The Néron-Tate Canonical Height

Def The (Néron-Tate) canonical height on $E(\mathbb{Q})$ is

$$\hat{h} : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

defined by

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

where f is any non-constant even function on E (e.g., the x-coordinate).

Note: We proved the limit exists and it is independent of the choice of f.

Thm. $E/\mathbb{Q}$, with can. height $\hat{h}$.

(e) $f \in \mathbb{Q}(E)$ even, then $(\deg f) \cdot \hat{h} = h_f + O(1)$ constant depends only on E, f.

(a) $\forall P, Q \in E(\mathbb{Q})$

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

(b) $\forall P \in E(\mathbb{Q})$, $m \in \mathbb{Z}$, $\hat{h}([m]P) = m^2 \hat{h}(P)$.

(c) $\hat{h}$ is a quad. form on E, i.e., $\hat{h}$ is even and

$$\langle , \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

$$(P, Q) \longmapsto \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$ is bilinear.

(d) $P \in E(\mathbb{Q})$, $\hat{h}(P) \geq 0$ and $\hat{h}(P) = 0 \iff P$ is torsion. (!! useful !!)

If $\hat{h}'$ satisfies (e) and (b) for any $m \geq 2$, then $\hat{h}' = \hat{h}$.

Pf $E/\mathbb{Q}$, $\hat{h}$.

(e) f even, then $(\deg f)\hat{h} = h_f + O(1)$

We proved: $\left| \frac{h_f([2^N]P)}{4^N} - \frac{h_f([2^M]P)}{4^M} \right| \leq \frac{C}{3 \cdot 4^M}$ for all $N \geq M \geq 0$.

Let $M=0$, $N \to \infty$ $\Rightarrow$ $\left| (\deg f)\hat{h}(P) - h_f(P) \right| \leq \frac{C}{3 \cdot 4}$ ▨

(a) P-law. We showed:

$$\left(h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1). \right) \times \frac{\deg f}{4^N}$$

$$\deg f \, \frac{h_f([2^N](P+Q))}{4^N} + \cdots = \cdots + 2\deg f \, \frac{h_f([2^N]Q)}{4^N} + \frac{O(1)}{4^N} \to 0$$

$N \to \infty$ $\quad \hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q).$ ▨

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

$$\left(h_f([m]P) = m^2 h_f(P) + O(1) \right) \times \frac{\deg f}{4^N} \quad N \to \infty$$

∎

(c)
- $\hat{h}$ is even: put $P = O$ in the par.-law

$$\hat{h}(Q) + \hat{h}(-Q) = 2\underbrace{\hat{h}(O)}_{=0} + 2\hat{h}(Q) \Rightarrow \hat{h}(Q) = \hat{h}(-Q).$$

- $\langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is $\boxed{\text{bilinear}}$

Suffices to show $\langle P+R, Q \rangle \overset{?}{=} \langle P, Q \rangle + \langle R, Q \rangle$

or $\hat{h}(P+R+Q) - \hat{h}(P+R) - \hat{h}(P+Q) - \hat{h}(R+Q) + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R) \overset{?}{=} 0$

Use the p-law:
$$\left.\begin{array}{l} +\ (P+R, Q) \\ -\ (P, R-Q) \\ +\ (P+Q, R) \\ -\ 2 \cdot (R, Q) \end{array}\right\}$$

∎

(d) $h_f(P) = \log |H(f(P))| \geq 0 \Longrightarrow \hat{h}(P) \geq 0.$

$\underline{P \text{ is torsion} \Longrightarrow \hat{h}(P) = 0}$ $\quad \exists m \geq 1$ $[m]P = O \Longrightarrow \hat{h}(P) = \dfrac{\hat{h}([m]P)}{m^2} = \dfrac{\hat{h}(O)}{m^2} = 0.$ $\blacksquare$

$\underline{\hat{h}(P) = 0 \Longrightarrow P \text{ is torsion}}$ $\quad \hat{h}([m]P) = m^2 \hat{h}(P) = 0$ for all $m \geq 1$.

From (c) $\exists C \ \forall m \in \mathbb{Z}$

$$h_f([m]P) = \Big| (\deg f) \underbrace{\hat{h}([m]P)}_{=0} - h_f([m]P) \Big| \leq C.$$

$\Rightarrow \{P, [2]P, [3]P, \dots\} \subseteq \{Q \in E(\mathbb{Q}) : h_f(Q) \leq C\}$ is a finite set!

$\Rightarrow [n]P = [m]P \Rightarrow [n-m]P = O \Longrightarrow P$ is torsion! $\blacksquare$

(Uniqueness of $\hat{h}$ ...)

Lemma $V/\mathbb{R}$ fin. dimensional vector space, $L \subseteq V$ is a lattice.

Suppose $q: V \to \mathbb{R}$ is a quad. form s.t.

(i) Let $P \in L$, $q(P) = 0 \iff P = 0$.

(ii) $\forall C \geq 0$ $\{P \in L : q(P) \leq C\}$ is finite

Then q is positive definite on V.

Prop The canonical height is a positive definite quad form on $E(\mathbb{Q}) \otimes \mathbb{R}$

Pf Apply lemma to lattice $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ inside $E(\mathbb{Q}) \otimes \mathbb{R}$. ∎

Def Néron-Tate pairing on $E(\mathbb{Q})$ is $\langle \, , \, \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$

$$\langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q). \quad (\langle P, P \rangle = 2\hat{h}(P))$$

WARNING: Some authors: $\langle P, Q \rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right)$ so $\langle P, P \rangle = \hat{h}(P)$

Def The elliptic regulator of $E(\mathbb{Q})$ is the volume of the lattice $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ computed using the quad. form $\hat{h}$.

Chose $P_1, \dots, P_r \in E(\mathbb{Q})$ that generate $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$

$$\mathrm{Reg}_{E/\mathbb{Q}} := \det\left(\langle P_i, P_j \rangle\right)_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}$$

If $r = 0$, $\mathrm{Reg}_{E/\mathbb{Q}} := 1$.

Also, $Q_1, \dots, Q_n \in E(\mathbb{Q})$, $\mathrm{Reg}(\{Q_1, \dots, Q_n\}) = \det\left(\langle Q_i, Q_j \rangle\right)_{1 \leq i,j \leq n}$.

Note $\mathrm{Reg}_{E/\mathbb{Q}} > 0$ (it's a volume of a non-trivial parallelopiped)

$\mathrm{Reg}(\{Q_i\}) = 0 \iff \{Q_i\}$ satisfy some $\mathbb{Z}$-linear dependence!

example $E: y^2 = x^3 - 82x$ (rank 3)

$P = (-9, 3)$, $Q = (-8, 12)$, $R = (-1, 9)$

$T = (98, -966)$

ex $\mathrm{Reg}(P,Q,T) = \det \begin{pmatrix} \overset{=\langle P,P\rangle}{2.546\ldots} & \overset{=\langle P,Q\rangle}{-0.2199\ldots} & \overset{=\langle P,T\rangle}{2.3282\ldots} \\ -0.2199\ldots & \overset{=\langle Q,Q\rangle}{2.1709\ldots} & 1.9509\ldots \\ 2.3282\ldots & 1.950\ldots & 4.27\ldots \end{pmatrix} = 2.768 \cdot 10^{-28}$

$\Rightarrow \mathrm{Ker} \approx \left\langle \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \right\rangle$

$\Rightarrow$??

$$\begin{aligned} \langle P,P\rangle + \langle P,Q\rangle &= \langle P,T\rangle \\ \langle P, P+Q\rangle &= \langle P,T\rangle \\ + \quad \langle Q, P+Q\rangle &= \langle Q,T\rangle \\ - \quad \langle T, P+Q\rangle &= \langle T,T\rangle \\ \hline \langle P+Q-T, P+Q\rangle &= \langle P+Q-T, T\rangle \end{aligned}$$

$\Rightarrow \langle P+Q-T, P+Q-T\rangle = 0$

$\Rightarrow \hat{h}(P+Q-T) = 0 \Rightarrow P+Q-T =$ TORSION PT!

$\langle P,P\rangle = \hat{h}(2P) - \hat{h}(P) - \hat{h}(P)$
$= 2\hat{h}(P)$

$\langle P,P\rangle = 0 \Leftrightarrow \hat{h}(P) = 0$

VERIFY:

$\boxed{P+Q = T}$ ✓

$\mathrm{Reg}(P,Q,R) = 10.20\ldots \neq 0$

$\Rightarrow \{P,Q,R\}$ ind

Computing The Mordell-Weil Group

$E/\mathbb{Q}$, M-W Thm $\Longrightarrow$ $E(\mathbb{Q}) \cong \underbrace{E(\mathbb{Q})_{tors}}_{\text{Nagell-Lutz thm.}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$. ??

- Find generators of $E(\mathbb{Q})/mE(\mathbb{Q})$.

m=2) $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{0,1 \text{ or } 2} \oplus (\mathbb{Z}/2\mathbb{Z})^{R_{E/\mathbb{Q}}}$.

An example: E/K , $m \geq 2$, assume $E[m] \subseteq E(K)$. Then,

$G_{\bar{K}/K}$ action on $E[m]$ is trivial!

$$K : E(K) \times Gal(\bar{K}/K) \longrightarrow E[m]$$

$$K(P,\sigma) = Q^\sigma - Q \quad \text{where } Q \text{ s.t. } [m]Q = P.$$

- kernel on left is $mE(K)$ $\Rightarrow$ $\delta_E : E(K)/mE(K) \longrightarrow \mathrm{Hom}(G_{\bar{K}/K}, E[m])$

$$(\delta_E(P))(\sigma) = K(P,\sigma)$$

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

$$\delta_E : E(k)/_{mE(k)} \longrightarrow \mathrm{Hom}(G_{\bar{k}/k}, E[m])$$

$$\big(\delta_E(P)\big)(\sigma) = \kappa(P,\sigma).$$

Recall Def'n of Weil pairing:

$T \in E[m]$, pick $f \in \bar{k}(E)$ w/ $\mathrm{div}(f) = m\cdot(T) - m\cdot(O)$.

$g \in \bar{k}(E)$ w/ $\mathrm{div}(g) = \sum_{R \in E[m]} (T'+R) - (R)$ where $[m]T' = T$.

s.t. $f \circ [m] = g^m$.

$$\to \quad e_m(S,T) = \frac{g(X+S)}{g(X)} \quad \text{any } X \in E.$$

Weil pairing: $e_m : E[m] \times E[m] \longrightarrow \mu_m$

(a) Bilinear, (b) Alternating, (c) Non-deg, (d) Gal-inv, (e) compatible

variable.

Consider: $e_m(\delta_E(P)(\cdot), T) \in \mathrm{Hom}(G_{\bar{k}/k}, \mu_m)$

Hilbert's Thm 90 : $H^1(Gal(\bar{K}/K), \bar{K}^\times) = 0$

$$\Longrightarrow H^1(Gal(\bar{K}/K), \mu_m) \cong K^\times/(K^\times)^m$$

$$\|$$

If $E[m] \subseteq E(K)$ then $\mu_m \subseteq K$ $\Longrightarrow$ $Hom(Gal(\bar{K}/K), \mu_m) \cong K^\times/(K^\times)^m$.

$\Longrightarrow$ every hom $G_{\bar{K}} \to \mu_m$ is of the form

$$\sigma \longmapsto \frac{\sigma(\beta)}{\beta} \text{ where } \beta \in \bar{K}^\times \text{ with } \beta^m \in K^\times.$$

In other words, iso : $\delta_K : K^\times/(K^\times)^m \xrightarrow{\cong} Hom(G_{\bar{K}/K}, \mu_m)$

$$b \longmapsto \delta_K(b)(\sigma) = \frac{\sigma(\beta)}{\beta}$$

where $\beta^m = b$.

It follows:

$$\boxed{\begin{array}{l} e_m(\delta_E(P)(\sigma), T) = \delta_K(b(P,T))(\sigma) \\ \quad \text{for some } b(P,T) \in K^\times/(K^\times)^m \end{array}}$$

$$e_m(\delta_E(P)(\cdot), T) = \delta_K(b(P,T))(\cdot)$$

$$\in \mathrm{Hom}(G_{\bar{K}/K}, \mu_m)$$