

# Heights and Finiteness theorems of abelian varieties

We start with an overview of heights on projective spaces and varieties to give a hint about their role in attacking finiteness problems of abelian varieties. We then try to explain the motivation for introducing the Faltings height on abelian varieties and do explicit computation in the case of elliptic curves. Finally we include a direct proof of the finiteness theorems of elliptic curves. Our main sources are [1], [2] and [3]. See also [4] and [5]. This is a note prepared for the [Faltings' Theorem seminar](#) at Harvard.

## [-] Contents

- Heights on projective spaces and projective varieties
- Finiteness of abelian varieties and Modular Heights
- Metrized line bundles and the Faltings height
- Comparison of heights for elliptic curves
- Finiteness theorems for elliptic curves

## Links

- Chao Li's Homepage
- Harvard University
- Math Department
- maTHµ

## Comments

Like 0 Share

0 Comments Sor

Add a comment...

Facebook Comments Plugin

## Heights on projective spaces and projective varieties

Let us start by reviewing several basic properties of heights on projective spaces. The general scheme of height functions is a measurement of "arithmetic complexity". For a rational number  $x \in \mathbb{Q}$ , we can write it as  $a/b$  for two integers  $a, b \in \mathbb{Z}$  without common divisors, and define the *height* of  $x$  as

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

It will be troublesome to draw a graph of this "function" defined on  $\mathbb{Q}$ . Nevertheless, the definition matches our intuition: the larger  $H(x)$  is, the more complicated  $x$  is.

More intrinsically, let  $K/\mathbb{Q}$  be a number field. Set the absolute values:

- $|\cdot|_v$  satisfies  $|p|_v = p^{-1}$  for  $v|p$  and  $|\cdot|_v$  is the real or complex absolute value for  $v$  real or complex.
- $\|\cdot\|_v := |\cdot|_v^{n_v}$ , where  $n_v = [K_v : \mathbb{Q}_v]$ . It takes the value  $\#k_v^{-1}$  on the uniformizer  $\pi_v$ .

**Definition 1** For any point  $x = [a, b] \in \mathbb{P}^1(K)$ , we define the *relative height*

$$H_K(x) = \prod_{v \in M_K} \max\{\|a\|_v, \|b\|_v\}.$$

Note that by the product formula,  $\prod_v \|\lambda\|_v = 1$  for  $\lambda \in K^\times$ , thus we know that  $H_K(x)$  does not depend on the choice of homogeneous coordinates  $[a, b]$ . Because for  $v \in M_K^0$ ,  $\|a\|_v > 1$  if and only if  $\text{ord}_v a < 0$ , it is easy to check that

**Proposition 1** If an element  $a \in K$  generates the ideal  $(x) = IJ^{-1}$ , where  $I, J$  are relative prime integral ideals of  $K$ , then

$$H_K(x) = \mathbb{N}_{K/\mathbb{Q}} J \cdot \prod_{v \in M_K^\infty} \max\{\|x\|_v, 1\}.$$

**Remark 1** In particular, we recover the height defined above when  $K = \mathbb{Q}$ , in that case  $J = (b)$  and  $I = (a)$ .

This definition of heights extends to projective spaces  $\mathbb{P}^N(K)$  of dimension  $N$  in an obvious way.

**Definition 2** Let  $x = [x_0, \dots, x_N] \in \mathbb{P}^N(K)$ . We define the *relative height*

$$H_K(x) := \prod_{v \in M_K} \max_{0 \leq i \leq N} \{\|x_i\|_v\},$$

the *absolute height*

$$H(x) := H_K(x)^{1/[K:\mathbb{Q}]},$$

and the *logarithmic height*

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

Note that for a finite extension  $L/K$ ,  $H_L(x) = H_K(x)^{[L:K]}$ , therefore the absolute height and the logarithmic height do not depend on the choice of  $K$ .

The following is a prototype of a finiteness result under the bounded height condition.

**Theorem 1 (Northcott)** For any constants  $C$  and  $d$ , there are only finitely many points  $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$  satisfying  $H(P) \leq C$  and  $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$ . In particular, for any number field  $K$ , there are only finitely many points  $P \in \mathbb{P}^1(K)$  with bounded height.

**Proof** Suppose  $P = [x, 1]$  and let  $x_1 = x, \dots, x_d$  be the Galois conjugates of  $x$ . Then the minimal polynomial of  $x$  is of the form

$$f(T) = T^d - (x_1 + \dots + x_d)T^{d-1} + \dots + (-1)^d x_1 \dots x_d.$$

Note that the heights of the  $x_i$ 's are all the same, therefore the coefficient of  $T^j$  is bounded by  $c_j H(x)^j$  for some constant  $c_j$  not depending on  $x$ . So these coefficients are rational numbers with bounded heights, therefore there are only finitely many choices of the coefficients, hence finitely many choices of  $f(T)$ .  $\square$

Here comes a neat corollary of the Northcott's property.

**Corollary 1** Let  $x \in \overline{\mathbb{Q}}^\times$ . Then  $x$  is a root of unity if and only if  $h(x) = 0$ .

**Proof** Suppose  $x^n = 1$  for some  $n$ . Then  $nh(x) = h(x^n) = h(1) = 0$ , hence  $h(x) = 0$ . Conversely, suppose  $h(x) = 0$ , then  $h(x^n) = nh(x) = 0$  for every  $n$ . By the Northcott's, some  $x^{n_1}$  and  $x^{n_2}$  have to be same, which implies  $x$  is a root of unity.  $\square$

**Remark 2** Though we do not need it in this talk, it does not harm to mention that there is a similar notion  $\hat{h}$ , called the *canonical height* (or *Neron-Tate height*) attached to every rational point on an abelian variety over  $K$ . It measures the arithmetic complexity of the point: for example,  $\hat{h}(P) = 0$  if and only if  $x$  is a torsion point analogously.

Slightly more generally, given a projective variety  $i : V \hookrightarrow \mathbb{P}^N$ , the embedding  $i$  associates with every point  $P \in V$  a height  $h(P) := h(i(P))$  using the height on the projective space  $\mathbb{P}^N$ . The height thus obtained does depend on the choice of the projective embedding, nevertheless, it turns out to be uniquely determined up to a *bounded function*. From the previous theorem, we know that over a number field  $K$ , there are only finitely many points in  $V(K)$  with bounded heights.

## Finiteness of abelian varieties and Modular Heights ▲

One of the key steps in proving Faltings' theorem is to prove the finiteness theorems of abelian varieties.

**Theorem 2 (Finiteness I, or Conjecture T)** Let  $A$  be an abelian variety over a number field  $K$ . Then there are only finitely many isomorphism classes of abelian varieties over  $K$  isogenous to  $A$ .

**Theorem 3 (Finiteness II, or Shafarevich's conjecture for abelian varieties)** There are only finitely many isomorphism classes of abelian varieties over  $K$  of dimension  $g$  having good reduction outside a finite set of places  $S$ .

Carl has showed the implication

$$\text{Finiteness I} + \text{Tate} + \text{Finiteness of characters} + \text{Riemann} \implies \text{Finiteness II}.$$

So it remains to show Finiteness I. Faltings' argument involves the usage of "heights":

**Height I** There are only finitely many isomorphism classes of polarized abelian varieties  $(A, \lambda)$  over  $K$  of dimension  $g$ ,  $\deg d$  with semistable reduction everywhere and bounded "heights".

**Height II** The "height" is bounded in every isogeny class of abelian varieties over  $K$ .

Assuming these two parts, then together with the semistable reduction theorem (every abelian variety has semistable reduction after a finite extension), we can easily deduce Finiteness I.

To possibly show the finiteness statement like Height I, we would like to associate a height to each abelian variety using Northcott's property. A natural option is to view an abelian variety as a point in the Siegel moduli variety and attach the height of that point to the corresponding abelian varieties. This motivates the notion of modular heights.

**Definition 3** Let  $(A, \lambda)$  be a polarized abelian variety over  $K$  of dimension  $g$  and degree  $d$ . Let  $\mathcal{A}_{g,d}$  be the Siegel modular variety with its canonical projective embedding. Then associated with  $(A, \lambda)$  we have a point  $j(A, \lambda) \in \mathcal{A}_{g,d}(K)$ . We define the *modular height* of  $(A, \lambda)$  to be  $h_M(A, \lambda) = h(j(A, \lambda))$ .

**Remark 3** When  $g = d = 1$ , the modular height of an elliptic curve is simply the height of its  $j$ -invariant.

**Theorem 4 (Height I)** Let  $C$  be a constant. Then there are only finitely many isomorphism classes of polarized abelian varieties  $(A, \lambda)$  over  $K$  of dimension  $g$ , degree  $d$  having semistable reduction everywhere and  $h_M(A, \lambda) \leq C$ .

**Remark 4** This is not true without the semistable reduction condition: for any  $c \in K^\times / (K^\times)^2$ ,  $E_c : y^2 = x^3 + ac^2x + bc^3$  are all isomorphic over  $\bar{K}$  but not isomorphic over  $K$ . These  $E_c$ 's have the same  $j$ -invariant, hence  $h_M(E_c) = h(j(E_c))$  are the same.

To clarify the proof, we recall the following lemma without proof.

**Lemma 1** Let  $(A, \lambda)$  be a polarized abelian variety. Then

- The group of automorphisms  $\text{Aut}(A, \lambda)$  is finite.
- Suppose  $n \geq 3$ , an automorphism of  $(A, \lambda)$  acting on  $A_n$  trivially must be the identity.

**Proof** (Height I) By Northcott's property, we know that the set of  $\bar{K}$ -isomorphism classes of such  $(A, \lambda)$  is finite. So we need to show that given a polarized abelian variety  $(A_0, \lambda_0)$  with semistable reduction everywhere, there are only finitely many  $K$ -isomorphism classes  $(A, \lambda)$  with semistable reduction everywhere which are isomorphic to  $(A_0, \lambda_0)$  over  $\bar{K}$ . We shall show that there exists a finite extension  $L/K$  such that all these  $(A, \lambda)$  are actually isomorphic to  $(A_0, \lambda_0)$  over  $L$ . Then  $(A, \lambda)$ 's are parametrized by  $H^1(\text{Gal}(L/K), \text{Aut}(A_L, \lambda_L))$ , which is finite, since  $\text{Gal}(L/K)$  and  $\text{Aut}(A_L, \lambda_L)$  (by the previous lemma) are finite. This completes the proof.

It remains to construct such an  $L$ . Because  $A, A_0$  have semistable reduction everywhere and they are isomorphic over a finite extension of  $K$ , we know that  $A, A_0$  have the same set  $S$  of places of bad reduction. Fix a prime  $\ell \geq 3$ , then  $K(A_\ell)/K$  is an extension of degree  $\leq \#GL_{2g}(\mathbb{F}_\ell)$  and is unramified outside  $S \cup \{v|\ell\}$  by Neron-Ogg-Shafarevich's criterion. Therefore by Hermite's theorem, the compositum field  $L$  of all  $K(A_\ell)$ 's must be a finite extension of  $K$ . We claim that all  $(A, \lambda)$ 's are isomorphic to  $(A_0, \lambda_0)$  over  $L$ . Let  $\alpha : (A, \lambda) \rightarrow (A_0, \lambda_0)$  be an isomorphism over  $\bar{K}$ . Then for any  $\sigma \in \text{Gal}(\bar{K}/L)$ ,  $\sigma\alpha \circ \alpha^{-1}$  is an automorphism of  $(A_0, \lambda_0)$  which leaves  $A_\ell$  fixed, therefore is the identity by the previous lemma. So the isomorphism  $\alpha$  is actually defined over  $L$ .  $\square$

It would be wonderful to show Height II for the modular height, unfortunately, it is not clear how  $h_M(A, \lambda)$  changes under isogeny. Faltings introduced what is now known as the Faltings height  $h_F$  to attack Finiteness II. It turns out miraculously that the Faltings height can be proved to change only slightly under isogeny, and thus Height II is true for  $h_F$ . More precisely,

**Theorem 5 (Height II)** Let  $A$  be an abelian variety over  $K$  having semistable reduction everywhere. Then  $h_F$  is bounded in the isogeny class of  $A$ .

Finally, to combine the Height I result for  $h_M$  and Height II result for  $h_F$ , one needs a comparison theorem between  $h_M$  and  $h_F$ : the boundedness of one of them implies the boundedness of the other.

**Theorem 6 (Comparison of heights)** There exists constants  $c_1, c_2, c_3$  such that for abelian varieties  $(A, \lambda)$  over  $K$  with semistable reduction everywhere,

$$|h_F(A) - c_1 h_M(A, \lambda)| \leq c_2 \log h_M(A, \lambda) + c_3.$$

Now the road-map for proving Finiteness I is

$$\text{Height I} + \text{Height II} + \text{Comparison} \implies \text{Finiteness I}$$

Height II (using the results of Raynaud and Tate on  $p$ -divisible groups) and the comparison theorem (using the compactified Siegel modular variety over  $\mathbb{Z}$ ) are the hardest parts of the whole proof and will occupy most of the remaining semester. In the rest of this talk, I will prove the comparison theorem for the case of elliptic curves, to somehow convince you that it is a reasonable thing to expect. If time permits, I will show Finiteness I for elliptic curves using a different argument, taking advantage of Siegel's theorem on integral points on elliptic curves.

We shall now motivate the definition of the Faltings height, which already showed up in Dick's introduction and also in Carl's talk. Suppose we have a complex elliptic curve  $E = \mathbb{C}/\Lambda$  for some period lattice  $\Lambda \subseteq \mathbb{C}$ . Intuitively,  $E$  is more complicated if  $\Lambda$  is more complicated, so we may attempt to define the height of  $E$  as

$$H(E) = \text{Vol}(D)^{-1},$$

where  $D$  is the fundamental domain for  $\Lambda$ . However, this quantity is not well defined for a given isomorphism class: for example, scaling  $\Lambda$  gives isomorphic elliptic curves, but  $\text{Vol}(D)$  is different. Notice that fixing the period lattice is equivalent to fixing a canonical choice for a differential  $\omega \in H^0(E, \Omega^1)$ :

$$\Lambda = \left\langle \int_{\alpha} \omega \right\rangle, \quad \alpha \in H_1(E, \mathbb{Z}).$$

If  $E$  is defined over  $\mathbb{Q}$ , this canonical choice can be made using the *minimal* Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}, \quad \Delta \text{ minimal.}$$

The differential

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

is then well defined up to multiplication by  $\mathbb{Z}^\times = \{\pm 1\}$  and the period lattice is uniquely determined by the isomorphism class of  $E$ . In this case,

$$\text{Vol}(D) = \int_D dx \wedge dy = \frac{i}{2} \int_D dz \wedge d\bar{z} = \frac{i}{2} \int_{E(\mathbb{C})} \omega \wedge \bar{\omega}.$$

We are using the crucial fact that  $\mathbb{Z}$  is a PID to define the minimal Weierstrass equation. In general, for  $E$  defined over a number field  $K$ , its ring of integers  $R$  is not necessarily a PID and a minimal Weierstrass equation does not exist. To obtain a canonical choice of the differential, we need the Neron models George talked about last time. Let  $\mathcal{E}/\mathbb{Z}$  be the Neron model of  $K/\mathbb{Q}$ . Then the sheaf of Neron differentials  $\Omega_{\mathcal{E}/\mathbb{Z}}$  is locally free of rank 1. So the pull back  $\omega_{\mathcal{E}/\mathbb{Z}} = e^* \Omega_{\mathcal{E}/\mathbb{Z}}$  by the zero section  $e: \text{Spec } \mathbb{Z} \rightarrow \mathcal{E}$  gives us a projective  $\mathbb{Z}$ -module of rank 1. Because  $\mathbb{Z}$  is a PID, this module is actually a free module of rank 1. Therefore it has a canonical generator up to sign, which is exactly the above differential  $\omega$ . For a number field  $K$ , the same construction gives a projective  $R$ -module of rank 1, where  $R$  is the ring of integers of  $K$ . When  $R$  is not a PID,  $\omega_{\mathcal{E}/R}$  is not necessarily free and we cannot take a global generator, but only a bunch of local generators for each finite place. This motivates us to define the notion of metrized line bundles, introduced by Arakelov.

**Definition 4** Let  $R$  be the ring of integers of  $K$ . A *metrized line bundle* on  $\text{Spec } R$  is a pair  $(\mathcal{L}, |\cdot|)$ , where  $\mathcal{L}$  is a line bundle on  $\text{Spec } R$  (i.e. a projective  $R$ -module of rank 1) and for each  $v \in M_K^\infty$ ,  $|\cdot|_v$  is a norm on the real or complex vector space  $\mathcal{L}_v = \mathcal{L} \otimes_R K_v$ .

**Definition 5** For  $v \in M_K^0$ , suppose  $\mathcal{L}_v = R_v \cdot l_v$ , we set  $\|t\|_v = \|a\|_v$  if  $t = a \cdot l_v$  for  $a \in R_v$ . For  $v \in M_K^\infty$ , we denote  $\|t\|_v = |t|_v^{n_v}$ . The *height* of a metrized line bundle  $(\mathcal{L}, |\cdot|)$  is defined to be

$$H(\mathcal{L}, |\cdot|) = \prod_{v \in M_K} \|t\|_v^{-1},$$

for any  $t \in \mathcal{L}$ . It is well-defined by the product formula. The *degree* of  $(\mathcal{L}, |\cdot|)$  is defined to be

$$\deg(\mathcal{L}, |\cdot|) = \log H(\mathcal{L}, |\cdot|).$$

**Remark 5** The nonarchimedean part is equal to  $[\mathcal{L} : Rl]$ . When  $R = \mathbb{Z}$  and  $L$  is the generator of  $\mathcal{L}$ , one then recovers that  $H(\mathcal{L}, |\cdot|) = \|t\|_\infty^{-1}$  (one thinks of  $\|t\|_\infty$  as the area  $\text{Vol}(D)$ ).

Now let us come back to the case of abelian varieties. Let  $A$  be an abelian variety of dimension  $g$  over  $K$ . Let  $\mathcal{A}/R$  be the Neron model of  $A$ . Then the sheaf of Neron differentials  $\Omega_{\mathcal{A}/R}$  is locally free of rank  $g$  on  $\mathcal{A}$ . So the top wedge power  $\bigwedge^g \Omega_{\mathcal{A}/R}$  is a locally free sheaf of rank 1 on  $\mathcal{A}$ . Pulling back by the zero section  $e: \text{Spec } R \rightarrow \mathcal{A}$ , we obtain a line bundle  $\omega_{\mathcal{A}/R} = e^* \bigwedge^g \Omega_{\mathcal{A}/R}$ . We specify the norm for every  $v \in M_K^\infty$  by

$$|\mu|_v = \sqrt{\left(\frac{i}{2}\right)^g \int_{K_v} \mu \wedge \bar{\mu}}.$$

**Definition 6** Let  $(\omega_{\mathcal{A}/R}, |\cdot|)$  be the metrized line bundle on  $R$  described above. The *Faltings height* of  $A$  is defined to be

$$h_F(A) = \frac{1}{[K:\mathbb{Q}]} \deg(\mathcal{L}, |\cdot|).$$

**Remark 6** Since the Neron model may change after field extension, the Faltings height *depends* on the base field  $K$ . However, by the semistable stable reduction theorem, the Neron model does not change after base change to some finite field extension. We thus define the *stable Faltings height* to be the Faltings height  $h_F(A_{K'})$ , for any  $K'/K$  such that  $A_{K'}$  has semistable stable reduction everywhere.

**Remark 7** For an elliptic curve  $E$  over  $\mathbb{Q}$ , we simply recover

$$h_F(E) = \log H(E) = -\frac{1}{2} \log \text{Vol}(D),$$

which coincides with our intuition.

## Comparison of heights for elliptic curves

We first give an explicit formula of the Faltings height  $h_F(E)$ .

**Theorem 7** Let  $E/K$  be an elliptic curve. Suppose  $E(\overline{K}_v) \cong \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau_v$  for  $v \in M_K^\infty$ . Then

$$h_F(E) = \frac{1}{12[K:\mathbb{Q}]} \left( \log |\mathbb{N}_{K/\mathbb{Q}} \Delta_{E/K}| - \sum_{v \in M_K^\infty} n_v \log (|\Delta(\tau_v)| (\text{Im } \tau_v)^6) \right),$$

where  $\Delta_{E/K}$  is the minimal discriminant and  $\Delta(\tau) = (2\pi)^{12} q \prod_n (1 - q^n)^{24}$  is the modular discriminant function.

**Remark 8** When  $K = \mathbb{Q}$ , we again recover  $h_F(E) = -\frac{1}{2} \log (\text{Im } \tau)$  for the minimal Weierstrass equation  $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ .

**Proof** Let  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$  be any Weierstrass equation of  $E/K$ . We shall utilize the invariance of the section

$$\beta = \Delta \cdot \frac{dx}{2y + a_1x + a_3}$$

of  $\omega_{\mathcal{E}/R}^{\otimes 12}$  under the change of coordinates to calculate the Faltings height locally. For  $v \in M_K^0$ , let

$$\alpha_v = \frac{dx_v}{2y_v + a_{1,v}x_v + a_{3,v}}$$

be the Neron differential at  $v$ , then by the invariance of  $\beta$ , we know that

$$\beta = \Delta_v \alpha_v^{\otimes 12},$$

where  $\Delta_v$  is the minimal discriminant of  $E$  at  $v$ . So for  $v \in M_K^0$ ,

$$\omega_{\mathcal{E}/R_v}^{\otimes 12} / R_v \beta^{\otimes 12} = R_v \alpha_v^{\otimes 12} / R_v \beta = R_v \alpha_v^{\otimes 12} / R_v \Delta_v \alpha_v^{\otimes 12}.$$

Hence the local contribution at  $v$  is  $\log |\mathbb{N}_{K_v/\mathbb{Q}_v} \Delta_v|_v$  and the total nonarchimedean contribution is  $\log |\mathbb{N}_{K/\mathbb{Q}} \Delta_{E/K}|$ . For  $v \in M_K^\infty$ , let

$$y_v^2 = 4x_v^3 - g_2(\tau_v)x_v - g_3(\tau_v)$$

be the Weierstrass equation given by  $E(\overline{K}_v) \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_v)$  and

$$\alpha_v = \frac{dx_v}{y_v},$$

then by the invariance of  $\beta$ , we know that

$$\beta = \Delta(\tau_v) \cdot \alpha_v^{\otimes 12}.$$

We compute

$$\frac{i}{2} \int_{E(\overline{K}_v)} |\Delta(\tau_v)|^{1/6} \alpha_v \wedge \bar{\alpha}_v = |\Delta(\tau_v)|^{1/6} \text{Im}(\tau),$$

therefore the local contribution at  $v$  is

$$\frac{n_v}{[K:\mathbb{Q}]} \log \left( |\Delta(\tau_v)|^{1/6} \text{Im } \tau_v \right)^{1/2},$$

and the total archimedean contribution is

$$\frac{1}{12[K:\mathbb{Q}]} \sum_{v \in M_K^\infty} n_v \log (|\Delta(\tau_v)| (\text{Im } \tau_v)^6).$$

This completes the proof.  $\square$

Using the previous explicit expression, now we can prove the comparison theorem of the Faltings height and the modular height for elliptic curves.

**Theorem 8** There exists some constant  $C$  such that for elliptic curves  $E/K$  with semistable reduction everywhere,

$$\left| h_F(E) - \frac{1}{12} h_M(E) \right| \leq \frac{1}{2} \log(1 + h_M(E)) + C.$$

**Proof** For any  $v \in M_K^\infty$ , we can suitably choose  $\tau_v$  such that  $\text{Im } \tau_v \geq \sqrt{3}/2$ , so that  $|q_v| \leq e^{-\pi\sqrt{3}}$ . Hence  $\Delta(\tau_v) = (2\pi)^{12} q_v \prod_n (1 - q_v^n)^{24}$  implies that

$$\log |\Delta(\tau_v)| = \log |q_v| + O(1).$$

Using the  $q$ -expansion of  $j(\tau)$ , one also knows that

$$\log(\max\{|j(\tau_v)|, 1\}) = \log |1/q_v| + O(1).$$

Therefore

$$-\log |\Delta(\tau_v)| = \log(\max\{|j(\tau_v)|, 1\}) + O(1).$$

Also from

$$\log |q_v| = -2\pi \text{Im } \tau,$$

we obtain

$$\log(\text{Im } \tau) = \log \log \max\{j(\tau), e\} + O(1).$$

Plugging into the explicit formula of the Faltings height gives

$$h_F(E) = \frac{1}{12[K : \mathbb{Q}]} \left( \log |\mathbb{N}_{K/\mathbb{Q}} \Delta_{E/K}| + \sum_{v \in M_K^\infty} n_v (\log \max\{|j(E)|_v, 1\} - 6 \log \log \max\{|j(\tau)|_v, e\} + O(1)) \right).$$

Since  $E/K$  has semistable reduction everywhere, we know that  $\text{ord}_v(j(E)) < 0$  if and only if  $v$  dividing  $\Delta_{E/K}$  and in this case  $\text{ord}_v(j(E)) = -\text{ord}_v(\Delta_{E/K})$ . Thus

$$\log |\mathbb{N}_{K/\mathbb{Q}} \Delta_{E/K}| + \sum_{v \in M_K^\infty} n_v \log \max\{|j(E)|_v, 1\} = \log H_K(j(E)) = [K : \mathbb{Q}] h(j(E)).$$

So it remains to show that

$$\sum_{v \in M_K^\infty} \log \log \max\{|j(\tau)|_v, e\} \leq [K : \mathbb{Q}] \log(1 + h(j(E))),$$

which I shall leave it as an exercise using the arithmetic-geometric mean inequality.  $\square$

## Finiteness theorems for elliptic curves

Finally, we shall utilize Siegel's theorem on the integral points of elliptic curves to give a completely different direct proof of Finiteness I for elliptic curves.

**Theorem 9 (Siegel)** Let  $E/K$  be an (affine) elliptic curve,  $S \subseteq M_K$  be a finite set containing  $M_K^\infty$  and  $R_S = \{x \in K : \text{ord}_v x \geq 0, \forall v \notin S\}$  be the ring of  $S$ -integers. Then the set of integral points  $\{P \in E(K) : x(P) \in R_S\}$  is finite.

Siegel's proof uses techniques from Diophantine approximations, which we do not get into here. We will deduce Finiteness I from the even stronger Shafarevich's theorem for elliptic curves. The following cute proof is due to Shafarevich.

**Theorem 10 (Shafarevich, Finiteness II)** Let  $S \subseteq M_K$  be a finite set containing  $M_K^\infty$ . Then there are only finitely many isomorphism classes  $E/K$  having good reduction outside  $S$ .

**Proof** We may enlarge  $S$  so that  $S$  contains all places over 2 and 3 and also  $R_S$  is a PID. Then for every  $E/K$ , we have a minimal Weierstrass equation

$$E : y^2 = x^3 + Ax + B, \quad A, B \in R_S.$$

If further  $E$  has good reduction outside  $S$ , we know the discriminant  $\Delta = -16(4A^3 + 27B^2) \in R_S^\times$ . Suppose we have an infinite sequence of elliptic curves  $E_i/K$  having good reduction outside  $S$ . Since the  $S$ -unit group  $R_S^\times$  is finitely generated, we know that  $R_S^\times / (R_S^\times)^{12}$  is a finite group. So we can find an infinite subsequence (still denoted by  $E_i/K$ ), such that  $\Delta_i$  are in the same class of  $R_S^\times / (R_S^\times)^{12}$ . In other words,  $\Delta_i = C D_i^{12}$  for a fixed  $C$ . From  $\Delta = -16(4A^3 + 27B^2)$ , we know that  $y^2 = x^3 + 27C$  has  $R_S$ -solutions  $(-12A_i/D_i^4, 72B_i/D_i^6)$ . Therefore by Siegel's theorem, there are only finitely many possibilities for  $A_i/D_i^4$  and  $B_i/D_i^6$ . Moreover, each of the identities  $A_i/D_i^4 = A_j/D_j^4$ ,  $B_i/D_i^6 = B_j/D_j^6$  gives a  $K$ -isomorphism  $E_i \rightarrow E_j$  via  $x = (D_i/D_j)^2 x'$ ,  $y = (D_i/D_j)^3 y'$ .  $\square$

**Theorem 11 (Finiteness I)** Fix an elliptic curve  $E/K$ . Then there are only finitely many elliptic curves  $K'/K$  which are isogenous to  $E$ .

**Proof** Suppose  $E'$  and  $E$  are isogenous over  $K$ . Then they have the same set of places of good reduction by Neron-Ogg-Shafarevich (the induced map  $E'[m] \rightarrow E[m]$  is an isomorphism of  $G_K$ -modules for all  $E$ 's prime to the characteristic of the residue field and the degree of the isogeny). The result then follows from Shafarevich's theorem.

□

## References

- [1] Silverman, Joseph H., *Heights and elliptic curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, 1986, 253--265.
- [2] Milne, James S., *Abelian Varieties (v2.00)*, Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [3] Joseph H. Silverman, *The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)*, Springer, 2010.
- [4] Enrico Bombieri and Walter Gubler, *Heights in Diophantine Geometry (New Mathematical Monographs)*, Cambridge University Press, 2007.
- [5] Marc Hindry and Joseph H. Silverman, *Diophantine Geometry: An Introduction (Graduate Texts in Mathematics)*, Springer, 2000.