

# Heights for Elliptic Curves

Paul Fili

Abelian Varieties, Spring 2006, Prof. Farkas

## Abstract

We introduce the notion of height for the points on an elliptic curve, an abelian variety of genus 1, and show how an appropriate measure of height and the technique of infinite descent are used to prove the Mordell-Weil theorem that the group of  $K$ -rational points of an elliptic curve is finitely generated when  $K$  is a number field. Our proof of the Mordell-Weil theorem follows that given in Silverman [4, §VIII].

## Contents

<b>1</b>	<b>Background</b>	<b>2</b>
1.1	Introduction . . . . .	2
1.2	Some Cohomology . . . . .	3
1.2.1	Finite Group Cohomology . . . . .	3
1.2.2	Galois Cohomology . . . . .	6
1.3	Torsion subgroups of Elliptic Curves . . . . .	7
1.4	The Technique of Descent . . . . .	7
<b>2</b>	<b>The Weak Mordell-Weil Theorem</b>	<b>9</b>
2.1	The Kummer Pairing . . . . .	10
2.2	A reduction lemma . . . . .	13
2.3	Finiteness of $L/K$ . . . . .	13
<b>3</b>	<b>Measuring Height</b>	<b>14</b>
3.1	Heights on $\mathbb{P}^n$ . . . . .	14
3.2	Heights on $E(K)$ . . . . .	16

# 1 Background

## 1.1 Introduction

Let  $K$  be a number field and let  $E/K$  be an elliptic curve, that is, a smooth projective curve of genus 1. The Mordell-Weil theorem states that

**Theorem 1.1** (Mordell-Weil). *The group  $E(K)$  of  $K$ -rational points on  $E$  is finitely generated, that is,*

$$E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^r$$

where the torsion subgroup  $E_{\text{tors}}(K)$  is finite.

This theorem was proven by Mordell in 1922 for  $K = \mathbb{Q}$  and extended to number fields by Weil in his 1928 thesis. In fact even more is known:

**Theorem 1.2.** *Let  $A$  be an abelian variety over a field  $K$  that is finitely generated over its prime field. Then  $A(K)$  is finitely generated.*

The more general theorem, published in 1959, is the result of the work of S. Lang and A. Néron [2]. Their proof follows the same basic pattern as the proof of the Mordell-Weil theorem. Both proofs begin by proving a weak version of the theorem:

**Theorem 1.3** (Weak Mordell-Weil). *For any positive  $m$ ,  $E(K)/mE(K)$  is a finite group.*

Of course, if an abelian group  $G$  is finitely generated, then  $G/mG$  is finite for all positive  $m$ , but the converse typically does not hold. We obtain the converse through the use of height functions and the so-called method of infinite descent. The basic idea is to develop a notion of the ‘size’ of a point, which is captured by a height function that satisfies certain properties. We then show that the number of points with size less than a fixed height is finite, and we make use of our finite generators for  $E(K)/mE(K)$  to write our point in the form  $Q_1 + mP$ , and we show that we can keep rewriting  $P$  in terms of some coset representatives  $Q_i$  of  $E(K)/mE(K)$  plus points of the form  $mP_i$  for  $P_i$  of decreasing height. When the height becomes smaller than our fixed value, we are inside the finite set of points of small height and we have written our point in terms of representatives for generators of  $E(K)/mE(K)$  and this finite set, thus demonstrating a finite set of generators for  $E(K)$ .

We start by reviewing some background and then establishing a theorem that encapsulates the method of infinite descent. Once this has been established, we will prove the assumptions needed in the theorem, namely, the weak Mordell-Weil theorem and the construction of an appropriate height function.

## 1.2 Some Cohomology

We will avail ourselves of some Galois cohomology as it makes several of the proofs in section 2 much easier than they otherwise might be. We review the basic finite group cohomology as covered in lecture, and then discuss what we will need from Galois cohomology (where our groups are profinite).

### 1.2.1 Finite Group Cohomology

**Definition 1.4.** A  $G$ -module is an abelian group  $M$  together with a homomorphism  $G \rightarrow \text{Aut}(M)$  that defines an action of  $G$  on  $M$ . We denote the action of  $g \in G$  by  $m \mapsto m^g$ .

For example, if  $E/K$  is an elliptic curve over a field  $K$ , then  $E(\overline{K})$  is naturally a  $\text{Gal}(\overline{K}/K)$ -module. We define the *zeroth-cohomology group* to be set of  $G$ -invariant elements of  $M$ :

$$H^0(G, M) = M^G = \{m \in M : m^g = m \ \forall g \in G\}.$$

If  $M, N$  are  $G$ -modules then a  $G$ -homomorphism is a map  $\phi : M \rightarrow N$  such that  $\phi(m^g) = \phi(m)^g$ , i.e., a map that respects the  $G$ -module structure. An exact sequence of  $G$ -modules

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

naturally induces an exact sequence

$$0 \longrightarrow H^0(G, L) \longrightarrow H^0(G, M) \longrightarrow H^0(G, N).$$

Notice that this last map may fail to be surjective, as a coset of  $L$  in  $M$  which is fixed by  $G$  need not be fixed for a single representative in  $M$ . However, as we shall see, we can extend this exact sequence to a long exact sequence in group cohomology.

For  $n \geq 0$ , define the  $n$ -cochain group  $C^n(G, M) = \{f : G^n \rightarrow M\}$  as the maps of sets of between  $G^n$  and  $M$ , endowed with the additive group structure from  $M$ . Then we define the  $n$ -th coboundary homomorphism  $d_n : C^n(G, M) \rightarrow C^{n+1}(G, M)$  to be

$$d_n(f)(g_1, \dots, g_{n+1}) = f(g_2, \dots, g_{n+1})^{g_1} + \sum_{i=1}^n f(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n).$$

Then it can be shown that

$$d_n \circ d_{n-1} = 0$$

and therefore by definition

$$0 \longrightarrow C^0(G, M) \xrightarrow{d_0} C^1(G, M) \xrightarrow{d_1} C^2(G, M) \xrightarrow{d_2} \dots$$

is a *cochain complex*. We define the  $n$ -cocycles  $Z^n(G, M)$  and the  $n$ -coboundaries  $B^n(G, M)$  by

$$Z^n(G, M) = \ker(d_n), \quad B^n(G, M) = \text{image}(d_{n-1})$$

for appropriate  $n$  (we let  $B^0(G, M) = 1$  for convenience).

**Definition 1.5.** The  $n$ -th cohomology of  $G$  with coefficients in  $M$  is defined to be

$$H^n(G, M) = Z^n(G, M) / B^n(G, M).$$

This is well defined as  $d_n \circ d_{n-1} = 0$  implies  $B^n(G, M) \subseteq Z^n(G, M)$ .

We will mostly be concerned with the zeroth and first cohomologies. For  $H^0(G, M)$ , we note that  $f \in C^0(G, M)$  is just a point  $f = m \in M$ , and  $d_0(f)(g) = m^g - m$ , so  $f \in \ker(d_0) = Z^0(G, M) = H^0(G, M)$  iff  $m^g - m = 0$  for all  $g \in G$ , that is,  $f = m \in M^G$ , which agrees with our above definition. In the case of the first cohomology, we calculate as we did in lecture:

$$B^1(G, M) = \{f \in C^1(G, M) : f(g) = m^g - m \text{ for some } m \in M\}$$

then to calculate  $\ker d_1$  we want

$$d_1(f)(g_1, g_2) = f(g_2)^{g_1} - f(g_1 g_2) + f(g_1) = 0$$

so

$$Z^1(G, M) = \{f \in C^1(G, M) : f(g_1g_2) = f(g_2)^{g_1} + f(g_1)\}.$$

We call  $Z^1(G, M)$  the *crossed homomorphisms* and  $B^1(G, M)$  the *principal crossed homomorphisms*.

We now return to the case of a short exact sequence of  $G$ -modules

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0.$$

We can construct a long exact sequence in cohomology

$$\begin{aligned} 0 \longrightarrow H^0(G, L) \longrightarrow H^0(G, M) \longrightarrow H^0(G, N) \xrightarrow{\delta_0} H^1(G, L) \\ \longrightarrow H^1(G, M) \longrightarrow H^1(G, N) \xrightarrow{\delta_1} H^2(G, L) \longrightarrow \dots \end{aligned}$$

The *connecting homomorphisms*  $\delta_n$  are a standard construction in homological algebra. We shall briefly describe  $\delta_0$  explicitly as we shall be primarily be making use of the zeroth and first cohomology in the proof of the weak Mordell-Weil theorem. Let  $n \in H^0(G, N)$ . Then  $n \in N^G$ , so let  $m \in M$  a preimage of  $n$ . We define  $f(g) = m^g - m$ , and notice that  $f$  is in fact a crossed homomorphism, and has range  $L$ . Therefore  $f \in Z^1(G, L)$ , and so we define  $\delta_0(n)$  to be the class of  $f$  in  $H^1(G, L)$ .

*Remark 1.6.* It is important to note here that if  $G$  acts trivially on  $M$ , that is,  $m^g = m$  for all  $g \in G$  and  $m \in M$ , then a crossed homomorphism satisfies

$$f(g_1g_2) = f(g_2) + f(g_1)$$

so is just a homomorphism of  $M$ , and  $B^1(G, M) = 0$ , so

$$H^1(G, M) = \text{Hom}(G, M)$$

when the action of  $G$  is trivial.

Lastly we discuss two common homomorphisms involving subgroups of  $G$ . If  $H$  is a subgroup of  $G$ , then a  $G$ -module  $M$  naturally inherits an  $H$ -module structure. Similarly, by restricting the domain of  $f \in C^n(G, M)$ , we get natural maps  $Z^n(G, M) \rightarrow Z^n(H, M)$  and  $B^n(G, M) \rightarrow B^n(H, M)$ . Therefore we get an induced map which we call the *restriction homomorphism*,

$$\text{Res} : H^n(G, M) \rightarrow H^n(H, M).$$

Now suppose  $H \triangleleft G$ , and notice that  $M^H$  has a natural structure as a  $G/H$ -module. If  $f \in C^n(G/H, M^H)$ , then we can compose  $f$  with the natural projection and injection maps:

$$\begin{array}{ccc} G^n & \dashrightarrow & M \\ \downarrow & & \uparrow \\ (G/H)^n & \xrightarrow{f} & M^H \end{array}$$

to get a map from  $G^n$  to  $M$ . It can easily be seen that this too induces a natural map on the cohomologies, called the *inflation map*

$$\text{Inf} : H^n(G/H, M^H) \rightarrow H^n(G, M).$$

It is not too hard to see [4, Prop. B1.3] that we have an exact sequence

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M).$$

### 1.2.2 Galois Cohomology

The Galois group  $\text{Gal}(\overline{K}/K)$  (which we shall also occasionally denote as  $G_{\overline{K}/K}$  to save space in our diagrams), and all its subgroups, have a natural action on  $E(\overline{K})$  for our elliptic curve  $E/K$ . Recall that the Galois groups for  $L/K$  for finite Galois extensions of  $K$  form a projective system, and in fact

$$\text{Gal}(\overline{K}/K) = \varprojlim \text{Gal}(L/K),$$

and thus is (by definition) a *profinite group*. As a profinite group it has a natural topology which makes it into a topological group by declaring the finite index normal subgroups to be open, and then requiring the group operation and inverse to be continuous.

**Definition 1.7.** A  $\text{Gal}(\overline{K}/K)$ -*module* is an abelian group  $M$  endowed with the discrete topology and an action of  $\text{Gal}(\overline{K}/K)$  on  $M$  that is continuous in this topology.

The construction of the *Galois cohomology groups*  $H^n(\text{Gal}(\overline{K}/K), M)$  mirrors that of the finite case except that we now define  $C^n(\text{Gal}(\overline{K}/K), M)$  to be maps  $\text{Gal}(\overline{K}/K)^n \rightarrow M$  that are continuous with respect to the topologies of  $\text{Gal}(\overline{K}/K)$  and  $M$ . With this construction, all of the results we listed

above for finite group cohomology hold, with the change that we require the subgroups  $H$  of  $G$  which we consider above to be closed. For example, the restriction homomorphism is defined the same way except that we require  $H$  to be a closed subgroup. Note that intermediate fields between  $K$  and  $\overline{K}$  correspond bijectively with the closed subgroups of  $\text{Gal}(\overline{K}/K)$ , and are of the form  $\text{Gal}(\overline{K}/L)$  where  $K \subset L \subset \overline{K}$ .

Lastly we note that  $E(\overline{K})$ , and all of its subgroups, are in fact  $\text{Gal}(\overline{K}/K)$ -modules with the above definition.

### 1.3 Torsion subgroups of Elliptic Curves

We will assume that the reader is familiar with the basic theory of elliptic curves, however, as we will make repeated use of this fact, we pause to note that for  $m \in \mathbb{Z}$ , the “multiplication by  $m$ ” map

$$\begin{aligned} [m] : E(\overline{K}) &\rightarrow E(\overline{K}) \\ P &\mapsto mP \end{aligned}$$

is an isogeny (that is, a morphism that fixes the identity of  $E(K)$ ) of degree  $m^2$  [4, §III.6.4]. Therefore the  $m$ -torsion subgroup

$$E[m] = \ker [m]$$

has order less than or equal to  $m^2$  (see [4, III.4.9]). In particular,  $E[m] \subset E(\overline{K})$  is finite. We record the following obvious result, as we will make use of it in the proof of the weak Mordell-Weil theorem.

**Lemma 1.8.** *For any field  $K$  and a fixed  $m \geq 2$ , there exists a finite extension  $K'/K$  such that  $E[m] \subset E(K')$ .*

*Proof.* As the set  $E[m] \subset E(\overline{K})$  is a finite group, we can adjoin the finite number of coordinates for the points of  $E[m]$  to  $K$ , which are all algebraic, and obtain the finite extension  $K' = K(E[m])$  which is the desired extension.  $\square$

### 1.4 The Technique of Descent

The course of our proof will be to show that  $E(K)/mE(K)$  is finite and then construct a height function that measures the “size” of our points in  $E(K)$

and has enough nice properties to allow us to use the technique of infinite descent. Roughly speaking, we want the set of points of height less than any fixed value to be finite, and we want multiplication by  $m$  to increase the height of a point suitably quickly. Specifically, we prove the following general theorem ([4, VIII.3.1]):

**Theorem 1.9** (Descent). *Suppose we have an abelian group  $A$  such that  $A/mA$  is finite for some integer  $m \geq 2$ , and suppose further that we have a function*

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

*which we call our height function, that satisfies the following properties:*

1. *Fix  $Q \in A$ . There is a constant  $C_1 = C_1(Q)$  such that for all  $P \in A$ ,*

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

2. *There is a constant  $C_2$  for all  $P \in A$ ,*

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

3. *Any set of points of bounded height is finite. That is, for any fixed  $C_3$ ,*

$$\#\{P \in A : h(P) \leq C_3\} < \infty.$$

*Then  $A$  is a finitely generated group.*

*Proof.* Choose  $Q_1, \dots, Q_r \in E(K)$  a set of representatives for the cosets of  $E(K)/mE(K)$ , and let

$$C_1 = \max_{1 \leq i \leq r} C_1(Q_i)$$

where  $C_1(Q_i)$  denotes the constant in property 1 of the height function for each  $Q_i$ . Suppose we have a point  $P$ . We wish to write  $P$  in terms of the  $Q_i$  and a set of points of height less than a constant (which we will determine later). We start by writing:

$$P = Q_{i_1} + mP_1$$

for some  $P_1 \in A$ , and likewise we write  $P_1$  as

$$P_1 = Q_{i_2} + mP_2.$$

We continue writing each  $P_n$  in the same fashion

$$P_{n-1} = Q_{i_n} + mP_n$$

and we wish to show that as we do this, the height of  $P_n$  is decreasing. We apply the properties of the height function to estimate

$$h(P_n) \leq \frac{1}{m^2} (h(mP_n) + C_2).$$

Then using  $P_{n-1} = Q_{i_n} + mP_n$ ,

$$h(P_n) \leq \frac{1}{m^2} (h(P_{n-1}) + C_1 + C_2).$$

We apply the same estimate to write the  $h(P_{n-1})$  in this estimate in terms of  $h(P_{n-2})$  and so forth, finally ending up with the inequality

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right) (C_1 + C_2) \\ &\leq 2^{-n} h(P) + \frac{C_1 + C_2}{m^2 - 2} \leq 2^{-n} h(P) + \frac{C_1 + C_2}{2}. \end{aligned}$$

As we can make  $2^{-n}$  as small as we like for any given  $h(P)$  by taking  $n$  sufficiently large, we find that eventually we can make  $h(P_n) \leq C$  for any constant  $C = C_3 + (C_1 + C_2)/2$  where  $C_3 > 0$ . We fix our value of  $C$ , and then we have shown that we can write any point  $P$  in terms of the  $Q_1, \dots, Q_r$  and a point in  $\{P' \in A : h(P') \leq C\}$ , which by assumption is a finite set. Thus we have our finite set of generators for  $A$ .  $\square$

Returning to  $E(K)$ , we see that it remains to show that  $E(K)/mE(K)$  is finite (the so-called weak Mordell-Weil theorem), and that a suitable height function satisfying the properties listed in theorem 1.9 exists. We start with the weak Mordell-Weil theorem.

## 2 The Weak Mordell-Weil Theorem

We are now ready to begin the proof of the weak Mordell-Weil theorem, which we restate here:

**Theorem 2.1** (Weak Mordell-Weil). *Let  $m \geq 2$ . Then  $E(K)/mE(K)$  is a finite group.*

Let  $E/K$  be our elliptic curve over a number field  $K$ . The basic idea of the proof is to show (lemma 2.8) that if we take a finite extension  $K'/K$  with  $E[m] \subset E(K')$ , such as the extension constructed in lemma 1.8 above, then  $E(K')/mE(K')$  is finite implies that  $E(K)/mE(K)$  is finite as well. So we can assume  $E[m] \subset E(K)$ , and then we construct a perfect pairing (prop. 2.6)

$$E(K)/mE(K) \times \text{Gal}(L/K) \rightarrow E[m]$$

where  $L/K$  is an abelian extension. Then proving that  $L/K$  is finite will show that  $E(K)/mE(K)$  must be finite as well (lemma 2.7).

## 2.1 The Kummer Pairing

We have a natural action of  $\text{Gal}(\bar{K}/K)$  on  $E(\bar{K})$  and all its subgroups. We start with the short exact sequence of  $G_{\bar{K}/K}$ -modules

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

where  $[m]$  as usual denotes the map  $P \mapsto mP$ . We then get a long exact sequence which starts

$$\begin{aligned} 0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta_0} H^1(G_{\bar{K},K}, E[m]) \\ \longrightarrow H^1(G_{\bar{K}/K}, E(\bar{K})) \xrightarrow{[m]} H^1(G_{\bar{K},K}, E(\bar{K})) \longrightarrow \dots \end{aligned}$$

where we have used the fact that  $P \in E(K) \iff P^\sigma = P$  for all  $\sigma \in G_{\bar{K}/K}$  and that the zeroth cohomologies are merely the fixed points of the group action. We extract and combine the last 5 terms listed above to obtain the so-called *Kummer sequence*

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta_0} H^1(G_{\bar{K}/K}, E[m]) \longrightarrow H^1(G_{\bar{K}/K}, E(\bar{K}))[m] \longrightarrow 0$$

where  $H^1(G_{\bar{K}/K}, E(\bar{K}))[m]$  denotes the  $m$ -torsion subgroup of  $H^1(G_{\bar{K}/K}, E(\bar{K}))$ . We compute  $\delta_0$  just as we did above in section 1.2: for any  $P \in E(K)$ , we

let<sup>1</sup>  $Q \in E(\overline{K})$  be a point such that  $mQ = P$ . We then let  $\delta_0(P)$  be the class of crossed homomorphism

$$\begin{aligned} c : G_{\overline{K}/K} &\rightarrow E[m] \\ c(\sigma) &= Q^\sigma - Q. \end{aligned}$$

**Definition 2.2.** We define the *Kummer pairing*

$$\kappa : E(K) \times G_{\overline{K}/K} \rightarrow E[m]$$

by, for any  $P \in E(K)$ , letting  $Q \in E(\overline{K})$  be such that  $mQ = P$  and defining  $\kappa(P, \sigma) = Q^\sigma - Q$ . Note that  $\delta_0(P) = \kappa(P, \cdot)$  above.

The Kummer pairing is, as it is not hard to show, independent of our choice of  $Q$  in general. In the case that matters to us this is most immediately seen when we note:

**Proposition 2.3.** *Suppose  $E[m] \subset E(K)$ . Then the Kummer pairing is well-defined, bilinear, and has kernel  $mE(K)$  on the left.*

*Proof.* Then the action of  $G_{\overline{K}/K}$  on  $E[m]$  is trivial, and therefore as we noted in Remark 1.6,

$$H^1(G_{\overline{K}/K}, E[m]) = \text{Hom}(G_{\overline{K}/K}, E[m]),$$

and thus the connecting homomorphism in the Kummer sequence becomes:

$$\begin{aligned} \delta_0 : E(K)/mE(K) &\hookrightarrow \text{Hom}(G_{\overline{K}/K}, E[m]) \\ P &\mapsto \kappa(P, \cdot) \end{aligned}$$

which gives us the claim. □

**Proposition 2.4.** *The kernel on the right of the Kummer pairing is  $\text{Gal}(\overline{K}/L)$  for the field  $L$  given by*

$$L = K([m]^{-1}E(K))$$

where  $K([m]^{-1}E(K))$  denotes that we are adding all of the (coordinates of the) points  $Q \in E(\overline{K})$  such that  $mQ \in E(K)$ . Further,  $L/K$  is a Galois extension.

---

<sup>1</sup>There are several ways to see that such a  $Q$  must exist. Perhaps easiest is to recall that  $[m]$  is an isogeny, and therefore either trivial or surjective, or we might note that  $\overline{K}$  is algebraically closed and the group law can be written as rational function of the coordinates  $x(P), y(P)$ .

*Proof.* The field  $L$  is well-defined, but that is as much as is immediately clear. Notice that if  $\sigma \in \text{Gal}(\overline{K}/L)$ , then  $\kappa(\cdot, \sigma) = Q^\sigma - Q = O$  (where  $O$  denotes our identity in  $E(K)$ ) since any such  $Q$  coming from a  $P \in E(K)$  lies in  $E(L)$ , and hence is fixed by the action of  $\text{Gal}(\overline{K}/L)$ . Conversely, if  $\sigma \in \text{Gal}(\overline{K}/K)$  is such that  $\kappa(P, \sigma) = O$  for all  $P$ , then it fixes all of the  $Q$  that generate  $L/K$ , and hence it fixes  $L$  as well and  $\sigma \in \text{Gal}(\overline{K}/L)$ .

That  $L/K$  is Galois is immediate, as  $G_{\overline{K}/L}$  is the kernel of a homomorphism and hence normal.  $\square$

**Definition 2.5.** A *perfect pairing*  $f : G \times H \rightarrow A$  is a homomorphism such that  $f(g, \cdot) : H \rightarrow A$  is the trivial homomorphism iff  $g$  is the identity of  $G$  and  $f(\cdot, h) : G \rightarrow A$  is trivial homomorphism iff  $h$  is the identity of  $H$ .

Then from propositions 2.3 and 2.4 it is immediate that:

**Proposition 2.6.** *The Kummer pairing induces a perfect pairing*

$$\kappa : E(K)/mE(K) \times \text{Gal}(L/K) \rightarrow E[m]$$

where  $L$  is the field defined in prop. 2.4.

Perfect pairings have the following nice property:

**Lemma 2.7.** *Let  $f : G \times H \rightarrow A$  be a perfect bilinear pairing into an abelian group  $A$ . Then if  $A$  is finite, either  $G$  and  $H$  are both infinite, or  $G$  and  $H$  are both finite.*

*Proof.* Without loss of generality, suppose  $G$  is finite and  $H$  is infinite. Note that  $\text{Hom}(G, A) \subset \text{Maps}(G, A)$  is a finite set, since both  $G$  and  $A$  are finite. Then we have the map

$$\begin{aligned} H &\rightarrow \text{Hom}(G, A) \\ h &\mapsto f(\cdot, h) \end{aligned}$$

of the infinite group  $H$  into the finite group  $\text{Hom}(G, A)$ . But then this map must have a nontrivial kernel, which is a contradiction to  $f$  being a perfect pairing.  $\square$

Our purpose should now be clear: as the Kummer pairing

$$\kappa : E(K)/mE(K) \times \text{Gal}(L/K) \rightarrow E[m]$$

is perfect, we have that  $E(K)/mE(K)$  is finite iff  $\text{Gal}(L/K)$  is finite, so we will show that  $L/K$  is a finite extension. First, however, let us prove the reduction lemma which we allowed us to assume that  $E[m] \subset E(K)$ .

## 2.2 A reduction lemma

**Lemma 2.8.** *Suppose  $K'/K$  is a finite Galois extension with  $E[m] \subset E(K')$ , and  $E(K')/mE(K')$  is finite. Then  $E(K)/mE(K)$  is finite.*

*Proof.* Note that we have a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \frac{E(K) \cap mE(K')}{mE(K)} & \xrightarrow{i} & E(K)/mE(K) & \longrightarrow & E(K')/mE(K') \\
 & & \downarrow \phi & & \downarrow \delta_0 & & \downarrow \delta'_0 \\
 0 & \longrightarrow & H^1(G_{L/K}, E[m]) & \xrightarrow{\text{Inf}} & H^1(G_{\bar{K}/K}, E[m]) & \xrightarrow{\text{Res}} & H^1(G_{\bar{K}'/K'}, E[m])
 \end{array}$$

where  $\delta_0, \delta'_0$  come from the connecting homomorphisms in the Kummer sequence and we noted above were injective, and  $\phi$  must be injective because  $\text{Inf} \circ \phi = \delta_0 \circ i$  is injective.

Now we note that  $(E(K) \cap mE(K'))/mE(K)$  is finite, because we have an injection into  $H^1(G_{L/K}, E[m])$ , which is a finite group because  $G_{L/K}$  and  $E[m]$  are both finite. By assumption,  $E(K')/mE(K')$  is finite as well, and therefore by the exactness of the top row,  $E(K)/mE(K)$  must be finite as well, which is what we wanted to show.  $\square$

Thus if necessary we can substitute  $K' = K(E[m])$  for  $K$  in our proof of the weak Mordell-Weil theorem and the proof is unaffected, so the assumption of prop. 2.3 is valid.

## 2.3 Finiteness of $L/K$

It remains to show that the field

$$L = K([m]^{-1}E(K))$$

defined in prop. 2.4 is a finite extension of  $K$ , and then proposition 2.6 and lemma 2.7 imply that  $E(K)/mE(K)$  is finite, which is the weak Mordell-Weil theorem. We will sketch the idea of the proof so as not to get too deeply into the class field theory and Kummer field theory behind the proof. The basic idea is to note that we have a finite set  $S \subset M_K$  of bad places which we can exclude so that  $E/K$  has good reduction over the places of  $M_K \setminus S$ . Then it can be shown that  $L/K$  is a maximal abelian extension of exponent  $m$  which is unramified outside of the places of  $S$ , and that any such extension must be finite. The proof can be found in [4, §VIII.1.4-6].

### 3 Measuring Height

From the descent theorem (1.9 above) and the weak Mordell-Weil theorem (2.1) we see that our proof of the Mordell-Weil theorem will be complete once we construct an appropriate height function on  $E(K)$ . We begin by defining height functions on  $\mathbb{P}^n(K)$  and  $\mathbb{P}^n(\overline{K})$ .

#### 3.1 Heights on $\mathbb{P}^n$

Over  $\mathbb{P}^n(\mathbb{Q})$  our starting point in measuring the height of a point  $P = [x_0, \dots, x_n]$  would be to clear denominators and remove common factors so that the coordinates  $x_i$  all lie in the ring of integers  $\mathbb{Z}$  and such that  $\gcd(x_0, \dots, x_n) = 1$ , and then define  $H(P) = \max\{|x_0|, \dots, |x_n|\}$ . Most proofs of the Mordell-Weil theorem over  $\mathbb{Q}$  start in this manner (see for ex. [1] or [3]). We are concerned with working over a number field  $K/\mathbb{Q}$ , so our construction must be more subtle. Let  $M_K$  denote the set of *standard* absolute values on  $K$ , that is, absolute values  $|\cdot|_v$  that restrict to a  $p$ -adic absolute value or the archimedean absolute value  $|\cdot|_\infty$  on  $\mathbb{Q}$ . As usual, we let  $K_v$  and  $\mathbb{Q}_v$  denote the completion of  $K$  and  $\mathbb{Q}$ , respectively, with respect to the absolute value  $|\cdot|_v$ . As  $K/\mathbb{Q}$  is a field extension, so too do we naturally have a field extension  $K_v/\mathbb{Q}_v$ . Define the *local degree at  $v$*  to be the degree of this extension,

$$n_v = [K_v : \mathbb{Q}_v].$$

We recall two very basic results about valuations [4, §VIII5.2,5.3]:

**Lemma 3.1** (Extension). *If  $L \supset K \supset \mathbb{Q}$  is a tower of number fields, and  $v \in M_K$ , then*

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K]n_v,$$

where  $w|v$  denotes  $w$  lies over  $v$ , that is,  $w$  restricts to  $v$  on  $K$ , and the sum is over such  $w$ .

**Lemma 3.2** (Product Formula). *If  $x \in K^\times$ , then*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1.$$

Taking our inspiration from the product formula, we now define our basic height function on  $\mathbb{P}^n(K)$ , and we will then show how to extend this notion to  $\mathbb{P}^n(\overline{\mathbb{Q}})$ .

**Definition 3.3.** Let  $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$ . Then the *height of  $P$  relative to  $K$*  is defined to be

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \dots, |x_n|_v\}^{n_v}.$$

The product formula 3.2 ensures that this is well-defined, and note too that it implies that  $H_K(P) \geq 1$ .

Observe that by the extension formula 3.1, if  $P \in \mathbb{P}^n(K)$  and  $L/K$  is a finite extension then

$$H_L(P) = H_K(P)^{[L:K]}.$$

This motivates our definition of the *absolute height* for any  $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ :

**Definition 3.4.** Let  $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$  for some number field  $K$  (we can find or construct such a field for any  $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ , simply by adjoining its coordinates, for example). Then the *absolute height* is defined to be

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

The extension formula 3.1 ensures that this definition is independent of the particular choice of  $K$ .

*Remark 3.5.* Notice that when  $P \in \mathbb{P}^n(\mathbb{Q})$ , if we write  $P = [x_0, \dots, x_n]$  with  $x_i \in \mathbb{Z}$  and such that  $\gcd(x_0, \dots, x_n) = 1$ , then for each non-archimedean absolute value  $|\cdot|_p$  there is some coordinate such that  $p \nmid x_i$  and hence  $|x_i|_p = 1$ , and therefore in the product  $H_{\mathbb{Q}}(P)$ , all of the terms are 1 except  $\max\{|x_0|_{\infty}, \dots, |x_n|_{\infty}\}$ . Therefore  $H(P)$  agrees with the “naïve” measure of height over  $\mathbb{Q}$  which we mentioned above.

We can describe the behavior of our measure of height through the following theorem:

**Theorem 3.6.** Let  $\phi : \mathbb{P}^n \rightarrow \mathbb{P}^m$  be a morphism of degree  $d$ . Then for any  $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ ,

$$H(\phi(P)) \asymp_{\phi} H(P)^d$$

where<sup>2</sup> the subscript indicates that the implied constants depend only on the particular morphism  $\phi$ .

---

<sup>2</sup>Recall that  $f \asymp g$  iff  $f \ll g$  and  $g \ll f$ .

*Proof.* The proof is computational in nature but not short. The interested reader is referred to [4, §VIII.5.6].  $\square$

If we think about our multiplication by  $m$  map as an isogeny of  $E$ , then we see that our absolute height behaves in a sense multiplicatively. As we want our height to behave additively, we will eventually define our height function as a logarithm of the absolute height  $H$  which we are currently developing.

The following proposition is used in proving the next theorem, and we will have use of it in proving the key property of our height function for  $E(K)$  in the next section as well:

**Proposition 3.7.** *Let  $f(x) = \sum_{i=0}^n a_i x^i \in \overline{\mathbb{Q}}[x]$  be a polynomial, and denote its roots in  $\overline{\mathbb{Q}}$  by  $\alpha_1, \dots, \alpha_n$ . Then*

$$2^{-n} H(\alpha_1) \cdots H(\alpha_n) \leq H([a_0, \dots, a_n]) \leq 2^{n-1} H(\alpha_1) \cdots H(\alpha_n).$$

*Proof.* See [4, §VIII.5.9].  $\square$

We note that our height function satisfies the important property that the set of points with height less than a fixed value is finite.

**Theorem 3.8.** *For any number field  $K/\mathbb{Q}$  and fixed constant value  $C$ , we have*

$$\#\{P \in \mathbb{P}^n(K) : H(P) \leq C\} < \infty.$$

*Proof.* The proof relies on a few easy estimates on  $H(P)$  and then a clever application of proposition 3.7 to the minimal polynomial for a coordinate of  $P$  over  $\mathbb{Q}$ . The details can be found in [4, §VIII.5.5].  $\square$

## 3.2 Heights on $E(K)$

As we noted above,  $H(P)$  behaves multiplicatively, so we will work with the logarithmic height:

**Definition 3.9.** Let  $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ . Then the *absolute logarithmic height* is defined to be

$$h(P) = \log H(P)$$

where  $H(P)$  is the absolute height defined in 3.4.

Recall that  $K(E)$  (or  $\overline{K}(E)$ ) is the field of rational functions over  $K$  (resp.  $\overline{K}$ ) on  $E$ . Note that if  $f \in K(E)$  is nonconstant, then it defines a nontrivial morphism of finite degree to  $\mathbb{P}^1$  by  $f(P) = [f(P), 1]$  if  $f(P)$  does not have a pole at  $P$ , and  $f(P) = [1, 0]$  if  $P$  is a pole of  $f$ . In particular,  $f$  is finite-to-one.

For any  $f \in \overline{K}(E)$ , we can define a height  $h_f(P) = h(f(P))$  that measures the size of points of  $E(\overline{K})$  under  $f$ .

**Theorem 3.10.** *Let  $f \in K(E)$  be a nonconstant rational function on  $E$  with coefficients in  $K$ . Then the set of points such that  $h_f(P) \leq C$  for any fixed  $C$  is finite.*

*Proof.* Note that if  $f$  is nonconstant, then as we noted above it defines a nontrivial morphism of finite degree to  $\mathbb{P}^1$ , and in particular  $f$  is finite-to-one. Then the result follows immediately from the finiteness of points less than or equal to a fixed height given in theorem 3.8 above.  $\square$

**Theorem 3.11** ([4, §VIII.6.2]). *Let  $E/K$  be given by a Weierstrass equation form*

$$E : y^2 = x^3 + Ax + B$$

*which we can do because we are in characteristic zero. Then  $x \in K(E)$  is even in the sense that  $x \circ [-1] = x$  as morphisms. Then for any  $P, Q \in E(\overline{K})$ ,*

$$h_x(P + Q) + h_x(P - Q) = 2h_x(P) + 2h_x(Q) + O_E(1)$$

*where the subscript indicates that the implied constant of the big- $O$  error term depends only on the elliptic curve  $E$  and not the points  $P, Q$ .*

*Proof.* We first note that if  $P$  or  $Q$  is the identity, the statement is trivial, so we can assume  $P, Q \neq O$ . We write

$$x(P) = [x_1, 1], \quad x(Q) = [x_2, 1], \quad x(P + Q) = [x_3, 1], \quad x(P - Q) = [x_4, 1].$$

Then the group law for an elliptic curve tells us that

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}$$

$$x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}.$$

This leads us to define a map  $g([t, u, v]) = [u^2 - 4tv, 2u(At + v) + 4Bt^2, (v - At)^2 - 4Btu]$ . Then if we let  $G : E \times E \rightarrow E \times E$  be given by  $G(P, Q) = (P + Q, P - Q)$ , we have a commutative diagram

$$\begin{array}{ccc}
 E \times E & \xrightarrow{G} & E \times E \\
 \downarrow & & \downarrow \\
 \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \\
 \downarrow & & \downarrow \\
 \mathbb{P}^2 & \xrightarrow{g} & \mathbb{P}^2
 \end{array}$$

$\sigma$  (curved arrow from top-left to bottom-left)       $\sigma$  (curved arrow from top-right to bottom-right)

where we define  $\sigma$  to be the composition of  $x(\cdot) \times x(\cdot) : E \times E \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$  with the map  $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^2 : ([u_1, v_1], [u_2, v_2]) \mapsto [v_1v_2, u_1v_2 + u_2v_1, u_1u_2]$ . Then it is easy to see that if  $E$  is smooth (which we always assume it is),  $g$  is a morphism and  $\deg g = 2$ . Our theorem 3.6, when we take logarithms, tells us that for a degree  $d$  morphism  $\phi$  we have:

$$h(\phi(P)) = dh(P) + O(1)$$

so in particular from our diagram we see that

$$h(\sigma(P + Q, P - Q)) = h(g \circ \sigma(P, Q)) = 2h(\sigma(P, Q)) + O(1).$$

Thus if we can show that for any  $P, Q$ ,  $h(\sigma(P, Q)) = h_x(P) + h_x(Q) + O(1)$  then we can apply it to both sides of the above equation and we will have the desired result. Note that

$$h(\sigma(P, Q)) = h([1, x_1 + x_2, x_1x_2])$$

But  $1, x_1 + x_2, x_1x_2$  are the coefficients of the polynomial  $(t - x_1)(t - x_2) \in \overline{\mathbb{Q}}[t]$ , and therefore we can apply proposition 3.7 and (upon taking logarithms) we find that

$$h(x_1) + h(x_2) - \log 4 \leq h(\sigma(P, Q)) \leq h(x_1) + h(x_2) + \log 2,$$

that is,

$$h(\sigma(P, Q)) = h(x_1) + h(x_2) + O(1).$$

But  $h(x_1) = h_x(P)$  and  $h(x_2) = h_x(Q)$  by definition, so we have the desired result.  $\square$

Theorem 3.11 immediately gives us the remaining properties of  $h_x$  which we wished to establish.

**Corollary 3.12.** *For any fixed  $Q \in E(\overline{K})$ , we have*

$$h_x(P + Q) \leq 2h_x(P) + C_1$$

for all  $P \in E(\overline{K})$  and some constant  $C_1 = C_1(Q)$ .

*Proof.* We take

$$h_x(P + Q) + h_x(P - Q) = 2h_x(P) + 2h_x(Q) + O_E(1)$$

and note that  $h_x(\cdot) \geq 0$  because  $H(\cdot) \geq 1$ , therefore we can drop the  $h_x(P - Q)$ , and absorb  $2h_x(Q)$  into the implied constant (hence the dependence of  $C_1$  on  $Q$ ) and we have

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

□

**Proposition 3.13.** *For any  $m \in \mathbb{Z}$ , we have*

$$h_x(mP) = m^2h_x(P) + O(1)$$

for all  $P \in E(\overline{K})$ , and consequently there exists a constant  $C_2$  such that

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

*Proof.* The proof is by induction. We note that we need only consider  $m \geq 0$  as  $h_x$  is an even function. The base cases of  $m = 0, 1$  are trivial. Then we use theorem 3.11 to get

$$h_x((m + 1)P) = -h_x((m - 1)P) + 2h_x(mP) + 2h_x(P) + O(1)$$

and by the induction hypothesis applied to  $h_x((m - 1)P)$  and  $h_x(mP)$ ,

$$h_x((m + 1)P) = (2m^2 - (m - 1)^2 + 2)h_x(P) + O(1) = (m + 1)^2h_x(P) + O(1)$$

and the proof is complete. □

*Remark 3.14.* We note in passing that we have shown that these results hold for all points in  $E(\overline{K})$ , but we only need them to hold  $E(K)$  to apply the descent theorem.

We proved in theorem 3.10 above that the set of points less than a fixed height is finite. Therefore, with corollary 3.12 and proposition 3.13, we have shown that our function  $h_x : E(K) \rightarrow \mathbb{R}$  satisfies all of the properties for a height function required by the descent theorem 1.9, and thus we have completed our proof of the Mordell-Weil theorem. Although we used  $h_x$  to complete our proof of the Mordell-Weil theorem,  $h_x$  is by no means the only height function on  $E(K)$  that meets the requirements of the descent theorem. We could have easily extended our results to even, and odd,  $f \in K(E)$ . It was also discovered by Néron and Tate that there is a canonical height that is a limit of  $h_f$  and is an actual quadratic form (which is to say, we have no error term in theorem 3.11). The interested reader is referred to [4, §VIII.9].

## References

- [1] Knapp, Anthony. *Elliptic Curves*. Mathematical Notes 40, Princeton University Press, Princeton, 1992.
- [2] Lang, S.; Néron, A. *Rational points of abelian varieties over function fields*. Amer. J. Math. 81, 1959 95–118.
- [3] Milne, J. *Elliptic Curves*, Course notes. Available online at <http://www.jmilne.org/math/CourseNotes/math679.html>.
- [4] Silverman, J. *The Arithmetic of Elliptic Curves*. Springer, New York, 1986.