不同椭圆曲线的二次扭之比较

张神星

合肥工业大学

南京大学 金陵数论与代数几何会议
2022 年 9 月 25 日

- 给定一个数域上的椭圆曲线 E/K, 我们关心它的二次扭族
$$E^{\chi}/K, \quad \text{其中 } \chi: G_K \to \{\pm 1\}$$
的各种算术量: Mordell-Weil 秩、Ш 群、Selmer 群等等.

背景

- 给定一个数域上的椭圆曲线 E/K, 我们关心它的二次扭族
$$E^\chi/K, \quad \text{其中 } \chi : G_K \to \{\pm 1\}$$
的各种算术量: Mordell-Weil 秩、Ш 群、Selmer 群等等.
- 那么反过来, 从这些算术量中在多大程度上能决定原来的椭圆曲线 E/K 呢?

背景

- 给定一个数域上的椭圆曲线 E/K, 我们关心它的二次扭族
$$E^\chi/K, \quad \text{其中 } \chi : G_K \to \{\pm 1\}$$
的各种算术量: Mordell-Weil 秩、Ш 群、Selmer 群等等.
- 那么反过来, 从这些算术量中在多大程度上能决定原来的椭圆曲线 E/K 呢?
- 我们知道, 如果 E_1 和 E_2 同源, 那么
$$\operatorname{rank}_{\mathbb{Z}} E_1^\chi(K) = \operatorname{rank}_{\mathbb{Z}} E_2^\chi(K)$$
对任意 χ 均成立.

背景

- 给定一个数域上的椭圆曲线 E/K, 我们关心它的二次扭族

$$E^\chi/K, \quad \text{其中 } \chi : G_K \to \{\pm 1\}$$

  的各种算术量: Mordell-Weil 秩、Ш 群、Selmer 群等等.
- 那么反过来, 从这些算术量中在多大程度上能决定原来的椭圆曲线 E/K 呢?
- 我们知道, 如果 E_1 和 E_2 同源, 那么

$$\mathrm{rank}_{\mathbb{Z}} E_1^\chi(K) = \mathrm{rank}_{\mathbb{Z}} E_2^\chi(K)$$

  对任意 χ 均成立.
- Zarhin(1989) 提出了如下猜想: 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

$$\mathrm{rank}_{\mathbb{Z}} A_1(F) = \mathrm{rank}_{\mathbb{Z}} A_2(F),$$

背景

- 给定一个数域上的椭圆曲线 E/K, 我们关心它的二次扭族
$$E^\chi/K, \quad \text{其中 } \chi : G_K \to \{\pm 1\}$$
的各种算术量: Mordell-Weil 秩、Ш 群、Selmer 群等等.
- 那么反过来, 从这些算术量中在多大程度上能决定原来的椭圆曲线 E/K 呢?
- 我们知道, 如果 E_1 和 E_2 同源, 那么
$$\operatorname{rank}_{\mathbb{Z}} E_1^\chi(K) = \operatorname{rank}_{\mathbb{Z}} E_2^\chi(K)$$
对任意 χ 均成立.
- Zarhin(1989) 提出了如下猜想: 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
$$\operatorname{rank}_{\mathbb{Z}} A_1(F) = \operatorname{rank}_{\mathbb{Z}} A_2(F),$$
那么 A_1 和 A_2 是否一定同源?

- Mazur 和 Rubin(2015) 考虑了 Selmer 秩的问题.

Selmer 秩的情形

- Mazur 和 Rubin(2015) 考虑了 Selmer 秩的问题.
- 给定数域上椭圆曲线 $E_1, E_2/K$, 如果有
    - G_K 模同构 $E_1[m] \cong E_2[m]$, 其中 $m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$
    - 相同的 potential 乘性约化素位集合 S
    - $\forall \mathfrak{l} \in S, \left(E_1[m]/K_{\mathfrak{l}}\right)^{\circ} \cong \left(E_2[m]/K_{\mathfrak{l}}\right)^{\circ}$
    - 一个分歧条件

Selmer 秩的情形

- Mazur 和 Rubin(2015) 考虑了 Selmer 秩的问题.
- 给定数域上椭圆曲线 $E_1, E_2/K$, 如果有
  - G_K 模同构 $E_1[m] \cong E_2[m]$, 其中 $m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$
  - 相同的 potential 乘性约化素位集合 S
  - $\forall \mathfrak{l} \in S, \left(E_1[m]/K_{\mathfrak{l}}\right)^{\circ} \cong \left(E_2[m]/K_{\mathfrak{l}}\right)^{\circ}$
  - 一个分歧条件

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

- Mazur 和 Rubin(2015) 考虑了 Selmer 秩的问题.
- 给定数域上椭圆曲线 $E_1, E_2/K$, 如果有
  - G_K 模同构 $E_1[m] \cong E_2[m]$, 其中 $m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$
  - 相同的 potential 乘性约化素位集合 S
  - $\forall \mathfrak{l} \in S, \left(E_1[m]/K_{\mathfrak{l}}\right)^{\circ} \cong \left(E_2[m]/K_{\mathfrak{l}}\right)^{\circ}$
  - 一个分歧条件

  则 $\mathrm{Sel}_{p^k}(E_1/F) \cong \mathrm{Sel}_{p^k}(E_2/F), \forall F/K$.
- 特别地, 存在不同源的 E_1, E_2 满足这个条件.

- Mazur 和 Rubin(2015) 考虑了 Selmer 秩的问题.
- 给定数域上椭圆曲线 $E_1, E_2/K$, 如果有
  - G_K 模同构 $E_1[m] \cong E_2[m]$, 其中 $m = \begin{cases} p^{k+1}, & p \le 3 \\ p^k, & p > 3 \end{cases}$
  - 相同的 potential 乘性约化素位集合 S
  - $\forall \mathfrak{l} \in S, \left(E_1[m]/K_{\mathfrak{l}}\right)^{\circ} \cong \left(E_2[m]/K_{\mathfrak{l}}\right)^{\circ}$
  - 一个分歧条件

  则 $\mathrm{Sel}_{p^k}(E_1/F) \cong \mathrm{Sel}_{p^k}(E_2/F), \forall F/K$.
- 特别地, 存在不同源的 E_1, E_2 满足这个条件.
- Chiu(2020) 证明了: 如果 $\mathrm{Sel}_p(E_1/F) \cong \mathrm{Sel}_p(E_2/F)$ 对所有的 F/K 和几乎所有 p 成立, 那么 E_1 和 E_2 同源.

记号

- 我们想要构造一些 E_1, E_2 使得对于它们二次扭族的一个子族具有相似的算术性质.

- 我们想要构造一些 E_1, E_2 使得对于它们二次扭族的一个子族具有相似的算术性质.
- 考虑具有全部有理 2 阶点的椭圆曲线

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

设 $c = -a - b$.

记号

- 我们想要构造一些 E_1, E_2 使得对于它们二次扭族的一个子族具有相似的算术性质.
- 考虑具有全部有理 2 阶点的椭圆曲线

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

设 $c = -a - b$.

- 通过一个平移可以看出, E 和 $\mathscr{E}_{b,c}, \mathscr{E}_{c,a}$ 同构.

记号

- 我们想要构造一些 E_1, E_2 使得对于它们二次扭族的一个子族具有相似的算术性质.
- 考虑具有全部有理 2 阶点的椭圆曲线

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

  设 $c = -a - b$.
- 通过一个平移可以看出, E 和 $\mathscr{E}_{b,c}, \mathscr{E}_{c,a}$ 同构.
- 由于我们想要研究二次扭族, 因此不妨设 $\gcd(a,b,c) = 1$ 或 2, 且 n 是奇数.

记号

- 现在我们考虑两条椭圆曲线

$$E_i : y^2 = x(x - a_i)(x + b_i), \quad c_i = -a_i - b_i, \quad i = 1, 2.$$

记号

- 现在我们考虑两条椭圆曲线

$$E_i : y^2 = x(x-a_i)(x+b_i), \quad c_i = -a_i - b_i, \quad i = 1, 2.$$

- 由于作为 $G_{\mathbb{Q}}$ 模, $E_1[2] \cong E_2[2]$, 因此二者的 2-Selmer 群落在同一个群 $\mathrm{H}^1(G_{\mathbb{Q}}, E_i[2])$ 中.

- 现在我们考虑两条椭圆曲线

$$E_i : y^2 = x(x-a_i)(x+b_i), \quad c_i = -a_i - b_i, \quad i = 1, 2.$$

- 由于作为 $G_{\mathbb{Q}}$ 模, $E_1[2] \cong E_2[2]$, 因此二者的 2-Selmer 群落在同一个群 $\mathrm{H}^1(G_{\mathbb{Q}}, E_i[2])$ 中.
- 由于技术上的原因, 我们进一步假设有 $G_{\mathbb{Q}}$ 模同构 $E_1[4] \cong E_2[4]$.

记号

- 现在我们考虑两条椭圆曲线

$$E_i : y^2 = x(x-a_i)(x+b_i), \quad c_i = -a_i - b_i, \quad i = 1, 2.$$

- 由于作为 $G_{\mathbb{Q}}$ 模, $E_1[2] \cong E_2[2]$, 因此二者的 2-Selmer 群落在同一个群 $\mathrm{H}^1(G_{\mathbb{Q}}, E_i[2])$ 中.
- 由于技术上的原因, 我们进一步假设有 $G_{\mathbb{Q}}$ 模同构 $E_1[4] \cong E_2[4]$.
- 此时有

$$a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}.$$

记号

- 现在我们考虑两条椭圆曲线

$$E_i : y^2 = x(x-a_i)(x+b_i), \quad c_i = -a_i - b_i, \quad i = 1, 2.$$

- 由于作为 $G_{\mathbb{Q}}$ 模, $E_1[2] \cong E_2[2]$, 因此二者的 2-Selmer 群落在同一个群 $\mathrm{H}^1(G_{\mathbb{Q}}, E_i[2])$ 中.
- 由于技术上的原因, 我们进一步假设有 $G_{\mathbb{Q}}$ 模同构 $E_1[4] \cong E_2[4]$.
- 此时有

$$a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}.$$

- 不失一般性, 我们假设

$$a_2 = a_1 A^2, \quad b_2 = b_1 B^2, \quad c_2 = c_1 C^2$$

且 $\gcd(A, B, C) = 1$.

主要结论

定理

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.
- 如果下述三种情形之一成立:

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.
- 如果下述三种情形之一成立:
  - n 的素因子都模 8 余 1, 且 $E_i^{(n)}$ 没有 4 阶有理点;

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.
- 如果下述三种情形之一成立:
  - n 的素因子都模 8 余 1, 且 $E_i^{(n)}$ 没有 4 阶有理点;
  - a_i, b_i 是奇数且 $2 \parallel c_i$; (例如 $y^2 = x(x-1)(x+1)$)

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.
- 如果下述三种情形之一成立:
  - n 的素因子都模 8 余 1, 且 $E_i^{(n)}$ 没有 4 阶有理点;
  - a_i, b_i 是奇数且 $2 \parallel c_i$; *(例如 $y^2 = x(x-1)(x+1)$)*
  - $2 \parallel a_i, b_i, 4 \mid c_i$, 且 $E_i^{(n)}$ 没有 4 阶有理点, *(例如 $y^2 = x(x-2)(x+2)$)*

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.
- 如果下述三种情形之一成立:
  - n 的素因子都模 8 余 1, 且 $E_i^{(n)}$ 没有 4 阶有理点;
  - a_i, b_i 是奇数且 $2 \parallel c_i$; (例如 $y^2 = x(x-1)(x+1)$)
  - $2 \parallel a_i, b_i, 4 \mid c_i$, 且 $E_i^{(n)}$ 没有 4 阶有理点, (例如 $y^2 = x(x-2)(x+2)$)
- 则 $\mathrm{Sel}_2\left(E_1^{(n)}/\mathbb{Q}\right) \cong \mathrm{Sel}_2\left(E_2^{(n)}/\mathbb{Q}\right)$,

主要结论

定理

- 假设 E_i 没有 4 阶有理点且 $\mathrm{Sel}_2(E_i/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ 达到最小.
- 假设 n 与 $a_1b_1c_1a_2b_2c_2$ 互素且对任意奇素数 $p \mid n, q \mid a_1b_1c_1a_2b_2c_2$, 有 $\left(\frac{p}{q}\right) = 1$.
- 如果下述三种情形之一成立:
  - n 的素因子都模 8 余 1, 且 $E_i^{(n)}$ 没有 4 阶有理点;
  - a_i, b_i 是奇数且 $2 \parallel c_i$; (例如 $y^2 = x(x-1)(x+1)$)
  - $2 \parallel a_i, b_i, 4 \mid c_i$, 且 $E_i^{(n)}$ 没有 4 阶有理点, (例如 $y^2 = x(x-2)(x+2)$)
- 则 $\mathrm{Sel}_2\left(E_1^{(n)}/\mathbb{Q}\right) \cong \mathrm{Sel}_2\left(E_2^{(n)}/\mathbb{Q}\right)$, 且下述等价
  - $\mathrm{rank}_{\mathbb{Z}}\, E_1^{(n)}(\mathbb{Q}) = 0, Ш\left(E_1^{(n)}/\mathbb{Q}\right)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;
  - $\mathrm{rank}_{\mathbb{Z}}\, E_2^{(n)}(\mathbb{Q}) = 0, Ш\left(E_2^{(n)}/\mathbb{Q}\right)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$.

证明方法

- 证明所使用的方法仍然是传统的 2-下降法.

- 证明所使用的方法仍然是传统的 2-下降法.
- 由于我们假设 E 没有 4 阶有理点, 因此由正合列

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

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

证明方法

- 证明所使用的方法仍然是传统的 2-下降法.
- 由于我们假设 E 没有 4 阶有理点, 因此由正合列

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

  可知 $E[2] \subseteq \mathrm{Sel}_2(E)$.
- 由于 $\mathrm{Sel}_2(E)$ 通过一些局部条件刻画, 通过比较 E_i 和 $E_i^{(n)}$ 的这些局部条件, 可以得到 Sel_2 相等.

证明方法

- 证明所使用的方法仍然是传统的 2-下降法.
- 由于我们假设 E 没有 4 阶有理点, 因此由正合列

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

  可知 $E[2] \subseteq \mathrm{Sel}_2(E)$.
- 由于 $\mathrm{Sel}_2(E)$ 通过一些局部条件刻画, 通过比较 E_i 和 $E_i^{(n)}$ 的这些局部条件, 可以得到 Sel_2 相等.
- 然后再通过计算可知二者的 Cassels 配对也是相同的, 从而可以得到我们的结论.

计算 Selmer 群

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

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

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

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

- 其中齐性空间

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

计算 Selmer 群

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

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

- 其中齐性空间

$$D_\Lambda = \begin{cases} H_1: & at^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ H_2: & bt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ H_3: & ct^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases}$$

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

$$(1,1,1),\ (-c,-ac,a),\ (-bc,c,-b),\ (b,-a,-ab).$$

- 记 $D_\Lambda^{(n)}$ 为 $E^{(n)}$ 的齐性空间.

- 记 $D_\Lambda^{(n)}$ 为 $E^{(n)}$ 的齐性空间.
- **情形 $\boldsymbol{p \nmid abcn}$.** 此时 $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \iff p \nmid d_1 d_2 d_3$.

计算 Selmer 群: 分情形讨论

- 记 $D_\Lambda^{(n)}$ 为 $E^{(n)}$ 的齐性空间.
- **情形 $\boldsymbol{p \nmid abcn}$.** 此时 $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \iff p \nmid d_1 d_2 d_3$.
- 故可不妨设 $d_i \mid abcn$ 且无平方因子.

- 记 $D_\Lambda^{(n)}$ 为 $E^{(n)}$ 的齐性空间.
- **情形 $\boldsymbol{p \nmid abcn}$.** 此时 $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \iff p \nmid d_1 d_2 d_3$.
- 故可不妨设 $d_i \mid abcn$ 且无平方因子.
- **情形 $\boldsymbol{p = \infty}$.** 容易证明

$$D_\Lambda^{(n)}(\mathbb{R}) \neq \emptyset \iff \begin{cases} d_1 > 0, & \text{若 } b > 0, c < 0; \\ d_2 > 0, & \text{若 } c > 0, a < 0; \\ d_3 > 0, & \text{若 } a > 0, b < 0. \end{cases}$$

- **情形 $\boldsymbol{p \mid n}$.** 此时 $p \nmid abc$. $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \iff$

$$\begin{cases} \left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) = 1, & \text{若 } p \nmid d_1d_2d_3; \\ \left(\frac{-bcd_1}{p}\right) = \left(\frac{cn/d_2}{p}\right) = \left(\frac{bn/d_3}{p}\right) = 1, & \text{若 } p \nmid d_1, p \mid d_2, p \mid d_3; \\ \left(\frac{-cn/d_1}{p}\right) = \left(\frac{-acd_2}{p}\right) = \left(\frac{-an/d_3}{p}\right) = 1, & \text{若 } p \mid d_1, p \nmid d_2, p \mid d_3; \\ \left(\frac{bn/d_1}{p}\right) = \left(\frac{-an/d_2}{p}\right) = \left(\frac{-abd_3}{p}\right) = 1, & \text{若 } p \mid d_1, p \mid d_2, p \nmid d_3. \end{cases}$$

- **情形 $p \mid n$.** 此时 $p \nmid abc$. $D_\Lambda^{(n)}(\mathbb{Q}_p) \neq \emptyset \iff$

$$\begin{cases} \left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \left(\frac{d_3}{p}\right) = 1, & \text{若 } p \nmid d_1d_2d_3; \\ \left(\frac{-bcd_1}{p}\right) = \left(\frac{cn/d_2}{p}\right) = \left(\frac{bn/d_3}{p}\right) = 1, & \text{若 } p \nmid d_1, p \mid d_2, p \mid d_3; \\ \left(\frac{-cn/d_1}{p}\right) = \left(\frac{-acd_2}{p}\right) = \left(\frac{-an/d_3}{p}\right) = 1, & \text{若 } p \mid d_1, p \nmid d_2, p \mid d_3; \\ \left(\frac{bn/d_1}{p}\right) = \left(\frac{-an/d_2}{p}\right) = \left(\frac{-abd_3}{p}\right) = 1, & \text{若 } p \mid d_1, p \mid d_2, p \nmid d_3. \end{cases}$$

- 第一种情形由希尔伯特符号容易得到, 后面的情形可以通过对 Λ 加上一个 $E[2]$ 对应的齐性空间化为第一种情形.

计算 Selmer 群: 分离含 n 的部分

- 设

$$n = p_1 \cdots p_k,$$

$$d_1 = p_1^{x_1} \cdots p_k^{x_k} \cdot \widetilde{d}_1, \quad x_i = v_{p_i}(d_1),$$

$$d_2 = p_1^{y_1} \cdots p_k^{y_k} \cdot \widetilde{d}_2, \quad y_i = v_{p_i}(d_2),$$

$$d_3 = p_1^{z_1} \cdots p_k^{z_k} \cdot \widetilde{d}_3, \quad z_i = v_{p_i}(d_3),$$

其中 $\widetilde{d}_i \mid abc$ 且无平方因子, 则 $\widetilde{d}_1\widetilde{d}_2\widetilde{d}_3 \in \mathbb{Q}^{\times 2}$.

计算 Selmer 群: 分离含 n 的部分

- 设

$$n = p_1 \cdots p_k,$$

$$d_1 = p_1^{x_1} \cdots p_k^{x_k} \cdot \widetilde{d}_1, \quad x_i = v_{p_i}(d_1),$$
$$d_2 = p_1^{y_1} \cdots p_k^{y_k} \cdot \widetilde{d}_2, \quad y_i = v_{p_i}(d_2),$$
$$d_3 = p_1^{z_1} \cdots p_k^{z_k} \cdot \widetilde{d}_3, \quad z_i = v_{p_i}(d_3),$$

其中 $\widetilde{d}_i \mid abc$ 且无平方因子, 则 $\widetilde{d}_1\widetilde{d}_2\widetilde{d}_3 \in \mathbb{Q}^{\times 2}$.

- 设

$$\mathbf{x} = (x_1, \ldots, x_k)^{\mathrm{T}}, \ \mathbf{y} = (y_1, \ldots, y_k)^{\mathrm{T}}, \ \mathbf{z} = (z_1, \ldots, z_k)^{\mathrm{T}} \in \mathbb{F}_2^k,$$

则 $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$.

计算 Selmer 群: 比较 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 和 $\mathrm{Sel}_2'(E)$

- 假设 n 素因子均模 8 余 1.

计算 Selmer 群: 比较 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 和 $\mathrm{Sel}_2'(E)$

- 假设 n 素因子均模 8 余 1.
- 设 $\widetilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_p)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_p)$ 的可解性.

计算 Selmer 群: 比较 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 和 $\mathrm{Sel}_2'(E)$

- 假设 n 素因子均模 8 余 1.
- 设 $\widetilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_p)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_p)$ 的可解性.
- $\boldsymbol{p = \infty}$. 由 d_i 和 $\tilde{d}_i$ 符号相同可知二者可解性相同.

计算 Selmer 群: 比较 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 和 $\mathrm{Sel}_2'(E)$

- 假设 n 素因子均模 8 余 1.
- 设 $\widetilde{\Lambda} = (\widetilde{d}_1, \widetilde{d}_2, \widetilde{d}_3)$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_p)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_p)$ 的可解性.
- $\boldsymbol{p = \infty}$. 由 d_i 和 $\widetilde{d}_i$ 符号相同可知二者可解性相同.
- $\boldsymbol{p \mid abc}$. 由 $n, d_i/\widetilde{d}_i \in \mathbb{Q}_p^{\times 2}$ 可知二者可解性相同.

计算 Selmer 群: 比较 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 和 $\mathrm{Sel}_2'(E)$

- 假设 n 素因子均模 8 余 1.
- 设 $\widetilde{\Lambda}=(\widetilde{d}_1,\widetilde{d}_2,\widetilde{d}_3)$. 我们对比 $D_\Lambda^{(n)}(\mathbb{Q}_p)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_p)$ 的可解性.
- $\boldsymbol{p=\infty}$. 由 d_i 和 $\widetilde{d}_i$ 符号相同可知二者可解性相同.
- $\boldsymbol{p\mid abc}$. 由 $n, d_i/\widetilde{d}_i\in\mathbb{Q}_p^{\times 2}$ 可知二者可解性相同.
- 如果 $\Lambda\in\mathrm{Sel}_2\left(E^{(n)}\right)$, 则 $\widetilde{\Lambda}\in\mathrm{Sel}_2(E)=E[2]$.

计算 Selmer 群: 比较 $\mathrm{Sel}_2'\left(E^{(n)}\right)$ 和 $\mathrm{Sel}_2'(E)$

- 假设 n 素因子均模 8 余 1.
- 设 $\widetilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_p)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_p)$ 的可解性.
- $\boldsymbol{p = \infty}$. 由 d_i 和 $\tilde{d}_i$ 符号相同可知二者可解性相同.
- $\boldsymbol{p \mid abc}$. 由 $n, d_i/\tilde{d}_i \in \mathbb{Q}_p^{\times 2}$ 可知二者可解性相同.
- 如果 $\Lambda \in \mathrm{Sel}_2\left(E^{(n)}\right)$, 则 $\widetilde{\Lambda} \in \mathrm{Sel}_2(E) = E[2]$.
- 如果 $\widetilde{\Lambda} = (-c, -ac, a)$, 则

$$\Lambda \cdot (-cn, -ac, an) = \left(\prod_{i=1}^{k} p_i^{1-x_i}, \prod_{i=1}^{k} p_i^{y_i}, \prod_{i=1}^{k} p_i^{1-z_i}\right).$$

其它情形也类似.

- 假设 n 素因子均模 8 余 1.
- 设 $\widetilde{\Lambda}=(\widetilde{d}_1,\widetilde{d}_2,\widetilde{d}_3)$. 我们对比 $D_{\Lambda}^{(n)}(\mathbb{Q}_p)$ 和 $D_{\widetilde{\Lambda}}^{(1)}(\mathbb{Q}_p)$ 的可解性.
- $\boldsymbol{p=\infty}$. 由 d_i 和 $\widetilde{d}_i$ 符号相同可知二者可解性相同.
- $\boldsymbol{p\mid abc}$. 由 $n, d_i/\widetilde{d}_i\in\mathbb{Q}_p^{\times 2}$ 可知二者可解性相同.
- 如果 $\Lambda\in\mathrm{Sel}_2\left(E^{(n)}\right)$, 则 $\widetilde{\Lambda}\in\mathrm{Sel}_2(E)=E[2]$.
- 如果 $\widetilde{\Lambda}=(-c,-ac,a)$, 则

$$\Lambda\cdot(-cn,-ac,an)=\left(\prod_{i=1}^{k}p_i^{1-x_i},\prod_{i=1}^{k}p_i^{y_i},\prod_{i=1}^{k}p_i^{1-z_i}\right).$$

其它情形也类似. 因此

$$\mathrm{Sel}_2'\left(E^{(n)}\right)=\mathrm{Sel}_2\left(E^{(n)}\right)/E[2]$$

中每个元素都有唯一代表元 (d_1,d_2,d_3) 满足 $0<d_i\mid n$.

计算 Selmer 群: 得到 $\mathrm{Sel}_2'\left(E_i^{(n)}\right)$

- $\boldsymbol{p \mid n}$.

- $\boldsymbol{p \mid n}$. 由于 $a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}$, 因此 $\Lambda = (d_1, d_2, d_3)$ 对应的 E_1, E_2 的齐性空间在 $\mathbb{Q}_p$ 的可解性相同.

计算 Selmer 群: 得到 $\mathrm{Sel}_2'\left(E_i^{(n)}\right)$

- $\boldsymbol{p \mid n}$. 由于 $a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}$, 因此 $\Lambda = (d_1, d_2, d_3)$ 对应的 E_1, E_2 的齐性空间在 $\mathbb{Q}_p$ 的可解性相同. 从而

$$\mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right).$$

计算 Selmer 群: 得到 $\mathrm{Sel}_2'\left(E_i^{(n)}\right)$

- $\boldsymbol{p \mid n}$. 由于 $a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}$, 因此 $\Lambda = (d_1, d_2, d_3)$ 对应的 E_1, E_2 的齐性空间在 $\mathbb{Q}_p$ 的可解性相同. 从而

$$\mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right).$$

- 若用矩阵语言来表达则是:

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

- $\boldsymbol{p \mid n}$. 由于 $a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}$, 因此 $\Lambda = (d_1, d_2, d_3)$ 对应的 E_1, E_2 的齐性空间在 $\mathbb{Q}_p$ 的可解性相同. 从而

$$\mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right).$$

- 若用矩阵语言来表达则是:

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

- 这个矩阵便是 Monsky 矩阵, 其中

$$\mathbf{A} = \left([p_j, -n]_{p_i}\right)_{i,j}, \qquad \mathbf{D}_u = \mathrm{diag}\left(\left[\frac{u}{p_1}\right], \ldots, \left[\frac{u}{p_k}\right]\right) \in M_k(\mathbb{F}_2),$$

计算 Selmer 群: 得到 $\mathrm{Sel}_2'\left(E_i^{(n)}\right)$

- $\boldsymbol{p} \mid \boldsymbol{n}$. 由于 $a_1/a_2, b_1/b_2, c_1/c_2 \in \mathbb{Q}^{\times 2}$, 因此 $\Lambda = (d_1, d_2, d_3)$ 对应的 E_1, E_2 的齐性空间在 $\mathbb{Q}_p$ 的可解性相同. 从而
$$\mathrm{Sel}_2'\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2'\left(E_2^{(n)}\right).$$
- 若用矩阵语言来表达则是:
$$\mathrm{Sel}_2'\left(E^{(n)}\right) \xrightarrow{\sim} \mathrm{Ker}\begin{pmatrix} \mathbf{A} + \mathbf{D}_{-c} & \mathbf{D}_{-bc} \\ \mathbf{D}_{-ac} & \mathbf{A} + \mathbf{D}_{c} \end{pmatrix}$$
$$(d_1, d_2, d_3) \mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix},$$
- 这个矩阵便是 Monsky 矩阵, 其中
$$\mathbf{A} = \left([p_j, -n]_{p_i}\right)_{i,j}, \qquad \mathbf{D}_u = \mathrm{diag}\left(\left[\frac{u}{p_1}\right], \ldots, \left[\frac{u}{p_k}\right]\right) \in M_k(\mathbb{F}_2),$$
- $[\cdot,\cdot]$ 是加性希尔伯特符号, $\left[\frac{\cdot}{\cdot}\right]$ 是加性勒让德符号.

计算 Cassels 配对

- Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2'(E)$ 上定义了一个反对称双线性型.

- Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2'(E)$ 上定义了一个反对称双线性型.
- 对于 Λ, Λ', 选择

$$P = (P_v)_v \in D_\Lambda(\mathbb{A}_\mathbb{Q}), \qquad Q_i \in H_i(\mathbb{Q}).$$

计算 Cassels 配对

- Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2'(E)$ 上定义了一个反对称双线性型.
- 对于 Λ, Λ', 选择

$$P = (P_v)_v \in D_\Lambda(\mathbb{A}_\mathbb{Q}), \qquad Q_i \in H_i(\mathbb{Q}).$$

- 令 L_i 为定义了 H_i 在 Q_i 处切平面的线性型, 定义

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

- Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2'(E)$ 上定义了一个反对称双线性型.
- 对于 Λ, Λ', 选择

$$P = (P_v)_v \in D_\Lambda(\mathbb{A}_\mathbb{Q}), \qquad Q_i \in H_i(\mathbb{Q}).$$

- 令 L_i 为定义了 H_i 在 Q_i 处切平面的线性型, 定义

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

- 它不依赖 P 和 Q_i 的选取.

计算 Cassels 配对

- Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2'(E)$ 上定义了一个反对称双线性型.
- 对于 Λ, Λ', 选择

$$P = (P_v)_v \in D_\Lambda(\mathbb{A}_\mathbb{Q}), \qquad Q_i \in H_i(\mathbb{Q}).$$

- 令 L_i 为定义了 H_i 在 Q_i 处切平面的线性型, 定义

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

- 它不依赖 P 和 Q_i 的选取.

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

计算 Cassels 配对: 约化到 Cassels 配对非退化

- 由正合列

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

计算 Cassels 配对: 约化到 Cassels 配对非退化

- 由正合列

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

- 得到长正合列

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

计算 Cassels 配对: 约化到 Cassels 配对非退化

- 由正合列

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

- 得到长正合列

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

- 注意到 Cassels 配对的核是 $\dfrac{\mathrm{Im}\,\mathrm{Sel}_4(E)}{E[2]}$.

- 由正合列
$$0 \to E[2] \to E[4] \xrightarrow{\times 2} E[2] \to 0$$
- 得到长正合列
$$0 \to \frac{E(\mathbb{Q})[2]}{2E(\mathbb{Q})[4]} \to \mathrm{Sel}_2(E) \to \mathrm{Sel}_4(E) \to \mathrm{Im}\,\mathrm{Sel}_4(E) \to 0.$$
- 注意到 Cassels 配对的核是 $\dfrac{\mathrm{Im}\,\mathrm{Sel}_4(E)}{E[2]}$.
- 因此 Cassels 配对非退化等价于
$$\mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q}) = 0, \quad Ш(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}.$$

- 由我们的假设,

$$a_2 = a_1 A^2, \quad b_2 = b_1 B^2, \quad c_2 = c_1 C^2,$$

其中 A, B, C 是互素的非零奇数.

- 由我们的假设,

$$a_2 = a_1 A^2, \quad b_2 = b_1 B^2, \quad c_2 = c_1 C^2,$$

  其中 A, B, C 是互素的非零奇数.
- 设 $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3')$.

- 由我们的假设,

$$a_2 = a_1 A^2, \quad b_2 = b_1 B^2, \quad c_2 = c_1 C^2,$$

其中 A, B, C 是互素的非零奇数.

- 设 $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3')$.
- 若能选取适当的 $Q_{i,j}$ 和 $P_{i,v}$, 使得

$$\color{red}{[L_{1,i}(P_{1,v}), d_i']_v} = \color{blue}{[L_{2,i}(P_{2,v}), d_i']_v},$$

则 E_1, E_2 对应的 Cassels 配对就相同了.

- 由我们的假设,

$$a_2 = a_1 A^2, \quad b_2 = b_1 B^2, \quad c_2 = c_1 C^2,$$

  其中 A, B, C 是互素的非零奇数.
- 设 $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3')$.
- 若能选取适当的 $Q_{i,j}$ 和 $P_{i,v}$, 使得

$$\color{red}{[L_{1,i}(P_{1,v}), d_i']_v} = \color{blue}{[L_{2,i}(P_{2,v}), d_i']_v},$$

  则 E_1, E_2 对应的 Cassels 配对就相同了.
- 在多数情形这不难证明, 我们仅说明相对复杂的一种情形.

- 由我们的假设,

$$a_2 = a_1 A^2, \quad b_2 = b_1 B^2, \quad c_2 = c_1 C^2,$$

  其中 A, B, C 是互素的非零奇数.
- 设 $\Lambda = (d_1, d_2, d_3), \Lambda' = (d_1', d_2', d_3')$.
- 若能选取适当的 $Q_{i,j}$ 和 $P_{i,v}$, 使得

$$[L_{1,i}(P_{1,v}), d_i']_v = [L_{2,i}(P_{2,v}), d_i']_v,$$

  则 E_1, E_2 对应的 Cassels 配对就相同了.
- 在多数情形这不难证明, 我们仅说明相对复杂的一种情形.
- 不妨设 $A \equiv B \equiv C \equiv 1 \bmod 4$.

计算 Cassels 配对: 比较局部符号 (续)

- $p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$.

计算 Cassels 配对: 比较局部符号 (续)

- $\boldsymbol{p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3}$. 设

$$Q_{1,1} = (\alpha, \beta, \gamma) \in H_{1,1}(\mathbb{Q}), \quad Q_{2,1} = (\alpha, A\beta, A\gamma) \in H_{2,1}(\mathbb{Q}).$$

$$P_{1,p} = (1, 0, u, v), \quad L_{1,1}(P_{1,p}) = a_1 n\alpha - d_3\gamma v + d_2\beta u,$$

$$P_{2,p} = (1, 0, Cu, Bv), \quad L_{2,1}(P_{2,p}) = Aa_1 n\alpha - Bd_3\gamma v + Cd_2\beta u,$$

计算 Cassels 配对: 比较局部符号 (续)

- $p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$. 设

$$Q_{1,1} = (\alpha, \beta, \gamma) \in H_{1,1}(\mathbb{Q}), \quad Q_{2,1} = (\alpha, A\beta, A\gamma) \in H_{2,1}(\mathbb{Q}).$$

$$P_{1,p} = (1, 0, u, v), \quad L_{1,1}(P_{1,p}) = a_1 n\alpha - d_3\gamma v + d_2\beta u,$$

$$P_{2,p} = (1, 0, Cu, Bv), \quad L_{2,1}(P_{2,p}) = Aa_1 n\alpha - Bd_3\gamma v + Cd_2\beta u,$$

$$L_{1,1}(P_{1,p})L_{2,1}(P_{2,p}) = \frac{(A+B)(B+C)(C+A)}{2}\left(\frac{a_1 n\alpha}{b+c} + \frac{d_2\beta u}{a+b} - \frac{d_3\gamma v}{a+c}\right)^2.$$

计算 Cassels 配对: 比较局部符号 (续)

- $\boldsymbol{p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3}$. 设

$$Q_{1,1} = (\alpha, \beta, \gamma) \in H_{1,1}(\mathbb{Q}), \quad Q_{2,1} = (\alpha, A\beta, A\gamma) \in H_{2,1}(\mathbb{Q}).$$

$$P_{1,p} = (1, 0, u, v), \quad L_{1,1}(P_{1,p}) = a_1 n\alpha - d_3\gamma v + d_2\beta u,$$

$$P_{2,p} = (1, 0, Cu, Bv), \quad L_{2,1}(P_{2,p}) = Aa_1 n\alpha - Bd_3\gamma v + Cd_2\beta u,$$

$$L_{1,1}(P_{1,p})L_{2,1}(P_{2,p}) = \tfrac{(A+B)(B+C)(C+A)}{2}\left(\frac{a_1 n\alpha}{b+c} + \frac{d_2\beta u}{a+b} - \frac{d_3\gamma v}{a+c}\right)^2.$$

- 这里需要用到 $a_1A^2 + b_1B^2 + c_1C^2 = 0$.

计算 Cassels 配对: 比较局部符号 (续)

- $\boldsymbol{p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3}$. 设

$$Q_{1,1} = (\alpha, \beta, \gamma) \in H_{1,1}(\mathbb{Q}), \quad Q_{2,1} = (\alpha, A\beta, A\gamma) \in H_{2,1}(\mathbb{Q}).$$

$$P_{1,p} = (1, 0, u, v), \quad L_{1,1}(P_{1,p}) = a_1 n\alpha - d_3\gamma v + d_2\beta u,$$

$$P_{2,p} = (1, 0, Cu, Bv), \quad L_{2,1}(P_{2,p}) = Aa_1 n\alpha - Bd_3\gamma v + Cd_2\beta u,$$

$$L_{1,1}(P_{1,p})L_{2,1}(P_{2,p}) = \tfrac{(A+B)(B+C)(C+A)}{2}\left(\frac{a_1 n\alpha}{b+c} + \frac{d_2\beta u}{a+b} - \frac{d_3\gamma v}{a+c}\right)^2.$$

- 这里需要用到 $a_1A^2 + b_1B^2 + c_1C^2 = 0$.

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.

计算 Cassels 配对: 其它情形

- 对于一些特殊的 (a, b, c), 我们不需要 $p \equiv 1 \bmod 8, \forall p \mid n$ 这么强的条件.

- 对于一些特殊的 (a,b,c), 我们不需要 $p\equiv 1 \bmod 8, \forall p \mid n$ 这么强的条件.
- 例如 $2\nmid a_i, b_i, 2\parallel c_i$ (如奇数同余椭圆曲线情形).

计算 Cassels 配对: 其它情形

- 对于一些特殊的 (a,b,c), 我们不需要 $p \equiv 1 \bmod 8, \forall p \mid n$ 这么强的条件.
- 例如 $2 \nmid a_i, b_i, 2 \parallel c_i$ (如奇数同余椭圆曲线情形).
- 此时需要对 $p = 2$ 情形进行单独处理, 最后也可以得到该结论.

计算 Cassels 配对: 其它情形

- 对于一些特殊的 (a, b, c), 我们不需要 $p \equiv 1 \bmod 8, \forall p \mid n$ 这么强的条件.
- 例如 $2 \nmid a_i, b_i, 2 \parallel c_i$ (如奇数同余椭圆曲线情形).
- 此时需要对 $p = 2$ 情形进行单独处理, 最后也可以得到该结论.
- 例如 $2 \parallel a_i, b_i, 4 \mid c_i$ (如偶数同余椭圆曲线情形).

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

- 对于一般的椭圆曲线 $E_1, E_2/\mathbb{Q}$, 假设有 Galois 模同构 $E_1[4] \cong E_2[4]$.

- 对于一般的椭圆曲线 $E_1, E_2/\mathbb{Q}$, 假设有 Galois 模同构 $E_1[4] \cong E_2[4]$.
- 设 n 是无平方因子正整数且对于 E_1 或 E_2 的每个坏约化 v, 均有 $n \in \mathbb{Q}_v^{\times 2}$.

进一步的思考

- 对于一般的椭圆曲线 $E_1, E_2/\mathbb{Q}$, 假设有 Galois 模同构 $E_1[4] \cong E_2[4]$.
- 设 n 是无平方因子正整数且对于 E_1 或 E_2 的每个坏约化 v, 均有 $n \in \mathbb{Q}_v^{\times 2}$.
- 我们需要什么样的条件能够推出

$$\mathrm{Sel}_2\left(E_1^{(n)}\right) \cong \mathrm{Sel}_2\left(E_2^{(n)}\right),$$

$$\mathrm{rank}_{\mathbb{Z}}\, E_1^{(n)}(\mathbb{Q}) = \mathrm{rank}_{\mathbb{Z}}\, E_2^{(n)}(\mathbb{Q})?$$

感谢各位的倾听!