Elliptic Curves

Lei Bichang

November 20, 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 (how??), 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) $E : y^2 = x(x^2 + 3x + 5)$.

$a = 3,\ b = 5,\ a_1 = -2a = -6,\ b_1 = a^2 - 4b = -11$. So the integers $r \mid b_1$ are

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

Write

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

which give the equation

$$r^2 l^4 + a_1 r l^2 m^2 + b_1 m^4 = rn^2. \tag{1}$$

The value $r = -11 = b_1 = a^2 - 4b$ corresponds to $(0, 0)$.

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 integer n that is not divided by $\operatorname{char} K$. Therefore $E(K)_{\text{tor}} \supset \bigcup_{n\geq 1} E(K)[n]$ 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 $\dfrac{\partial \tilde{F}}{\partial X}(x_0, y_0) \neq 0$. 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

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

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