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 4 月 5 日

记号

考虑椭圆曲线

$$E = \mathscr{E}_{e_1,e_2} : y^2 = x(x-e_1)(x+e_2),\ \ e_1, e_2 \in \mathbb{Z}.$$

设 $e_3 = -e_1 - e_2$. 容易看出, E 和 $\mathscr{E}_{e_2,e_3}, \mathscr{E}_{e_3,e_1}$ 同构, 因此 (e_1, e_2, e_3) 循环对称. 我们想要比较不同的 (e_1, e_2, e_3) 对应的 $\{E^{(n)}\}$, 因此不妨设 $\gcd(e_1, e_2, e_3) = 1$ 或 2, n 是奇数.

我们总假设 E 没有 4 阶有理点, 即 $E(\mathbb{Q})[2^\infty] = E[2]$. 设 $\mathrm{Sel}_2(E)$ 是 $E/\mathbb{Q}$ 的 2 Selmer 群, 则由正合列

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

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

Selmer 群与齐性空间

经典的下降理论告诉我们, $\mathrm{Sel}_2(E)$ 可以表为

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

其中齐性空间

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

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

$$(1,1,1),\ (-e_3, -e_1 e_3, e_1),\ (-e_2 e_3, e_3, -e_2),\ (e_2, -e_1, -e_1 e_2).$$

Cassels 配对

Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}'_2(E) = \mathrm{Sel}_2(E)/E(\mathbb{Q})[2]$ 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. 这里 $[-,-]_v \in \mathbb{F}_2$ 表示加性希尔伯特符号.

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 $\langle -,- \rangle_p = 0$.

Cassels 配对的非退化性

正合列

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

诱导了长正合列

$$0 \to E[2] = \frac{E(\mathbb{Q})[2]}{2E(\mathbb{Q})[4]} \to \mathrm{Sel}_2(E) \to \mathrm{Sel}_4(E) \to \mathrm{ImSel}_4(E) \to 0.$$

如果 $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ 且 $\text{Ш}(E/\mathbb{Q})$ 没有 4 阶元, 则 $\mathrm{Sel}_2(E) \cong \mathrm{Sel}_4(E)$. 而 Cassels 配对的核是 $\mathrm{ImSel}_4(E)/E[2]$, 因此 Cassels 配对非退化. 反之亦然, 因此二者等价.

主要结果

设 (a, b, c) 是满足 $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ 的本原三元奇数组. 令

$$\mathcal{E} : y^2 = x(x - e_1 a^2)(x + e_2 b^2),$$

$$\mathcal{E}^{(n)} : y^2 = x(x - n e_1 a^2)(x + n e_2 b^2).$$

定理

假设 n 与 $e_1 e_2 e_3 abc$ 互素且

- $\left(\frac{p}{q}\right) = 1, p \equiv 1 \bmod 8$, 其中 $p \mid n, q \mid e_1 e_2 e_3 abc$ 是奇素数;
- E 和 $E^{(n)}$ 没有 4 阶有理点.

如果 $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, 则下述等价:

1. $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0, Ш(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
2. $\mathrm{rank}_{\mathbb{Z}} \mathcal{E}^{(n)}(\mathbb{Q}) = 0, Ш(\mathcal{E}^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

主要结果：特殊情形

上述条件 $p \equiv 1 \bmod 8$ 对于特殊的 (e_1, e_2, e_3) 可以去除.

定理

假设 n 与 $e_1e_2e_3abc$ 互素且

- $\left(\frac{p}{q}\right) = 1$, 其中 $p \mid n, q \mid e_1e_2e_3abc$ 是奇素数;
- e_1, e_2 是奇数, $2 \parallel e_3$.

如果 $\mathrm{Sel}_2(E/\mathbb{Q}) \cong \mathrm{Sel}_2(\mathcal{E}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, 则下述等价:

1. $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0, Ш(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
2. $\mathrm{rank}_{\mathbb{Z}} \mathcal{E}^{(n)}(\mathbb{Q}) = 0, Ш(\mathcal{E}^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

对于 $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ 情形也有类似结论.

$\mathbb{R}$ 处可解性

现在我们考虑 $\mathrm{Sel}_2\left(E^{(n)}\right)$.

由下降法一般结论, 若 $p \nmid 2e_1e_2e_3n$, 则 $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \iff p \nmid d_1d_2d_3$. 所以我们可不妨设 $d_i \mid 2e_1e_2e_3n$ 平方自由.

引理

$D_\Lambda^{(n)}(\mathbb{R}) \neq \emptyset$ 当且仅当

- $d_1 > 0$, 若 $e_2 > 0, e_3 < 0$;
- $d_2 > 0$, 若 $e_3 > 0, e_1 < 0$;
- $d_3 > 0$, 若 $e_1 > 0, e_2 < 0$.

$p \mid n$ 处可解性

引理

设 n 和 $e_1e_2e_3$ 互素, $p \mid n$. $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset$ 当且仅当

- $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) = 1$, if $p \nmid d_1d_2d_3$;
- $\left(\frac{-e_2e_3d_1}{p}\right) = \left(\frac{e_3n/d_2}{p}\right) = \left(\frac{-e_2n/d_3}{p}\right) = 1$, if $p \nmid d_1, p \mid d_2, p \mid d_3$;
- $\left(\frac{-e_3n/d_1}{p}\right) = \left(\frac{-e_3e_1d_2}{p}\right) = \left(\frac{e_1n/d_3}{p}\right) = 1$, if $p \mid d_1, p \nmid d_2, p \mid d_3$;
- $\left(\frac{e_2n/d_1}{p}\right) = \left(\frac{-e_1n/d_2}{p}\right) = \left(\frac{-e_1e_2d_3}{p}\right) = 1$, if $p \mid d_1, p \mid d_2, p \nmid d_3$.

第一种情形是显然的, 后面的通过将 Λ 乘以某个 $E[2]$ 点化归为第一种情形.

转化为线性代数语言

记

$$
\begin{aligned}
d_1 &= p_1^{x_1} \cdots p_k^{x_k} \cdot \widetilde{d}_1, \\
d_2 &= p_1^{y_1} \cdots p_k^{y_k} \cdot \widetilde{d}_2, \\
d_3 &= p_1^{z_1} \cdots p_k^{z_k} \cdot \widetilde{d}_3.
\end{aligned}
$$

$$x_i = v_{p_i}(d_1), \quad y_i = v_{p_i}(d_2), \quad z_i = v_{p_i}(d_3).$$

我们有 $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$, $\widetilde{d}_1 \widetilde{d}_2 \widetilde{d}_3 \in \mathbb{Q}^{\times 2}$, 其中 $\mathbf{x} = (x_1, \ldots, x_k)^{\mathrm{T}} \in \mathbb{F}_2^k$ 等等.

Selmer 群

定理

假设 n 与 $e_1e_2e_3abc$ 互素且

- $\left(\frac{p}{q}\right) = 1, p \equiv 1 \bmod 8$, 其中 $p \mid n, q \mid e_1e_2e_3abc$ 是奇素数;
- E 和 $E^{(n)}$ 没有 4 阶有理点.

如果 $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, 则

$$\mathrm{Sel}_2'(E^{(n)}) \xrightarrow{\sim} \mathrm{Ker}\begin{pmatrix} \mathbf{A} & \\ & \mathbf{A} \end{pmatrix}$$

$$(d_1, d_2, d_3) \mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix},$$

其中 $0 < d_i \mid n$, $\mathbf{A} = \left([p_j, -n]_{p_i}\right)_{i,j} \in M_k(\mathbb{F}_2)$.

Selmer 群

设 $\widetilde{\Lambda} = (\widetilde{d}_1, \widetilde{d}_2, \widetilde{d}_3)$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_v)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$ 的可解性.

- $v = \infty$, 由二者符号相同得到.
- $v = q \mid 2e_1e_2e_3$, 由 $n, d_i/\widetilde{d}_i$ 是 q 进平方得到.

因此 $\Lambda \in \mathrm{Sel}_2\left(E^{(n)}/\mathbb{Q}\right) \iff \widetilde{\Lambda} \in \mathrm{Sel}_2(E/\mathbb{Q}), D_{\Lambda}^{(n)}(\mathbb{Q}_p) \neq \emptyset, \forall p \mid n$.

由假设可知 $\widetilde{\Lambda} \in E[2]$, 例如 $\widetilde{\Lambda} = (-e_3, -e_1e_3, e_1)$, 则

$$\Lambda \cdot (-e_3 n, -e_1e_3, e_1 n) = \left(\prod_{i=1}^{k} p_i^{1-x_i}, \prod_{i=1}^{k} p_i^{y_i}, \prod_{i=1}^{k} p_i^{1-z_i}\right).$$

其它情形类似. 因此 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 中每个元素都有唯一代表元 (d_1, d_2, d_3) 满足 $0 < d_i \mid n$.

Cassels 配对的计算

设 $e_1a^2+e_2b^2+e_3c^2=0$, a,b,c 是互素的非零奇数. 不妨设 $a\equiv b\equiv c\equiv 1 \bmod 4$. 首先 $\mathrm{Sel}_2'(E^{(n)})\cong \mathrm{Sel}_2'(\mathcal{E}^{(n)})$. 我们用花体来表示 $\mathcal{E}^{(n)}$ 对应的齐性空间等记号. 设 $\Lambda=(d_1,d_2,d_3),\Lambda'=(d_1',d_2',d_3')$.

对于素位 $v\mid 2e_1e_2e_3abc$, 由于 d_i' 是 $\mathbb{Q}_v$ 中的平方, 因此 $[\mathcal{L}_i(\mathcal{P}_v),d_i']_v=0=[L_i,d_i']_v$.

设 $Q_i=(\alpha_i,\beta_i,\gamma_i)\in H_i(\mathbb{Q})$. 对于 $v=p\mid n$, 我们有 $[a,d_i']_p=[b,d_i']_p=[c,d_i']_p=0$. 若 $p\nmid d_1d_2d_3$. 选取 $\mathcal{P}_p=(0,1/\sqrt{d_1},1/\sqrt{d_2},1/\sqrt{d_3})=P_p$. 则

$$\mathcal{L}_1(\mathcal{P}_p)=\beta_1\sqrt{d_2}-\gamma_1\sqrt{d_3}=L_1(P_p).$$

类似地, $\mathcal{L}_2(\mathcal{P}_p)=L_2(P_p)$, $\mathcal{L}_3(\mathcal{P}_p)=L_3(P_p)$.

Cassels 配对的计算 (续)

若 $p \nmid d_1, p \mid d_2, p \mid d_3$, 则 $e_3 n/d_2, -e_2 n/d_3 \in \mathbb{Q}_p^{\times 2}$. 选取 $\mathcal{P}_p = (1, 0, cu, bv)$, $u^2 = e_3 n/d_2$, $v^2 = -e_2 n/d_3$. 则 $P_p = (1, 0, u, v)$,

$$\begin{aligned}
\mathcal{L}_1(\mathcal{P}_p) &= ae_1 n\alpha_1 - bd_3\gamma_1 v + cd_2\beta_1 u,\\
\mathcal{L}_2(\mathcal{P}_p) &= be_2 n\alpha_2 + bd_3\beta_2 v = bL_2(P_p),\\
\mathcal{L}_3(\mathcal{P}_p) &= ce_3 n\alpha_3 - cd_2\gamma_3 u = cL_3(P_p).
\end{aligned}$$

由下一页的引理可知

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

加上下下页的引理, 可得 $[\mathcal{L}_i(\mathcal{P}_p), d_i']_p = [L_i(P_p), d_i']_p$.

因此二者的 Cassels 配对也是一样的.

一个引理

设 $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$. 则

$$
\begin{aligned}
&(ax+by+cz)(x+y+z) - \frac{1}{2}(e_1 a + e_2 b + e_3 c)\left(\frac{x^2}{e_1} + \frac{y^2}{e_2} + \frac{z^2}{e_3}\right) \\
&= \frac{1}{2}(a+b)(b+c)(c+a)\left(\frac{x}{b+c} + \frac{y}{c+a} + \frac{z}{a+b}\right)^2.
\end{aligned}
$$

这由下述等式以及轮换得到的另两个等式推出:

$$
\begin{aligned}
a - \frac{(a+b)(a+c)}{2(b+c)} &= \frac{a(b+c) - bc - a^2}{2(b+c)} = \frac{e_1 a(b+c) - e_1 bc - e_1 a^2}{2e_1(b+c)} \\
&= \frac{e_1 a(b+c) + (e_2+e_3)bc + e_2 b^2 + e_3 c^2}{2e_1(b+c)} = \frac{e_1 a + e_2 b + e_3 c}{2e_1}.
\end{aligned}
$$

另一个引理

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.

设互素的整数 α, β 满足 $\frac{\beta}{\alpha} = \frac{e_1(a-c)}{e_2(b+c)}$. 则 α 是奇数, β 是偶数. 可以验证

$$\lambda a = e_1\alpha^2 + 2e_2\alpha\beta - e_2\beta^2 \equiv e_1 \bmod 4,$$
$$\lambda b = e_1\alpha^2 - 2e_1\alpha\beta - e_2\beta^2 \equiv e_1 \bmod 4,$$
$$\lambda c = e_1\alpha^2 + e_2\beta^2 \equiv e_1 \bmod 4,$$

其中 $\lambda \equiv e_1 \bmod 4$.

另一个引理 (续)

于是

$$\lambda(a+b)=2(\alpha-\beta)(e_1\alpha+e_2\beta),$$
$$\lambda(b+c)=2e_1\alpha(\alpha-\beta),$$
$$\lambda(c+a)=2\alpha(e_1\alpha+e_2\beta)$$

$$\frac{1}{8}(a+b)(b+c)(c+a)=e_1\lambda\left(\lambda^{-2}\alpha(\alpha-\beta)(e_1\alpha+e_2\beta)\right)^2\equiv 1 \bmod 4.$$

设 $q\mid\lambda$. 通过整除关系可以证明 $q\mid e_1e_2e_3$. 于是对于 $p\mid n$,

$$\left(\frac{e_1\lambda}{p}\right)=\left(\frac{p}{e_1\lambda}\right)=\prod_{q\mid e_1\lambda}\left(\frac{p}{q}\right)^{v_q(e_1\lambda)}=1.$$

特殊情形

设 e_1, e_2 是奇数, e_3 是偶数. 若 $D_\Lambda^{(n)}(\mathbb{Q}_2) \neq \emptyset$, 可以证明 d_1, d_2 同奇偶. 如果需要的话, 我们将 Λ 乘上 2 阶扭点 $(-e_3 n, -e_1 e_3, e_1)$, 可以保证 d_1, d_2, d_3 都是奇数.

在此前提下, 可以证明: 若 $D_\Lambda^{(n)}$ 在 2 以外处处有解, 则每个单独的 H_i 也是在 2 以外处处有解. 由 Hilbert 符号的乘积公式,

$$[e_1 n d_3, d_1]_2 = [e_2 n d_1, d_2]_2 = [e_3 n d_2, d_3]_2 = 0.$$

由此可以证明 $D_\Lambda^{(n)}$ 在 2 处也有解. 这样我们就不用担心 2 处的可解性.

计算 Cassels 配对时, 在 $v = 2$ 处所需要的比较的 Hilbert 符号也可以用前述引理证明相等.

特殊情形

设 $2 \parallel e_1, 2 \parallel e_2$, $4 \mid e_3$. 此时总可以通过乘以一个扭点使得 d_1, d_2, d_3 都是奇数. 若 $D_\Lambda^{(n)}(\mathbb{Q}_2) \neq \emptyset$, 可以证明 $d_3 \equiv 1 \bmod 4$ 同奇偶. 在此前提下, 可以证明: 若 $D_\Lambda^{(n)}$ 在 2 以外处处有解, $D_\Lambda^{(n)}$ 在 2 处也有解.

若 $e_2 > 0, e_3 < 0$, 则 $d_1 > 0$. 此时我们需要记

$$
\begin{aligned}
d_1 &= p_1^{x_1} \cdots p_k^{x_k} \cdot \widetilde{d}_1, \\
d_2 &= p_1^{y_1} \left(\frac{-1}{p_1}\right)^{z_1} \cdots p_k^{y_k} \left(\frac{-1}{p_1}\right)^{z_k} \cdot \widetilde{d}_2, \\
d_3 &= (p_1^*)^{z_1} \cdots (p_k^*)^{z_k} \cdot \widetilde{d}_3.
\end{aligned}
$$

通过考虑在 $q \mid e_1 e_2 e_3$ 处的可解性, 我们可以得到类似但条件更复杂的结论.

感谢各位的倾听!