Rational points on curves

December 6, 2013

Contents

1 Curves of genus 0

1.1 Rational points

Let C be a curve of genus 0 defined over rational. We are concerning the question when C has a rational point in $\mathbb{Q}$. Notice that if $C(\mathbb{Q}) \neq \emptyset$ then $C(\mathbb{Q}_p) \neq \emptyset$ where $p = \infty$ or primes, and $\mathbb{Q}_\infty = \mathbb{R}$ and $\mathbb{Q}_p$ is the field of p-adic numbers.

Theorem 1.1 (Hasse principle)**.** *The $C(\mathbb{Q}) \neq \emptyset$ if and only if $C(\mathbb{Q}_p) \neq \emptyset$ for all places p of $\mathbb{Q}$. In this case $C \simeq \mathbb{P}^1$.*

Proof. First, there is an embedding of C into $\mathbb{P}^2$ by anti-canonical bundle Ω_C^{-1}. The image is defined by a quadratic equation $f(x, y, z) = 0$. We may diagonalize this form to

$$ax^2 + by^2 + cz^2 = 0$$

with $a, b, c \in \mathbb{Q}^\times$. Scaling equation and coordinates will make an equation like

$$ax^2 + by^2 = z^2$$

with a and b square free integers and $|a| \leq |b|$. There is nothing to prove if $a = 1$. Otherwise any rational solution will have $y \neq 0$. Notice that a solution of this equation makes b a norm of the form $z/y + x/y\sqrt{a}$. Recall that the set of norms of $\mathbb{Q}(\sqrt{a})$ for a subgroup in $\mathbb{Q}^\times$.

Assume $C(\mathbb{Q}_p) \neq \emptyset$ for every place p. We want to prove that $C(\mathbb{Q}) \neq \emptyset$ by induction on $m = |a| + |b|$.

If $m = 2$, then $a = -1$ and $b = 1$. It is clear that $C(\mathbb{Q}) \neq \emptyset$.

Now assume that $m > 2$, or $|b| \geq 2$. We claim that a is a square mod b. By Chinese Remainder Theorem, it suffices to show this mod every prime factor p of b. Let $(x, y, z) \in \mathbb{Q}_p^3$ be a nonzero solution to the equation. Then we may assume that $x, y, z \in \mathbb{Z}_p$ such that one of them is a unit in $\mathbb{Z}_p$. If x is not a unit, then so is z. Then it is easy to see that y is not a unit neither. This gives a contradiction. Thus we have $a = (z/x)^2 \mod p$. Thus claim follows.

By claim we have a $t \in \mathbb{Z}$ such that $t^2 = a + bb'$. We may take t such that $|t| \le |b|/2$. Then we have $bb' = t^2 - a$. Thus bb' is the norm of $t + \sqrt{a}$. Thus b is a norm if and only if b' is a norm, namely

$$ax^2 + b'y^2 = z^2$$

has a rational solution. Now $|b'| = |(t^2 - a)/b| \le (|b|/4 + 1) < |b|$. Induction works.

If $C(\mathbb{Q}) \neq \emptyset$, pick a point $P \in C(\mathbb{Q})$, then for any $Q \in C(\mathbb{Q})$ the line defined a bijection between C and moduli of lines in $\mathbb{P}^2$ passing through P. Thus we have shown $C \simeq \mathbb{P}^1$. □

Hilbert symbol

How to check if $C(\mathbb{Q}_p) \neq \emptyset$? For $a, b \in \mathbb{Q}_p$, let us define $(a, b)_p \in \{\pm 1\}$ takes value 1 if and only if the equation $ax^2 + by^2 = z^2$ has a solution. We need to compute this symbol. If $p = \infty$, then $(a, b)_\infty = 1$ unless $a < 0, b < 0$. In the following we assume that $p \neq \infty$.

This symbol depends on the classes of a and b in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. If one the class of a and b is trivial then it is clear that $(a, b)_p = 1$. Otherwise $(a, b)_p = 1$ if and only if a is norm in $\mathbb{Q}_p(\sqrt{b})$ and if and only if b is a norm in $\mathbb{Q}_p(\sqrt{a})$. These facts together imply that the symbol $(a, b)_p$ is bilinear on $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. We have some simple formulae: $(a, -a)_p = 1$ and $(a, 1 - a)_p = 1$ if $a \neq 0, 1$.

Recall that

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mu_p \times (1 + p\mathbb{Z}_p) \quad (p \neq 2), \qquad \mathbb{Q}_2^\times = 2^{\mathbb{Z}} \times \mu_2 \times (1 + 4\mathbb{Z}_2).$$

The subgroups of squares are given by

$$(\mathbb{Q}_p^\times)^2 = p^{2\mathbb{Z}} \times \mu_p^2 \times (1 + p\mathbb{Z}_p) \quad (p \neq 2), \qquad (\mathbb{Q}_2^\times)^2 = 2^{2\mathbb{Z}} \times (1 + 8\mathbb{Z}_2).$$

Thus the quotient group has rank 2 over $\mathbb{F}_2$ if $p \neq 2$ and rank 3 if $p = 2$.

First let us consider the case where $p \neq 2$. We has a three cases.

If both a, b are non-square in μ_p, then the equation $ax^2 + by^2 = z^2$ has good reduction over $\mathbb{F}_p$. Thus it suffices to solve this equation mod p. We claim there is always a solution with $z = 1$ by consider the subsets A and B of $\mathbb{F}_p$ of the elements of the form ax^2 and $1 - by^2$ respectively. In fact both sets has size $1 + (p - 1)/2 = (p + 1)/2$. Thus must have non-empty intersection.

If a is a non-square in μ_p, and $b = p$, then any primitive solution of $ax^2 + py^2 = z^2$ will have x to be unit. Mod p gives a solution $ax^2 \equiv y^2$. A contradiction.

If both $a = b = p$, then $(p, p)_p = (p, -p^2) = (p, -1) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)2}$. In summary, we have shown for $a = p^\alpha u, b = p^\beta v$,

$$(a, b)_p = (-1)^{\alpha\beta(p-1)/2} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

Now let us work on $p = 2$. The quotient group is generated by 2, -1 and 5.

If both $a = 5$ and b are unit, then $a + 4b \equiv 1 \mod 8$. Thus we have a solution $(1, 2, z)$. Thus $(5, 5)_2 = (5, -1)_2 = 1$. If both $a = b = -1$, then the equation becomes $x^2 + y^2 + z^2 = 0$. A primitive solution will have residue $0, 1$ mod 8. This is impossible. Thus $(-1, -1)_2 = -1$.

If $a = 2$ and b a unit, then any primitive solution will have both y and z are unit. Mod 8 gives $2x^2 + b \equiv 1 \mod 8$. This implies that $b \equiv -1$ with solution $(1, 1, 1)$.

If $a = b = 2$, then $(2, 2)_2 = (2, -1)_2 = 1$. In summary, we have shown for $a = 2^\alpha u$ and $b = 2^\beta v$, then

$$(a, b)_2 = (-1)^{(u-1)(v-1)/4+\alpha(v^2-1)/8+\beta(u^2-1)/8}.$$

A direct computation shows that for any $a, b \in \mathbb{Q}^\times$, $\prod(a, b)_p = 1$. Conversely for given $a_i \in \mathbb{Z}\backslash 0$, $\epsilon_{ip} \in \pm 1$, the solvability of the equation

$$(x, a_i)_p = \epsilon_{ip}$$

is equivalent to local solvability x_p. Let S be a set of primes including ∞, 2 and all prime factors. Let T be the set of primes where some $\epsilon_{ip} = -1$. First let us reduce to the case $S \cap T = \emptyset$ by choosing a $x' \in \mathbb{Q}^\times$ such that x_p/x' is a square of $\mathbb{Q}_p^\times$. Then we may replacing ϵ_{ip} by $\epsilon_{ip}(x', a_i)$.

When $S \cap T = \emptyset$, we take $a = \prod_{\ell \in T} \ell$, $m = 8 \prod_{\ell \in S\backslash\{2\}} \ell$. Choose a prime q not in S and T such that $q \equiv a \mod m$. Then $x = ap$ is a solution. It is clear that $(x, a_i)_p = 1$ for $p \in S$ or not in $\{q\} \cap T$. If $p \in T$, then there is a x_p such that $(x_p, a_i)_p = \epsilon_{ip}$. Since one of $\epsilon_{ip} = -1$, $\mathrm{ord} x_p = 1$. Thus it equal to (x, a_i). The case at $p = q$ follows from the product formula.

1.2 Representation by quadratic forms

A generalization of above theorem is the following:

Theorem 1.2. *Let f be a non-degenerate quadratic form on $\mathbb{Q}$ of n variebles. Then an element $a \in \mathbb{Q}$ is represented by f if and only if it is represented locally.*

It suffices to reduce to the case where $a = 0$. In fact, if f represents zero then f represents any number since there is a direct decomposition $f = g \oplus h$ with h a hyperbolic form. Otherwise, we replace f by $f \oplus -az^2$. In the following we assume that $a = 0$ and f represents 0 locally. We have shown that f represent 0 in the case $n = 3$.

If $n = 2$, then f has form $ax^2 + by^2$. If f locally represents 0, then $-ab$ is a square in all $\mathbb{Q}_p$. It follows that $-ab$ is a square in $\mathbb{Q}^\times$. Thus f represents 0 over $\mathbb{Q}$.

If $n = 4$ and $f = \sum_{i=1}^4 a_i x_i^2$, then local solvability implies that there are $A_p \in \mathbb{Q}_p^\times$ represented by both

$$a_1x_1^2 + a_2x_2^2, \qquad -a_3x_3^2 - a_4x_4^2.$$

Using Hilbert symbol, this is equivalent to the equation

$$(A_p, -a_1a_2)_p = (a_1, a_2)_p, \qquad (A_p, -a_3a_4)_p = (-a_3, a_4)_p.$$

The local solvability of these equations and the product formula imply the global solvability: there is a $x \in \mathbb{Q}^\times$ such that

$$(A, -a_1a_2)_p = (a_1, a_2)_p, \qquad (A, -a_3a_4)_p = (-a_3, a_4)_p.$$

This means that A is represented by both above equations in $\mathbb{Q}_p$ thus in $\mathbb{Q}$ by induction. Done!

If $n \geq 5$, we write

$$f = g(x_1, x_2) - h(x_3, \cdots x_n), \qquad g = a_1x_1^2 + a_2x_2^2, \quad h = a_3x_3^2 + \cdots a_nx_n^2.$$

Let S be the set of places including 2, ∞ and all places dividing a_i. Since f represents 0 at each place p, then there are $\alpha_p \in \mathbb{Q}_p^\times$ represented by both g and h. Then by approximation at places at S, there is a $\alpha \in \mathbb{Q}^\times$ represented by g such that α/α_p is a square in $\mathbb{Q}_p^\times$ for all $p \in S$. It remains to show that such an a is represented by h as well. It reduces to show that 0 is represented by the form

$$f_1 = az^2 - h.$$

This form represents 0 at places in S. At places p outside of S, the form h has unit coefficients with unit discriminant. Thus it lifts all zero mod p. Since h has more than 3 variable, it represents 0 at $\mathbb{F}_p$. This last statement is done by study the characteristic function of $V(f)$ given by

$$\sum_{x \in \mathbb{F}_p^{n-1}} (1 - h(x)^{p-1}).$$

Thus we have shown that f_1 represents 0 locally. By induction it represents 0 globally.

Theorem 1.3. *Two quadratic forms f, f' are equivalent over $\mathbb{Q}$ if and only if they are equivalent to $\mathbb{Q}_p$.*

By the previous theorem, there is an $a \in \mathbb{Q}^\times$ represented by both f and f'. Thus we have orthogonal decompositions $f = az^2 + g, f' = az^2 + g'$. To finish the proof, we need to prove that g is locally equivalent to g'. This can be done by proving the following stamens about quadratic space: let e and e' be two elements in a non-degenerate space with same non-zero norms: $e^2 = (e')^2$. then there is an automorphism of V bring e to e'. Choose $\epsilon = \pm 1$ such that $z = e + \epsilon e'$ has non-zero norm. Then we have a decomposition $V = kz + H$. Take an automorphism σ of V which is identity on H but -1 on z. Then $\sigma(e - \epsilon e') = e - \epsilon e'$ and $\sigma(e + \epsilon e') = -e - \epsilon e'$. It follows that $\sigma e = -\epsilon e'$. Then $-\epsilon\sigma$ will take e to e'.

1.3 Local representatbility

For a quadratic form over $\mathbb{Q}_p$ with diagonal decomposition $f = \sum a_i x_i^2$, define the Hasse invariant by $\epsilon = \prod_{i<j}(a_i, a_j) = \pm 1$ and discriminant $d = \prod d_i \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

Theorem 1.4. *For a form f to represent 0 if and only if the following holds:*

1. *$n = 2$ and $d = -1$;*

2. *$n = 3$ and $(-1, d) = \epsilon$;*

3. *$n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$*

4. *$n \geq 5$.*

For $a \in \mathbb{Q}_p^\times$, apply the theorem to $f_a = f - az^2$. Then we have:

Corollary 1.5. *The f represents a if and only if the following holds:*

1. *$n = 1$ and $a = d$;*

2. *$n = 2$, and $(a, -d) = \epsilon$;*

3. *$n=3$ and either $a \neq -d$ or $a=-d$ and $(-1,-d)=\epsilon$;*

4. *$n \geq 4$.*

Proof of theorem: $n=2$ and $n=3$ are basically follow from definition. When $n=4$, f represents 0 if and only if there is a $x \in \mathbb{Q}_p^\times$ represented by two forms $a_1x_1^2+a_2x_2^2$ and $-a_3x_3^2-a_4x_4^2$. By definition, we have

$$(xa_1, xa_2) = (-xa_3, -xa_4) = 1$$

This is equivalent to

$$(x, -a_1a_2) = (a_1, a_2), \qquad (x, -a_3a_4) = (-a_3, -a_4).$$

The non-solvability is equivalent to the following condition:

$$a_1a_2 = a_3a_4, \qquad (a_1, a_2) = -(-a_3, -a_4).$$

The first condition is equivalent to $d=1$. If it is fulfilled then the second condition can be written as $\epsilon = -(-1,-1)$. When $n \geq 5$, then f represents an $a \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ different than d. Then f has the form $f = ax^2+g$, where the discriminant of g is not 1. Thus it represents 0.

Theorem 1.6. *Two quadratic forms are equivalent if and only if they have same rank, same discriminant, and same Hasse invariant.*

When $n=4$, there is a unique form does not represent 0:

$$z^2 - ax^2 - by^2 + abt^2, \qquad (a,b)=1.$$

When $n=3$, there is a unique form up to scale does not represent 0 given by $-ax^2-by^2+abt^2$.

Theorem 1.7 (Classification of curves of genus 0)**.** *For each curve C, let $\Sigma(C)$ denote the set of places p such that $C(\mathbb{Q}_p)=\emptyset$. Then $\Sigma(C)$ is even and the correspondence $C \mapsto \Sigma(C)$ defines a bijection between the set of isomorphism classes of C and the set of even subsets of V.*

2 Curves of genus 1

2.1 Basic algebraic geometry of curves

1. Geometric description: A algebraic curve C over a field k is usually defined by homogenous equations in projective space $\mathbb{P}^n$, which is smooth and connected of dimension 1; C may or may not have rational point. But it has closed points.

2. Algebraic description: The function field $k(C)$ of C over k is a field extension of k of transcendental degree 1. In fact for any $x \in k(C)$ which is not algebraic over k, $k(C)$ is finite extension of $k(x)$. The closed points p are described as normalized non-trivial k-evaluations of $k(C)$:

$$v: \quad k(C) \longrightarrow \mathbb{Z} \cap \{\infty\}$$

such that

(a) $v(x) = \infty$ iff $x = \infty$,

(b) $v(a) = 0$ for all $a \in k^\times$,

(c) $v(t) = 1$ for some $t \in k(C)$,

(d) $v(f + g) \geq \min(v(f), v(g))$.

3. For a closed point p, let ord_p denote the corresponding valuation function, denote the following:

   (a) local ring $\mathscr{O}_p \subset k(C)$ of elements $t \in k(C)$ with non-negative order functions,

   (b) the maximal ideal $m_p \subset \mathscr{O}_p$ of elements $t \in k(C)$ with positive order functions,

   (c) the residue field $k(p) := \mathscr{O}_p/m_p$.

   (d) $\deg p := [k(p) : k]$

4. By a divisor D on C, we mean a finite formal sum

$$D = \sum_p a_p p, \qquad p \in C.$$

   The degree of D is defined as $\sum a_p \deg p$. Let $\mathrm{Div}(C)$ denote the group of divisors.

5. For a non-zero rational functions f, its divisor is defined as

$$\mathrm{div}(f) = \sum_p \mathrm{ord}_p(f)p.$$

   It can be shown that $\deg \mathrm{div}(f) = 0$. Such a divisor called a principle divisor. Let $\mathrm{Pr}(C)$ denote the group of principal divisors.

6. The quotient $\mathrm{Cl}(C) := \mathrm{Div}(C)/\mathrm{Pr}(C)$ is called the group of divisors on C.

7. The set k' of elements of $x \in k(C)$ with vanishing order are exactly invertible elements in the algebraic closure of k in $k(C)$ which is a finite extension of k. The curve C is called geometrically connected if $k' = k$.

8. Let $\Omega^1_{k(C)/k}$ denote the group of rational 1-forms on C: $k(C)$-vector space of form $\sum f_i dg_i$ modulo Leibnitz rule and the equation $dx = 0$ for $x \in k$. When k'/k is separable then $\Omega^1_{k(C)/k}$ is of dimension 1 over $k(C)$.

9. Assume k'/k is separable. For any $\omega \in \Omega^1_{k(C)/k}$ and any closed point p with local parameter t, we may write $\omega = f(t)dt$. Define

$$\mathrm{ord}_p\omega = \mathrm{ord}_p(f) \in \mathbb{Z}, \qquad \mathrm{div}(\omega) = \sum_p \mathrm{ord}_p\omega \cdot p.$$

   The class of $\mathrm{div}(\omega)$ in $\mathrm{Cl}(C)$ does not depend on the choice of ω and called the canonical divisor of C. Let $\Gamma(C, \Omega^1_C)$ de note the k-vector space of

10. The genus of C is defined as $1 + \frac{1}{2} \deg \omega$.

11. Assume $k = k'$. For any divisor D, denote $\Gamma(C, D)$ the space of rational functions f with at poles bounded by D:
$$\mathrm{div}(f) + D \geq 0.$$
Then we have Riemann–Roch theorem:
$$\dim_k \Gamma(C, D) - \dim_k \Gamma(C, \mathrm{div}(\omega) - D) = \deg D + 1 - g.$$
Take $D = \mathrm{div}(\omega)$, then we have $g = \Gamma(C, \Omega_C^1)$, the space of forms with non-negative order at every point p.

12. A morphism $f : \quad C \longrightarrow C'$ of curves gives a finite field extension $k(C') \subset k(C)$, vice visa. Assume f is separable. Then for any point $p \in C$ with image $q \in C'$. We define the ramification $e_p(f)$ as $\mathrm{ord}_p(t) - 1$ where t is a local parameter at q. We define the ramification divisor as $R(f) = \sum_p e_p(f)p$. Then we have Hurwitz formula
$$2g(C) - 2 = \deg f(2g(C') - 2) + \deg R.$$

2.2 Curves of genus 1

Now we consider the curves C of genus 1 defined over k. We always it is geometrically connected. These are smooth and projective curves carried a nowhere vanishing differential form ω_C. Thus there is no canonical way to give an embedding of C into projective space. Let $\mathrm{Div}(C)$ denote the group of divisors on C. Then there is a divisor of C with minimal positive degree e called the index of C which is also the minimal degree of number field K such that $C(K) \neq \emptyset$. Any divisor of D has degree a multiple of e. If $d = \deg D > 0$, by Riemann-Roch, we have
$$\dim \Gamma(C, D) = \deg D, \qquad \dim \Gamma(C, D - p) = d - 1.$$
Thus if $\deg D \geq 2$, we have a morphism
$$\varphi_D : C \longrightarrow \mathbb{P}^{d-1}.$$
Moreover if $\deg D \geq 3$, $\dim(C, D - p - q) = \dim D - 2$, then φ_D is an embedding.

If $e = 1$, then C has a rational point over $\mathbb{Q}$ denoted by O. The pair $E := (C, O)$ is called an elliptic curve. Then we can use $\Gamma(2O)$ to obtain a double cover $\pi : \quad C \longrightarrow \mathbb{P}^1$. We may assume that $\pi(O) = \infty$. Then we obtain an equation
$$y^2 = f(x), \qquad \deg f = 3.$$
This equation is unique up affine linear transformation. Thus we may take Weierstrass equation.
$$y^2 = x^3 + ax + b, \quad \Delta = 4a^3 + 27b^2 \neq 0$$
This equation is unique up to scaling $(x, y) \longrightarrow (u^2x, u^3y)$ with $u \in k^\times$. In this case, the numbers (a, b) is unique up to scale $(a, b) \mapsto (au^4, bu^6)$. Thus we have an invariant
$$j(C) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

For example, $y^2 = x^3 + ax$ has $j = 1728$, and $y^2 = x^3 + b$ has invariant $j = 0$. Two elliptic curves over $\mathbb{Q}$ has same j-invariant are called twists of each other. If $j \neq 0, 1728$, then are quadratic twist of each other:
$$y^2 = x^3 + ax + b, \qquad y^2 = x^3 + D^2ax + D^3b \qquad \text{or} \qquad Dy^2 = x^3 + ax + b.$$

Theorem 2.1. *Let (E, O) be an elliptic curve. Then E has an natural group structure with origin O defined by the following role: $P + Q = R$ if and only if $(P) + (Q) = (R) + (O)$.*

Proof. Define a map $E(\bar{k}) \longrightarrow \mathrm{Div}^0(E/\bar{k})/\Pr(E/\bar{k})$ by $P \mapsto (P) - (O)$. Then it is easy to see this is a bijection: if two points maps to same point, then their difference is a principle divisor. This means that there is a map $E \longrightarrow \mathbb{P}^1$ of degree 1. Contradiction. Furthermore for any divisor D of degree 0, $D + (O)$ has degree 1. By Riemann–Roch, it is equivalent to a point P. Next thing, we need to show that the group law is algebraic. This can be proved by explicit formula. □

Theorem 2.2. *Let C be a curve of genus 1. Then there is a pair (E, s) of an elliptic curve (E, O) and a morphism $s : C \times E \longrightarrow C$ which makes C a principle homogenuous space of E. Moreover the pair (E, s) is unique up to isomorphism. Moreover if D is an effective divisor on C of deg n then $T_D := \{p \in C, n(p) \sim D\}$ is an torsor over $E[n]$, and we have*

$$C = T_D \times_{E[n]} E, \qquad E = (-T_D) \times_{E[n]} C.$$

Proof. Let p be a divisor with minimal degree e on C. Define a map $\varphi : C(\bar{k}) \longrightarrow \mathrm{Cl}(C/\bar{k})$ by $x \longrightarrow e(x) - p$. It is clear that this is compatible with Galois action. The fibers of this morphism are homogenous space of the group $G := \mathrm{Cl}(C/\bar{k})[n]$. More precisely for any $x \in C(\bar{k})$ and $\in \mathrm{Cl}(C/\bar{k})[n]$, then $(x) + D$ will have degree 1 and this represented by a point y. Let k' be a finite Galois extension of k so that all divisors class in $\mathrm{Cl}(C/\bar{k})[n]$ are rational over k'. Then we have an action $G := \mathrm{Cl}(C/\bar{k})[n] \rtimes \mathrm{Gal}(k'/k)$ on $C_{k'}$ and induced an action on $k'(C)$. Let E denote algebraic curve with functional field $k'(C)^G$. Then the homomorphism φ induces an isomorphism $E(\bar{k}) \longrightarrow \mathrm{Cl}(C/\bar{k})$ compatible with $\mathrm{Gal}(\bar{k}/k)$. In particular E is an elliptic curve. Now the action of E on C can be defined by Riemann–Roch. □

The theorem shows that the pair (C, D) defines an element in $H^1(k, E[n])$ and thus showing the class of C in $H^1(k, E)[n]$. If D is changed to a point $D + p$, then its class changed to the image in $E(k)/pE(k)$. Thus (C, D) corresponds to the lifting of C in the exact sequence:

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

If $e = 2$, then C is a double of $\mathbb{P}^1$ thus is defined by an equation

$$y^2 = f(x)$$

where $\deg f = 4$ which does not have a root in $\mathbb{Q}$. This equation is unique up to Mobüs transform:

$$f(x) \longrightarrow (cx + b)^4 f\left(\frac{ax + b}{cx + d}\right), \qquad ad - bc \neq 0.$$

If $e = 3$, then C can be embedded into $\mathbb{P}^3$ and is defined by a cubic equation

$$f(x, y, z) = 0.$$

Thus equation is unique up action by $\mathrm{GL}_3(k)$.

If $e = 4$, then C can be embedded into $\mathbb{P}^4$ and is the intersection of two quadratics....

2.3 Elliptic curves over $\mathbb{C}$ or finite fields

If E is an elliptic curve over $\mathbb{C}$ then E is an complex torus of the form $\mathbb{C}/\Lambda$. More precisely let ω be a form on E. Then integration defines a lattices of in $\mathbb{C}$ of periods. Conversely, given such a lattice, then we can form a Weierstrass function

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

Then we have an embedding $\mathbb{C}/\lambda \longrightarrow \mathbb{P}^2$ by $z \mapsto (\wp(z), \wp'(z)$. The image has equation

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

where

$$g_2(\Lambda) = 60 \sum_{\lambda \neq 0} \frac{1}{\lambda^4}, \qquad g_3(\Lambda) = 140 \sum_{\lambda \neq 0} \frac{1}{\lambda^6}.$$

The moduli if elliptic curves is given by $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathscr{H}$. The j-invariant is given by

$$j = 1728 \frac{g_2^3}{g_2^3 - 27 g_3^2}$$

Genus 1 over finite field k

Let k be a finite field of q elements and let C be a curve of genus 1 over k.

Theorem 2.3. *The number of rational points on C has the following estimate:*

$$|q + 1 - \#C(k)| \leq 2\sqrt{q}.$$

In particular $C(k) \neq \emptyset$.

Proof. First let us show that $C(k) \neq \emptyset$. Let ϕ be the Frobenus map on C. Then $C(k)$ is the set of fixed points under ϕ. Let us define a morphism $C \longrightarrow E$ by $x \longrightarrow \phi(x) - x$. Then $C(k)$ is the fiber over 0. If this set is empty, then $C \longrightarrow E$ is a constant map. Thus we have $\phi(x) = x + t$ for some $t \in E(k)$. Since $E(k)$ is finite, t is torsion of some order n. It follows that ϕ^n satisfies $\phi^n(x) = x$, or equivalently, every point of C is defined over $\mathbb{F}_{q^n}$. This is impossible. □

The second part will be given later.

3 Arithmetic curves

3.1 Divisors and line bundles

Let K be a number field with ring of integers. The arithmetic curve with function field K is defined to be the union

$$C_K := \widehat{\mathrm{Spec}\mathscr{O}_K} = \mathrm{Spec}\mathscr{O}_K \coprod \{v \mid \infty\} = \{\eta\} \coprod S_K$$

where each $v \mid \infty$ denote the equivalence of archimedean norms of K, and 0 means the generic point corresponding to zero ideal. The set of closed points of K is called the set of places of K. For each place v, define its degree by

$$\deg v = \begin{cases} \log \mathrm{N}(v) & \text{if } v \nmid \infty \\ 1 & \text{if } v \text{ is real} \\ 2 & \text{if } v \text{ is complex} \end{cases}$$

where $\mathrm{N}(\wp_v) = \#\mathscr{O}_K/\wp_v$ if v is non-archimedean corresponding to a prime ideal $\wp_v$. We extend the definition of the order ord_v to real place v by $\mathrm{ord}_v(x) = \log |i_v(x)|$ if v is an archimedean place corresponding to an embedding $i_v : K \longrightarrow \mathbb{C}$. We normalize the norm by

$$|x|_v = e^{-\mathrm{ord}_v(x)\deg v} = \begin{cases} \mathrm{N}(v)^{-\mathrm{ord}_v(x)} & v \nmid \infty \\ |i_v(x)|^{\deg v} & v \mid \infty. \end{cases}$$

In this way, we have a product formula $\prod_v |x|_v = 1$ for $x \in K^\times$ or equivalently,

$$\sum_v \mathrm{ord}_v x \deg v = 0.$$

Define the group of divisors on $\widehat{\mathrm{Div}}(K))$ to be the formal finite sum

$$\oplus_{v \nmid \infty} \mathbb{Z}[v] \bigoplus \oplus_{v \mid \infty} \mathbb{R}[v].$$

We have a subgroup $\widehat{\mathrm{Pr}}(K)$ of principle divisors

$$\mathrm{div} x = \sum \mathrm{ord}_v x[v]$$

and the quotient group $\widehat{\mathrm{Cl}}(K)$. Notice that functions with zero divisors are exactly the roots of unity: those are only constant functions on $\widehat{\mathrm{Spec}\mathscr{O}_K}$ which is not an additive group.

Define a degree map by mapping $[v] \longrightarrow \deg v$. By product formula this extends to a degree map on $\widehat{\mathrm{Cl}}(K)$. Let $\widehat{\mathrm{Cl}}^0(K)$ denote the subgroup of degree 0. Then forget about archimedean place define an exact sequence:

$$0 \longrightarrow \frac{(\mathbb{R}^{r_1+r_2})_0}{\log \mathscr{O}_K^\times} \longrightarrow \widehat{\mathrm{Cl}}(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 0$$

where $(\mathbb{R}^{r_1+r_2})_0$ means the hyperplane of elements x_v such that $\sum x_v \deg v = 0$.

Line bundles

By a line bundle on an arithmetic curve C_K we mean a pair $\bar{L} = (L, \{\| \cdot \|_v, v \mid \infty\})$ of a line bundle L and a set of norms at each archimedean place. For each section ℓ, we can define the divisor $\mathrm{div}\ell$ by

$$\sum_v \mathrm{ord}_v(\ell)[v]$$

where $\mathrm{ord}_v(\ell)$ is defined such that $\pi_v^{-\mathrm{ord}_v(\ell)}\ell$ is an invertible section at $v \nmid \infty$, and $\mathrm{ord}_v(\ell)\deg v = -\log\|\ell\|$ if $v \mid \infty$. In this way we can define the Picard group $\widehat{\mathrm{Pic}}(K)$ which is isomorphic to $\widehat{\mathrm{Cl}}(K)$. We define the cohomology of L by

$$H^0(\bar{L}) = \{\ell \in L, \|\ell\|_v \leq 1\}, \qquad h^0(\bar{L}) := \log \# H^0(\bar{L}).$$

Example 3.1. For $a := (a_v) \in \mathbb{R}^{r_1+r_2}$ define the divisor $\sum a_v[v]$ and line bundle $\mathscr{O}(a) = \mathscr{O}(\sum_v a_v)$ with metic $|1|_v = e^{-a_v \deg v}$. Then $\deg \mathscr{O}(a) = \sum_v a_v$.

$$H^0(\mathscr{O}(a)) = \{x \in \mathscr{O}_K, |x|_v \leq e^{a_v}\}.$$

The decomposition $L \otimes_{\mathbb{Q}} \mathbb{R} = \oplus_{v|\infty} L \otimes K_v$ has a norm

$$\|\ell\|_\infty := \max_v(\|\ell\|_v^{1/\deg v}).$$

Let B be the unit ball in $L \otimes \mathbb{R}$ and define the Euler characteristic class of $\bar{L}$ by

$$\chi(\bar{L}) = 1 - \log\frac{2^n \mathrm{vol}(L \otimes \mathbb{R}/L)}{\mathrm{vol}(B)}$$

where the volume is computed using any Haar measure.

Theorem 3.1 (Minkowski). *If $\chi(\bar{L}) \geq 1$ then $h^0(\bar{L}) > 0$ and $\deg \bar{L} \geq 0$.*

Proof. Consider the map

$$\frac{1}{2}B \longrightarrow L \otimes \mathbb{R}/L.$$

If $\chi(\bar{L}) \geq 0$, then this can't be injective. Thus we have two points $x_1, x_2 \in \frac{1}{2}B$ maps to the same point. In other words, $x_1 - x_2 \in L$. But $x_1 - x_2 \in B$. Done! □

The genus of a number field is defined to be $g(K) = 1 - \chi(\mathscr{O}_K)$.

Proposition 3.2.

$$g(K) = \log\left(\left(\frac{2}{\pi}\right)^{r_2} D_K^{1/2}\right).$$

Proof. Let us use the standard measure on $L \otimes \mathbb{C}$ using the orthogonal norm

$$\|\ell\|_2^2 = \sum_v \|\ell\|_v^{2/e_v}.$$

Then $\mathrm{vol}(B) = 2^{r_1}\pi^{r_2}$. Let $e_1, \cdots e_n$ be a basis for $\mathscr{O}_K/\mathbb{Z}$. Write $e_i = (x_{ik})$ with respect to the decomposition $K \otimes \mathbb{R} = \mathbb{R}^{r_1} \otimes \mathbb{C}^{r_2} = \mathbb{R}^n$. Then $\mathrm{vol}(K \otimes \mathbb{R}/\mathscr{O}_K) = |\det(x_{ij})|$. The discriminant is given by

$$D_K = \det(\mathrm{tr}(e_i e_j)) = \det(\sum_{k=1}^{r_1} x_{ik}x_{jk} + \sum_{k=r_1+1}^{n} 2x_{ik}x_{jk}) = 2^{2r_2}\det X^2.$$

It follows that $\mathrm{vol}(K \otimes \mathbb{R})/\mathscr{O}_K = 2^{-r_2}|D_K|^{1/2}$. Thus

$$g(K) = \log\frac{2^{r_1+r_2}|D_K|^{1/2}}{2^{r_1}\pi^{r_2}} = \log\left(\left(\frac{2}{\pi}\right)^{r_2} D_K^{1/2}\right).$$

□

3.2 Riemann–Roch

Theorem 3.3 (Riemann–Roch). *For any line bundle $\bar{L}$ on C_K,*

$$\chi(L) = \deg L + 1 - g(K).$$

Proof. Let ℓ be a non-zero section of L then we have a morphism

$$K \otimes \mathbb{R}/\mathscr{O}_K \longrightarrow L \otimes \mathbb{R}/L.$$

With respect to the standard volume form, $\mathrm{vol}(\ell\Omega) = \prod_{v|\infty} \|\ell\|_v$, and the degree of this morphism is given by $[L : \ell\mathscr{O}_K]$. Thus we have

$$\mathrm{vol}(L \otimes \mathbb{R}/L) = \frac{\prod_{v|\infty} \|\ell\|_v}{[L : \ell\mathscr{O}_K]} \mathrm{vol}(K \otimes \mathbb{R}/\mathscr{O}_K).$$

Taking $-\log$ to obtain

$$\chi(L) - \chi(\mathscr{O}_K) = \log[L : \ell\mathscr{O}_K)] - \sum_{v|\infty} \log \|\ell\|_v.$$

Now theorem follows because $[L : \ell\mathscr{O}_K] = \prod_{v\nmid\infty} \mathrm{N}(v)^{\mathrm{ord}_v(\ell)}$. □

Theorem 3.4 (Hermite-Minkowski). *If $K \neq \mathbb{Z}$, then $g(K) > 0$. In particular $\mathbb{Q}$ is the only number field with $D_K = 1$.*

Proof. For $a := (a_v) \in \mathbb{R}^{r_1+r_2}$ define the divisor $\sum a_v[v]$ and line bundle $\mathscr{O}(a) = \mathscr{O}(\sum_v a_v)$ with metic $|1|_v = e^{-a_v \deg v}$. Then $\deg \mathscr{O}(a) = \sum_v a_v$. If $\deg \mathscr{O}(a) \leq 0$, then $\chi(\mathscr{O}(a)) < 1$. Thus $\deg \mathscr{O}(a) + \chi(\mathscr{O}_K) \leq 1$. Taking limit this gives $\chi(\mathscr{O}_K) \leq 1$ or $g(X) \geq 0$. Now assume that $\chi(\mathscr{O}_K) = 1$ and $K \neq \mathbb{Q}$. Then $r_2 = 0$ and $r_1 = n > 1$. Then for any $a \in \mathbb{R}^n$ with sum 0, then $H^0(\mathscr{O}(a)) \neq 0$. By product formula, this gives $x_a \in \mathscr{O}_K$ such that $|x_a|_v = e^{a_v}$. This is impossible since there are uncountably many a's with condition $\sum a_v = 0$. □

3.3 Applications

Theorem 3.5 (Dirichlet). *Every class in $\mathrm{Cl}(\mathscr{O}_K)$ is represented by a class with norm bounded by $e^{g(K)}$. In particular $\mathrm{Cl}(K)$ is finite.*

Proof. Let $c \in \mathrm{Cl}(K)$ and represents c^{-1} by an integral ideal I, and form a line bundle $L = (I, \|\cdot\|)$ with $\chi(L) = 1$. Then $H^0(L) \neq 0$, so there is an element $a \in I$ such that $\|a\|_v \leq 1$.

$$g(K) = \deg L = \log \#(L/a\mathscr{O}_K) - \sum_{v|\infty} \log \|a\|_v \geq \log \#(L/a\mathscr{O}_K).$$

In other words the ideal aI^{-1} has norm bounded by $e^{g(K)}$. □

Theorem 3.6. *Let $(\mathbb{R}^{r_1+r_2})_0$ be the hyperplane of infinite divisors of degree 0. Then $\log \mathscr{O}_K^\times$ is a lattice inside.*

Proof. For discretness, it is sufficiently show that 0 is not a limit point in $\log(\mathscr{O}_K^\times)$. In fact, there are only finitely many $x \in \mathscr{O}_K$ with bounded norm.

For compactness, we will prove that any infinite sequence $a_i \in (\mathbb{R}^{r_1+r_2})_0$ has a subsequence convergent modulo $\log \mathscr{O}_K^\times$. Consider the sequence $b_i := a_i + g/n = (a_{iv} + g/n \deg v)$ and corresponding bundle $\mathscr{O}(b_i)$ which has degree g. It follows that $H^0(\mathscr{O}(b_i)) \neq 0$. It follows that there exists $x_i \in \mathscr{O}_K^\times$ such that $\mathrm{div} x + b_i \geq 0$. It follows that the ideal $x_i\mathscr{O}_K$ has norm bounded by e^g. Since there are only finitely such ideals, thus replacing a_i by a subsequence, we may assume that all such ideal are equal to each other. Write $x_i = u_i x_1$ and replace a_i by $a_i + \mathrm{div} u_i$ then we have $\mathrm{div} x_1 + b_i \geq 0$ or $b_i \leq -\mathrm{div} x_1$. This last set is a compact set in $\mathbb{R}^{r_1+r_2}$. □

Theorem 3.7 (Hermite). *Let n be a positive inter and S a finite set of primes. Then the set of number field with degree bounded by n, unramified out side of S is finite.*

Proof. It suffices to prove the following two statements:

1. D_K is bounded
2. for given D_K, K has finite possibility.

For the first statement, it suffices to work locally. For $K \longrightarrow L$ a Galois extension of local field of degree n with Galois group G, let G_i the subgroup acts trivially on $\mathscr{O}_L/\wp_L^{i+1}$. Then we have

1. $\mathrm{ord}(D) = \sum_{i=0}^\infty (\#G_i - 1)$.
2. G_i/G_{i+1} is a subgroup of $\wp_L^i/\wp_L^{i+1}$.
3. $G_i = (1)$ for $i > \mathrm{ord}_K(p)/(p-1)$.

For the second statement, we take $a \in \mathbb{R}^{r_1+r_2}$ such that $\deg a = g$ and $a_i = -1$ for all $i \geq 2$. Then $H^0(\mathscr{O}_K) \neq 0$. Thus there is an element $x \in \mathscr{O}_K$ such that $|x|_{v_i} < 1$ for $i > 1$. Now consider $F = \mathbb{Q}[x]$. The minimal polynomial of x has bounded coefficients. Thus there are only finitely many such F.

It is clear that K has at most one place dividing v_1. Thus $[K : F] \leq 2$. Now it reduces to the following question: given a number field F and a finite set of primes in $\mathscr{O}_F$, there are only finitely many quadratic extension K of F unramified out off S. Recall that every quadratic extension K of F has form $K = F(\sqrt{m})$ with $m \in F^\times$ with $m \in F_v^2$ for $v \notin S$. It follows that the ideal $m\mathscr{O}_F$ has a decomposition as follows:

$$m\mathscr{O}_F = \mathfrak{a}^2 \cdot \prod_{v \in S} \wp_v^{\epsilon_v}, \qquad \epsilon_v = 0, 1$$

Since let $\mathfrak{a}_j$ represent elements in $\mathrm{Cl}(F)$, then we have a j such that $\mathfrak{a} = t^2\mathfrak{a}_j$. Thus replacing m by mt^{-2}, we may assume that

$$m\mathscr{O}_F = \mathfrak{a}_j^2 \cdot \prod_{v \in S} \wp_v^{\epsilon_v}, \qquad \epsilon_v = 0, 1.$$

This show that $m\mathscr{O}_F$ is in a finite list. In other words, m is in a finite coset of $\mathscr{O}_F^\times (F^\times)^2$. On other hand $\mathscr{O}_F^\times$ is finitely generated group, we see that m is in a finite list of coset $\mod (F^\times)^2$.

□

4 Mordell–Weil theorem

4.1 Mordell–Weil theorem

Theorem 4.1 (Mordell–Weil)**.** *Let E be an elliptic curve defined over a number field K. The $E(K)$ is finitely generated.*

This theorem follows from two statements:

Theorem 4.2 (Weak Mordell–Weil)**.** *For any positive integer $m > 1$, $E(K)/mE(K)$ is finite.*

Theorem 4.3 (Neron–Tate hight machinary)**.** *There is a function $h : E(K) \longrightarrow \mathbb{R}$ with the following properties:*

1. *h is quadratic:*
$$< x, y >:= \frac{1}{2}\left(h(x+y) - h(x) - h(y)\right)$$
is bilinear.

2. *For any H, the set of points $x \in E(K)$ with $h(x) < H$ is finite.*

It is easy to see that the height function satisfying the following properties:

1. $h(nx) = n^2h(x)$ for any $n \in \mathbb{Z}$;

2. $h(x) \geq 0$ and $h(x) = 0$ if and only if $x = 0$.

We first prove that the Weak Mordell–Weil and Neron–Tate imply Mordell–Weil. Right $|P| = h(P)^{1/2}$ as a semi-norm on $E(K)$. Let $Q_1, \cdots Q_n \in E(K)$ represent $E(K)/mE(K)$. Then for any $P \in E(K)$, we have an Q_i and $P_1 \in E(K)$ such that $P = Q_i + mP_1$. The following is an estimate of height of P_1:

$$|P_1| = \frac{1}{m}(\|P - Q_i\|) \leq \frac{1}{m}|P - Q_i| \leq |P|/m + |P_i|/m \leq |P|/m + C/m$$

where $C = \max_i |Q_i|$. We repeat the above process for P_1, then we have P_2 such that $P_1 - mP_2 \in \sum \mathbb{Z}Q_i$ such that
$$|P_2| \leq |P|/m^2 + C/m^2 + C/m.$$
Keep going we get a sequence P_i such that $P_i - mP_{i+1} \in \sum \mathbb{Z}Q_i$ such that

$$|P_i| \leq |P|/m^i + C/m + C/m^2 + \cdots + C/m^i \leq |P|/m^i + C/(1 - 1/m).$$

For i sufficiently large we can take $|P|/m^i \leq 1$. Thus we have show that $E(K)$ is generated by elements with height bounded by $1 + C/(1 - 1/m)$. Since the set of those elements is finite, $E(K)$ is finitely generated.

4.2 Weak Mordell–Weil theorem

Now let us prove the weak Mordell–Weil theorem. We consider the exact sequence:

$$0 \longrightarrow E[m](\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{\cdot m} E(\bar{K}) \longrightarrow 0.$$

Taking cohomology for the action of $\mathrm{Gal}(\bar{K}/K)$ we have

$$0 \longrightarrow E[m](K) \longrightarrow E(K) \xrightarrow{\cdot m} E(K) \xrightarrow{\partial} H^1(K, E[m]) \longrightarrow H^1(K, E) \longrightarrow H^1(K, E).$$

Here $H^1(K, E[m])$ and $H^1(K, E)$ means the first cohomology for the $\mathrm{Gal}(\bar{K}/K)$-modules $E[m](\bar{K})$ and $E(\bar{K})$.

Recall that for a group G and a $\mathbb{Z}[G]$-module M, $H^1(G, M)$ is defined to the quotient $Z^1(G, M)/B^1(G, M)$ where $Z^1(G)$ is the group of M-valued functions c on G such that

$$c(g_1g_2) = g_1c(g_2) + c(g_1)$$

and $B^1(G, M)$ is the group of functions of the form $c(g) = ga - a$ for a fixed $a \in M$. The boundary map $E(K) \longrightarrow H^1(K, E[m])$ is defined as follows: for any $P \in E(K)$, let $Q \in E(\bar{K})$ such that $P = mQ$, then

$$\partial P(g) := gQ - Q.$$

Notice that $E[m](\bar{K})$ as an abstract group is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$.

Anyway the above exact sequence define an embedding

$$E(K)/mE(K) \longrightarrow H^1(K, E[m]).$$

If we can show that $H^1(K, E[m])$ is finite, then we are done. Unfortunately, this is not true!

To improve our argument, we consider the integral model of E. From an Weistrass equation

$$y^2 = x^3 + ax + b, \qquad \Delta = 4a^3 + 27b^2 \neq 0$$

we may first clear denominate a and b so that $a, b \in \mathscr{O}_K$. Let S be the set of primes in K including factors in Δ and m and let $U = \mathrm{Spec}\mathscr{O}_K \setminus S$. The above equation defines a relative elliptic curve $\mathscr{E}$ over U. Let K_U be the maximal extension of K which is unramified over U. Then we have an exact sequence:

$$0 \longrightarrow E[m](K_U) \longrightarrow E(K_U) \xrightarrow{\cdot m} E(K_U) \longrightarrow 0.$$

Taking cohomology for the action of $G_U = \mathrm{Gal}(K_U/K)$ we have

$$0 \longrightarrow E[m](K_U) \longrightarrow E(K) \xrightarrow{\cdot m} E(K) \xrightarrow{\partial} H^1(G_U, E[m]) \longrightarrow H^1(G_U, E) \longrightarrow H^1(G_U, E).$$

Thus have an embedding

$$E(K)/mE(K) \longrightarrow H^1(G_U, E[m]).$$

Lemma 4.4. *The group $H^1(G_U, E[m])$ is finite.*

Proof. Let $L \subset K_U$ be the field generated by elements generated by coordinates of elements in $E[m]$. The have an extant sequence:

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), E[m]) \longrightarrow H^1(G_U, E[m]) \longrightarrow H^1(\mathrm{Gal}(K_U/L), E[m])^{\mathrm{Gal}(L/K)}$$

The first term is clearly finite since $\mathrm{Gal}(L/K)$ is finite. We need to prove the finiteness of the last part. It is given by $\mathrm{Hom}(\mathrm{Gal}(K_U/L), E[m])$. Since $E[m]$ is abelian killed by m, this homomorphism factors through quotient group $\mathrm{Gal}(L'/L)$, where L' is the union of all abelian Galois extension of L in K_U with degree dividing m. By Minkowski–Hermit theorem, there are only finitely many field extension of L of bounded degree and bounded ramification. Thus L' is a finite extension of L. □

5 Hermitian line bundles

5.1 Divisors, line bundles, and metrics

Let X be a normal integral scheme which is by definition to be noetherian, reduced, irreducible, and integrally closed. Let $K(X)$ be the function field of X. Let $\mathrm{Div}_W(X)$ be the group of Weil divisors which by definition are integral linear combinations $\sum n_i[Y_i]$ of integral subvariety of codimension 1. For a non-zero rational function f of X, we can define its (principle) divisor $\mathrm{div}(f) = \sum_Y \mathrm{ord}_Y(f)[Y]$. Here for each integral sub variety Y with ord_Y is the valuation of $K(X)^\times$ defined by the generic point of Y. Let $\Pr_W(X)$ be the subgroup of principle divisors. Then we have a Weil divisor class $\mathrm{Cl}_W(X) = \mathrm{Div}_W(X)/\Pr_W(X)$.

For a quasi-finite morphism $f : X \longrightarrow Y$ of integral and normal varieties, we can define the push-forward maps of Weil divisors:

$$f_*(\sum n_i[Y_i]) = \sum n_i \deg(f_i|_Y)[f(Y_i)]$$

where $\deg(f_i|_Y)$ is the degree extension $[K(Y_i) : K(f(Y_i))]$ if it is finite, otherwise, it is defined to be 0. However Weil divisor is not well behaved under pull-back morphism. For this reason, we will only consider the Cartier divisors in this section which is defined to be a section of the sheaf $K_X^\times/\mathscr{O}_X^\times$ where $K_X^\times$ is constant sheaf on X with fiber $K(X)^\times$. Thus for an affine covering $\{U_i\}$, it is represented by $f_i \in K(X)^\times = K(U_i)^\times$ such that $f_i f_j^{-1} \in \mathscr{O}(U_i \cap U_j)^\times$. We can define the group $\Pr(X)$ of principle divisors when all f_i take a same element, and define the group $\mathrm{Cl}(X)$ to the quotient

$$\mathrm{Cl}(X) = \mathrm{Div}(X)/\Pr(X).$$

There are natural morphism form Cartier divisors to Weil divisors which sends $D = \{(U_i, f_i)\}$ to $\sum_Y \mathrm{ord}_Y(D)[Y]$ where for an integral sub variety Y of X, $\mathrm{ord}_Y(D) := \mathrm{ord}_Y(f_i)$ if $Y \cap U_i \neq \emptyset$. If X is regular, two notion of divisors are identical.

The divisor group can be identified with the Picard group $\mathrm{Pic}(X)$ of X which is defined as the isomorphism classes of line bundle of X. Recall that a line bundle on X is a sheaf of invertible $\mathscr{O}_X$-modules. From a Cartier divisor D represented by (U_i, f_i), we can form the line bundle $\mathscr{O}(D)$ to be a sub-bundle of K_X generated locally by f_i^{-1} on U_i: $\mathscr{L}|_{U_i} = f_i^{-1}\mathscr{O}_{U_i}$. Conversely, from a Cartier divisor $\mathscr{L}$ and a non-zero rational section $\ell \in \mathscr{L} \otimes K_X$, we take a trivialization $\varphi_i : \mathscr{L}_{U_i} \simeq \mathscr{O}_{U_i}$ over some affine cover U_i, and then define the Cartier divisor $\mathrm{div}(\ell)$ to be represented by $(U_i, \varphi_i(\ell))$.

For example, we take $X = \mathbb{P}^n$ over $\mathrm{Spec}\mathbb{Z}$. Then X has homogeneous coordinates. For any $n \in \mathbb{Z}$, we can define the bundle $\mathscr{O}(n)$ of homogeneous function on X of degree n.

Hermitian line bundle on complex variety

By a complex variety X we mean a variety over $\mathrm{Spec}(\mathbb{C})$. The set of complex points $X(\mathbb{C})$ forms an analytic variety. By a metric $\|\cdot\|$ on a line bundle $\bar{\mathscr{L}}$ on X we mean a collection of nonzero norms $\|\cdot\| : \mathscr{L}(x) \longrightarrow \mathbb{R}$ over closed points x:

$$\|a\ell\|_x = |a|\|\ell\|_x, \qquad a \in \mathbb{C}, \ell \in \mathscr{L}(x) := \mathscr{L}/m_x\mathscr{L}.$$

We always require continuity of metric: if ℓ is a local section of $\mathscr{L}$ over an open sub variety U, then $x \mapsto \|\ell\|(x)$ is a continuous function on U. For example a metric on a trivial line bundle $\mathscr{O}_X$ is determined by the positive function $\|1\|(x)$, or the continous function $\varphi(x) = -\log\|1\|(x)$.

Conversely any continuous function $\varphi(x)$ on $X(\mathbb{C})$ define a metric on the trivial line bundle. If $\varphi(x) = 0$ then the corresponding metric is trivial.

Obviously we can form a group $\widehat{\mathrm{Pic}}(X)$ of metrized line bundles $\bar{\mathscr{L}} := (\mathscr{L}, \|\cdot\|)$ on X. The map $\bar{\mathscr{L}} \mapsto \mathscr{L}$ define an exact sequence:

$$0 \longrightarrow C^0(X) \longrightarrow \widehat{\mathrm{Pic}}(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow 0$$

where the first map sending a continuous function φ to a metrized line bundle $\mathscr{O}_X(\varphi) = (\mathscr{O}_X, \|\cdot\|_\varphi)$ where $\|1\| = e^{-\varphi}$.

For example for $\mathbb{P}^n_{\mathbb{C}}$ we can define some norms L^p-norm ($p > 0$) on $\mathscr{O}(d)$ as follows: for any homogenous function $f \in \mathbb{C}[s_0, \cdots, s_n]$ of degree d, and a point x with homogenuous coordinates $[x_0, \cdots, x_n]$,

$$\|f\|_p(x) := \frac{|f(x_0, \cdots, x_n)|}{\|(x_0, \cdots, x_n)\|_p^d}, \qquad \|(x_0, \cdots, x_n)\|_p := \sum |x_i|^p)^{1/p}.$$

Take $p \longrightarrow \infty$, we have L^∞-norm

$$\|f\|_p := \frac{|f(x_0, \cdots, x_n)|}{(\max_i |x_i|)^d}.$$

The L^2-norm is usually called Fubini-Study metric. Lets call L^∞-norm the naive norm.

5.2 Arithmetic line bundles and arithmetic divisors

By an arithmetic variety $\mathscr{X}$ over the ring $\mathscr{O}_K$ of integers in a number field K, we mean a morphism $\mathscr{X} \longrightarrow \mathrm{Spec}\mathscr{O}_K$ which is projective, flat, such that $\mathscr{X}$ is integral and normal. Let $X = \mathscr{X}_K$ the generic fiber. Then $\mathscr{X}$ is called an integral model of X. Notice that there is a bijection $X(K)$ and $\mathscr{X}(\mathscr{O}_K)$ by taking Zariski closure. For each complex embedding $\sigma : K \longrightarrow \mathbb{C}$, we have a complex analytic variety $X_\sigma(\mathbb{C})$ over $\mathbb{C}$. The complex conjugation $\mathrm{Frob}_\infty \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ takes one complex embedding σ to another one $\bar{\sigma}$, and induces a bijection $X_\sigma(\mathbb{C}) \longrightarrow X_{\bar{\sigma}}(\mathbb{C})$.

By a hermitian metric on a line bundle $\mathscr{L}$ on $\mathscr{X}$ we mean a collection $\|\cdot\|_\sigma$ invariant under complex conjugation under $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. We denote $\bar{\mathscr{L}} = (\mathscr{L}, \|\cdot\|)$. We let $\widehat{\mathrm{Pic}}(\mathscr{X})$ denote the group of isomorphism class of hermitian line bundles on $\mathscr{X}$. Then we have an exact sequence

$$0 \longrightarrow \widehat{\mathrm{Pic}}(\mathscr{X})_\infty \longrightarrow \widehat{\mathrm{Pic}}(\mathscr{X}) \longrightarrow \mathrm{Pic}(\mathscr{X}) \longrightarrow 0.$$

where $\widehat{\mathrm{Pic}}(\mathscr{X})_\infty$ is the hermitian line bundle which are trivial at $\mathscr{X}$. Thus these bundle has an invertible section ℓ. Its norms define invertible positive consitnous function on $X(\mathbb{C})$ which is invariant under the complex conjugation. Thus $-\log\|\ell\|$ is a continous function. Two different section is differed by a unit $u \in \mathscr{O}_K$ which changes $-\log\|\ell\|$ by a function $-\log|u|$. Thus we have proved that

$$\widehat{\mathrm{Pic}}(\mathscr{X})_\infty \simeq \frac{C(X(\mathbb{C}))^{\mathrm{Frob}_\infty}}{\log|\mathscr{O}_K^\times|}.$$

$$0 \longrightarrow \widehat{\mathrm{Pic}}(\mathscr{X})_{vert} \longrightarrow \widehat{\mathrm{Pic}}(\mathscr{X}) \longrightarrow \mathrm{Pic}(X) \longrightarrow 0.$$

where $\widehat{\mathrm{Pic}}(\mathscr{X})_{vert}$ is the subgroup of bundles which is trivial at the generated fiber. Thus there is a rational section ℓ which is trivial at the generated fiber. The divisor ℓ define a vertical divisor $\mathrm{div}(\ell)$.

Two different section differed by an element $u \in K^{\times}$. Thus we have the following isomorphism:

$$\widehat{\mathrm{Pic}}(\mathscr{X})_{vert} \simeq \frac{C(X(\mathbb{C}))^{\mathrm{Frob}_\infty} \oplus \mathrm{Div}(\mathscr{X})_{vert}}{\mathrm{div}(K^{\times})}.$$

Notation:

$$\widehat{\mathrm{Div}}(\mathscr{X})_\infty := \widehat{C}(X(\mathbb{C}))^{\mathrm{Frob}_\infty}, \qquad \widehat{\mathrm{Div}}(\mathscr{X})_{vert} = \widehat{\mathrm{Div}}(\mathscr{X})_\infty \oplus \mathrm{Div}(\mathscr{X})_{vert}.$$

5.3 Heights

Let $\mathscr{X}/\mathscr{O}_K$ be an arithmetic variety over number field K and let $\bar{\mathscr{L}}$ be a hermitian line bundle on X. Then for each $x \in X(K)$ we have a section $\bar{x} \in \mathscr{X}(\mathscr{O}_K)$ and a hermitian line bundle $\bar{x}^*\bar{\mathscr{L}}$ on $\mathrm{Spec}\mathscr{O}_K$. We can define the degree and height

$$\deg x^*\bar{\mathscr{L}} = \log[x^*\bar{\mathscr{L}} : \ell\mathscr{O}_K] - \sum_{\sigma:K\longrightarrow\mathbb{C}} \log\|\ell\|_\sigma(x),$$

$$h_{\bar{L}}(x) = \frac{1}{[K(x):K]}\deg \bar{x}^*\bar{\mathscr{L}},$$

where ℓ is a section of $\mathscr{L}$ non-vanishing at x.

The first property is that the height does not change under base change.

Heights on projective space

For example, $\mathscr{X} = \mathbb{P}^n$ over $\mathrm{Spec}\mathbb{Z}$, take $\bar{\mathscr{L}} = (\mathscr{O}(1), \|\cdot\|_2)$ with coordinate function s_i. Let $x = (x_0, \cdots, x_n)$ be a point on X with $x_i \in K$. Then $\bar{x}^*\mathscr{O}(1)$ is the space of linear functions at x:

$$x^*\mathscr{O}(1) = \sum \mathscr{O}_K s_i, \qquad [s_0, \cdots, s_n] = [x_0, \cdots, x_n].$$

For any $s = \sum a_i s_i \in x^*\mathscr{O}(1)$ with norm

$$\|s\|_\sigma = \frac{|\sigma(\sum a_i x_i)|}{(\sum |\sigma(x_i)|^p)^{1/p}}.$$

Thus

$$\begin{aligned} x^*\mathscr{O}(1) =& \log[\sum \mathscr{O}_K s_i(x) : \mathscr{O}_K s(x)] - \sum_{\sigma:K\longrightarrow\mathbb{C}} \log\|s\|_\sigma \\ =& \log\frac{[\sum \mathscr{O}_K x_i : \mathscr{O}_K \sum a_i x_i]}{\mathrm{N}(\sum a_i x_i)} + \sum_\sigma \log\|x\|_\sigma \\ =& -\log \mathrm{N}(\sum \mathscr{O}_K x_i) + \sum_\sigma \log\|x\|_\sigma \end{aligned}$$

Thus we have a formula for the height:

$$\begin{aligned} h_{\bar{\mathscr{O}}(1)}(x) &= -\frac{1}{[K:\mathbb{Q}]}\log \mathrm{N}(\sum \mathscr{O}_K x_i) + \frac{1}{[K:\mathbb{Q}]}\sum_\sigma \log\|x\|_\sigma \\ &= \frac{1}{[K:\mathbb{Q}]}\log\frac{\prod_\sigma \|x\|_\sigma}{\mathrm{N}(\sum \mathscr{O}_K x_i)}. \end{aligned}$$

We can also write this in a much symmetric way using the fact:

$$\log \mathrm{N}(\sum \mathscr{O}_K x_i) = -\sum_{v<\infty} \log \max(|x_0|_v, \cdots, |x_n|_v).$$

Then

$$h(x) = \frac{1}{[K:\mathbb{Q}]}\sum_v \log \max(|x_0|_v, \cdots, |x_n|_v).$$

Take example $K = \mathbb{Q}$, and that $x = [x_0, \cdots, x_n]$ with $x_i \in \mathbb{Z}$ without common divisor. Then $\sum \mathbb{Z}x_i = \mathbb{Z}$, and then

$$h(x) = \log \|x\|.$$

Heights of generically trivial line bundles

Let $\bar{\mathscr{L}}$ be a hermitian line bundle with trivial generic fiber $\mathscr{L}_X \simeq \mathscr{O}_X$. Thus we can consider $\bar{\mathscr{L}}$ as a sub sheaf of K_X. There is a positive number m such that

$$m\mathscr{O}_X \subset \mathscr{L} \subset m^{-1}\mathscr{O}_X.$$

Also we have $c > 1$ such that for any $\sigma : K \longrightarrow \mathbb{C}$,

$$\frac{1}{c} \le \|1\|_\sigma \le c.$$

It follows that the height of $\bar{\mathscr{L}}$ is bounded. It also implies that the height function up to a bounded function does not depend on the model of (X, L). Thus we have a map

$$\mathrm{Pic}(X) \longrightarrow \{\text{real value functions on } X(\bar{K})\}/\{\text{Bounded functions}\}.$$

6 Heights without hermitian line bundles

In the following we study heights on projective spaces without using hermitian line bundles. We start with definitions. For each $p \le \infty$, let $\mathbb{C}_p$ denote the completion of $\bar{\mathbb{Q}}_p$ with a norm normalized such that $|p|_p = \frac{1}{p}$ if $p < \infty$ and the usual complex norm if $p = \infty$. For any $x \in \mathbb{C}_p^m$, let $\|x\|_p = \max |x_i|_p$ be the L^∞-norm. For any $x = (x_i) \in \mathbb{P}^n(\bar{\mathbb{Q}})$ which is rational over a field L, we define

$$h(x) := \frac{1}{[L:\mathbb{Q}]}\sum_p \sum_{\sigma:K\longrightarrow\bar{\mathbb{Q}}_p} \log \|\sigma x\|_p.$$

Using product formula, it is easy to see that this definition does not depend not the choice of homogeneous coordinates, and on the choice of L.

Here are some basic properties of heights:

1. If taking x with one coordinate equal to 1, we have $h(x) \ge 0$.
2. Raising power d gives:
$$h(x^d) = dh(x).$$
3. If x has coordinates 0 or roots of unity then $h(x) = 0$.
4. If $x \in \mathbb{P}^n(\mathbb{Q})$ represented by a homogeneous integral coordinates $[x_0, \cdots, x_n]$ without common divisor > 1, then
$$h(x) = \log \max |x_i|.$$

6.1 Behavior under morphisms

Theorem 6.1. *Let $\phi : \mathbb{P}^m \longrightarrow \mathbb{P}^n$ be a rational morphism over a number field K defined by homogeneous polynomial of degree d, Then for any $x \in \mathbb{P}^m$ at which ϕ is well-defined,*

$$h(\phi(x)) \leq dh(x) + O(1).$$

Moreover if $m = n$ and ϕ is an endomorphism $\phi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$, then

$$h(\phi(x)) = \deg \phi \cdot h(x) + O(1), \qquad x \in \mathbb{P}^n(\bar{K}).$$

Proof. For a place p, and a homogeneous polynomial $f \in \mathbb{C}_p[x_0, x_1, \cdots, x_m]$ in $\mathbb{C}_p$, let $\|f\|_p$ denote the maximum (reps. sum) of absolute values of coefficients of f if $p \neq \infty$ (reps. if $p = \infty$). Then for any $x \in \mathbb{C}_p^{m+1}$,

$$|f(x)|_p \leq \|f\|_p \cdot \|x\|_p^d.$$

For $f = (f_0, f_1, \cdots, f_n)$ of $n+1$-tuples of homogeneous polynomials of same degree d, define $\|f\|_p = \max \|f_i\|_p$. Then consider f as a map $\mathbb{C}_p^{m+1} \longrightarrow \mathbb{C}_p^{n+1}$, we have

$$\|f(x)\|_p \leq \max_i |f_i(x)|_p \leq \max_i (\|f_i\|_p \|x\|^d) = \|f\|_p \|x\|_p^d.$$

Write $\phi(x) = (\phi_0(x), \cdots, \phi_n(x))$ in homogeneous coordinates of degree d in coefficients in K. For each emebdding $\sigma : K \longrightarrow \mathbb{C}_p$, we have

$$\|\sigma(\phi(x))\|_p \leq \|\sigma(\phi)\|_p \leq \|\sigma\phi\|_p \cdot \|\sigma x\|^d.$$

From this, we have

$$\begin{aligned}
h(\phi(x)) =& \frac{1}{[L:\mathbb{Q}]} \sum_p \sum_{\sigma : L \longrightarrow \bar{\mathbb{Q}}_p} \log \|\sigma\phi(x)\|_p \\
\leq& \frac{1}{[L:\mathbb{Q}]} \sum_p \sum_{\sigma : L \longrightarrow \bar{\mathbb{Q}}_p} \log \|\sigma\phi\|_p \cdot \|x\|_p^d \\
\leq& \frac{1}{[L:\mathbb{Q}]} \sum_p \sum_{\sigma : L \longrightarrow \bar{\mathbb{Q}}_p} (\log \|\sigma\phi\|_p + d \log \|x\|_p) \\
=& dh(x) + h(\phi)
\end{aligned}$$

where

$$h(\phi) = \frac{1}{[K:\mathbb{Q}]} \sum_p \sum_{\sigma : K \longrightarrow \bar{\mathbb{Q}}_p} \log \|\sigma\phi\|_p.$$

Notice the above sum has finitely many non-zero terms.

The condition that ϕ is well-defined is equivalent to that ϕ_i has no-common zero on $\mathbb{P}^n$. Thus the ideal I of $S := K[x_0, \cdots, x_n]$ generated by $\phi_0, \cdots, \phi_n$ has only zero $(0, \cdots, 0)$. By Hilbert's Nullstellensatz, the radical idea $\sqrt{I}$ is equal to $\sum x_i S$. Thus for some $N > 0$, x^N is a linear combinations of ϕ_i: there are homogeneous polynomials f_{ij} of degree $N - d$ such that

$$x_i^N = \sum f_{ij} \phi_j$$

It follows that for each $\sigma : L \longrightarrow \mathbb{C}_p$:

$$\begin{aligned} \|\sigma x^N\|_p &\le \max_i(\|\sigma f_i(x)\|_p |\sigma \phi_j(x)|_p) \\ &\le \max_i(\|\sigma f_i\|_p)\|\sigma x\|_p^{N-d}\|\sigma\phi_j(x)\|_p) \end{aligned}$$

where $f_i(x)$ means the vector $(f_{ij}(x))$. Let $\|\sigma f\|_p = \max_j \|\sigma f_{ij}\|_p$, we have

$$\|\sigma x\|^d \le \|\sigma f\|_p \cdot \|\sigma\phi_j(x)\|_p.$$

Put this in the definition of heights we have

$$dh(x) \le h(\phi(x)) + h(f)$$

where

$$h(f) = \frac{1}{[K:\mathbb{Q}]}\sum_p \sum_{\sigma:K\longrightarrow\mathbb{C}_p} \log \|f\|_p.$$

Thus we have shown

$$|h(\phi(x)) - dh(x)| \le \max(h(\phi), h(f)).$$

□

Define a map $S : \quad (\mathbb{P}^1)^n \longrightarrow \mathbb{P}^n$ using elementary symmetric polynomials. In other wolds if P_i has homogeneus coordinates $[a_i, b_i]$ then $\Pi(P_1, \cdots, P_n)$ has coordinates $[f_0, \cdots, f_n]$ such that

$$\prod_i (a_i x + b_i y) = \sum_{i=0}^n f_i x^i y^{n-i}.$$

This map identifies $\mathbb{P}^n$ as symmetric quotient of $(\mathbb{P}^1)^n$, or in other words $\mathrm{Div}^n(\mathbb{P}^1)$.

Theorem 6.2. *For $(P_1, \cdots, P_n) \in \mathbb{P}^1(\bar{\mathbb{Q}})^n$,*

$$\sum_i h(P_i) = h(S(P_1, \cdots, P_n)) + O(1).$$

Proof. We need to compare the local norms for $v_i := (a_i, b_i) \in \mathbb{C}_p^2$ and $f := (f_0, \cdots, f_n)$: by Gauss lemma for $p \neq \infty$,

$$\prod \|v_i\|_p = \|f\|_p$$

and for $p = \infty$ using compactness, we have positive constants $c > 1$:

$$c^{-1} \le \frac{\prod \|v_i\|_\infty}{\|f\|_\infty} \le c.$$

It follows that

$$|\sum_i h(P_i) - h(S(P_1, \cdots, P_n))| \le \log c.$$

□

6.2 Nothcott property

Theorem 6.3 (Northcott)**.** *For any two numbers D, H the set*

$$S(D,H) := \{x \in \mathbb{P}^n(\bar{\mathbb{Q}}) : \qquad \deg x \le D, \quad h(x) \le H\}$$

is finite.

Proof. It is clear that the Theorem is true in case $d = 1$.

Take $x \in S(D,H)$ and let $y_1, \cdots y_n \in \mathbb{P}^1$ such that $S(y_1, \cdots y_n) = x$. Then $\deg y_i \le \deg x n!$ and $h(y_i) \le h(x) + C(n)$ with $C(n)$ a constant. Thus we reduce to the case $n = 1$.

Assume that $n = 1$, and let $x = x_1, \cdots x_d$ be conjugates of x. Then $S(x_1, \cdots x_d) \in \mathbb{P}^n(\mathbb{Q})$. Thus we are reduced to the case where $d = 1$. □

Theorem 6.4. *Let $\phi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ be an endomorphism of degree $d^n > 1$ defined over a number field K. Then there is a unique height function:*

$$h_\phi : \mathbb{P}^n(\bar{K}) \longrightarrow \mathbb{R}$$

with the following properties:

$$h_\phi(x) = h(x) + O(1), \qquad h_\phi(\phi(x)) = dh_\phi(x).$$

Moreover for such a height function: $h_\phi(x) \ge 0$ and $h_\phi(x) = 0$ if and only if x has finite orbit under iteration of ϕ.

Proof. For the existence, from above theorem, define a constant:

$$C = \sup_{x \in \mathbb{P}^n(\bar{K})} |\frac{1}{d} h(\phi(x)) - h(x)|.$$

For any $m \ge 0$, define

$$h_m(x) = \frac{1}{d^m} h(\phi^m(x)).$$

Then for any $m_1 \ge m_2$ we have

$$\begin{aligned} |h_{m_1}(x) - h_{m_2}(x)| =& |\sum_{i=m_2+1}^{m_1} (h_i(x) - h_{i-1}(x)| \\ \le& \sum_{i=m_2}^{m_1-1} |h_{i+1}(x) - h_i(x)| \\ \le& \sum_{i=m_2+1}^{m_1} \frac{C}{d^i} \le \frac{C}{d^{m_2}(1-1/d)}. \end{aligned}$$

This shows that the sequence $h_m(x)$ is a Cauchy sequence with a limit $h_\phi(x)$ whose difference with $h(x) = h_0(x)$ is bounded.

For uniqueness, we notice that difference of two such a function is a bounded function f on $\mathbb{P}^n(\bar{K})$ such that $f(\phi(x)) = df(x)$. Taking maximal value D of $|f(x)|$ which is also the maximal of $f(\phi(x))$ since ϕ is surjective. Thus $D = dD$. Then $D = 0$.

The non-nagativity follows from the non-nagativity of h_m. If $h(x) = 0$, then so all elements $h(\phi^i(x))$. By Northcott, x has a finite orbit under ϕ. Conversely, if x has finite orbit, then there are $\ell \ne m$ such that $\phi^\ell(x) = \phi^m(x)$. They heights satisfy $d^\ell h_\phi(x) = d^m h_\phi(x)$. Thus $h_\phi(x) = 0$. □

6.3 Neron–Tate height on elliptic curves

Let E be an elliptic curve defined over a number field K. Then E is defined by a Weistrass equation

$$y^2 = x^3 + ax + b.$$

We have a morphism $\pi : E \longrightarrow \mathbb{P}^1$ by taking x coordinates. We define the naive height on $E(\bar{K})$ by its height of x:

$$h(P) := h(\pi(P)).$$

Notice that the morphism π identify $\mathbb{P}^1$ with $E/\pm 1$.

Theorem 6.5. *For $P, Q \in E(\bar{K})$,*

$$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1).$$

Proof. First we notice as a function of $(P, Q) \in E \times E$, both sides are invariant under the group $G := \{\pm 1\}^2 \times S_2$, where S_2 is the symmetric group switching two factors. Thus both sides can be expressed in terms of the quotient variety $(E \times E)/G$. It is given by $(\mathbb{P}^1)^2/S_2$ which is isomorphic to $\mathbb{P}^2$. Let $f : E \times E \longrightarrow \mathbb{P}^2$ be the composition of the map. By Theorem 6.2:

$$h(f(P, Q)) = h(P) + h(Q) + O(1).$$

Thus we are reduced to the following problem:

$$h(f(P+Q, P-Q)) = 2h(f(P, Q)) + O(1).$$

Consider the morphism $\psi : E \times E \longrightarrow E \times E$ such that $\psi(P, Q) = (P+Q, P-Q)$. Then the above equation is given by

$$h(f\psi(P, Q)) = 2h(f(P, Q)) + O(1).$$

This morphism commutes with action of G and thus inducing a morphism ϕ on $\mathbb{P}^2$:

$$\phi \circ f = f \circ \psi.$$

Thus we need only show the following:

$$h(\phi(x)) = 2h(x) + O(1).$$

By previous theorem, it suffices to show $\deg \phi = 4$. In fact we have

$$\deg \phi \cdot \deg f = \deg f \deg \psi.$$

It follows that $\deg \phi = \deg \psi$ which has degree 4:

$$\psi(P, Q) = \psi(P', Q') \iff P - P' = Q - Q' \in E[2].$$

□

Notice that the multiplication by 2 commutes with quotient morphism $\pi : E \longrightarrow \mathbb{P}^1$ and thus defines a morphism $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ of degree 2.

Theorem 6.6. *Let $\widehat{h} : E(\bar{K}) \longrightarrow \mathbb{R}$ be the canonical height defined by $\widehat{h}(P) = h_\phi(\pi(P))$. Then we have the following properties:*

1. *$\widehat{h}$ is quadratic in the sense that*

$$\langle x, y\rangle := \frac{1}{2}\left(\widehat{h}(x+y) - \widehat{h}(x) - \widehat{h}(y)\right)$$

is bilinear in x and y;

2. *$\widehat{h}(x)$ is non-negative and vanishing exactly at torsion points.*

3. *$\widehat{h}(x)$ satisfies the Northcott propery: for any $D > 0$, $H > 0$ the set*

$$\{x \in E(\bar{K}) : \qquad \deg x \leq D, \quad \widehat{h}(x) \leq H\}$$

is finite.

Proof. The last two properties are already proved Theorem 6.3 and 6.4. The first property is equivalent to the following cubic relation of heights:

$$\widehat{h}(x+y+z) - \widehat{h}(x+y) - \widehat{h}(y+z) - \widehat{h}(z+x) + \widehat{h}(x) + \widehat{h}(y) + \widehat{h}(z) = 0.$$

From the definition of $\widehat{h}(x)$ it is suffices to show

$$h(x+y+z) - h(x+y) - h(y+z) - h(z+x) + h(x) + h(y) + h(z) = O(1).$$

This follows from Theorem 6.5 applying to the following situations with

$$(P+R, Q), \quad (P, R-Q), \quad (P+Q.R), \quad (R, Q).$$

□

7 Birch and Swinnerton-Dyer conjectures

7.1 Tate–Shafarevich groups

Let E be an elliptic curve defined over a number field K. We have proved that $E(K)$ is finitely generated. Recall that as a first step, we have proved a weak Mordell–Mordell theorem. Consider the exact sequence

$$0 \longrightarrow E_{\mathrm{tor}}(\bar{K}) \longrightarrow E(\bar{F}) \longrightarrow E(\bar{F}) \otimes \mathbb{Q} \longrightarrow 0.$$

Taking cohomology, we have a Kumar sequence:

$$0 \longrightarrow E(F) \otimes \mathbb{Q}/\mathbb{Z} \longrightarrow H^1(K, E_{\mathrm{tor}}) \longrightarrow H^1(K, E) \longrightarrow 0.$$

Recall that the Tate –Shafarevich group Ш is defined by the exact sequence:

$$0 \longrightarrow Ш(E) \longrightarrow H^1(K, E) \longrightarrow \prod_v H^1(K_v, A).$$

Pulling back by this sequence defines an exact sequence

$$0 \longrightarrow E(F) \otimes \mathbb{Q}/\mathbb{Z} \longrightarrow \mathbb{S}(E) \longrightarrow \text{Ш}(E) \longrightarrow 0.$$

Here $\mathbb{S}(E)$ is the reduced Selmer group: $\mathbb{S}(E) = \mathrm{Sel}(E)/E(K)_{\mathrm{tor}}$. The Weak Mordell–Weil theorem is proved basically by showing that $\mathbb{S}(E)[m]$ is finite for any $m > 1$.

Notice that $\text{Ш}(E)$ measures the failure of the local and global principle. The first part of BSD is as follows:

Conjecture 7.1 (BSD1)**.**

$$\#\text{Ш}(E) < \infty.$$

If $E(F)$ has rank r, then $E(F) \otimes \mathbb{Q}/\mathbb{Z} \simeq (\mathbb{Z}/\mathbb{Z})^r$. The conjecture implies that

$$\mathbb{S}(E) \simeq (\mathbb{Q}/\mathbb{Z})^r \oplus \text{Ш}(E).$$

7.2 L-functions

Then E can be extended into a scheme $\mathscr{E}$ over $\mathrm{Spec}\mathscr{O}_K$ with minimal discriminant ideal Δ of $\mathscr{O}_K$. Locally at a finite place v of K, $\mathscr{E}$ is given by a Weiestrass equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with minimal discriminant Δ_v ideal of $\mathscr{O}_v := \mathscr{O}_{K_v}$, see Tate, *The arithmetic of elliptic curves*, Invent Math. 23, 179-206 (1974). Let q_v denote the cardinality of residue field k_v of v and let define

$$a_v := q_v + 1 - \#\mathscr{E}(k_v).$$

It is known by Hasse that $|a_v| \leq 2\sqrt{q_v}$. If $\mathrm{ord}_v(\Delta) > 0$, then $a_v = 1, -1, 0$ depending on the type of bad reduction: nodal with rational tangents, nodal with irrational tangents, or cuspidal. Finally we define L-function by Euler product:

$$L(E,s) = \prod_v L_v(E,s) = \prod_{v|\Delta}(1 - a_v q_v^{-s})^{-1} \cdot \prod_{v\nmid\Delta}(1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}.$$

By Hasse's estimate, this L-series is absolutely convergent for $\mathrm{Re}(s) > 3/2$. Define the complete L-function

$$\Lambda(E,s) = (2\pi^{-s}\Gamma(s))^d L(E,s)$$

Then it is conjectured that $\Lambda(E,s)$ has a holomorphic continuation to whole complex plane and satisfies a functional equation

$$\Lambda(E,s) = \epsilon(E) N_E^{1-s} \Lambda(E, 2-s)$$

where N_E is the conductor of E and $\epsilon(E) = \pm 1$ is the root number.

Alternatively, $L(E,s)$ can be defined using Tate module as follows. Fix a prime ℓ and define $\mathrm{T}_\ell(E) = \varprojlim_n E[\ell^n]$, and $\mathrm{V}_\ell(E) = \mathrm{T}_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. For v a finite place of K and embedding $K \longrightarrow K_v \subset \mathrm{Gal}(\bar{K}/K)$, we have an embedding $\mathrm{Gal}(\bar{K}_v/K_v)$. Let I_v denote the inertia group defined by

$$1 \longrightarrow I_v \longrightarrow \mathrm{Gal}(\bar{K}_v/K_v) \longrightarrow \mathrm{Gal}(\bar{k}_v/k_v) \longrightarrow 1.$$

Then if $v \nmid \ell$, then the polynomial

$$P_v(T) := \det(1 - \mathrm{Frob}_v T | \mathrm{V}_\ell^{I_v}) \in \mathbb{Z}_\ell[T]$$

actually takes values in $\mathbb{Z}$, and we have

$$L_v(E, s) = \frac{1}{P_v(q_v^{-s})}.$$

By local Lanlgnds correspondence, each local representation $\mathrm{Gal}(\bar{K}_v/K_v)$ corresponds to representation π_v of $\mathrm{GL}_2(K_v)$. For example, if $\mathscr{E}$ has good reduction at v, then π_v is a principle series induced by two unramified characters χ_1 and χ_2 of $K_v^\times$ such that

$$P(T) = (1 - a_v T + q_v T^2) = (1 - \chi_1(\varpi_v)T)(1 - \chi_2(\varpi_v)T).$$

In this way, we can form a global representation $\pi = \otimes_v \pi_v$ of $\mathrm{GL}_2(\mathbb{A}_K)$.

Conjecture 7.2. *The representation π of $\mathrm{GL}_2(\mathbb{A}_K)$ is automorphic and cuspidal.*

Notice that the central character is given by $x \longrightarrow |x|$.

The second part of BSD is as follows:

Conjecture 7.3. *(BSD2)*

$$\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank} E(K).$$

Let $r = \mathrm{rank} E(K)$ and write $E(K) = \sum_{i=1}^r \mathbb{Z}P_i \oplus E(K)_{\mathrm{tor}}$ and define

$$R(E) := \frac{\det(\langle P_i, P_j \rangle)}{\# E(K)_{\mathrm{tor}}^2}.$$

Here the height pairing is using base K, i.e., $\deg K$ times the absolute height paring. Let ω be a non-zero invariant differential form on E. Let $dx = \otimes dx_v$ be a normalized measure on $\mathbb{A}_K$ such that $\mathrm{vol}(K \backslash \mathbb{A}_K) = 1$. In this way, there is a measure $|\omega|_v$ on $E(K_v)$ for each place v: locally at each point $P \in E(K_v)$ with local coordinates x_v, $\omega = f(x_v)dx_v$, $|\omega|_v = |f(x_v)|_v dx_v$. We define

$$c_v(\omega) = \begin{cases} \int_{E(K_v)} |\omega|_v & v \mid \infty \\ L_v(E, 1) \int_{E(K_v)} |\omega|_v & v \nmid \infty \end{cases}$$

If v is a finite place such that $\mathscr{E}$ has good reduction at v, and that $\mathrm{vol}(\mathscr{O}_v) = 1$, and that ω is invertible on $\mathscr{E}_v$, then $c_v(\omega) = 1$. Write $c(E) = \prod c_v(\omega)$. Then third part of BSD is

Conjecture 7.4. *(BSD3)*

$$\lim_{s \longrightarrow 1} L(E, s)(s-1)^r = c(E) \cdot R(E) \cdot \#Ш(E).$$

7.3 Geometric analog

Let k be a finite field of q elements, and B a smooth and projective curve over k with function field K. Let E be an elliptic curve defined over k. Then BSD makes sense here. In fact, the modularity of $L(E,s)$ is already known due to Drinfeld. In this case we have the following

Theorem 7.5. *(Tate, Milne).*

$$(BSD1) \equiv (BSD2) \Longrightarrow (BSD3).$$

In the following we want to explain its relation with Tate's conjecture on divisors on the minimal regular model $\mathscr{E}$ of E. Let $\mathrm{NS}(\mathscr{E})$ be the Neron-Severi group. Then for each prime ℓ we have a morphism

$$\mathrm{NS}(X) \otimes \mathbb{Z}_\ell \longrightarrow H^2(\bar{X}, \mathbb{Z}_\ell(1))^{\mathrm{Gal}(\bar{k}/k)}.$$

Conjecture 7.6 ((Tate))**.** *The above morphism is bijective.*

Theorem 7.7. *(BSD2) is equivalent to (Tate).*

Proof. The main idea is to repress $L(E,s)$ using cohomology of $\mathscr{E}$. Recall that for a variety X over a finite field $\mathbb{F}_q$, the zeta function of X is defined as

$$\zeta(X,s) = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

This function is always a rational function. In fact, if X is projective and smooth of dimension d, then

$$\zeta(X,s) = \frac{P_1(X,q^{-s})P_3(X,q^{-s}) \cdots P_{2d-1}(X,q^{-s})}{P_0(q^{-s})P_2(X,q^{-s}) \cdots P_{2d}(X,q^{-s})}$$

where $P_i(X,T) = \det(1 - T\mathrm{Frob}_q | H^i(\bar{X}, \mathbb{Q}_\ell))$ and $\bar{X} = X \otimes \bar{\mathbb{F}}_q$. Moreover by hard Lefshetz or Poincare duality,

$$P_{2d-i}(T) = P_i(q^{d-i}T),$$

and by RH, the reciprocity roots of P_i all have absolute value $q^{i/2}$.

Using ζ function, we can write local L-function at each closed point $v \in B$ as

$$P_v(q_v^{-s}) = \zeta(\mathscr{E}_v, s) \cdot (1 - q_v^{-s})(1 - q_v^{1-s})^{m_v}$$

where m_v is the number of irreducible components in $\mathscr{E}_v$. Taking product over v we have

$$L(\mathscr{E}, s) = \frac{\zeta(B,s)\zeta(B,s-1)}{\zeta(\mathscr{E},s)} \prod_{v \in B^0} (1 - q_v^{1-s})^{1-m_v}.$$

Recall that the zeta function of $\mathscr{E}$ and B have decompositions:

$$\zeta(\mathscr{E},s) = \frac{P_1(\mathscr{E},q^{-s})P_1(\mathscr{E},q^{1-s})}{(1-q^{-s})P_2(\mathscr{E},q^{-s})(1-q^{2-s})}, \qquad \zeta(B,s) = \frac{P_1(B,q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

Thus we have an expression of $L(\mathscr{E}, s)$ as follows:

$$L(E,s) = P_2(\mathscr{E},q^{-s})(1-q^{1-s})^{-2} \prod_{v \in B^0} (1 - q_v^{1-s})^{1-m_v} \cdot \frac{P_1(B,q^{-s})P_1(B,q^{1-s})}{P_1(\mathscr{E},q^{-s})P_1(\mathscr{E},q^{1-s})}.$$

This identity shows that

$$\mathrm{ord}_{s=1}L(E,s) = \mathrm{ord}_{s=1}P_2(\mathscr{E}, q^{-s}) - 2 - \sum(m_v - 1).$$

Let $\mathrm{NS}(\mathscr{E})$ denote the Neron group of divisors on $\mathscr{E}$. Consider the following filtration:

$$\pi^*\mathrm{NS}(B) \subset \mathrm{NS}(\mathscr{E})^{00} \subset \mathrm{NS}(\mathscr{E})^0 \subset \mathrm{NS}(\mathscr{E})$$

where $\mathrm{NS}(\mathscr{E})^{00}$ is the subgroup of elements supported on fibers, $\mathrm{NS}(\mathscr{E})^0$ is the subgroup which has degree 0 at the generic fiber. Then we have an exact sequence

$$0 \longrightarrow \mathrm{NS}(\mathscr{E})^{00} \longrightarrow \mathrm{NS}(\mathscr{E})^0 \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0.$$

Because $\mathrm{NS}(B)$ has rank 1 and $\mathrm{NS}(\mathscr{E})^0$ has corank 1, this shows that

$$\mathrm{rank}\mathrm{NS}(\mathscr{E}) = \mathrm{rank}E(K) + 2 + \sum_v (m_v - 1).$$

In this way, we shown that

$$\mathrm{ord}_{s=1}L(E,s) - \mathrm{rank}E(K) = \mathrm{ord}_{s=1}P_2(q^{-s}) - \mathrm{rank}\mathrm{NS}(\mathscr{E}).$$

□

8 Constant elliptic curves: finiteness of Ш

Let k be a finite field with q elements. Let B be a smooth and projective curve over k which is geometrically connected with function field K. By a constant variety over K, we mean a variety of the form $X_K = X \otimes_k K$ where X is a variety over k. The variety X is called the fiber of X. If X is projective, then X_K is projective, and the set of $X_K(K)$ of rational points over K is identical to the space of maps $B \longrightarrow X$; and set of points $X_K(\bar{K})$ is identical to horizontal curves C in $B \times_k X$. In this section, we want to discuses the finiteness of $Ш(E_K)$ for a constant elliptic curve E_K after some concrete descriptions of the Mordell–Weil group $E(K)$ and the Selmer group $\mathbb{S}(E_K)$ in the exact sequence:

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow \mathbb{S}(E_K)[\ell^\infty] \longrightarrow Ш(E_K)[\ell^\infty] \longrightarrow 0.$$

8.1 Mordell–Weil group and Homomorphisms

Let E_K be a constant elliptic curve over K. We want to give a concrete description of the Mordell–Weil group $E(K)$ in terms of Tate modules of B and E defines as follows. Note that any morphism $x \in E(K)$ induces an morphism $\bar{x} : B \longrightarrow E$ and thus a morphism of their Jacobian (as moduli of divisors of degree 0):

$$J := \mathrm{Jac}(B) \longrightarrow \mathrm{Jac}(E) = E$$

This induces a homomorphism

$$E(K) \longrightarrow \mathrm{Hom}(J, E).$$

This homomorphism has finite kernel $E(K)_{\mathrm{tor}} = E(k)$ and finite cokernel. In fact, if D is any divisor on B with minimal positive degree e, then we can define a morphism $i_D : \quad B \longrightarrow J$ by sending x to the class of $ex - D$. Then the composition with i_D defines a homomorphism

$$\mathrm{Hom}(J, E) \longrightarrow E(K).$$

The composition of these two morphisms is given by multiplications by e modulo $E(k)$. In particular when $B(k) \neq \emptyset$, then we have have an isomorphism:

$$E(K)/E(K)_{\mathrm{tor}} \simeq \mathrm{Hom}(J, B).$$

To describe the second group, we use Tate modules: for any abelain group G, we write $\mathrm{T}_\ell(G) = \varprojlim_n G[\ell^n]$. Then have a morphism

$$\mathrm{T}_\ell : \qquad \mathrm{Hom}(J, B) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_\varphi(\mathrm{T}_\ell(J), \mathrm{T}_\ell(E)).$$

Tate has proved the following general facts about homomorphisms:

Theorem 8.1 (Tate)**.** *Let A_1 and A_2 be two Abelian varieties defined over a finite field k. The following natural map is bijective:*

$$\mathrm{T}_\ell : \qquad \mathrm{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \simeq \mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(\mathrm{T}_\ell(A_1), \mathrm{T}_\ell(A_2)),$$

Proof. In this section, we want to prove this in the simplest case when $A_1 = A_2$ is an elliptic curve E defined over a finite field k.

$$\mathrm{T}_\ell : \quad \mathrm{End}(E) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{End}(\mathrm{T}_\ell(E)) = \mathrm{End}_\varphi(\mathrm{T}_\ell(E)).$$

Then we see what to generalize for general case. First of all $\mathrm{End}(E)$ is finitely generated by Mordell–Weil. Thus

$$\mathrm{End}(E) \otimes \mathbb{Z}_\ell = \varprojlim_n \mathrm{End}(E)/\ell^n.$$

Step 1: T_ℓ is injective with free cokernel.

Let $\phi \in \mathrm{End}(E) \otimes \mathbb{Z}_\ell$ such that $\mathrm{T}_\ell(\phi) = 0$. Then ϕ is a p-adic limit of $\phi_i \in \mathrm{End}(E)$. It follows that for any n, $\mathrm{T}_\ell(\phi_i)$ is divisible by ℓ^n when i is sufficiently large, i.e., ϕ_i vanishes on $E[\ell^n]$. or equivalently ϕ_i is divisible by ℓ^n. Thus $\phi = 0$. This shows that T_ℓ is injective. For the second part, let $\psi \in \mathrm{End}(\mathrm{T}_\ell(E))$ such that $\ell^n\psi = \mathrm{T}_\ell(\phi)$ for some $\phi \in \mathrm{End}(E) \otimes \mathbb{Z}_\ell$. Write $\phi = \lim \phi_i$ then $\phi_i(E[\ell^n]) = 0$ for i large. Thus ϕ_i is divisible by ℓ^n. It follows that ϕ is divible by ℓ^n.

By Step 1, we are reduce the statement to

$$\mathrm{T}_\ell : \quad \mathrm{End}(E) \otimes \mathbb{Q}_\ell \xrightarrow{\sim} \mathrm{End}_L(\mathrm{V}_\ell(E)),$$

where $L = \mathbb{Q}(\varphi) \subset \mathrm{End}(E) \otimes \mathbb{Q}$ embedded in to $\mathrm{End}_L(\mathrm{V}_\ell(E))$. We see that $\deg L$ is either 1 or 2. If L is quadratic over $\mathbb{Q}$, then both sides are isomorphic to $L \otimes \mathbb{Q}_\ell$. Now we assume that $L = \mathbb{Q}$. Let A be the image of $\mathrm{End}(E) \otimes \mathbb{Q}_\ell$ in $\mathrm{End}(V_\ell(E))$. Then A is semi-simple. If T_ℓ is not subjective, then A commutative. We want to get a contradiction by constructing many elements in $\mathrm{End}(E) \otimes \mathbb{Q}_\ell$:

Step 2: for any line W in $V_\ell(E)$ there is an element $u \in \mathrm{End}(E) \otimes \mathbb{Q}_\ell$ such that $u(V_\ell(E)) = W$.

For each $n \in \mathbb{N}$, set $T_n = W \cap T_\ell(E) + \ell^n T_\ell(E)$, and let K_n be the image of T_n on $E[\ell^n]$. Form the quotient $\pi_n : E \longrightarrow E_n := E/K_n$, and its dual $\lambda_n : E_n \longrightarrow E$. Then

$$\mathrm{T}_\ell(\lambda_n)\mathrm{T}_\ell(E_n) = T_n.$$

Since there are only finitely many elliptic curves defined over k, there is an infinite set I of integers with minimal n such that E_i are all isomorphic to each other: $v_i : E_i \simeq E_n$. Consider $u_i = \lambda_i v_i \lambda_n^{-1} \in \mathrm{End}^0(E)$. Then

$$\mathrm{T}_\ell(u_i) T_n = T_i \subset T_n.$$

It follows that $\mathrm{T}_\ell(u_i) \in \mathrm{End}(T_n)$. Since $\mathrm{End}(T_n)$ is compact, we can find infinite subsequence u_j ($j \in J$) which convergent to u. This $u \in \mathrm{End}(E) \otimes \mathbb{Q}_\ell$ and we have

$$u(T_n) = \cap_{j \in J} u_j(T_n) = \cap_{j \in J} T_j = T \cap W.$$

□

Remark 8.1. For A a simple abelain variety over k, $\mathrm{End}(A) \otimes \mathbb{Q}$ will be a division algebra $\mathbb{Q}$. Thus any elements $\phi \in \mathrm{End}(A)$ will have a minimal polynomial $f(T)$ such that $\mathbb{Q}(\phi) = \mathbb{Q}[T]/(f(T))$. The isomorphism shows that ϕ acts on $\mathbb{V}_\ell(A)$ is semi simple with characteristic polynomial $P(T)$ a power of $f(T)$.

8.2 Selmer group

We want to give a concrete description of $\mathbb{S}(E_K)$ in terms of Tate modules of B and E. For simplicity, we assume that $B(k)$ is not empty.

Proposition 8.2. *There is an isomorphism:*

$$\mathbb{S}(E_K)[\ell^\infty] \simeq \mathrm{Hom}_\varphi(\mathrm{T}_\ell(J), \mathrm{T}_\ell(E) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)$$

with compatible maps from $E(K) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$.

Proof. Recall that $\mathbb{S}(E_K)[\ell^\infty]$ and $\text{Ш}[\ell^\infty]$ are defined by exact sequence:

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow H^1(K, E[\ell^\infty]) \longrightarrow H^1(K, E)[\ell^\infty] \longrightarrow 0$$

from the exact sequence

$$0 \longrightarrow \text{Ш}(E_K)[\ell^\infty] \longrightarrow H^1(K, E)[\ell^\infty] \longrightarrow \prod_v H^1(K_v, E)[\ell^\infty].$$

For each place we also have an exact sequence

$$0 \longrightarrow E(K_v) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow H^1(K_v, E[\ell^\infty]) \longrightarrow H^1(K_v, E)[\ell^\infty] \longrightarrow 0.$$

It follows that $\mathbb{S}(E_K)[\ell^\infty]$ fits in the exact sequence:

$$0 \longrightarrow \mathbb{S}(E_K)[\ell^\infty] \longrightarrow H^1(K, E[\ell^\infty]) \longrightarrow \prod_v H^1(K_v, E)[\ell^\infty].$$

Lemma 8.3. *For each place v, let I_v be the inertia subgroup of* $\mathrm{Gal}(\bar{K}_v/K_v)$ *with quotient group* $\mathrm{Gal}(\bar{k}_v/k_v)$. *Then*

$$H^1(K_v, E)[\ell^\infty] = H^1(I_v, E[\ell^\infty])^{\mathrm{Gal}(\bar{k}_v/k_v)}$$

as quotient spaces of $H^1(K_v, E[\ell^\infty])$.

Proof. This is a general fact for elliptic curves with good reduction. First we have the following exact sequences

$$0 \longrightarrow H^1(k_v, E[\ell^\infty]) \longrightarrow H^1(K_v, E[\ell^\infty]) \longrightarrow H^1(I_v, E[\ell^\infty])^{\mathrm{Gal}(\bar{k}_v/k_v)} \longrightarrow 0$$

$$0 \longrightarrow E(k_v) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow H^1(k_v, E[\ell^\infty]) \longrightarrow H^1(k_v, E)[\ell^\infty] \longrightarrow 0.$$

Since $H^1(k_vE) = 0$ (every genus one curve over finite field k_v has a rational point), we reduce the lemma to the identity

$$E(K_v) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \xrightarrow{\sim} E(k_v) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

This last identity follows form the exact sequence of groups

$$0 \longrightarrow E^0(K_v) \longrightarrow E(K_v) \longrightarrow E(k_v) \longrightarrow 0,$$

where $E^0(K_v)$ is the subgroup of points reducing to $0 \in E(k_v)$ which is isomorphic to p-adic group $\mathscr{O}_v$. □

To get a further description of $\mathbb{S}(E_K)$, we recall the exact sequence:

$$1 \longrightarrow \mathrm{Gal}(\bar{L}/L) \longrightarrow \mathrm{Gal}(\bar{K}/K)[\ell^\infty] \longrightarrow \mathrm{Gal}(\bar{k}/k)[\ell^\infty] \longrightarrow 1$$

with $L = \bar{k}K$ the function field of $\bar{B} = B \otimes \bar{k}$ over $\bar{k}$. Then we have exact sequence

$$0 \longrightarrow H^1(k, E[\ell^\infty]) \longrightarrow H^1(K, E[\ell^\infty]) \longrightarrow H^1(L, E[\ell^\infty])^{\mathrm{Gal}(\bar{k}/k)} \longrightarrow 0.$$

Since $\mathrm{Gal}(\bar{k}/k)$ is generated by Frobenius φ, we have that

$$H^1(k, E[\ell^\infty]) = E[\ell^\infty]/(\varphi - 1)E[\ell^\infty] = 0$$

since $E[\ell^\infty]$ is ℓ-divisible and that $\ker(\varphi - 1) = E(k)$ is finite. It follows that

$$H^1(K, E[\ell^\infty]) \simeq H^1(L, E[\ell^\infty])^{\mathrm{Gal}(\bar{k}/k)} = \mathrm{Hom}_\varphi(\mathrm{Gal}(L^{\mathrm{ab}}/L) \otimes \mathbb{Z}_\ell, E[\ell^\infty]).$$

Let b be a place of B. Then the inertial group I_v is included in $\mathrm{Gal}(\bar{L}/L)$ as inertial subgroup points $\bar{b}$ over b. Thus we have the following identification:

$$\mathbb{S}(E_K) = \mathrm{Hom}_\varphi(\mathrm{Gal}(L^{\mathrm{ab,ur}}/L) \otimes \mathbb{Z}_\ell, E[\ell^\infty]).$$

In terms of Jacobians, we have

$$\mathrm{Gal}(L^{\mathrm{ab,ur}}/L) \otimes \mathbb{Z}_\ell = \mathrm{T}_\ell(J), \qquad E[\ell^\infty] = \mathrm{T}_\ell(E) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

Thus we have the following identity

$$\mathbb{S}(E_K)[\ell^\infty] = \mathrm{Hom}_\varphi(\mathrm{T}_\ell(J), \mathrm{T}_\ell(E) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell).$$

□

8.3 Finiteness of $\text{Ш}(E_K)[\ell^\infty]$

Finally we want to discuss the proof of the following theorem:

Theorem 8.4 (Tate, Milne)**.**

$$\#\text{Ш}(E_K) < \infty.$$

This theorem is equivalent to that $\text{Ш}(E_K)[\ell^\infty]$ is finite for all prime ℓ and vanish for all but finitely many ℓ. In the following we only discuss the finiteness of $\text{Ш}(E_K)(\ell^\infty)$ when $\ell \neq p$. Let M denote φ-module $\mathrm{Hom}(\mathrm{T}_\ell(J), \mathrm{T}_\ell(E))$. The semi-simplicity of φ on on both $\mathrm{V}_\ell(J)$ and $\mathrm{V}_\ell(E)$ implies the semi simplicity of $M \otimes \mathbb{Q}_\ell$. If λ_i, μ_j are eigenvalues of φ on $\mathrm{V}_\ell(J)$ and $\mathrm{V}_\ell(E)$ respectively, then φ has eigenvalues $\lambda_i^{-1}\mu_j$ on $M \otimes \mathbb{Q}_\ell$. It follows that the minimal polynomial $P(T)$ of φ on M does not depend on the choice of ℓ. Let $Q(T)$ be $P(T)$ if $M^\varphi = 0$ or $P(T)/(T-1)$ if $M^\varphi \neq 0$. The Weil pairing on $\mathrm{T}_\ell(J)$ and on $\mathrm{T}_\ell(E)$ induces a φ-invariant pairing on M. Let N_φ denote the annihilator of M^φ.

Proposition 8.5. *With notation as above,*

$$\text{Ш}(E_K)[\ell^\infty] \simeq N_\varphi/(1-\varphi)M.$$

Moreover, $\text{Ш}(E_K)[\ell^\infty]$ *is finite and annihilated by* $Q(1)$.

Proof. From main results in previous two subsections, we see that $\text{Ш}(E_K)[\ell^\infty]$ is fit in the following exact sequence:

$$0 \longrightarrow M^\varphi \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow (M \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)^\varphi \longrightarrow \text{Ш}(E)[\ell^\infty] \longrightarrow 0.$$

From the exact sequence

$$0 \longrightarrow M \longrightarrow M \otimes \mathbb{Q}_\ell \longrightarrow M \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow 0,$$

$\text{Ш}(E_k)$ fits in the exact sequence:

$$0 \longrightarrow \text{Ш}(E_K)[\ell^\infty] \longrightarrow H^1(k, M) \longrightarrow H^1(k, M) \otimes \mathbb{Q}_\ell.$$

For the last two terms, use $H^1(k, M) = M/(1-\varphi)M$. It follows that

$$\text{Ш}(E_K)[\ell^\infty] \simeq (M/(1-\varphi)M)[\ell^\infty].$$

Now use the perfect paring $M \otimes M \longrightarrow \mathbb{Z}_\ell$. It is clear that $(1-\varphi)M$ is included in the the annihilator N_φ of M^φ. Since M/N_φ is torsion free (as a $\mathbb{Z}_\ell$-dual of M^φ), we see that

$$\text{Ш}(E_K)[\ell^\infty] \simeq (N_\varphi/(1-\varphi)M)[\ell^\infty].$$

It remains to show that $N_\varphi/(1-\varphi)M$ is already torsion. Here we use the semi-simplicity of φ on $M \otimes \mathbb{Q}_\ell$ follows from semisimplities of φ on both $\mathrm{V}_\ell(J)$ and $\mathrm{V}_\ell(E)$. By semisimplicty, we have a direct decomposition

$$M \otimes \mathbb{Q}_\ell = M^\varphi \otimes \mathbb{Q}_\ell \oplus (1-\varphi)M \otimes \mathbb{Q}_\ell.$$

For the last statement, we notice that $Q(\varphi)$ annihilates $(1-\varphi)M \otimes \mathbb{Q}_\ell = N_\varphi \otimes \mathbb{Q}_\ell$. It follows that $Q(1)$ annihilates $N_\varphi/(1-\varphi)M$. □

9 Constant elliptic curves: BSD conjecture

9.1 L-function

Let E_K be a constant elliptic curve with $K = k(B)$ as before. We want to compute the L-function of E_K. By definition it is given by

$$L(E_K, s) = \prod_{v \in |B|} (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$$

where $q_v = q^{\deg v}$ and

$$a_v = q_v + 1 - \#E(k_v)) = \alpha_1^{\deg v} + \alpha_2^{\deg v}.$$

Bring this to above equation, we obtain

$$L(E_K, s) = \prod_{v \in B} (1 - (\alpha_1 q^{-s})^{\deg v})^{-1} (1 - (\alpha_2 q^{-s})^{\deg v})^{-1} = Z(B, \alpha_1 q^{-s}) Z(B, \alpha_2 q^{-s})$$

where $Z(B, T)$ is the Zeta function of the curve B:

$$Z(B, T) = \prod_v (1 - T^{\deg v})^{-1} = \exp\left(\sum_{n=1}^{\infty} \#B(\mathbb{F}_{q^n}) \frac{T^n}{n} \right).$$

By Weil, we have an expression

$$Z(B, T) = \frac{\prod_{i=1}^{2g} (1 - \beta_i T)}{(1 - T)(1 - qT)}$$

where β_i are eigenvalues of φ on $\mathrm{T}_\ell(J)$ which is related to the set of rational points of B as follows:

$$B(\mathbb{F}_{q^n}) = q^n + 1 - \sum_i \beta_i^n.$$

Combining these computations, we have proved the following:

Theorem 9.1. *The L-function of E_K is given as follows:*

$$L(E_K, s) = \frac{\prod_{ij} (1 - \alpha_i \beta_j q^{-s})}{(1 - \alpha_1 q^{-s})(1 - \alpha_2 q^{-s})(1 - \alpha_1 q^{1-s})(1 - \alpha_2 q^{1-s})}.$$

By Weil' $|\beta_i| = \sqrt{q}$. It follows that the order of vanishing of $L(E_K, s)$ is the number of $(i, j) \in \{1, 2\} \times \{1, \cdots 2g\}$ such that $\alpha_i \beta_j = q$. Since $\alpha_1 \cdot \alpha_2 = q$, this is same as numbers of pairs (i, j) such that $\alpha_i = \beta_j$. This is the same as the rank of $\mathrm{Hom}(\mathrm{T}_\ell(B), \mathrm{T}_\ell(E))$. Thus we have proved the following:

Corollary 9.2. *Let $r = \mathrm{rank} E(K)$, then $L(E_K, s)$ has rank r at $s = 1$ and the leading term $L(E_K, s)$ at $s = 1$ is given by*

$$\lim_{s \longrightarrow 1} \frac{L(E_K, s)}{(s-1)^r} = \frac{q \prod_{\alpha_i \neq \beta_j} (1 - \alpha_i / \beta_j)}{\#E(k)^2} (\log q)^r.$$

9.2 Periods

In this section, we want to compute the periods $c(E_K)$.

Theorem 9.3. *Let g be the genus of B then*

$$c(E_K) = q^{1-g}.$$

Proof. We take an invariant differential ω of E_K and a measure dx on $\mathbb{A}_K$ such that $\mathrm{vol}(K\backslash\mathbb{A}_K) = 1$. Then $c(E_K) = \prod_v c(E_v, \omega, dx_v)$ where

$$c(E_v, \omega, dx_v) = L_v(E_K, 1) \int_{E(K_v)} |\omega|_v.$$

The reduction mod v induces an exact sequence

$$0 \longrightarrow E^0(K_v) \longrightarrow E(K_v) \longrightarrow E(k_v) \longrightarrow 0.$$

It follows that

$$c(E_v, \omega, dx_v) = L_v(E_K, 1) \cdot \#E(k_v) \cdot \mathrm{vol}(E^0(K_v)).$$

The three terms on the right hand side are given as follows:

$$L_v(E_K, 1) = (1 - a_v q^{-1} + q^{-1})^{-1}, \qquad \#E(k_v) = 1 + q_v - a_v, \qquad \mathrm{vol}(E^0(K_v)) = \frac{1}{q}\mathrm{vol}(\mathscr{O}_{K,v}).$$

It follows that

$$c(E_v, \omega, dx_v) = \mathrm{vol}(\mathscr{O}_{K,v}), \qquad c(E_K) = \mathrm{vol}(\widehat{\mathscr{O}}_K) \tag{9.1}$$

where $\widehat{\mathscr{O}}_K = \prod_v \mathscr{O}_{K,v}$.

To prove the volume of $\mathrm{vol}(\mathscr{O}_K)$ we use an exact sequence

$$0 \longrightarrow k \longrightarrow \widehat{\mathscr{O}}_K \longrightarrow K\backslash\mathbb{A}_K \longrightarrow K\backslash\mathbb{A}_K/\widehat{\mathscr{O}}_K \longrightarrow 0.$$

It follows that

$$\mathrm{vol}(\mathscr{O}_K) = q \cdot \mathrm{vol}(\widehat{\mathscr{O}}_K/k) = q/\#(K\backslash\mathbb{A}_K/\widehat{\mathscr{O}}_K). \tag{9.2}$$

To compute the last term, we consider the following exact sequence of abelian sheaves on B:

$$0 \longrightarrow \mathscr{O}_B \longrightarrow K_B \longrightarrow K_B/\mathscr{O}_B \longrightarrow 0.$$

Since K_B is flasq, we have the following exact sequence:

$$0 \longrightarrow k \longrightarrow K \longrightarrow \mathbb{A}_K/\widehat{\mathscr{O}}_K \longrightarrow H^1(B, \mathscr{O}_B) \longrightarrow 0$$

It follows that

$$\#K\backslash\mathbb{A}_K/\widehat{\mathscr{O}}_K = \#H^1(B, \mathscr{O}_B) = q^g. \tag{9.3}$$

The Theorem follows from (9.1)-(9.3).

□

9.3 Regulator

It remains to compute the regulator of E_K:

$$R(E_K) = \frac{\det(\langle P_i, P_j\rangle_{NT})}{\#E(k)^2}$$

where $\{P_1, \cdots P_r\}$ is a base of $E(K)/E(k)_{\mathrm{tor}}$, and $\langle\cdot,\cdot\rangle_{NT}$ is the Neron–Tate height paring.

Recall that we have define N_φ to the orthogonal complement of M^φ in the Weil paring of $M = \mathrm{Hom}(\mathrm{T}_\ell(J), \mathrm{T}_\ell(E))$. Let $\mathbb{Z}_{(\ell)}$ be the localization of $\mathbb{Z}$ at the prime ideal $\ell\mathbb{Z}$.

Theorem 9.4. *There is an element $u \in \mathbb{Z}_{(\ell)}^\times$ such that*

$$R(E_K) = u\frac{\#[M/(M^\varphi + N_\varphi)]}{\#E(k)^2}(\log q)^r.$$

By definition, the identity in Theorem is equivalent to the following:

$$\det(\langle P_i, P_j\rangle_{NT}) = u\#[M/(M^\varphi + N_\varphi)](\log q)^r. \tag{9.4}$$

The Neron–Tate heights on $E(K)$ can be defined by the same process as before. It can be computed using the Weil pairing $\langle\cdot,\cdot\rangle_{Weil}$.

Proposition 9.5. *Let $x, y \in E(K)$ and let x_ℓ, y_ℓ be their images in M. Then*

$$\langle x, y\rangle_{NT} = \langle x_\ell, y_\ell\rangle_{Weil}\log q.$$

Proof. (Sketch) Extend x and y to two morphisms $\bar{x}, \bar{y} : B \longrightarrow E$. Let Γ_x, Γ_y be their graphs in $B \times E$, then we have

$$\langle x, y\rangle_{NT}/\log q = -\Gamma_x \cdot \Gamma_y + \deg\bar{x} + \deg\bar{y}.$$

The right hand can be computed using $H^2(\bar{B} \times \bar{E}, \mathbb{Q}_\ell(1))$. The formula in Proposition follows from the Kunneth decomposition:

$$H^2(\bar{B} \times \bar{E}, \mathbb{Q}_\ell(1)) = H^2(\bar{B}, \mathbb{Q}_\ell(1)) \oplus [H^1(\bar{B}, \mathbb{Q}_\ell) \otimes H^1(\bar{E}, \mathbb{Q}_\ell)(1)] \oplus H^2(\bar{E}, \mathbb{Q}_\ell(1)).$$

The middle term is M. □

By Proposition, $\det\langle P_i, P_j\rangle_{NT}/(\log q)^r$ generates the discriminant ideal in $\mathbb{Z}_\ell$ of the pairing:

$$M^\varphi \otimes M^\varphi \longrightarrow \mathbb{Z}_\ell.$$

This pairing induces an embedding $M^\varphi \longrightarrow \mathrm{Hom}(M^\varphi, \mathbb{Z}_\ell)$. Thus

$$\det\langle P_i, P_j\rangle_{NT}/(\log q)^r = u\#[\mathrm{Hom}(M^\varphi, \mathbb{Z}_\ell)/M^\varphi]$$

for some $u \in \mathbb{Z}_{(\ell)}^\times$. On the other hand, by definition, N_φ is the orthogonal complement of M^φ. The perfect paring on M induces a perfect paring

$$M^\varphi \otimes M/N_\varphi \longrightarrow \mathbb{Z}_\ell.$$

Thus we have $\mathrm{Hom}(M^\varphi, \mathbb{Z}_\ell) = M/N_\varphi$. The formula (9.4) follows.

Now we are ready to prove the last part of BSD:

Theorem 9.6. *For $\ell \neq p$ there is a unit $u \in \mathbb{Z}_{(\ell)}^{\times}$ such that*

$$\lim_{s \longrightarrow 1} \frac{L(E_K, s)}{(s-1)^r} = u \cdot c(E_K) \cdot R(E_K) \cdot \#\text{Ш}(E_K).$$

Proof. We have seen that $c(E_K) = q^{1-g}$ is a ℓ-unit. It remains to compute the product $|R(E_K)\text{Ш}(E_K)|$ which is given by

$$u \frac{\#M/(N_\varphi + M^\varphi)}{\#E(k)^2} (\log q)^r \cdot \#[N_\varphi/(1-\varphi)M] = u \frac{\#M/((1-\varphi)M + M^\varphi)}{\#E(k)^2} (\log q)^r.$$

Let $L = M/M^\varphi$. Since φ is semi simple, $\varphi - 1$ has non-zero determinant on L, and

$$\#M/((1-\varphi)M + M^\varphi) = \#L/(1-\varphi)L = \det(1-\varphi|L) = \prod_{\alpha_i \neq \beta_j} (1 - \alpha_i/\beta_j).$$

The theorem follows. □

10 Faltings Heights

In this and next section, we are going to sketch Faltings' proof on Tate's conjecture and Shafarevich conjecture. Let K be a number field with Galois group $\Gamma := \mathrm{Gal}(\bar{K}/K)$.

Theorem 10.1 (Tate's conjecture)**.** *Let E/K be an elliptic curves over a number field and ℓ be a prime. Then the representation of Γ on the Tate module $\mathrm{T}_\ell(E)$ is semi simple, and the morphism*

$$\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_\Gamma(\mathrm{T}_\ell(E))$$

is an isomorphism.

Theorem 10.2 (Shafarevich's conjture)**.** *Let S be a finite set of places of K. Then there are only finitely many isomorphism classes of elliptic curves over K with good reduction outside of S.*

There are two ingredients in his proofs: the theory of Faltings' heights and theory of p-divisible groups. In this section, we are focusing on height theory.

10.1 Stable elliptic curves and modular curves

Let S be an scheme. A group scheme $\pi : E \longrightarrow S$ is called a stable elliptic curve if the following hold:

1. there is an dense open subscheme U of S called good or elliptic locus such that E_U/U is an elliptic curve scheme.
2. if s is a geometric point of S not in U, then the fiber E_s is a multiplicative group $\mathbb{G}_m$, the complement $S \setminus U$ is called bad locus or cuspidal locus.

For a stable elliptic curve with zero section $e: \quad S \longrightarrow E$. Define the line bundle on S by

$$\omega_{E/S} = e^*\Omega_{E/S}.$$

Over the elliptic locus U, $\omega_{E_U/U}$ is isomorphic to $\pi_*\Omega^1_{E_U/U}$. Recall that the j-invariants defines an morphism $U \longrightarrow \mathbb{A}^1$. If S is integral and normal, then this morphism extend to a morphism $S \longrightarrow \mathbb{P}^1$. One can show the following isomorphism:

$$\omega_{E/S}^{\otimes 12} = j^*\mathscr{O}(1).$$

If S is a complex variety, then we can define matrix on $\omega_{E_U/U}$ such that at each point $s \in U$,

$$\langle \alpha, \beta \rangle = \frac{i}{2}\int_{E_s(\mathbb{C})} \alpha \wedge \bar{\beta}, \qquad \forall \alpha, \beta \in \Gamma(E_s, \Omega^1).$$

The following are basic facts about stable elliptic curves:

1. Stable under base change: if E/S is stable, then for any morphism $f: T \longrightarrow S$, the base change E_T/T is stable, and $f^*\omega_{E/S} = \omega_{E_T/T}$.
2. Stable reduction theorem: if $S = \mathrm{Spec}R$ with a R a complete discrete valuation ring with fractional field K, and let E_K/K be an elliptic curve. Then there is a finite extension L of K such that $E_L := E_K \otimes L$ has a stable model over the ring of integers $\mathscr{O}_L$. For example, we can take $L = K(E[n])$ for any integer $n \geq 3$ prime to the residue characteristic of R.

One family of important examples are the universal elliptic curves $\mathscr{E}$ over the moduli curve $X := X(N)$ of full level N-structure, where $N = N_1 \cdot N_2$ is a product of two relative prime numbers $N_i \geq 3$. (Thus the minimal such N is 12). The X is a regular 2-dimensional scheme whose projection over $\mathrm{Spec}\mathbb{Z}[\zeta_N]$ is projective, flat, and geometrically connected, where ζ_N is a fixed primitive N-th root of unity. The scheme X is a union of affine scheme Y and a cuspidal divisor Cups. The restriction of $\mathscr{E}_Y$ on Y is a family of elliptic curves with a level structure, i.e., a surjective group scheme homomorphism with prescribed Weil paring

$$\phi: (\mathbb{Z}/N\mathbb{Z})^2 \longrightarrow \mathscr{E}_Y[N], \qquad \langle \phi(1,0), \phi(0,1) \rangle = \zeta_N.$$

We have an isomorphism of bundles:

$$\omega_{\mathscr{E}/X}^{\otimes 2} \simeq \Omega_{X/\mathbb{Z}[\zeta_N]}(\mathrm{Cups}).$$

This implies that $\omega_{\mathscr{E}/X}$ is an ample line bundle on X.

Over the open subscheme $\mathrm{Spec}\mathbb{Z}[1/N]$, such an isomorphism is an isomorphism. Its base change to $\mathrm{Spec}\mathbb{C}$ is the usual modular curve

$$X(\mathbb{C}) = Y(\mathbb{C}) \cup \mathrm{Cups}, \qquad Y(\mathbb{C}) = \Gamma(N)\backslash\mathscr{H}$$

The universal elliptic curve $\mathscr{E}_Y$ and the level structure over a point represented by $\tau \in \mathscr{H}$ is given by

$$\mathscr{E}_\tau = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \qquad \phi(a,b) = \frac{a}{N} + \frac{b}{N}\tau.$$

The isomorphism of bundles is given by identifying the sections $(2\pi i du)^{\otimes 2}$ and $2\pi i d\tau$.

The family $\mathscr{E}/X$ is the moduli space of stable elliptic curves with full level N-structure in the following sense:

Proposition 10.3. *Let S be a normal scheme of dimension 1, E/S a stable elliptic curve, and ϕ a full level N-structure over elliptic locus U with Weil paring ζ_N. Then there is a unique morphism $f : S \longrightarrow X$ such that $E = f^*\mathscr{E}$.*

If E/S is a general stable elliptic curve with S integral, then we can construct a finite base change $S' \longrightarrow S$ with degree bonded by N^4 such that S' admits a morphism to $S' \longrightarrow X$ as follows. First all after a normalization, we may assume that S is normal. Then over the elliptic locus U, we have a fine covering $E_U[N] \longrightarrow U$ of degree N^2. Let V be the normalization of $E_U[N] \times_U E_U[N]$. Then over V we have a homomorphism

$$(\mathbb{Z}/N\mathbb{Z})^2 \longrightarrow E_V[N].$$

Let U' be the open subscheme of V over which this homomorphism is surjective. Let S' be the normalization of $U' \longrightarrow S$. Then the base change E' over S' have the require property.

10.2 Tate curves and compactifications

First let us consider the Tate curve over $\mathbb{Z}[[q]]$ defined by

$$E_q : \quad Y^2Z + XYZ = X^3 + a_4XZ^2 + a_6Z^3$$

where

$$\begin{aligned} -a_4 =& 5\sum_n \frac{n^3q^n}{1-q^n} = 5q + 45q^2 + 140q^3 + \cdots \\ -a_6 =& \sum_n \frac{7n^5+5n^3}{12} \times \frac{q^n}{1-q^n} = q + 23q^2 + 154q^3 + \cdots \end{aligned}$$

are power series with integer coefficients. When $q = 0$, $a_4 = a_6 = 0$. Thus Equation becomes

$$Y^2Z + XYZ = Z^3$$

which is parametrized by $\mathbb{P}^1$:

$$[X : Y : Z] = [ts(s+t) : t^2(s+t) : s^3].$$

Smooth part of Tate's curve is parameterized by open part of $\mathbb{P}^1$ given by $t = 0$ and $s = -t$. Thus it is isomorphic to $\mathbb{G}_m$. This shows that smooth part of E_q is a stable curve. One can show that the total space of Tate's curve is actually a regular three dimensional scheme and the relative singularity is given by simple node at $X = Y = 0$, thus it has local equation likes

$$uv = q.$$

On $\mathbb{Z}[\frac{i}{2}][[q]]$, this can be seen directly by completion of square:

$$y^2 + xy - x^3 = (y + x/2)^2 + x^2/4(1+4x) = (y + \frac{1}{2}x + \frac{i}{2}x\sqrt{1+4x})(y + \frac{1}{2}x - \frac{i}{2}x\sqrt{1+4x}).$$

So we can set $u, v \in \mathbb{Z}[\frac{i}{2}][[x, y, q]]$ as

$$u = \frac{y + \frac{1}{2}x + \frac{i}{2}x\sqrt{1+4x}}{\sqrt{(a_4x + a_6)/q}}, \qquad v = \frac{y + \frac{1}{2}x - \frac{i}{2}x\sqrt{1+4x}}{\sqrt{(a_4x + a_6)/q}}.$$

Let k be a a complete field with respect to some absolute value $|\cdot|$. Let R be ring of elements with norm ≤ 1 and I be the ideal of elements with norm < 1. Let $f : \mathrm{Spec} R \longrightarrow \mathrm{Spec}\mathbb{Z}[[q]]$ be a morphism such that $t := f^*q \neq 0$. The pull-back of Tate curve on $\mathrm{Spec} k$ is isomorphic to $k^*/t^{\mathbb{Z}}$, taking $w \in k^\times$ to $(x(w), y(w))$ for w not a power of q, where

$$\begin{aligned} x(w) &= -\, y(w) - y(w^{-1}) \\ y(w) &= \sum_{m \in Z} \frac{(t^m w)^2}{(1 - t^m w)^3} + \sum_{m \geq 1} \frac{t^m w}{(1 - t^m w)^2} \end{aligned}$$

Fix $N = N_1 \cdot N_2$ with $N_i \geq 3$ and consider the modular curve $X = X(N)$ over $\mathrm{Spec}\mathbb{Z}[\zeta_N]$. The cuspidal divisor Cups is a disjoint union of cuspidal section of $X \longrightarrow \mathrm{Spec}\mathbb{Z}[\zeta_N]$ parametrized by surjective morphism

$$\lambda : \quad (\mathbb{Z}/N\mathbb{Z})^2 \longrightarrow \mathbb{Z}/N\mathbb{Z}.$$

Each cuspidal section s_λ has a formal neighborhood

$$\mathrm{Spec}\mathbb{Z}[\zeta_N][[q^{1/N}]] \longrightarrow X$$

over which $\mathscr{E}$ is given by the smooth part of the Tate curve E_q. For a morphism $f : \mathrm{Spec} R \longrightarrow X$ as above, the group $f^*\mathscr{E}[N]$ is generated by unity ζ_N and the image $t^{1/N}$ of $q^{1/N}$. The level structure ϕ on $f^*\mathscr{E}$ determines λ as follows:

$$(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\phi} f^*\mathscr{E}[N] \longrightarrow \mathbb{Z}/N\mathbb{Z}$$

where the second morphemes takes $\zeta_N^a \cdot t^{b/N}$ to b.

10.3 Faltings Heights

Let K be a number field with ring of integers $\mathscr{O}_K$ and $E/\mathscr{O}_K$ a stable elliptic curve. Then we have a bundle $\omega_{E/\mathscr{O}_K}$ with a Faltings metric $\|\cdot\|_F$ metric defined at each infinite place v as before:

$$\|\alpha\|^2_{F,v} = \frac{i}{2} \int_{E_v(\mathbb{C})} \alpha \wedge \bar{\alpha}.$$

The Faltings' height is defined as

$$h_F(E) = \frac{1}{[K : \mathbb{Q}]} \deg \omega_{E/\mathscr{O}_K}.$$

The first main theorem of this section is the following Northcott property of Faltings height:

Theorem 10.4. *For any positive numbers H and D, there only finitely many stable elliptic curves E/K with $\deg K < D$ and $h_F(E) < H$.*

We first reduce the theorem to the Northcott property on modular curve X parametrizing full level structure $N = N_1 \cdot N_2$. It clear that the Faltings height does not depend on base change. So we may assume that $E/\mathscr{O}_K$ has full level N-structure. Thus it is given by a morphism

$$f : \quad \mathrm{Spec}\mathscr{O}_K \longrightarrow X$$

such that $f^*\mathscr{E} = E$, and that $\omega_{E/\mathscr{O}_K} = f^*\omega_{\mathscr{E}/X}$. Notice that same formula actually define a metric on $\mathscr{E}_Y/Y$, where Y is elliptic locus of X. Thus we have a Faltings height function h_F on $Y(\bar{\mathbb{Q}})$, and reduce the theorem to the following:

Theorem 10.5. *For any positive numbers H and D, there only finitely many point $y \in Y(\bar{\mathbb{Q}})$ such that* $\deg y < D$ *and* $h_F(y) < D$.

Secondly, recall that we have an isomorphism over X of the bundle:

$$\omega_{\mathscr{E}/X}^{\otimes 12} = j^*\mathscr{O}(1)$$

where $j : X \longrightarrow \mathbb{P}^1$. Define $h_j(x) = \frac{1}{12}h(j(x))$. Since the Northcott theorem holds for $\mathbb{P}^1$, it suffices to show that $h_F(y) - h_j(y)$ is bounded on $Y(\bar{\mathbb{Q}})$. Unfortunately, this is not true. But one can prove the following

Proposition 10.6. *There are constants a and b such that for any $y \in Y(\bar{\mathbb{Q}})$:*

$$|h_F(y) - h_j(y)| \leq a + b\log^+ h_j(y)$$

where $\log^+ z = \log\max(1, |z|)$ *for an* $z \in \mathbb{C}$.

This proposition implies Theorem since

$$h_j(y) - b\log^+ h_j(y) \leq h_F(y) + a.$$

The bound $h_F(y) < H$ will imply $h_j(y) < H'$ for some H' depending only on H.

Thirdly, we reduce the proposition to an estimate of singularity of norm. Let $\|\cdot\|_j$ be the metric on $\omega_{\mathscr{E}/X}$ induced by a metric on $\mathscr{O}(1)$. Then the above inequality is implied by the following on $Y(\mathbb{C})$:

$$\left|\log\frac{\|\cdot\|_F}{\|\cdot\|_j}\right| \leq a + b\log^+\log^+ j.$$

This is a local problem near a cusp s Recall that $j^{-1} \simeq q = t^N$ where t is a local coordinate at s. Let $\alpha \in \omega_{\mathscr{E}/X}$ in the neighborhood $B_\epsilon := \{t : |t| < \epsilon\}$ for a small ϵ. We need only show that

$$|\log\|\alpha\||(t) \leq c + d\log^+\log^+ t^{-1}.$$

Now we want to prove this estimate. Notice the curve $\mathscr{E}$ over $B(\epsilon)$ has a singularity $uv = q = t^N$ and α has the form $fdu/u = -fdv/v$ near singularity with f holomorphic on $\mathscr{E}_{B(\epsilon)}$ with $f(0,0) = 1$. Thus for $t \neq 0$,

$$\|\alpha\|_t^2 = \frac{i}{2}\int_{\mathscr{E}_t(\mathbb{C})}\alpha\wedge\bar{\alpha}.$$

We write this integration as some over two parts: $\max(|u|,|v|) < 1$, and $\max(|u|,|v|) < 1$. Thus we have

$$\|\alpha\|_t^2 = \frac{i}{2}\int_{|t|^N\leq|u|\leq 1}|f|^2\frac{du d\bar{u}}{|u|^2} + O(1).$$

Using polar coordinates $u = \rho e^{i\theta}$, then we have

$$\|\alpha\|_t^2 = \int_{|t|^N}^1\frac{d\rho}{\rho}\int_0^{2\pi}|f|(\rho,\theta)d\theta + O(1) = 2\pi N\log|t|^{-1} + O(1).$$

It follows that

$$\log\|\alpha\|_t = \log\log|t|^{-1} + O(1).$$

The second main theorem of Fatings heights is its behavior under isogeny.

Let K be a number field with ring of integers $\mathscr{O}_K$. Let $\phi : E_1 \longrightarrow E_2$ be an isogeny of two stable elliptic curves defined over $\mathscr{O}_K$ with kernel G (as a finite group scheme over $\mathscr{O}_K$). Then we have

Theorem 10.7.

$$h_F(E_1) - h_F(E_2) = \frac{1}{[K:\mathbb{Q}]}\log \# e^*\Omega^1_{G/\mathscr{O}_K} - \frac{1}{2}\log\deg\phi.$$

Proof. The morphism ϕ induces an exact sequence of sheaves of differentials on E_1:

$$0 \longrightarrow \phi^*\Omega_{E_2/\mathscr{O}_K} \longrightarrow \Omega_{E_1/\mathscr{O}_K} \longrightarrow \Omega_{E_1/E_2} \longrightarrow 0.$$

Taking restriction on the unit section e, this gives an exact sequence over Spec$\mathscr{O}_K$

$$0 \longrightarrow \omega_{E_2/\mathscr{O}_K} \xrightarrow{\phi^*} \omega_{E_1/\mathscr{O}_K} \longrightarrow e^*\Omega_{G/\mathscr{O}_K} \longrightarrow 0.$$

Thus we can view ϕ^* as a section of bundle

$$\mathscr{L} := \omega_{E_1/\mathscr{O}_K} \otimes \omega_{E_2/\mathscr{O}_K}^{\otimes -1}.$$

The hermitian metrics on $\omega_{E_i/\mathscr{O}_K}$ induce a hermtian structure on $\mathscr{L}$. Now we compute the degree using section ϕ^* to obtain

$$h_F(E_1) - h_F(E_2) = \frac{1}{[K:\mathbb{Q}]}\deg\mathscr{L} = \frac{1}{[K:\mathbb{Q}]}\left(\log \#\mathscr{L}/\mathscr{O}_K\phi^* - \log\prod_v \|\phi^*\|_v\right).$$

For the first term, we have directly

$$\#\mathscr{L}/\ell\mathscr{O}_K = \#\omega_{E_1/\mathscr{O}_K}/\phi^*\omega_{E_2/\mathscr{O}_K} = \#e^*\Omega_{G/\mathscr{O}_K}.$$

For the second term, by definition, at an archimedean place v, and an nonzero form $\alpha \in \Gamma(E_{2v})$,

$$\|\phi^*\|_v^2 = \frac{\|\phi^*\alpha\|_v^2}{\|\alpha\|_v^2} = \deg\phi, \qquad 0 \neq \alpha \in \Gamma(E_{2v}, \Omega^1).$$

It follows that

$$\prod_v \|\phi^*\|_v = \deg\phi^{[K:\mathbb{Q}]/2}.$$

The theorem follows. □

11 Finiteness theorems of elliptic curves

In this section, we are going to prove Tate's conjecture and Shafarevich's conjecture for elliptic curves E defined over number field K. The key tool is the Tate module $\mathrm{T}_\ell(E)$ as a $\mathrm{Gal}(\bar{K}/K)$ representation ρ and its restriction ρ_v on decomposition group D_v at a finite place v of K. So we will first study the local representations.

11.1 Local representations

In this subsection we fix a prime p and a finite extension K of $\mathbb{Q}_p$ with ring of integers $\mathscr{O}_K$ and residue field $k \simeq \mathbb{F}_q$. Let E/K be an elliptic curve with stable reduction. Let ℓ be a prime and consider the representation ρ of $\Gamma_K := \mathrm{Gal}(\bar{K}/K)$ on $\mathrm{T}_\ell(E)$. We will describe this action according to $\ell \neq p$ and $\ell = p$ separately.

Theorem 11.1. *Assume that $\ell \neq p$. Then we have the following:*

1. *if E has a good reduction, then the representation ρ is unramifed and semi simple, and the* Frob *has the characterstic polynomial $P(T) = T^2 - aT + q$ such that $P(1) = \#E(k)$;*
2. *if E has a bad reduction, then the inertial group acts unimportant but nontrivial, and the representation ρ is ramified with following triangulation:*

$$\begin{pmatrix} \epsilon\chi_0 & * \\ 0 & \epsilon \end{pmatrix}$$

where ϵ is a non-trivial quadratic character of Γ_K, and χ_0 is the cyclotomic character acting on $\mathbb{Z}_\ell(1) := \mathrm{T}_\ell(\mathbb{G}_m)$. The $\epsilon = 1$ if and only if the reduction is split multiplicative.

Now we treat the case where $\ell = p$. Let $\mathbb{C}_p$ be the completion of $\bar{K}$ which carries a continuous action of $\mathrm{Gal}(\bar{K}/K)$. Then the p-adic Hodge–Tate decomposition is the following:

Theorem 11.2. *There is a canonical isomorphism of Γ_K-modules:*

$$\mathrm{T}_p(E)_{\mathbb{C}_p} \simeq \mathrm{Lie}(E_{\mathbb{C}_p})^\vee \bigoplus \mathrm{Lie}(E_{\mathbb{C}_p})(1)$$

where (1) *means twists by the module $\mathbb{Z}_p(1) = \mathrm{T}_p(\mathbb{G}_m)$.*

Sketch of proof. By using the fact that $H^0(K, \mathbb{C}_p) = K$ and $H^0(K, \mathbb{C}_p(n)) = 0$ for $n \neq 0$, the theorem is equivalent to

$$\mathrm{Lie}(E)^\vee = H^0(K, \mathrm{T}_p(E)_{\mathbb{C}_p}), \qquad \mathrm{Lie}(E) = H^0(K, \mathrm{T}_p(E)_{\mathbb{C}_p}(-1)).$$

Using Weil's pairing, both are equivalent to a non-trivial Γ_K-equivariant paring:

$$\mathrm{Lie}(E_{\mathbb{C}_p}) \otimes_{\mathbb{Z}_p} \mathrm{T}_p(E) \longrightarrow \mathbb{C}_p.$$

Take an extension $\mathscr{E}$ of group scheme over $\mathscr{O}_K$ and consider the formal completion $H := \widehat{O}_k$ of $\mathscr{E}$ at the origin O_k at the special fiber E_k over the residue field k. Then H is a connected formal group scheme over $\mathscr{O}_K$ of dimension 1 and we have

$$\mathrm{T}_p(H) \subset \mathrm{T}_p(E), \qquad \mathrm{Lie}(H_K) = \mathrm{Lie}(E).$$

Let $H^\vee$ be the Cartier dual of H: Then we have a surjective morphism $\mathrm{T}_p(E) \longrightarrow \mathrm{T}_p(H^\vee)$. Then we are reduced to construct a non-trivial paring

$$\mathrm{Lie}(H_{\mathbb{C}_p}) \otimes_{\mathbb{Z}_p} \mathrm{T}_p(H^\vee) \longrightarrow \mathbb{C}_p.$$

Let $H_n = H[p^n]$ and $G_n^\vee = H^\vee[p^n]$. Then by definition,

$$H_n^\vee(\mathscr{O}_{\mathbb{C}_p}) = \mathrm{Hom}(H_n \otimes \mathscr{O}_{\mathbb{C}_p}, \widehat{\mathbb{G}}_m \widehat{\otimes} \mathscr{O}_{\mathbb{C}_p}).$$

Take projective limit to obtain:

$$\mathrm{T}_p H^\vee = \mathrm{Hom}(H \widehat{\otimes} \mathscr{O}_{\mathbb{C}_p}, \widehat{\mathbb{G}}_m \otimes \mathscr{O}_{\mathbb{C}_p}).$$

Here the right hand side is the group of formal group homomorphisms.

Apply differential to obtain an injective morphism

$$\mathrm{T}_p H^\vee \longrightarrow \mathrm{Hom}(\mathrm{Lie}(H_{\mathbb{C}_p}), \mathbb{C}_p).$$

□

The same proof shows that for any (ind-finite) p-divisible group G over R,

$$\mathrm{T}_p(G)_{\mathbb{C}_p} = \mathrm{Lie}(G^\vee_{\mathbb{C}_p})^* \bigoplus \mathrm{Lie}(G_{\mathbb{C}_p})(1).$$

We want to extend this fact for any divisible subgroup of $E[p^\infty]$ (not necessarily ind-finite over $\mathscr{O}_K$):

Theorem 11.3. *Let G be a p-divisible subgroup of $E[p^\infty]$ of height h of dimension $d := \dim G \cap H$.Then*

$$\mathrm{T}_p(G)_{\mathbb{C}_p} = \mathbb{C}_p^{h-d} \oplus \mathbb{C}_p^d(1).$$

This theorem follows from the exact sequence

$$0 \longrightarrow H \cap G \longrightarrow G \longrightarrow G/G \cap H \longrightarrow 0$$

and the following result is about irreducibility of $\mathrm{T}_p(E)$ under inertial subgroup I_K of Γ_K.

Proposition 11.4. *Let H is the formal completion of $\mathscr{E}$ at the origin O_k in $\mathscr{E}_k$. Then*

1. *The action I_K on $\mathrm{T}_p(H)$ is irreducible and does not factor through finite quotient.*
2. *The action of I_K on $\mathrm{T}_p(E)/\mathrm{T}_p(H)$ factors through a finite quotient.*

Proof. The first part is clear because H is a formal group of dimension 1. For second part, we may assume that $H \neq E[p^\infty]$. Then E has either good ordinary reduction or multiplicative bad reduction. In either case after a finite extension, we have $H = \widehat{\mathbb{G}}_m$. It follows that $\mathrm{T}_p(H) \simeq \mathbb{Z}_p(1)$. By Weil paring $\mathrm{T}_p(E)/\mathrm{T}_p(H)$ is a trivial I_p-module. □

11.2 Endomorphisms

Theorem 11.5. *Let K be a number field and let $E/\mathscr{O}_K$ be a stable elliptic curve and $G \subset E[\ell^\infty]$ a ℓ-divisible subgroup, and $E_n = E/G[\ell^n]$. Then*

$$h_F(E_n) = h_F(E)$$

Proof. There is nothing to prove if $G = E[\ell^\infty]$ or $G = 0$. Thus we consider the case where G is of height 1. Recall that we have a formula:

$$h_F(E) - h_F(E_n) = \frac{1}{[K:\mathbb{Q}]} \log e^*\Omega^1_{G[\ell^n]/\mathscr{O}_K} - \frac{1}{2}\log \#G[\ell^n].$$

The second term is $\frac{n}{2}\log \ell$. For the first term, we notice that it is sum over places $s_1, \cdots s_r$ of $\mathrm{Spec}\mathscr{O}_K$ over $\ell \in \mathrm{Spec}\mathbb{Z}$:

$$\log e^*\Omega^1_{G[\ell^n]/\mathscr{O}_K} = \sum_i \log e^*\Omega^1_{G[\ell^n]/\mathscr{O}_{K,s_i}}.$$

At each point s_i, we may replace G by the maximal subgroup G_i which is pro-finite over $\mathscr{O}_{K,s_i}$. The group G_i can be constructed as follows: Let $H_i = \widehat{O}_{s_i}[\ell^\infty]$, the maximal connected subgroup of $E[\ell^\infty]$, then $G_i = G \cap H_i$. Let d_i and h_i are dimension and height of G_i. Then

$$d_i \le h_i \le 1.$$

If $d_i = 1$, then G_i an one-dimensional torus after a base change. Thus

$$G_i[\ell^n] \simeq \mu_{\ell^n} \otimes \mathscr{O}_{K,s_i} = \mathrm{Spec}\mathscr{O}_{K,s_i}[X]/(X^{\ell^n} - 1).$$

It follows that

$$\Omega^1_{G_i[\ell^n]/\mathscr{O}_{K,s_i}} \simeq \mathscr{O}_{K,s_i}[X]/(\ell^n, X^{\ell^n} - 1)dX.$$

The evaluation at $X = 1$ gives

$$\#e^*\Omega^1_{G_i[\ell^n]/\mathscr{O}_{K,s_i}} = \#\mathscr{O}_{K,s_i}/\ell^n = \ell^{nm_i}$$

where $m_i = [K_{s_i} : \mathbb{Q}_\ell]$. Thus we obtain

$$h_F(E) - h_F(E_n) = \frac{n}{m}\left(\sum m_i d_i - \frac{m}{2}\right)$$

where $m = [K : \mathbb{Q}]$.

It remains to prove $\sum m_i d_i = \frac{m}{2}$. Now consider the $\Gamma_\mathbb{Q}$ module $V = \mathrm{Ind}_K^\mathbb{Q}(\mathrm{T}_\ell(E))$ of dimension $2m$ and its submodule $W = \mathrm{Ind}_{\Gamma_K}^{\Gamma_\mathbb{Q}}(\mathrm{T}_\ell(G))$ of dimension m respectively and form the line

$$L = \wedge^m W \subset \wedge^m V.$$

The action of $\Gamma_\mathbb{Q}$ on L is given by a character $\chi : \Gamma_\mathbb{Q} \longrightarrow \mathbb{Z}_\ell^\times$. By class field theory, up to finite character, this character is a ℓ-adic power of the cyclotomic character χ_0. We first compute this power using Hodge–Tate decomposition and then compare it with Hasse's estimate to get conclusion.

First, we notice that the restriction of these modules on the decomposition group D at ℓ is given by

$$W|_D = \oplus_i \mathrm{Ind}_{D_i}^D(\mathrm{T}_\ell(G)).$$

By Theorem 11.3, we have an isomorphism of D_i-module:

$$\mathrm{T}_\ell(G)_{\mathbb{C}_\ell} = \mathbb{C}_\ell^{1-d_i} \bigoplus \mathbb{C}_\ell(d_i).$$

It follows that

$$\mathbb{C}_\ell \otimes W|_D = \oplus_i \mathrm{Ind}_{D_i}^D(\mathbb{C}_\ell^{1-d_i} \oplus \mathbb{C}_\ell(d_i)) = \oplus_i \mathrm{Ind}_{D_i}^D(\mathbb{C}_\ell^{1-d_i}) \bigoplus \oplus(\mathrm{Ind}_{D_i}^D \mathbb{C}_\ell)(d_i).$$

Since $\det \mathrm{Ind}_{D_i}^D \mathbb{C}_\ell = \mathbb{C}_\ell(\chi_i)$ with χ_i a finite character,

$$L \otimes \mathbb{C}_\ell = \mathbb{C}_\ell(\chi)(\sum_i m_i d_i)$$

where χ is a finite character.

Finally, we apply Hasse theorem: for almost all ℓ, all eigenvalues of Frob_ℓ on $\mathrm{T}_\ell(E)$ are algebraic integers with absolute value $\ell^{1/2}$. It follows that the eigenvalues of Frob_ℓ on L are algebraic integer with eigenvalues $\ell^{m/2}$. Thus we must have

$$\sum m_i = \frac{m}{2}.$$

□

Theorem 11.6. *Let E/K be an elliptic curve (not necessary having stable reductions). The action of Γ_K on $\mathrm{V}_\ell(E)$ is semi simple and the map*

$$\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell(E))$$

is an isomorphism.

Proof. As in the case over finite field, it suffices to show that the map

$$\mathrm{T}_\ell : \quad \mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \longrightarrow \mathrm{End}_{\Gamma_K}(\mathrm{V}_\ell(E))$$

is bijective. After a finite base change, we may assume that E/K has stable reduction. We want to show that for any line $W \subset \mathrm{V}_\ell(E)$ invariant under Γ_K, there is an morphism $\phi \in \mathrm{End}(E) \otimes \mathbb{Q}_\ell$ such that $\mathrm{T}_\ell(\phi)$ has image W. We will argue by exact same method as in §8.1. Let G be the ℓ-divisible subgroup of $E[\ell^\infty]$ such that $\mathrm{V}_\ell(G) = W$. Define $\pi_n : E \longrightarrow E_n = E/G_n$ and $\lambda_n : E_n \longrightarrow E$ the dual map. Then

$$\mathrm{T}_\ell(\lambda_n)(\mathrm{T}_\ell(E_n)) = \mathrm{T}_n := \mathrm{T}_\ell(G) + \ell^n \mathrm{T}(E).$$

Since $h_F(E_n)$ are equal to each other, then there is a set I of infinite numbers with minimal n such that all E_i $(i \in I)$ are isomorphic to each other. Choose isomorphisms

$$v_i : \quad E_n \simeq E_i, \qquad i \in I.$$

Set $u_i = \lambda_i \nu_i \lambda_n^{-1} \in \mathrm{End}^0(E)$. Then

$$\mathrm{T}_\ell(u_i)(\mathrm{T}_n) = \mathrm{T}_i \subset \mathrm{T}_n.$$

It follows that $\mathrm{T}_\ell(u_i) \in \mathrm{End}(\mathrm{T}_n)$. By compactness, we can find a subsequence J of I such that u_j $(j \in J)$ is convergent to $u \in \mathrm{End}(E) \otimes \mathbb{Q}_\ell$. We have

$$\mathrm{T}_\ell(u)(\mathrm{T}_n) = \mathrm{T}_\ell(E) \cap W.$$

□

11.3 Finiteness theorem

In future, we will generalize above theorem to abelian varieties A over K. Taking $= E_1 \oplus E_2$, we will get the following

Theorem 11.7 (Tate's conjecrure)**.** *Let E_1 and E_2 be two elliptic curves over K. Then*

$$\mathrm{Hom}_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell(E_1), \mathrm{T}_\ell(E_2))$$

is an isomorphism.

The firs consequence of this theorem is that the isogeny class of an elliptic curve is determined by its L-series.

Corollary 11.8. *Let E_1, E_2 be two elliptic curves over a number field K. The following are equivalent:*

1. *E_1, E_2 are isogenous;*
2. *$\mathrm{V}_\ell(E_1) \simeq \mathrm{V}_\ell(E_2)$ as Γ_K-modules for all ℓ;*
3. *$\mathrm{V}_\ell(E_1) \simeq \mathrm{V}_\ell(E_2)$ as Γ_K-modules for one ℓ;*
4. *$L_v(E_1, s) = L_v(E_2, s)$ for all finite plave v of K;*
5. *$L_v(E_1, s) = L_v(E_2, s)$ for almost all v.*

Proof. The equivalence of first 4 conditions is the previous theorem. They are equivalent to (5) by Chebotarev density theorem. □

Theorem 11.9 (Shafarevich conjecture)**.** *Let S be a finite set of places of K. There are only finitely many isomorphic classes of elliptic curves with good reduction outside of S.*

We will prove this theorem in several steps. The first step is to prove the statement with "isomorphic classes" replaced by "isogenous cases". By Weil conjecture, we need only strengthen the previous corollary:

Proposition 11.10. *Fix a prime ℓ outside of S and let K' be the union of all field extensions of K of degree $< \ell^8$ unramified outside S. Let $G = \mathrm{Gal}(K'/K)$ and let T be a finite set places v of K whose Frobenuous gives every conjugacy classes of G. Then two elliptic curves are isogenous if they have same local L-functions at places $v \in T$.*

Proof. Let E_1 an E_2 be two elliptic curves over K with same L-series at places in T. Let

$$M \subset \mathrm{End}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(E_1)) \oplus \mathrm{End}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(E_2))$$

be the image of $\mathbb{Z}_\ell[\Gamma_K]$. By Tate's conjecture and E_1 and E_2 are isogenous to each other if and only if

$$\mathrm{tr}(m|\mathrm{T}_\ell(E_1)) = \mathrm{tr}(m\mathrm{T}_\ell(E_2)), \qquad \forall m \in M.$$

By assumption, this is already true for Frobenius $m_i := \mathrm{Frob}(v_i)$. We need to show that these m_i generate M. By Nakayama lemma, we need only prove this mod ℓ. When mod ℓ, we have

$$M/\ell M \subset \mathrm{End}(E_1[\ell]) \oplus \mathrm{End}(E_2[\ell]).$$

Since $K(E_i[\ell])$ are unramified outside of S and rank$M$ is at most 8, we see that the representation of Γ_K on $M/\ell M$ factors through G. We are done. □

By this proposition, it remains to prove there are only finitely many isomorphic classes of elliptic isogenous to a give one E. After a base change, we may assume that E has stable reductions over $\mathscr{O}_K$. Let E' be an curve isogenois to E. Then we can pick up an cyclic isogeny $E \longrightarrow E'$. By decompositions of kernel, we have can write E' has direct coproduct of isogenies $E \longrightarrow E_i$ of prime-prower degree. Thus we are reduce to the following statement: there are only finitely many isomorphic classes of elliptic curves E' which has an isogeny to E with degree a power of a prime ℓ. We prove this statement in next two steps: the case of a fixed ℓ and the case of all large ℓ.

Proposition 11.11. *Let ℓ be a prime. There are only finitely many isomorphic classes of elliptic curves E' which has an isogeny to E with ℓ-power degree.*

Proof. If we have infinitely such non-isomorphism classes of E_i, then we have infinitely many cyclic finite subgroups G_i of $E[\ell^\infty]$ such that $E_i = E/G_i$. Then a finite set of such G_i will form a ℓ-divisible group G. The main result in the last subsection gives a contradiction. □

The last step is devoted to show that for a prime ℓ sufficiently large, there are only finitely finitely isomorphism classes of E with an isogeny to E of ℓ-power degree. We need only consider the cyclic isogeny of rank 1

Proposition 11.12. *There is positive integer N such for any two isogeny $\phi : E_1 \longrightarrow E_2$ of degree $\ell \nmid N$ of two elliptic curves E_i isogenous to E,*

$$h_F(E_1) = h_F(E_2).$$

Proof. Let G be the kernel of ϕ. Then by height formula,

$$h_F(E_1) - h_F(E_2) = \frac{1}{[K:\mathbb{Q}]} \log \# e^* \Omega_{G/\mathscr{O}_K} - \frac{1}{2} \log \ell.$$

We need to prove that the right hand side vanishes, i.e, the exponent d in $e^*\Omega_{G/\mathscr{O}_K} = \ell^d$ is equal to $m/2$ where $m = [K : \mathbb{Q}]$. We will use a result of Raynaud about group scheme over local ring of type $(\ell, \cdots, \ell)$. For this, we define N_1 to be the all primes over which either $\mathscr{O}_K$ is ramified or E has a bad reduction. If ℓ is prime to N_1, the scheme G is finite over all places of ℓ. Let $\widetilde{G} = (\mathrm{Res}_{\mathscr{O}_K/\mathbb{Z}} G)$. Then $\widetilde{G}$ is a finite and flat group scheme of type $(\ell, \cdots, \ell)$, then

$$e^*\Omega_{G/\mathscr{O}_K} = e^*\Omega_{\widetilde{G}_{\mathbb{Z}_\ell}/\mathbb{Z}_\ell} = \ell^d.$$

By a theorem of Raynaud, this d can be read out from the action of $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$:

$$\wedge^m \widetilde{G}(\bar{\mathbb{Q}}_\ell) = \mathbb{F}_\ell(d).$$

If $\ell - 1 > m \geq d$, then d is unequaly determined by this equality. Thus we assume ℓ is prime to the product N_2 of all primes $\leq m + 1$.

On the other hand, $\mathrm{Res}_{K/\mathbb{Q}} G$ itself is a group over $\mathbb{Z}$ whose geometric points carries an action by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The induced action on $\wedge^m \widetilde{G}(\bar{\mathbb{Q}})$ is given by a character χ. To compute this character, we notice

$$(\mathrm{Res}_{K/\mathbb{Q}})G(\bar{\mathbb{Q}}) = \mathrm{Ind}_{\Gamma_K}^{\Gamma_\mathbb{Q}} G(\bar{K}).$$

Let $\epsilon : \Gamma_{\mathbb{Q}} \longrightarrow \{\pm 1\}$ be the character of $\Gamma_{\mathbb{Q}}$ on $\wedge \mathrm{Ind}_{\Gamma_K}^{\Gamma_{\mathbb{Q}}} \mathbb{Z}$, then $\chi \cdot \epsilon$ is an unramified outside ℓ. This because by stability, at places v K not dividing ℓ, the inertial groups I_v act uniportently on $G(\bar{K})$. It follows that $\chi\epsilon$ is a power of cyclotomic character χ_0. By Raynaud's theorem, we have

$$\chi = \chi_0^d \epsilon.$$

Let p be a fixed prime not dividing N_1. If $p \neq \ell$, then p unramfied in $\mathrm{Ind}_{\Gamma_K}^{\Gamma_{\mathbb{Q}}} \mathrm{T}_\ell(E)$. Let $P(T)$ be the characteristic tic polynomial of Frob_p over on $\mathrm{Ind}_{\Gamma_K}^{\Gamma_{\mathbb{Q}}} \mathrm{T}_\ell(E)$. Then the above identity shows that $\chi(\mathrm{Frob}_\ell) = \pm \ell^d$ is one eigenvalue of $P(T)$ modulo ℓ. Notice that $P(T)$ is independent of ℓ with eigenvalues of absolute value $\ell^{m/2}$. Thus we can define a non-zero integer by

$$N_3 := p \prod_{\substack{0 \leq j \leq m \\ j \neq m/2}} (P(\ell^j) P(-\ell^j)).$$

If $\ell \nmid N_3$, then we must have $d = \frac{m}{2}$.

In summary, the number $N = N_1 \cdot N_2 \cdot N_3$ will fulfill the requirement of Propostion.

□