NOTE ON THE MORDELL CONJECTURE

Jinghao Yang

Contents

1 Faltings' Theory of Heights

The classical height theory shows that there are only finitely many points of bounded height (the Northcott property), which can be extended to arithmetic geometry by Arakelov's theory. It reminds us to embed the moduli space of the principally polarized abelian varieties into $\mathbb{P}^n$, and then use Zarhin's trick to remove the condition of principal polarization. As a result, we obtain a finiteness theorem on the isomorphism classes of abelian varieties.

Further, we want a similar finiteness statement for the isogeny classes of abelian varieties. Thus we introduce the concept of Faltings height, which changes according to a nice formula under isogeny. All that remains is to compare the two heights.

1.1 Faltings heights

Let K be a number field and denote by $\mathcal{O}_K$ its ring of integers. The completion of K at a place v is denoted by K_v, and $v \mid \infty$ means that v is an Archimedean valuation.

Definition 1.1. A Hermitian line bundle $\widehat{\mathcal{L}} = (\mathcal{L}, \|\cdot\|)$ over $\operatorname{Spec} \mathcal{O}_K$ consists of a line bundle $\mathcal{L}$ over $\operatorname{Spec} \mathcal{O}_K$ and a collection $\|\cdot\| = \{\|\cdot\|_\sigma\}_\sigma$, where $\|\cdot\|_\sigma$ is a metric of the complex line $\mathcal{L}_\sigma = \mathcal{L} \otimes_\sigma \mathbb{C}$ for each embedding $\sigma : F \to \mathbb{C}$ and is invariant under the action of the complex conjugate.

Definition 1.2. The arithmetic degree (Arakelov degree) of a Hermitian line bundle $\widehat{\mathcal{L}} = (\mathcal{L}, \|\cdot\|)$ is defined to be

$$\deg \widehat{\mathcal{L}} = \log \# (\mathcal{L}/s\mathcal{O}_K) - \sum_{\sigma : K \to \mathbb{C}} \log \|s\|_\sigma,$$

where $s \in \mathcal{L}$ is a nonzero element. By the product formula, the definition is independent of the choice of s.

Remark 1.3. For v a finite place, $\mathcal{L} \otimes \mathcal{O}_{K_v} \subset \mathcal{L} \otimes K_v$ provides a norm $\|\cdot\|_v$ on $\mathcal{L} \otimes K_v$, with unit ball $\mathcal{L} \otimes \mathcal{O}_{K_v}$; For Archimedean places, we just use Hermitian metrics. Then the definition of arithmetic degree can be rewritten to a more symmetric formula

$$\deg(\mathcal{L}) = \sum_{v:\text{ places}} -\log \|s\|_v.$$

If $(\mathcal{L}_i, \|\cdot\|_i)$ over $\operatorname{Spec} \mathcal{O}_K$ are given for $i = 1, 2$, then $\mathcal{L}_1 \otimes \mathcal{L}_2$ equipped $\|\cdot\|_1 \otimes \|\cdot\|_2$ is also metrized. Same for the dual line bundles $\mathcal{L}^\vee$. The arithmetic degree is additive under these operations, which pass to isomorphism classes.

Now we introduce a special Hermitian line bundle. For a semi-abelian S-scheme G of relative dimension g and unit section e, we have so-called Hodge line bundle on S

$$\omega_G := e^* \Omega^g_{G|S}.$$

Grothendieck's semistable reduction theorem asserts that every abelian variety becomes semistable after a finite extension of the ground field. For such a semistable abelian variety A, its connected Néron model $\widetilde{A} := \mathfrak{A}^\circ$ is semi-abelian, which gives rise to a Hodge line bundle on $\mathcal{O}_K$, denoted by ω_A, with a canonical Hermitian metric given by

$$\|\alpha\|^2_\sigma = \int_{A_\sigma(\mathbb{C})} \left|\alpha \wedge \bar{\alpha}\right|,$$

where $\sigma : K \to \mathbb{C}$ is any embedding and $\alpha \in \omega_A \otimes_\sigma \mathbb{C}$ is any global holomorphic g-form on the complex torus $A_\sigma(\mathbb{C})$.

Definition 1.4. Let A be an abelian variety over K. The Faltings height of A is defined to be

$$h_F(A) = \frac{1}{[K' : \mathbb{Q}]} \deg \omega_A,$$

where K' is a finite extension of K such that $A_{K'}$ has everywhere semistable reduction over $\mathcal{O}_{K'}$. This definition does not depend on the choice of K' and is invariant under base change.

Remark 1.5. We hope there are only finitely many abelian varieties over K of fixed dimension and bounded Faltings height. However, for an elliptic curve $E/\mathbb{Q}$, all quadratic twists of E have the same Faltings height but are not isomorphic. Thus we only consider semistable abelian varieties, which in this example corresponds to throwing out all but finitely many of these quadratic twists

[B B, Ex. 3.4]. At the same time, the semistable condition ensures that the Faltings height does not decrease under base change [Mil, p. 153], and taking Néron models commutes with base change.

Proposition 1.6. *Let $\phi : A \to B$ be an isogeny of degree n, where A and B are abelian varieties over a number field K, with semistable reduction at places over n. Then,*

$$h(A) - h(B) = \frac{1}{[K:\mathbb{Q}]} \log \left| s^*\Omega^1_{\mathcal{G}/\mathcal{O}_K} \right| - \frac{1}{2}\log n,$$

where $\mathcal{G} = \ker(\phi : \widetilde{A} \to \widetilde{B})$.

Proof. We can assume that $M := \Gamma(\widetilde{A}, \Omega^g_{\widetilde{A}/\mathcal{O}_K})$ and $N := \Gamma(\widetilde{B}, \Omega^g_{\widetilde{B}/\mathcal{O}_K})$ are both rank one free modules by possibly enlarging K. Now let α be a generator of M, and α' a generator of N, then we have $\phi^*\alpha' = a\alpha$ for some $a \in \mathcal{O}_K$. In terms of α, the Faltings height is just

$$h(A) = -\frac{1}{2[K:\mathbb{Q}]} \sum_{\sigma : K \to \mathbb{C}} \log \int_{A_\sigma(\mathbb{C})} \left| \alpha \wedge \bar{\alpha} \right|.$$

Note

$$|\omega|_i = \frac{1}{n} \left| \phi^*\omega \right|_i = \frac{i(a)\overline{i(a)}}{n} \left| \omega_i \right|,$$

by looking at how $A(\mathbb{C})$ is $\mathbb{C}^g$ mod a lattice, and seeing that A is defined by an index n sublattice of that defining B. We therefore have

$$\begin{aligned} h(B) &= -\frac{1}{2[K:\mathbb{Q}]} \sum_{i:K\to\mathbb{C}} \log \left| \omega' \right|_i \\ &= -\frac{1}{2[K:\mathbb{Q}]} \sum_{i:K\to\mathbb{C}} \Big(-\log(n) + \log(i(a)\overline{i(a)}) \Big) + h(A) \\ &= \frac{1}{2}\log n - \frac{1}{[K:\mathbb{Q}]} \log \left| \operatorname{Norm}_{K/\mathbb{Q}}(a) \right| + h(A) \end{aligned}$$

Thus,

$$h(A) - h(B) = -\frac{1}{2}\log n + \frac{1}{[K:\mathbb{Q}]} \log | \operatorname{Norm}_{K/\mathbb{Q}}(a).$$

To showing that $\operatorname{Norm}_{K/\mathbb{Q}}(a) = \left| s^*\Omega^1_{\mathcal{G}/\mathcal{O}_K} \right|$, there is a standard exact sequence

$$\phi^*\Omega^1_{\widetilde{B}/\mathcal{O}_K} \longrightarrow \Omega^1_{\widetilde{A}/\mathcal{O}_K} \longrightarrow \Omega^1_{\widetilde{A}/\widetilde{B}} \longrightarrow 0.$$

A Néron differential is a global invariant differential, so it is determined by its value at the identity. Pulling back along the identity section, we obtain a short exact sequence

$$0 \longrightarrow s^*\phi^*\Omega^1_{\widetilde{B}/\mathcal{O}_K} = s^*\Omega^1_{\widetilde{B}/\mathcal{O}_K} \xrightarrow{\phi_s} s^*\Omega^1_{\widetilde{A}/\mathcal{O}_K} \longrightarrow s^*\Omega^1_{\widetilde{A}/\widetilde{B}} \longrightarrow 0.$$

Since $\phi^*\omega' = a\omega$, we have $\det \phi^* = a$. Thus, by taking top wedge powers of this short exact sequence, $\left| s^*\Omega^1_{\widetilde{A}/\widetilde{B}} \right| = \operatorname{Norm}_{K/\mathbb{Q}}(a)$.

It remains to show that $\left| s^*\Omega^1_{\widetilde{A}/\widetilde{B}} \right| = \left| s^*\Omega^1_{\mathcal{G}/\mathcal{O}_K} \right|$. In fact, these two modules over $\mathcal{O}_K$ are isomorphic. Let $f : \mathcal{G} \hookrightarrow A$ denote the inclusion. Note also that $\mathcal{G} \to \operatorname{Spec} \mathcal{O}_K$ is the base change of $A \to B$ with respect to identity on B so $f^*\Omega^1_{\widetilde{A}/\widetilde{B}} \cong \Omega^1_{\mathcal{G}/\mathcal{O}_K}$. The morphism s factors through

f, so clearly

$$s^*f^*\Omega^1_{\widetilde{A}/\widetilde{B}} \cong s^*\Omega^1_{\widetilde{A}/\widetilde{B}} \cong s^*\Omega^1_{\mathcal{G}/\mathcal{O}_K}.$$

□

Proposition 1.7. *If A is an abelian variety over K with semistable reduction, then $h\left(A^\vee\right) = h(A)$, where $A^\vee$ denotes the dual abelian variety to A.*

Proof. After possibly passing to a larger finite extension, it suffices to consider the case when A is isogenous to a principally polarized abelian variety. If A is actually isomorphic to a principally polarized abelian variety, then we are done, since $A \cong A^\vee$. Thus, it suffices to show that $h(A^\vee) - h(A)$ is an isogeny invariant. Since any isogeny can be factored (over another finite field extension) into ones of prime degree, we are reduced to showing that

$$h(A^\vee) - h(B^\vee) + h(B) - h(A) = 0,$$

when there is an isogeny $\varphi : A \to B$ of prime degree p. By using the formula for change of Faltings height under isogeny, it suffices to show

$$[K : \mathbb{Q}] \cdot \log p = \log\left(\left|s^*\Omega^1_{G/\mathcal{O}_K}\right| \cdot \left|s^*\Omega^1_{G^\vee/\mathcal{O}_K}\right|\right),$$

where $G = \ker(\varphi : A \to B)$ and $G^\vee = \ker\left(\varphi^\vee : B^\vee \to A^\vee\right)$. After this, by completing at each place dividing p, it suffices to show

$$\left|s^*\Omega^1_{G_v/\mathcal{O}_{K,v}}\right| \cdot \left|s^*\Omega^1_{G_v^\vee/\mathcal{O}_{K,v}}\right| = \left|\mathcal{O}_{K,v}/p\mathcal{O}_{K,v}\right|$$

The rest of the argument uses the decomposition of Tate modules T_ℓ into torsion and free parts, after which you do some diagram chasing involving formal schemes; see [Fal+92, Bh. IV, Prop. 3.7]. □

1.2 The Northcott property

Definition 1.8 (Arakelov height)**.** Let X be a projective K-variety with a proper $\mathcal{O}_K$-model $\mathcal{X}$. Every point $x \in X(K)$ extends uniquely to a morphism Spec $\mathcal{O}_K \to \mathcal{X}$ by the valuative criterion. For a line bundle $\mathcal{L}$ with integral structure relative to $\mathcal{X}$, we can make $x^*\mathcal{L}$ a metrized line bundle over Spec $\mathcal{O}_K$ as in Remark 1.3 and put

$$h_{\widehat{\mathcal{L}}}(x) := \frac{1}{[K : \mathbb{Q}]} \deg x^*\mathcal{L}.$$

The factor $[K : \mathbb{Q}]^{-1}$ ensures that $h_{\widehat{\mathcal{L}}}(x) = h_{\widehat{\mathcal{L}}_E}(x)$ for any finite extension $E \mid K$. Clearly,

$$h_{\widehat{\mathcal{L}}_1 \otimes \widehat{\mathcal{L}}_2} = h_{\widehat{\mathcal{L}}_1} + h_{\widehat{\mathcal{L}}_2}, \quad h_{\widehat{\mathcal{L}}^\vee} = -h_{\widehat{\mathcal{L}}}$$

Degrees and heights also respect pull-backs: let $X \xrightarrow{f} Y$ be a morphism between projective K-varieties, compatible with the given $\mathcal{O}_K$-models, and let $\widehat{\mathcal{L}}$ be on Y. Then the pull-back $f^*\widehat{\mathcal{L}}$ makes sense and we won't go into the details.

Example 1.9. Consider $X = \mathbb{P}^N, \mathcal{L} = \mathcal{O}(1)$ endowed with the standard $\mathbb{Z}$-integral structure. Write $X_0, \ldots, X_N$ for the standard global sections of $\mathcal{O}(1)$. Here we use the Fubini-Study metric on Archimedean places:

$$\|(a_0X_0 + \cdots + a_NX_N)(x)\|_{v,x} = \frac{\left|\sum_{i=0}^N a_ix_i\right|_v}{\sqrt{\sum_{i=0}^N |x_i|_v^2}}, \quad v \mid \infty,$$

where $a_0, \ldots, a_N \in K_v$ and $x = (x_0 : \cdots : x_N)$.

Let $x = (x_0 : \cdots : x_N) \in \mathbb{P}^N(K)$. It extends to $\mathbb{P}^N(\mathcal{O}_K)$. For $v \nmid \infty$, its image in $\mathbb{P}^N(\mathcal{O}_{K_v})$ is easily described as $(x_0/t : \cdots : x_N/t)$, where $t \in K_v$ satisfies $|t|_v = \max\limits_{0 \leqslant i \leqslant N} |x_i|_v$.

Without loss of generality, suppose $x_0 \neq 0$. Take $\ell := X_0$ and use the observation above to compute the degree:

$$\|\ell\|_v = \begin{cases} \dfrac{|x_0|_v}{\sqrt{\sum_{i=0}^N |x_i|_v^2}}, & v \mid \infty \\ \dfrac{|x_0|_v}{\max_{0 \leqslant i \leqslant N} |x_i|_v} & v \nmid \infty \end{cases}$$

The terms $|x_0|_v$ drop out after taking $\prod_v$, by the product formula. We obtain

$$h_{\widehat{\mathcal{L}}}(x) = \frac{1}{[K:\mathbb{Q}]}\left(\sum_{v|\infty} \log \sqrt{\sum_{i=0}^N |x_i|_v^2} + \sum_{v \nmid \infty} \log \max_{0 \leqslant i \leqslant N} |x_i|_v\right).$$

Proposition 1.10. *Modulo $O(1)$, the set of bounded functions on $X(\overline{\mathbb{Q}})$, then the function $h_{\mathcal{L}}$ depends only on the line bundle $\mathcal{L}$ over X.*

Proof. We want to compare $\exp h_{\widehat{\mathcal{L}}}(x)$ for two families of v-adic metrics $\|\cdot\|_v, \|\cdot\|'_v$ defining metrized line bundles on X. One should bound the other by multiplicative constants.

By compactness, there exists $C_\infty > 0$ such that for each embedding $\iota : K \hookrightarrow \mathbb{C}$, the corresponding Hermitian forms satisfy

$$\|\cdot\|'_\iota \leqslant C_\infty \|\cdot\|_\iota$$

For the non-Archimedean case, suppose that the integral structures for $\|\cdot\|$ and $\|\cdot\|'$ give rise to "lattices" $\mathcal{L}^\circ, \mathcal{L}^\dagger$ in $\mathcal{L}$, respectively. Then there is $N \in \mathbb{Z}_{\geqslant 1}$ such that

$$N\mathcal{L}^\circ \subset \mathcal{L}^\dagger$$

This is a general property for K-schemes of finite type, and can be checked on affine open subsets. It entails that for every place $v \nmid \infty$ of K,

$$\|\cdot\|'_v \leqslant |N|_v^{-1} \|\cdot\|_v$$

Note that $|N|_v = 1$ for almost all v. This gives the required bound of $(\prod_v \|\cdot\|')^{1/[K:\mathbb{Q}]}$ by $(\prod_v \|\cdot\|_v)^{1/[K:\mathbb{Q}]}$

Moreover, the implied constants in the inequalities must be uniform when K is replaced by some finite extension E. This is guaranteed by the power $1/[K:\mathbb{Q}]$ and the equality $[E:K] = \sum_{w|v} [E_w : K_v]$, etc. □

We will denote this $O(1)$-coset as $h_{\mathcal{L}}$.

Theorem 1.11 (Northcott property for heights)**.** *If $\mathcal{L}$ is ample, then for all $d \in \mathbb{Z}_{\geqslant 1}$ and $B \in \mathbb{R}$, the set*

$$\left\{x \in X(L) : [L : K] \leqslant d, h_{\widehat{\mathcal{L}}}(x) \leqslant B\right\}$$

is finite. Here $\widehat{\mathcal{L}}$ is any metrization of $\mathcal{L}$.

Proof. We are free to alter the Hermitian and integral structures on $\mathcal{L}$. Upon replacing $\mathcal{L}$ by $\mathcal{L}^{\otimes m}$ (thus $h_{\widehat{L}}$ by $mh_{\widehat{\mathcal{L}}}$) with $m \gg 0$, we may assume $\mathcal{L} = i^*\mathcal{O}(1)$ via a projective embedding $i : X \hookrightarrow \mathbb{P}^N$. The problem reduces to the case $X = \mathbb{P}^N$ and $\mathcal{L} = \mathcal{O}(1)$, with the standard integral structure and Fubini-Study metrics. Denote the corresponding height function as h.

Consider $x = (x_0 : \cdots : x_N) \in \mathbb{P}^N(K)$. When $K = \mathbb{Q}$, we may further assume that $x_0, \ldots, x_N \in \mathbb{Z}$ are coprime. The formula for $h(x)$ reduces our assertion to showing that

$$\left\{ \vec{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N : \vec{x} \neq 0, \log \sqrt{\sum_{i=0}^{N} x_i^2} \leqslant B \right\}$$

is a finite set. This is trivial.

For general K, let $\{x^{(1)}, \ldots, x^{(d)}\}$ be the Galois orbit of x in $\mathbb{P}^N(\overline{\mathbb{Q}})$, so they have the same height and $d \leqslant [K : \mathbb{Q}]$. We may identify x with the $\mathbb{Q}$-point $\{x^{(1)}, \ldots, x^{(d)}\}$ of the variety $\operatorname{Sym}^d \mathbb{P}^N$. We are reduced to the previous case using an explicit embedding $\phi : \operatorname{Sym}^d \mathbb{P}^N \hookrightarrow \mathbb{P}^M$ over $\mathbb{Q}$, for example, Chow embeddings. The key is a bound of the form $h(\phi(x)) \leqslant ah(x) + b$, where a, b depend solely on N, d. □

1.3 Modular heights

Consider the moduli stack $\mathcal{A}_g$ over $\mathbb{Z}$ of principally polarized abelian schemes of dimension g. What matters for us is just its coarse moduli space. It is the base of the universal principally polarized abelian scheme $A_{\text{univ}} \to \mathcal{A}_g$. We obtain the Hodge line bundle ω over $\mathcal{A}_g$.

There are some compactifications of $\mathcal{A}_g$ over $\mathbb{Z}$.

1. The minimal compactification $\mathcal{A}_g \hookrightarrow \mathcal{A}_g^*$ of Baily-Borel. Its definition over $\mathbb{C}$ is relatively easy: simply take the normal projective embedding of $\mathcal{A}_g$ induced by the graded algebra of Siegel modular forms. This compactification is rarely smooth.

2. The toroidal compactifications $\mathcal{A}_g \hookrightarrow \overline{\mathcal{A}_g}$. They are defined in terms of rational polyhedral combinatorial data. Toroidal compactifications are not canonical: only the tower thereof is a canonical object. Each $\overline{\mathcal{A}_g}$ is proper and smooth over Spec $\mathbb{Z}$, and there is a semi-abelian scheme $G \to \overline{\mathcal{A}_g}$ extending $A_{\text{univ}} \to \mathcal{A}_g$. Consequently, ω extends to a line bundle over $\overline{\mathcal{A}_g}$, namely $\omega_{G|\overline{\mathcal{A}_g}}$.

Remark 1.12. To obtain moduli spaces as bona fide schemes, one can rigidify A by adding level structures $(\mathbb{Z}/n\mathbb{Z})_S^{2g} \xrightarrow{\sim} A[n]$ with $n \geqslant 3$ []. Faltings didn't assume this in his original proof. Besides, the arithmetic theory of toroidal compactifications of $\mathcal{A}_g$ was not yet available at that time. Now these are best treated by the Faltings-Chai theory (cf. [FC, V.4]), where the argument below follows.

Every toroidal compactification dominates the minimal one via a proper surjection $\overline{\mathcal{A}_g} \xrightarrow{\pi} \mathcal{A}_g^*$. In [FC, V.2.3 Theorem] is defined a very ample line bundle $\mathcal{L}_m$ on $\mathcal{A}_g^*$, obtained as the descent of $\omega^{\otimes m}$ along π for large $m \in \mathbb{Z}_{\geqslant 1}$.

Putting a level structure, we can assume that $\mathcal{A}_g$ is a quasi-projective variety over $\mathbb{Q}$. This permits us to define the height $h_{\widehat{\mathcal{L}}_m} : \mathcal{A}_g(\overline{\mathbb{Q}}) \to \mathbb{R}$ using that Hermitian form on $\omega\big|_{\mathcal{A}_{g,\mathbb{C}}}$ passes to $\mathcal{L}_m\big|_{\mathcal{A}_{g,\mathbb{C}}} \simeq \omega^{\otimes m}\big|_{\mathcal{A}_{g,\mathbb{C}}}$ and the integral structure inherent in $\mathcal{L}_m$ and $\mathcal{A}_g^*$.

Definition 1.13. Let A be principally polarized and identify it as an element of $\mathcal{A}_g(F)$. The modular height of A is

$$h_{\text{mod}}(A) := \frac{1}{m} h_{\widehat{\mathcal{L}}_m}(A).$$

By construction, $h_{\text{mod}}(A)$ is independent of m.

Modular heights are "continuous" functions on compact space, which means they are bounded. The relationship between the modular height and the Faltings height is quite easy.

From [FC13, IV.5.7 Theorem (5)] or [FC13, IV.5.1 Proposition] (in essence, the uniqueness of semi-abelian models) we infer the existence of

- ◇ a toroidal compactification $\overline{\mathcal{A}_g}$ of $\mathcal{A}_g$,
- ◇ a morphism Spec $\mathcal{O}_F \xrightarrow{f} \overline{\mathcal{A}_g}$ whose generic fiber is the morphism Spec $F \to \mathcal{A}_g$ classifying A,

such that $\mathfrak{A}^\circ \to$ Spec $_F$ is the pullback of the semi-abelian scheme $G \to \overline{\mathcal{A}_g}$. Summing up,

$$\begin{tikzcd}
\mathcal{A}_g \arrow[r, hook] & \mathcal{A}_g^* & \overline{\mathcal{A}_g} \arrow[l, two heads, "\pi"'] \\
\operatorname{Spec} F \arrow[u] \arrow[r] & \operatorname{Spec} \mathcal{O}_F \arrow[u] \arrow[ur, "f"'] &
\end{tikzcd}$$

commutes.

Therefore $\mathcal{L}$ pulled back to Spec $\mathcal{O}_F$ equals $\omega^{\otimes m} = \pi^*\mathcal{L}$ pulled back from $\overline{\mathcal{A}_g}$ to Spec $\mathcal{O}_F$ as metrized line bundles. Remember that in defining $h_F(A)$ (resp. $h_{\text{mod}}(A)$) the integral structure on ω_A (resp. on $\mathcal{L}$) is retrieved from $\widetilde{A} \to \operatorname{Spec} \mathcal{O}_F$ (resp. from $G \to \overline{\mathcal{A}_g}$). This compatibility suffices to draw the following conclusion.

Lemma 1.14. *Suppose that A is principally polarized and has semi-stable reduction. Then*

$$h_{\text{mod}}(A) = h_F(A).$$

Remark 1.15. For a semistable principally polarized abelian variety A, we want to define the Faltings height $h_F(A)$ as the "degree" of the classifying map

$$\operatorname{Spec} \mathcal{O}_K \longrightarrow \overline{\mathcal{A}_g}$$

for the Néron model $\mathfrak{A}/\mathcal{O}_K$. The issue is that $\operatorname{Spec} \mathcal{O}_K$ is not proper, so the usual notion of degree doesn't make sense. That's why we need Arakelov's insight.

Lemma 1.16. *Let K/F be a finite extension of number fields. For all principally polarized abelian varieties $A = A_F$ over F of dimension g, we have $h_F(A_F) \geqslant h_{\mathrm{mod}}(A_K)$.*

Proof. The characterization of Néron models gives a morphism of abelian $\mathcal{O}_K$-schemes

$$\mathfrak{A}_F \underset{\mathcal{O}_F}{\times} \mathcal{O}_K \to \mathfrak{A}_K,$$

inducing a canonical arrow between invertible $\mathcal{O}_K$-modules In turn, it induces an isomorphism on generic fibers, whence an isometry at each $v \mid \infty$. For each $v \nmid \infty$, we claim:

$$\|\ell\|_v \geqslant \|\Phi(\ell)\|_v \ , \ \ell \in \omega_{A_K} \underset{\mathcal{O}_F}{\otimes} K_v$$

with respect to integral structures on ω_{A_K} and $\omega_{A_F} \underset{\mathcal{O}_F}{\otimes} \mathcal{O}_K$. To see this, simply take ℓ to be a generator of ω_{A_K}, so that the left hand side is 1 and the right hand side is $\leqslant 1$ (being integral). Taking the sum of $-\log\|\cdot\|_v$, it follows that

$$[K:\mathbb{Q}]^{-1}\deg\omega_{A_K} \leqslant [K:\mathbb{Q}]^{-1}\deg\left(\omega_{A_F} \underset{\mathcal{O}_F}{\otimes} \mathcal{O}_K\right) = [F:\mathbb{Q}]^{-1}\deg\omega_{A_F}$$

as required. □

Theorem 1.17. *Let A be a principally polarized abelian variety over a number field F, we have $h_{mod}(A) \geqslant h_{geom}(A)$.*

Proof. There exists a finite extension $K \mid F$ such that A_K acquires semi-stable reduction. Then

$$h_{\mathrm{mod}}(A) \geqslant h_{\mathrm{mod}}(A_K) = h_{\mathrm{geom}}(A_K) = h_{\mathrm{geom}}(A),$$

where the last equation is a general property of Arakelov heights. □

1.4 Logarithmic singularities

In order to apply the Northcott property, we also need to study the singularities of the functions as they approach the boundary. To control the contributions at the finite primes, this has to be done over $\mathbb{Z}$, that's why we have worked with a compactification of moduli space over $\mathbb{Z}$.

We shall begin with the complex story. Let $\overline{X}$ be a compact complex analytic space, $Y \subset \overline{X}$ a closed subspace and $X := \overline{X}\backslash Y$.

Definition 1.18. A log-distance to Y is a function $\rho : X \to \mathbb{R}_{>0}$ such that, locally around each $y \in Y$, we have

$$\rho \approx -\log\sum_{i=1}^{r}|f_i|^2$$

where $f_1 = \cdots = f_r = 0$ is a system of local equations for Y around y.

Now let $\mathcal{L}$ be a line bundle over $\overline{X}$, equipped with an Hermitian metric $\|\cdot\|$ over X. In fact, we can always equip $\mathcal{L}$ with some $\|\cdot\|_0$ over all X, say by local trivializations and partition of unity.

Definition 1.19. We say that $(\mathcal{L}, \|\cdot\|)$ has logarithmic singularity along the boundary Y if there exists an Hermitian metric $\|\cdot\|_0$ on $\mathcal{L}$ over all $\overline{X}(\mathbb{C})$, such that

$$\max\left\{\frac{\|\cdot\|_0}{\|\cdot\|}, \frac{\|\cdot\|}{\|\cdot\|_0}\right\} = O\left(\rho^r\right)$$

near $Y(\mathbb{C})$, where $r \gg 0$ and ρ is some log-distance to Y.

It is routine but somewhat laborious to check that the notion above is invariant under pull backs, and can be checked "upstairs" under proper morphisms.

Now revert to the global setting. Let K be a number field.

Definition 1.20. Suppose that $\overline{X}$ is the base change to K of a proper $\mathcal{O}_K$-scheme $\overline{X}$, and $\overline{X}$ is projective. Let $\mathcal{L}$ be a line bundle over $\overline{X}$ with an $\mathcal{O}_K$-model. Consider an open K-subscheme $X \subset \overline{X}$. Suppose that we are given Hermitian metrics $\|\cdot\|_\iota$ on $\mathcal{L}_{\mathbb{C},l}$ for each $\iota : K \hookrightarrow \mathbb{C}$, of logarithmic singularity along $Y := \overline{X}\backslash X$. These data allow us to define

$$h_{\mathcal{L},\|\cdot\|}(x) := \deg x^*\mathcal{L}$$

Indeed, in computing $\deg x^*\mathcal{L}$, the integral structure is only used at non-Archimedean places, and the Hermitian metrics involve just $x : \text{Spec } K \to X$.

Theorem 1.21. *In the situation above, suppose $\mathcal{L}$ is ample. Then for all $d \in \mathbb{Z}_{\geqslant 1}$ and $B \in \mathbb{R}$, the set*

$$\left\{x \in X(L) : [L : K] \leqslant d, h_{\mathcal{L},\|\cdot\|}(x) \leqslant B\right\}$$

is finite.

Proof. To simply notation, we shall assume that there is only one Archimedean place for K. Take an Hermitian metric $\|\cdot\|_0$ for $\mathcal{L}_{\mathbb{C}}$ defined over $\overline{X}_{\mathbb{C}}$. Fix a projective embedding $\overline{X} \hookrightarrow \mathbb{P}^N$. Let $D \subset \mathbb{P}^N$ be a hypersurface containing Y. For every $\epsilon > 0$, take an Hermitian metric $\|\cdot\|_{D,\epsilon}$ on $\overline{X}_{\mathbb{C}}\backslash D_{\mathbb{C}}$ with the following asymptotic behavior near $D_{\mathbb{C}}$

$$\|\cdot\|_{D,\epsilon} \approx \|\cdot\|_0 \cdot |f|^{-\epsilon}$$

where f is a local equation for D. This is always possible. As polynomials dominate logarithms, we have

$$\|\cdot\| \ll_\epsilon \|\cdot\|_{D,\epsilon} \quad \text{on } X_{\mathbb{C}}\backslash D$$

Hence $h_{\mathcal{L},\|\cdot\|} \gg_\epsilon h_{\mathcal{L},\|\cdot\|_{D,\epsilon}}$ on $(X\backslash D)(\overline{\mathbb{Q}})$. Now take $n \in \mathbb{Z}_{\geqslant 1}$ and $\epsilon := \frac{1}{n}$. Note that $\|\cdot\|_0^n \cdot |f|^{-1}$ is an Hermitian metric for $\mathcal{L}^{\otimes n}(-D)$ over the whole $\overline{X}_{\mathbb{C}}$. Over $(\overline{X}\backslash D)(\overline{\mathbb{Q}})$ we have

$$n \cdot h_{\mathcal{L},\|\cdot\|_{D,1/n}} \approx h_{\mathcal{L}^{\otimes n},\|\cdot\|_0^n\cdot|f|^{-1}} = h_{\mathcal{L}^{\otimes n}(-D)} + \text{ bdd fcn on } \overline{X}(\overline{\mathbb{Q}})$$

Hence over $(X\backslash D)(\mathbb{Q})$ we have

$$h_{\mathcal{L},\|\cdot\|} \gg h_{\mathcal{L},\|\cdot\|_{D,1/n}} \geqslant \frac{1}{n}h_{\mathcal{L}^{\otimes n}(-D)} + \text{ bdd fcn on } \overline{X}(\overline{\mathbb{Q}})$$

Take $n \gg 0$ so that $\mathcal{L}^{\otimes n}(-D)$ is ample and $\left\{x \in \overline{X}(\overline{\mathbb{Q}}) : h_{\mathcal{L}^{\otimes n}(-D)}(x) \leqslant \text{const }\right\}$ is finite. Then $\left\{x \in (X\backslash D)(\overline{\mathbb{Q}}) : h_{\mathcal{L},\|\cdot\|}(x) \leqslant \text{const }\right\}$ is finite as well. Vary D to conclude. □

In order to apply h_F, the following result will be crucial.

Theorem 1.22. *Consider the line bundle $\mathcal{L}_m$ over $\mathcal{A}^*_{g,\mathbb{C}}$. The Hermitian form $(\cdot \mid)$ on $\mathcal{L}_m\big|_{\mathcal{A}_{g,\mathbb{C}}}$ has logarithmic singularity along the boundary.*

Proof. We only discuss the simplest case $g = 1$. Then $\mathcal{A}_g$ equals the modular curve $Y(1)$, and the $\mathbb{C}$-analytifications of $\mathcal{A}^*_g$ and $\overline{\mathcal{A}_g}$ both equal $X(1) = Y(1) \sqcup \{\infty\}$. It suffices to look at the vicinity of the cusp ∞, namely

$$\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ & 1 \end{smallmatrix}\right) \backslash \{\tau \in \mathbb{C} : \Im(\tau) > c\}, \quad c \gg 0$$

Each τ parameterizes the complex torus $E_\tau := \mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z})$ with its unique principal polarization. Let z be the standard coordinate function on E_τ. The line bundle ω is trivialized in this neighborhood of ∞ by the $\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ & 1 \end{smallmatrix}\right)$-invariant section $\mathrm{d}z$. Now compute the Hermitian form: we have

$$(\mathrm{d}z \mid \mathrm{d}z) = \sqrt{-1} \int_{E_\tau} \mathrm{d}z \wedge \overline{\mathrm{d}z} = 2\Im(\tau)$$

The local coordinate function around ∞ is $q := e^{2\pi\sqrt{-1}\tau}$. Note that $\log|q| = -2\pi\Im\tau$. The logarithmic singular behavior is thus evident.

For general g, the logarithmic singularity is checked "upstairs" on the toroidal compactifications $\overline{\mathcal{A}_g}$. This requires some knowledge about the local structure of toroidal compactifications over $\mathbb{C}$. For complete arguments, see [FC13, V.4.5 Proposition]. □

Theorem 1.23. *For every $g, d \in \mathbb{Z}_{\geqslant 1}$ and $B \in \mathbb{R}$, the set*

$$\left\{ \begin{array}{c|c} F: \textit{number field}, & [F:\mathbb{Q}] \leqslant d, \dim A = g \\ A: \textit{abelian variety over } F/\simeq & h_{\textit{mod}}(A) \leqslant B \\ \textit{principally polarized} & \end{array} \right\}$$

is finite.

Proof. This follows immediately from $h_{\mathrm{mod}}(A) \geqslant h_{\mathrm{geom}}(A)$ and the Northcott property for $h_{\widehat{\mathcal{L}}}$, as latter has logarithmic singularities along $\mathcal{A}^*_g \backslash \mathcal{A}_g$. □

One can use Proposition 1.7 and Zarhin's trick to remove the condition of principal polarization.

2 Tate Conjecture

It's known that an abelian variety A over $\mathbb{C}$ can be determined by $H^1(A,\mathbb{Z}) = \Lambda$. To construct analogues of Λ in the characteristic $p > 0$ case, there are no analytic tools at this point, so we consider analogues of $\Lambda \otimes \mathbb{Z}_l$ and define the Tate module $T_lA = \varprojlim_n A\left[l^n\right]$ for every prime l. If $l \neq p$, then $T_lA \cong \left(H^1_{et}(A_{\bar{k}}, \mathbb{Z}_l)\right)^*$ as a Galois representation.

If $l = p$, one idea is to put $G_n = A\left[p^n\right]$ as a finite p-group scheme. Over a perfect field k of characteristic p, the crystal cohomology group $H^1_{cris}(A/W(k))$ canonically isomorphic to the D-module $D(A[p^\infty])$ corresponding to the p-divisible group $A[p^\infty]$.

After a basic introduction of p-divisible groups, in §2.2 we will show that $h(A/G_n)$ is eventually constant as a function of n, from which a sequence can be constructed to prove the Tate conjecture in §2.3. We won't use the above cohomology theory, but a result about the Hodge-Tate decomposition will appear in §2.2.

2.1 p-divisible groups

Let R be a commutative ring.

Definition 2.1. A finite (flat) group scheme over R is a scheme $\Gamma = \operatorname{Spec} A$, where A is a locally free R-module of finite rank, and Γ has the structure of a group scheme. If A has rank m over R, we say Γ is of order m, and denote $\operatorname{ord}\Gamma = m$.

We will always assume them to be commutative.

Example 2.2. If Γ is a usual finite abelian group of order n, we can construct a finite flat group scheme $\Gamma = \operatorname{Spec} A$ of order n, by setting A to be the ring of R-valued functions on Γ. Then, the comultiplication is given by identifying $A \otimes_R A$ with R-valued functions on $\Gamma \times \Gamma$, so the comultiplication map $\mu : A \to A \otimes_R A$ can be defined by $\mu(f)(s,t) = f(st)$.

Now let R be a local, complete, Noetherian ring with residue field k. Then, given $G = \operatorname{Spec} A$, we define $G^{\text{ét}} = \operatorname{Spec} A^{\text{ét}}$, where $A^{\text{ét}} \hookrightarrow A$ is the maximal étale subalgebra of A. Then, there is a faithfully flat surjection $\operatorname{Spec} A \to \operatorname{Spec} A^{\text{ét}} \to 0$, and letting $G^0 = \ker\left(\operatorname{Spec} A \to \operatorname{Spec} A^{\text{ét}}\right) = \operatorname{Spec} A^0$ where A^0 is the local quotient of A such that the coidentity $A \to R$ factors through A^0, we see that G^0 is connected, and we have a short exact sequence

$$0 \longrightarrow G^0 \xrightarrow{i} G \xrightarrow{j} G^{\text{ét}} \longrightarrow 0$$

Grothendick's Galois theory asserts that the functors $G \mapsto G^0$ and $G \mapsto G^{\text{ét}}$ are both exact. G is connected if and only if $G = G^0$. In this case, $\operatorname{ord} G$ is a power of the residue field characteristic. Thus, if k is of characteristic 0, then every finite flat group scheme is étale; see [Lip].

From now, R is a complete Noetherian local ring with residue field k of chracteristic $p > 0$.

Definition 2.3. A p-divisible group over R of height $h \geqslant 0$ is an inductive system (G_ν, i_ν) of (commutative) finite flat group schemes over R, such that

(i) Each G_ν is a finite group of order $p^{\nu h}$;

(ii) For every $\nu \geqslant 0$, there exists an exact sequence

$$0 \longrightarrow G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{p^\nu} G_{\nu+1}.$$

Remark 2.4. This is the scheme-theoretic analogue of the fact that in the world of abelian groups, letting $G_\nu = \mathbb{Z}/p^v$, we have $\varprojlim G_\nu = \mathbb{Q}_p$.

By iteration, there exists a closed immersion $i_{\nu,\mu} : G_\nu \to G_{\nu+\mu}$, which fits into the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & G_\nu \arrow[r, "i_{\nu,\mu}"] & G_{\nu+\mu} \arrow[r, "p^\nu"] \arrow[dr, dashed, "j_{\nu,\mu}"'] & G_{\nu+\mu} \\
& & & G_\mu \arrow[u, hook, "i_{\mu,\nu}"']
\end{tikzcd}$$

for all $v, \mu \geqslant 0$, and so there is a short exact sequence

$$0 \longrightarrow G_\nu \xrightarrow{i_{\nu,\mu}} G_{\nu+\mu} \xrightarrow{j_{\nu,\mu}} G_\mu \longrightarrow 0.$$

Example 2.5. If A is an abelian variety (or abelian scheme) over R, then $A \xrightarrow{p^\nu} A$ and $A\left[p^\nu\right] = \ker\left(p^\nu\right)$ give a divisible group denoted by $A[p^\infty]$.

Definition 2.6. An n-dimensional formal Lie group over R is a family $F = \left(F_i(\vec{X}, \vec{Y})\right)$ of n power series in $2n$ variables (so $F_i(\vec{X}, \vec{Y}) \in R[\![X_1, \ldots, X_n, Y_1, \ldots, Y_n]\!]$) that satisfies the axioms:

(i) $X = F(X, 0) = F(0, X)$;

(ii) $F(X, Y) = F(Y, X)$;

(iii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

Even though X and Y are strictly speaking vectors, we will usually suppress the vector notation.

By (i) and (ii), we get that $F(X, Y) = X + Y +$ higher order terms. In particular, $F_i(\vec{X}, \vec{Y}) = X_i + Y_i +$ higher order terms.

Definition 2.7. We define $X * Y = F(X, Y)$, and

$$\underbrace{X * X * \cdots * X}_{m \text{ times}} = [m]X.$$

Using this definition, $[m]$ defines a homomorphism $F \to F$, that is, we have the equality

$$[m](F(X, Y)) = F([m]X, [m]Y)$$

and $[m]$ corresponds to a ring homomorphism

$$R[\![X_1, \ldots, X_n]\!] \xrightarrow{\psi} R[\![X_1, \ldots, X_n]\!],$$

where $\psi\left(X_i\right)$ is the i th coordinate of $[m]X$.

Definition 2.8. If Γ is a formal Lie group with $F(X,Y)$ a formal group law, we say Γ is divisible if $[p]$ is an isogeny, that is,

$$R[\![X_1,\dots,X_n]\!] \xrightarrow{\psi} R[\![X_1,\dots,X_n]\!]$$

makes $R[\![X_1,\dots,X_n]\!]$ into a free module of finite rank over itself.

The following is very important, and we will use it.

Proposition 2.9. *If Γ is divisible, then $\Gamma_p := \operatorname{Spec} A$ where $A := \frac{R[\![X_1,\dots,X_n]\!]}{(\psi(X_i))}$ is a connected finite flat group scheme over R.*

Proof. First, the formal group law induces a comultiplication and group scheme structure on Γ_p, since the formal group law can be thought of as a map $R[\![\vec{X}]\!] \to R[\![\vec{Y},\vec{Z}]\!]$, and modding out by $\psi\left(X_i\right)$ induces a comultiplication.

Next, $R[\![X_1,\dots,X_n]\!] \xrightarrow{\psi} R[\![X_1,\dots,X_n]\!]$ gives the target a finite free module structure over itself, hence $R \hookrightarrow A$ is a finite extension.

Finally, we claim A is local (and hence Γ_p is connected). Denote $\mathfrak{m}$ to be the maximal ideal of R. Since $R \overset{\phi}{\hookrightarrow} A$ is finite, it is integral, and so it satisfies Going-Up. This implies $\phi^{-1}(\max) = \mathfrak{m}$, and so every maximal ideal of A contains pA. Now $[p]X = pX+$ higher order terms. This implies that X is in every maximal ideal of A. Thus, A has a unique maximal ideal.

Setting $\Gamma_\nu = \operatorname{Spec} A_\nu$ where $A_\nu = R[\![X_1,\dots,X_n]\!]/\left(\psi^\nu\left(X_i\right)\right)$ form an inductive system, so these Γ_ν form a p-divisible group $\Gamma(p)$, where each Γ_ν is connected. □

Proposition 2.10. *The functor $\Gamma \to \Gamma(p)$ which sends divisible formal Lie groups over R to connected p-divisible groups over R is an equivalence of categories.*

We won't have time to go through this proof carefully. Full-faithfulness follows by the fact that R is p-adically complete. Essential surjectivity is the harder part: the idea is to create a projective system of rings that end up being a power series ring.

Definition 2.11. If G is any p-divisible group over $R, G = (G_\nu, i_\nu)$, we can define

$$0 \longrightarrow G_\nu^0 \xrightarrow{i} G_\nu \xrightarrow{j} G_\nu^{\text{ét}} \longrightarrow 0$$

and we can define a new p-divisible group $\left(G_\nu^0, i_\nu\right) =: G^0$, a connected p-divisible group. Similarly, we can define $G^{\text{ét}} = \left(G_\nu^{\text{é}}, \cdot\right)$. We define the dimension of $\left(G_\nu^0, i_\nu\right)$ to be the dimension of its associated formal Lie group, and define $\dim G = \dim G^0$.

2.2 Computation of Faltings height

"Although p-divisible groups are interesting enough in their own right, our main motivation for studying them has been their applications to abelian varieties. " [Tat67]

Let K be a number field, and let A/K be an abelian variety. We fix $G \subset A\left[\ell^\infty\right]$ an ℓ-divisible group, where we denote $G_n = G\left[\ell^n\right]$, and $A_n = A/G_n$. Each isogeny $A \to B_n$ extends to an isogeny $\widetilde{A} \to \widetilde{B}_n$ over $\mathcal{O}_K$ with kernel $\mathcal{G}_n$ (the Zariski closure of G_n in the Néron model).

Remark 2.12. We can assume $\mathcal{G} = \{\mathcal{G}_n\}_n$ is an ℓ-divisible group. This is valid if $\widetilde{A}$ is proper. Otherwise, we study $\mathcal{G}_{n,v} := \mathcal{G}_n \underset{\mathcal{O}_K}{\otimes} \mathcal{O}_v$ for each place v dividing ℓ (essentially by the Chinese remainder theorem), whose maximal proper subgroup has a finite subgroup scheme such that the quotient gives rise to an ℓ-divisible group. See [Lev] for details.

Using the formula for change of Faltings height under isogeny, we have

$$h(A_n) - h(A) = \log\left(\left|s^*\Omega^1_{\mathcal{G}_n/\mathbb{Z}_\ell}\right|^{\ell - \frac{1}{2}nh}\right),$$

where $h = \mathrm{ht}(\mathcal{G})$.

Remind ourselves of the definition of the discriminant.

Definition 2.13. Let $R \hookrightarrow A$ be a R-algebra homomorphism that realizes A as a finite R-module. Then, $\mathrm{disc}(A/R)$ is the ideal of R generated by $\det\left(\mathrm{Tr}\left(\alpha_i\alpha_j\right)_{ij}\right)$ for any basis $\alpha_1, \ldots, \alpha_n \in A$, where n is the rank of A over R.

To comppute $\left|s^*\Omega^1_{\mathcal{G}_n/\mathbb{Z}_\ell}\right|$, we will use following result:

Proposition 2.14. *If $G = (G_\nu, i_\nu)$ is a p-divisible group of height h over R, and $G_\nu = \operatorname{Spec} A_\nu$ where A_ν is a R-module via a finite map $R \hookrightarrow A_\nu$, the discriminant ideal* $\mathrm{disc}\,(A_\nu/R)$ *is generated by $p^{\nu n p^{h\nu}}$, where $n = \dim G$.*

Proof. Let G be a p-divisible group, and consider the short exact sequence

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 0,$$

where $G = (G_\nu, i_\nu)\,, G_\nu = \operatorname{Spec} A_\nu$, and for all ν, we have

$$0 \longrightarrow G^0_\nu \longrightarrow G_\nu \longrightarrow G^{\text{ét}}_\nu \longrightarrow 0.$$

Since the discriminant behaves well with short exact sequences (i.e., if $0 \to H' \to H \to H'' \to 0$ is a short exact sequence of finite flat group schemes over R, we have $\mathrm{disc}(H) = \mathrm{disc}(H')^{\mathrm{ord}(H'')} \cdot \mathrm{disc}(H'')^{\mathrm{ord}(H')}$), we may assume G_ν is connected. This is because the discriminant of $G^{\text{ét}}$ is 1 (the discriminant measures ramification).

Now let $G_\nu = \operatorname{Spec} A_\nu$ be connected, so that there exists a corresponding divisible formal Lie group Γ such that $A_\nu \simeq R[\![X_1, \ldots, X_n]\!]/\left(\psi^\nu\left(X_i\right)\right)$, where n is the dimension of G. From now on, denote $A = R[\![X_1, \ldots, X_n]\!]$, and denote A' to be the copy of A such that there is a finite injection $A' \overset{\phi}{\hookrightarrow} A$, where $\phi = \psi^\nu$. It therefore suffices to show that $\mathrm{disc}\,(A/A') = p^{n\nu p^{h\nu}}$.

For $A' \overset{\phi}{\hookrightarrow} A$, take Ω to be the formal module of differential forms on A, and Ω' that on A'.Ω is a free A-module generated by dX_i, and dX'_i generate Ω'. Then, $\Lambda^n\Omega$ is free of rank 1 over A, with generator θ, and $\bigwedge^n \Omega'$ is free of rank 1 over A', with generator θ'. We then have $d\psi^\nu : \bigwedge^n \Omega' \to \bigwedge^n \Omega$ defined by $\theta' \mapsto a\theta$ for some a. We claim that $a = p^{n\nu}$. This follows since Ω has a basis of invariant differential forms ω_i, and similarly Ω' has one with ω'_i, where invariance means that if $A \overset{\epsilon}{\hookrightarrow} A\hat{\otimes}A$ defines a group law $\epsilon_*\left(\omega_i\right) = \omega_i \otimes \omega_i$. Claim. $d\psi^\nu\left(\omega'_i\right) = p^\nu\omega_i$. The idea is that $d\psi^\nu\left(\omega'_i\right) = \omega_i \circ [p]^\nu$, and so taking a derivative gives the correct number of powers of p. The final step uses the trace map $\mathrm{Tr} : \Lambda^n\Omega \to \Lambda^n\Omega'$, which satisfies the following properties:

1. Tr is A'-linear;
2. $\alpha \mapsto [\omega \mapsto \mathrm{Tr}(\alpha\omega)]$ gives an A'-module isomorphism $A \xrightarrow{\sim} \mathrm{Hom}_A\left(\bigwedge^n \Omega, \bigwedge^n \Omega'\right)$;
3. for all $\alpha \in A$, and all $\omega' \in \bigwedge^n \Omega'$, the equation
$$\mathrm{Tr}\left(\alpha d\psi^\nu\left(\omega'\right)\right) = \mathrm{Tr}_{A/A'}(\alpha)\cdot\omega'$$
holds.

Finally, $\mathrm{Tr}\left(\alpha p^{n\nu}\theta'\right) = \mathrm{Tr}_{A/A'}(\alpha)\theta'$ so $p^{n\nu}\,\mathrm{Tr}\left(\alpha\theta'\right) = \mathrm{Tr}_{A/A'}(\alpha)\theta'$ by A'-linearity, which implies $\mathrm{Tr}_{A/A'}(\alpha) \in (p^{n\nu})$. We conclude that $\operatorname{disc}\left(A_\nu/R\right) \subseteq p^{n\nu p^{h\nu}}$.

For the reverse inclusion, we use that $\operatorname{disc}\left(A_\nu/R\right) = \mathrm{Norm}_{A_\nu/R}\left(\mathcal{D}_{A_\nu/R}\right)$, where $\mathcal{D}$ is the differential ideal. We would then need to show $p^{n\nu} \in \mathcal{D}^*_{A_\nu/R}$. □

We also need a general result about connected finite flat group schemes.

Lemma 2.15. *Suppose $H/\mathbb{Z}_\ell$ is a connected finite flat group scheme. Then,*
$$\left|s^*\Omega^1_{H/\mathbb{Z}_\ell}\right|^{\#H} = \left|\mathbb{Z}_\ell/\operatorname{disc}(H)\right|.$$

Proof. Let $H = \operatorname{Spec} R$, where R is a finite local $\mathbb{Z}_\ell$-algebra; note it is local since H is connected. Then, we have a homomorphism $R \to \mathbb{Z}_\ell$ corresponding to $0 \in H\left(\mathbb{Z}_\ell\right)$. Let $I \subset R$ be its kernel. Then,
$$I/I^2 = s^*\Omega^1_{H/\mathbb{Z}_\ell}.$$
We have an isomorphism $\Omega^1_{H/\mathbb{Z}_\ell} \cong R \otimes_{\mathbb{Z}_\ell} I/I^2$, since $\Omega^1_{H/\mathbb{Z}_\ell}$ has a basis of translation-invariant one-forms, which we can think of as coming from I/I^2 (since H is connected). As a $\mathbb{Z}_\ell$-module, $R \cong \mathbb{Z}_\ell^{\#H}$, and so as a group, $\left|\Omega^1_{H/\mathbb{Z}_\ell}\right| = \left|I/I^2\right|^{\#H} = \left|s^*\Omega^1_{H/\mathbb{Z}_\ell}\right|^{\#H}$. We then have that
$$\left|\Omega^1_{H/\mathbb{Z}_\ell}\right| = \left|\mathbb{Z}_\ell/\operatorname{disc}(H)\right|.$$
□

Let $\mathcal{G}_n^0$ be the connected part of $\mathcal{G}_n$. Then,
$$s^*\Omega^1_{\mathcal{G}_n/\mathbb{Z}_\ell} = s^*\Omega^1_{\mathcal{G}_n^0/\mathbb{Z}_\ell},$$
which implies
$$\left|s^*\Omega^1_{\mathcal{G}_n/\mathbb{Z}_\ell}\right| = \left|s^*\Omega^1_{\mathcal{G}_n^0/\mathbb{Z}_\ell}\right| = \left|\mathbb{Z}_\ell/\operatorname{disc}\left(\mathcal{G}_n^0\right)\right|^{1/\#\mathcal{G}_n^0} = \left(\ell^{dn\#\mathcal{G}_n^0}\right)^{1/\#\mathcal{G}_n^0} = \ell^{dn},$$
where the second equality is by Lemma 2.15, and the third is by Tate's theorem (Proposition 2.14), which says that $\operatorname{disc}\left(\mathcal{G}_n^0\right) = \ell^{dn\#\mathcal{G}_n^0}$, where d is the dimension of the formal group of $\mathcal{G}^0$.

To show $\ell - \frac{1}{2}nh$ is zero, the next step is to introduce a third invariant k from the Tate module of $\mathcal{G}$.

Definition 2.16. Let G be a p-divisible group over R or K. Then the Tate module of G is
$$T(G) = \varprojlim G_n(\overline{K}),$$

where the maps are induced by multiplication by p; this is a finite free $\mathbb{Z}_p$-module equipped with a continuous action of the Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$.

Let $K/\mathbb{Q}_\ell$ be a finite extension, and denote $\mathbb{C}_\ell = \widehat{\overline{K}}$. The Galois action on $\overline{K}$ extends by continuity on $\mathbb{C}_\ell$. Define $\mathbb{C}_\ell(i)$ to be $\mathbb{C}_\ell$ equipped with the twisted Galois action given by

$$\sigma.x = \chi_\ell^i(\sigma) * \sigma(x).$$

Definition 2.17. Let V be a continuous representation of G_K, where V is a finite dimensional $\mathbb{Q}_\ell$-vector space. Then, we say V is Hodge-Tate if

$$V \otimes_{\mathbb{Q}_\ell} \mathbb{C}_\ell \cong \bigoplus_{n\in\mathbb{Z}} \mathbb{C}_\ell(n)^{\oplus h(n)}$$

for some $h(n) \in \mathbb{Z}$, where G_K acts on each factor on the left, and (n) denotes Tate twist. The n such that $h(n) \neq 0$ are called Hodge-Tate weights, which we say occur with multiplicity $h(n)$.

Proposition 2.18. *Let V be a Hodge-Tate representation, then $\det(V)$ is Hodge-Tate with the unique weight.*

Proof. If $V \otimes_{\mathbb{Q}_\ell} \mathbb{C}_\ell \cong \oplus_i \mathbb{C}_\ell(i)^{h_i}$, then clearly $\det(V) \otimes \mathbb{C}_\ell \cong \det(V \otimes \mathbb{C}_\ell) \cong \mathbb{C}_\ell\left(\sum_i ih_i\right)$. □

By Hodge-Tate decomposition for p-divisible groups [Tat67, §4, Cor. 2], the representation $V_\ell(G)|_{G_{\mathbb{Q}_\ell}}$ is Hodge-Tate with weights 0,1 . The multiplicity of the weight 1 is d, the dimension of G. Writing this out, we have

$$V_\ell(G) \otimes \mathbb{C}_\ell = \mathbb{C}_\ell(0)^{\oplus h(0)} \oplus \mathbb{C}_\ell(1)^{\oplus d}$$

and so the determinant $\det(V_\ell(G))$ has Hodge-Tate weight d.

Remark 2.19. Here we can also use the Hodge-Tate decomposition for abelian varieties, see [B B, §5 & §7].

Proposition 2.20. *Let $\alpha : G_{\mathbb{Q}} \to \mathbb{Q}_\ell^*$ be a continuous character which ramifies at only finitely many places, such that $\alpha|_{G_{\mathbb{Q}_\ell}}$ is Hodge-Tate of weight k. Then, $\alpha = \psi\chi_\ell^k$, where $\psi : G_{\mathbb{Q}} \to \mathbb{Q}_\ell^*$ has finite order.*

Proof. First, we may replace α with $\frac{\alpha}{\chi_\ell^k}$, so now $\alpha|_{G_{\mathbb{Q}_\ell}}$ has weight zero. Thus, $\alpha|_{I_{\mathbb{Q}_\ell}}$ is of finite order. Then, since $\mathbb{Q}_\ell^*$ is abelian, α factors to give a character $\alpha : G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathbb{Q}_\ell^*$, where by class field theory,

$$G_{\mathbb{Q}}^{\mathrm{ab}} = \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times,$$

where each factor at p is the inertial group at p. By assumption, since α ramifies at only finitely many places, α factors through some quotient of the form $\prod_{p|N} \mathbb{Z}_p^\times$ for some N. So we know that $\alpha|_{\mathbb{Z}_\ell}$ is of finite order by the Hodge-Tate condition. It is also true that $\alpha|_{\mathbb{Z}_\ell}$ is of finite order for $p \neq \ell$, since any homomorphism $\mathbb{Z}_p^\times \to \mathbb{Q}_\ell^\times$ is of finite order. Finally, this implies that α is of finite order. □

Proposition 2.19 implies that the determinant $\alpha := \det(V_\ell) = \psi\chi_\ell^k$, where k is the weight of $\alpha|_{G_{\mathbb{Q}_\ell}}$, and ψ is of finite order.

Finally, we need to show that $h = 2d$. So far, we haven't used the global information; this is where it is used, in the form of the Riemann hypothesis part of the Weil conjectures for abelian varieties.

The Tate module $V_\ell(G) \subset V_\ell(A)$ is a h-dimensional $G_{\mathbb{Q}}$-subrepresentation, where $h = \mathrm{ht}(G)$. Now let $p \neq \ell$ be a prime of good reduction for A. Then, $V_\ell(A)$ is unramified at p, and so $V_\ell\left(A_{\mathbf{F}_p}\right)$ is a representation of $G_{\mathbf{F}_p} = \langle \mathrm{Frob}_p \rangle$. This representation is semisimple, and the eigenvalues of Frobenius are Weil numbers of weight 1 (that is, $|\cdot| = p^{1/2}$ under any complex embedding). The same statement is true for $V_\ell(G)$, which is a subrepresentation. Thus, $\det\left(V_\ell(G)\right)$ Frobenius acts by a weight h Weil number, and so

$$|\alpha\left(\mathrm{Frob}_p\right)| = p^{h/2}.$$

On the other hand, we know that

$$|\alpha\left(\mathrm{Frob}_p\right)| = |\psi\left(\mathrm{Frob}_p\right)| \cdot |\chi_\ell\left(\mathrm{Frob}_p\right)|^k = p^k,$$

and so $k = \frac{1}{2}h$.

2.3 Tate modules for abelian varieties

The key result we will prove latter:

Proposition 2.21. *If A is an abelian variety over a number field K, and $W \subset V_\ell(A)$ is a subrepresentation of the rational Tate module, then there exists $u \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ such that $u\left(V_\ell(A)\right) = W$.*

It suffices to prove the following two important theorems:

Theorem 2.22 (Semisimplicity of the Tate module)**.** *If A is an abelian variety over K, then $V_\ell(A)$ is a semisimple G_K-representation.*

Proof. Denote

$$E_\ell := \mathrm{End}_K(A) \otimes \mathbb{Z}\mathbb{Q}_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}\left(V_\ell(A)\right).$$

Let $W \subset V_\ell(A)$ be G_K-semistable; it suffices to show that there exists a G_K-stable complement W'. The right ideal

$$\mathfrak{a} := \{u \in E_\ell \mid u\left(V_\ell(A)\right) \subset W\} \subset E_\ell,$$

is principally generated by some element u_0 such that $u_0^2 = u_0$, as are all right ideals in semisimple algebras [Lev11, Prop. 4.4]. Now since there exists $u \in E_\ell$ such that $u\left(V_\ell(A)\right) = W$, we have that

$$u_0\left(V_\ell(A)\right) = u_0 E_\ell\left(V_\ell(A)\right) = \mathfrak{a}\left(V_\ell(A)\right) = W$$

so u_0 is a projection operator on $V_\ell(A)$ with image W. Thus, $1 - u_0$ is a projection operator onto a direct complement W' of W, and $V_\ell(A)$ is therefore semisimple. □

Remark 2.23. The fact that all right ideals in a semi-simple algebra over a field k are principal is [Lev11, Prop. 4.4], and goes as follows. By decomposing the semi-simple algebra, you reduce to the case of central simple algebras over k. This is isomorphic to a matrix algebra $\mathrm{Mat}_n(D)$ for some central division algebras D over k. In this case, you can do an explicit matrix analysis.

Theorem 2.24 (Faltings's isogeny theorem)**.** *If A and B are two abelian varieties over K, then the natural map*

$$\mathrm{Hom}_K(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{G_K}(T_\ell(A), T_\ell(B)) \tag{$\star$}$$

is an isomorphism for all primes ℓ.

Proof. We just have to show the natural map

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \longrightarrow \mathrm{End}_{G_K}(V_\ell(A)) \tag{$\star\star$}$$

is a surjection. Injectivity in ($\star$) holds in general, so it suffices to show it is surjective. The morphism ($\star$) is surjective if and only if ($\star$) $\otimes\, \mathbb{Q}_\ell$ is surjective since $\mathrm{cok}(\star)$ is torsion-free. To replace Hom with End, we apply the endomorphism statement with $A \times B$ replacing A.

Let C be the centralizer of E_ℓ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. The centralizer C° of C equals E_ℓ by the double centralizer theorem [Jac89, Thm. 4.10], since E_ℓ is a semisimple algebra.

Now let $\alpha \in \mathrm{End}_{G_K}(V_\ell(A))$; we want to show that $\alpha \in C^\circ$. Consider any $d \in C$. Then, $d \oplus d$ commutes with everything in $\mathrm{End}_K(A \times A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. In particular, by proposition 2.20, there exists $u \in \mathrm{End}_K(A \times A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ such that

$$u\,(V_\ell(A \times A)) = \{(x, \alpha x) \in V_\ell(A \times A)\} =: W,$$

and $(d \oplus d)$ commutes with u. By applying $(d \oplus d)$ to both sides of this equation, we have $(d \oplus d)W \subset W$, which implies $d\alpha = \alpha d$, i.e., $\alpha \in C^\circ$. Thus, ($\star\star$) is surjective. □

Now we proceed to prove proposition 2.20.

Proposition 2.25. *Let A be an abelian variety over K. If proposition 2.20 holds for $A_L = A \times_K L$, where L is a finite extension of K, it holds for A.*

Proof. Let $W \subset V_\ell(A)$ be a G_K-invariant subspace, so there exists $u \in \mathrm{End}_L(A) \otimes \mathbb{Z}\mathbb{Q}_\ell$ such that $u\,(V_\ell(A)) = W$. Choose representatives $\{\sigma_i\} = G_K/G_L$, and let

$$u' = \frac{1}{[L:K]} \sum_i \sigma_i(u).$$

Since W is G_K-invariant, each $\sigma_i(u)$ satisfies the same property as u, and thus, so does u'. Galois descent of morphisms then implies $u' \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$. □

Proposition 2.26. *For m coprime to ℓ, there exists a finite field extension L of K such that every A_n has level m-structure.*

Proof. It suffices to produce level m-structure on A, since the m-torsion parts of A_n are isomorphic to those of A. But this happens we know after base extension to $\overline{K}$, so base changing to the fixed field L of the kernel of the representation

$$G_K \longrightarrow \mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$$

defined by acting on $A_{\overline{K}}[m]$ suffices, since the degree of the field extension L/K is bounded above by $|\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})|$. □

Proof of Proposition 2.20. Let $W \subset V_\ell(A)$ be a G_K-invariant subspace. Then, letting $U := W \cap T_\ell(A)$, for $n \geqslant 1$ we can define an ℓ-divisible subgroup $G \subset A\left[\ell^\infty\right]$ with levels

$$U/\ell^n U \hookrightarrow T_\ell(A)/\ell^n T_\ell(A) = A\left[\ell^n\right]\left(\overline{K}\right)$$

which is actually defined over K since W is G_K-invariant. We can then consider the subgroups $G_n = G\left[\ell^n\right]$ and the quotients $A_n = A/G_n$ appearing in Theorem α. Since A has semistable reduction, the Faltings height $h\left(A_n\right)$ of the A_n are bounded uniformly by some constant C. By Theorem 1.23, this implies there is a sequence $n_1 < n_2 < \cdots$ such that $A_{n_i} \cong A_{n_j}$. We then define isogenies

$$u_i : A \xrightarrow{f_{n_1}^{-1}} A_{n_1} \underset{\sim}{\xrightarrow{v_i}} A_{n_i} \xrightarrow{f_{n_i}} A,$$

where we note f_{n_i} is of order $\ell^{n_i \dim X}$, and satisfies

$$f_{n_i}\left(T_\ell\left(A_n\right)\right) = W \cap T_\ell(A) + \ell^n T_\ell(A) =: X_n.$$

Viewed in $\mathrm{End}_{\mathbb{Q}_\ell}\left(V_\ell(A)\right)$, each u_i maps X_{n_1} onto $X_{n_i} \subset X_{n_1}$, since

$$u_i\left(X_{n_1}\right) = u_i f_{n_1}\left(T_\ell\left(A_{n_1}\right)\right) = f_{n_i} v_i T_\ell\left(A_{n_1}\right) = f_{n_i} T_\ell\left(A_{n_i}\right) = X_{n_i}.$$

Since by definition $X_{n_i} \subset X_{n_1}$, this says the u_i all preserve the lattice X_{n_1} in $T_\ell(A)$. Thus, the u_i all lie in a compact subspace $\mathrm{End}_{\mathbb{Z}_\ell}\left(X_{n_1}\right) \cap E_\ell \subset E_\ell := \mathrm{End}_K(A) \otimes \mathbb{Z}\mathbb{Q}_\ell$. By compactness, passing to a subsequence of the n_i, the sequence u_i converge to a limit $u \in \mathrm{End}_{\mathbb{Z}_\ell}\left(X_{n_1}\right) \cap E_\ell$. Now consider

$$U := W \cap T_\ell(A) = \bigcap_{i \in I} X_{n_i}.$$

Since $u_i\left(T_{n_1}\right) = T_{n_i}$, every $x \in U$ is a limit $\lim_{i \in I} u_i\left(x_i\right)$ of $x_i \in T_{n_1}$. Passing to a convergent subsequence x_j of these x_i gives that x is the limit of $u\left(\lim_{j \in J} x_j\right)$, and so $u\left(T_\ell(A)\right) = W \cap T_\ell(A)$, and so $u\left(V_\ell(A)\right) = W$. □

Corollary 2.27. *Let A_1, A_2 be abelian varieties over K. Then, the following are equivalent:*

(i) *A_1 and A_2 are isogenous;*

(ii) *For all $\ell, V_\ell\left(A_1\right) \cong V_\ell\left(A_2\right)$ as G_K-modules;*

(iii) *For some $\ell, V_\ell\left(A_1\right) \cong V_\ell\left(A_2\right)$ as G_K-modules.*

Proof. $(i) \Leftarrow (ii)$. Note that $f : A_1 \to A_2$ is an isogeny if and only if $T_\ell(f)$ has full rank, i.e., $\det T_\ell(f) \neq 0$.

$(ii) \Rightarrow (iii)$ is clear.

$(iii) \Rightarrow (i)$. Suppose $\varphi : V_\ell\left(A_1\right) \rightarrow V_\ell\left(A_2\right)$ is an isomorphism of G_K-modules. Choose n such that $\ell^n \varphi \in \operatorname{Hom}\left(T_\ell\left(A_1\right), T_\ell\left(A_2\right)\right)$. By the isogeny theorem, this comes from $\operatorname{Hom}_K\left(A_1, A_2\right) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, and can be approximated by elements of $\operatorname{Hom}_K\left(A_1, A_2\right)$. Since $\det\left(\ell^n \varphi\right) \neq 0$, these approximations will also have nonvanishing determinant, and this way you can get an isogeny. □

Corollary 2.28. *Let A be an abelian variety over K. Then, there are only finitely many isomorphism classes of abelian varieties B over K such that for all $\ell, T_\ell(A) \cong T_\ell(B)$.*

Sketch of proof. By assumption and the isogeny theorem, there exists an isogeny $A \rightarrow B$ with degree prime to ℓ for all ℓ. As before, we can freely extend the ground field, and therefore assume A and all B 's have semistable reduction and have level structure. By choosing the isogenies above correctly, there exists an N such that for every prime number ℓ and all B, there exist isogenies $\phi : A \rightarrow B$ for which the greatest power of ℓ in deg ϕ divides N (see [Fal+86, V, Lem. 3.2]). Finally, it's easy to see that $\left|s^* \Omega^1_{\mathcal{G}/\mathcal{O}_K}\right|$ is divisible by primes only dividing $\deg(\phi)$ because $\mathcal{G}$ is a commutative group scheme killed by $\deg(\phi)$, so

$$\exp(2[K : \mathbb{Q}] \cdot (h(B) - h(A))) \in \mathbb{Q},$$

whose numerator and denominator divide a certain power of N. Applying Theorem 1.23, we are done. □

3 Shafarevich Conjecture

3.1 The proof of Shafarevich Conjecture

Conjecture 3.1 (Shafarevich Conjecture)**.** *Let S be a finite set of places of $K, d > 0$. There are only finitely many isomorphism classes of abelian varieties over K of a given dimension, which have good reduction outside of S.*

By Corollary 2.25, we just have to show following theorem.

Theorem 3.2. *Let S be a finite set of places of number field K. Then there are only finitely many isogeny classes of abelian varieties of a given dimension g with good reduction outside S.*

Passing to Tate modules, the problem reduces to the finiteness principle for rational semisimple ℓ-adic representations:

Theorem 3.3. *Let K be a number field and S a finite set of primes of K. Then there are finitely many isomorphism classes of rational, semisimple ℓ-adic representations of G_K of dimension d which are unramified outside of S.*

Lemma 3.4. *There exists a finite set T of primes of K (depending on S and d) satisfying the following two properties:*

1. *T is disjoint from $S_\ell := S \cup \{v \mid \ell\}$.*

2. *Two representations $\rho_1, \rho_2 \in \operatorname{Rep}_S(G_K, d)$ are isomorphic if and only if*

$$\operatorname{trace}(\rho_1(\operatorname{Frob}_v)) = \operatorname{trace}(\rho_2(\operatorname{Frob}_v)), \quad \textit{for all } v \in T.$$

Proof. Consider the set of all extensions of K of degree $\leqslant l^{2d^2}$ which are unramified outside S_ℓ. By the Hermite-Minkowki Theorem, there are finitely many such extensions, and hence their compositum L is a finite extension of K. Let $T = \{v_1, \ldots v_N\}$ be a set of primes of K which are not in S and such that the Frobenius conjugacy classes $\operatorname{Frob}_{v_i}$ generate $\operatorname{Gal}(L/K)$. The existence of such a finite set follows from the Chebotarev density theorem. We claim that this set T satisfies the conclusion of Lemma 3.3. Given $\rho_1, \rho_2 \in \operatorname{Rep}_S(G_K, d)$, a choice of G_K-stable $\mathbb{Z}_\ell$-lattices in the underlying representation spaces makes it possible to view each ρ_i as a homomorphism from $\mathbb{Z}_\ell[[G_K]]$ to $M_d(\mathbb{Z}_\ell)$. Let

$$j = \rho_1 \oplus \rho_2 : \mathbb{Z}_\ell[[G_K]] \longrightarrow M_d(\mathbb{Z}_\ell) \times M_d(\mathbb{Z}_\ell),$$

and let M denote the image of j. The induced homomorphism

$$\bar{j} : G_K \longrightarrow (M/\ell M)^\times$$

factors through $\operatorname{Gal}(L/K)$, since the cardinality of $M/\ell M$ is at most ℓ^{2d^2} and $\bar{j}$ is unramified outside of S_ℓ. It follows that the elements

$$\bar{j}(\operatorname{Frob}_{v_1}), \ldots, \bar{j}(\operatorname{Frob}_{v_N})$$

generate $M/\ell M$. By Nakayama's lemma, the elements

$$j\left(\mathrm{Frob}_{v_1}\right), \ldots, j\left(\mathrm{Frob}_{v_N}\right)$$

generate M as a $\mathbb{Z}_\ell$-module.

In particular, if

$$\operatorname{trace}\left(\rho_1\left(\mathrm{Frob}_{v_j}\right)\right) = \operatorname{trace}\left(\rho_2\left(\mathrm{Frob}_{v_j}\right)\right), \quad \text{for } j = 1, \ldots, N,$$

then

$$M \subseteq \Delta \subset M_d\left(\mathbb{Z}_\ell\right) \times M_d\left(\mathbb{Z}_\ell\right),$$

where $\Delta = M_d\left(\mathbb{Z}_\ell\right)$ is embedded diagonally. Therefore one has

$$\operatorname{trace}\left(\rho_1(\sigma)\right) = \operatorname{trace}\left(\rho_2(\sigma)\right) \quad \text{for all } \sigma \in \Pi_K.$$

Hence ρ_1 and ρ_2 have the same traces. Since they are semisimple, it follows that they are isomorphic as Π_K-representations. □

Proof of Theorem 3.2. Let $T = \{v_1, \ldots, v_N\}$ be as in the statement of Lemma 3.3. The assignment

$$\rho \mapsto \left(\operatorname{Tr}\left(\rho\left(\mathrm{Frob}_{v_1}\right)\right), \ldots, \operatorname{Tr}\left(\rho\left(\mathrm{Frob}_{v_N}\right)\right)\right)$$

is injective on $\mathrm{Rep}_S\left(G_K, d\right)$, and can only assume finitely many values, by the rationality of ρ. (More precisely, each $\operatorname{Tr}\left(\mathrm{Frob}_{v_i}\right)$ is a rational integer of absolute value $\leqslant dNv_i^{1/2}$.) Theorem 3.2 follows. □

Corollary 3.5. *Fix a number field K, a set of places S of K, and an integer g. Then there are finitely many isomorphism classes of complete curves C of genus g with good reduction outside of S.*

Proof. For such a curve C, we claim that the Jacobian of C is a principally polarized abelian variety with good reduction outside of S. Let v be a place of K not in S, and let $\mathcal{C}/\mathcal{O}_{K,v}$ be a smooth model of C. Then $\mathrm{Pic}_{\mathcal{C}/\mathcal{O}_{K,v}}$ is an abelian scheme over $\mathcal{O}_{K,v}$ whose generic fiber is the Jacobian of C. Thus, $\mathrm{Jac}(C)$ has good reduction outside S.

Now Torelli's theorem says that a curve of genus > 1 over a perfect field is determined (up to isomorphism) by the isomorphism class of its Jacobian as a principally polarized abelian variety. Thus, for $g > 1$ we have an injective map from the set of isomorphism classes of genus- g smooth proper curves (with geometrically connected fibers) over $\mathcal{O}_{K,S}$ into the set of isomorphism classes of principally polarized abelian schemes over $\mathcal{O}_{K,S}$. We want to say that the target of this injection is finite, so the source is finite as well. The Shafarevich conjecture implies that (up to isomorphism) there are only finitely many abelian varieties over K with good reduction outside of S admitting a principal polarization. Besides, there are only finitely many (isomorphism classes of) pairs (A, ϕ), where A is such an abelian variety and ϕ is a principal polarization. □

Remark 3.6. It is a classical fact that Jacobians of curves over an algebraically closed field are canonically principally polarized. The same fact for curves over more general bases is Proposition 6.9 in [MFK94].

3.2 Shafarevich Conjecture implies Mordell Conjecture

Theorem 3.7 (Mordell Conjecture)**.** *Let X be a smooth projective curve of genus $\geqslant 2$ defined over a number field K. Then $X(K)$ is finite.*

Proof. Let X be a curve of genus $g > 1$ defined over a number field K. To each point $P \in X(K)$ one associates a curve X_P and a covering map $\phi_P : X_P \longrightarrow X$ with the following properties:

1. The curve X_P and the map ϕ_P can be defined over a finite extension K' of K which does not depend on P.

2. The genus g' of X_P (and the degree of ϕ_P) is fixed and in particular does not depend on P.

3. The map ϕ_P is ramified only over the point P.

4. The curve X_P has good reduction outside a finite set of primes S' of K' which does not depend on P.

We will describe one approach here, which consists in considering the embedding $X \longrightarrow J$ of X into its jacobian that sends P to the origin of J, and letting $\tilde{X}$ be the pullback to X of the multiplication-by-2 map [2]: $J \longrightarrow J$. This map induces an unramified covering $\pi : \tilde{X} \longrightarrow X$ of degree 2^{2g}, and hence the genus of $\tilde{X}$ can be calculated explicitly using the Riemann-Hurwitz formula. The fiber $\pi^{-1}(P)$ can be written as

$$\pi^{-1}(P) = \tilde{P} + D,$$

where $\tilde{P}$ corresponds to the identity element of J, and hence belongs to $\tilde{X}(K)$, and D is an effective divisor of degree $2^{2g} - 1$ defined over K with support disjoint from $\tilde{P}$. Let J_D be the generalised jacobian attached to $\tilde{X}$ and D : the group $J_D(\overline{K})$ is identified with the group of degree zero divisors on $\tilde{X}$ with support outside D, modulo the subgroup of principal divisors of the form $\operatorname{div}(f)$, as f ranges over the functions satisfying $f(D_0) = 1$, for all degree zero divisors D_0 supported on D. The functor $L \mapsto J_D(\overline{K})^{G_L}$ (where $G_L := \operatorname{Gal}(\bar{L}/L)\big)$ on finite extensions of K is representable by the algebraic group over K denoted J_D, which is an extension of J by a torus T over K of rank $\left(2^{2g} - 2\right)$. In other words, there is a natural exact sequence

$$1 \longrightarrow T \longrightarrow J_D \longrightarrow J \longrightarrow 1$$

of commutative algebraic groups over K. One can embed $\tilde{X} - D_{\tilde{P}}$ into J_D by sending a point Q to the equivalence class of the divisor $(Q) - (\tilde{P})$. The multiplication-by-2 map [2] on J_D induces a map $X_P^0 \longrightarrow \tilde{X} - D$, as summarised by the following diagram with cartesian squares in which the vertical maps are induced by multiplication by 2 :

$$\begin{tikzcd}
J_D \arrow[d] & X_P^0 \arrow[l] \arrow[d] & \\
J_D & \tilde{X} - D \arrow[l] \arrow[r] \arrow[d] & J \arrow[d] \\
& X \arrow[r] & J
\end{tikzcd}$$

The closure X_P of X_P^0 has the desired properties 1-4: it is defined over K, and it follows directly from the Riemann-Hurwitz formula that its genus g' does not depend on P. Furthermore, the map $X_P^0 \longrightarrow \tilde{X} - D$ is unramified, and hence $X_P \longrightarrow X$ is ramified only over the point P. Finally, if X is smooth over $\mathrm{Spec}(\mathcal{O})$, the curve X_P has a smooth model over $\mathcal{O}' := \mathcal{O}[1/2]$.

The assignment $P \mapsto X_P$ therefore gives rise to a well-defined map

$$R_1 : X(K) \longrightarrow \mathcal{M}_{g'}\left(\mathcal{O}'\right).$$

But this assignment is finite-to-one; for otherwise there would be a curve Y and infinitely many (by property 3) distinct maps $\phi_P : Y \longrightarrow X$. This would contradict the following geometric finiteness result of De Franchis [Maz86, p.227].

Theorem 3.8. *If X and Y are curves over any field K, and Y has genus $g \geqslant 2$, then the set $\mathrm{Mor}_K(X, Y)$ of K-morphisms from X to Y is finite.*

The Shafarevich conjecture for curves, which asserts the finiteness of $\mathcal{M}_{g'}(\mathcal{O}')$, therefore implies the finiteness of $X(K)$. This completes the proof. □

References

[B B] A. Snowden B. Bhatt. *Faltings's Proof of the Mordell Conjecture*. URL: `http://www-personal.umich.edu/~takumim/Mordell.pdf`..

[Fal+86] Gerd Faltings et al. *Rational points*. Springer, 1986.

[FC13] Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties*. Vol. 22. Springer Science & Business Media, 2013.

[Lev] B. Levin. *Tate conjecture over number fields*. URL: `https://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L19.pdf`.

[Lip] Michael Lipnowski. *p-divisible groups*. URL: `https://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L09.pdf`.

[Maz86] Barry Mazur. "Arithmetic on curves". In: *Bulletin of the American Mathematical Society* 14.2 (1986), pp. 207–259.

[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory*. Vol. 34. Springer Science & Business Media, 1994.

[Mil] J. S. Milne. *Abelian Varieties*. URL: `https://www.jmilne.org/math/CourseNotes/AV.pdf`.

[Tat67] John T Tate. "p-Divisible groups". In: *Proceedings of a Conference on Local Fields: NUFFIC Summer School held at Driebergen (The Netherlands) in 1966*. Springer. 1967, pp. 158–183.