Mordell-Weil Theorem using Galois Cohomology

Mehedi Hasan Nowshad

Department of Mathematics,
University of Dhaka.

Prerequisites

- Field extension and its degree, splitting field
- Topological group
- modules, exact sequences
- Variety (affine/algebraic/projective), its dimension
- Morphism of algebraic varieties, product variety
- Group operation on elliptic curve using chord/tangent.

At least knowing their definitions and some very basic results regarding them is needed.

Introduction

- A curve is a Projective variety of dimension 1.
- An elliptic curve $E(K)$ over a field K is a smooth genus 1 curve with a specified base point.
  - Roughly speaking, **genus** $g = \frac{(d-1)(d-2)}{2}$, where d is the degree of the curve
  - **Smooth** curve means the Jacobian formed by the derivatives of the defining equations of the curve at every point has rank 1.
- If $char(K) \neq 2, 3$, a consequence of Riemann-Roch theorem says that every elliptic curve is isomorphic to this form: (See [Sil09], Ch. 3 or [Mil06], Ch 2)

$$y^2z = x^3 + axz^2 + bz^3$$

This is non-singular if $\Delta = -(4a^3 + 27b^2)$ is non-zero.

Contents

1. Galois Theory
2. Group (Galois) Cohomology
3. Algebraic Geometry
4. Selmer and Sha
5. Algebraic Number Theory
6. Some results in elliptic curves
7. Weak Mordell-Weil Theorem
8. Mordell-Weil Theorem

Galois Theory

Field Extension

- A **number field** is a finite field extension of $\mathbb{Q}$.
- A field extension E/K is a **separable field extension** if minimal polynomial of every element in E is separable.
  - Every number field is separable over $\mathbb{Q}$.
- A field extension E/K is a **normal field extension** if minimal polynomial of every element in E splits in $E[x]$.

Example

The equation $x^3 = 2$ has roots $\sqrt[3]{2}, \omega\sqrt[3]{2},$ and $\omega^2\sqrt[3]{2}$.
It can be easily seen that $\mathbb{Q}(\sqrt[3]{2})$ is not normal, while the splitting field of $x^3 - 2$ (which is just $\mathbb{Q}(\sqrt[3]{2}, \omega)$) is a normal extension of $\mathbb{Q}$.

- A **Galois extension** is an algebraic field extension E/F that is normal and separable

Field automorphism

- An automorphism of E/F is a field automorphism of E which fixes F.
- Any automorphism just shuffles the roots of any polynomial in $F[x]$.

Example

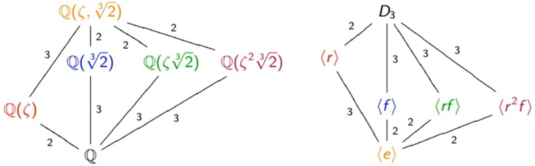
An automorphism σ of $\mathbb{Q}(\sqrt[3]{2})$ is completely determined by $\sigma(\sqrt[3]{2})$, which is again a root of $x^3 - 2$. However, $\sqrt[3]{2}$ is the only root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$. Thus,

$$Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$$

Subfield Lattice vs Subgroup Lattice

Example

$Aut(\mathbb{Q}(\sqrt[3]{2}, \omega)) = S_3$ (or D_3) where an automorphism is determined by how roots of $x^3 - 2$ is shuffled.



Subfield lattice of $\mathbb{Q}(\zeta, \sqrt[3]{2})$

Subgroup lattice of $\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})) \cong D_3$.

Image source: Visual Group Theory (Professor Macauley)

Fundamental theorem of Galois Theory

Theorem

Let E/F be a finite Galois extension with Galois group $G = Gal(E/F) = Aut(E/F)$. Then there is a order reversing correspondence between the subgroups of G and field extensions of F contained in E. ([Mil21], Chapter 3)

- *The correspondence is given by $G \supseteq H \to E^H \subseteq E$ with the inverse being $E \supseteq K \to Gal(E/K) \subseteq G$.*
- *So we have, $Gal(E/E^H) = H$.*
- *$H \trianglelefteq G \iff E^H/F$ is normal.*
  Then $Gal(E^H/F) = G/H$

Infinite Galois Theory

Definition (Krull topology)

Let E/F be a Galois extension (possibly infinite). Then $Gal(E/F)$ can be made into a topological group with its neighbourhood basis of the identity being the subgroups $Gal(E/K)$ where K/F is a finite galois extension.

Fundamental Theorem of Galois theory also holds in case of infinite Galois extension if we replace “subgroups" by “closed subgroups". ([Mil21], Ch. 7)

Definition

- *A field F is* ***perfect*** *if every finite extension of F is separable. (ex: Number fields)*
- *Absolute Galois group of $F = G_F = Gal(F^{sep}/F)$*
- *If K is Perfect, $K^{sep} = \overline{K}$ and $G_K = Gal(\overline{K}/K)$*

Group (Galois) Cohomology

Group Cohomology

- Let M be a $G-$module
- Crossed homomorphism is a map $f : G \to M$ such that $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$
- f is a principal crossed homomorphism if $f(\sigma) = \sigma m - m$ for some $m \in M$
- Note that, principal crossed homos $\trianglelefteq$ crossed homos.

Definition ($0-th$ and $1st$ cohomology groups)

- $H^0(G, M) = M^G = \{m \in M \mid m^\sigma = m \ \ \forall \sigma \in G\}$
- $H^1(G, M) = \frac{crossed\ homomorphisms}{principal\ crossed\ homomorphisms}$

Example

$$H^0(G_\mathbb{Q}, E(\overline{\mathbb{Q}})) = E(\overline{\mathbb{Q}})^{G_\mathbb{Q}} = E(\overline{\mathbb{Q}})^{Gal(\overline{\mathbb{Q}}/\mathbb{Q})} = E(\mathbb{Q})$$

Group Cohomology

- For an infinite Galois group, crossed homos are replaced by continuous crossed homos (with G having Krull topology and M having discrete topology) and $G \times M \to M$ needs to be continuous.
- Note that principal crossed homos are always continuous.

Example

If the action of G on M is trivial, then

$$H^0(G, M) = M \quad , \quad H^1(G, M) = Hom(G, M)$$

Example of Galois Cohomology

Let L/K be a finite Galois extension with $Gal(L/K) = G$. Then $H^1(G, L^\times) = 0$

Proof.

In multiplication notation, crossed homo becomes:

$$f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau)), \qquad \sigma, \tau \in G$$

We want $y \in L^\times$ such that $f(\sigma) = \sigma(y)/y$ for all $\sigma \in G$.
As $f(\tau)$ are nonzero, Dedekind's theorem on the independence of characters implies

$$\sum_{\tau \in G} f(\tau)\tau : \ L \to L$$

is not the zero map.

Example of Galois Cohomology

Proof.

So there exists $\beta \in L$ has

$$\beta^* = \sum_{\tau \in G} f(\tau)\tau\beta \neq 0.$$

Then for $\sigma \in G$,

$$\begin{aligned} \sigma\beta^* = \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau\beta &= \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau\beta \\ &= f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau\beta = f(\sigma)^{-1}\beta^*, \end{aligned}$$

so $f(\sigma) = \beta^*/\sigma\beta^* = \sigma(y)/y$ with $y = (\beta^*)^{-1}$. ■

Exact sequence of Cohomology groups

Theorem

Let $0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$ be a short exact sequence of G-modules. Then there is a natural long exact sequence of cohomology groups

$$0 \longrightarrow H^0(G,A) \xrightarrow{\iota_0} H^0(G,B) \xrightarrow{\pi_0} H^0(G,C) \xrightarrow{\delta}$$

$$H^1(G,A) \xrightarrow{\iota_1} H^1(G,B) \xrightarrow{\pi_1} H^1(G,C) \longrightarrow \cdots .$$

The maps are defined by

- $\iota_0 = i|_{A^G}$
- $\pi_0 = \pi|_{B^G}$
- $\iota_1(f) = i \circ f$
- $\pi_1(g) = \pi \circ g$.

Exact sequence of Cohomology groups

- Let $c \in H^0(G, C) = C^G$
  So $\sigma c = c$, $\forall \sigma \in G$.
  As π is surjective, we have,

  $$\exists b \in B \mid \pi(b) = c$$

  Let $a' = \sigma b - b$. Then,

  $$\pi(a') = \sigma\pi(b) - \pi(b) = \sigma c - c = 0$$

  So, $a' \in \ker(\pi) = im(\iota)$
  We define, $\delta(\mathbf{c})(\sigma) := \mathbf{a}$ with $\iota(a) = a'$.

Example of Galois Cohomology exact sequence

- $\mu_n(L) = \{\zeta \in L^\times \mid \zeta^n = 1\}$
- Exact sequence $1 \to \mu_n(\overline{k}) \to \overline{k}^\times \xrightarrow{(\ )^n} \overline{k}^\times \to 1$ implies the following sequence of cohomology groups:

$$1 \to \mu_n(k) \to k^\times \xrightarrow{(\ )^n} k^\times \to H^1(G_k, \mu_n(\overline{k})) \to H^1(G_k, k^\times) = 1$$

- $H^1(G, \mu_n(\overline{k})) \cong k^\times / k^{\times n}$
- When k is a number field and $n > 1$, this group is infinite.
- For example, the numbers

$$(-1)^{\varepsilon(\infty)} \prod_{p \text{ prime}} p^{\varepsilon(p)},$$

with each exponent 0 or 1 and only finitely many nonzero, form a set of representatives for the elements of $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$.

Restriction-Inflation exact sequence

- Let M be a G-module with $H \trianglelefteq G$.
- $f \to f|_H$ defines the restriction morphism:

$$res : \ H^1(G, M) \to H^1(H, M)$$

- M^H is naturally a G/H-module.
- $G \to G/H \to M^H \to M$ defines the inflation morphism:

$$inf : \ H^1(G/H, M^H) \to H^1(G, M)$$

- Together we get the exact sequence:

$$0 \to H^1(G/H, M^H) \xrightarrow{inf} H^1(G, M) \xrightarrow{res} H^1(H, M)$$

Algebraic Geometry

Separated variety (analogue of Hausdorffness)

Definition

A variety X is separated if its diagonal Δ_X is closed.

Example

A line with a double origin is not separated.

$$\mathbb{A}^1 \times \{0,1\}/\sim \ \text{, where } (x,0) \sim (x,1) \ \text{ if } \ x \neq 0$$

Example

$\mathbb{A}^n$ is separated as the diagonal is the zero set of the polynomials $x_i - y_i$.

Example

$\mathbb{P}^n$ is separated as the diagonal is the zero set of the homogeneous polynomials $x_i y_j - x_j y_i$.

Complete Variety (analogue of compactness)

Definition

An algebraic variety V is said to be complete if for all algebraic varieties W, the projection

$$q : V \times W \to W$$

is closed.

Example

$\mathbb{A}^1$ *is not complete as under the projection* $(x, y) \mapsto y : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$*, the image of* $V(xy - 1)$ *is not closed in* $\mathbb{A}^1$*.*

Properties of Complete Variety

Theorem

Let V be a complete variety.

(a) *A closed subvariety of V is complete.*

(b) *If V' is complete, so is $V \times V'$.*

(c) *For any morphism $\varphi : V \to W$ (W is separated), $\varphi(V)$ is closed and complete; in particular, if V is a subvariety of W, then it is closed in W.*

(d) *If V is connected and C is a curve, then any regular map $\varphi : V \to C$ is either constant or onto.*

(e) *If V is connected, then any regular function on V is constant.*

Proof.

Straightforward definition chasing. ■

Isogeny

Theorem

Projective space $\mathbb{P}^n$ is complete (so is any projective variety).

- Non-constant morphism between a projective variety and a curve is surjective (so is between two curves)

Definition

An isogeny between E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$. (E_is are elliptic curves over $\overline{k}$)

Theorem

Isogeny defined by multiplication by m is non-constant, hence surjective.

Selmer and Sha

Elliptic Curve exact sequences

- We have the following exact sequence:

$$0 \longrightarrow E(\overline{k})[n] \longrightarrow E(\overline{k}) \xrightarrow{n} E(\overline{k}) \longrightarrow 0$$

- Applying Galois cohomology, we have:

$$0 \longrightarrow E(k)[n] \longrightarrow E(k) \xrightarrow{n} E(k) \longrightarrow H^1(k, E[n])$$

$$\longrightarrow H^1(k, E) \longrightarrow H^1(k, E)$$

- Then we can extract another exact sequence:

$$0 \longrightarrow E(k)/nE(k) \longrightarrow H^1(k, E[n]) \longrightarrow H^1(k, E)[n] \longrightarrow 0.$$

- We are interested in $k = \mathbb{Q}$ and $\mathbb{Q}_p$ (p prime), but before that, let's see what $\mathbb{Q}_p$ is.

p-adic Numbers, $\mathbb{Q}_p$

For $s = p^n t \in \mathbb{Z}$ *with* $p \nmid t$, define $v_p(s) = n$. For $q = \frac{a}{b} \in \mathbb{Q}$, define $v_p(q) = v_p(a) - v_p(b)$.

Definition

$|\cdot|_p = p^{-v_p(\cdot)}$ *defines a p-adic norm on* $\mathbb{Q}$.
The completion of $\mathbb{Q}$ *with respect to this norm is the set of p-adic numbers* $\mathbb{Q}_p$.

- $a \in \mathbb{Q}_p$ takes the form $a = \sum_{k=n}^{\infty} p^k a_k$, where $k \in \mathbb{Z}$ and $a_k \in \{0, 1, \cdots, p-1\}$.
- Note that such an expression indeed converges in the p-adic metric.
- Also notice the similarity with the base $p-$expansion of a number. In fact, it is indeed so, when $a \in \mathbb{N} \subset \mathbb{Q} \subset \mathbb{Q}_p$.
- We will see more on this field later in the algebraic number theory section.

Some embeddings/mappings

- We have the following embedding:

$$\begin{tikzcd}
\overline{\mathbb{Q}} \arrow[r, hook] \arrow[d, phantom, "\cup"] & \overline{\mathbb{Q}_p} \arrow[d, phantom, "\cup"] \\
\mathbb{Q} \arrow[r, hook] & \mathbb{Q}_p
\end{tikzcd}$$

  Restricting the Galois action on $\overline{Q} \subset \overline{Q_p}$, we have the following embedding:

$$G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$$

- Hence, any crossed homo $G_{\mathbb{Q}} \to E(\overline{Q})$ defines a crossed homo $G_{\overline{\mathbb{Q}_p}} \to E(\overline{\mathbb{Q}_p})$
- Thus, we get a homomorphism: $H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_p, E)$

Elliptic Curve exact sequences

- Taking $k = \mathbb{Q}$ and $\mathbb{Q}_p$, and using $\mathbb{Q} \subset \mathbb{Q}_p$, we get the following exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbb{Q})/nE(\mathbb{Q}) \arrow[r] \arrow[d] & H^1(\mathbb{Q}, E[n]) \arrow[r] \arrow[d] & H^1(\mathbb{Q}, E)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) \arrow[r] & H^1(\mathbb{Q}_p, E[n]) \arrow[r] & H^1(\mathbb{Q}_p, E)[n] \arrow[r] & 0
\end{tikzcd}$$

- We want to replace $H^1(\mathbb{Q}, E[n])$ with a subset containing the image of $E(\mathbb{Q})/nE(\mathbb{Q})$, but which we shall be able to prove is finite.
- We do this as: if $\gamma \in H^1(\mathbb{Q}, E[n])$ comes from $E(\mathbb{Q})$, then certainly its image $\gamma_p \in H^1(\mathbb{Q}_p, E[n])$ comes from $E(\mathbb{Q}_p)$. So the following subset is a good candidate.

$$S^n(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, E[n]) \longrightarrow \prod_p H^1(\mathbb{Q}_p, E)\right).$$

Selmer and Sha

Theorem (kernel–cokernel exact sequence)

From any pair of maps of abelian groups (or modules, etc.)

$$A \xrightarrow{f} B \xrightarrow{g} C$$

there is an exact sequence

$$0 \longrightarrow \ker f \longrightarrow \ker(g \circ f) \longrightarrow \ker g \longrightarrow \operatorname{coker} f$$

$$\longrightarrow \operatorname{coker}(g \circ f) \longrightarrow \operatorname{coker} g \longrightarrow 0.$$

Applying the theorem to

$$H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E)[n] \longrightarrow \prod_p H^1(\mathbb{Q}_p, E)[n]$$

Selmer and Sha

We get,

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S^n(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[n] \longrightarrow 0.$$

where,

$$S^n(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E[n]) \longrightarrow \prod_p H^1(\mathbb{Q}_p, E) \right).$$

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \longrightarrow \prod_p H^1(\mathbb{Q}_p, E) \right).$$

These are called **Selmer** and **Sha** group respectively.
We are interested in proving the **finiteness** of the Selmer group as the Weak Mordell-Weil group **injects** into it.
Remark: (We won't need it later) The Sha group provides a measure of the failure of the Hasse principle for genus 1 curves.

Algebraic Number Theory

Number Field

- Let L be a number field (finite extension of $\mathbb{Q}$)
- Ring of integers, $O_L :=$ all such number in L which is a root of a monic polynomial with integer coefficients.
- In general, factorisation into irreducible elements in O_L is not unique. e.g in $\mathbb{Z}[\sqrt{-5}]$,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

- As O_L is not necessarily a PID in general, hence it is not necessarily a UFD. e.g in $\mathbb{Z}[\sqrt{-5}]$, the ideal $(2, 1 + \sqrt{-5})$ is not principal.

Ideals are the "new numbers"

- However, any proper ideal $\mathfrak{a} \subset O_L$ can be written uniquely as:

  $$\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_n^{r_n} \quad , \quad \mathfrak{p}_i s \text{ are prime ideals, } r_i \in \mathbb{N}$$

  Compare the above with prime power factorisation of a usual integer.
- A fractional ideal is a finitely generated O_L submodule in L. It is principle if it is generated by a single element.

Example

$\frac{1}{2}\mathbb{Z}$, the set of half integers in $\mathbb{Q}$ is an example of a fractional ideal which is also principal.
In fact, one can show that any fractional ideal in $\mathbb{Q}$ is principle i.e can be written as $q\mathbb{Z}$ for some $q \in \mathbb{Q}$.

Thus an ideal is an analogue of a usual integer, while a fractional ideal resembles a rational number.

Ideal Class Group

- The set of all fractional ideals of L is denoted by $Id(O_L)$ and the set of all principle fractional ideals is denoted by $P(O_L)$.
- Product of two fractional ideals is again a fractional ideal.

$$\mathfrak{a} \cdot \mathfrak{b} = \{ \sum_{finite} a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \}$$

- O_L is a identity as $\mathfrak{a} \cdot O_L = O_L \cdot \mathfrak{a} = \mathfrak{a}$.
- It turns out that every element in $Id(O_L)$ is invertible, hence forms an abelian group with $P(O_L)$ being a subgroup.

Example

Inverse of $q\mathbb{Z}$ in $\mathbb{Q}$ is the fractional ideal $q^{-1}\mathbb{Z}$.

Ideal Class Group

- In fact, any fractional ideal can be uniquely written as:

  $$\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_n^{r_n} \qquad , \quad \mathfrak{p}_i s \;\text{ are prime ideals, } r_i \in \mathbb{Z}$$

  Thus, fractional ideals indeed mimic the rational numbers, and we further have that $Id(O_L) = \bigoplus_{\mathfrak{p}\ prime} \mathbb{Z}$.
- We write, $v_{\mathfrak{p}_i}(\mathfrak{a}) = r_i$ (valuation of $\mathfrak{p}_i$ at $\mathfrak{a}$)

Definition (Ideal Class group)

$$Cl(O_L) = Id(O_L)/P(O_L)$$

$Cl(O_L)$ is a measure of the failure of O_L to be a PID and it is a finite group.

Example

$$Cl(\mathbb{Z}) = CL(O_{\mathbb{Q}}) = \{e\}$$

Unit group

- $\mu(L) :=$ group of invertible elements in O_L

Example

$$\mu(\mathbb{Q}) = \{\pm 1\}$$

$$\mu(\mathbb{Q}(i)) = \{\pm 1, \pm i\}$$

$$\mu(\mathbb{Q}(\sqrt{3})) = \{\pm(2+\sqrt{3})^n \mid n \in \mathbb{Z}\}$$

Theorem

$\mu(L)$ is finitely generated.

- Note that we have the following exact sequence:

$$0 \to \mu(L) \to L^\times \xrightarrow{v_\mathfrak{p}} \bigoplus_{\mathfrak{p}\ prime} \mathbb{Z} \to Cl(O_L) \to 0$$

- Indeed, if $\alpha \in \mu(L)$, $v_\mathfrak{p}(\alpha) = 0$ for all $\mathfrak{p}$.

Units and Ideal Class group

- Let T be a finite set of prime ideals.
- $T-$units group and $T-$ideal class group is defined by the exactness of the following sequence:

$$0 \to \mu(L)_T \to L^\times \xrightarrow{v_\mathfrak{p}} \bigoplus_{\mathfrak{p}\notin T} \mathbb{Z} \to Cl(O_L)_T \to 0$$

Theorem

$\mu_T := \mu(L)_T$ is finitely generated and $C_T := Cl(O_L)_T$ is finite.

Proof sketch:

Apply ker-coker exact seq to $L^\times \to \bigoplus_\mathfrak{p} \mathbb{Z} \to \bigoplus_{\mathfrak{p}\notin T} \mathbb{Z}$ to get

$$0 \to \mu(L) \to \mu_T \to \bigoplus_{\mathfrak{p}\in T} \mathbb{Z} \to CL(O_L) \to C_T \to 0$$

An important theorem

Theorem

Following is a finite set.

$$N = \{a \in L^\times : v_{\mathfrak{p}}(a) \equiv 0 \pmod{n} \text{ \textit{for all} } \mathfrak{p} \notin T\}/L^{\times n}$$

$$= Ker\left(a \mapsto (v_{\mathfrak{p}}(a) \bmod n) : L^\times/L^{\times n} \longrightarrow \bigoplus_{\mathfrak{p} \notin T} \mathbb{Z}/n\mathbb{Z}\right)$$

Proof.

As μ_T is finitely generated and C_T is finite, note that it is enough to prove the existence of the following exact sequence:

$$0 \longrightarrow \mu_T/\mu_T^n \longrightarrow N \longrightarrow (C_T)[n]$$

We will chase the following diagram:

An important theorem

Proof.

$$\begin{tikzcd}
0 \arrow[r] & \mu_T \arrow[r] \arrow[d, "n"] & L^\times \arrow[r] \arrow[d, "n"] & \bigoplus_{\mathfrak{p}\notin T}\mathbb{Z} \arrow[r] \arrow[d, "n"] & C_T \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & \mu_T \arrow[r] & L^\times \arrow[r] \arrow[d] & \bigoplus_{\mathfrak{p}\notin T}\mathbb{Z} \arrow[r] \arrow[d] & C_T \arrow[r] & 0 \\
. & . & L^\times/L^{\times n} \arrow[r] & \bigoplus_{\mathfrak{p}\notin T}\mathbb{Z}/n\mathbb{Z} & . & .
\end{tikzcd}$$

let $\alpha \in L^\times$ represent an element of N. Then $n \mid v_\mathfrak{p}(\alpha)$ for all $\mathfrak{p} \notin T$. So if we let c in C_T to be the class of $\frac{v_\mathfrak{p}(\alpha)}{n}$, then clearly $nc = 0$ as nc comes from an element in $L^\times$. If $c = 0$, then there exists a $\beta \in L^\times$ such that $v_\mathfrak{p}(\beta) = v_\mathfrak{p}(\alpha)/n$ for all $\mathfrak{p} \notin T$. Now α/β^n lies in U_T, and is well-defined up to an element of U_T^n. ■

Local Fields

Definition

A local field is a locally compact complete field with respect to an absolute value (absolute values are often called primes).

Example

$\mathbb{R}$ *is the completion of* $\mathbb{Q}$ *with respect to the usual absolute value (which is referred as infinite prime) and* $\mathbb{Q}_p$ *is the completion of* $\mathbb{Q}$ *with respect to p-adic absolute value (which is referred as finite prime).*

- $\mathbb{Z}_p := \{a \in \mathbb{Q}_p \mid v_p(a) \geq 0\}$ is a local ring with its unique maximal ideal being $p\mathbb{Z}_p$ which has p as a generator/uniformizer.
- $\mathbb{Z}_p/p\mathbb{Z}_p \cong F_p$ is its residue field.

Local Fields

Example

Let K be a number field. We get infinite primes from the embeddings $K \to \mathbb{C}$ and finite primes from the prime ideals $\mathfrak{p}$ where the $\mathfrak{p}$-adic absolute values are defined as:

$$v_{\mathfrak{p}}(\alpha) := v_{\mathfrak{p}}(\alpha O_K) \ \ \textit{(defined in fractional ideal section)}$$

- By Ostrowski, every prime is of this form.
- $K_{\mathfrak{p}}$ is a finite extension of $\mathbb{Q}_p$.
- Ring of integers (in $K_{\mathfrak{p}}$), $R_{\mathfrak{p}} := \{a \in K_{\mathfrak{p}} \mid v_{\mathfrak{p}}(a) \geq 0\}$ is a local ring with its unique maximal ideal being $\mathfrak{m} := \{a \in K_{\mathfrak{p}} \mid v_{\mathfrak{p}}(a) > 0\}$. Any $\pi \in \mathfrak{m} \backslash \mathfrak{m}^2$ is a generator/uniformizer.
- $R_{\mathfrak{p}}/\mathfrak{m}$ is its residue field which is a finite extension of F_p and denoted as $F_{\mathfrak{p}}$.

Ramification

- Let L/K be finite number field extension and $\mathfrak{b}$ is a prime ideal in L which is over the prime ideal $\mathfrak{p}$ in K i.e $\mathfrak{p}O_L \subset \mathfrak{b}$.
- Then we have a field extension $L_\mathfrak{b}/K_\mathfrak{p}$ with uniformizers being $\pi_\mathfrak{b}$ and $\pi_\mathfrak{p}$ respectively.
- $R_\mathfrak{b}$ being a local ring, we have,

$$\pi_\mathfrak{p} R_\mathfrak{b} = \pi_\mathfrak{b}^e R_\mathfrak{b}$$

  for some integer $e > 0$ which we call ramification index.
- The extension $L_\mathfrak{b}/K_\mathfrak{p}$ is said to be unramified if $e = 1$.

Ramification

Theorem

Let $F/\mathbb{Q}_p$ be a finite extension. Then there is an absolute value on F which extends the p-adic absolute value.

Theorem

For each integer $f > 0$, there exists a unique unramified extension $F/\mathbb{Q}_p$ of degree f. It is obtained by adjoining a primitive $(p^f - 1)$-th root of unity to $\mathbb{Q}_p$.

Corollary

For any finite extension k of $\mathbb{F}_p$, there exists an unramified extension K of $\mathbb{Q}_p$ of degree $[k : \mathbb{F}_p]$ such that $\mathcal{O}_K/p\mathcal{O}_K = k$.

See [Feo] for proofs.

More on $p-$adic numbers

Theorem (Hensel Lemma)

Let $f \in \mathbb{Z}_p[x]$ and $x_0 \in \mathbb{Z}_p$ such that $f(x_0) \equiv 0 \pmod{p}$ and $f'(x_0) \not\equiv 0 \pmod{p}$. Then, $\exists x \in \mathbb{Z}_p$ such that $f(x) = 0$ and $x \equiv x_0 \pmod{p}$.

The proof is similar to Newton-Raphsan method in numerical analysis and can be found at [Poo09].

The theorem is very powerful as it reduces to finding the solution in $\mathbb{F}_p$, and so finitely many values to check.

Corollary

$\mathbb{Z}_p$ contains all $(p-1)$-th roots of unity.

A filtration on p-adics

- Any $x \in \mathbb{Q}_p^\times$ can be written uniquely as $x = up^m$ with $u \in \mathbb{Z}_p^\times$ and $m \in \mathbb{Z}$.
- k-th principal unit grp, $U^k = \{u \in \mathbb{Z}_p^\times \mid u \equiv 1 \pmod{p^k}\}$
- We have the filtration:

$$\mathbb{Q}_p^\times \supset U^0 = \mathbb{Z}_p^\times \supset U^1 \supset U^2 \supset \cdots$$

- $\bigcap U^i = \{1\}$
- $\mathbb{Q}_p^\times / \mathbb{Z}_p^\times \cong \mathbb{Z}$, and $U^0/U^1 \cong \mathbb{F}_p^\times$
- $U^n/U^{n+1} \cong \mathbb{F}_p^+$ (additive group)
  where the map is given by $u \to p^{-n}(u - u_0) \bmod (p)$ given that the first term in the base-p expansion of u is u_0.

Theorem

The multiplication by m map, $m : U^1 \to U^1$, is bijective.

A filtration on p-adics

Proof.

Let u be in U^1. Consider the polynomial $f(x) = x^m - u$. $1 \in \mathbb{F}_p$ is a simple root of f mod p. By Hensel's lemma, it lifts to a root of $f(x)$. We are left with proving uniqueness of m-th roots in U^1.

- We first prove that 1 is the only m-th root of 1 in U^1. If $u \neq 1$ is an element in $U^{(1)}$ such that $u^m = 1$, there is some n such that u lies in $U^n \backslash U^{n+1}$. If we set $\bar{u}$ to be the image of u in $\mathbb{F}_p^+ \cong U^n/U^{n+1}$, we have $\bar{u} \neq 0$ and thus $m\bar{u} \neq 0$ as $(m, p) = 1$. Under the isomorphism, $m\bar{u}$ corresponds to u^m, so we get a contradiction.
- If a, b are elements in U^1 such that $a^m = b^m = u$, then a/b is an m-th root of 1 which belongs to U^1. By the above, $a/b = 1$ so that $a = b$.

■

Some results in elliptic curves

Reduction of an Elliptic Curve

Consider an elliptic curve

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

We make a change of variables $X \mapsto X/c^2$, $Y \mapsto Y/c^3$ with c chosen so that the new a, b are integers and Δ is minimal — the equation is then said to be minimal.

The following equation is called the *reduction of E mod p*.

$$\tilde{E} : Y^2Z = X^3 + \bar{a}XZ^2 + \bar{b}Z^3; \quad (\bar{a}, \bar{b}) = (a, b) \ mod \ p$$

Definition

If $p \neq 2$ and $p \nmid \Delta$ (i.e $\tilde{E}$ is smooth over $\mathbb{F}_p$), then E is said to have a good reduction modulo p.

Otherwise, it is said to have a bad reduction.

A Filtration

We can define filtration of elliptic curves similar to that of p-adics and it has similar results:

$$E(\mathbb{Q}_p) \supseteq E^0(\mathbb{Q}_p) \supseteq E^1(\mathbb{Q}_p) \supseteq \cdots$$

First, define

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \bar{P} \text{ is nonsingular}\}.$$

Write $\tilde{E}^{\text{ns}} = \tilde{E}/\text{singular points}$. The following reduction map is a homomorphism.:

$$P \mapsto \bar{P} : E^0(\mathbb{Q}_p) \to \tilde{E}^{\text{ns}}(\mathbb{F}_p)$$

We define $E^1(\mathbb{Q}_p)$ to be its kernel which are smooth points (x, y, z) with $p|x, z$ and $p \nmid y$. Generally we define:

$$E^n(\mathbb{Q}_p) = \{P \in E^1(\mathbb{Q}_p) \mid \frac{x(P)}{y(P)} \in p^n\mathbb{Z}_p\}$$

Filtration theorem

We have similar kind of properties of the filtration like the ones in p-adics.

Theorem

The filtration

$$E(\mathbb{Q}_p) \supseteq E^0(\mathbb{Q}_p) \supseteq E^1(\mathbb{Q}_p) \supseteq \cdots$$

has the following properties:

1. $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ *is finite;*
2. $P \mapsto \bar{P}$ *gives an isomorphism* $E^0(\mathbb{Q}_p)/E^1(\mathbb{Q}_p) \cong \tilde{E}^{ns}(\mathbb{F}_p)$*;*
3. $E^n(\mathbb{Q}_p)$ *(with* $n \geq 1$*) is a subgroup of* $E(\mathbb{Q}_p)$*, and the map* $P \mapsto p^{-n}\frac{x(P)}{y(P)} \pmod p$ *mod* p *is an isomorphism* $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \cong \mathbb{F}_p$*;*
4. *the filtration is exhaustive, i.e.* $\bigcap_n E^n(\mathbb{Q}_p) = \{0\}$.

Filtration theorem

Corollary

For every integer m not divisible by p, the map

$$P \mapsto mP : E^1(\mathbb{Q}_p) \to E^1(\mathbb{Q}_p)$$

is a bijection.

Detailed proofs at [Sza; Mil06].

All theorems we discuss in this section remains valid if we replace $\mathbb{Q}_p$ by a finite unramified extension K of it, p by the uniformizer π, F_p by F_π, v_p by v_π. The reason it remains valid is because we can choose p to be the uniformiser of the extension. For the sake of simplicity, we provide the proofs of the next theorems for $\mathbb{Q}_p$ only, even though they are valid for finite unramified extensions of $\mathbb{Q}_p$.

Why good reduction is good

Theorem

Let $E(\mathbb{Q}_p)$ has good reduction, and $p \nmid n$. $P \in E(\mathbb{Q}_p)$ is of the form nQ for some $Q \in E(\mathbb{Q}_p)$ iff its image $\bar{P} \in \tilde{E}(\mathbb{F}_p)$ is of the form $n\bar{Q}$ for some $\bar{Q} \in \tilde{E}(\mathbb{F}_p)$.

Proof.

Chase the diagram along with the fact that the first vertical arrow is an isomorphism.

$$\begin{tikzcd}
0 \arrow[r] & E^1(\mathbb{Q}_p) \arrow[r] \arrow[d, "n", "\simeq"'] & E(\mathbb{Q}_p) \arrow[r] \arrow[d, "n"] & \tilde{E}(\mathbb{F}_p) \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & E^1(\mathbb{Q}_p) \arrow[r] & E(\mathbb{Q}_p) \arrow[r] & \tilde{E}(\mathbb{F}_p) \arrow[r] & 0
\end{tikzcd}$$

$\blacksquare$

Why good reduction is good

Theorem

Let $E(\mathbb{Q}_p)$ has a good reduction and $p \nmid n$. For any $P \in E(\mathbb{Q}_p)$, there exists a finite unramified extension K of $\mathbb{Q}_p$ such that $P \in nE(K)$.

Proof.

As multiplication by n is surjective on $E(\overline{\mathbb{F}_p})$, there is a finite extension $k/\mathbb{F}_p$ such that $P \in nE(k)$. Recall the theorem:

Theorem

For any finite extension k of $\mathbb{F}_p$, there exists an unramified extension K of $\mathbb{Q}_p$ of degree $[k : \mathbb{F}_p]$ such that $\mathcal{O}_K/p\mathcal{O}_K = k$.

Then our proof is done using this theorem and the theorem in last slide where $\mathbb{Q}_p$ is replaced by a finite unramified extension (and $\mathbb{F}_p$ by $\mathbb{F}_{p^r}$). ■

Selmer group revisited

Definition

Let $m > 1$ be an integer. The m-Selmer group of E is

$$S^m(E/K) := \ker\left(H^1(K, E[m]) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E)\right).$$

The Tate-Shafarevich group of E is

$$\text{III}(E/K) := \ker\left(H^1(K, E) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E)\right).$$

We get the following exact sequence:

$$0 \to E(K)/mE(K) \to S^m(E/K) \to \text{III}(E/K)[m] \to 0.$$

Selmer group revisited

Lemma

If $L|K$ is a finite extension, then the following map has finite kernel.

$$\mathrm{Res}\colon H^1(K, E[m]) \to H^1(L, E[m])$$

Proof.

Applying the inflation-restriction sequence with $G = Gal(\overline{K}/K)$, $H = Gal(\overline{L}/L) = Gal(\overline{K}/L)$ and $M = E[m]$, there is an exact sequence

$$0 \to H^1(G/H, E[m](L)) \xrightarrow{\mathrm{Inf}} H^1(K, E[m]) \xrightarrow{\mathrm{Res}} H^1(L, E[m]).$$

Selmer group revisited

Proof.

But $H^1(G/H, E[m](L))$ is finite because both $G/H \cong Gal(L/K)$ and $E[m](L)$ are finite (will show finiteness of $E[m]$ later briefly), so there are finitely many maps between them. ■

As a consequence, we get the following result.

Corollary (Corollary 9.13)

The map $S^{(m)}(E/K) \to S^{(m)}(E/L)$ has finite kernel (the map is induced from restriction map).

Thus to prove Weak Mordell-Weil, we may replace K by a finite extension. So we can assume that K is so large that $E[m](K)$ is contained in $E(K)$ and that K contains μ_m.

Weak Mordell-Weil Theorem

Structure of *m*-th torsion group (quick sketch)

Definition

A lattice in $\mathbb{C}$ is an additive subgroup $\Lambda \subseteq \mathbb{C}$ of the form

$$\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\} \ \ ; Im(\omega_2/\omega_1) \neq 0$$

Definition

An elliptic function is a meromorphic function on $\mathbb{C}$ such that $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in \Lambda$, where Λ is a lattice in $\mathbb{C}$.

Example (Weierstrass $\wp$-function)

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Structure of *m*-th torsion group (quick sketch)

- $\wp'$ (Complex derivative of $\wp$) satisfies:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

  with $g_2 = 60\sum_{\omega\neq 0}\omega^{-4}$, $g_3 = 140\sum_{\omega\neq 0}\omega^{-6}$

- Elliptic curve $E(\mathbb{C})$ defined by the above equation is smooth.
- Every elliptic curve arises as the image of the following group homomorphism:

$$\psi:\ \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2, \qquad z \mapsto \Big(\wp(z), \wp'(z), 1\Big)$$

- $E(\mathbb{C})[m] \cong \mathbb{C}/\Lambda[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$
- If $E(\mathbb{C})$ is defined by a rational polynomial, it is easy to see that every torsion point is algebraic. Hence,

$$E(\overline{\mathbb{Q}})[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Weak Mordell-Weil

Theorem

$E(\mathbb{Q})/mE(\mathbb{Q})$ is finite.

Proof.

- It is enough to show $S^m(E/K)$ is finite with $K/\mathbb{Q}$ finite.
- Let $K/\mathbb{Q}$ be the finite extension which contains all $m-$torsion points, $E[m]$ and $m-$th roots of unity, μ_m.
- So action of G_K is trivial on $E[m]$ and μ_m, thus we have:

$$H^1(K, E[m]) \cong H^1(K, (\mathbb{Z}/m\mathbb{Z})^2) \cong Hom(G_K, (\mathbb{Z}/m\mathbb{Z})^2)$$

$$\cong Hom(G_K, \mathbb{Z}/m\mathbb{Z})^2 \cong Hom(G_K, \mu_m)^2$$

$$\cong H^1(K, \mu_m)^2 \cong (K^\times/K^{\times^m})^2$$

Weak Mordell-Weil

Proof.

- Thus $S^m(E/K)$ is a subgroup of $(K^\times/K^{\times^m})^2$
- Let $S = S_1 \cup S_2 \cup S_3$ be the finite set of primes, where $S_1 =$ bad primes, $S_2 =$ primes dividing (m), and $S_3 =$ infinite primes
- Let $\alpha \in S^n(E/K)$ with image $\alpha_\mathfrak{p} \in H^1(K_\mathfrak{p}, E[m])$, $\mathfrak{p} \notin S$
- As $\alpha_\mathfrak{p}$ maps to 0 in $H^1(K_\mathfrak{p}, E)$, it comes from an element $\beta_\mathfrak{p} \in E(K_\mathfrak{p})/mE(K_\mathfrak{p})$.
- Let $\beta_\mathfrak{p}$ is represented by $\tilde{Q} \in E(K_\mathfrak{p})$.
- As $\mathfrak{p} \notin S$, there is a finite unramified extension $L_\mathfrak{p}/K_\mathfrak{p}$ such that Q is m-divisible in $E(L_\mathfrak{p})$

Weak Mordell-Weil

Proof.

- Hence, $\beta_{\mathfrak{p}}$ maps to zero in $E(L_{\mathfrak{p}})/mE(L_{\mathfrak{p}})$, thus $\alpha_{\mathfrak{p}}$ maps to zero in $H^1(L_{\mathfrak{p}}, E[m])$.

$$\begin{tikzcd}
\beta_{\mathfrak{p}} \arrow[d] & E(K_{\mathfrak{p}})/mE(K_{\mathfrak{p}}) \arrow[r] \arrow[d] & H^1(K_{\mathfrak{p}}, E[m]) \arrow[d] & \alpha_{\mathfrak{p}} \arrow[d] \\
0 & E(L_{\mathfrak{p}})/mE(L_{\mathfrak{p}}) \arrow[r] & H^1(L_{\mathfrak{p}}, E[m]) & 0
\end{tikzcd}$$

- Since L_p/K_p is unramified, we get the following diagram:

$$\begin{tikzcd}
\alpha_{\mathfrak{p}} \arrow[d] & H^1(K_{\mathfrak{p}}, E[m]) \arrow[r, "\sim"] \arrow[d] & (K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times m})^2 \arrow[r, "\nu_{K_{\mathfrak{p}}}"] \arrow[d] & (\mathbb{Z}/m\mathbb{Z})^2 \arrow[d, "id"] \\
0 & H^1(L_{\mathfrak{p}}, E[m]) \arrow[r, "\sim"] & (L_{\mathfrak{p}}^{\times}/L_{\mathfrak{p}}^{\times m})^2 \arrow[r, "\nu_{L_{\mathfrak{p}}}"] & (\mathbb{Z}/m\mathbb{Z})^2
\end{tikzcd}$$

Weak Mordell-Weil

Proof.

- So, $\alpha_{\mathfrak{p}}$ corresponds to a pair $(\alpha_1, \alpha_2) \in (K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times^m})^2$ such that $v_{K_{\mathfrak{p}}}(\alpha_1) \equiv v_{K_{\mathfrak{p}}}(\alpha_2) \equiv 0 \pmod{m}$.
- Hence, finitely many choices for α
- $\therefore S^m(E/K) < \infty$

■

Mordell-Weil Theorem

Descent Procedure

Theorem

Let A be an abelian group. Assume there exists a "height" function

$$h : A \longrightarrow \mathbb{R}$$

with the following properties:

(i) *Let $Q \in A$. For all $P \in A$, there exists a constant C_1 (depending only on A and Q) such that*

$$h(P+Q) \leq 2h(P) + C_1.$$

(ii) *There is an integer $m \geq 2$ and a constant C_2 (depending only on A) such that for all $P \in A$,*

$$h(mP) \geq m^2 h(P) - C_2.$$

Descent Procedure

Theorem

(iii) *For each constant C_3, the set*

$$\{P \in A : h(P) \leq C_3\}$$

is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite. Then A is finitely generated.

Proof.

Let $Q_1, \ldots, Q_r \in A$ be representatives of the finitely many cosets of A/mA. The strategy is to subtract suitable multiples of the Q_i from any $P \in A$ so that the resulting point has bounded height independent of P. Thus, the Q_i's together with finite points of bounded height, will generate A.

Descent Procedure

Proof.

Let $P \equiv Q_{i_1} \pmod{mA} \implies P = mP_1 + Q_{i_1}$.
Proceeding recursively, we obtain

$$P_1 = mP_2 + Q_{i_2}, \quad P_2 = mP_3 + Q_{i_3}, \quad \ldots, \quad P_{n-1} = mP_n + Q_{i_n}.$$

Now, for any j, using property (ii) and (i), we compute:

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}\Big(h(mP_j) + C_2\Big) \\ &= \frac{1}{m^2}\Big(h(P_{j-1} - Q_{i_j}) + C_2\Big) \\ &\leq \frac{1}{m^2}\Big(2h(mP_{j-1}) + C_0 + C_2\Big) \end{aligned}$$

where C_0 is the max of the constants in (i) for $Q = -Q_i$.

Descent Procedure

Proof.

Iterating the above inequality from P down to P_n, we deduce:

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right) \\ &\qquad (C_0 + C_2) \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_0 + C_1}{m^2 - 2} \\ &\leq 2^{-n} h(P) + \frac{C_0 + C_1}{2} \qquad [Recall \quad m \geq 2] \end{aligned}$$

For sufficiently large n, we have, $h(P_n) \leq 1 + \frac{C_0+C_1}{2}$

Hence we are done! ■

Height on Elliptic Curve

Definition

Let $x = \frac{a}{b} \in \mathbb{Q}$ *(a, b coprime) . The height on* $\mathbb{Q}$ *is defined as:*

$$H(x) = \max\{|a|, |b|\}.$$

The ***height on*** $E(\mathbb{Q})$ *(With Weierstrass eqn) is defined by:*

$$h(P) = \begin{cases} log(H(x(P)) & if \quad P \neq O \\ 0 & else \end{cases}$$

One can check that the above functions are indeed height functions (using addition formulas for coordinates on Weierstrass elliptic curves),

Mordell-Weil Theorem

Theorem

$E(\mathbb{Q})$ is finitely generated.

Proof.

Trivial by the Weak Mordell-Weil and the Descent procedure. ■

References

[Feo] Feog. *p-adic fields: Chapter 7 of Algebraic Number Theory Lecture Notes*. URL: https://feog.github.io/antchap7.pdf.

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishing, 2006. ISBN: 978-1-59973-112-6.

[Mil21] James S Milne. “Fields and Galois theory (v5. 10)”. In: *Amer. Math. Monthly* 128.8 (2021), pp. 753–754.

[Poo09] Bjorn Poonen. *Introduction to Arithmetic Geometry: Lecture Notes for MIT 18.782*. MIT. 2009. URL: https://math.mit.edu/~poonen/782/782notes.pdf.

References

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[Sza] Tam ´as Szamuely. *Lectures On Elliptic Curves*. URL: https://pagine.dm.unipi.it/tamas/Elliptic_Curves.pdf.

Thank you!