不同椭圆曲线的二次扭之比较

张神星

2022年 L-函数及相关主题研讨会
福建 漳州

2022年8月8日

背景

给一个椭圆曲线
$E/\mathbb{Q}: y^2 = f(x)$

我们关心它的二次扭族
$E^{(n)}: ny^2 = f(x)$
其中 n 是一无平方因子的正整数

Mordell-Weil 秩

Ш 群

Selmer 群

⋮

多大程度能决定

Zarhin 问道:

给定阿贝尔簇 $A_1, A_2/K$, 如果对于任意有限扩张 F/K, 均有 $\mathrm{rank}(A_1/F) = \mathrm{rank}(A_2/F)$, 那么是否一定有 A_1 和 A_2 同源?

Mazur & Rubin: 或许我可以试试 Selmer 秩.

给定数域上椭圆曲线 $E_1, E_2/K$, 如果有

- G_K 模同构 $E_1[m] \cong E_2[m], m = \begin{cases} p^{k+1}, & p \leqslant 3 \\ p^k, & p > 3 \end{cases}$
- 相同的potential乘性约化素位集合 S
- $\forall \mathfrak{l} \in S, (E_1[m]/K\_\mathfrak{l})^\circ \cong (E_2[m]/K\_\mathfrak{l})^\circ$
- 一个分歧条件

则 $\mathrm{Sel}_{p^k}(E_1/F) \cong \mathrm{Sel}_{p^k}(E_2/F)$.

Chiu: 如果

$\mathrm{Sel}_p(E_1/F) \cong \mathrm{Sel}_p(E_2/F)$ 对所有的 F 和几乎所有 p 成立, 那么 E_1 和 E_2 确实同源.

存在不同源的 E_1, E_2 满足这个条件

主要结论

我们想构造一些 E_1, E_2 使得对很多 n 都有 $E_1^{(n)}$ 和 $E_2^{(n)}$ 有类似的算术性质.

记号

- $E_1: y^2 = x(x-e_1)(x+e_2)$, $\quad e_1+e_2+e_3=0$,
- $E_2: y^2 = x(x-e_1a^2)(x+e_2b^2)$, $\quad e_1a^2+e_2b^2+e_3c^2=0, 2\nmid abc$,

这些条件都是用来确保 Sel_2 同构的条件可能冗余

- 假设 n 与 $2e_1e_2e_3abc$ 互素, $\left(\frac{p}{q}\right)=1, \forall p\mid n, \forall 2\neq q\mid e_1e_2e_3abc$.
- 假设 $\mathrm{Sel}_2(E_1/\mathbb{Q})\cong\mathrm{Sel}_2(E_2/\mathbb{Q})\cong(\mathbb{Z}/2\mathbb{Z})^2$ 是最小的.

如果下述三种情况之一成立

(1) n 的素因子都模 8 余 1,

(2) e_1, e_2 是奇数, $2 \| e_3$,

(3) $2 \| e_1, 2 \| e_2, 4 \mid e_3$, 再加一些模 4 余 1 的条件.

奇同余椭圆曲线
$e_1 = e_2 = 1, e_3 = -2$

偶同余椭圆曲线
$e_1 = e_2 = 2, e_3 = -4$

则下述等价

- $\operatorname{rank}_{\mathbb{Z}}\left(E_1^{(n)}/\mathbb{Q}\right) = 0, Ш\left(E_1^{(n)}/\mathbb{Q}\right)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
- $\operatorname{rank}_{\mathbb{Z}}\left(E_2^{(n)}/\mathbb{Q}\right) = 0, Ш\left(E_2^{(n)}/\mathbb{Q}\right)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

- 证明所使用的方法仍然是传统的 2-下降法.
- 首先注意到 $\mathrm{Sel}_2(E_i/\mathbb{Q})$ 极小蕴含 $E = E_1, E_2, E_1^{(n)}, E_2^{(n)}$ 没有 4 阶有理点.
- 由正合列

$$0 \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \mathrm{Sel}_2(E) \to Ш(E/\mathbb{Q})[2] \to 0$$

- 可知 $E[2] \subseteq \mathrm{Sel}_2(E)$.

计算 Selmer 群

- 经典的下降理论告诉我们, $\mathrm{Sel}_2(E)$ 可以表为

$$\{\Lambda=(d_1,d_2,d_3)\in(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^3\colon\ D_\Lambda(\mathbb{A}_\mathbb{Q})\neq\emptyset, d_1d_2d_3\equiv 1 \bmod \mathbb{Q}^{\times 2}\},$$

其中齐性空间
$$D_\Lambda=\begin{cases} H_1: & e_1t^2+d_2u_2^2-d_3u_3^2=0,\\ H_2: & e_2t^2+d_3u_3^2-d_1u_1^2=0,\\ H_3: & e_3t^2+d_1u_1^2-d_2u_2^2=0.\end{cases}$$

- 那么 $E[2]\subseteq\mathrm{Sel}_2(E)$ 对应到

$$(1,1,1),\ (-e_3,-e_1e_3,e_1),\ (-e_2e_3,e_3,-e_2),\ (e_2,-e_1,-e_1e_2).$$

- **$p \nmid 2e_1e_2e_3n$**
- 由下降法一般结论，此时 $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow\ p \nmid d_1d_2d_3$.
- 故可不妨设 $d_i \mid 2e_1e_2e_3n$ 且无平方因子.
- **$p = \infty$**
- 很容易证明 $D_\Lambda^{(n)}(\mathbb{R}) \neq \emptyset \Leftrightarrow \begin{cases} d_1 > 0, & \text{若 } e_2 > 0, e_3 < 0; \\ d_2 > 0, & \text{若 } e_3 > 0, e_1 < 0; \\ d_3 > 0, & \text{若 } e_1 > 0, e_2 < 0. \end{cases}$

- $\boldsymbol{p \mid n (\Longrightarrow p \nmid e_1 e_2 e_3)}$
- $D_{\Lambda}^{(n)}(\mathbb{Q}_p) \neq \emptyset \Longleftrightarrow$

$$D_{\Lambda} = \begin{cases} H_1: & e_1 t^2 + d_2 u_2^2 - d_3 u_3^2 = 0, \\ H_2: & e_2 t^2 + d_3 u_3^2 - d_1 u_1^2 = 0, \\ H_3: & e_3 t^2 + d_1 u_1^2 - d_2 u_2^2 = 0. \end{cases}$$

第一种情形是显然的，后面的情形可以通过加上一个 $E[2]$ 对应的齐性空间化为第一种情形

$$\begin{cases} \left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) = 1, & 若\ p \nmid d_1 d_2 d_3 \\ \left(\frac{-e_2 e_3 d_1}{p}\right) = \left(\frac{e_3 n/d_2}{p}\right) = \left(\frac{e_2 n/d_3}{p}\right) = 1, & 若\ p \nmid d_1, p \mid d_2, p \mid d_3; \\ \left(\frac{-e_3 n/d_1}{p}\right) = \left(\frac{-e_3 e_1 d_2}{p}\right) = \left(\frac{e_1 n/d_3}{p}\right) = 1, & 若\ p \mid d_1, p \nmid d_2, p \mid d_3; \\ \left(\frac{e_2 n/d_1}{p}\right) = \left(\frac{-e_1 n/d_2}{p}\right) = \left(\frac{-e_1 e_2 d_3}{p}\right) = 1, & 若\ p \mid d_1, p \mid d_2, p \nmid d_3; \end{cases}$$

- 转化为线性代数语言

$$d_1 = p_1^{x_1} \cdots p_k^{x_k} \bullet \widetilde{d_1}, \qquad x_i = v_{p_i}(d_1)$$
$$d_2 = p_1^{y_1} \cdots p_k^{y_k} \bullet \widetilde{d_2}, \qquad y_i = v_{p_i}(d_2)$$
$$d_3 = p_1^{z_1} \cdots p_k^{z_k} \bullet \widetilde{d_3}, \qquad z_i = v_{p_i}(d_3)$$

- $\widetilde{d_i} \mid 2e_1e_2e_3$ 且无平方因子.
- 设 $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{F}_2^k$ 等等, 则

$$\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}, \qquad \widetilde{d_1}\widetilde{d_2}\widetilde{d_3} \in \mathbb{Q}^{\times 2}.$$

- 设 $\tilde{\Lambda}=(\widetilde{d_1},\widetilde{d_2},\widetilde{d_3})$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_v)$ 和 $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$ 的可解性. (假设 n 素因子都 $\equiv 1 \bmod 8$)

用于计算 $\mathrm{Sel}_2(E^{(n)})$

用于计算 $\mathrm{Sel}_2(E)$

- $v=\infty$, 由 d_i 和 $\widetilde{d_i}$ 符号相同知二者可解性相同.
- $v=q\mid 2e_1e_2e_3$, 由 $n, d_i/\widetilde{d_i}$ 是 $\mathbb{Q}_q$ 中的平方知二者可解性相同.
- 由于我们假设 $\mathrm{Sel}_2(E)=E[2]$ 极小, $\tilde{\Lambda}\in E[2]$.
- 如果 $\tilde{\Lambda}=(-e_3,-e_1e_3,e_1)$,(其它情形类似) 则

因此
$\mathrm{Sel}_2'(E^{(n)})=\mathrm{Sel}_2(E^{(n)})/E[2]$
中每个元素都有唯一代表元
(d_1,d_2,d_3) 满足 $0<d_i\mid n$.

$$\Lambda\bullet(-e_3n,-e_1e_3,e_1n)=\left(\prod_{i=1}^{k}p_i^{1-x_i},\prod_{i=1}^{k}p_i^{y_i},\prod_{i=1}^{k}p_i^{1-z_i}\right).$$

- 加上在 $v \mid n$ 处的可解性条件(一堆剩余符号条件)，我们得到

Monsky 矩阵

$$\begin{aligned} \mathrm{Sel}_2'(E^{(n)}) &\xrightarrow{\sim} \mathrm{Ker}\begin{pmatrix} \mathbf{A}+\mathbf{D}_{-e_3} & \mathbf{D}_{-e_2e_3} \\ \mathbf{D}_{-e_1e_3} & \mathbf{A}+\mathbf{D}_{e_3} \end{pmatrix} \\ (d_1,d_2,d_3) &\mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \end{aligned}$$

加性勒让德符号
事实上 $\mathbf{D}_u = \mathbf{O}$

希尔伯特符号

- 其中 $\mathbf{A} = \left(\left[p_j, -n\right]_{p_i}\right)_{i,j} \in M_k(\mathbb{F}_2)$，$\mathbf{D}_u = \mathrm{diag}\left(\left[\frac{u}{p_1}\right], \dots, \left[\frac{u}{p_k}\right]\right) \in M_k(\mathbb{F}_2)$.
- 特别地，对于 $\mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right)$.

$E_1: (e_1, e_2, e_3)$
$E_2: (e_1a^2, e_2b^2, e_3c^2)$

计算 Cassels 配对

- Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2'(E^{(n)})$ 上定义了一个反对称双线性型:
- 对于 Λ, Λ', 选择 $P = (P_v)_v \in D_\Lambda(\mathbb{A}_\mathbb{Q}), Q_i \in H_i(\mathbb{Q})$. 令 L_i 为定义了 H_i 在 Q_i 处切平面的线性型, 定义

$$\langle \Lambda, \Lambda' \rangle = \sum_v \langle \Lambda, \Lambda' \rangle_v , \qquad \text{其中 } \langle \Lambda, \Lambda' \rangle_v = \sum_{i=1}^{3} [L_i(P_v), d_i']_v \, .$$

- 它不依赖 P 和 Q_i 的选择.

引理(Cassels1998) 如果 $p \nmid 2\infty$, H_i 和 L_i 的系数均是 p 进整数, 且模 p 后, $\overline{D}_\Lambda$ 仍定义了一条亏格 1 的曲线并带有切平面 $\overline{L}_i = 0$, 则 $\langle \Lambda, \Lambda' \rangle_p = 0$.

- 由正合列

$$0 \longrightarrow E[2] \longrightarrow E[4] \xrightarrow{\times 2} E[2] \longrightarrow 0$$

- 得长正合列

$$0 \longrightarrow E[2] \longrightarrow \mathrm{Sel}_2(E) \longrightarrow \mathrm{Sel}_4(E) \longrightarrow \mathrm{Im}\,\mathrm{Sel}_4(E) \longrightarrow 0.$$

- 而 Cassels 配对的核是 $\frac{\mathrm{Im}\,\mathrm{Sel}_4(E)}{E[2]}$, 因此 **Cassels 配对非退化**等价于

$$\mathbf{rank}_{\mathbb{Z}}(\boldsymbol{E}/\mathbb{Q}) = \mathbf{0}, \qquad Ш(\boldsymbol{E}/\mathbb{Q})[\mathbf{2}^{\infty}] \cong (\mathbb{Z}/\mathbf{2}\mathbb{Z})^{\mathbf{2}t}.$$

- 回忆

$$E_1^{(n)}: ny^2 = x(x-e_1)(x+e_2), \qquad E_2^{(n)}: ny^2 = x(x-e_1a^2)(x+e_2b^2)$$

- 其中 $e_1a^2 + e_2b^2 + e_3c^2 = 0, a, b, c$ 是互素的奇数.
- 首先 $\mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right)$. 我们分别用正体和花体来表示 $E_1^{(n)}$ 和 $E_2^{(n)}$ 对应的记号.
- 设 $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right)$.
- 若能证明 $[L_i(P_v), d_i']_v = [\mathcal{L}_i(\mathcal{P}_v), d_i']_v$, 则对应的 Cassels 配对就同构了.
- 在多数情形这不难证明, 我们仅说明相对复杂的一种情形.

- $v = p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$

$\in D_\Lambda(\mathbb{Q}_p)$ $\in \mathcal{D}_\Lambda(\mathbb{Q}_p)$

- 设 $Q_i = (\alpha_i, \beta_i, \gamma_i) \in H_i(\mathbb{Q})$. 选取 $P_p = (1,0,u,v)$, $\mathcal{P}_p = (1,0,cu,bv)$, 则

$$L_1(P_p) = e_1 n\alpha_1 - d_3\gamma_1 v + d_2\beta_1 u$$

$$\mathcal{L}_1(\mathcal{P}_p) = ae_1 n\alpha_1 - bd_3\gamma_1 v + cd_2\beta_1 u$$

利用 $e_1a^2 + e_2b^2 + e_3c^2 = 0$

$$L_1(P_p)\mathcal{L}_1(\mathcal{P}_p) = \frac{1}{2}(a+b)(a+c)(b+c)\left(\frac{e_1 n\alpha_1}{b+c} + \frac{d_2\beta_1 u}{a+b} - \frac{d_3\gamma_1 v}{a+c}\right)^2$$

引理 若 $a \equiv b \equiv c \equiv 1 \bmod 4$, 则 $(a+b)(b+c)(c+a)/8 \equiv 1 \bmod 4$ 是模 $p \mid n$ 的二次剩余.

- 对于一些特殊的 (e_1, e_2, e_3), 我们不需要 $p \equiv 1 \bmod 8, \forall p \mid n$ 这么强的条件.
- 例如 e_1, e_2 是奇数, $2 \| e_3$ (如奇数同余椭圆曲线情形), 此时需要对 $v = 2$ 情形进行单独处理, 最后也可以得到该结论.
- 例如 $2 \| e_1, 2 \| e_2, 4 \mid e_3$ (如偶数同余椭圆曲线情形), 此时除了需要对 $v = 2$ 情形进行单独处理, 还需要考虑齐性空间在 $v = \infty$ 的解的问题.