



南京大學
NANJING UNIVERSITY

含非同余数因子的非同余数

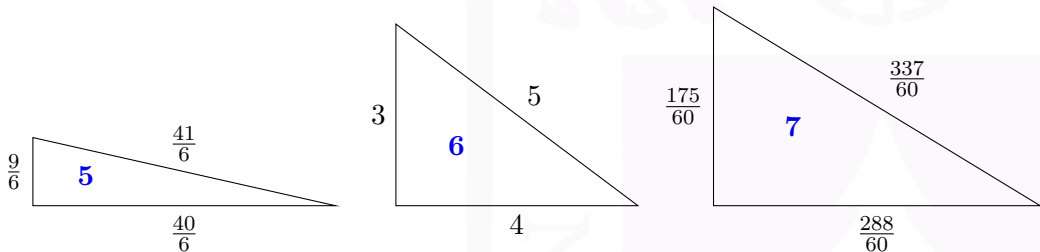
张神星 (合肥工业大学)

2025 南京大学数论与自守表示研讨会

zhangshenxing@hfut.edu.cn

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**. congruent number



- 显然我们只需要考虑无平方因子正整数.
- 设直角三角形的三条边分别为 a, b, c , 设 $x = \frac{n(a-c)}{b}, y = \frac{2nx}{b}$.

- 显然我们只需要考虑无平方因子正整数.
- 设直角三角形的三条边分别为 a, b, c , 设 $x = \frac{n(a-c)}{b}, y = \frac{2nx}{b}$.
- 那么由勾股定理 $a^2 + b^2 = c^2$ 可得 $a = \frac{x^2 - n^2}{y}, b = \frac{2nx}{y}$.

- 显然我们只需要考虑无平方因子正整数.
- 设直角三角形的三条边分别为 a, b, c , 设 $x = \frac{n(a-c)}{b}, y = \frac{2nx}{b}$.
- 那么由勾股定理 $a^2 + b^2 = c^2$ 可得 $a = \frac{x^2 - n^2}{y}, b = \frac{2nx}{y}$.
- 于是 $n = \frac{1}{2}ab = \frac{x^3 - n^2x}{y^2}$.

- 显然我们只需要考虑无平方因子正整数.
- 设直角三角形的三条边分别为 a, b, c , 设 $x = \frac{n(a-c)}{b}, y = \frac{2nx}{b}$.
- 那么由勾股定理 $a^2 + b^2 = c^2$ 可得 $a = \frac{x^2 - n^2}{y}, b = \frac{2nx}{y}$.
- 于是 $n = \frac{1}{2}ab = \frac{x^3 - n^2x}{y^2}$.
- 换言之, (x, y) 是椭圆曲线

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

的一个满足 $y \neq 0$ 的有理点.

- 显然我们只需要考虑无平方因子正整数.
- 设直角三角形的三条边分别为 a, b, c , 设 $x = \frac{n(a-c)}{b}, y = \frac{2nx}{b}$.
- 那么由勾股定理 $a^2 + b^2 = c^2$ 可得 $a = \frac{x^2 - n^2}{y}, b = \frac{2nx}{y}$.
- 于是 $n = \frac{1}{2}ab = \frac{x^3 - n^2x}{y^2}$.
- 换言之, (x, y) 是椭圆曲线

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

的一个满足 $y \neq 0$ 的有理点.

- 而 $E_n(\mathbb{Q})$ 全体构成有限生成交换群, 且挠群为

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

- 显然我们只需要考虑无平方因子正整数.
- 设直角三角形的三条边分别为 a, b, c , 设 $x = \frac{n(a-c)}{b}, y = \frac{2nx}{b}$.
- 那么由勾股定理 $a^2 + b^2 = c^2$ 可得 $a = \frac{x^2 - n^2}{y}, b = \frac{2nx}{y}$.
- 于是 $n = \frac{1}{2}ab = \frac{x^3 - n^2x}{y^2}$.
- 换言之, (x, y) 是椭圆曲线

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

的一个满足 $y \neq 0$ 的有理点.

- 而 $E_n(\mathbb{Q})$ 全体构成有限生成交换群, 且挠群为

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

- 故 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.

- 我们可以利用 Selmer 群来估计 $E_n(\mathbb{Q})$ 的秩.

- $$\text{III}(E_n) := \text{Ker}\left(H^1(G_{\mathbb{Q}}, E_n) \rightarrow \prod_v H^1(G_{\mathbb{Q}_v}, E_n)\right).$$

- 

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(G_{\mathbb{Q}}, E_n)$$

$$\dim_{\mathbb{F}_2} S$$

$$\dim_{\mathbb{F}_2} \mathcal{S}$$

$\dim_{\mathbb{F}_2} S$

非同余数: $s_2(n) = 0$ 情形

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

非同余数: $s_2(n) = 0$ 情形

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

非同余数: $s_2(n) = 0$ 情形

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

非同余数: $s_2(n) = 0$ 情形

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

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

且此时 BSD 猜想 2 部分成立.

非同余数: $s_2(n) = 0$ 情形

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

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

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 $\text{III}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n) = 1, h_8(-n) \equiv (d-1)/4 \pmod{2}$,

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 $\text{III}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n) = 1, h_8(-n) \equiv (d-1)/4 \pmod{2}$,

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 ± 1 素数乘积, 则下述等价:

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

定理 (Zhang 2023)

若 n 是模 8 余 ± 1 素数乘积, 则下述等价:

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

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

定理 (Zhang 2023)

若 n 是模 8 余 ± 1 素数乘积, 则下述等价:

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

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

- 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 ± 1 素数乘积, 则下述等价:

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

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

- 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 $p \equiv 1 \pmod{8}$ 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 $\text{III}(E_p/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/4\mathbb{Z})^2$.

- 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, 我们希望能从一个满足 $s_2(Q) = 0$ 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 $p_i \equiv 1 \pmod{8}$.

假设

- 假设存在 \mathbb{F}_2 上的向量 $\mathbf{u} = (u_1, \dots, u_k)^T$, $\mathbf{v} = (v_1, \dots, v_\ell)^T$,

假设

- 假设存在 \mathbb{F}_2 上的向量 $\mathbf{u} = (u_1, \dots, u_k)^T$, $\mathbf{v} = (v_1, \dots, v_\ell)^T$,
- 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 $\log: \{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.
- 换言之, 定义矩阵

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

假设

- 假设存在 \mathbb{F}_2 上的向量 $\mathbf{u} = (u_1, \dots, u_k)^T$, $\mathbf{v} = (v_1, \dots, v_\ell)^T$,
- 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 $\log: \{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.
- 换言之, 定义矩阵

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

- 并类似定义 A_Q, A_n , 则

$$\mathbf{A}_n = \begin{pmatrix} \mathbf{A}_P + \mathbf{U}_P & \mathbf{u}\mathbf{v}^\top \\ \mathbf{v}\mathbf{u}^\top & \mathbf{A}_Q \end{pmatrix},$$

其中 $\mathbf{1}^\top \mathbf{u} = 0, \mathbf{1}^\top \mathbf{v} = 1, \mathbf{U}_P = \text{diag}\{u_1, \dots, u_k\}$.

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 $\text{III}(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $\text{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$ 且 $\left[\frac{\gamma}{d}\right] = \left[\frac{\sqrt{2}+1}{d}\right] + 1$,

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 $\text{III}(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $\text{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$ 且 $\left[\frac{\gamma}{d}\right] = \left[\frac{\sqrt{2}+1}{d}\right] + 1$,

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 $\text{III}(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-P) = 1$ 且 $\left[\frac{\gamma}{P}\right] = h_8(-P)$;
- $h_4(-P) = 1$ 且 $\left[\frac{\gamma}{P}\right] = r_4(K_2\mathcal{O}_P)$,

其中 (α, β, γ) 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 $\text{III}(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n) = 1$ 且 $h_8(-n) = 0$;
- $r_4(K_2\mathcal{O}_n) = 0$.

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

- $h_4(-f_i) = 1, h_8(-f_i) = 0, \forall i$;
- $h_8(-n) = r$; 或 $h_8(-n) = r - 1, [(2, \sqrt{-n})] \notin \mathcal{A}_{-n}^4$;
- $\left[\frac{p}{p'}\right] = 0$, 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 $\text{III}(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$.

(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 $\text{III}(E_{2n}) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$.

- 通过对这些齐性空间可解性的分析, Monsky 将 $\text{Sel}'_2(E_n)$ 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, $\text{Sel}'_2(E_n)$ 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

$$\begin{aligned} \mathrm{Sel}'_2(E_n) &\rightarrow \mathrm{Ker} M_n, & M_n &= \begin{pmatrix} A_n + D_{n,2} & D_{n,2} \\ D_{n,2} & A_n + D_{n,-2} \end{pmatrix} \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \psi_n(d_2) \\ \psi_n(d_1) \end{pmatrix}, \end{aligned}$$

- 通过对这些齐性空间可解性的分析, Monsky 将 $\text{Sel}'_2(E_n)$ 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, $\text{Sel}'_2(E_n)$ 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

$$\mathrm{Sel}'_2(E_n) \rightarrow \mathrm{Ker} M_n, \quad M_n = \begin{pmatrix} A_n + D_{n,2} & D_{n,2} \\ D_{n,2} & A_n + D_{n,-2} \end{pmatrix}$$

$$(d_1, d_2, d_3) \mapsto \begin{pmatrix} \psi_n(d_2) \\ \psi_n(d_1) \end{pmatrix},$$

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

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

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

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

- 仅知道 $s_2(n) = \text{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \text{III}(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\text{Sel}'_2(E_n)$ 上定义了一个 (反) 对称双线性型 $\langle -, - \rangle \in \mathbb{F}_2$.
- 对于 $\Lambda \in \text{Sel}_2(E_n)$, 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 $s_2(n) = \text{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \text{III}(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\text{Sel}'_2(E_n)$ 上定义了一个 (反) 对称双线性型 $\langle -, - \rangle \in \mathbb{F}_2$.
- 对于 $\Lambda \in \text{Sel}_2(E_n)$, 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 $\Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}_2(E_n)$, 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 $s_2(n) = \text{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} \text{III}(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\text{Sel}'_2(E_n)$ 上定义了一个 (反) 对称双线性型 $\langle -, - \rangle \in \mathbb{F}_2$.
- 对于 $\Lambda \in \text{Sel}_2(E_n)$, 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 $\Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}_2(E_n)$, 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 $P_v \in D_\Lambda(\mathbb{Q}_v)$.

引理 (Wang2016)

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

引理 (Wang2016)

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

- 由正合列

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

得到长正合列

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

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

引理 (Wang2016)

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

- 由正合列

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

得到长正合列

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

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

- $\cdot + U_P)$.

$\cdot + U_P)$.

$\cdot + U_P)$.

- $+ U_P).$
- 情形类似,

$+ U_P).$

情形类似,

$+ U_P).$

情形类似,

- $+ U_P).$
- 情形类似,

- 现在我们开始证明主要结果.

引理

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

- 我们只证明 n 是奇数的情形, 偶数情形类似,
- 设

$$\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} \in \operatorname{Ker} M_n = \operatorname{Ker} \begin{pmatrix} A_P + U_P & uv^T & O_k & \\ vu^T & A_Q + D_{Q,2} & & D_{Q,2} \\ O_k & & A_P + U_P & uv^T \\ & D_{Q,2} & vu^T & A_Q + D_{Q,-2} \end{pmatrix}.$$

- 则

$$(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{u}\mathbf{v}^T\mathbf{y}, \quad (\mathbf{A}_P + \mathbf{U}_P)\mathbf{z} = \mathbf{u}\mathbf{v}^T\mathbf{w}$$

$$M_Q \begin{pmatrix} y \\ w \end{pmatrix} = \begin{pmatrix} vu^T x \\ vu^T z \end{pmatrix}.$$

- 则

$$(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{u}\mathbf{v}^T\mathbf{y}, \quad (\mathbf{A}_P + \mathbf{U}_P)\mathbf{z} = \mathbf{u}\mathbf{v}^T\mathbf{w}$$

$$M_Q \begin{pmatrix} y \\ w \end{pmatrix} = \begin{pmatrix} vu^T x \\ vu^T z \end{pmatrix}.$$

- 从 $\mathbf{1}^T(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{1}^T\mathbf{u}\mathbf{v}^T\mathbf{y}$ 得到 $\mathbf{u}^T\mathbf{x} = 0$. (假设 $\mathbf{1}^T\mathbf{u} = 0$)

- 则

$$(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{u}\mathbf{v}^T\mathbf{y}, \quad (\mathbf{A}_P + \mathbf{U}_P)\mathbf{z} = \mathbf{u}\mathbf{v}^T\mathbf{w}$$

$$M_Q \begin{pmatrix} y \\ w \end{pmatrix} = \begin{pmatrix} vu^T x \\ vu^T z \end{pmatrix}.$$

- 从 $\mathbf{1}^T(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{1}^T\mathbf{u}\mathbf{v}^T\mathbf{y}$ 得到 $\mathbf{u}^T\mathbf{x} = 0$. (假设 $\mathbf{1}^T\mathbf{u} = 0$)
- 同理 $\mathbf{u}^T\mathbf{z} = 0$, 故 $M_Q \begin{pmatrix} \mathbf{y} \\ \mathbf{w} \end{pmatrix} = \mathbf{0}$.

- 则

$$(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{u}\mathbf{v}^T\mathbf{y}, \quad (\mathbf{A}_P + \mathbf{U}_P)\mathbf{z} = \mathbf{u}\mathbf{v}^T\mathbf{w}$$

$$M_Q \begin{pmatrix} y \\ w \end{pmatrix} = \begin{pmatrix} vu^T x \\ vu^T z \end{pmatrix}.$$

- 从 $\mathbf{1}^T(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{1}^T\mathbf{u}\mathbf{v}^T\mathbf{y}$ 得到 $\mathbf{u}^T\mathbf{x} = 0$. (假设 $\mathbf{1}^T\mathbf{u} = 0$)
- 同理 $\mathbf{u}^T\mathbf{z} = 0$, 故 $M_Q \begin{pmatrix} \mathbf{y} \\ \mathbf{w} \end{pmatrix} = \mathbf{0}$.
- 由于 $s_2(Q) = 0$, M_Q 可逆, 从而 $\mathbf{y} = \mathbf{w} = \mathbf{0}$,

- 则

$$(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{u}\mathbf{v}^T\mathbf{y}, \quad (\mathbf{A}_P + \mathbf{U}_P)\mathbf{z} = \mathbf{u}\mathbf{v}^T\mathbf{w}$$

$$M_Q \begin{pmatrix} y \\ w \end{pmatrix} = \begin{pmatrix} vu^T x \\ vu^T z \end{pmatrix}.$$

- 从 $\mathbf{1}^T(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{1}^T\mathbf{u}\mathbf{v}^T\mathbf{y}$ 得到 $\mathbf{u}^T\mathbf{x} = 0$. (假设 $\mathbf{1}^T\mathbf{u} = 0$)
- 同理 $\mathbf{u}^T\mathbf{z} = 0$, 故 $M_Q \begin{pmatrix} \mathbf{y} \\ \mathbf{w} \end{pmatrix} = \mathbf{0}$.
- 由于 $s_2(Q) = 0$, M_Q 可逆, 从而 $\mathbf{y} = \mathbf{w} = \mathbf{0}$,
- $\mathbf{x}, \mathbf{z} \in \text{Ker}(\mathbf{A}_P + \mathbf{U}_P)$, $s_2(n) = 2 \text{corank}(\mathbf{A}_P + \mathbf{U}_P)$.

- 则

$$(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{u}\mathbf{v}^T\mathbf{y}, \quad (\mathbf{A}_P + \mathbf{U}_P)\mathbf{z} = \mathbf{u}\mathbf{v}^T\mathbf{w}$$

$$M_Q \begin{pmatrix} y \\ w \end{pmatrix} = \begin{pmatrix} vu^T x \\ vu^T z \end{pmatrix}.$$

- 从 $\mathbf{1}^T(\mathbf{A}_P + \mathbf{U}_P)\mathbf{x} = \mathbf{1}^T\mathbf{u}\mathbf{v}^T\mathbf{y}$ 得到 $\mathbf{u}^T\mathbf{x} = 0$. (假设 $\mathbf{1}^T\mathbf{u} = 0$)
- 同理 $\mathbf{u}^T\mathbf{z} = 0$, 故 $M_Q \begin{pmatrix} \mathbf{y} \\ \mathbf{w} \end{pmatrix} = \mathbf{0}$.
- 由于 $s_2(Q) = 0$, M_Q 可逆, 从而 $\mathbf{y} = \mathbf{w} = \mathbf{0}$,
- $\mathbf{x}, \mathbf{z} \in \text{Ker}(\mathbf{A}_P + \mathbf{U}_P)$, $s_2(n) = 2 \text{corank}(\mathbf{A}_P + \mathbf{U}_P)$.
- 由此可立得主要结论中 $s_2(n) = 0$ 的情形.

[illegible]
$$+ U_P). \quad \text{令}$$

1. *Journal of the American Medical Association*, 2000; 284: 2689-2695.

the 1990s, the number of people in the United States who are 65 years of age or older has increased by 50 percent, and the number of people 75 years of age or older has increased by 75 percent. The number of people 85 years of age or older has increased by 150 percent.

[illegible]

$$\frac{n}{f_i} \beta_i'^2 = 4\gamma_i'^2$$

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

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

- 取

$$Q_1 = (\beta'_i, f_i \alpha'_i, 2\gamma'_i) \in H_1(\mathbb{Q}),$$

$$L_1 = \frac{n}{f_i} \beta'_i t - \alpha'_i u_2 + 2\gamma'_i u_3,$$

$$Q_2 = (0, 1, -1) \in H_2(\mathbb{Q}),$$

$$L_2 = u_3 + u_1.$$

Cassles 配对的计算 (再续)

- 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.
- $[L_1(P_v), f_t]_v = [\beta'_i \frac{n}{f_i} + 2\gamma'_i \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma'_i \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma'_i \sqrt{-\frac{n}{f_i}}, f_t]_v$.

Cassles 配对的计算 (再续)

- 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.
- $[L_1(P_v), ft]_v = [\beta'_i \frac{n}{f_i} + 2\gamma'_i \sqrt{-\frac{n}{f_i}}, ft]_v = [4\gamma'_i \sqrt{-\frac{n}{f_i}}, ft]_v = [\gamma'_i \sqrt{-\frac{n}{f_i}}, ft]_v$.
- $[L_2(P_v), ft]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, ft]_v$,

Cassles 配对的计算 (再续)

- 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.
- $[L_1(P_v), ft]_v = [\beta'_i \frac{n}{f_i} + 2\gamma'_i \sqrt{-\frac{n}{f_i}}, ft]_v = [4\gamma'_i \sqrt{-\frac{n}{f_i}}, ft]_v = [\gamma'_i \sqrt{-\frac{n}{f_i}}, ft]_v$.
- $[L_2(P_v), ft]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, ft]_v, \quad [L_1 L_2(P_v), ft]_v = [(\sqrt{2} + 1)\gamma'_i, ft]_v$.

- 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.
- $[L_1(P_v), f_t]_v = [\beta'_i \frac{n}{f_i} + 2\gamma'_i \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma'_i \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma'_i \sqrt{-\frac{n}{f_i}}, f_t]_v$.
- $[L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\sqrt{-\frac{n}{f_i}}, f_t]_v$, $[L_1 L_2(P_v), f_t]_v = [(\sqrt{2} + 1)\gamma'_i, f_t]_v$.
- 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 $[L_1 L_2(P_v), f_t]_v = [\gamma'_i, f_t]_v$.

主要结论: $s_2(n) = 2$ 情形

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

主要结论: $s_2(n) = 2$ 情形

- 根据前面的计算 $s_2(n) = 2 \iff \text{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$.
- 此时 $\text{Sel}'_2(E_n)$ 由 $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$ 生成, 其中 $\psi_P(d) \in \text{Ker}(\mathbf{A}_P + \mathbf{U}_P)$.

主要结论: $s_2(n) = 2$ 情形

- 根据前面的计算 $s_2(n) = 2 \iff \text{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$.
- 此时 $\text{Sel}'_2(E_n)$ 由 $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$ 生成, 其中 $\psi_P(d) \in \text{Ker}(\mathbf{A}_P + \mathbf{U}_P)$.
- 于是 $\langle \Lambda, \Lambda' \rangle = \left[\frac{\sqrt{2} + 1}{d} \right] + \left[\frac{\gamma}{d} \right]$.

主要结论: $s_2(n) = 2$ 情形

- 根据前面的计算 $s_2(n) = 2 \iff \text{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$.
- 此时 $\text{Sel}'_2(E_n)$ 由 $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$ 生成, 其中 $\psi_P(d) \in \text{Ker}(\mathbf{A}_P + \mathbf{U}_P)$.
- 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.
- 设 $n = p_1 \cdots p_k \equiv 1 \pmod{4}$.

- 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.
- 设 $n = p_1 \cdots p_k \equiv 1 \pmod{4}$.
- 根据高斯型理论, $h_2(-n) = k + 1$, $h_4(-n) = \text{corank } \mathbf{R}_{-n} - 1$,

- 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.
- 设 $n = p_1 \cdots p_k \equiv 1 \pmod{4}$.
- 根据高斯型理论, $h_2(-n) = k + 1$, $h_4(-n) = \text{corank } \mathbf{R}_{-n} - 1$,
- 其中 R edei 矩阵 $\mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A}_n & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-1}^\text{T} & \begin{bmatrix} 2 \\ - \\ n \end{bmatrix} \end{pmatrix}$, $\mathbf{b}_{n,\varepsilon} = \mathbf{D}_{n,\varepsilon} \mathbf{1}$.

- 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.
- 设 $n = p_1 \cdots p_k \equiv 1 \pmod{4}$.
- 根据高斯型理论, $h_2(-n) = k + 1$, $h_4(-n) = \text{corank } \mathbf{R}_{-n} - 1$,
- 其中 R edei 矩阵 $\mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A}_n & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-1}^\text{T} & \begin{bmatrix} 2 \\ -n \end{bmatrix} \end{pmatrix}$, $\mathbf{b}_{n,\varepsilon} = \mathbf{D}_{n,\varepsilon} \mathbf{1}$.
- 对于 $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2]$, $\theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \mathbf{b}_{n,\gamma} \in \text{Im } \mathbf{R}'_{-n}$.
- 这里 \mathbf{R}'_{-n} 是 \mathbf{R}_{-n} 去掉最后一行, (α, β, γ) 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.
- 设 $n = p_1 \cdots p_k \equiv 1 \pmod{4}$.
- 根据高斯型理论, $h_2(-n) = k + 1$, $h_4(-n) = \text{corank } \mathbf{R}_{-n} - 1$,
- 其中 R edei 矩阵 $\mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A}_n & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-1}^\text{T} & \begin{bmatrix} 2 \\ -n \end{bmatrix} \end{pmatrix}$, $\mathbf{b}_{n,\varepsilon} = \mathbf{D}_{n,\varepsilon} \mathbf{1}$.
- 对于 $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2]$, $\theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \mathbf{b}_{n,\gamma} \in \text{Im } \mathbf{R}'_{-n}$.
- 这里 \mathbf{R}'_{-n} 是 \mathbf{R}_{-n} 去掉最后一行, (α, β, γ) 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.

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

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

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

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

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

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

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

主要结论: $s_2(n) = 2k$ 情形

- 此时 $\mathbf{A}_P + \mathbf{U}_P = \mathbf{A}_P = \text{diag}\{\mathbf{A}_{f_1}, \dots, \mathbf{A}_{f_r}\}$.
- 由 $h_4(-f_i) = 1$ 可知 $\text{corank } \mathbf{A}_{f_i} = 1$, $s_2(n) = 2r$.
- 此时由 $\text{Ker } \mathbf{M}_n$ 可知 $\text{Sel}'_2(E_n)$ 由 $\Lambda_i = (f_i, 1, f_i), \Lambda'_i = (f_i, f_i, 1)$ 生成.

主要结论: $s_2(n) = 2k$ 情形

- 此时 $\mathbf{A}_P + \mathbf{U}_P = \mathbf{A}_P = \text{diag}\{\mathbf{A}_{f_1}, \dots, \mathbf{A}_{f_r}\}$.
- 由 $h_4(-f_i) = 1$ 可知 $\text{corank } \mathbf{A}_{f_i} = 1$, $s_2(n) = 2r$.
- 此时由 $\text{Ker } M_n$ 可知 $\text{Sel}'_2(E_n)$ 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

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

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

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



主要结论: $s_2(n) = 2k$ 情形

- 此时 $\mathbf{A}_P + \mathbf{U}_P = \mathbf{A}_P = \text{diag}\{\mathbf{A}_{f_1}, \dots, \mathbf{A}_{f_r}\}$.
- 由 $h_4(-f_i) = 1$ 可知 $\text{corank } \mathbf{A}_{f_i} = 1, s_2(n) = 2r$.
- 此时由 $\text{Ker } \mathbf{M}_n$ 可知 $\text{Sel}'_2(E_n)$ 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

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

$$\mathbf{B} = \left(\begin{bmatrix} \gamma_i \\ f_j \end{bmatrix} \right)_{r \times r} = \text{diag} \left\{ h_8(-f_1), \dots, h_8(-f_r) \right\},$$

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

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

推论: $s_2(2n) = 2k$ 情形

- 我们来看偶数 $2n$ 情形.

推论: $s_2(2n) = 2k$ 情形

- 我们来看偶数 $2n$ 情形.
- 此时在假设条件下,

$$R_{-2n} = \text{diag}\{\mathbf{A}_n, 0\} = \text{diag}\{\mathbf{A}_{f_1}, \dots, \mathbf{A}_{f_r}, 0\}.$$

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

推论: $s_2(2n) = 2k$ 情形

- 我们来看偶数 $2n$ 情形.
- 此时在假设条件下,

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

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

$$0 = \mathbf{1}^T \mathbf{b}_{f_j, \gamma_i} = \begin{bmatrix} \gamma_i \\ f_j \end{bmatrix}.$$

推论: $s_2(2n) = 2k$ 情形

- 我们来看偶数 $2n$ 情形.
- 此时在假设条件下,

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

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

$$0 = \mathbf{1}^T \mathbf{b}_{f_j, \gamma_i} = \begin{bmatrix} \gamma_i \\ f_j \end{bmatrix}.$$

- 奇数情形类似.

謝 謝