $E'' \to E$ is

$$x = x''/4, \quad y = y''/8,$$

so the corresponding point in $E(\mathbb{Q})$ is $(1, -3)$.

- **Determine** $E(\mathbb{Q})/\psi(E'(\mathbb{Q}))$.
  Next, solve

$$r^2l^4 + 3rl^2m^2 + 5m^4 = rn^2 \tag{3}$$

  for $r \mid 5$. The value $r = b = 5$ corresponds to $(0, 0)$. Because $a^2 - 4b < 0$, we have $rs^2 = u^2 + au + b > 0$, so $r > 0$. Hence $[-1], [-5] \notin \operatorname{im} q'$, and thus $(0, 0)$ generates $E(\mathbb{Q})/\psi(E'(\mathbb{Q}))$.

Finally, $E(\mathbb{Q})/2E(\mathbb{Q}) = \langle(0, 0), (1, -3)\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Rank. The rank of E is 1. Since $(0, 0)$ has order 2, the rank of E is 0 or 1, depending on whether $(1, -3)$ has finite order or not. I don't know how to do this by hand without spending too much time and ink, but using Sage I can tell that $(1, -3)$ has infinite order by computing iP for $2 \le i \le 12$ or by letting the program tell me its order directly.

(b) $E : y^2 = x(x^2 - 2x + 9)$.

$a = -2,\ b = 9,\ a_1 = -2a = 4,\ b_1 = a^2 - 4b = -32.$

- Solve

$$rl^4 + 4l^2m^2 - \frac{32}{r}m^4 = n^2 \tag{4}$$

  for $r \mid 32$ square-free, that is $r = \pm1, \pm2$. $[r] = [-2] = [-32]$ corresponds to $(0, 0)$, so $\operatorname{im} q = \{[1], [-2]\}$ or $\{[1], [-2], [-1], [2]\}$. Let $r = 2$, so that

$$2l^4 + 4l^2m^2 - 16m^4 = n^2. \tag{5}$$

  Completing the square then modulo 3

$$\implies \{0, 2\} \ni 2(l^2 + m^2)^2 = n^2 \in \{0, 1\} \bmod 3,$$

$$\implies l^2 \equiv m^2 \equiv n^2 \equiv 0 \bmod 3,$$

$\implies 3 \mid l$ and $3 \mid m$, contradicting $(l, m) = 1$. Hence Eq. (5) has no nontrivial solution in $\mathbb{Z}^3$.

- Solve
$$rl^4 - 2l^2m^2 + \frac{9}{r}m^4 = n^2 \tag{6}$$
for $r \mid 9$ square free, i.e., $r = \pm1, \pm3$. $[r] = [1] = [9]$ corresponds to $(0,0)$. $b_1 = a^2 - 4b < 0$, so $rs^2 = u^2 + au + b > 0$. Thus it remains to check $r = 3$:
$$3l^4 - 2l^2m^2 + 3m^4 = n^2. \tag{7}$$
This equation has solution $(l, m, n) = (1, 1, 2)$, corresponding to
$$(u, v) = \left(\frac{rl^2}{m^2}, \frac{rln}{m^3}\right) = (3, 6) \in E(\mathbb{Q}).$$
Since $(0,0)$ corresponds to the identity $[1]$, we have $E(\mathbb{Q})/\psi(E'(\mathbb{Q})) = \langle(3,6)\rangle$.

So $E(\mathbb{Q})/2E(\mathbb{Q}) = \langle(3,6)\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Rank. The rank of E is 0, because $(0,0)$ has order 2.

(c) $E : y^2 = x(x^2 + 2x + 9)$.

$a = 2,\ b = 9,\ a_1 = -2a = -4,\ b_1 = a^2 - 4b = -32.$

- Solve
$$rl^4 - 4l^2m^2 - \frac{32}{r}m^4 = n^2 \tag{8}$$
for $r = \pm1, \pm2$. $[r] = [-1] = [-32]$ corresponds to $(0,0)$. Let $r = 2$, then
$$2l^4 - 4l^2m^2 - 16m^4 = n^2. \tag{9}$$
has a solution $(2, 1, 0)$, corresponding to
$$(u, v) = (8, 0) \in \psi^{-1}((0,0)) \subset E'(\mathbb{Q}).$$

- Solve
$$rl^4 + 2l^2m^2 + \frac{9}{r}m^4 = n^2 \tag{10}$$
for $r = \pm1, \pm3$. Since $b_1 < 0$, we have $r = 1, 3$. Let $r = 3$:
$$3l^4 + 2l^2m^2 + 3m^4 = n^2. \tag{11}$$
Modulo 3, we get
$$\{0, 2\} \ni 2(lm)^2 = n^2 \in \{0, 1\},$$
$$\implies (lm)^2 = n^2 = 0 \mod 3,$$
$\implies 3 \mid lm$ and $3 \mid n$. If $3 \mid l$, then Eq. (11) shows that $3^2 \mid 3m^4$, so $3 \mid m$, which is a contradiction. Similarly, $3 \mid m \implies 3 \mid l$ and leads to contradiction. Therefore, Eq. (11) has no nontrivial integer solution.

So $E(\mathbb{Q})/2E(\mathbb{Q}) = \langle(0,0)\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Rank. The rank of E is 0, because $(0,0)$ is a point of order 2.

Exercise 3

(a) A finitely generated abelian group has finitely many torsion elements. If K is algebraically closed, then $E(K)[n] = E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for all integers n that are not divided by $\operatorname{char} K$. Therefore $E(K)_{\text{tor}} = \bigcup_{n\geq 1} E(K)[n]$ cannot be finite, thus $E(K)$ is not of finite type.

(b) For a set S, denote by $|S|$ the cardinality of a set S.

A finitely generated abelian group is finite or countable. So to prove that $E(\mathbb{R})$ is not of finite type, it suffices to show that $E(\mathbb{R})$ is uncountable.

As $\operatorname{char} \mathbb{R} = 0$, we may assume that E is defined by $y^2 = f(x)$, where $f(X) = X^3 + aX + b \in \mathbb{R}[X]$. Then $f(\mathbb{R}) = \mathbb{R}$. So for every $y \in \mathbb{R}$, there exists $x \in \mathbb{R}$ s.t. $(x, y) \in E$. This means that the map

$$E(\mathbb{R}) \setminus \{O\} \to \mathbb{R},\ (x, y) \mapsto y$$

is surjective, and thus $|E(\mathbb{R})| \geq |\mathbb{R}| > \aleph_0$.

(c) Similar to (b), we show that $E(\mathbb{Q}_p)$ is uncountable using Hensel's lemma.

Assume that E is given by a minimal Weierstrass equation $F(x, y) = 0$, where $F(X, Y) \in \mathbb{Z}_p[X, Y]$, so that the curve $\tilde{E}$ is given by $\tilde{F}(x, y) = 0$. Let $\pi : E_0(\mathbb{Q}_p) \to \tilde{E}_{\text{ns}}(\mathbb{F}_p)$ be the reduction map. Take $P_0 = (x_0, y_0) \in \tilde{E}_{\text{ns}}(\mathbb{F}_p) \setminus \{O\} \neq \varnothing$. By the definition of singularity,

$$\frac{\partial \tilde{F}}{\partial X}(x_0, y_0) \neq 0 \quad \text{or} \quad \frac{\partial \tilde{F}}{\partial Y}(x_0, y_0) \neq 0.$$

- Assume first that $\frac{\partial \tilde{F}}{\partial X}(x_0, y_0) \neq 0$. Denote by $a \mapsto \bar{a}$ the quotient map $\mathbb{Z}_p \to \mathbb{F}_p$.
  Let $y \in \mathbb{Z}_p$ be any lift of $y_0 \in \mathbb{F}_p$, and let

  $$f_y(X) := F(X, y) \in \mathbb{Z}_p[X].$$

  Then modulo p, we have $\overline{f_y(x_0)} = 0$ in $\mathbb{F}_p$, and

  $$\overline{f_y'(x_0)} = \frac{\overline{\partial F(X,Y)}}{\partial X}(x_0, y_0) = \frac{\partial \tilde{F}}{\partial X}(x_0, y_0) \neq 0.$$

  So by Hensel's lemma, there is a unique $x \in \mathbb{Z}_p$ s.t. $F(x, y) = f_y(x) = 0$.
  The set

  $$y + p\mathbb{Z}_p = \{z \in \mathbb{Z}_p \mid \bar{z} = y_0\}$$

  has cardinality equal to $\mathbb{Z}_p$, which is an uncountable set. The above construction gives an injection $y + p\mathbb{Z}_p \hookrightarrow E_0(\mathbb{Q}_p)$. Therefore, there are uncountably many points in $E_0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$.

- If $\frac{\partial \tilde{F}}{\partial Y}(x_0, y_0) \neq 0$, we can argue in a much similar way that $E(\mathbb{Q}_p)$ is uncountable.