

An Introduction to Height Functions

Joseph H. Silverman

Brown University

MSRI Workshop on Rational and Integral Points
on Higher-Dimensional Varieties

Jan 17–21, 2006

What Are Height Functions

Let X/K be a variety over a number field K .

A **height function** on $X(K)$ is a function

$$H : X(K) \longrightarrow \mathbb{R}$$

whose value $H(P)$ measures the *arithmetic complexity* of the point P .

For example, in some sense the rational numbers

$$\frac{1}{2} \quad \text{and} \quad \frac{100000}{200001}$$

are “close” to one another, but intuitively the second is more arithmetically complicated than the first.

Guiding Principles for a Theory of Height Functions:

- (1) Only finitely many points of bounded height.
- (2) Geometric relations lead to height relations.

Heights on Projective Space

The Height of \mathbb{Q} -Rational Points

The **height** of a rational number $a/b \in \mathbb{Q}$, written in lowest terms, is

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

More generally, the **height** of a point $P \in \mathbb{P}^N(\mathbb{Q})$ is defined by writing

$$P = [x_0, \dots, x_N] \quad \text{with} \\ x_0, \dots, x_N \in \mathbb{Z} \quad \text{and} \quad \gcd(x_0, \dots, x_N) = 1$$

and setting

$$H(P) = \max\{|x_0|, \dots, |x_N|\}.$$

It is easy to see that there are only finitely many points $P \in \mathbb{P}^N(\mathbb{Q})$ with height $H(P) \leq B$.

The Height of Points over Number Fields

Let K/\mathbb{Q} be a number field and let M_K be a complete set of (normalized) absolute values on K . Thus M_K contains an archimedean absolute value for each embedding of K into \mathbb{R} or \mathbb{C} and a p -adic absolute value for each prime ideal in the ring of integers of K .

The **height** of a point $P = [x_0, \dots, x_N] \in \mathbb{P}^N(K)$ is defined by

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

It is often convenient to use the **absolute logarithmic height**

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \log H_K(P).$$

The absolute height is well-defined for $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$.

A Finiteness Property of the Height on \mathbb{P}^N

The height satisfies a fundamental finiteness property.

Theorem. (*Northcott*) There are only finitely many $P \in \mathbb{P}^N(K)$ with $H_K(P) \leq B$.

Corollary. (*Kronecker's Theorem*) Let $\alpha \in K^*$. Then $H_K(\alpha) = 1$ if and only if α is a root of unity.

Proof. Suppose $H_K(\alpha) = 1$. Then

$$H_K(\alpha^n) = H_K(\alpha)^n = 1 \quad \text{for all } n \geq 1.$$

Hence $\{1, \alpha, \alpha^2, \dots\}$ is a set of bounded height, hence finite, hence $\alpha^i = \alpha^j$ for some $i > j$. Therefore α is a root of unity. (The other direction is trivial.) QED

More generally, there are only finitely many points of bounded height and bounded degree:

$$\#\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : h(P) \leq b \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\} < \infty$$

Two Ways in Which Height Functions Are Used

Let $V/K \subset \mathbb{P}_K^N$ be a variety and let $\mathcal{S} \subset V(K)$ be a set of “arithmetic interest.”

- (1) In order to prove that \mathcal{S} is finite, show that it is a set of bounded height.
- (2) If \mathcal{S} is infinite, describe its “density” by estimating the growth rate of the **counting function**

$$N(\mathcal{S}, B) = \#\{P \in \mathcal{S} : H_K(P) \leq B\}$$

Example. Consider $\mathbb{Q} \subset \mathbb{P}^1(\mathbb{Q})$. Then

$$\begin{aligned} N(\mathbb{Q}, B) &= \#\left\{\frac{a}{b} \in \mathbb{Q} : H\left(\frac{a}{b}\right) \leq B\right\} \\ &= \frac{12}{\pi^2} B^2 + O(B \log B) \quad \text{as } B \rightarrow \infty. \end{aligned}$$

Counting Algebraic Points in \mathbb{P}^N

More generally, it is an interesting problem to estimate the size of the set

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq B\}$$

as a function of B .

Theorem. (*Schanuel*) As $B \rightarrow \infty$,

$$\#\{P \in \mathbb{P}^N(K) : H_K(P) \leq B\} \sim C_{K,N} B^{N+1}.$$

The constant $C_{K,N}$ is given explicitly by

$$C_{K,N} = \frac{h_K R_K / w_K}{\zeta_K(N+1)} \left(\frac{2^{r_1} (2\pi)^{r_2}}{\sqrt{\text{Disc}_K}} \right)^{N+1} (N+1)^{r_1+r_2-1}.$$

The quest for analogous counting formulas for other varieties is the subject of much current research. It will be discussed in detail by other speakers at this workshop.

A Transformation Property of the Height on \mathbb{P}^N

The height satisfies a natural transformation property.

Theorem. Let $\phi : \mathbb{P}^N \rightarrow \mathbb{P}^M$ be a *morphism* of degree d . Then

$$dh(P) - C_{1,\phi} \leq h(\phi(P)) \leq dh(P) + C_{2,\phi}$$

for all $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$.

- The proof of the upper bound uses only the triangle inequality. It holds even if ϕ is only a rational map.
- The proof of the lower bound requires some version of the Nullstellensatz.
- Notice how the theorem translates geometric information (the degree of ϕ) into arithmetic information (relation among heights).

Heights on Projective Varieties

Heights on Projective Varieties

Let X be a projective variety with a given projective embedding

$$\phi : X \hookrightarrow \mathbb{P}^N.$$

(Everything defined over $\bar{\mathbb{Q}}$.)

The embedding allows us to define a height function

$$h_\phi : X(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}, \quad h_\phi(P) = h(\phi(P)).$$

More intrinsically, a projective embedding corresponds to a very ample divisor D and choice of sections generating $\mathcal{L}(D)$.

So for each very ample divisor D we can choose an embedding $\phi_D : X \rightarrow \mathbb{P}^N$ and get a height function

$$h_D : X(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}, \quad h_D(P) = h(\phi_D(P)).$$

These height functions have the following properties:

- (1) Choosing a different embedding ϕ'_D only changes h_D by a bounded function. We write

$$h(\phi_D(P)) = h(\phi'_D(P)) + O(1),$$

where the $O(1)$ represents a function that is bounded independent of the choice of $P \in X(\bar{\mathbb{Q}})$.

- (2) If $D \sim E$ (linear equivalence), then

$$h_D = h_E + O(1).$$

So up to a bounded function, h_D only depends on the linear equivalence class of D .

- (3) If D and E are both very ample, then

$$h_{D+E} = h_D + h_E + O(1).$$

The Weil Height Machine

There is a (unique) *homomorphism*

$$h : \text{Pic}(X) \longrightarrow \frac{(\text{Functions } X(\bar{\mathbb{Q}}) \rightarrow \mathbb{R})}{(\text{Bounded Functions } X(\bar{\mathbb{Q}}) \rightarrow \mathbb{R})}$$

satisfying:

- **Normalization:** If D is very ample, then

$$h_D = h \circ \phi_D + O(1).$$

- **Functoriality:** Let $\phi : X \rightarrow Y$ be a morphism.

Then

$$h_{X, \phi^*D} = h_{Y, D} \circ \phi + O(1).$$

- **Positivity:** $h_D \geq O(1)$ for all points not in the base locus of D .

The Weil Height Machine

Normalization says that height functions contain a great deal of arithmetic information.

Additivity and functoriality for morphisms say that



Thus Weil's Height Machine may be viewed as a tool that turns geometry into arithmetic.

Heights on Abelian Varieties

Abelian Varieties

Recall that an **abelian variety** is a projective variety A that has a group structure given by morphisms

$$\begin{aligned} + : A \times A &\xrightarrow{\text{addition}} A, \\ [-1] : A &\xrightarrow{\text{inversion}} A. \end{aligned}$$

In particular, for every integer m there is a **multiplication-by- m morphism**

$$[m] : A \longrightarrow A, \quad [m](P) = \underbrace{P + P + \cdots + P}_{m \text{ copies}}.$$

A Divisor Relation on Abelian Varieties

An important divisor relation that is a consequence of the theorem of the cube:

Theorem. Let $D \in \text{Div}(A)$ be a symmetric divisor, i.e., $[-1]^*D \sim D$. Then

$$[m]^*D \sim m^2D.$$

This immediately yields a relation on heights:

$$h_D([m]P) = m^2h_D(P) + O(1) \quad \text{for all } P \in A(\bar{\mathbb{Q}}).$$

Thus multiplication-by- m greatly increases the height of a point. Roughly, the coordinates of mP have $O(m^2)$ digits.

The Quadratic Growth of the Height on Abelian Varieties

We illustrate with the elliptic curve and point

$$E : y^2 = x^3 + x + 1 \quad \text{and} \quad P = (0, 1).$$

Here is a table of $H(x(nP))$ for $n = 1, 2, \dots, 25$.

1	1
2	2
3	13
4	36
5	685
6	7082
7	196249
8	9781441
9	645430801
10	54088691834
11	23545957758733
12	3348618159624516
13	3438505996705270765
14	2389279734043328028530
15	3568842156502352911081681
16	9147174028201584695660404993
17	40437302897155037003168469209281
18	144041052884595077187155035625188225
19	4077551427539061268365818617070082487981
20	29247742836717181569573123126609380958628633
21	1644662183623605030943992459758717959368038089933
22	76795559807444450146033952048248025474377706486132570
23	6037390795706541540397642739132383429233648456214266105001
24	816297679393916005694837838808362431503501229559444925278681793
25	242513738949178952234806483689465816559631390124939658301320990605073
26	47803232530993255659471421491008524334965293857886857075847338386784976289
27	67559659782039617237841184516992302782851604142385500859648938761010393239431661
28	32014345486637038681521545788678891610665676156825092102996356573331436095404542962201
29	75366079100860358183774143789438882594269554344230013075428451465317687946832468865183904333
30	235596097713466330738098972552422422374156906907547045290688341377958875910979032848694872594995042
31	949929776724866709094954536710367778326401614961417743163923974793524931042092311077415673676701373662241
32	6939337780803547166840419022721964472182663632045063388197164628060008767530358928827755424306465309623700644865
33	138560009627230805680861712729089150246171433367872626810509092219015283874452951868081163892328387927559567336088640513
34	147049618365879421249612296174369213111146178506210220498201965316622031402984538002285644372077836633186409902489575338782721
35	107010592458999940561955702180302050658481740392774624430340775789803872514791716886258854994198364978765941985457904860326401460918221

Notice the parabolic shape, reflecting the quadratic growth in the number of digits.

A Parallelogram Divisor Relation

There are many other divisor relations on abelian varieties that give important height relations. For example, consider the following four maps

$$\pi_1, \pi_2, \sigma, \delta : A \times A \longrightarrow A.$$

$$\begin{aligned} \pi_1(P, Q) &= P, & \sigma(P, Q) &= P + Q, \\ \pi_2(P, Q) &= Q, & \delta(P, Q) &= P - Q. \end{aligned}$$

Theorem. (Geometry) For any divisor $D \in \text{Div}(A)$,

$$\sigma^*D + \delta^*D \sim 2\pi_1^*D + 2\pi_2^*D.$$

This yields the **height parallelogram law**:

Theorem. (Arithmetic)

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

Canonical Heights on Abelian Varieties

Canonical Heights

On abelian varieties we can get rid of those pesky $O(1)$'s.

Theorem (*Néron, Tate*). Let $D \in \text{Div}(A)$ be a symmetric divisor. Then the limit

$$\hat{h}_D(P) = \lim_{n \rightarrow \infty} \frac{1}{n^2} h_D([n]P)$$

exists and has the following properties:

- $\hat{h}_D(P) = h_D(P) + O(1)$.
- $\hat{h}_D([n]P) = n^2 \hat{h}_D(P)$.
- $\hat{h}_D(P + Q) + \hat{h}_D(P - Q) = 2\hat{h}_D(P) + 2\hat{h}_D(Q)$.
- If D is ample, then $\hat{h}_D(P) = 0$ iff $P \in A(\bar{K})_{\text{tors}}$.
- More generally, \hat{h}_D for ample D induces a positive definite quadratic form on the real vector space

$$A(K) \otimes \mathbb{R} \cong \mathbb{R}^r, \quad \text{where } r = \text{rank } A(K).$$

The Height Regulator

The inner product

$$\langle P, Q \rangle_D := \hat{h}_D(P + Q) - \hat{h}_D(P) - \hat{h}_D(Q)$$

gives $A(K) \otimes \mathbb{R} \cong \mathbb{R}^r$ the structure of a Euclidean space, and $A(K)/A(K)_{\text{tors}} \cong \mathbb{Z}^r$ is a lattice in \mathbb{R}^r . The volume of a fundamental domain of this lattice is the **regulator of A/K (with respect to D)**.

Concretely, let $P_1, \dots, P_r \in A(K)$ be a basis for the quotient $A(K)/A(K)_{\text{tors}}$. Then

$$\text{Regulator}(A/K) = R_{A/K} = \det(\langle P_i, P_j \rangle)_{1 \leq i, j \leq r}.$$

Notice the analogy with the classical regulator, which measures the volume of a fundamental domain of the unit group via the logarithmic embedding

$$\mathcal{O}_K^* \longrightarrow \mathbb{R}^{r_1+r_2}, \quad \alpha \longmapsto (\log \|\alpha\|_v)_{v \in M_K}.$$

Descent and the Mordell-Weil Theorem

Mordell-Weil Theorem Let A/K be an abelian variety. Then $A(K)$ is a finitely generated abelian group.

The proof of the Mordell-Weil Theorem proceeds in two steps. The first uses reduction modulo \mathfrak{p} to limit the ramification in the field extension $K([m]^{-1}A(K))$ and deduce the

Weak Mordell-Weil Theorem There is an $m \geq 2$ such that $A(K)/mA(K)$ is a finite.

The second step is prove the implication

Weak Mordell-Weil \implies Mordell-Weil.

The descent argument uses height functions and is quite elegant when done with canonical heights.

Weak Mordell-Weil Theorem \implies Mordell-Weil Theorem

Let $P_1, \dots, P_n \in A(K)$ be representatives for the finite set $A(K)/mA(K)$.

Claim: $A(K)$ is generated by the finite set

$$G = \left\{ R \in A(K) : \hat{h}_D(R) \leq \max_i \hat{h}_D(P_i) \right\}.$$

Proof. Suppose not. Let $P \in A(K)$ be a point of smallest height not in $\text{Span}(G)$. Write $P = mQ + P_j$ for some index j . Then

$$\begin{aligned} m^2 \hat{h}_D(Q) &= \hat{h}_D(mQ) \\ &= \hat{h}_D(P - P_j) \\ &\leq 2\hat{h}_D(P) + 2\hat{h}_D(P_j) \\ &< 4\hat{h}_D(P) \quad \text{since } P_j \in G \text{ and } P \notin G. \end{aligned}$$

Since $m \geq 2$, we conclude $\hat{h}_D(Q) < \hat{h}_D(P)$. Therefore $Q \in \text{Span}(G)$, contradicting $P \notin \text{Span}(G)$. QED

A Diophantine Question About Canonical Heights

Let D be an ample symmetric divisor on an abelian variety A . As already noted,

$$\hat{h}_D(P) = 0 \iff P \in A_{\text{tors}}.$$

If $P \notin A_{\text{tors}}$, it is natural to ask about the arithmetic properties of the number $\hat{h}_D(P)$.

Analog. $\alpha \in \mathbb{Z}, \alpha \geq 2 \implies \log \alpha$ is transcendental.

Current Status. There are no examples of points with $\hat{h}_D(P) \neq 0$ for which it is known that $\hat{h}_D(P) \notin \mathbb{Q}$!

Wild Conjecture. If $P_1, \dots, P_r \in A(\bar{\mathbb{Q}})$ are independent,* then

$\hat{h}_D(P_1), \dots, \hat{h}_D(P_r)$ are algebraically indep. over $\bar{\mathbb{Q}}$.

* **Independent** means over the group ring $(\text{End}(A) \otimes \mathbb{Q})[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$.

Variation of the Canonical Height in Families - I

Let

$$\pi : A \longrightarrow T$$

be a one-parameter family of abelian varieties. Thus for each $t \in T^0 \subset T$, the fiber $A_t = \pi^{-1}(t)$ is an abelian variety.

We know that on any fiber, the difference

$$\hat{h}_{A_t, D_t}(P) - h_{A, D}(P)$$

is bounded, independent of $P \in A_t(\bar{K})$, but it is useful to know how the bound varies with t .

Theorem (*Silverman, Tate*) Fix a height on T . There are constants $c_1, c_2 > 0$ so that

$$\begin{aligned} |\hat{h}_{A_t, D_t}(P) - h_{A, D}(P)| &\leq c_1 h_T(t) + c_2 \\ &\text{for all } P \in A^0(\bar{K}) \text{ and } t = \pi(P). \end{aligned}$$

Variation of the Canonical Height in Families - II

Now consider an algebraic family of points

$$P : T \longrightarrow A.$$

These **sections** form a group $A(T)$, and there is a function field canonical height $\hat{h}_{A,D} : A(T) \rightarrow \mathbb{R}$.

Theorem (*Silverman*) For all $P \in A(T)$,

$$\lim_{\substack{t \in T(\bar{K}) \\ h(t) \rightarrow \infty}} \frac{\hat{h}_{A_t, D_t}(P_t)}{h_T(t)} = \hat{h}_{A,D}(P).$$

Corollary Assume that $A \rightarrow T$ has no constant part. Then the specialization homomorphism

$$\sigma_t : A(T) \longrightarrow A_t(\bar{K}), \quad \sigma_t(P) = P_t,$$

is injective except on a set of bounded height in $T(\bar{K})$.

Counting Rational Points on Abelian Varieties

The canonical height allows us to accurately count the rational points of bounded height on abelian varieties.

Theorem. (*Néron*) Let D be an ample symmetric divisor on A/K and let $r = \text{rank } A(K)$. Then

$$\#\{P \in A(K) : \hat{h}_D(P) \leq B\} \sim CB^{r/2}.$$

The constant C is given explicitly by

$$C = C(A/K) = \frac{\pi^{r/2}}{\Gamma(r/2 + 1)} \cdot \frac{\#A(K)_{\text{tors}}}{R_{A/K}}.$$

The theorem is stated using the logarithmic height. For comparison with later results, we rewrite it as

$$\#\{P \in A(K) : H_D(P) \leq B\} \sim C(\log B)^{r/2}.$$

Counting Rational Points on Varieties

What Do Counting Functions Look Like?

Let $X/K \subset \mathbb{P}_K^N$ be a projective variety and let $U \subset X$ be a Zariski open subset with $U(K) \neq \emptyset$. What sort of behavior might we expect for the counting function

$$N(U(K), B) = \#\{P \in U(K) : H_K(P) \leq B\}?$$

The answer depends on the particular embedding (i.e., choice of a particular height function), but all known examples grow roughly like a power of B or like a power of $\log B$.

Thus the growth rate of the quantity

$$\log \log N(U(K), B)$$

seems to be independent of the embedding and to provide a coarse measure of the distribution of rational points. This leads to the following question.

A Coarse Question About Counting Functions

Question. Let $X/K \subset \mathbb{P}_K^N$ be a projective variety and let $U \subset X$ be a Zariski open subset with $U(K) \neq \emptyset$. Is it true that $N(U(K), B)$ always satisfies one of the following conditions?*

$$\lim_{B \rightarrow \infty} \frac{\log \log N(U(K), B)}{\log \log B} = 1 \quad (\text{polynomial growth})$$

$$\lim_{B \rightarrow \infty} \frac{\log \log N(U(K), B)}{\log \log \log B} = 1 \quad (\text{logarithmic growth})$$

$$N(U(K), B) = O(1) \quad (\text{bounded growth})$$

To describe $N(U(K), B)$ more precisely, we must consider the relationship between geometry and arithmetic.

* At the conference, Bjorn Poonen noted that if \mathbb{Z} is Diophantine in \mathbb{Q} , then $\log \log N(U(K), B)$ may have many other types of growth rates, including any log iterate $\log \log \cdots \log B$.

Geometry to Arithmetic

A fundamental tenet of the modern theory of Diophantine equations is

Geometry Determines Arithmetic

One aspect of this philosophy is a growing body of conjectures and theorems describing the growth rate of the counting function $N(U(K), B)$ in terms of the underlying geometry of U and X .

The case of curves is well-understood (which is why this semester is devoted to “higher dimensions”!):

genus	type of curve (metric)	rational points
0	rational curve (parabolic)	$N(B) \approx cB^2$
1	elliptic curve (flat)	$N(B) \approx c(\log B)^{r/2}$
≥ 2	general (hyperbolic)	$N(B) \approx c$

Geometry to Arithmetic

A coarse, but extremely useful, measure of the geometric complexity of a variety is the “size” of its canonical class.

Recall that a variety is of **general type** if a multiple of its canonical divisor \mathcal{K}_X gives a birational embedding

$$X \xrightarrow{\text{birat.}} |m\mathcal{K}_X|.$$

These are analogues of “curves of genus ≥ 2 .”

At the opposite extreme are Fano varieties, whose anti-canonical divisors $-\mathcal{K}_X$ are ample. These are analogues of “curves of genus 0.”

And in the middle are varieties with $\mathcal{K}_X \sim 0$ (or more generally, $n\mathcal{K}_X \sim 0$). These are analogues of “curves of genus 1.” Examples include abelian varieties, K3 surfaces, and Calabi-Yau varieties.

Refined Counting Questions — Fano Varieties

Let X/K be a smooth projective variety whose anti-canonical divisor $-\mathcal{K}_X$ is ample. We use the height $H_{-\mathcal{K}}$ to count points.

Conjecture. (*Batyrev-Manin*) There is a Zariski open subset $U \subset X$, an integer $\rho \geq 1$, and a finite extension K'/K so that for all finite extensions L/K' ,

$$N(U(L), B) \sim cB(\log B)^{\rho-1} \quad \text{as } B \rightarrow \infty.$$

With a careful choice of counting function, Peyre has given a conjectural formula for $c = c(U, L)$ in terms of local data such as the measure of $X(L_w)$ for completions $w \in M_L$.

This conjecture of Batyrev and Manin and various refinements will be prominently featured in other talks during this workshop and during the rest of the semester.

Refined Counting Questions — Trivial Canonical Bundle

Conjecture. (*Batyrev-Manin*) Let X/K be a smooth projective variety and suppose that the canonical divisor is trivial (or even $n\mathcal{K}_X \sim 0$ for some $n \geq 1$). Then for every $\epsilon > 0$ there is a Zariski open subset $U_\epsilon \subset X$ satisfying

$$N(U_\epsilon(K), B) \ll B^\epsilon.$$

We have seen that the conjecture is true for abelian varieties in the stronger form

$$N(A(K), B) \ll (\log B)^{r/2}.$$

However, it is easy to produce examples of K3 surfaces X/\mathbb{Q} with the property that for every nonempty open subset $U \subset X$ there is a $\delta = \delta(U) > 0$ satisfying

$$N(U(\mathbb{Q}), B) \gg B^\delta.$$

Refined Counting Questions — Ample Canonical Bundle

Conjecture (*Bombieri, Lang*). If X is of general type, then $X(K)$ is not Zariski dense in X .

Notice that if X is a curve, then it is of general type if and only if $g(X) \geq 2$.

A refinement of the Bombieri-Lang conjecture due to Vojta quantifies the relation between the canonical divisor \mathcal{K}_X and the heights of rational (and integral) points on X . However, before stating Vojta's conjecture, we need to explain how to decompose height functions into a sum of local heights.

Local Heights
and
Integral Points

Local Heights

Recall that the height $h(P)$ of a point in projective space is a sum over the different completions,

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} \log \max \{ \|x_0\|_v, \dots, \|x_N\|_v \}.$$

In general, it is possible to decompose heights into a sum of local pieces.

Theorem. Let D be an effective divisor on X . Then for each $v \in M_K$ there is a function

$$\lambda_{D,v} : X(\bar{K}_v) \setminus \text{Support}(D) \longrightarrow \mathbb{R}$$

that makes sense of the intuition

$$\lambda_{D,v}(P) = -\log(v\text{-adic distance from } P \text{ to } D).$$

Local Heights

Example. Let $X = \mathbb{P}^N$ and $D = \{x_0 = 0\}$. Let v be a p -adic absolute value and write $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\mathbb{Q})$ as usual. Then

$$\lambda_{D,v}(P) = -\log |x_0|_v.$$

Local heights fit together to give the global height

$$h_D(P) = \sum_{v \in M_K} \lambda_{D,v}(P) + O(1) \quad \text{for } P \notin \text{Support}(D).$$

This often allows one to exploit geometric and/or analytic properties of local heights in order to make global arithmetic deductions. E.g., let $P_1, P_2, \dots, P_n \in X(K)$.

$$\text{Avg. Ht.} = \frac{1}{n} \sum_{i=1}^n h_D(P_i) = \sum_{v \in M_K} \left(\frac{1}{n} \sum_{i=1}^n \lambda_{D,v}(P_i) \right) + O(1).$$

Local Heights and Integrality

We can use local heights to characterize **integrality**.

Continuing with the example, we have

$$\begin{aligned} P \in \mathbb{A}^N(\mathbb{Z}) &\iff \lambda_{D,v}(P) = 0 \quad \text{for all } p\text{-adic } v \\ &\iff h_D(P) = \sum_{v \text{ arch}} \lambda_{D,v}(P) \end{aligned}$$

In general, let $S \subset M_K$ and let D be an effective ample divisor, so we can embed $X \setminus \text{Support}(D) \hookrightarrow \mathbb{A}^N$.

Then a set of S -integral points in $X \setminus \text{Support}(D)$ is characterized by the condition

$$h_D(P) = \sum_{v \in S} \lambda_{D,v}(P) + O(1).$$

Vojta's Conjecture

Vojta's Conjecture

Conjecture (*Vojta*) Let

K/\mathbb{Q} a number field,

X/K a smooth projective variety,

\mathcal{A} a **big** divisor on X (ample on an open subset),

\mathcal{K}_X a canonical divisor on X ,

D an effective normal crossings divisor on X ,

S a finite subset of M_K ,

$\epsilon > 0$ an arbitrary small constant.

Then there is a constant C and a proper Zariski closed subset $Z \subset X$ so that

$$\sum_{v \in S} \lambda_{D,v}(P) + h_{\mathcal{K}_X}(P) \leq \epsilon h_{\mathcal{A}}(P) + C$$

for all $P \in (X \setminus Z)(K)$.

Vojta's Conjecture and Sets of S -Integral Points

Suppose that $D + \mathcal{K}_X$ is big and let P be an S -integral point in $X \setminus \text{Support}(D)$. Then Vojta's conjecture with $\mathcal{A} = D + \mathcal{K}_X$ says that

$$h_{\mathcal{A}}(P) \leq \epsilon h_{\mathcal{A}}(P) + C \quad \text{for } P \notin Z.$$

But there are only finitely many points of bounded \mathcal{A} -height. Hence:

Consequence of Vojta's Conjecture.

If $D + \mathcal{K}_X$ is big, then the set of S -integral points in $X \setminus \text{Support}(D)$ is not Zariski dense.

Special Case (Bombieri-Lang Conjecture) If X is of general type, then $X(K)$ is not Zariski dense in X (since we can take $\mathcal{A} = \mathcal{K}_X$ and $D = 0$).

Vojta's Conjecture on Varieties with Trivial \mathcal{K}_X

Let X be a variety with trivial canonical bundle, or more generally satisfying $n\mathcal{K}_X \sim 0$ for some $n \geq 1$. Then Vojta's conjecture says

$$D \text{ big} \\ \implies (X \setminus \text{Support } D)(R_S) \text{ not Zariski dense.}$$

In particular, the conjecture predicts that S -integral points on affine subvarieties of K3 surfaces and Calabi-Yau varieties should not be Zariski dense.

A Concrete Example

The simplest examples of K3 surfaces are nonsingular quartic hypersurfaces in \mathbb{P}^3 .

So let $F(x, y, z) \in \mathbb{Z}[x, y, z]$ be a homogeneous polynomial of degree 4 (with appropriate nonsingularity conditions). Then Vojta's conjecture predicts that the solutions to

$$F(x, y, z) = 1 \quad \text{with } x, y, z \in \mathbb{Z}_S$$

are not Zariski dense on the surface $F(x, y, z) = w^4$.

Challenge Problem. Prove that

$$\{(x, y, z) \in \mathbb{Z}^3 : x^4 + y^4 - z^4 = 1\} \text{ is not Zariski dense.}$$

Sparsity of Rational and Integral Points

Schmidt's Subspace Theorem

There are many conjectures, but few general theorems, proving that rational or integral points are sparse on higher dimensional varieties. One of the most important is Wolfgang Schmidt's generalization of Roth's theorem.

Subspace Theorem. (Schmidt, ...) Let D_0, \dots, D_N be hyperplanes in \mathbb{P}^N in general position (defined over \bar{K}) and let $D = D_0 + \dots + D_N$. Let S be a finite set of places of K , extended in a fixed way to \bar{K} , and let $\epsilon > 0$. Then the set

$$\left\{ P \in \mathbb{P}^N(K) : \sum_{v \in S} \lambda_{D,v}(P) \geq (N + 1 + \epsilon)h(P) \right\}$$

is contained in a finite union of hyperplanes in \mathbb{P}^N .

The canonical bundle on \mathbb{P}^N is $-(N + 1)$ times a hyperplane, so this is Vojta's conjecture in this setting.

Rational and Integral Points on Abelian Varieties

Vojta developed new methods of Diophantine approximation to give a new proof of the Mordell Conjecture. Faltings generalized these ideas to prove strong results for both rational and integral points on abelian varieties.

Theorem (*Faltings*) Let X be an abelian variety, let $Y \subset X$ be a subvariety that contains no translate of an abelian subvariety of X , and let $U \subset X$ be an affine open subset of X .

- (a) $Y(K)$ is finite.
- (b) $U(R_S)$ is finite.

The abelian variety A has trivial canonical bundle and the subvariety Y is of general type, so these are (essentially) cases of Vojta's conjecture.

Vojta's Inequality and Finiteness of $Y(K) \subset A(K)$

Proof Sketch. Assume $P_1, \dots, P_m \in Y(K)$ are points of rapidly increasing height.

Construct auxiliary functions as sections to line bundles for certain **Vojta divisors** $D_V \in \text{Div}(A^m)$.

Prove the functions do not vanish to too high order at (P_1, \dots, P_m) . [Roth Lemma, Faltings Product Thm.]

Use the fact that the pullback of D_V to Y^m has certain effectivity properties to conclude that for some i, j :

$$\langle P_i, P_j \rangle \leq \frac{3}{4} \sqrt{\hat{h}(P_i) \hat{h}(P_j)} \quad \text{Vojta's Inequality}$$

Consequence: $A(K) \otimes \mathbb{R} = \mathbb{R}^r$ is covered by finitely many cones Γ_j with the property that $\Gamma_j \cap Y(K)$ contains only finitely many points.

Vojta's Conjecture and Blowups

Let X be $\mathbb{P}^1 \times \mathbb{P}^1$ blown up at $(1, 1)$, let E be the exceptional divisor, and let

$$D = ((0) \times \mathbb{P}^1) + ((\infty) \times \mathbb{P}^1) + (\mathbb{P}^1 \times (0)) + (\mathbb{P}^1 \times (\infty))$$

A canonical divisor on X is $\mathcal{K}_X = -D + E$, so Vojta's conjecture says that

$$h_E(P) \leq \epsilon h_{\mathcal{A}}(P) \quad \text{for } P \in (X \setminus D)(R_S) = (R_S^*)^2.$$

Corvaja and Zannier prove this result via an ingenious argument reducing it to Schmidt's Subspace Theorem. Here is a striking special case (proven similarly):

Theorem (*Bugeaud, Corvaja, Zannier*) Let $a, b \in \mathbb{Z}$ be multiplicatively independent. Then for all $\epsilon > 0$,

$$\gcd(a^n - 1, b^n - 1) \leq e^{\epsilon n}$$

for all $n \geq C(a, b, \epsilon)$.

Points of Small Height

Points of Small Height

Recall Kronecker's Theorem: Let $\alpha \in \bar{\mathbb{Q}}^*$. Then

$$h(\alpha) = 0 \iff \alpha \text{ is a root of unity.}$$

Roots of unity are torsion points in the multiplicative group \mathbb{G}_m . Similarly for abelian varieties:

Let D be an ample symmetric divisor on an abelian variety A and let $P \in A(\bar{\mathbb{Q}})$. Then

$$\hat{h}_D(P) = 0 \iff P \in A_{\text{tors}}.$$

These statements lead to the natural question:

Question. If the height is positive, how small can it be?

Height lower bounds have various applications, including estimating the number of solutions to Diophantine problems and making Diophantine algorithms effective.

The Lehmer Conjecture

The formulæ

$$h(\sqrt[m]{a}) = \frac{1}{m}h(a) \quad \text{and} \quad \hat{h}_D\left(\frac{1}{m}P\right) = \frac{1}{m^2}\hat{h}_D(P)$$

show that nonzero heights can be arbitrarily small.

However, $\sqrt[m]{a}$ and $\frac{1}{m}P$ are defined over fields of increasingly large degree. Let

$$d(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad \text{and} \quad d(P) = [\mathbb{Q}(A, P) : \mathbb{Q}]$$

denote the degree of the minimal field of definition.

Lehmer Conjecture. Let $\alpha \in \bar{\mathbb{Q}}^*$ be a nonroot of unity. Then

$$h(\alpha) \geq \frac{c}{d(\alpha)}.$$

(Maybe even with $c = \log(1.17628\dots) = 0.16235\dots$)

The Lehmer Conjecture for Abelian Varieties

There is a natural analog of the Lehmer conjecture for abelian varieties.

Lehmer Conjecture for Abelian Varieties. Let $A/\bar{\mathbb{Q}}$ be an abelian variety and D an ample symmetric divisor on A . Then

$$\hat{h}_D(P) \geq \frac{c_{A,D}}{d(P)} \quad \text{for all nontorsion } P \in A(\bar{\mathbb{Q}}).$$

The past few decades have seen a great deal of work on the Lehmer conjecture and its various generalizations. This will be discussed in subsequent talks.

Height Lower Bounds in a Different Direction

The Lehmer conjecture fixes a group variety and asks for a lower bound as the field of definition of P varies.

Dem'janenko and Lang ask for bounds in which the field is kept constant and the (abelian) variety varies.

Their original conjecture suggests that “complicated elliptic curves” should have “complicated points.”

Conjecture. (*Dem'janenko, Lang*) There are absolute constants $c_1, c_2 > 0$ so that for all elliptic curves E/\mathbb{Q} and all nontorsion points $P \in E(\mathbb{Q})$,

$$\hat{h}(P) \geq c_1 \log |\text{Disc}_{E/\mathbb{Q}}| - c_2.$$

The conjecture is known to be true for elliptic curves with integral j -invariant. It is also known to be a consequence of the *abc* conjecture.

A Height Lower Bound for Varying Abelian Varieties

To generalize to higher dimensional abelian varieties, we need something to replace the discriminant.

Definition Let \mathfrak{M}_g be the moduli space of abelian varieties of dim. g . Fix an embedding $j : \mathfrak{M}_g \hookrightarrow \mathbb{P}^N$. The **height of an abelian variety A/K** is

$$h(A) = h(j(A)) + \frac{1}{[K : \mathbb{Q}]} \log(N_{K/\mathbb{Q}} \text{Cond}_{A/K}).$$

Conjecture (*Dem'janenko, Lang, Silverman*)

Let K/\mathbb{Q} be a number field and $g \geq 1$. There are constants $c_1, c_2 > 0$, depending only on K and g , so that for all principally polarized abelian varieties $(A, D)/K$ of dimension g and all points $P \in A(K)$ with $\mathbb{Z}P$ Zariski dense in A ,

$$\hat{h}_D(P) \geq c_1 h(A) - c_2.$$

Points of Small Height on Subvarieties

Manin and Mumford conjectured that “complicated” curves should contain very few torsion points.

Theorem. (*Raynaud*) Let $C \hookrightarrow A$ be a curve of genus ≥ 2 embedded in an abelian variety. Then

$C \cap A_{\text{tors}}$ is finite.

The torsion points in A are characterized as being points of height 0. Bogomolov suggested that one might allow points of slightly larger height.

Theorem. (*Ullmo, Zhang*) Let $X \subset A$ be a subvariety of an abelian variety and assume that X is not a translate of an abelian subvariety of A . Let D be an ample symmetric divisor on A . Then there is a constant $\epsilon = \epsilon_{X,A,D} > 0$ so that

$\{P \in X(\bar{\mathbb{Q}}) : \hat{h}_D(P) < \epsilon\}$ is not Zariski dense.

Equidistribution of Points of Small Height

Points of small height are not merely sparse, their Galois conjugates are well spread out.

Theorem (*Szpiro-Ullmo-Zhang*) Fix an embedding $\bar{K} \subset \mathbb{C}$. Let $P_1, P_2, \dots \in A(\bar{K})$ be a “generic” sequence of points satisfying $\hat{h}(P_i) \rightarrow 0$. Let μ_i denote the uniform probability measure on the finite set

$$\{P_i^\sigma : \sigma \in \text{Gal}(\bar{K}/K)\}.$$

Then μ_i converges weakly to normalized Haar measure on $A(\mathbb{C})$.

Remark. I have restricted attention to abelian varieties, but there are important analogs for tori, for semi-abelian varieties, and more generally for preperiodic points and/or points of small height associated to morphisms $\phi : X \rightarrow X$.

Height Zeta Functions

Height Zeta Functions

Let X/K be a smooth projective variety and D an ample divisor on X . Fix a height $H_D \geq 1$. Following Batyrev and Manin, we define the **Height Zeta Function** of an open subset $U \subset X$ to be

$$Z(U(K), D; s) = Z_D(s) = \sum_{P \in U(K)} \frac{1}{H_D(P)^s}.$$

The **abscissa of convergence** of $Z_D(s)$ is denoted

$$\beta_D = \inf \{ b \in \mathbb{R} : Z_D(s) \text{ converges for } \operatorname{Re}(s) > b \}.$$

Clearly there is a relation between β_D and the growth rate of the **counting function**

$$N(U(K), D; B) = \#\{ P \in U(K) : H_D(P) \leq B \}.$$

Height Zeta Functions

In many situations, one expects (i.e., hopes!) that for a careful choice of H_D there will be a relation

$$N(U(K), D; B) \sim cB^{\beta_D} (\log B)^{t-1} \quad \text{as } B \rightarrow \infty$$

$$\iff Z_D(s) \sim \frac{c\Gamma(t)\beta_D}{(s - \beta_D)^t} \quad \text{as } s \rightarrow \beta_D^+.$$

In any case, it would be extremely interesting to find a geometric interpretation for the arithmetic invariant

$$\beta_D = \beta_D(U/K).$$

The **Nevanlinna invariant** α_D is defined by

$$\alpha_D = \inf \left\{ \frac{p}{q} \in \mathbb{Q}_{\geq 0} : pD + q\mathcal{K}_X \text{ is big} \right\}$$

The Batyrev-Manin Conjecture

Conjecture (*Batyrev, Manin*). Let X/K be a smooth variety and D an ample divisor on X .

- (a) For every $\epsilon > 0$ there is a Zariski open subset $U_\epsilon \subset X$ such that

$$\beta_D(U_\epsilon(K)) \leq \alpha_D + \epsilon.$$

- (b) Assume that no multiple of \mathcal{K}_X is effective. Then for all sufficiently large number fields L/K and all sufficiently small Zariski open subsets $U \subset X$,

$$\beta_D(U(L)) = \alpha_D.$$

Example. If $\mathcal{K}_X = 0$, then $\alpha_D = 0$, so the conjecture implies

$$N(U(K), D; B) \ll B^\epsilon \quad \text{for all } \epsilon > 0.$$

Example. If $-\mathcal{K}_X$ is big, then $\alpha_{-\mathcal{K}_X} = 1$, so the conjecture says

$$N(U(L), -\mathcal{K}_X; B) \approx B$$

Dynamics and Canonical Heights

Dynamical Canonical Heights on \mathbb{P}^N

Let $\phi : \mathbb{P}^N \rightarrow \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over a number field K . A standard property of height functions says that

$$h(\phi(P)) = dh(P) + O(1) \quad \text{for all } P \in \mathbb{P}^N(\bar{K}).$$

The Néron-Tate construction gives a **canonical height function**

$$\hat{h}_\phi(P) = \lim_{n \rightarrow \infty} \frac{1}{d^n} h(\phi^n(P))$$

satisfying

$$\begin{aligned} \hat{h}_\phi(\phi(P)) &= d\hat{h}_\phi(P) \\ &\text{and} \\ \hat{h}_\phi(P) &= h(P) + O(1). \end{aligned}$$

An Application to Rational Preperiodic Points

Definition. A point $P \in \mathbb{P}^N(\bar{K})$ is called **preperiodic for ϕ** if its forward orbit

$$\{P, \phi(P), \phi^2(P), \dots\} \text{ is finite.}$$

Theorem. $\hat{h}_\phi(P) = 0$ if and only if P is **preperiodic** for ϕ .

Proof. One way is trivial. For the other, suppose $\hat{h}_\phi(P) = 0$. Then $\hat{h}_\phi(\phi^n(P)) = d^n \hat{h}_\phi(P) = 0$. Hence

$$\{\phi^n(P) : n = 0, 1, 2, \dots\}$$

is a set of bounded height, so it is finite. QED.

Corollary. (*Northcott*)

Let $\phi : \mathbb{P}^N \rightarrow \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over a number field K . Then $\mathbb{P}^N(K)$ contains only finitely many preperiodic points of ϕ .

Additional Topics

Additional Topics and Acknowledgements

Important topics that have not been covered due to time constraints:

- Heights Over Function Fields
- Metrized Line Bundles
 - Height of a Subvariety
 - Modular Height of an Abelian Variety
 - Arakelov Intersection Theory
- p -adic Heights
- Mahler Measure and Special Values of L -Series

Acknowledgements. I would like to thank Matt Baker, Bjorn Poonen and Paul Vojta for their helpful comments on the material in this presentation.

An Introduction to Height Functions

- What Are Height Functions
- 1. Heights on Projective Space
 - The Height of \mathbb{Q} -Rational Points
 - The Height of Points over Number Fields
 - A Finiteness Property of the Height on \mathbb{P}^N
 - Two Ways in Which Height Functions Are Used
 - Counting Algebraic Points in \mathbb{P}^N
 - A Transformation Property of the Height on \mathbb{P}^N
- 2. Heights on Projective Varieties
 - Heights on Projective Varieties
 - The Weil Height Machine
- 3. Heights on Abelian Varieties
 - Abelian Varieties
 - A Divisor Relation on Abelian Varieties
 - The Quadratic Growth of the Height on Abelian Varieties
 - A Parallelogram Divisor Relation
- 4. Canonical Heights on Abelian Varieties
 - Canonical Heights
 - Variation of the Canonical Height in Families
 - The Height Regulator
 - Descent and the Mordell-Weil Theorem
 - Weak Mordell-Weil Theorem \implies Mordell-Weil Theorem
 - A Diophantine Question About Canonical Heights
 - Counting Rational Points on Abelian Varieties
- 5. Counting Rational Points on Varieties
 - What Do Counting Functions Look Like?
 - A Coarse Question About Counting Functions
 - Geometry to Arithmetic
 - Refined Counting Questions — Fano Varieties
 - Refined Counting Questions — Trivial Canonical Bundle
 - Refined Counting Questions — Ample Canonical Bundle

An Introduction to Height Functions

5. Local Heights and Integral Points
 - Local Heights
 - Local Heights and Integrality
6. Vojta's Conjecture
 - Vojta's Conjecture
 - Vojta's Conjecture and Sets of S -Integral Points
 - Vojta's Conjecture on Varieties with Trivial \mathcal{K}_X
 - A Concrete Example
7. Theorems on Sparsity of Rational and Integral Points
 - Schmidt's Subspace Theorem
 - Rational and Integral Points on Abelian Varieties
 - Vojta's Inequality and Finiteness of $Y(K) \subset A(K)$
 - Vojta's Conjecture and Blowups
8. Points of Small Height
 - Points of Small Height
 - The Lehmer Conjecture
 - The Lehmer Conjecture for Abelian Varieties
 - Height Lower Bounds in a Different Direction
 - A Height Lower Bound for Varying Abelian Varieties
 - Points of Small Height on Subvarieties
 - Equidistribution of Points of Small Height
9. Height Zeta Functions
 - Height Zeta Functions
 - The Batyrev-Manin Conjecture
10. Dynamics and Canonical Heights
 - Dynamical Canonical Heights on \mathbb{P}^N
 - An Application to Rational Preperiodic Points
11. Additional Topics

Metriized Line Bundles; Height of a Subvariety; The Modular Height of an Abelian Variety; p -adic Heights; Mahler Measure;