

## Heights on Abelian Varieties

We want  $h : A(K) \rightarrow [0, \infty)$  (with  $K$  a global field) such that

1.  $\{P : h(P) \leq c\}$  is finite for all  $c$ ,
2.  $h(mP) = m^2h(P) + O(1)$ ,
3.  $\forall P_0 \in A(K), \exists c(P_0)$  such that  $h(P + P_0) \leq 2h(P) + c(P_0)$ .

We defined a height function  $h : \mathbb{P}^n \rightarrow [0, \infty)$ . As  $A \hookrightarrow \mathbb{P}^n$ , we get a height function on  $A$ . It satisfies 1 automatically. We proved “ $h(\Phi(a)) \leq dh(a) + O(1)$ .” This implies 3 and  $h(mP) \leq m^2h(P) + O(1)$  (multiplication by  $m$  is a degree  $m^2$  polynomial map). We will only show this for elliptic curves and  $m = 2$ .

To get the lower bound on 2 requires some extra geometric properties of the embedding  $A \hookrightarrow \mathbb{P}^n$ ; namely, the map  $P \mapsto -P$  is induced by a linear transformation of  $\mathbb{P}^n$ .

**Remark.** Different embeddings  $A \hookrightarrow \mathbb{P}^n$  give different heights.

We will do the proof in detail now for elliptic curves and  $m = 2$ :

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

$P_0 = (x_0, y_0)$ ,  $P = (x, y)$ ,  $h((x, y)) = h((1 : x : y))$ . The equation  $y^2 = x^3 + ax + b$  implies  $3h(x) = 2h(y) + O(1)$ . It is sufficient to work with  $h(x)$ ; i.e. with the function  $(x, y) \mapsto h(x)$ .

We start with property 3.  $P + P_0$  has  $x$ -coordinate given by

$$\begin{aligned} \left(\frac{y - y_0}{x - x_0}\right)^2 - (x + x_0) &= \frac{(y - y_0)^2 - (x + x_0)(x^2 - 2xx_0 + x_0^2)}{(x - x_0)^2} \\ &= \frac{x^3 + ax + b - 2yy_0 + y_0^2 - (x^3 - x^2x_0 - xx_0^2 + x_0^3)}{(x - x_0)^2} \\ &= \frac{2yy_0 - y_0^2 + ax + b + x^2x_0 + xx_0^2 - x_0^3}{(x - x_0)^2}. \end{aligned}$$

The numerator and denominator have degree 2 in  $x$  and degree 1 in  $y$ . So “ $h(\Phi(a)) \leq dh(a) + O(1)$ ” gives 3.

Now 2. The  $x$ -coordinate of  $2P$  is given by

$$\begin{aligned} \left(\frac{3x^2 + a}{2y}\right)^2 &= \frac{(3x^2 + a)^2 - 8xy^2}{4y^2} \\ &= \frac{(3x^2 + a)^2 - 8x(x^3 + ax + b)}{4(x^3 + ax + b)} = \frac{A(x)}{B(x)}, \end{aligned}$$

where  $\deg A = 4$ ,  $\deg B = 3$ ; so “ $h(\Phi(a)) \leq dh(a) + O(1)$ ” gives  $h(2P) \leq 4h(P) + O(1)$ . Now we just need to show  $h(2P) \geq 4h(P) + O(1)$

$$h(2P) = h\left(\frac{A(x)}{B(x)}\right) = \sum_v n_v \log(\max\{|A(x)|_v, |B(x)|_v\})$$

likewise,

$$h(P) = h(x) = \sum_v n_v \log(\max\{|x|_v, 1\}).$$

Assume  $|x|_v > 1$ ,

$$\begin{aligned} |A(x)|_v &= |a_0x^4 + a_1x^3 + \cdots + a_n|_v \\ &= |x^4|_v |a_0 + a_1x^{-1} + \cdots + a_nx^{-4}|_v \\ &\geq |x|_v^4 (|a_0|_v - |x|_v^{-1} |a_1 + \cdots + a_nx^{-3}|_v) \\ &\geq |x|_v^4 (|a_0|_v - C_v), \end{aligned}$$

for some constant  $C_v$ . Thus,  $\log(|A(x)|_v) \geq 4 \log(|x|_v) + C'_v$ . Note in the non-archimedean case, we can take  $C_v = 1$  using the strong triangle inequality. Also  $|a_0|_v$  is almost always 1 (that is, all but finitely many are 1). Likewise for  $B$ , we have  $|B(x)|_v \leq |x|_v^3 + C_v$ ; so for those  $v$  with  $|x|_v > 1$ , we get

$$\log(\max\{|A(x)|_v, |B(x)|_v\}) \geq 4 \log(|x|_v) + C'_v,$$

where the  $C'_v$  are almost always 0.

Now look at  $|x|_v \leq 1$ . Then  $\log(\max\{|x|_v, 1\}) = 0$ ; so we want to show  $\log(\max\{|A(x)|_v, |B(x)|_v\}) \geq C'_v$  with  $C'_v = 0$  for all but finitely many  $v$ . Now  $B(x) = 4f(x)$  (where  $f(x) = x^3 + ax + b$ ) and  $A(x) = (f'(x))^{1/2} - 2xf(x)$ .

**Claim.**  $(A(x), B(x)) = 1$ .

*Proof.* If  $p(x)|B(x)$  then  $p(x)|f(x)$ . If also  $p(x)|A(x)$ , then  $p(x)|f'(x)$ . But  $(f(x), f'(x)) = 1$ , since  $f(x)$  has distinct roots (as we are working on an elliptic curve).  $\square$

Then  $\exists u(x), v(x) \in K[x]$  such that  $u(x)A(x) + v(x)B(x) = 1$ . Hence

$$\begin{aligned} 1 &= |u(x)A(x) + v(x)B(x)| \\ &\leq C_v'' \max\{|A(x)|_v, |B(x)|_v\} \quad C_v'' = 1 \text{ for almost all } v, \end{aligned}$$

(the non-archimedean case). So  $\max\{|A(x)|_v, |B(x)|_v\} \geq C_v'$ .

This gives us our desired height function; so we have proven the Mordell-Weil Theorem.

## Néron-Tate canonical height

The *canonical height* is a positive-definite quadratic form on  $A(\overline{K})$  modulo torsion;  $\hat{h}(mP) = m^2\hat{h}(P)$ , and  $\hat{h}(P) = 0$  if and only if  $P$  is torsion.

**Néron's approach:**

$$\hat{h}(P) = \sum_v \lambda_v(P).$$

**Tate's approach:**

$$\hat{h}(P) = \lim_{n \rightarrow \infty} \frac{h(2^n P)}{4^n}.$$

We have  $h(2P) \sim 4h(P)$ , which implies  $\frac{h(2P)}{4} \sim h(P)$ ; thus

$$\left\{ \frac{h(2^n P)}{4^n} \right\} \text{ is a Cauchy sequence.}$$

Formally, you get  $\hat{h}(2P) = 4\hat{h}(P)$ ; one needs to prove it works for all values of  $m$ .

**Remark.** Now everytime you have a positive-definite quadratic form on a finitely generated abelian group  $\Gamma$  of rank  $r$  means that you can embed  $\Gamma$  in  $\mathbb{R}^r$  in such a way that the quadratic form is the restriction of  $\sum x_i^2$ . This leads to many geometric question about the resulting lattice.

## Open Problems

1. What is the “shape” of the Lattice? (square, skew, etc.)
2. Finding lower bounds for the smallest positive value of  $\hat{h}(P)$  for  $P \in A(K)$ . (There is a conjecture of Lang in this direction.)
3. Are there elliptic curves  $E$  over  $\mathbb{Q}$  with rank  $E(\mathbb{Q})$  of arbitrarily large values? (The largest known is something like 28.)
4. How often is the rank large? More generally, what is the distribution of ranks?
5. For elliptic curves, there is a bound  $C(K)$  such that  $\#(E(K))_{\text{tors}} \leq C(K)$  for all  $E/K$ . Does the corresponding statement hold for abelian varieties of fixed dimension? (It is known that  $C(\mathbb{Q}) = 16$ . Note for number fields  $C(K)$  depends on  $[K : \mathbb{Q}]$ .)
6. Birch and Swinnerton-Dyer Conjecture (to be discussed)

**Remark.** Some key facts about the proof of  $C(\mathbb{Q}) = 16$ . Let  $Y_1(m)$  be the set of isomorphism classes of pairs  $(E, P)$ , where  $E$  is an elliptic curve  $P \in E$  is of order  $m$ . It turns out that  $Y_1(m)$  is an algebraic curve; It has a map to  $\mathbb{A}^1$  via the  $j$ -invariant which comes from  $(E, P) \mapsto E$ . One finds that  $Y_1(m)(\mathbb{Q})$  is finite if the genus of  $Y_1(m)$  is at least 2. For  $m$  large, the set is actually empty. Proving  $C(\mathbb{Q}) = 16$  is extremely difficult.