Math 6170 C, Lecture on April 29, 2020

Yongchang Zhu

Plan

(1) VIII. §5. Heights on Projective Spaces (Review).

(2) VIII. §6. Heights on Elliptic Curves (Continued).

(3) VIII. §9. The Canonical Height.

Let K be a number field,

M_K be the set of standard absolute values on K.

For each $v \in M_K$, let n_v be the local degree at v, i.e.,

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

where $w \in M_{\mathbb{Q}}$ is the restriction of v on $\mathbb{Q}$.

Definition.

Let $P \in \mathbb{P}^N(K)$ with homogeneous coordinates

$$P = [x_0, x_1, \ldots, x_N].$$

The **height** of P is defined by

$$H_K(P) = \Pi_{v \in M_K} \max(|x_0|_v, \ldots, |x_N|_v)^{n_v}$$

The infinite product on the right makes sense because almost all the terms are 1.

Proposition VIII 5.4.

Let $P \in \mathbb{P}^N(K)$.

(a) The height $H_K(P)$ does not depend on the choice of the homogeneous coordinates for P.

(b) Let L/K be a finite extension. Then

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

Definition.

Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. The **absolute height** of P, denoted by $H(P)$, is defined as follows. Choose any number field K such that $P \in \mathbb{P}^N(K)$. Then

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

The **absolute logarithmic height** on projective space is the function

$$h : \mathbb{P}^N(\bar{Q}) \to \mathbb{R}$$

given by

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

Theorem VIII 5.6.

Let $F : \mathbb{P}^N \to \mathbb{P}^M$ be a morphism of degree d. Then there are constants C_1 and C_2, such that for all $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$,

$$C_1 \, H(P)^d \leq H(F(P)) \leq C_2 \, H(P)^d.$$

For $a \in \bar{\mathbb{Q}}$, we define

$$H(a) = H([a, 1])$$

$$h(a) = h([a, 1]) = \log\ H(a)$$

Theorem VIII 5.9.

Let

$$f(T) = a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0 = a_d(T - \alpha_1) \cdots (T - \alpha_d) \in \bar{\mathbb{Q}}[T]$$

Then

$$2^{-d} \Pi_{j=1}^{d} H(\alpha_j) \leq H([a_0, \ldots, a_d]) \leq 2^{d-1} \Pi_{j=1}^{d} H(\alpha_j)$$

Theorem VIII 5.11.

Let C and d be constants. Then the set

$$\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) \mid H(P) \leq C,\ [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

is finite.

VIII. §6. Heights on Elliptic Curves (continued).

Let E/K be an elliptic curve over K (K is a number field). For every $f \in \bar{K}(E)$, $f \notin \bar{K}$, f defines a surjective morphism $f : E \to \mathbb{P}^1$.

Definition. Let $f \in \bar{K}(E)$ be a non-constant function. The **height** on E relative to f is the function

$$h_f : \; E(\bar{K}) \to \mathbb{R}$$

$$h_f(P) = h(f(P)).$$

where h is the absolute logarithmic height.

Proposition VIII 6.1.

Let E/K be an elliptic curve and $f \in K(E)$ is a non-constant function. The for every C,

$$\{P \in E(K) \mid h_f(P) \leq C\}$$

is a finite set.

Definition.

Let S be a set, f, g are $\mathbb{R}$-valued functions on S, we write

$$f = g + O(1)$$

if there exists constant C_1, C_2 such that

$$C_1 \leq f(P) - g(P) \leq C_2$$

for all $P \in S$.

The relation

$$f = g + O(1)$$

is an equivalence relation on the space of $\mathbb{R}$-valued functions on S. That is

$f = g + O(1)$ implies $g = f + O(1)$

$f = g + O(1)$ and $g = h + O(1)$ imply

$$f = h + O(1).$$

Theorem VIII 6.2.

Let E/K be an elliptic curve over K and $f \in K(E)$ be an non-constant even function (i.e., $f \circ [-1] = f$). Then for all $P, Q \in E(\bar{K})$,

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$$

That is, as functions on $E(\bar{K}) \times E(\bar{K})$,
$h_f(P+Q) + h_f(P-Q)$ and $2h_f(P) + 2h_f(Q)$ are equivalent.

Sketch of Proof.

Let

$$K(E) = \mathrm{Frac}\, K[x, y] / \left(y^2 - (x^3 + Ax + B)\right)$$

We will prove the case $f = x$ first.

If $P = (x_1, y_1), Q = (x_2, y_2) \in E$, then

$$x_3 = x(P+Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$x_4 = x(P-Q) = \left(\frac{-y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

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

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

The following diagram is commutative

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

where $G : (P, Q) \mapsto (P + Q, P - Q)$
(to be continued)

Two vertical arrow $E \times E \to \mathbb{P}^1 \times \mathbb{P}^1$ is

$$(P, Q) \mapsto (x(P), x(Q)).$$

Two vertical arrow $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ is

$$([\alpha_1, \beta_1], [\alpha_2, \beta_2]) \mapsto [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2].$$

$g : \mathbb{P}^2 \to \mathbb{P}^2$ is

$$[t, u, v] \mapsto [u^2 - 4tv, 2u(At + v), (v - At)^2 - 4Btu]$$

The above diagram is commutative,
that is, $g(\sigma(P,Q)) = \sigma(P+Q, P-Q)$.

Idea:

$$h(\sigma(P,Q)) \sim h_x(P) + h_x(Q)$$

$$h(\sigma(P+Q, P-Q)) \sim h_x(P+Q) + h_x(P-Q)$$

Because $g(\sigma(P,Q)) = \sigma(P+Q, P-Q)$, because $\deg g = 2$, so by Theorem 5.6,

$$h(\sigma(P+Q, P-Q)) \sim 2\, h(\sigma(P,Q))$$

Because $\sim$ is an equivalence relation, we have

$$h_x(P+Q) + h_x(P-Q) \sim 2(h_x(P) + h_x(Q))$$

$\sim$ above means the equivalence relation $f = g + O(1)$ defined earlier. We prove here

$$h(\sigma(P, Q)) \sim h_x(P) + h_x(Q)$$

$$\sigma(P, Q) = [1, x(P) + x(Q), x(P)x(Q)]$$

Apply Theorem 5.9, we have

$$h(\sigma(P, Q)) \sim h_x(P) + h_x(Q).$$

For arbitrary non-constant even function $f \in K(E)$, we use the following lemma to prove Theorem 6.2 for height function h_f.

Lemma VIII 6.3. Let $f, g \in K(E)$ be non-constant even functions. Then

$$\deg(g)\, h_f = \deg(f)\, h_g + O(1)$$

Corollary VIII 6.4.

Let E/K be an elliptic curve and $f \in K(E)$ a non-constant even function.

(a). Let $Q \in E(\bar{K})$, then

$$h_f(P+Q) \leq 2h_f(P) + O(1)$$

where $O(1)$ depends on Q.

(b). Let $m \in \mathbb{Z}$. Then for all $P \in E(\bar{K})$,

$$h_f([m]P) = m^2 h_f(P) + O(1)$$

where $O(1)$ depends on m.

Proof of (a). By Theorem 6.2.,

$$h_f(P+Q) + h_f(P-Q) \leq 2h_f(P) + 2h_f(Q) + C$$

Note that

$$H(P) \geq 1 \quad \text{for } P \in \mathbb{P}^N(\bar{\mathbb{Q}})$$

so $h(P) = \log H(P) \geq 0$

$$h_f(P+Q) \leq h_f(P+Q) + h_f(P-Q) \leq 2h_f(P) + 2h_f(Q) + C$$

Proof of (b). Since f is even, $h_f(P) = h_f(-P)$, it is enough to consider $m \geq 1$. We use the induction on m. Case $m = 1$ is obvious.

$m = 2$, use $h_f([2]P) + h_f(O) = 2(h_f(P) + h_f(P)) + O(1)$. We see (b) is true.

Assume (b) for $1, 2 \ldots, m$, for $m + 1$, we use

$$h_f([m+1]P) + h_f([m-1]P) = 2(h_f([m]P) + h_f(P)) + O(1)$$

Theorem VIII 6.7 (Mordell-Weil theorem)

Let K be a number field and E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.

Proof. $h_f : E(K) \to \mathbb{R}$ satisfies the conditions in Proposition 3.1 (Decent Theorem) and we know $E(K)/mE(K)$ is finite (Theorem 1.1. Weak Mordell-Weil Theorem). By Prop. 3.1. $E(K)$ is finitely generated.

One of the results in VIII §7 can roughly described as the heights of torsion points in $E(K)$ are small.

VIII §9. The Canonical Height.

Theorem 6.2 states that for arbitrary non-constant even function $f \in K(E)$, the height function $h_f : E(\bar{K}) \to \mathbb{R}$ is a quadratic form up to $O(1)$:

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

One can modify h_f to a "canonical height" which is an actual quadratic form.

Proposition VIII 9.1 (Tate).

Let E/K be an elliptic curve, $f \in K(E)$ be a non-constant even function, and $P \in E(\bar{K})$. Then the limit

$$\frac{1}{\deg(f)} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

exists, and is independent of f.

Proof. We prove the sequence $4^{-N}h_f([2^N]P)$ is Cauchy. By Corollary 6.4 (b) for $m = 2$, there is a constant C so that for all $Q \in E(\bar{K})$,

$$|h_f([2]Q) - 4h_f(Q)| \leq C$$

For $N \geq M \geq 0$,

$$\begin{aligned}
&|4^{-N}h_f([2^N]P) - 4^{-M}h_f([2^M]P)| \\
&= |\sum_{n=M}^{N-1}(4^{-n-1}h_f([2^{n+1}]P) - 4^{-n}h_f([2^n]P)| \\
&\leq \sum_{n=M}^{N-1} 4^{-n-1}|h_f([2^{n+1}]P) - 4h_f([2^n]P)| \\
&\leq \sum_{n=M}^{N-1} 4^{-n-1}C \leq \frac{C}{4^{M+1}}
\end{aligned}$$

Proof (continued). This shows $4^{-N}h_f([2^N]P)$ is Cauchy, so the limit exists.

For another non-constant even function $g \in K(E)$. Then we have

$$\deg(g)h_f = deg(f)h_g + O(1),$$

So

$$\deg(g)4^{-N}h_f([2^N]P) - \deg(f)4^{-N}h_g([2^N]P) = 4^{-N}O(1) \to 0.$$

One can prove that, for any positive integer $m > 1$,

$$\frac{1}{\deg(f)} \lim_{N \to \infty} m^{-2N} h_f([m^N]P)$$

exists and is independent of f by the same method.

And the above limit is equal to the limit in the theorem.

Definition.

The **canonical height** on E/K, denoted by $\hat{h}$, is the function

$$\hat{h} : E(\bar{K}) \to \mathbb{R}$$

defined by

$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f([2^N]P).$$

Theorem VIII 9.3.

Let E/K be an elliptic curve and $\hat{h}$ the canonical height on E.

(a) For all $P, Q \in E(\bar{K})$

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

(b) For all $P \in E(\bar{K})$ and $m \in \mathbb{Z}$,

$$\hat{h}([m]P) = m^2 \hat{h}(P)$$

(c) $\hat{h}$ is a quadratic form on $E(\bar{K})$, i.e., the pairing

$$(\ ) : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$$

$$(P, Q) = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

is bilinear.

Theorem VIII 9.3 (continued).

(d) Let $P \in E(\bar{K})$. Then $\hat{h}(P) \geq 0$, and $\hat{h}(P) = 0$ iff P is a torsion point.

(e) Let $f \in K(E)$ be an even function, non-constant. Then

$$\deg(f)\hat{h} = h_f + O(1)$$

where $O(1)$ depends on E and f.

Proof of (e). In the proof of Proposition VIII 9.1, we proved that there is C such that

$$|4^{-N}h_f([2^N]P) - 4^{-M}h_f([2^M]P)| \leq \frac{C}{4^{M+1}}$$

for all P and $0 \leq M \leq N$. Take $M = 0$, we have

$$|4^{-N}h_f([2^N]P) - h_f(P)| \leq C/4$$

Take $lim_{N\to\infty}$ we get

$$|\deg(f)\hat{h}(P) - h_f(P)| \leq C/4$$

This proves (e)

Proof of (a).

For all P, Q, we have

$$2h_f(P) + 2h_f(Q) + C_1 \leq h_f(P+Q) + h_f(P-Q) \leq 2h_f(P) + 2h_f(Q) + C_2$$

$$\begin{aligned} & 2 \cdot 4^{-N} h_f([2^N]P) + 2 \cdot 4^{-N} h_f([2^N]Q) + 4^{-N} C_1 \\ \leq\ & 4^{-N} h_f([2^N](P+Q)) + 4^{-N} h_f([2^N](P-Q)) \\ & 2 \cdot 4^{-N} h_f([2^N]P) + 2 \cdot 4^{-N} h_f([2^N]Q) + 4^{-N} C_2 \end{aligned}$$

Take $\lim_{N\to\infty}$, we obtain the desired result.

Proof of (d). Since $h_f(P) \geq 0$, so $\hat{h}(P) \geq 0$. It is easy to see that P is torsion point implies that $\hat{h}(P) = 0$.
Conversely, if $\hat{h}(P) = 0$, then for any integer m,

$$\hat{h}([m]P) = m^2 \hat{h}(P) = 0$$

Hence from (e), there is a constant C such that for every $m \in \mathbb{Z}$,

$$h_f([m]P) = |\deg(f)\hat{h}([m]P) - h_f([m]P)| \leq C$$

Suppose $P \in E(K')$.
So the set $\{P, [2]P, [3]P, \dots\}$ is contained in

$$\{Q \in E(K') \mid h_f(Q) \leq C\}$$

which is a finite set by Theorem 6.1. So P must have finite order.
This proves (d).

In the remaining lectures, we will discuss modular forms and Eichler-Shimura Theory.

We will follow
Chapters 8, 9, 10, 11, 12 in Knapp's book "Elliptic Curves".

End