

# 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

- 给一个数域上的椭圆曲线  $E/K$ , 我们关心它的二次扭族

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

的各种算术量: Mordell-Weil 秩、 $\text{III}$  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

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

对任意  $\chi$  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

$$\text{rank}(A_1/F) = \text{rank}(A_2/F),$$

那么  $A_1$  和  $A_2$  是否一定同源?

- 给一个数域上的椭圆曲线  $E/K$ , 我们关心它的二次扭族

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

的各种算术量: Mordell-Weil 秩、 $\text{III}$  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

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

对任意  $\chi$  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

$$\text{rank}(A_1/F) = \text{rank}(A_2/F),$$

那么  $A_1$  和  $A_2$  是否一定同源?

- 给一个数域上的椭圆曲线  $E/K$ , 我们关心它的二次扭族

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

的各种算术量: Mordell-Weil 秩、III 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

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

对任意  $\chi$  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

$$\text{rank}(A_1/F) = \text{rank}(A_2/F),$$

那么  $A_1$  和  $A_2$  是否一定同源?

- 给一个数域上的椭圆曲线  $E/K$ , 我们关心它的二次扭族

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

的各种算术量: Mordell-Weil 秩、III 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

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

对任意  $\chi$  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

$$\text{rank}(A_1/F) = \text{rank}(A_2/F),$$

那么  $A_1$  和  $A_2$  是否一定同源?

- 给一个数域上的椭圆曲线  $E/K$ , 我们关心它的二次扭族

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

的各种算术量: Mordell-Weil 秩、III 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

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

对任意  $\chi$  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

$$\text{rank}(A_1/F) = \text{rank}(A_2/F),$$

那么  $A_1$  和  $A_2$  是否一定同源?

- 给一个数域上的椭圆曲线  $E/K$ , 我们关心它的二次扭族

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

的各种算术量: Mordell-Weil 秩、III 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

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

对任意  $\chi$  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

$$\text{rank}(A_1/F) = \text{rank}(A_2/F),$$

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. 给定数域上椭圆曲线  $E_1, E_2/K$ , 如果有

- $G_K$  模同构  $E_1[m] \cong E_2[m], m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$

- 相同的potential乘性约化素位集合  $S$
- $\forall l \in S, (E_1[m]/K_l)^\circ \cong (E_2[m]/K_l)^\circ$
- 一个分歧条件

则  $\text{Sel}_{p^k}(E_1/F) \cong \text{Sel}_{p^k}(E_2/F), \forall F/K$ . 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  $\text{Sel}_p(E_1/F) \cong \text{Sel}_p(E_2/F)$  对所有的  $F/K$  和几乎所有  $p$  成立, 那么  $E_1$  和  $E_2$  确实同源.



- 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  $E_1[m] \cong E_2[m], m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$

- 相同的potential乘性约化素位集合  $S$
- $\forall l \in S, (E_1[l]/K_l)^\circ \cong (E_2[l]/K_l)^\circ$
- 一个分歧条件

则  $\text{Sel}_{p^k}(E_1/F) \cong \text{Sel}_{p^k}(E_2/F), \forall F/K$ . 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  $\text{Sel}_p(E_1/F) \cong \text{Sel}_p(E_2/F)$  对所有的  $F/K$  和几乎所有  $p$  成立, 那么  $E_1$  和  $E_2$  确实同源.

- 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  $E_1[m] \cong E_2[m], m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$

- 相同的potential乘性约化素位集合  $S$
- $\forall I \in S, (E_1[m]/K_I)^\circ \cong (E_2[m]/K_I)^\circ$
- 一个分歧条件

则  $\text{Sel}_{p^k}(E_1/F) \cong \text{Sel}_{p^k}(E_2/F), \forall F/K$ . 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  $\text{Sel}_p(E_1/F) \cong \text{Sel}_p(E_2/F)$  对所有的  $F/K$  和几乎所有  $p$  成立, 那么  $E_1$  和  $E_2$  确实同源.

- 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  $E_1[m] \cong E_2[m], m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$

- 相同的potential乘性约化素位集合  $S$
- $\forall l \in S, (E_1[l]/K_l)^\circ \cong (E_2[l]/K_l)^\circ$
- 一个分歧条件

则  $\text{Sel}_{p^k}(E_1/F) \cong \text{Sel}_{p^k}(E_2/F), \forall F/K$ . 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  $\text{Sel}_p(E_1/F) \cong \text{Sel}_p(E_2/F)$  对所有的  $F/K$  和几乎所有  $p$  成立, 那么  $E_1$  和  $E_2$  确实同源.

- 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  $E_1[m] \cong E_2[m], m = \begin{cases} p^{k+1}, & p \leq 3 \\ p^k, & p > 3 \end{cases}$

- 相同的potential乘性约化素位集合  $S$
- $\forall l \in S, (E_1[l]/K_l)^\circ \cong (E_2[l]/K_l)^\circ$
- 一个分歧条件

则  $\text{Sel}_{p^k}(E_1/F) \cong \text{Sel}_{p^k}(E_2/F), \forall F/K$ . 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  $\text{Sel}_p(E_1/F) \cong \text{Sel}_p(E_2/F)$  对所有的  $F/K$  和几乎所有  $p$  成立, 那么  $E_1$  和  $E_2$  确实同源.

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

$$E_1: y^2 = x(x - e_1)(x + e_2), E_2: y^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 + e_2 + e_3 = 0, e_1 a^2 + e_2 b^2 + e_3 c^2 = 0, 2 \nmid abc$ .

- 此时  $E_1[4] \cong E_2[4]$ .
- 假设  $n$  与  $2e_1 e_2 e_3 abc$  互素, 且对任意奇素数  $p \mid n, q \mid e_1 e_2 e_3 abc$ , 有  $\left(\frac{p}{q}\right) = 1$ .
- 假设  $\text{Sel}_2(E_1/\mathbb{Q}) \cong \text{Sel}_2(E_2/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$  是最小的.

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

$$E_1: y^2 = x(x - e_1)(x + e_2), E_2: y^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 + e_2 + e_3 = 0, e_1 a^2 + e_2 b^2 + e_3 c^2 = 0, 2 \nmid abc$ .

- 此时  $E_1[4] \cong E_2[4]$ .
- 假设  $n$  与  $2e_1 e_2 e_3 abc$  互素, 且对任意奇素数  $p \mid n, q \mid e_1 e_2 e_3 abc$ , 有  $\left(\frac{p}{q}\right) = 1$ .
- 假设  $\text{Sel}_2(E_1/\mathbb{Q}) \cong \text{Sel}_2(E_2/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$  是最小的.

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

$$E_1: y^2 = x(x - e_1)(x + e_2), E_2: y^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 + e_2 + e_3 = 0, e_1 a^2 + e_2 b^2 + e_3 c^2 = 0, 2 \nmid abc$ .

- 此时  $E_1[4] \cong E_2[4]$ .
- 假设  $n$  与  $2e_1 e_2 e_3 abc$  互素, 且对任意奇素数  $p \mid n, q \mid e_1 e_2 e_3 abc$ , 有  $\left(\frac{p}{q}\right) = 1$ .
- 假设  $\text{Sel}_2(E_1/\mathbb{Q}) \cong \text{Sel}_2(E_2/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$  是最小的.

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

$$E_1: y^2 = x(x - e_1)(x + e_2), E_2: y^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 + e_2 + e_3 = 0, e_1 a^2 + e_2 b^2 + e_3 c^2 = 0, 2 \nmid abc$ .

- 此时  $E_1[4] \cong E_2[4]$ .
- 假设  $n$  与  $2e_1 e_2 e_3 abc$  互素, 且对任意奇素数  $p \mid n, q \mid e_1 e_2 e_3 abc$ , 有  $\left(\frac{p}{q}\right) = 1$ .
- 假设  $\text{Sel}_2(E_1/\mathbb{Q}) \cong \text{Sel}_2(E_2/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$  是最小的.



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

$$E_1: y^2 = x(x - e_1)(x + e_2), E_2: y^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 + e_2 + e_3 = 0, e_1 a^2 + e_2 b^2 + e_3 c^2 = 0, 2 \nmid abc$ .

- 此时  $E_1[4] \cong E_2[4]$ .
- 假设  $n$  与  $2e_1 e_2 e_3 abc$  互素, 且对任意奇素数  $p \mid n, q \mid e_1 e_2 e_3 abc$ , 有  $\left(\frac{p}{q}\right) = 1$ .
- 假设  $\text{Sel}_2(E_1/\mathbb{Q}) \cong \text{Sel}_2(E_2/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$  是最小的.

- 如果下述三种情况之一成立:
  - $n$  的素因子都模 8 余 1;
  - $e_1, e_2$  是奇数,  $2 \parallel e_3$ ; (例如  $y^2 = x(x-1)(x+1)$ )
  - $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ , 再加一些模 4 余 1 的条件, (例如  $y^2 = x(x-2)(x+2)$ )
- 则  $\text{Sel}_2(E_1^{(n)}/\mathbb{Q}) \cong \text{Sel}_2(E_2^{(n)}/\mathbb{Q})$ , 且下述等价
  - $\text{rank}_{\mathbb{Z}}(E_1^{(n)}/\mathbb{Q}) = 0, \text{III}(E_1^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ ;
  - $\text{rank}_{\mathbb{Z}}(E_2^{(n)}/\mathbb{Q}) = 0, \text{III}(E_2^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ .

- 如果下述三种情况之一成立:
  - $n$  的素因子都模 8 余 1;
  - $e_1, e_2$  是奇数,  $2 \parallel e_3$ ; (例如  $y^2 = x(x-1)(x+1)$ )
  - $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ , 再加一些模 4 余 1 的条件, (例如  $y^2 = x(x-2)(x+2)$ )
- 则  $\text{Sel}_2(E_1^{(n)}/\mathbb{Q}) \cong \text{Sel}_2(E_2^{(n)}/\mathbb{Q})$ , 且下述等价
  - $\text{rank}_{\mathbb{Z}}(E_1^{(n)}/\mathbb{Q}) = 0, \text{III}(E_1^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ ;
  - $\text{rank}_{\mathbb{Z}}(E_2^{(n)}/\mathbb{Q}) = 0, \text{III}(E_2^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ .

- 如果下述三种情况之一成立:
  - $n$  的素因子都模 8 余 1;
  - $e_1, e_2$  是奇数,  $2 \parallel e_3$ ; (例如  $y^2 = x(x-1)(x+1)$ )
  - $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ , 再加一些模 4 余 1 的条件, (例如  $y^2 = x(x-2)(x+2)$ )
- 则  $\text{Sel}_2(E_1^{(n)}/\mathbb{Q}) \cong \text{Sel}_2(E_2^{(n)}/\mathbb{Q})$ , 且下述等价
  - $\text{rank}_{\mathbb{Z}}(E_1^{(n)}/\mathbb{Q}) = 0, \text{III}(E_1^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ ;
  - $\text{rank}_{\mathbb{Z}}(E_2^{(n)}/\mathbb{Q}) = 0, \text{III}(E_2^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ .

- 如果下述三种情况之一成立:
  - $n$  的素因子都模 8 余 1;
  - $e_1, e_2$  是奇数,  $2 \parallel e_3$ ; (例如  $y^2 = x(x-1)(x+1)$ )
  - $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ , 再加一些模 4 余 1 的条件, (例如  $y^2 = x(x-2)(x+2)$ )
- 则  $\text{Sel}_2(E_1^{(n)}/\mathbb{Q}) \cong \text{Sel}_2(E_2^{(n)}/\mathbb{Q})$ , 且下述等价
  - $\text{rank}_{\mathbb{Z}}(E_1^{(n)}/\mathbb{Q}) = 0, \text{III}(E_1^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ ;
  - $\text{rank}_{\mathbb{Z}}(E_2^{(n)}/\mathbb{Q}) = 0, \text{III}(E_2^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ .

- 如果下述三种情况之一成立:
  - $n$  的素因子都模 8 余 1;
  - $e_1, e_2$  是奇数,  $2 \parallel e_3$ ; (例如  $y^2 = x(x-1)(x+1)$ )
  - $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$ , 再加一些模 4 余 1 的条件, (例如  $y^2 = x(x-2)(x+2)$ )
- 则  $\text{Sel}_2(E_1^{(n)}/\mathbb{Q}) \cong \text{Sel}_2(E_2^{(n)}/\mathbb{Q})$ , 且下述等价
  - $\text{rank}_{\mathbb{Z}}(E_1^{(n)}/\mathbb{Q}) = 0, \text{III}(E_1^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ ;
  - $\text{rank}_{\mathbb{Z}}(E_2^{(n)}/\mathbb{Q}) = 0, \text{III}(E_2^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ .

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

$$0 \rightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \rightarrow \text{Sel}_2(E) \rightarrow \text{III}(E/\mathbb{Q})[2] \rightarrow 0$$

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

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

$$0 \rightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \rightarrow \text{Sel}_2(E) \rightarrow \text{III}(E/\mathbb{Q})[2] \rightarrow 0$$

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



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

$$0 \rightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \rightarrow \text{Sel}_2(E) \rightarrow \text{III}(E/\mathbb{Q})[2] \rightarrow 0$$

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

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

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

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

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

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

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

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

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

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

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

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

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

- 情形  $p \nmid 2e_1e_2e_3n$ .

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.

- 情形  $p = \infty$ .

很容易证明  $D_{\Lambda}^{(n)}(\mathbb{R}) \neq \emptyset \Leftrightarrow \begin{cases} d_1 > 0, & \text{若 } e_2 > 0, e_3 < 0; \\ d_2 > 0, & \text{若 } e_3 > 0, e_1 < 0; \\ d_3 > 0, & \text{若 } e_1 > 0, e_2 < 0. \end{cases}$

- 情形  $p \nmid 2e_1e_2e_3n$ .

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.

- 情形  $p = \infty$ .

很容易证明  $D_{\Lambda}^{(n)}(\mathbb{R}) \neq \emptyset \Leftrightarrow \begin{cases} d_1 > 0, & \text{若 } e_2 > 0, e_3 < 0; \\ d_2 > 0, & \text{若 } e_3 > 0, e_1 < 0; \\ d_3 > 0, & \text{若 } e_1 > 0, e_2 < 0. \end{cases}$

- 情形  $p \nmid 2e_1e_2e_3n$ .

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.

- 情形  $p = \infty$ .

很容易证明  $D_{\Lambda}^{(n)}(\mathbb{R}) \neq \emptyset \Leftrightarrow \begin{cases} d_1 > 0, & \text{若 } e_2 > 0, e_3 < 0; \\ d_2 > 0, & \text{若 } e_3 > 0, e_1 < 0; \\ d_3 > 0, & \text{若 } e_1 > 0, e_2 < 0. \end{cases}$

- 情形  $p \mid n (\Rightarrow p \nmid e_1 e_2 e_3)$ .  $D_{\Lambda}^{(n)}(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow$

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

- 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.



- 情形  $p \mid n (\Rightarrow p \nmid e_1 e_2 e_3)$ .  $D_{\Lambda}^{(n)}(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow$

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

- 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.

- 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  $\widetilde{d}_i \mid 2e_1e_2e_3$  且无平方因子.

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

$$\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}, \quad \widetilde{d}_1 \widetilde{d}_2 \widetilde{d}_3 \in \mathbb{Q}^{\times 2}.$$

- 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  $\widetilde{d}_i \mid 2e_1e_2e_3$  且无平方因子.

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

$$\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}, \quad \widetilde{d}_1 \widetilde{d}_2 \widetilde{d}_3 \in \mathbb{Q}^{\times 2}.$$

- 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  $\widetilde{d}_i \mid 2e_1e_2e_3$  且无平方因子.

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

$$\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}, \quad \widetilde{d}_1 \widetilde{d}_2 \widetilde{d}_3 \in \mathbb{Q}^{\times 2}.$$

- 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  $\widetilde{d}_i \mid 2e_1e_2e_3$  且无平方因子.

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

$$\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}, \quad \widetilde{d}_1 \widetilde{d}_2 \widetilde{d}_3 \in \mathbb{Q}^{\times 2}.$$

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对比  $D_{\tilde{\Lambda}}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对比  $D_{\Lambda}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对比  $D_{\Lambda}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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



## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对比  $D_{\tilde{\Lambda}}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对比  $D_{\tilde{\Lambda}}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod 8$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对比  $D_{\tilde{\Lambda}}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对  $D_{\tilde{\Lambda}}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 比较 $\text{Sel}'_2(E^{(n)})$ 与 $\text{Sel}'_2(E)$

- 假设  $n$  素因子均  $\equiv 1 \pmod{8}$ . 设  $\tilde{\Lambda} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$ . 我们对  $D_{\tilde{\Lambda}}^{(n)}(\mathbb{Q}_v)$  和  $D_{\tilde{\Lambda}}^{(1)}(\mathbb{Q}_v)$  的可解性.
- $v = \infty$ . 由  $d_i$  和  $\tilde{d}_i$  符号相同知二者可解性相同.
- $v = q \mid 2e_1e_2e_3$ . 由  $n, d_i/\tilde{d}_i \in \mathbb{Q}_q^{\times 2}$  知二者可解性相同.
- 由于我们假设  $\text{Sel}_2(E) = E[2]$  极小, 故  $\tilde{\Lambda} \in E[2]$ . 如果  $\tilde{\Lambda} = (-e_3, -e_1e_3, e_1)$ , 则

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

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

## 计算 Selmer 群: 得到 $\text{Sel}'_2(E^{(n)})$

- 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

$$\begin{aligned} \text{Sel}'_2(E^{(n)}) &\xrightarrow{\sim} \text{Ker} \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-e_3} & \mathbf{D}_{-e_2 e_3} \\ \mathbf{D}_{-e_1 e_3} & \mathbf{A} + \mathbf{D}_{e_3} \end{pmatrix} \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \end{aligned}$$

- 这个矩阵便是Monsky矩阵, 其中

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

- $[\bullet, \bullet]$  是加性希尔伯特符号,  $\left[ \frac{\bullet}{\bullet} \right]$  是加性勒让德符号.
- 由于  $E_1, E_2$  对应的  $(e_1, e_2, e_3)$  相差平方, 故

$$\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)}).$$

## 计算 Selmer 群: 得到 $\text{Sel}'_2(E^{(n)})$

- 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

$$\begin{aligned} \text{Sel}'_2(E^{(n)}) &\xrightarrow{\sim} \text{Ker} \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-e_3} & \mathbf{D}_{-e_2 e_3} \\ \mathbf{D}_{-e_1 e_3} & \mathbf{A} + \mathbf{D}_{e_3} \end{pmatrix} \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \end{aligned}$$

- 这个矩阵便是Monsky矩阵, 其中

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

- $[\cdot, \cdot]$  是加性希尔伯特符号,  $\left[ \frac{\cdot}{\cdot} \right]$  是加性勒让德符号.
- 由于  $E_1, E_2$  对应的  $(e_1, e_2, e_3)$  相差平方, 故

$$\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)}).$$

## 计算 Selmer 群: 得到 $\text{Sel}'_2(E^{(n)})$

- 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

$$\begin{aligned} \text{Sel}'_2(E^{(n)}) &\xrightarrow{\sim} \text{Ker} \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-e_3} & \mathbf{D}_{-e_2 e_3} \\ \mathbf{D}_{-e_1 e_3} & \mathbf{A} + \mathbf{D}_{e_3} \end{pmatrix} \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \end{aligned}$$

- 这个矩阵便是Monsky矩阵, 其中

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

- $[\bullet, \bullet]$  是加性希尔伯特符号,  $[\frac{\bullet}{\bullet}]$  是加性勒让德符号.
- 由于  $E_1, E_2$  对应的  $(e_1, e_2, e_3)$  相差平方, 故

$$\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)}).$$



## 计算 Selmer 群: 得到 $\text{Sel}'_2(E^{(n)})$

- 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

$$\begin{aligned} \text{Sel}'_2(E^{(n)}) &\xrightarrow{\sim} \text{Ker} \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-e_3} & \mathbf{D}_{-e_2 e_3} \\ \mathbf{D}_{-e_1 e_3} & \mathbf{A} + \mathbf{D}_{e_3} \end{pmatrix} \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \end{aligned}$$

- 这个矩阵便是Monsky矩阵, 其中

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

- $[\bullet, \bullet]$  是加性希尔伯特符号,  $\left[ \frac{\bullet}{\bullet} \right]$  是加性勒让德符号.
- 由于  $E_1, E_2$  对应的  $(e_1, e_2, e_3)$  相差平方, 故

$$\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)}).$$

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

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

- 令  $L_i$  为定义了  $H_i$  在  $Q_i$  处切平面的线性型, 定义

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

- 它不依赖  $P$  和  $Q_i$  的选择.

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

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

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

- 令  $L_i$  为定义了  $H_i$  在  $Q_i$  处切平面的线性型, 定义

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

- 它不依赖  $P$  和  $Q_i$  的选择.

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

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

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

- 令  $L_i$  为定义了  $H_i$  在  $Q_i$  处切平面的线性型, 定义

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

- 它不依赖  $P$  和  $Q_i$  的选择.

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

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

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

- 令  $L_i$  为定义了  $H_i$  在  $Q_i$  处切平面的线性型, 定义

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

- 它不依赖  $P$  和  $Q_i$  的选择.

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

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

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

- 令  $L_i$  为定义了  $H_i$  在  $Q_i$  处切平面的线性型, 定义

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

- 它不依赖  $P$  和  $Q_i$  的选择.

### 引理 (Cassels 1998)

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

- 由正合列

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

得长正合列

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

- 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

$$\mathrm{rank}_{\mathbb{Z}}(E/\mathbb{Q}) = 0, \quad \mathrm{III}(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}.$$

- 由正合列

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

得长正合列

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

- 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

$$\mathrm{rank}_{\mathbb{Z}}(E/\mathbb{Q}) = 0, \quad \mathrm{III}(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}.$$



- 回忆

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

其中  $e_1a^2 + e_2b^2 + e_3c^2 = 0$ ,  $a, b, c$  是互素的奇数.

- 首先  $\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)})$ . 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  $\Lambda = (d_1, d_2, d_3), \Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}'_2(E_i^{(n)})$ .
- 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.

- 回忆

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

其中  $e_1a^2 + e_2b^2 + e_3c^2 = 0$ ,  $a, b, c$  是互素的奇数.

- 首先  $\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)})$ . 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  $\Lambda = (d_1, d_2, d_3), \Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}'_2(E_i^{(n)})$ .
- 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.

- 回忆

$$E_1^{(n)}: ny^2 = x(x - e_1)(x + e_2), \quad E_2^{(n)}: ny^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ ,  $a, b, c$  是互素的奇数.

- 首先  $\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)})$ . 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  $\Lambda = (d_1, d_2, d_3), \Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}'_2(E_i^{(n)})$ .

- 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.

- 回忆

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

其中  $e_1a^2 + e_2b^2 + e_3c^2 = 0$ ,  $a, b, c$  是互素的奇数.

- 首先  $\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)})$ . 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  $\Lambda = (d_1, d_2, d_3), \Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}'_2(E_i^{(n)})$ .
- 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.

- 回忆

$$E_1^{(n)}: ny^2 = x(x - e_1)(x + e_2), \quad E_2^{(n)}: ny^2 = x(x - e_1 a^2)(x + e_2 b^2)$$

其中  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ ,  $a, b, c$  是互素的奇数.

- 首先  $\text{Sel}'_2(E_1^{(n)}) \cong \text{Sel}'_2(E_2^{(n)})$ . 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  $\Lambda = (d_1, d_2, d_3), \Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}'_2(E_i^{(n)})$ .
- 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.

## 计算 Cassels 配对: 比较局部符号(续)

- $v = p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$ . 设  $Q_i = (\alpha_i, \beta_i, \gamma_i) \in H_i(\mathbb{Q})$ .  
选取

$$P_p = (1, 0, u, v), \quad \mathcal{L}_1(P_p) = e_1 n \alpha_1 - d_3 \gamma_1 v + d_2 \beta_1 u$$

$$\mathcal{P}_p = (1, 0, cu, bv), \quad \mathcal{L}_1(\mathcal{P}_p) = a e_1 n \alpha_1 - b d_3 \gamma_1 v + c d_2 \beta_1 u$$

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

- 这里需要利用  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ .

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

## 计算 Cassels 配对: 比较局部符号(续)

- $v = p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$ . 设  $Q_i = (\alpha_i, \beta_i, \gamma_i) \in H_i(\mathbb{Q})$ .  
选取

$$P_p = (1, 0, u, v), \quad L_1(P_p) = e_1 n \alpha_1 - d_3 \gamma_1 v + d_2 \beta_1 u$$

$$\mathcal{P}_p = (1, 0, cu, bv), \quad \mathcal{L}_1(\mathcal{P}_p) = a e_1 n \alpha_1 - b d_3 \gamma_1 v + c d_2 \beta_1 u$$

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

- 这里需要利用  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ .

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

## 计算 Cassels 配对: 比较局部符号(续)

- $v = p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$ . 设  $Q_i = (\alpha_i, \beta_i, \gamma_i) \in H_i(\mathbb{Q})$ .  
选取

$$P_p = (1, 0, u, v), \quad L_1(P_p) = e_1 n \alpha_1 - d_3 \gamma_1 v + d_2 \beta_1 u$$

$$\mathcal{P}_p = (1, 0, cu, bv), \quad \mathcal{L}_1(\mathcal{P}_p) = a e_1 n \alpha_1 - b d_3 \gamma_1 v + c d_2 \beta_1 u$$

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

- 这里需要利用  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ .

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



## 计算 Cassels 配对: 比较局部符号(续)

- $v = p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$ . 设  $Q_i = (\alpha_i, \beta_i, \gamma_i) \in H_i(\mathbb{Q})$ .  
选取

$$P_p = (1, 0, u, v), \quad L_1(P_p) = e_1 n \alpha_1 - d_3 \gamma_1 v + d_2 \beta_1 u$$

$$\mathcal{P}_p = (1, 0, cu, bv), \quad \mathcal{L}_1(\mathcal{P}_p) = ae_1 n \alpha_1 - bd_3 \gamma_1 v + cd_2 \beta_1 u$$

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

- 这里需要利用  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ .

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

- $v = p \mid n, p \nmid d_1, p \mid d_2, p \mid d_3$ . 设  $Q_i = (\alpha_i, \beta_i, \gamma_i) \in H_i(\mathbb{Q})$ .  
选取

$$P_p = (1, 0, u, v), \quad L_1(P_p) = e_1 n \alpha_1 - d_3 \gamma_1 v + d_2 \beta_1 u$$

$$\mathcal{P}_p = (1, 0, cu, bv), \quad \mathcal{L}_1(\mathcal{P}_p) = ae_1 n \alpha_1 - bd_3 \gamma_1 v + cd_2 \beta_1 u$$

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

- 这里需要利用  $e_1 a^2 + e_2 b^2 + e_3 c^2 = 0$ .

## 引理

若  $a \equiv b \equiv c \equiv 1 \pmod{4}$ , 则  $(a+b)(b+c)(c+a)/8 \equiv 1 \pmod{4}$  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  $p \equiv 1 \pmod{8}, \forall p \mid n$  这么强的条件.
- 例如  $e_1, e_2$  是奇数,  $2 \parallel e_3$  (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  $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$  (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.

- 对于一些特殊的  $(e_1, e_2, e_3)$ , 我们不需要  $p \equiv 1 \pmod{8}, \forall p \mid n$  这么强的条件.
- 例如  $e_1, e_2$  是奇数,  $2 \parallel e_3$  (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  $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$  (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.

- 对于一些特殊的  $(e_1, e_2, e_3)$ , 我们不需要  $p \equiv 1 \pmod{8}, \forall p \mid n$  这么强的条件.
- 例如  $e_1, e_2$  是奇数,  $2 \parallel e_3$  (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  $2 \parallel e_1, 2 \parallel e_2, 4 \mid e_3$  (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.

感谢各位的倾听!