



# 含非同余数因子的非同余数

张神星 (合肥工业大学)

2025 南京大学数论与自守表示研讨会

 ${\tt zhangshenxing@hfut.edu.cn}$ 

# 同余数问题

• 同余数问题是一个古老的数学问题.

### 同余数问题

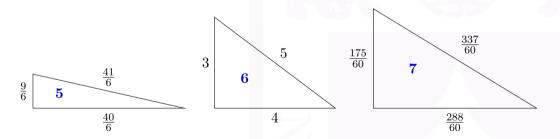
同余数问题是一个古老的数学问题.

congruent number

• 如果正整数 n 可以表达为一个有理边长直角三角形的面积. 则称 n 是同余数.

#### 同余数问题

- 同余数问题是一个古老的数学问题.
- 如果正整数 n 可以表达为一个有理边长直角三角形的面积. 则称 n 是同余数.



• 显然我们只需要考虑无平方因子正整数.

- 显然我们只需要考虑无平方因子正整数.
- 注意到本原的勾股数总可表达为  $(2ab, a^2 b^2, a^2 + b^2)$  的形式, 此时它的面积为  $ab(a+b)(a-b) = n \cdot \square$ .

- 显然我们只需要考虑无平方因子正整数.
- 注意到本原的勾股数总可表达为  $(2ab,a^2-b^2,a^2+b^2)$  的形式, 此时它的面积为  $ab(a+b)(a-b)=n\cdot\square$ .
- 通过变量替换  $x=\frac{na}{b}, y=\frac{n^2}{b^2}\sqrt{\square}$  可将其变为椭圆曲线

$$E_n: y^2 = x^3 - n^2 x.$$

- 显然我们只需要考虑无平方因子正整数.
- 注意到本原的勾股数总可表达为  $(2ab,a^2-b^2,a^2+b^2)$  的形式, 此时它的面积为  $ab(a+b)(a-b)=n\cdot\square$ .
- 通过变量替换  $x=\frac{na}{b}, y=\frac{n^2}{b^2}\sqrt{\square}$  可将其变为椭圆曲线

$$E_n: y^2 = x^3 - n^2 x.$$

• 于是 n 是同余数当且仅当该椭圆曲线的有理点全体  $E_n(\mathbb{Q})$  构成无限群.

• 不难知道  $E_n(\mathbb{Q})$  的所有挠点为

$$E_n(\mathbb{Q})_{\text{tors}} = E_n[2] = \{(\pm n, 0), (0, 0), O\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

• 不难知道  $E_n(\mathbb{Q})$  的所有挠点为

$$E_n(\mathbb{Q})_{\text{tors}} = E_n[2] = \{(\pm n, 0), (0, 0), O\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

• 由正合列

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

• 不难知道  $E_n(\mathbb{Q})$  的所有挠点为

$$E_n(\mathbb{Q})_{\text{tors}} = E_n[2] = \{(\pm n, 0), (0, 0), O\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

• 由正合列

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

可得

$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) \leqslant \dim_{\mathbb{F}_2} \operatorname{Sel}_2(E_n) - 2 = s_2(n),$$

• 不难知道  $E_n(\mathbb{Q})$  的所有挠点为

$$E_n(\mathbb{Q})_{\text{tors}} = E_n[2] = \{(\pm n, 0), (0, 0), O\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

• 由正合列

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

可得

$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) \leqslant \dim_{\mathbb{F}_2} \operatorname{Sel}_2(E_n) - 2 = s_2(n),$$

其中 s<sub>2</sub>(n) 是

$$\operatorname{Sel}_2'(E_n) := \frac{\operatorname{Sel}_2(E_n)}{E_n(\mathbb{Q})[2]}$$

的维数.

• BSD 猜想断言: 若 n 是非同余数, 则  $L(E_n,1) \neq 0$ , 从而  $n \equiv 1,2,3 \mod 8$ .

- BSD 猜想断言: 若 n 是非同余数, 则  $L(E_n,1) \neq 0$ , 从而  $n \equiv 1,2,3 \mod 8$ .
- 当  $n \equiv 1, 2, 3 \mod 8$  时,  $s_2(n)$  是偶数.

- BSD 猜想断言: 若 n 是非同余数, 则  $L(E_n, 1) \neq 0$ , 从而  $n \equiv 1, 2, 3 \mod 8$ .
- 当  $n \equiv 1, 2, 3 \mod 8$  时,  $s_2(n)$  是偶数.
- 自然地,  $s_2(n)=0$  蕴含 n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]=0$ .

- BSD 猜想断言: 若 n 是非同余数, 则  $L(E_n,1) \neq 0$ , 从而  $n \equiv 1,2,3 \mod 8$ .
- 当  $n \equiv 1, 2, 3 \mod 8$  时,  $s_2(n)$  是偶数.
- 自然地,  $s_2(n) = 0$  蕴含 n 是非同余数且  $III(E_n)[2^{\infty}] = 0$ .
- 此时由 Tian-Yuan-Zhang (2017) 和 Smith (2016), 它等价于

$$\sum_{\substack{n=d_0d_1\cdots d_k\\d_1\equiv \cdots\equiv d_k\equiv 1 \bmod 8\\h_4(-d_i)=0, \forall i}}1=1\in \mathbb{F}_2,$$

且此时 BSD 猜想 2 部分成立.

- BSD 猜想断言: 若 n 是非同余数, 则  $L(E_n,1) \neq 0$ , 从而  $n \equiv 1,2,3 \mod 8$ .
- 当  $n \equiv 1, 2, 3 \mod 8$  时,  $s_2(n)$  是偶数.
- 自然地,  $s_2(n) = 0$  蕴含 n 是非同余数且  $III(E_n)[2^{\infty}] = 0$ .
- 此时由 Tian-Yuan-Zhang (2017) 和 Smith (2016), 它等价于

$$\sum_{\substack{n=d_0d_1\cdots d_k\\d_1\equiv \cdots\equiv d_k\equiv 1 \bmod 8\\h_4(-d_i)=0,\forall i}}1=1\in\mathbb{F}_2,$$

且此时 BSD 猜想 2 部分成立.

• 这里  $h_4(-d) = r_4(\mathcal{A}_{-d})$  是  $F_{-d} = \mathbb{Q}(\sqrt{-d})$  整数环  $\mathcal{O}_{-d}$  缩理想类群  $\mathcal{A}_{-d}$  的 4 秩,

$$r_{2^a}(A) := \dim_{\mathbb{F}_2} \left( \frac{2^{a-1}A}{2^a A} \right).$$

#### 定理 (Wang 2016)

若 n 是模 4 余 1 素数乘积,则下述等价:

- n 是非同余数且  $\mathrm{III}(E_n)[2^{\infty}]\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-n) = 1, h_8(-n) \equiv (d-1)/4 \mod 2$ ,

其中  $0 < d \mid n$  满足  $(d, -n)_v = 1, \forall v, d \neq 1, n$ , 或  $(2d, -n)_v = 1, \forall v$ .

这里  $(d,-n)_v$  是希尔伯特符号.

#### 定理 (Wang 2016)

若 n 是模 4 余 1 素数乘积,则下述等价:

- n 是非同余数且  $\mathrm{III}(E_n)[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-n) = 1, h_8(-n) \equiv (d-1)/4 \mod 2$ ,

其中  $0 < d \mid n$  满足  $(d, -n)_v = 1, \forall v, d \neq 1, n$ , 或  $(2d, -n)_v = 1, \forall v$ .

这里  $(d,-n)_v$  是希尔伯特符号.

### 定理 (Wang-Zhang 2022)

若 n 是模 8 余  $\pm 1$  素数乘积,则下述等价:

- n 是非同余数且  $\mathrm{III}(E_n)[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-n) = 1, h_8(-n) = 0.$

### 定理 (Zhang 2023)

若 n 是模 8 余  $\pm 1$  素数乘积,则下述等价:

- 2n 是非同余数且  $\mathrm{III}(E_{2n})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-n) = 1, d \equiv 9 \mod 16$ ,

其中  $d \mid n$  满足  $(d,n)_v = 1, \forall v$  且  $d \neq 1, d \equiv 1 \mod 4$ .

### 定理 (Zhang 2023)

若 n 是模 8 余  $\pm 1$  素数乘积,则下述等价:

- 2n 是非同余数且  $\mathrm{III}(E_{2n})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-n) = 1, d \equiv 9 \mod 16$ ,

其中  $d \mid n$  满足  $(d, n)_v = 1, \forall v$  且  $d \neq 1, d \equiv 1 \mod 4$ .

• 这实际上也等价于  $h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1.$ 

# 定理 (Zhang 2023)

若 n 是模 8 余  $\pm 1$  素数乘积,则下述等价:

- 2n 是非同余数且  $\mathrm{III}(E_{2n})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-n) = 1, d \equiv 9 \mod 16$ ,

其中  $d \mid n$  满足  $(d, n)_v = 1, \forall v$  且  $d \neq 1, d \equiv 1 \mod 4$ .

- 这实际上也等价于  $h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1.$
- 此外, Qin (2021) 证明了当素数  $p \equiv 1 \mod 8$  且  $r_8(K_2\mathcal{O}_p) = 0$  时, p 是非同余数. 且若此时  $r_4(K_2\mathcal{O}_p) = 1$ , 则  $\text{III}(E_p/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/4\mathbb{Z})^2$ .

### 设定

• 这些结论都是指定 n 的素因子落在某个同余类中来研究.

- 这些结论都是指定 n 的素因子落在某个同余类中来研究.
- 我们想要考虑的问题略有不同, 我们希望从一个满足  $s_2(Q) = 0$  的非同余数 Q 出发, 构造它的一个倍数 n = PQ, 使得 n 依然是非同余数.

- 这些结论都是指定 n 的素因子落在某个同余类中来研究.
- 我们想要考虑的问题略有不同, 我们希望从一个满足  $s_2(Q) = 0$  的非同余数 Q 出发, 构造它的一个倍数 n = PQ, 使得 n 依然是非同余数.
- 设  $P = p_1 \cdots p_k$ , 其中素因子  $p_i \equiv 1 \mod 8$ .

- 这些结论都是指定 n 的素因子落在某个同余类中来研究.
- 我们想要考虑的问题略有不同, 我们希望从一个满足  $s_2(Q) = 0$  的非同余数 Q 出发, 构造它的一个倍数 n = PQ, 使得 n 依然是非同余数.
- 设  $P = p_1 \cdots p_k$ , 其中素因子  $p_i \equiv 1 \mod 8$ .
- $\mathfrak{P} Q = \gcd(2, Q)q_1 \cdots q_\ell$ .

• 假设存在  $\mathbb{F}_2$  上的向量  $oldsymbol{u}=(u_1,\ldots,u_k)^{\mathrm{T}}$ ,  $oldsymbol{v}=(v_1,\ldots,v_\ell)^{\mathrm{T}}$ ,

- 假设存在  $\mathbb{F}_2$  上的向量  $oldsymbol{u}=(u_1,\ldots,u_k)^{\mathrm{T}}$ ,  $oldsymbol{v}=(v_1,\ldots,v_\ell)^{\mathrm{T}}$ ,
- 使得  $\sum_i u_i = 0, \sum_j v_j = 1, \left[\frac{p_i}{q_i}\right] = u_i v_j.$

- 假设存在  $\mathbb{F}_2$  上的向量  $oldsymbol{u}=(u_1,\ldots,u_k)^{\mathrm{T}}$ ,  $oldsymbol{v}=(v_1,\ldots,v_\ell)^{\mathrm{T}}$ ,
- 使得  $\sum_i u_i = 0, \sum_j v_j = 1, \left[\frac{p_i}{q_j}\right] = u_i v_j.$
- 这里  $\left[\frac{p_i}{q_i}\right] = \log\left(\frac{p_i}{q_i}\right)$  是加性勒让德符号, 其中  $\log: \{\pm 1\} \stackrel{\sim}{\longrightarrow} \mathbb{F}_2$ .

- 假设存在  $\mathbb{F}_2$  上的向量  $oldsymbol{u}=(u_1,\ldots,u_k)^{\mathrm{T}}$ ,  $oldsymbol{v}=(v_1,\ldots,v_\ell)^{\mathrm{T}}$ ,
- 使得  $\sum_i u_i = 0, \sum_j v_j = 1, \left[\frac{p_i}{q_j}\right] = u_i v_j.$
- 这里  $\left[\frac{p_i}{q_j}\right] = \log\left(\frac{p_i}{q_j}\right)$  是加性勒让德符号, 其中  $\log: \{\pm 1\} \stackrel{\sim}{\longrightarrow} \mathbb{F}_2$ .
- 换言之, 定义矩阵

$$A_{2P} = A_P := ([p_j, -P]_{p_i}) \in M_k(\mathbb{F}_2),$$
 (每行元素之和为 0)

- 假设存在  $\mathbb{F}_2$  上的向量  $\boldsymbol{u}=(u_1,\ldots,u_k)^{\mathrm{T}}$ ,  $\boldsymbol{v}=(v_1,\ldots,v_\ell)^{\mathrm{T}}$ ,
- 使得  $\sum_i u_i = 0, \sum_j v_j = 1, \left[\frac{p_i}{q_i}\right] = u_i v_j.$
- 这里  $\left[\frac{p_i}{q_i}\right] = \log\left(\frac{p_i}{q_i}\right)$  是加性勒让德符号, 其中  $\log: \{\pm 1\} \stackrel{\sim}{\longrightarrow} \mathbb{F}_2$ .
- 换言之, 定义矩阵

$$A_{2P} = A_P := ([p_j, -P]_{p_i}) \in M_k(\mathbb{F}_2),$$
 (每行元素之和为 0)

• 并类似定义  $A_Q$ ,  $A_n$ , 则

$$oldsymbol{A}_n = egin{pmatrix} oldsymbol{A}_P + oldsymbol{U}_P & oldsymbol{u} oldsymbol{v}^{\mathrm{T}} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} & oldsymbol{A}_Q \end{pmatrix},$$

其中  $\mathbf{1}^{\mathrm{T}} \boldsymbol{u} = 0, \mathbf{1}^{\mathrm{T}} \boldsymbol{v} = 1, \ \boldsymbol{U}_{P} = \mathrm{diag}\{u_{1}, \dots, u_{k}\}.$ 

主要结果:  $s_2(n) = 0$  情形

#### 定理

在前述假设下, 如下等价:

- n 是非同余数且  $\text{III}(E_n) = 0$ ;
- $A_P + U_P$  可逆.

#### 定理

在前述假设下, 如下等价:

- n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $\operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$   $\mathbb{E}\left[\frac{\gamma}{d}\right] = \left[\frac{\sqrt{2}+1}{d}\right] + 1$ ,

其中  $0 < d \mid P$  满足  $d \neq 1, [d, -P]_{p_i} = u_i, \forall p_i \mid d; [d, -P]_{p_i} = 0, \forall p_i \mid \frac{P}{d}; (\alpha, \beta, \gamma)$  是  $d\alpha^2 + \frac{n}{d}\beta^2 = 4\gamma^2$  的一组本原正整数解.

#### 定理

在前述假设下, 如下等价:

- n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $\operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$   $\mathbb{E}\left[\frac{\gamma}{d}\right] = \left[\frac{\sqrt{2}+1}{d}\right] + 1$ ,

其中  $0 < d \mid P$  满足  $d \neq 1, [d, -P]_{p_i} = u_i, \forall p_i \mid d$ ;  $[d, -P]_{p_i} = 0, \forall p_i \mid \frac{P}{d}$ ;  $(\alpha, \beta, \gamma)$  是  $d\alpha^2 + \frac{n}{d}\beta^2 = 4\gamma^2$  的一组本原正整数解.

这里, 本原正整数解是指满足  $gcd(\alpha, \beta, \gamma) = 1$  的正整数解.

推论:  $s_2(n) = 2, u = 0$  情形

若取 u = 0 则我们得到:

推论:  $s_2(n) = 2, u = 0$  情形

若取 u=0 则我们得到:

#### 推论

在前述假设下,若  $\left[\frac{p_i}{q_j}\right]=0, \forall i,j$ ,则如下等价:

- n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-P) = 1$  **A**  $\left[\frac{\gamma}{P}\right] = h_8(-P)$ ;
- $h_4(-P) = 1$   $\mathbb{H}\left[\frac{\gamma}{P}\right] = r_4(K_2\mathcal{O}_P)$ ,

其中  $(\alpha, \beta, \gamma)$  是  $P\alpha^2 + Q\beta^2 = 4\gamma^2$  的一组本原正整数解.

推论:  $s_2(n) = 2, u = 0$  情形

若取 u=0 则我们得到:

### 推论

在前述假设下,若  $\left[\frac{p_i}{q_j}\right]=0, \forall i,j$ ,则如下等价:

- n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
- $h_4(-P) = 1$   $\mathbb{E}\left[\frac{\gamma}{P}\right] = h_8(-P)$ ;
- $h_4(-P) = 1$  **L**  $\left[\frac{\gamma}{P}\right] = r_4(K_2\mathcal{O}_P)$ ,

其中  $(\alpha, \beta, \gamma)$  是  $P\alpha^2 + Q\beta^2 = 4\gamma^2$  的一组本原正整数解.

• 这里  $K_2$  是 Milnor K 群 (或叫 tame kernel).

推论:  $s_2(n) = 2, \ell = 0$  情形

若  $\ell = 0$ , 即 Q = 1, 2, 则:

推论: 
$$s_2(n) = 2, \ell = 0$$
 情形

若  $\ell = 0$ , 即 Q = 1, 2, 则:

## 推论

设 n 是模 8 余 1 素数乘积.

推论: 
$$s_2(n) = 2, \ell = 0$$
 情形

若  $\ell = 0$ , 即 Q = 1, 2, 则:

#### 推论

设 n 是模 8 余 1 素数乘积.

- (1) 下述等价:
  - n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
  - $h_4(-n) = 1$  **L**  $h_8(-n) = 0$ ;
  - $r_4(K_2\mathcal{O}_n) = 0$ .

推论: 
$$s_2(n) = 2, \ell = 0$$
 情形

若  $\ell = 0$ , 即 Q = 1, 2, 则:

### 推论

设 n 是模 8 余 1 素数乘积.

- (1) 下述等价:
  - n 是非同余数且  $\coprod(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
  - $h_4(-n) = 1 \perp h_8(-n) = 0$ ;
  - $r_4(K_2\mathcal{O}_n) = 0$ .
- (2) 下述等价:
  - 2n 是非同余数且  $III(E_{2n}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ ;
  - $h_4(-n) = 1$  **L**  $h_8(-n) + h_8(-2n) = 1$ ;
  - $r_4(K_2\mathcal{O}_{-2n}) = 0$ .

### 定理

假设前述条件以及  $\left[rac{p_i}{q_j}
ight]=0, orall i,j$ . 若存在分解  $P=f_1\cdots f_r$  满足

- $h_4(-f_i) = 1, \forall i$ ;
- $\left[\frac{p}{p'}\right]=0$ , 其中  $p\mid f_i,p'\mid f_j$  是任意素因子,  $i\neq j$ ;
- $\left[\frac{\gamma_i}{f_i}\right]=0$ ,  $\forall i \neq j$ ;  $\left[\frac{\gamma_i}{f_i}\right]=h_8(-f_i)$ ,

则 n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^{2r}$ ,其中  $(\alpha_i,\beta_i,\gamma_i)$  是  $f_i\alpha_i^2+\frac{n}{f_i}\beta_i^2=4\gamma_i^2$  的一组本原正整数解.

推论:  $s_2(n) \geqslant 2, \ell = 0$  情形

## 推论

设奇数 n 的所有素因子均模 8 余 1.

- (1) (Wang 2016) 若存在分解  $n = f_1 \cdots f_r$  使得
  - $h_4(-f_i) = 1, h_8(-f_i) = 0, \forall i$ ;
  - $h_8(-n) = r$ ;  $\mathbf{g}$   $h_8(-n) = r 1, [(2, \sqrt{-n})] \notin \mathcal{A}_{-n}^4$ ;
  - $\left[\frac{p}{p'}\right]=0$ ,其中  $p\mid f_i,p'\mid f_j$  是任意素因子, $i\neq j$ ,

则 n 是非同余数且  $\mathrm{III}(E_n)\cong (\mathbb{Z}/2\mathbb{Z})^{2r}$ .

推论:  $s_2(n) \geqslant 2, \ell = 0$  情形

### 推论

设奇数 n 的所有素因子均模 8 余 1.

- (1) (Wang 2016) 若存在分解  $n = f_1 \cdots f_r$  使得
  - $h_4(-f_i) = 1, h_8(-f_i) = 0, \forall i$ ;
  - $h_8(-n) = r$ ; **x**  $h_8(-n) = r 1, [(2, \sqrt{-n})] \notin \mathcal{A}_{-n}^4$ ;
  - $\left[\frac{p}{p'}\right]=0$ , 其中  $p\mid f_i,p'\mid f_j$  是任意素因子,  $i\neq j$ ,

则 n 是非同余数且  $\coprod (E_n) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$ .

- (2) 若存在分解  $n = f_1 \cdots f_r$  使得
  - $h_4(-f_i) = 1, h_8(-f_i) = 0, \forall i;$
  - $h_8(-2n) = r$ ;
  - $\left[\frac{p}{p'}\right]=0$ , 其中  $p\mid f_i,p'\mid f_j$  是任意素因子,  $i\neq j$ ,

则 2n 是非同余数且  $\coprod (E_{2n}) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$ .

descent method
 证明主要工具是下降法.

descent method

- 证明主要工具是下降法.
- 根据 2-下降法,  $Sel_2(E_n)$  可等同于集合

$$\{\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}\},\$$

#### descent method

- 证明主要工具是下降法.
- 根据 2-下降法,  $Sel_2(E_n)$  可等同于集合

$$\{\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  $D_{\Lambda}$  是齐性空间

$$\begin{cases} H_1: & -nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ H_2: & -nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ H_3: & 2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases}$$

#### descent method

- 证明主要工具是下降法.
- 根据 2-下降法,  $Sel_2(E_n)$  可等同于集合

$$\{\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  $D_{\Lambda}$  是齐性空间

$$\begin{cases} H_1: & -nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ H_2: & -nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ H_3: & 2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases}$$

• 一般地  $E(\mathbb{Q}) \ni (x,y) \mapsto (x-n,x+n,x)$ ,

#### descent method

- 证明主要工具是下降法.
- 根据 2-下降法,  $Sel_2(E_n)$  可等同于集合

$$\{\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  $D_{\Lambda}$  是齐性空间

$$\begin{cases} H_1: & -nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ H_2: & -nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ H_3: & 2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases}$$

- 一般地  $E(\mathbb{Q}) \ni (x,y) \mapsto (x-n,x+n,x)$ ,
- $O \mapsto (1,1,1), (n,0) \mapsto (2,2n,n), (-n,0) \mapsto (-2n,2,-n), (0,0) \mapsto (-n,n,-1).$

• 通过对这些齐性空间可解性的分析, Monsky 将  $\mathrm{Sel}_2'(E_n)$  与一  $\mathbb{F}_2$  上矩阵  $M_n$  的核 联系起来.

- 通过对这些齐性空间可解性的分析, Monsky 将  $\mathrm{Sel}_2'(E_n)$  与一  $\mathbb{F}_2$  上矩阵  $M_n$  的核 联系起来.
- 当  $n = p_1 \cdots p_k$  是奇数时,  $Sel_2'(E_n)$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的正因子.

- 通过对这些齐性空间可解性的分析, Monsky 将  $\mathrm{Sel}_2'(E_n)$  与一  $\mathbb{F}_2$  上矩阵  $M_n$  的核 联系起来.
- 当  $n = p_1 \cdots p_k$  是奇数时,  $Sel_2'(E_n)$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的正因子.
- 此时

$$\operatorname{Sel}_{2}'(E_{n}) \to \operatorname{Ker} \boldsymbol{M}_{n}, \quad \boldsymbol{M}_{n} = \begin{pmatrix} \boldsymbol{A}_{n} + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,2} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_{n} + \boldsymbol{D}_{n,-2} \end{pmatrix}$$
$$(d_{1}, d_{2}, d_{3}) \mapsto \begin{pmatrix} \psi_{n}(d_{2}) \\ \psi_{n}(d_{1}) \end{pmatrix},$$

- 通过对这些齐性空间可解性的分析, Monsky 将  $\mathrm{Sel}_2'(E_n)$  与一  $\mathbb{F}_2$  上矩阵  $M_n$  的核 联系起来.
- 当  $n = p_1 \cdots p_k$  是奇数时,  $Sel_2'(E_n)$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的正因子.
- 此时

$$\operatorname{Sel}_{2}'(E_{n}) \to \operatorname{Ker} \boldsymbol{M}_{n}, \quad \boldsymbol{M}_{n} = \begin{pmatrix} \boldsymbol{A}_{n} + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,2} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_{n} + \boldsymbol{D}_{n,-2} \end{pmatrix}$$
$$(d_{1}, d_{2}, d_{3}) \mapsto \begin{pmatrix} \psi_{n}(d_{2}) \\ \psi_{n}(d_{1}) \end{pmatrix},$$

• 其中  $\psi_n(d) := (v_{p_1}(d), \dots, v_{p_k}(d))^{\mathrm{T}} \in \mathbb{F}_2^k$ ,

- 通过对这些齐性空间可解性的分析, Monsky 将  $\mathrm{Sel}_2'(E_n)$  与一  $\mathbb{F}_2$  上矩阵  $M_n$  的核 联系起来.
- 当  $n = p_1 \cdots p_k$  是奇数时,  $Sel_2'(E_n)$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的正因子.
- 此时

$$\operatorname{Sel}_{2}'(E_{n}) \to \operatorname{Ker} \boldsymbol{M}_{n}, \quad \boldsymbol{M}_{n} = \begin{pmatrix} \boldsymbol{A}_{n} + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,2} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_{n} + \boldsymbol{D}_{n,-2} \end{pmatrix}$$
$$(d_{1}, d_{2}, d_{3}) \mapsto \begin{pmatrix} \psi_{n}(d_{2}) \\ \psi_{n}(d_{1}) \end{pmatrix},$$

- 其中  $\psi_n(d) := (v_{p_1}(d), \dots, v_{p_k}(d))^{\mathrm{T}} \in \mathbb{F}_2^k$ ,
- $D_{n,\varepsilon} := \operatorname{diag} \left\{ \left[ \frac{\varepsilon}{p_1} \right], \dots, \left[ \frac{\varepsilon}{p_k} \right] \right\}.$

• 类似地,  $Sel_2'(E_{2n})$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的 因子且  $d_2 > 0$ ,  $d_3 \equiv 1 \mod 4$ .

- 类似地,  $Sel_2'(E_{2n})$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的 因子且  $d_2 > 0$ ,  $d_3 \equiv 1 \mod 4$ .
- 此时

$$\operatorname{Sel}_{2}'(E_{2n}) \to \operatorname{Ker} \boldsymbol{M}_{2n}, \quad \boldsymbol{M}_{2n} = \begin{pmatrix} \boldsymbol{A}_{n}^{\mathrm{T}} + \boldsymbol{D}_{2} & \boldsymbol{D}_{n,-1} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_{n} + \boldsymbol{D}_{n,2} \end{pmatrix}$$
$$(d_{1}, d_{2}, d_{3}) \mapsto \begin{pmatrix} \psi_{n}(|d_{3}|) \\ \psi_{n}(d_{2}) \end{pmatrix},$$

- 类似地,  $Sel_2'(E_{2n})$  中的元素可选取一代表元  $(d_1, d_2, d_3)$  使得  $d_1, d_2, d_3$  均为 n 的 因子且  $d_2 > 0$ ,  $d_3 \equiv 1 \mod 4$ .
- 此时

$$\operatorname{Sel}_{2}'(E_{2n}) \to \operatorname{Ker} \boldsymbol{M}_{2n}, \quad \boldsymbol{M}_{2n} = \begin{pmatrix} \boldsymbol{A}_{n}^{\mathrm{T}} + \boldsymbol{D}_{2} & \boldsymbol{D}_{n,-1} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_{n} + \boldsymbol{D}_{n,2} \end{pmatrix}$$
$$(d_{1}, d_{2}, d_{3}) \mapsto \begin{pmatrix} \psi_{n}(|d_{3}|) \\ \psi_{n}(d_{2}) \end{pmatrix},$$

• 两种情形下均有

$$s_2(n) = \dim_{\mathbb{F}_2} \operatorname{Sel}'_2(E_n) = \operatorname{corank} \mathbf{M}_n.$$

• 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.

- 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.
- Cassels 在  $Sel_2'(E_n)$  上定义了一个 (反) 对称双线性型  $\langle -, \rangle \in \mathbb{F}_2$ .

- 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.
- Cassels 在  $Sel_2'(E_n)$  上定义了一个 (反) 对称双线性型  $\langle -, \rangle \in \mathbb{F}_2$ .
- 对于  $\Lambda \in Sel_2(E_n)$ ,  $H_i$  局部均可解, 从而存在整体解  $Q_i$  (Hasse-Minkowski 原理).

- 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.
- Cassels 在  $Sel_2'(E_n)$  上定义了一个 (反) 对称双线性型  $\langle -, \rangle \in \mathbb{F}_2$ .
- 对于  $\Lambda \in \mathrm{Sel}_2(E_n)$ ,  $H_i$  局部均可解, 从而存在整体解  $Q_i$  (Hasse-Minkowski 原理).
- 令  $L_i$  为一线性型, 使得它定义了  $H_i$  在  $Q_i$  处的切平面.

- 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.
- Cassels 在  $Sel_2'(E_n)$  上定义了一个 (反) 对称双线性型  $\langle -, \rangle \in \mathbb{F}_2$ .
- 对于  $\Lambda \in \mathrm{Sel}_2(E_n)$ ,  $H_i$  局部均可解, 从而存在整体解  $Q_i$  (Hasse-Minkowski 原理).
- 令  $L_i$  为一线性型, 使得它定义了  $H_i$  在  $Q_i$  处的切平面.
- 对于  $\Lambda' = (d'_1, d'_2, d'_3) \in Sel_2(E_n)$ , 定义

$$\langle \Lambda, \Lambda' \rangle = \sum_{v} \langle \Lambda, \Lambda' \rangle_{v} \in \mathbb{F}_{2}, \quad \langle \Lambda, \Lambda' \rangle_{v} = \sum_{i=1}^{3} [L_{i}(P_{v}), d'_{i}]_{v},$$

- 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.
- Cassels 在  $Sel_2'(E_n)$  上定义了一个 (反) 对称双线性型  $\langle -, \rangle \in \mathbb{F}_2$ .
- 对于  $\Lambda \in \mathrm{Sel}_2(E_n)$ ,  $H_i$  局部均可解, 从而存在整体解  $Q_i$  (Hasse-Minkowski 原理).
- 令  $L_i$  为一线性型, 使得它定义了  $H_i$  在  $Q_i$  处的切平面.
- 对于  $\Lambda' = (d'_1, d'_2, d'_3) \in Sel_2(E_n)$ , 定义

$$\langle \Lambda, \Lambda' \rangle = \sum_{v} \langle \Lambda, \Lambda' \rangle_{v} \in \mathbb{F}_{2}, \quad \langle \Lambda, \Lambda' \rangle_{v} = \sum_{i=1}^{3} [L_{i}(P_{v}), d'_{i}]_{v},$$

• 其中对  $\mathbb{Q}$  的任意素位 v, 选取  $P_v \in D_{\Lambda}(\mathbb{Q}_v)$ .

- 仅知道  $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E_n)[2]$  还不足以得到非同余数.
- Cassels 在  $Sel_2'(E_n)$  上定义了一个 (反) 对称双线性型  $\langle -, \rangle \in \mathbb{F}_2$ .
- 对于  $\Lambda \in \mathrm{Sel}_2(E_n)$ ,  $H_i$  局部均可解, 从而存在整体解  $Q_i$  (Hasse-Minkowski 原理).
- 令  $L_i$  为一线性型, 使得它定义了  $H_i$  在  $Q_i$  处的切平面.
- 对于  $\Lambda' = (d'_1, d'_2, d'_3) \in Sel_2(E_n)$ , 定义

$$\langle \Lambda, \Lambda' \rangle = \sum_{v} \langle \Lambda, \Lambda' \rangle_{v} \in \mathbb{F}_{2}, \quad \langle \Lambda, \Lambda' \rangle_{v} = \sum_{i=1}^{3} [L_{i}(P_{v}), d'_{i}]_{v},$$

- 其中对  $\mathbb{Q}$  的任意素位 v, 选取  $P_v \in D_{\Lambda}(\mathbb{Q}_v)$ .
- 这是一个有限和: 当  $v \nmid 2\infty$ ,  $H_i, L_i$  系数的分母, 且  $D_\Lambda$  和  $L_i = 0$  模 v 后依然分别是亏格 1 的曲线和它的一个切平面时,  $\langle -, \rangle_v = 0$ .

# 引理 (Wang2016)

n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]\cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}\iff \mathrm{Sel}_2'(E_n)$  上 Cassels 配对非退化.

n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]\cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}\iff \mathrm{Sel}_2'(E_n)$  上 Cassels 配对非退化.

• 由正合列

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

$$0 \to E_n(\mathbb{Q})[2]/2E_n(\mathbb{Q})[4] \to \operatorname{Sel}_2(E_n) \to \operatorname{Sel}_4(E_n) \to \operatorname{Im} \operatorname{Sel}_4(E_n) \to 0,$$

n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]\cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}\iff \mathrm{Sel}_2'(E_n)$  上 Cassels 配对非退化.

• 由正合列

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

得到长正合列

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

• 其中  $\operatorname{Im} \operatorname{Sel}_4(E_n)$  是映射  $\operatorname{Sel}_4(E_n) \xrightarrow{\times 2} \operatorname{Sel}_2(E_n)$  的像.

n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]\cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}\iff \mathrm{Sel}_2'(E_n)$  上 Cassels 配对非退化.

• 由正合列

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

$$0 \to E_n(\mathbb{Q})[2]/2E_n(\mathbb{Q})[4] \to \operatorname{Sel}_2(E_n) \to \operatorname{Sel}_4(E_n) \to \operatorname{Im} \operatorname{Sel}_4(E_n) \to 0,$$

- 其中  $\operatorname{Im} \operatorname{Sel}_4(E_n)$  是映射  $\operatorname{Sel}_4(E_n) \xrightarrow{\times 2} \operatorname{Sel}_2(E_n)$  的像.
- 而  $Sel_2(E_n)$  上 Cassels 配对的核就是这个像.

n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]\cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}\iff \mathrm{Sel}_2'(E_n)$  上 Cassels 配对非退化.

由正合列

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

$$0 \to E_n(\mathbb{Q})[2]/2E_n(\mathbb{Q})[4] \to \operatorname{Sel}_2(E_n) \to \operatorname{Sel}_4(E_n) \to \operatorname{Im} \operatorname{Sel}_4(E_n) \to 0,$$

- 其中  $\operatorname{Im} \operatorname{Sel}_4(E_n)$  是映射  $\operatorname{Sel}_4(E_n) \xrightarrow{\times 2} \operatorname{Sel}_2(E_n)$  的像.
- 而  $Sel_2(E_n)$  上 Cassels 配对的核就是这个像.
- 因此引理左侧等价于  $\#\mathrm{Sel}_2(E_n) = \#\mathrm{Sel}_4(E_n)$ ,

n 是非同余数且  $\mathrm{III}(E_n)[2^\infty]\cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}\iff \mathrm{Sel}_2'(E_n)$  上 Cassels 配对非退化.

由正合列

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

$$0 \to E_n(\mathbb{Q})[2]/2E_n(\mathbb{Q})[4] \to \operatorname{Sel}_2(E_n) \to \operatorname{Sel}_4(E_n) \to \operatorname{Im} \operatorname{Sel}_4(E_n) \to 0,$$

- 其中  $\operatorname{Im} \operatorname{Sel}_4(E_n)$  是映射  $\operatorname{Sel}_4(E_n) \xrightarrow{\times 2} \operatorname{Sel}_2(E_n)$  的像.
- 而  $Sel_2(E_n)$  上 Cassels 配对的核就是这个像.
- 因此引理左侧等价于  $\#\mathrm{Sel}_2(E_n) = \#\mathrm{Sel}_4(E_n)$ ,
- 等价于  $\operatorname{Im} \operatorname{Sel}_4(E_n) = E_n[2] \subseteq \operatorname{Sel}_2(E_n)$ , 等价于引理右侧.

# Selmer 群的计算

• 现在我们开始证明主要结果.

## Selmer 群的计算

• 现在我们开始证明主要结果.

## 引理

在前述假设下,  $s_2(n) = 2 \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P)$ .

#### Selmer 群的计算

• 现在我们开始证明主要结果.

#### 引理

在前述假设下, 
$$s_2(n) = 2 \operatorname{corank}(A_P + U_P)$$
.

• 我们只证明 n 是奇数的情形, 偶数情形类似,

• 现在我们开始证明主要结果.

#### 引理

在前述假设下, 
$$s_2(n) = 2 \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P)$$
.

- 我们只证明 n 是奇数的情形, 偶数情形类似,
- 设

$$egin{pmatrix} egin{pmatrix} oldsymbol{x} \ oldsymbol{y} \ oldsymbol{z} \ oldsymbol{w} \end{pmatrix} \in \operatorname{Ker} oldsymbol{M}_n = \operatorname{Ker} egin{pmatrix} oldsymbol{A}_P + oldsymbol{U}_P & oldsymbol{u} oldsymbol{v}^{\mathrm{T}} & oldsymbol{O}_k & oldsymbol{O}_{Q,2} \ oldsymbol{O}_k & oldsymbol{A}_P + oldsymbol{U}_P & oldsymbol{u} oldsymbol{v}^{\mathrm{T}} \ oldsymbol{O}_{Q,2} & oldsymbol{v} oldsymbol{u}^{\mathrm{T}} & oldsymbol{A}_Q + oldsymbol{D}_{Q,2} \ oldsymbol{U}^{\mathrm{T}} & oldsymbol{A}_Q + oldsymbol{D}_{Q,-2} \end{pmatrix}.$$

• 则

$$(oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{x} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{y}, \qquad (oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{z} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{x} \ M_Q egin{pmatrix} oldsymbol{y} & = egin{pmatrix} oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{x} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{z} \end{pmatrix}.$$

• 则

$$(oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{x} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{y}, \qquad (oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{z} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{x} \ M_Q egin{pmatrix} oldsymbol{y} &= egin{pmatrix} oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{x} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{z} \end{pmatrix}.$$

• 从  $\mathbf{1}^{\mathrm{T}}(\mathbf{A}_{P}+\mathbf{U}_{P})\mathbf{x}=\mathbf{1}^{\mathrm{T}}\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y}$  得到  $\mathbf{u}^{\mathrm{T}}\mathbf{x}=0$ .

(假设  $\mathbf{1}^{\mathrm{T}}\mathbf{u} = 0$ )

• 则

$$(oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{x} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{y}, \qquad (oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{z} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{x} \ M_Q egin{pmatrix} oldsymbol{y} & = egin{pmatrix} oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{x} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{z} \end{pmatrix}.$$

• 从  $\mathbf{1}^{\mathrm{T}}(\mathbf{A}_{P} + \mathbf{U}_{P})\mathbf{x} = \mathbf{1}^{\mathrm{T}}\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y}$  得到  $\mathbf{u}^{\mathrm{T}}\mathbf{x} = 0$ .

(假设  $\mathbf{1}^{\mathrm{T}}\mathbf{u} = 0$ )

• 同理  $m{u}^{\mathrm{T}}m{z}=0$ , 故  $m{M}_{Q}egin{pmatrix} m{y} \\ m{w} \end{pmatrix}=m{0}$ .

• 则

$$(oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{x} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{y}, \qquad (oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{z} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{x} \ M_Q egin{pmatrix} oldsymbol{y} & = egin{pmatrix} oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{x} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{z} \end{pmatrix}.$$

• 从  $\mathbf{1}^{\mathrm{T}}(\mathbf{A}_{P} + \mathbf{U}_{P})\mathbf{x} = \mathbf{1}^{\mathrm{T}}\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y}$  得到  $\mathbf{u}^{\mathrm{T}}\mathbf{x} = 0$ .

(假设  $\mathbf{1}^{\mathrm{T}}\mathbf{u} = 0$ )

- 同理  $oldsymbol{u}^{\mathrm{T}}oldsymbol{z}=0$ , 故  $oldsymbol{M}_{Q}egin{pmatrix} oldsymbol{y} \\ oldsymbol{w} \end{pmatrix}=oldsymbol{0}.$
- 由于  $s_2(Q)=0$ ,  $M_Q$  可逆, 从而  $\boldsymbol{y}=\boldsymbol{w}=\boldsymbol{0}$ ,

则

$$(oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{x} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{y}, \qquad (oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{z} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{x} \ M_Q egin{pmatrix} oldsymbol{y} & = egin{pmatrix} oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{x} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{z} \end{pmatrix}.$$

• 从  $\mathbf{1}^{\mathrm{T}}(\mathbf{A}_{P} + \mathbf{U}_{P})\mathbf{x} = \mathbf{1}^{\mathrm{T}}\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y}$  得到  $\mathbf{u}^{\mathrm{T}}\mathbf{x} = 0$ .

(假设  $\mathbf{1}^{\mathrm{T}}\mathbf{u} = 0$ )

- 同理  $oldsymbol{u}^{\mathrm{T}}oldsymbol{z}=0$ , 故  $oldsymbol{M}_{Q}egin{pmatrix} oldsymbol{y} \\ oldsymbol{w} \end{pmatrix}=oldsymbol{0}.$
- 由于  $s_2(Q)=0$ ,  $M_Q$  可逆, 从而 y=w=0,
- $x, z \in \text{Ker}(\mathbf{A}_P + \mathbf{U}_P), \ s_2(n) = 2 \operatorname{corank}(\mathbf{A}_P + \mathbf{U}_P).$

则

$$(oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{x} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{y}, \qquad (oldsymbol{A}_P + oldsymbol{U}_P) oldsymbol{z} = oldsymbol{u} oldsymbol{v}^{\mathrm{T}} oldsymbol{x} \ M_Q egin{pmatrix} oldsymbol{y} & = egin{pmatrix} oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{x} \ oldsymbol{v} oldsymbol{u}^{\mathrm{T}} oldsymbol{z} \end{pmatrix}.$$

• 从  $\mathbf{1}^{\mathrm{T}}(\mathbf{A}_{P} + \mathbf{U}_{P})\mathbf{x} = \mathbf{1}^{\mathrm{T}}\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y}$  得到  $\mathbf{u}^{\mathrm{T}}\mathbf{x} = 0$ .

(假设  $\mathbf{1}^{\mathrm{T}}\mathbf{u}=0$ )

- 同理  $oldsymbol{u}^{\mathrm{T}}oldsymbol{z}=0$ , 故  $oldsymbol{M}_{Q}egin{pmatrix} oldsymbol{y} \\ oldsymbol{w} \end{pmatrix}=oldsymbol{0}.$
- 由于  $s_2(Q)=0$ ,  $M_Q$  可逆, 从而  $\boldsymbol{y}=\boldsymbol{w}=\boldsymbol{0}$ ,
- $x, z \in \text{Ker}(A_P + U_P)$ ,  $s_2(n) = 2 \operatorname{corank}(A_P + U_P)$ .
- 由此可立得主要结论中  $s_2(n) = 0$  的情形.

## Cassles 配对的计算

#### 命题

设 
$$0 < f_i, f_j \mid P$$
 满足  $\gcd(f_i, f_j) = 1$ ,  $\psi_P(f_i), \psi_P(f_j) \in \operatorname{Ker}(A_P + U_P)$ . 令  $\Lambda_t = (f_t, 1, f_t), \Lambda_t' = (f_t, f_t, 1)$ , 那么

$$\begin{split} \langle \Lambda_i', \Lambda_i \rangle &= \left[ \frac{\sqrt{2} + 1}{f_i} \right] + \left[ \frac{\gamma_i}{f_i} \right] = \left[ \frac{\sqrt{2} + 1}{f_i} \right] + \left[ \frac{\gamma_i'}{f_i} \right], \\ \langle \Lambda_i', \Lambda_j \rangle &= \left[ \frac{\gamma_i}{f_j} \right] = \left[ \frac{\gamma_j'}{f_i} \right], \\ \langle \Lambda_i', \Lambda_i' \rangle &= \left[ \frac{\gamma_i \gamma_i'}{f_i} \right], \qquad \langle \Lambda_i', \Lambda_j' \rangle = \left[ \frac{\gamma_i \gamma_i'}{f_j} \right], \end{split}$$

其中  $(\alpha_i, \beta_i, \gamma_i), (\alpha'_i, \beta'_i, \gamma'_i)$  分别是方程  $f_i\alpha_i^2 + \frac{n}{f_i}\beta_i^2 = 4\gamma_i^2$ ,  $f_i\alpha'_i^2 - \frac{n}{f_i}\beta'_i^2 = 4\gamma'_i^2$  的本原正整数解.

$$D_{\Lambda_i}: \begin{cases} H_1: & -nt^2 + u_2^2 - f_i u_3^2 = 0, \\ H_2: & -\frac{n}{f_i}t^2 + u_3^2 - u_1^2 = 0, \\ H_3: & 2nt^2 + f_i u_1^2 - u_2^2 = 0. \end{cases}$$

$$D_{\Lambda_i} : \begin{cases} H_1 : & -nt^2 + u_2^2 - f_i u_3^2 = 0, \\ H_2 : & -\frac{n}{f_i} t^2 + u_3^2 - u_1^2 = 0, \\ H_3 : & 2nt^2 + f_i u_1^2 - u_2^2 = 0. \end{cases}$$

取

$$Q_1 = (\beta_i', f_i \alpha_i', 2\gamma_i') \in H_1(\mathbb{Q}),$$
  $L_1 = \frac{n}{f_i} \beta_i' t - \alpha_i' u_2 + 2\gamma_i' u_3,$ 

$$D_{\Lambda_i}: \begin{cases} H_1: & -nt^2 + u_2^2 - f_i u_3^2 = 0, \\ H_2: & -\frac{n}{f_i} t^2 + u_3^2 - u_1^2 = 0, \\ H_3: & 2nt^2 + f_i u_1^2 - u_2^2 = 0. \end{cases}$$

#### 取

$$Q_{1} = (\beta'_{i}, f_{i}\alpha'_{i}, 2\gamma'_{i}) \in H_{1}(\mathbb{Q}), \qquad L_{1} = \frac{n}{f_{i}}\beta'_{i}t - \alpha'_{i}u_{2} + 2\gamma'_{i}u_{3},$$

$$Q_{2} = (0, 1, -1) \in H_{2}(\mathbb{Q}), \qquad L_{2} = u_{3} + u_{1}.$$

$$D_{\Lambda_i}: \begin{cases} H_1: & -nt^2 + u_2^2 - f_i u_3^2 = 0, \\ H_2: & -\frac{n}{f_i} t^2 + u_3^2 - u_1^2 = 0, \\ H_3: & 2nt^2 + f_i u_1^2 - u_2^2 = 0. \end{cases}$$

取

$$Q_{1} = (\beta'_{i}, f_{i}\alpha'_{i}, 2\gamma'_{i}) \in H_{1}(\mathbb{Q}), \qquad L_{1} = \frac{n}{f_{i}}\beta'_{i}t - \alpha'_{i}u_{2} + 2\gamma'_{i}u_{3},$$

$$Q_{2} = (0, 1, -1) \in H_{2}(\mathbb{Q}), \qquad L_{2} = u_{3} + u_{1}.$$

• 根据假设不难得到

$$\left[\frac{f_i}{q_s}\right] = 0, \quad \left[\frac{n/f_i}{p}\right] = 0, \forall p \mid f_i, \quad \left[\frac{f_i}{p}\right] = 0, \forall p \mid \frac{P}{f_i}.$$

• 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v$

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,  $[L_1L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma_i', f_t]_v$ .

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,  $[L_1L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma_i', f_t]_v$ .
- 对于  $v \mid \frac{P}{f_i}$ , 取  $P_v = (t, u_1, u_2, u_3) = (0, 1, \sqrt{f_i}, 1)$ .

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,  $[L_1L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma_i', f_t]_v$ .
- 对于  $v \mid \frac{P}{f_i}$ , 取  $P_v = (t, u_1, u_2, u_3) = (0, 1, \sqrt{f_i}, 1)$ .
- 类似可得  $[L_1L_2(P_v), f_t]_v = [\gamma_i', f_t]_v$ .

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,  $[L_1L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma_i', f_t]_v$ .
- 对于  $v \mid \frac{P}{f_i}$ , 取  $P_v = (t, u_1, u_2, u_3) = (0, 1, \sqrt{f_i}, 1)$ .
- 类似可得  $[L_1L_2(P_v), f_t]_v = [\gamma_i', f_t]_v$ .
- $\langle \Lambda_i, \Lambda_i' \rangle = \sum_{v|f_i} \left[ (\sqrt{2} + 1)\gamma_i', f_i \right]_v + \sum_{v|\frac{P}{f_i}} \left[ \gamma_i', f_i \right]_v = \left[ \frac{(\sqrt{2} + 1)\gamma_i'}{f_i} \right].$

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,  $[L_1L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma_i', f_t]_v$ .
- 对于  $v \mid \frac{P}{f_i}$ , 取  $P_v = (t, u_1, u_2, u_3) = (0, 1, \sqrt{f_i}, 1)$ .
- 类似可得  $[L_1L_2(P_v), f_t]_v = [\gamma_i', f_t]_v$ .
- $\langle \Lambda_i, \Lambda_i' \rangle = \sum_{v|f_i} \left[ (\sqrt{2} + 1)\gamma_i', f_i \right]_v + \sum_{v|\frac{P}{f_i}} \left[ \gamma_i', f_i \right]_v = \left[ \frac{(\sqrt{2} + 1)\gamma_i'}{f_i} \right].$
- $\langle \Lambda_i, \Lambda'_j \rangle = \sum_{v|f_i} \left[ (\sqrt{2} + 1)\gamma'_i, f_j \right]_v + \sum_{v|\frac{P}{f_i}} [\gamma'_i, f_j]_v = \left[ \frac{\gamma'_i}{f_j} \right].$

- 对于  $v \mid f_i$ , 取  $P_v = (t, u_1, u_2, u_3) = (1, \sqrt{-2\frac{n}{f_i}}, 0, \sqrt{-\frac{n}{f_i}})$ . 这里根号取正负不影响最后的结果.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v.$
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$ ,  $[L_1L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma_i', f_t]_v$ .
- 对于  $v \mid \frac{P}{f_i}$ , 取  $P_v = (t, u_1, u_2, u_3) = (0, 1, \sqrt{f_i}, 1)$ .
- 类似可得  $[L_1L_2(P_v), f_t]_v = [\gamma_i', f_t]_v$ .
- $\langle \Lambda_i, \Lambda_i' \rangle = \sum_{v|f_i} \left[ (\sqrt{2} + 1)\gamma_i', f_i \right]_v + \sum_{v|\frac{P}{f_i}} \left[ \gamma_i', f_i \right]_v = \left[ \frac{(\sqrt{2} + 1)\gamma_i'}{f_i} \right].$
- $\langle \Lambda_i, \Lambda'_j \rangle = \sum_{v|f_i} \left[ (\sqrt{2} + 1) \gamma'_i, f_j \right]_v + \sum_{v|\frac{P}{f}} \left[ \gamma'_i, f_j \right]_v = \left[ \frac{\gamma'_i}{f_j} \right].$
- 其它情形类似.

• 根据前面的计算  $s_2(n) = 2 \iff \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$ .

- 根据前面的计算  $s_2(n) = 2 \iff \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$ .
- 此时  $Sel_2'(E_n)$  由  $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$  生成, 其中  $\psi_P(d) \in Ker(A_P + U_P)$ .

- 根据前面的计算  $s_2(n) = 2 \iff \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$ .
- 此时  $Sel_2'(E_n)$  由  $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$  生成, 其中  $\psi_P(d) \in Ker(A_P + U_P)$ .
- 于是  $\langle \Lambda, \Lambda' \rangle = \left[ \frac{\sqrt{2}+1}{d} \right] + \left[ \frac{\gamma}{d} \right].$

- 根据前面的计算  $s_2(n) = 2 \iff \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$ .
- 此时  $Sel_2'(E_n)$  由  $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$  生成, 其中  $\psi_P(d) \in Ker(A_P + U_P)$ .
- 于是  $\langle \Lambda, \Lambda' \rangle = \left[ \frac{\sqrt{2}+1}{d} \right] + \left[ \frac{\gamma}{d} \right].$

若进一步假设 u = 0, 则 d = P.

• 为了将我们的结果与类群、  $K_2$  群联系起来, 我们回顾有关结论.

- 为了将我们的结果与类群、  $K_2$  群联系起来, 我们回顾有关结论.
- $\mathfrak{P}_n = p_1 \cdots p_k \equiv 1 \mod 4$ .

- 为了将我们的结果与类群、  $K_2$  群联系起来, 我们回顾有关结论.
- $\mathfrak{P}_n = p_1 \cdots p_k \equiv 1 \mod 4$ .
- 根据高斯型理论,  $h_2(-n) = k + 1$ ,  $h_4(-n) = \operatorname{corank} \mathbf{R}_{-n} 1$ ,

- 为了将我们的结果与类群、  $K_2$  群联系起来, 我们回顾有关结论.
- $\mathfrak{P}_n = p_1 \cdots p_k \equiv 1 \mod 4$ .
- 根据高斯型理论,  $h_2(-n) = k + 1$ ,  $h_4(-n) = \operatorname{corank} \mathbf{R}_{-n} 1$ ,
- 其中 Rèdei 矩阵  $m{R}_{-n} = egin{pmatrix} m{A}_n & m{b}_{n,2} \ m{b}_{n,-1} & \begin{bmatrix} 2 \\ n \end{bmatrix} \end{pmatrix}$ ,  $m{b}_{n,arepsilon} = m{D}_{n,arepsilon}$ 1.

- 为了将我们的结果与类群、K<sub>2</sub> 群联系起来, 我们回顾有关结论.
- $\mathfrak{P}_n = p_1 \cdots p_k \equiv 1 \mod 4$ .
- 根据高斯型理论,  $h_2(-n) = k + 1$ ,  $h_4(-n) = \operatorname{corank} \mathbf{R}_{-n} 1$ ,
- 其中 Rèdei 矩阵  $m{R}_{-n} = egin{pmatrix} m{A}_n & m{b}_{n,2} \ m{b}_{n,-1} & igg[rac{2}{n}igg] \end{pmatrix}$ ,  $m{b}_{n,arepsilon} = m{D}_{n,arepsilon}$ 1.
- 对于  $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2]$ ,  $\theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \boldsymbol{b}_{n,\gamma} \in \operatorname{Im} \boldsymbol{R}'_{-n}$ .

- 为了将我们的结果与类群、K<sub>2</sub> 群联系起来, 我们回顾有关结论.
- $\mathfrak{P}_n = p_1 \cdots p_k \equiv 1 \mod 4$ .
- 根据高斯型理论,  $h_2(-n) = k + 1$ ,  $h_4(-n) = \operatorname{corank} \mathbf{R}_{-n} 1$ ,
- 其中 Rèdei 矩阵  $m{R}_{-n}=egin{pmatrix} m{A}_n & m{b}_{n,2} \ m{b}_{n,-1} & iggl[ rac{2}{n} iggr] \end{pmatrix}$ ,  $m{b}_{n,arepsilon}=m{D}_{n,arepsilon}$ 1.
- 对于  $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2], \ \theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \boldsymbol{b}_{n,\gamma} \in \operatorname{Im} \boldsymbol{R}'_{-n}.$
- 这里  $R'_{-n}$  是  $R_{-n}$  去掉最后一行,  $(\alpha, \beta, \gamma)$  是  $d\alpha^2 + \frac{n}{d}\beta^2 = 4\gamma^2$  的本原正整数解.

- 为了将我们的结果与类群、  $K_2$  群联系起来, 我们回顾有关结论.
- $\mathfrak{P}_n = p_1 \cdots p_k \equiv 1 \mod 4$ .
- 根据高斯型理论,  $h_2(-n) = k + 1$ ,  $h_4(-n) = \operatorname{corank} \mathbf{R}_{-n} 1$ ,
- 其中 Rèdei 矩阵  $m{R}_{-n}=egin{pmatrix} m{A}_n & m{b}_{n,2} \ m{b}_{n,-1} & \left[rac{2}{n}
  ight] \end{pmatrix}$ ,  $m{b}_{n,arepsilon}=m{D}_{n,arepsilon}$ 1.
- 对于  $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2], \ \theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \boldsymbol{b}_{n,\gamma} \in \operatorname{Im} \boldsymbol{R}'_{-n}.$
- 这里  $R'_{-n}$  是  $R_{-n}$  去掉最后一行,  $(\alpha, \beta, \gamma)$  是  $d\alpha^2 + \frac{n}{d}\beta^2 = 4\gamma^2$  的本原正整数解.
- 对于  $h_{2^a}(-2n)$ , 我们有类似结论.

## $K_2$ 群

• 根据 Browkin-Schinzel (1982) 和 Qin (1995) 的工作,

## $K_2$ 群

- 根据 Browkin-Schinzel (1982) 和 Qin (1995) 的工作,
- 当 m = n, 2n > 2 时

$$2^{r_4(K_2\mathcal{O}_m)+1}=\#\{oldsymbol{x}:oldsymbol{B}_moldsymbol{x}=oldsymbol{b}_{n,\pm 1},oldsymbol{b}_{n,\pm 2},oldsymbol{b}_{n,\pm \mu}\}.$$

#### $K_2$ 群

- 根据 Browkin-Schinzel (1982) 和 Qin (1995) 的工作,
- 当 m = n, 2n > 2 时

$$2^{r_4(K_2\mathcal{O}_m)+1} = \#\{ \boldsymbol{x} : \boldsymbol{B}_m \boldsymbol{x} = \boldsymbol{b}_{n,\pm 1}, \boldsymbol{b}_{n,\pm 2}, \boldsymbol{b}_{n,\pm \mu} \}.$$

$$2^{r_4(K_2\mathcal{O}_m)+2} = \begin{cases} \#\{\boldsymbol{x} : \boldsymbol{B}_m \boldsymbol{x} = \boldsymbol{0}, \boldsymbol{b}_{n,2}, \boldsymbol{b}_{n,\mu}\}, & \text{if } \boldsymbol{b}_{n,-1} \notin \operatorname{Im} \boldsymbol{B}_m; \\ 2\#\{\boldsymbol{x} : \boldsymbol{B}_m \boldsymbol{x} = \boldsymbol{0}, \boldsymbol{b}_{n,2}, \boldsymbol{b}_{n,\mu}\}, & \text{if } \boldsymbol{b}_{n,-1} \in \operatorname{Im} \boldsymbol{B}_m. \end{cases}$$

• 设 n 是模 8 余 1 素数乘积.

- 设 n 是模 8 余 1 素数乘积.
  - $h_4(-n) = h_4(-2n) = \operatorname{corank} \mathbf{A}_n$ .



- 设 n 是模 8 余 1 素数乘积.
  - $h_4(-n) = h_4(-2n) = \operatorname{corank} \mathbf{A}_n$ .
  - $r_4(K_2\mathcal{O}_n) = 0 \iff h_4(-n) = 1, h_8(-n) = 0.$

- 设 n 是模 8 余 1 素数乘积.
  - $h_4(-n) = h_4(-2n) = \operatorname{corank} \mathbf{A}_n$ .
  - $r_4(K_2\mathcal{O}_n) = 0 \iff h_4(-n) = 1, h_8(-n) = 0.$
  - $r_4(K_2\mathcal{O}_{-2n}) = 0 \iff h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1.$

- 设 n 是模 8 余 1 素数乘积.
  - $h_4(-n) = h_4(-2n) = \operatorname{corank} \mathbf{A}_n$ .
  - $r_4(K_2\mathcal{O}_n) = 0 \iff h_4(-n) = 1, h_8(-n) = 0.$
  - $r_4(K_2\mathcal{O}_{-2n}) = 0 \iff h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1.$
  - 若  $h_4(-n) = 1$ , 则  $h_8(-n) = 1 \left[\frac{\sqrt{2}+1}{n}\right]$ ,  $h_8(-2n) = 1 \left[\frac{\sqrt{2}}{n}\right]$ ,  $r_4(K_2\mathcal{O}_{-2n}), r_4(K_2\mathcal{O}_n) \leq 1$ .

- 设 n 是模 8 余 1 素数乘积。
  - $h_4(-n) = h_4(-2n) = \operatorname{corank} \mathbf{A}_n$ .
  - $r_4(K_2\mathcal{O}_n) = 0 \iff h_4(-n) = 1, h_8(-n) = 0.$
  - $r_4(K_2\mathcal{O}_{-2n}) = 0 \iff h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1.$
  - 若  $h_4(-n) = 1$ , 则  $h_8(-n) = 1 \left[\frac{\sqrt{2}+1}{n}\right]$ ,  $h_8(-2n) = 1 \left[\frac{\sqrt{2}}{n}\right]$ ,  $r_4(K_2\mathcal{O}_{-2n}), r_4(K_2\mathcal{O}_n) \leqslant 1$ .
- 由此可得  $s_2(n) = 0$ , u = 0 情形的结论.

• 此时  $A_P + U_P = A_P = \operatorname{diag}\{A_{f_1}, \cdots A_{f_r}\}.$ 

- 此时  $\boldsymbol{A}_P + \boldsymbol{U}_P = \boldsymbol{A}_P = \mathrm{diag}\{\boldsymbol{A}_{f_1}, \cdots \boldsymbol{A}_{f_r}\}.$
- 由  $h_4(-f_i) = 1$  可知 corank  $A_{f_i} = 1$ ,  $s_2(n) = 2r$ .

- 此时  $\boldsymbol{A}_P + \boldsymbol{U}_P = \boldsymbol{A}_P = \mathrm{diag}\{\boldsymbol{A}_{f_1}, \cdots \boldsymbol{A}_{f_r}\}.$
- 此时由 Ker  $M_n$  可知 Sel<sub>2</sub>( $E_n$ ) 由  $\Lambda_i = (f_i, 1, f_i), \Lambda'_i = (f_i, f_i, 1)$  生成.

- 此时  $\boldsymbol{A}_P + \boldsymbol{U}_P = \boldsymbol{A}_P = \mathrm{diag}\{\boldsymbol{A}_{f_1}, \cdots \boldsymbol{A}_{f_r}\}.$
- 此时由 Ker  $M_n$  可知 Sel $_2'(E_n)$  由  $\Lambda_i = (f_i, 1, f_i), \Lambda_i' = (f_i, f_i, 1)$  生成.
- 相应的 Cassels 配对对应矩阵

$$oldsymbol{X} = egin{pmatrix} * & oldsymbol{B}^{\mathrm{T}} + oldsymbol{C} \ oldsymbol{B} + oldsymbol{C} & oldsymbol{B} + oldsymbol{B}^{\mathrm{T}} \end{pmatrix},$$

$$\boldsymbol{B} = \left( \left[ \frac{\gamma_i}{f_j} \right] \right)_{r \times r} = \operatorname{diag} \left\{ h_8(-f_1), \dots, h_8(-f_r) \right\},$$

$$C = \operatorname{diag}\left\{\left[\frac{\sqrt{2}+1}{f_1}\right], \dots, \left[\frac{\sqrt{2}+1}{f_r}\right]\right\} = \operatorname{diag}\left\{1 - h_8(-f_1), \dots, 1 - h_8(-f_r)\right\}.$$

- 此时  $A_P + U_P = A_P = \operatorname{diag}\{A_{f_1}, \cdots A_{f_r}\}.$
- 此时由 Ker  $M_n$  可知 Sel<sub>2</sub>( $E_n$ ) 由  $\Lambda_i = (f_i, 1, f_i), \Lambda'_i = (f_i, f_i, 1)$  生成.
- 相应的 Cassels 配对对应矩阵

$$oldsymbol{X} = egin{pmatrix} * & oldsymbol{B}^{\mathrm{T}} + oldsymbol{C} \ oldsymbol{B} + oldsymbol{C} & oldsymbol{B} + oldsymbol{B}^{\mathrm{T}} \end{pmatrix},$$

$$\boldsymbol{B} = \left( \left[ \frac{\gamma_i}{f_j} \right] \right)_{r \times r} = \operatorname{diag} \left\{ h_8(-f_1), \dots, h_8(-f_r) \right\}, \\
\boldsymbol{C} = \operatorname{diag} \left\{ \left[ \frac{\sqrt{2} + 1}{f_1} \right], \dots, \left[ \frac{\sqrt{2} + 1}{f_r} \right] \right\} = \operatorname{diag} \left\{ 1 - h_8(-f_1), \dots, 1 - h_8(-f_r) \right\}.$$

• 因此 
$$oldsymbol{X} = \begin{pmatrix} * & oldsymbol{I} \ oldsymbol{I} & oldsymbol{O} \end{pmatrix}$$
 可逆, Cassels 配对非退化.

• 我们来看偶数 2n 情形.

- 我们来看偶数 2n 情形.
- 此时在假设条件下,

$$\mathbf{R}_{-2n} = \operatorname{diag}\{\mathbf{A}_n, 0\} = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots, \mathbf{A}_{f_r}, 0\}.$$

- 我们来看偶数 2n 情形.
- 此时在假设条件下,

$$\mathbf{R}_{-2n} = \operatorname{diag}\{\mathbf{A}_n, 0\} = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots, \mathbf{A}_{f_r}, 0\}.$$

• 所以  $h_4(-2n) = r$  且  $\mathcal{A}_{-2n}[2] \cap \mathcal{A}_{-2n}^2$  由  $\theta_{-2n}(f_1), \ldots, \theta_{-2n}(f_{r-1})$  生成.

- 我们来看偶数 2n 情形.
- 此时在假设条件下,

$$\mathbf{R}_{-2n} = \operatorname{diag}\{\mathbf{A}_n, 0\} = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots, \mathbf{A}_{f_r}, 0\}.$$

- 所以  $h_4(-2n) = r$  且  $\mathcal{A}_{-2n}[2] \cap \mathcal{A}_{-2n}^2$  由  $\theta_{-2n}(f_1), \ldots, \theta_{-2n}(f_{r-1})$  生成.
- 由  $h_8(-2n) = r$  可知它们都属于  $\mathcal{A}_{-2n}^4$ .

- 我们来看偶数 2n 情形.
- 此时在假设条件下,

$$\mathbf{R}_{-2n} = \operatorname{diag}\{\mathbf{A}_n, 0\} = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots, \mathbf{A}_{f_r}, 0\}.$$

- 所以  $h_4(-2n) = r$  且  $\mathcal{A}_{-2n}[2] \cap \mathcal{A}_{-2n}^2$  由  $\theta_{-2n}(f_1), \ldots, \theta_{-2n}(f_{r-1})$  生成.
- 由  $h_8(-2n) = r$  可知它们都属于  $\mathcal{A}_{-2n}^4$ .
- 从而  $oldsymbol{b}_{n,\gamma_i}\in\operatorname{Im}oldsymbol{A}_n$ ,

$$0 = \mathbf{1}^{\mathrm{T}} \boldsymbol{b}_{f_j, \gamma_i} = \left[\frac{\gamma_i}{f_j}\right].$$

- 我们来看偶数 2n 情形.
- 此时在假设条件下,

$$\mathbf{R}_{-2n} = \operatorname{diag}\{\mathbf{A}_n, 0\} = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots, \mathbf{A}_{f_r}, 0\}.$$

- 所以  $h_4(-2n) = r$  且  $\mathcal{A}_{-2n}[2] \cap \mathcal{A}_{-2n}^2$  由  $\theta_{-2n}(f_1), \ldots, \theta_{-2n}(f_{r-1})$  生成.
- 由  $h_8(-2n) = r$  可知它们都属于  $\mathcal{A}_{-2n}^4$ .
- 从而  $oldsymbol{b}_{n,\gamma_i}\in\operatorname{Im}oldsymbol{A}_n$ ,

$$0 = \mathbf{1}^{\mathrm{T}} \boldsymbol{b}_{f_j, \gamma_i} = \left[\frac{\gamma_i}{f_j}\right].$$

• 奇数情形类似.

