6

2020年7月6日 15:36

弱MW $\Rightarrow$ MW (Fermat猜想)

H $\quad H: \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}$.

Th $d \geq 1$, $B > 0$ $d \in \mathbb{N}$, $B \in \mathbb{R}$. 则

① (Northcott) $S(n,d,B) = \{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid [\mathbb{Q}(P):\mathbb{Q}] \leq d$ 且 $H(P) \leq B\}$ 是有限的. 其中 $\mathbb{Q}(P)$ 是 P 的刚生域 即包含 P 的某组齐次坐标的最小的域.

② (Kronecker) $H(P) > 1$, 除非 P 的某个齐次坐标全由单位根或 0 构成.

Pf. ① 令 $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ 坐标不全为 0. 不妨设 $x_0 \neq 0$.

则 $P = (1 : \alpha_1 : \cdots : \alpha_n)$ $\alpha_i \in \overline{\mathbb{Q}}$ 且由 $H(\alpha_i) \leq H(P)$

$[\mathbb{Q}(\alpha_i):\mathbb{Q}] \leq [\mathbb{Q}(P):\mathbb{Q}]$ 于是只需证明 $\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha):\mathbb{Q}] \leq d$ 且 $H(\alpha) \leq B\}$ 是有限的.

α 在 $\mathbb{Z}[x]$ 中的极小多项式系数个数 $\leq d+1$

α 的共轭元也有界, 韦达定理 $\Rightarrow$ 系数有界, 这种极小多项式只有有限个.

从而 $\hookrightarrow$ 是有限集.

② $P = (1 : \alpha_1 : \cdots : \alpha_n) \in \mathbb{P}^n(K)$

则 $H_K(P) = \prod_{v \in \Omega_K} \max(1, |\alpha_1|_v, \cdots, |\alpha_n|_v) \geq 1$

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

若 $H(P) = 1$, 则 $\forall i \forall v$ 有 $|\alpha_i|_v \leq 1$ 于是 $\forall m \in \mathbb{N}$ $|\alpha_i^m|_v \leq 1$

由①. $\{(1 : \alpha_1^m : \cdots : \alpha_n^m) \mid m \in \mathbb{N}\}$ 是有限的.

只可能 α_i 为 0 或单位根 #

问题: 希望定义 $E(\overline{\mathbb{Q}})$ 上的高度, 已有 $\mathbb{P}^n(\overline{\mathbb{Q}})$ 上的高度 $\mathbb{P}^2(\overline{\mathbb{Q}})$

$\mathbb{P}^1 \cong \mathbb{P}^n$

问题：希望定义 $E(\mathbb{Q})$ 上的高度，已有 $\mathbb{P}^1(\mathbb{Q})$ 上的高度 $\mathbb{P}^2(\overline{\mathbb{Q}})$

$E(\mathbb{Q}) \subset \mathbb{P}^2(\overline{\mathbb{Q}}) \xrightarrow{H} \mathbb{R}$

$E \to \mathbb{P}^n \xrightarrow{\text{嵌入}} \mathbb{P}^n$

Prop 令 $P_0, \cdots, P_m$ 是 d 次齐次多项式 $\in k[x_0, \cdots, x_n]$

Z 为 P_i 的公共零点集。于是以下映射是良好定义的

$$\varphi : \mathbb{P}^n \setminus Z \longrightarrow \mathbb{P}^m$$
$$x = (x_0 : \cdots : x_n) \longmapsto (P_0(x) : \cdots : P_m(x))$$

那么：(1) 存在常数 $c_1 = c_1(\varphi)$ 使得对所有 $x \in (\mathbb{P}^n \setminus Z)(\overline{\mathbb{Q}})$ 有：

$$H_{\mathbb{P}^n}(\varphi(x)) \leq c_1 H_{\mathbb{P}^n}(x)^d$$

(2) 令 $V \subseteq \mathbb{P}^n$ 为一个闭子代数簇且 $V \cap Z = \emptyset$，则存在两个常数 $c_1 = c_1(\varphi)$，$c_2 = c_2(\varphi)$ 使对任何 $x \in V(\overline{\mathbb{Q}})$ 有：

$$c_2 H(x)^d \leq H(\varphi(x)) \leq c_1 H(x)^d.$$

Rk. 无论把 V 如何嵌入 $\mathbb{P}^n$（n 可不同），定义得到的高度出来的相差之间的差异是可控的.

$V \xrightarrow{f} \mathbb{P}^n \xrightarrow{H} \mathbb{R}$，$V \xrightarrow{H_V} \mathbb{R}$

cf. Hindry «Arithmétique» Th 2.1.16.

或 Milne «elliptic curve» 讲义 2006 版 Prop 4.1

Rk $h = \log H$，$h(\varphi(x)) = d h(x) + O(1)$

现在考虑 $E(\overline{\mathbb{Q}})$ 上的高度：Weil 高度.

Def $E \subseteq \mathbb{P}^2$ 由 $Y^2Z = X^3 + aXZ^2 + bZ^3$ 定义. $\forall P \in E(\overline{\mathbb{Q}})$ 定义 P 的高度为

$$h(P) = \begin{cases} h(X(P) : Z(P)) & \text{若 } P \neq O \\ 0 & \text{若 } P = O \end{cases}$$

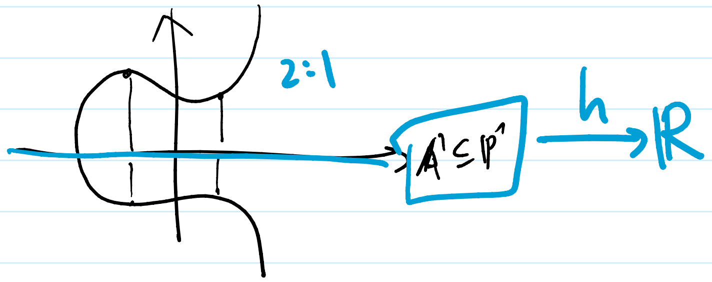
这相当于在 xy 平面中（即 $Z \neq 0$）考虑以下复合 $E \setminus O \subseteq \mathbb{A}^2$

$(E \setminus O)(\overline{\mathbb{Q}}) \subset \mathbb{A}^2(\overline{\mathbb{Q}}) \subset \mathbb{A}^1(\overline{\mathbb{Q}}) \xrightarrow{h = \log H} \mathbb{R}$

映射在 x,y 坐标中(即 2:1) 描述如下

$$(E\setminus O)(\overline{\mathbb{Q}})\subset\mathbb{A}^2(\overline{\mathbb{Q}})\longrightarrow\mathbb{A}^1(\overline{\mathbb{Q}})\xrightarrow{h=\log H}\mathbb{R}.$$

$y^2=x^3+ax+b$ $\quad P(x,y)\mapsto(x,y)\longmapsto x=(x:1)$



Weil 高度: Northcott 性质 ✓.

Th 存在常数 $c_1=c_1(E)$ 使得上述 Weil 高度 $h:E(\overline{\mathbb{Q}})\longrightarrow\mathbb{R}$ 满足:

$$-c_1\le h([2]P)-4h(P)\le c_1$$ 对 $\forall P\in E(\overline{\mathbb{Q}})$ 成立.

Pf. 由于仅有 4 个 2 扭点 (2-torsion) (O 及 $y=0$ 的三个点)
适当扩大 c_1 总可使 P 为 2-torsion 时上式成立. 以下可设 $P\notin E[2]$.

$[2]P$ 的 x 坐标公式 $$x([2]P)=\frac{x(P)^4-2ax(P)^2-8bx(P)+a^2}{4(x(P)^3+ax(P)+b)}$$

$(X:T)$
$\mathbb{P}^1\to\mathbb{P}^1$

考虑 $\Phi(X:T):=(X^4-2aX^2T^2-8bXT^3+a^2T^4:4T(X^3+aXT^2+bT^3))$

则有 $\Phi(x(P):1)=(x(2P):1)$

另一方面, 当 $\Delta=4a^3+27b^2\neq0$ 时, 多项式 x^3+ax+b 与 $x^4-2ax^2-8bx+a^2$
是互素的 (Euclid 除法)

于是 $\Phi(T,X)$ 的坐标不同时为 0, 即 $\Phi:\mathbb{P}^1\to\mathbb{P}^1$ 是良好定义的
$d=4$ 次的映射

由之前 Prop 及 Rk, $\quad h(\Phi(x))=4h(x)+O(1)$

考虑 $$(E\setminus E[2])(\overline{\mathbb{Q}})\longrightarrow\mathbb{P}^1(\overline{\mathbb{Q}})\xrightarrow{\Phi}\mathbb{P}^1(\overline{\mathbb{Q}})\xrightarrow{h}\mathbb{R}$$

$\cap$
$\mathbb{A}^2(\overline{\mathbb{Q}})\quad P(x,y)\longmapsto x(P)=(x(P):1)\longmapsto(x(2P):1)$

得 $h(2P)=h(x(2P):1)=h(\Phi(x(P):1))=h(\Phi(x(P)))=4h(x(P))+O(1)$
$=4h(x(P):1)+O(1)=4h(P)+O(1)$ #

$$= 4h(x(P):1)+O(1) = 4h(P)+O(1)$$ #

Th. E上的Weil高度h是对称的(即 $h(P)=h(-P)$),而且h满足平行四边形法则:

(*) $$h(P+Q)+h(P-Q)=2h(P)+2h(Q)+O(1)$$

Pf. P与−P的x坐标相同,故 $h(P)=h(-P)$.

(*)式 明显对 $P=0$ 或 $Q=0$ 成立. 上一个Th也说明 $P=\pm Q$ 时也成立.

以下设 $P,Q\in E\setminus O$ 且 $Q\neq\pm P$.

令 $x_1=x(P)$, $x_2=x(Q)$, $x_3=x(P+Q)$, $x_4=x(P-Q)$

$x_1+x_2=u$, $x_1\cdot x_2=v$.

$$(\#)\begin{cases} x_3+x_4=\dfrac{2u(a+v)+4b}{u^2-4v} \\ x_3\cdot x_4=\dfrac{(v-a^2)-4bu}{u^2-4v}\end{cases}$$

$(3x^2+4a)(x^4-2ax^2-8bx+a^2)-(3x^3-5ax-27b)(x^3+ax+b)=\Delta$

定义 $\Phi: \mathbb{P}^2\longrightarrow\mathbb{P}^2$ 良好定义($\Delta\neq0\Rightarrow$ 3个坐标不同为0.)

$$(T:U:V)\longmapsto(U^2-4TV : 2U(aT+V)+4bT^2 : (aT-V)^2-4bTU)$$

d=2次映射

(※) $$h(\Phi(T:U:V))=2h(T:U:V)+O(1)$$

定义 $\psi: (E\setminus O)\times(E\setminus O)\longrightarrow\mathbb{P}^2$

$$(P,Q)\mapsto(1: x(P)+x(Q) : x(P)\cdot x(Q))$$

$$\mu: E\times E\to E\times E$$
$$(P,Q)\mapsto(P+Q,P-Q)$$

由(#)知 $\psi\circ\mu=\Phi\circ\psi$

Lem $\alpha,\beta\in\overline{\mathbb{Q}}$, 则 $\frac{1}{2}H(\alpha)H(\beta)\le H(1,\alpha+\beta,\alpha\beta)\le 2H(\alpha)H(\beta)$

$\alpha=x(P)$, $\beta=x(Q)\Rightarrow$ (Δ) $h(\psi(P,Q))=h(x(P))+h(x(Q))+O(1)$

从而有 $h(P+Q)+h(P-Q)=h(x(P+Q))+h(x(P-Q))$

$$\overset{\Delta}{=} h(\psi(P+Q,P-Q))+O(1)$$
$$= h(\psi(\mu(P,Q)))+O(1)$$
$$\overset{\psi\circ\mu=\Phi\circ\psi}{=} h(\Phi(\psi(P,Q)))+O(1)$$

$$= h(\psi(\mu(P,Q))) + O(1)$$

$\psi\circ\mu = \sigma\circ\psi$

$$= h(\sigma(\psi(P,Q))) + O(1)$$

$(*)'$

$$= 2h(\psi(P,Q)) + O(1)$$

$(*)$

$$= 2h(P) + 2h(Q) + O(1) \qquad \#$$

Pf. $v \in \Omega_K$ $(\alpha, \beta \in K)$, 分 $|\alpha|_v \le |\beta|_v \le 1$, $|\alpha|_v \le 1 \le |\beta|_v$, $1 \le |\alpha|_v \le |\beta|_v$ 三种情况讨论.

若 $v \in \Omega_K^\infty$, $\max(1, |\alpha+\beta|_v, |\alpha\beta|_v) = \max(1, |\alpha|_v)\cdot\max(1, |\beta|_v)$

若 v 为 $\mathbb{R}, \mathbb{C}$ 值. $\Rightarrow \frac{1}{2}\max(1,|\alpha|_v)\max(1,|\beta|_v) \le \max(1, |\alpha+\beta|_v, |\alpha\beta|_v)$

$$\le 2\max(1,|\alpha|_v)(\max(1,|\beta|_v)$$

依 h 的定义, 取 $\prod_{v\in\Omega_K}$ 即得 $\#$.

最存在不影响 Northcott 性质前提下, 调整一下 Weil 高度定义为一个二次型.

Lem. S 集合. $d \in \mathbb{Z}$, $d > 1$, $h: S \to \mathbb{R}$ 及 $f: S \to S$ 使 $|h\circ f - dh| \le C$, 那么 $\forall x \in S$ 序列 $\frac{h(f^n(x))}{d^n}$ 是收敛的

记其极限为 $\hat{h}_f(x)$

我们已有 $\forall x \in S$ $\quad |h(x) - \hat{h}_f(x)| \le \frac{C}{d-1}$

且 $\hat{h}_f(f(x)) = d\,\hat{h}_f(x)$

(潜在用场景: f: d 次映射 把 h 调整为 $\hat{h}_f$ 之后, 常数 C 可取为 0.)
h: 高度.

Pf. 由 $|h\circ f - dh| \le C$ 多次复合后得:

$\forall x \in S$ $\quad -\frac{C}{d^k} \le \frac{h(f^k(x))}{d^k} - \frac{h(f^{k-1}(x))}{d^{k+1}} \le \frac{C}{d^k}$

对 $k = n+1, n+2, \cdots, m$ $(n < m)$ 求和:

$$-\frac{C}{d^n(d-1)} \le \frac{h(f^m(x))}{d^m} - \frac{h(f^n(x))}{d^n} \le \frac{C}{d^n(d-1)}$$

$$-\frac{c}{d^n(d-1)} \le \frac{h(f^m(x))}{d^m} - \frac{h(f^n(x))}{d^n} \le \frac{c}{d^n(d-1)}$$

于是 $\frac{h(f^n(x))}{d^n}$ 是 Cauchy, 从而收敛, 到 $\hat{h}_f(x)$.

→ 取 $m \to +\infty$ 得:

$$-\frac{c}{d^n(d-1)} \le \hat{h}_f(x) - \frac{h(f^n(x))}{d^n} \le \frac{c}{d^n(d-1)}$$

取 $n=0$: $\left|\hat{h}_f(x) - h(x)\right| \le \frac{c}{d-1}$.

$$\hat{h}_f(f(x)) = \lim_n \frac{h(f^{n+1}(x))}{d^n} = d \lim_n \frac{h(f^{n+1}(x))}{d^{n+1}} = d\,\hat{h}_f(x) \quad \#$$

把此引理应用到 $f=[2]: E \to E$ 这个 $d=4$ 次的映射以及 Weil 高度.

Th (Néron-Tate) K: 数域, E/K 椭圆曲线.

定义 $E(K)$ 上的 Néron-Tate 高度(又称典范高度):

$$\hat{h}(P) = \lim_{n\to+\infty} \frac{h([2^n]P)}{4^n} \qquad (h: \text{Weil 高度})$$

它满足 $\hat{h}(P) = h(P) + O(1)$ 以及

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

即 $\hat{h}$ 是 $E(K)$ 上的二次型, 特别地 $\hat{h}([m]P) = m^2 \hat{h}(P)$ $(\forall m \in \mathbb{Z})$ ✓

而且 $\hat{h}(P) = 0 \iff P$ 是一个挠点

Pf $\hat{h}(P) = h(P) + O(1)$ (→ 上述引理)

$$h(P'+Q') + h(P'-Q') = 2h(P') + 2h(Q') + O(1) \quad \forall P', Q' \in E(K)$$

取 $P' = [2^n]P$ 及 $Q' = [2^n]Q$ 即有:

$$\frac{-c}{4^n} \le \frac{h(2^n(P+Q)) + h(2^n(P-Q)) - 2h(2^nP) - 2h(2^nQ)}{4^n} \le \frac{c}{4^n}$$

取 $\lim_{n\to+\infty}$ 得出 $\hat{h}$ 的平行四边形法则.

若 P 为挠点, 则 $\exists m$, $[m]P = 0$. $\hat{h}(0) = 0$ 即 $\hat{h}([m]P) = 0 \Rightarrow \hat{h}(P) = 0$

若 P 挠元，$\exists m$，$mP=0$.　　$\hat{h}(0)=0$ 及 $\hat{h}(mP)=0 \Rightarrow \hat{h}(P)=0$

反之 若 $\hat{h}(P)=0$ 则 $\forall m$ $\hat{h}(mP)=0$ 由 Northcott $\Rightarrow \exists m' \neq m$ 使 $m'P=mP \Rightarrow P$ 挠元. #

Cor K 数域 E/K 椭圆曲线，则 $E(K)_{tor}$ 有限

之前已知满足 Northcott 性质 $\Rightarrow$ 二次型半正定

但对于 $\hat{h}$，知道更多：

Th 把 $\hat{h}$ 延拓到 $\mathbb{R}$-向量空间上 $E(K)\otimes\mathbb{R} \longrightarrow \mathbb{R}$ 这个二次型是正定的.

Rk. 证明需要代数数论中 Minkowski 数的几何

cf. Hindry «Arithmétique» Th. V.2.2.4.

（⚠ 在 $\mathbb{Q}$-向量空间上的二次型 q "$q(x)>0\ \forall x\neq 0$" $\not\Rightarrow$ q 正定.

例如在 $\mathbb{Q}(\sqrt{2})$ 上的 $q(x_1,x_2)=(x_1+x_2\sqrt{2})^2$）

这个正定二次型 $\hat{h}: E(K)\otimes\mathbb{R} \longrightarrow \mathbb{R}$

相应于一个内积 $\langle x,y\rangle := \frac{1}{2}\left(\hat{h}(x+y)-\hat{h}(x)-\hat{h}(y)\right)$

$$=\frac{1}{4}\left(\hat{h}(x+y)-\hat{h}(x-y)\right)$$

Def（先承认从 MW）取 $P_1,\cdots,P_r \in E(K)$ 使之成为 $E(K)/E(K)_{tor}$ 的一组基.

称 $\mathrm{Reg}(E/K) := \det\left(\langle P_i,P_j\rangle\right)_{1\le i,j\le r}$ 为 E/K 的 regulator.

↳ 这个量将会出现在 BSD 猜想中.

相应代数数论中单位群 $\mathcal{O}_K^\times$，表明也有 regulator 这个量.