含非同余数因子的非同余数

张神星 (合肥工业大学)

2026 年山东大学数论研讨会

zhangshenxing@hfut.edu.cn

同余数问题

- 同余数问题是一个古老的数学问题.

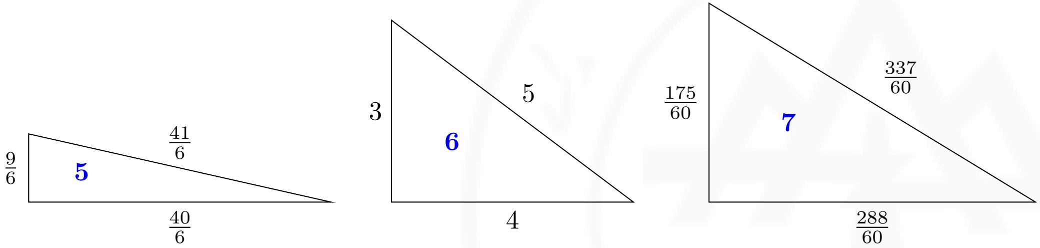
- 同余数问题是一个古老的数学问题.
- 如果正整数 n 可以表达为一个有理边长直角三角形的面积, 则称 n 是**同余数** (congruent number).

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.

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.



同余数与椭圆曲线

- 设直角三角形的三条边分别为 a, b, c, 则 $(x, y) = \left(\frac{n(a-c)}{b}, \frac{2nx}{b}\right)$ 是椭圆曲线

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

  的一个满足 $y \neq 0$ 的有理点.

- 设直角三角形的三条边分别为 a, b, c, 则 $(x, y) = \left(\frac{n(a-c)}{b}, \frac{2nx}{b}\right)$ 是椭圆曲线

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

的一个满足 $y \neq 0$ 的有理点.

- 反之, 若 (x, y) 是椭圆曲线 E_n 的一个满足 $y \neq 0$ 的有理点, 则

$$(a, b, c) = \left(\left|\frac{x^2 - n^2}{y}\right|, \left|\frac{2nx}{y}\right|, \left|\frac{x^2 - n^2}{y}\right|\right)$$

是一个面积为 n 的直角三角形的三条边.

- 设直角三角形的三条边分别为 a, b, c, 则 $(x, y) = \left(\frac{n(a-c)}{b}, \frac{2nx}{b}\right)$ 是椭圆曲线

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

  的一个满足 $y \neq 0$ 的有理点.
- 反之, 若 (x, y) 是椭圆曲线 E_n 的一个满足 $y \neq 0$ 的有理点, 则

$$(a, b, c) = \left(\left|\frac{x^2 - n^2}{y}\right|, \left|\frac{2nx}{y}\right|, \left|\frac{x^2 - n^2}{y}\right|\right)$$

  是一个面积为 n 的直角三角形的三条边.
- 而 $E_n(\mathbb{Q})$ 全体构成有限生成交换群, 且挠群为

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

- 设直角三角形的三条边分别为 a,b,c, 则 $(x,y)=\left(\frac{n(a-c)}{b},\frac{2nx}{b}\right)$ 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.
- 反之, 若 (x,y) 是椭圆曲线 E_n 的一个满足 $y\neq 0$ 的有理点, 则

$$(a,b,c)=\left(\left|\frac{x^2-n^2}{y}\right|,\left|\frac{2nx}{y}\right|,\left|\frac{x^2-n^2}{y}\right|\right)$$

  是一个面积为 n 的直角三角形的三条边.
- 而 $E_n(\mathbb{Q})$ 全体构成有限生成交换群, 且挠群为

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

- 故 n **是同余数** $\Longleftrightarrow$ $E_n(\mathbb{Q})$ **是无限群** $\Longleftrightarrow$ $\mathrm{rank}_{\mathbb{Z}}\,E_n(\mathbb{Q})>0$;

- 设直角三角形的三条边分别为 a, b, c, 则 $(x, y) = \left(\frac{n(a-c)}{b}, \frac{2nx}{b}\right)$ 是椭圆曲线

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

的一个满足 $y \neq 0$ 的有理点.

- 反之, 若 (x, y) 是椭圆曲线 E_n 的一个满足 $y \neq 0$ 的有理点, 则

$$(a, b, c) = \left(\left|\frac{x^2 - n^2}{y}\right|, \left|\frac{2nx}{y}\right|, \left|\frac{x^2 - n^2}{y}\right|\right)$$

是一个面积为 n 的直角三角形的三条边.

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

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

- 故 n **是同余数** $\iff$ $E_n(\mathbb{Q})$ **是无限群** $\iff$ $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) > 0$;
- n **是非同余数** $\iff$ $E_n(\mathbb{Q}) = E_n[2]$ $\iff$ $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$.

- 我们可以利用 Selmer 群的大小来控制 $E_n(\mathbb{Q})$ 的秩.

- 我们可以利用 Selmer 群的大小来控制 $E_n(\mathbb{Q})$ 的秩.
- 通过对短正合列 $0 \to E_n[2] \to E_n \xrightarrow{\times 2} E_n \to 0$ 取 $G_{\mathbb{Q}}$ 上同调可得

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

其中

$$\mathrm{Sel}_2(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n[2]) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big),$$

$$Ш(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big).$$

- 我们可以利用 Selmer 群的大小来控制 $E_n(\mathbb{Q})$ 的秩.
- 通过对短正合列 $0 \to E_n[2] \to E_n \xrightarrow{\times 2} E_n \to 0$ 取 $G_{\mathbb{Q}}$ 上同调可得

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

其中

$$\mathrm{Sel}_2(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n[2]) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big),$$

$$Ш(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big).$$

- 故 $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) \leqslant \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_n) - 2$,

- 我们可以利用 Selmer 群的大小来控制 $E_n(\mathbb{Q})$ 的秩.
- 通过对短正合列 $0 \to E_n[2] \to E_n \xrightarrow{\times 2} E_n \to 0$ 取 $G_{\mathbb{Q}}$ 上同调可得

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

其中

$$\mathrm{Sel}_2(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n[2]) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big),$$

$$Ш(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big).$$

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

- 我们可以利用 Selmer 群的大小来控制 $E_n(\mathbb{Q})$ 的秩.
- 通过对短正合列 $0 \to E_n[2] \to E_n \xrightarrow{\times 2} E_n \to 0$ 取 $G_{\mathbb{Q}}$ 上同调可得

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

其中

$$\mathrm{Sel}_2(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n[2]) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big),$$

$$Ш(E_n) := \mathrm{Ker}\Big(\mathrm{H}^1(G_{\mathbb{Q}}, E_n) \to \prod_v \mathrm{H}^1(G_{\mathbb{Q}_v}, E_n)\Big).$$

- 故 $\mathrm{rank}_{\mathbb{Z}}\, E_n(\mathbb{Q}) \leqslant \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_n) - 2 = \dim_{\mathbb{F}_2} \mathrm{Sel}_2'(E_n) =: s_2(n)$,
- 其中 $\mathrm{Sel}_2'(E_n) := \dfrac{\mathrm{Sel}_2(E_n)}{E_n(\mathbb{Q})[2]}$.

$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0 \underset{\text{Coates-Wiles}}{\overset{\text{BSD 猜想}}{\rightleftarrows}} L(E_n, 1) \neq 0 \implies n \equiv 1, 2, 3 \bmod 8$$

$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0 \underset{\text{Coates-Wiles}}{\overset{\text{BSD 猜想}}{\rightleftarrows}} L(E_n, 1) \neq 0 \implies n \equiv 1, 2, 3 \bmod 8 \implies s_2(n) \text{ 是偶数}$$

$$\mathrm{rank}_{\mathbb{Z}}\, E_n(\mathbb{Q})=0 \underset{\text{Coates-Wiles}}{\overset{\text{BSD 猜想}}{\rightleftarrows}} L(E_n,1)\neq 0 \implies n\equiv 1,2,3 \bmod 8 \implies s_2(n) \text{ 是偶数}$$

- 自然地, $s_2(n)=0 \implies n$ 是非同余数且 $Ш(E_n)[2^\infty]=0$.

非同余数: $s_2(n) = 0$ 情形

$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0 \underset{\text{Coates-Wiles}}{\overset{\text{BSD 猜想}}{\rightleftarrows}} L(E_n, 1) \neq 0 \implies n \equiv 1, 2, 3 \bmod 8 \implies s_2(n) \text{ 是偶数}$$

- 自然地, $s_2(n) = 0 \implies n$ 是非同余数且 $Ш(E_n)[2^\infty] = 0$.
- 此时由 Tian-Yuan-Zhang (2017) 和 Smith (2016), 它等价于

$$\sum_{\substack{n = d_0 d_1 \cdots d_k \\ d_1 \equiv \cdots \equiv d_k \equiv 1 \bmod 8 \\ h_4(-d_i) = 0, \forall i}} 1 = 1 \in \mathbb{F}_2,$$

且此时 BSD 猜想 2 部分成立.

非同余数: $s_2(n)=0$ 情形

$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q})=0 \underset{\text{Coates-Wiles}}{\overset{\text{BSD 猜想}}{\rightleftarrows}} L(E_n,1)\neq 0 \implies n\equiv 1,2,3 \bmod 8 \implies s_2(n) \text{ 是偶数}$$

- 自然地, $s_2(n)=0 \implies n$ 是非同余数且 $Ш(E_n)[2^\infty]=0$.
- 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,

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

非同余数: $s_2(n) = 2$ 情形

- $s_2(n) = 2r > 0$ 情形目前尚无对 n 的完整刻画.

- $s_2(n) = 2r > 0$ 情形目前尚无对 n 的完整刻画.
- 不过, 若 n 的素因子落在特定的同余类中, 有下列结果:

- $s_2(n)=2r>0$ 情形目前尚无对 n 的完整刻画.
- 不过, 若 n 的素因子落在特定的同余类中, 有下列结果:

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

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-Z 2022)

若 n 是模 8 余 ± 1 素数乘积, 则下述等价:

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

定理 (Wang-Z 2022)

若 n 是模 8 余 ± 1 素数乘积，则下述等价:

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

定理 (Z 2023, Z 2026)

若 n 是模 8 余 ± 1 素数乘积，则下述等价:

- $2n$ 是非同余数且 $\text{Ш}(E_{2n})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n) = 1, d \equiv 9 \bmod 16$;
- $h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1$,

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

- 还有其它类似结果, 此处不再列出.

- 还有其它类似结果, 此处不再列出.
- 这些结果均可通过考虑 $\mathrm{Sel}_2'(E_n)$ 上的 Cassels 配对的非退化性来得到.

- 还有其它类似结果, 此处不再列出.
- 这些结果均可通过考虑 $\mathrm{Sel}_2'(E_n)$ 上的 Cassels 配对的非退化性来得到.
- 与此不同的是, Qin (2021) 证明了当素数 $p\equiv 1 \bmod 8$ 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 $\text{Ш}(E_p/\mathbb{Q})[2^\infty]\cong(\mathbb{Z}/4\mathbb{Z})^2$.

非同余数: $s_2(n) = 2$ 情形

- 还有其它类似结果, 此处不再列出.
- 这些结果均可通过考虑 $\mathrm{Sel}_2'(E_n)$ 上的 Cassels 配对的非退化性来得到.
- 与此不同的是, Qin (2021) 证明了当素数 $p \equiv 1 \bmod 8$ 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 $Ш(E_p/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/4\mathbb{Z})^2$.
- 这里, K_2 是 Milnor K 群 (或叫 tame kernel).

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,

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, 这样的结果可以用类群的 4 秩或 8 秩来表达.

- 这些结论都是指定 n 的素因子落在某个同余类中来研究, 这样的结果可以用类群的 4 秩或 8 秩来表达.
- 是否总可以使用 h_4, h_8 或者 $r_4(K_2)$ 等来表达 III 群 2 部分第二小的非同余数呢?

- 这些结论都是指定 n 的素因子落在某个同余类中来研究, 这样的结果可以用类群的 4 秩或 8 秩来表达.
- 是否总可以使用 h_4, h_8 或者 $r_4(K_2)$ 等来表达 III 群 2 部分第二小的非同余数呢?
- 我们考虑一种不同设定下的情形, 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, 这样的结果可以用类群的 4 秩或 8 秩来表达.
- 是否总可以使用 h_4, h_8 或者 $r_4(K_2)$ 等来表达 Ш 群 2 部分第二小的非同余数呢?
- 我们考虑一种不同设定下的情形, 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 $p_i \equiv 1 \bmod 8$.

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, 这样的结果可以用类群的 4 秩或 8 秩来表达.
- 是否总可以使用 h_4, h_8 或者 $r_4(K_2)$ 等来表达 Ш 群 2 部分第二小的非同余数呢?
- 我们考虑一种不同设定下的情形, 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 $p_i\equiv 1 \bmod 8$.
- 设 $Q=\gcd(2,Q)q_1\cdots q_\ell$.

技术性假设

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

技术性假设

- 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 $\sum_i u_i = 0, \sum_j v_j = 1, \left[\dfrac{p_i}{q_j}\right] = u_i v_j$.

技术性假设

- 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 $\sum_i u_i = 0, \sum_j v_j = 1$, $\left[\dfrac{p_i}{q_j}\right] = u_i v_j$.
- 这里 $\left[\dfrac{a}{b}\right] = \log\left(\dfrac{a}{b}\right)$ 是加性勒让德 (雅克比) 符号, 其中 $\log : \{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.

技术性假设

- 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 $\sum_i u_i = 0, \sum_j v_j = 1$, $\left[\frac{p_i}{q_j}\right] = u_i v_j$.
- 这里 $\left[\frac{a}{b}\right] = \log\left(\frac{a}{b}\right)$ 是加性勒让德 (雅克比) 符号, 其中 $\log : \{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.
- 换言之, 定义矩阵

$$\boldsymbol{A}_{2P} = \boldsymbol{A}_P := ([p_j, -P]_{p_i})_{ij} \in M_k(\mathbb{F}_2), \qquad (\text{每行元素之和为 } 0)$$

技术性假设

- 假设存在 $\mathbb{F}_2$ 上的向量 $\boldsymbol{u}=(u_1,\dots,u_k)^{\mathrm{T}}$, $\boldsymbol{v}=(v_1,\dots,v_\ell)^{\mathrm{T}}$,
- 使得 $\sum_i u_i=0, \sum_j v_j=1$, $\left[\frac{p_i}{q_j}\right]=u_iv_j$.
- 这里 $\left[\frac{a}{b}\right]=\log\left(\frac{a}{b}\right)$ 是加性勒让德 (雅克比) 符号, 其中 $\log:\{\pm1\}\xrightarrow{\sim}\mathbb{F}_2$.
- 换言之, 定义矩阵

$$\boldsymbol{A}_{2P}=\boldsymbol{A}_P:=([p_j,-P]_{p_i})_{ij}\in M_k(\mathbb{F}_2),\qquad \text{(每行元素之和为 0)}$$

- 并类似定义 $\boldsymbol{A}_Q$, $\boldsymbol{A}_n$, 则

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

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 $\text{Ш}(E_n)[2^\infty] = 0$;
- $\boldsymbol{A}_P + \boldsymbol{U}_P$ 可逆.

定理

在前述假设下，如下等价:

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

其中 $0<d\mid P$ 满足 $d\neq 1, [d,-P]_{p_i}=u_i, \forall p_i\mid d$; $[d,-P]_{p_i}=0, \forall p_i\mid \frac{P}{d}$; (α,β,γ) 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 $\text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $\operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = 1$ 且 $\left[\frac{\gamma}{d}\right] = \left[\frac{\sqrt{2}+1}{d}\right] + 1$,

其中 $0 < d \mid P$ 满足 $d \neq 1, [d, -P]_{p_i} = u_i, \forall p_i \mid d$; $[d, -P]_{p_i} = 0, \forall p_i \mid \frac{P}{d}$; (α, β, γ) 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.

若取 $\boldsymbol{u}=\mathbf{0}$ 则我们得到:

推论: $s_2(n)=2, \boldsymbol{u}=\mathbf{0}$ 情形

若取 $\boldsymbol{u}=\mathbf{0}$ 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 $\text{Ш}(E_n)[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-P)=1$ 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.

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.

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 $\text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n) = 1$ 且 $h_8(-n) = 0$;
- $r_4(K_2\mathcal{O}_n) = 0$.

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 $\text{Ш}(E_n)[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n)=1$ 且 $h_8(-n)=0$;
- $r_4(K_2\mathcal{O}_n)=0$.

(2) 下述等价:

- $2n$ 是非同余数且 $\text{Ш}(E_{2n})[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-n)=1$ 且 $h_8(-n)+h_8(-2n)=1$;
- $r_4(K_2\mathcal{O}_{-2n})=0$.

定理

假设前述条件以及 $\left[\frac{p_i}{q_j}\right] = 0, \forall i, j$. 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, $i \neq j$;
- $\left[\frac{\gamma_i}{f_j}\right] = 0, \forall i \neq j$; $\left[\frac{\gamma_i}{f_i}\right] = h_8(-f_i)$,

则 n 是非同余数且 $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$, 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

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

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

(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 $\text{Ш}(E_{2n})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$.

2-下降法

- 证明主要工具是$\overset{\text{descent method}}{\text{下降法}}$.

- 证明主要工具是下降法 (descent method).
- 根据 2-下降法, $\mathrm{Sel}_2(E_n)$ 可等同于集合

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

- 证明主要工具是下降法. (descent method)
- 根据 2-下降法, $\mathrm{Sel}_2(E_n)$ 可等同于集合

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

- 其中 D_Λ 是齐性空间

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

- 证明主要工具是下降法 (descent method).
- 根据 2-下降法, $\mathrm{Sel}_2(E_n)$ 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_Λ 是齐性空间

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

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

- 证明主要工具是下降法 (descent method).
- 根据 2-下降法, $\mathrm{Sel}_2(E_n)$ 可等同于集合

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

- 其中 D_Λ 是齐性空间

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

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

Monsky 矩阵: 奇数 n

- 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 $\boldsymbol{M}_n$ 的核联系起来.

Monsky 矩阵: 奇数 n

- 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 $\boldsymbol{M}_n$ 的核联系起来.
- 当 $n = p_1 \cdots p_k$ 是奇数时, $\mathrm{Sel}_2'(E_n)$ 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.

Monsky 矩阵: 奇数 n

- 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 $\boldsymbol{M}_n$ 的核联系起来.
- 当 $n = p_1 \cdots p_k$ 是奇数时, $\mathrm{Sel}_2'(E_n)$ 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

$$\mathrm{Sel}_2'(E_n) \to \mathrm{Ker}\, \boldsymbol{M}_n, \quad \boldsymbol{M}_n = \begin{pmatrix} \boldsymbol{A}_n + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,2} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_n + \boldsymbol{D}_{n,-2} \end{pmatrix}$$

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

Monsky 矩阵: 奇数 n

- 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 $\boldsymbol{M}_n$ 的核联系起来.
- 当 $n = p_1 \cdots p_k$ 是奇数时, $\mathrm{Sel}_2'(E_n)$ 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

$$\mathrm{Sel}_2'(E_n) \to \mathrm{Ker}\,\boldsymbol{M}_n, \quad \boldsymbol{M}_n = \begin{pmatrix} \boldsymbol{A}_n + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,2} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_n + \boldsymbol{D}_{n,-2} \end{pmatrix}$$

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

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

- 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 $\boldsymbol{M}_n$ 的核联系起来.
- 当 $n = p_1 \cdots p_k$ 是奇数时, $\mathrm{Sel}_2'(E_n)$ 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

$$\mathrm{Sel}_2'(E_n) \to \mathrm{Ker}\, \boldsymbol{M}_n, \quad \boldsymbol{M}_n = \begin{pmatrix} \boldsymbol{A}_n + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,2} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_n + \boldsymbol{D}_{n,-2} \end{pmatrix}$$

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

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

- 类似地, $\mathrm{Sel}_2'(E_{2n})$ 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 $d_2 > 0$, $d_3 \equiv 1 \bmod 4$.

Monsky 矩阵: 偶数 $2n$

- 类似地, $\mathrm{Sel}_2'(E_{2n})$ 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 $d_2 > 0$, $d_3 \equiv 1 \bmod 4$.
- 此时

$$\mathrm{Sel}_2'(E_{2n}) \to \mathrm{Ker}\, \boldsymbol{M}_{2n}, \quad \boldsymbol{M}_{2n} = \begin{pmatrix} \boldsymbol{A}_n^{\mathrm{T}} + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,-1} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_n + \boldsymbol{D}_{n,2} \end{pmatrix}$$

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

- 类似地，$\mathrm{Sel}_2'(E_{2n})$ 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 $d_2 > 0$, $d_3 \equiv 1 \bmod 4$.
- 此时

$$\mathrm{Sel}_2'(E_{2n}) \to \mathrm{Ker}\, \boldsymbol{M}_{2n}, \quad \boldsymbol{M}_{2n} = \begin{pmatrix} \boldsymbol{A}_n^{\mathrm{T}} + \boldsymbol{D}_{n,2} & \boldsymbol{D}_{n,-1} \\ \boldsymbol{D}_{n,2} & \boldsymbol{A}_n + \boldsymbol{D}_{n,2} \end{pmatrix}$$

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

- 两种情形下均有

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

Cassels 配对

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

Cassels 配对

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

Cassels 配对

- 仅知道 $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\mathrm{Sel}_2'(E_n)$ 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).

- 仅知道 $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\mathrm{Sel}_2'(E_n)$ 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.

Cassels 配对

- 仅知道 $s_2(n) = \operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\mathrm{Sel}_2'(E_n)$ 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 $\Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2(E_n)$, 定义

$$\langle \Lambda, \Lambda' \rangle = \sum_v \langle \Lambda, \Lambda' \rangle_v \in \mathbb{F}_2, \quad \langle \Lambda, \Lambda' \rangle_v = \sum_{i=1}^{3} \left[L_i(P_v), d_i' \right]_v,$$

Cassels 配对

- 仅知道 $s_2(n) = \mathrm{rank}_{\mathbb{Z}}\, E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\mathrm{Sel}_2'(E_n)$ 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 $\Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2(E_n)$, 定义

$$\langle \Lambda, \Lambda' \rangle = \sum_v \langle \Lambda, \Lambda' \rangle_v \in \mathbb{F}_2, \quad \langle \Lambda, \Lambda' \rangle_v = \sum_{i=1}^{3} \left[L_i(P_v), d_i'\right]_v,$$

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

Cassels 配对

- 仅知道 $s_2(n) = \mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E_n)[2]$ 还不足以得到非同余数.
- Cassels 在 $\mathrm{Sel}_2'(E_n)$ 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 $\Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2(E_n)$, 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_Λ 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 (Wang 2016)

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

引理 (Wang 2016)

n **是非同余数且** $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)} \iff \mathrm{Sel}_2'(E_n)$ **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

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

Cassels 配对的核

引理 (Wang 2016)

n 是非同余数且 $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)} \iff \mathrm{Sel}_2'(E_n)$ 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 $\mathrm{Im}\,\mathrm{Sel}_4(E_n)$ 是映射 $\mathrm{Sel}_4(E_n) \xrightarrow{\times 2} \mathrm{Sel}_2(E_n)$ 的像.

引理 (Wang 2016)

n 是非同余数且 $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)} \iff \mathrm{Sel}_2'(E_n)$ 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 $\mathrm{Im}\,\mathrm{Sel}_4(E_n)$ 是映射 $\mathrm{Sel}_4(E_n) \xrightarrow{\times 2} \mathrm{Sel}_2(E_n)$ 的像.
- 而 $\mathrm{Sel}_2(E_n)$ 上 Cassels 配对的核就是这个像.

Cassels 配对的核

引理 (Wang 2016)

n 是非同余数且 $\text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)} \iff \mathrm{Sel}_2'(E_n)$ 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

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

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

引理 (Wang 2016)

n 是非同余数且 $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)} \iff \mathrm{Sel}_2'(E_n)$ 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 $\mathrm{Im}\,\mathrm{Sel}_4(E_n)$ 是映射 $\mathrm{Sel}_4(E_n) \xrightarrow{\times 2} \mathrm{Sel}_2(E_n)$ 的像.
- 而 $\mathrm{Sel}_2(E_n)$ 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 $\mathrm{Im}\,\mathrm{Sel}_4(E_n) = E_n[2] \subseteq \mathrm{Sel}_2(E_n)$, 等价于引理右侧.

- 现在我们开始证明主要结果.

- 现在我们开始证明主要结果.
- 设 n 是奇数, 设

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

- 现在我们开始证明主要结果.
- 设 n 是奇数, 设

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

- 则

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

$$\boldsymbol{M}_Q \begin{pmatrix} \boldsymbol{y} \\ \boldsymbol{w} \end{pmatrix} = \begin{pmatrix} \boldsymbol{v}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{x} \\ \boldsymbol{v}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{z} \end{pmatrix}.$$

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

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

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

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

$$s_2(n)=\dim_{\mathbb{F}_2}\mathrm{Ker}\,\boldsymbol{M}_n=2\,\mathrm{corank}(\boldsymbol{A}_P+\boldsymbol{U}_P).$$

Selmer 群的计算 (续)

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

$$s_2(n)=\dim_{\mathbb{F}_2}\operatorname{Ker}\boldsymbol{M}_n=2\operatorname{corank}(\boldsymbol{A}_P+\boldsymbol{U}_P).$$

- 由此可立得: n 是非同余数且 $\text{Ш}(E_n)[2^\infty]=0 \iff \boldsymbol{A}_P+\boldsymbol{U}_P$ 可逆.

命题

设 $0 < f_i, f_j \mid P$ 满足 $\gcd(f_i, f_j) = 1$，$\psi_P(f_i), \psi_P(f_j) \in \mathrm{Ker}(\boldsymbol{A}_P + \boldsymbol{U}_P)$. 令 $\Lambda_t = (f_t, 1, f_t), \Lambda_t' = (f_t, f_t, 1)$，那么

$$\langle \Lambda_i', \Lambda_i \rangle = \left[\frac{\sqrt{2}+1}{f_i}\right] + \left[\frac{\gamma_i}{f_i}\right] = \left[\frac{\sqrt{2}+1}{f_i}\right] + \left[\frac{\gamma_i'}{f_i}\right],$$

$$\langle \Lambda_i', \Lambda_j \rangle = \left[\frac{\gamma_i}{f_j}\right] = \left[\frac{\gamma_j'}{f_i}\right],$$

$$\langle \Lambda_i', \Lambda_i' \rangle = \left[\frac{\gamma_i \gamma_i'}{f_i}\right], \qquad \langle \Lambda_i', \Lambda_j' \rangle = \left[\frac{\gamma_i \gamma_i'}{f_j}\right],$$

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.

Cassles 配对的计算 (续)

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

Cassles 配对的计算 (续)

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

- 取

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

$$D_{\Lambda_i}:\begin{cases} H_1: & -nt^2+u_2^2-f_iu_3^2=0,\\ H_2: & -\frac{n}{f_i}t^2+u_3^2-u_1^2=0,\\ H_3: & 2nt^2+f_iu_1^2-u_2^2=0.\end{cases}$$

- 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

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

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.

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.
- $\left[L_1(P_v), f_t\right]_v = \left[\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t\right]_v$

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

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

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

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.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v$.
- $[L_2(P_v), f_t]_v = [(\sqrt{2}+1)\sqrt{-\frac{n}{f_i}}, f_t]_v, \quad [L_1L_2(P_v), f_t]_v = [(\sqrt{2}+1)\gamma_i', f_t]_v$.
- 对于 $v \mid \frac{P}{f_i}$, 取 $P_v = (t, u_1, u_2, u_3) = (0, 1, \sqrt{f_i}, 1)$.

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.
- $[L_1(P_v), f_t]_v = [\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v = [\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t]_v$.
- $[L_2(P_v), f_t]_v = [(\sqrt{2}+1)\sqrt{-\frac{n}{f_i}}, f_t]_v, \quad [L_1L_2(P_v), f_t]_v = [(\sqrt{2}+1)\gamma_i', f_t]_v$.
- 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 $[L_1L_2(P_v), f_t]_v = [\gamma_i', f_t]_v$.

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.
- $[L_1(P_v),f_t]_v=[\beta_i'\frac{n}{f_i}+2\gamma_i'\sqrt{-\frac{n}{f_i}},f_t]_v=[4\gamma_i'\sqrt{-\frac{n}{f_i}},f_t]_v=[\gamma_i'\sqrt{-\frac{n}{f_i}},f_t]_v$.
- $[L_2(P_v),f_t]_v=[(\sqrt{2}+1)\sqrt{-\frac{n}{f_i}},f_t]_v$, $\quad [L_1L_2(P_v),f_t]_v=[(\sqrt{2}+1)\gamma_i',f_t]_v$.
- 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 $[L_1L_2(P_v),f_t]_v=[\gamma_i',f_t]_v$.
- $\langle\Lambda_i,\Lambda_i'\rangle=\sum_{v|f_i}[(\sqrt{2}+1)\gamma_i',f_i]_v+\sum_{v|\frac{P}{f_i}}[\gamma_i',f_i]_v=\left[\frac{(\sqrt{2}+1)\gamma_i'}{f_i}\right]$.

- 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.
- $\left[L_1(P_v), f_t\right]_v = \left[\beta_i' \frac{n}{f_i} + 2\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t\right]_v = \left[4\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t\right]_v = \left[\gamma_i' \sqrt{-\frac{n}{f_i}}, f_t\right]_v$.
- $\left[L_2(P_v), f_t\right]_v = \left[(\sqrt{2}+1)\sqrt{-\frac{n}{f_i}}, f_t\right]_v, \quad \left[L_1 L_2(P_v), f_t\right]_v = \left[(\sqrt{2}+1)\gamma_i', f_t\right]_v$.
- 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 $\left[L_1 L_2(P_v), f_t\right]_v = [\gamma_i', f_t]_v$.
- $\langle \Lambda_i, \Lambda_i' \rangle = \sum_{v \mid f_i} \left[(\sqrt{2}+1)\gamma_i', f_i\right]_v + \sum_{v \mid \frac{P}{f_i}} [\gamma_i', f_i]_v = \left[\frac{(\sqrt{2}+1)\gamma_i'}{f_i}\right]$.
- $\langle \Lambda_i, \Lambda_j' \rangle = \sum_{v \mid f_i} \left[(\sqrt{2}+1)\gamma_i', f_j\right]_v + \sum_{v \mid \frac{P}{f_i}} [\gamma_i', f_j]_v = \left[\frac{\gamma_i'}{f_j}\right]$.

- 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.
- $\left[L_1(P_v),f_t\right]_v=\left[\beta_i'\frac{n}{f_i}+2\gamma_i'\sqrt{-\frac{n}{f_i}},f_t\right]_v=\left[4\gamma_i'\sqrt{-\frac{n}{f_i}},f_t\right]_v=\left[\gamma_i'\sqrt{-\frac{n}{f_i}},f_t\right]_v$.
- $\left[L_2(P_v),f_t\right]_v=\left[(\sqrt{2}+1)\sqrt{-\frac{n}{f_i}},f_t\right]_v$, $\quad \left[L_1L_2(P_v),f_t\right]_v=\left[(\sqrt{2}+1)\gamma_i',f_t\right]_v$.
- 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 $\left[L_1L_2(P_v),f_t\right]_v=[\gamma_i',f_t]_v$.
- $\langle\Lambda_i,\Lambda_i'\rangle=\sum\limits_{v\mid f_i}\left[(\sqrt{2}+1)\gamma_i',f_i\right]_v+\sum\limits_{v\mid\frac{P}{f_i}}[\gamma_i',f_i]_v=\left[\dfrac{(\sqrt{2}+1)\gamma_i'}{f_i}\right]$.
- $\langle\Lambda_i,\Lambda_j'\rangle=\sum\limits_{v\mid f_i}\left[(\sqrt{2}+1)\gamma_i',f_j\right]_v+\sum\limits_{v\mid\frac{P}{f_i}}[\gamma_i',f_j]_v=\left[\dfrac{\gamma_i'}{f_j}\right]$.
- 其它情形类似.

主要结论: $s_2(n) = 2$ 情形

- 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 $\mathrm{Sel}_2'(E_n)$ 由 $\Lambda = (d, 1, d), \Lambda' = (d, d, 1)$ 生成, 其中 $\psi_P(d) \in \operatorname{Ker}(\boldsymbol{A}_P + \boldsymbol{U}_P)$.

- 根据前面的计算 $s_2(n)=2 \iff \operatorname{corank}(\boldsymbol{A}_P+\boldsymbol{U}_P)=1$.
- 此时 $\operatorname{Sel}_2'(E_n)$ 由 $\Lambda=(d,1,d), \Lambda'=(d,d,1)$ 生成, 其中 $\psi_P(d)\in\operatorname{Ker}(\boldsymbol{A}_P+\boldsymbol{U}_P)$.
- 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 $\mathrm{Sel}_2'(E_n)$ 由 $\Lambda=(d,1,d),\Lambda'=(d,d,1)$ 生成, 其中 $\psi_P(d)\in\operatorname{Ker}(\boldsymbol{A}_P+\boldsymbol{U}_P)$.
- 于是 $\langle\Lambda,\Lambda'\rangle=\left[\frac{\sqrt{2}+1}{d}\right]+\left[\frac{\gamma}{d}\right]$.
- 故 n 是非同余数且 $\text{Ш}(E_n)[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2 \iff$

$$\operatorname{corank}(\boldsymbol{A}_P+\boldsymbol{U}_P)=1,\quad \left[\frac{\gamma}{d}\right]=\left[\frac{\sqrt{2}+1}{d}\right]+1.$$

- 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.

- 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 $n = p_1 \cdots p_k \equiv 1 \bmod 4$.

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

- 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 $n = p_1 \cdots p_k \equiv 1 \bmod 4$.
- 根据高斯型理论, $h_2(-n) = k+1$, $h_4(-n) = \operatorname{corank} \boldsymbol{R}_{-n} - 1$,
- 其中 Rèdei 矩阵 $\boldsymbol{R}_{-n} = \begin{pmatrix} \boldsymbol{A}_n & \boldsymbol{b}_{n,2} \\ \boldsymbol{b}_{n,-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}$, $\boldsymbol{b}_{n,\varepsilon} = \boldsymbol{D}_{n,\varepsilon}\mathbf{1}$.

- 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 $n = p_1 \cdots p_k \equiv 1 \bmod 4$.
- 根据高斯型理论, $h_2(-n) = k+1$, $h_4(-n) = \operatorname{corank} \boldsymbol{R}_{-n} - 1$,
- 其中 Rèdei 矩阵 $\boldsymbol{R}_{-n} = \begin{pmatrix} \boldsymbol{A}_n & \boldsymbol{b}_{n,2} \\ \boldsymbol{b}_{n,-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}$, $\boldsymbol{b}_{n,\varepsilon} = \boldsymbol{D}_{n,\varepsilon}\boldsymbol{1}$.
- 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_2 群联系起来, 我们回顾有关结论.
- 设 $n = p_1 \cdots p_k \equiv 1 \bmod 4$.
- 根据高斯型理论, $h_2(-n) = k+1$, $h_4(-n) = \operatorname{corank} \boldsymbol{R}_{-n} - 1$,
- 其中 Rèdei 矩阵 $\boldsymbol{R}_{-n} = \begin{pmatrix} \boldsymbol{A}_n & \boldsymbol{b}_{n,2} \\ \boldsymbol{b}_{n,-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}$, $\boldsymbol{b}_{n,\varepsilon} = \boldsymbol{D}_{n,\varepsilon}\mathbf{1}$.
- 对于 $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2]$, $\theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \boldsymbol{b}_{n,\gamma} \in \operatorname{Im} \boldsymbol{R}'_{-n}$.
- 这里 $\boldsymbol{R}'_{-n}$ 是 $\boldsymbol{R}_{-n}$ 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 $n = p_1 \cdots p_k \equiv 1 \bmod 4$.
- 根据高斯型理论，$h_2(-n) = k+1$, $h_4(-n) = \operatorname{corank} \boldsymbol{R}_{-n} - 1$,
- 其中 Rèdei 矩阵 $\boldsymbol{R}_{-n} = \begin{pmatrix} \boldsymbol{A}_n & \boldsymbol{b}_{n,2} \\ \boldsymbol{b}_{n,-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}$, $\boldsymbol{b}_{n,\varepsilon} = \boldsymbol{D}_{n,\varepsilon}\mathbf{1}$.
- 对于 $\theta_{-n}(d) := [(d, \sqrt{-n})] \in \mathcal{A}_{-n}[2]$, $\theta_{-n}(d) \in \mathcal{A}_{-n}^4 \iff \boldsymbol{b}_{n,\gamma} \in \operatorname{Im} \boldsymbol{R}'_{-n}$.
- 这里 $\boldsymbol{R}'_{-n}$ 是 $\boldsymbol{R}_{-n}$ 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

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

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

$$\#\{\boldsymbol{x}:\boldsymbol{B}_m\boldsymbol{x}=\boldsymbol{b}_{n,\pm1},\boldsymbol{b}_{n,\pm2}\}+\#\{\boldsymbol{x}:\boldsymbol{B}_m\boldsymbol{x}=\boldsymbol{b}_{n,\pm\mu}\}=2^{r_4(K_2\mathcal{O}_m)+1}.$$

- 当 $m=-n, -2n<-2$ 时

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

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

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

- 当 $m = -n, -2n < -2$ 时

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

- 其中 $\boldsymbol{B}_m = \boldsymbol{A}_n + \boldsymbol{D}_{n,m/n}$.

- 设 n 是模 8 余 1 素数乘积.

主要结论: $s_2(n) = 2, \boldsymbol{u} = \mathbf{0}$ 情形

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

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

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

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

- 设 n 是模 8 余 1 素数乘积.
  - $h_4(-n) = h_4(-2n) = \operatorname{corank} \boldsymbol{A}_n$.
  - $r_4(K_2\mathcal{O}_n) = 0 \iff h_4(-n) = 1, h_8(-n) = 0$.
  - $r_4(K_2\mathcal{O}_{-2n}) = 0 \iff h_4(-n) = 1, h_8(-n) + h_8(-2n) = 1$.
  - 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: 当 $s_2(n) = 0, \boldsymbol{u} = \boldsymbol{0}$ 时, $d = \boldsymbol{P}$,

$$1 = \operatorname{corank}(\boldsymbol{A}_P + \boldsymbol{U}_P) = \operatorname{corank} \boldsymbol{A}_P \iff h_4(-P) = 1$$

$$\left[\frac{\gamma}{P}\right] = \left[\frac{\sqrt{2}+1}{P}\right] + 1 = h_8(-P) = r_4(K_2\mathcal{O}_P).$$

主要结果: $s_2(n) \geqslant 2$

- 假设前述条件以及 $\left[\dfrac{p_i}{q_j}\right] = 0, \forall i, j.$

- 假设前述条件以及 $\left[\frac{p_i}{q_j}\right] = 0, \forall i, j$.
- 假设存在分解 $P = f_1 \cdots f_r$ 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, $i \neq j$;
  - $\left[\frac{\gamma_i}{f_j}\right] = 0, \forall i \neq j$; $\left[\frac{\gamma_i}{f_i}\right] = h_8(-f_i)$,

  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.

- 假设前述条件以及 $\left[\frac{p_i}{q_j}\right] = 0, \forall i, j.$
- 假设存在分解 $P = f_1 \cdots f_r$ 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, $i \neq j;$
  - $\left[\frac{\gamma_i}{f_j}\right] = 0, \forall i \neq j;$ $\left[\frac{\gamma_i}{f_i}\right] = h_8(-f_i),$

  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.
- 那么 $\boldsymbol{A}_P + \boldsymbol{U}_P = \boldsymbol{A}_P = \mathrm{diag}\{\boldsymbol{A}_{f_1}, \cdots \boldsymbol{A}_{f_r}\}.$

- 假设前述条件以及 $\left[\dfrac{p_i}{q_j}\right] = 0, \forall i, j.$
- 假设存在分解 $P = f_1 \cdots f_r$ 满足
  - $h_4(-f_i) = 1, \forall i;$
  - $\left[\dfrac{p}{p'}\right] = 0$, 其中 $p \mid f_i, p' \mid f_j$ 是任意素因子, $i \neq j;$
  - $\left[\dfrac{\gamma_i}{f_j}\right] = 0, \forall i \neq j;\ \left[\dfrac{\gamma_i}{f_i}\right] = h_8(-f_i),$

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

主要结果: $s_2(n) \geqslant 2$

- 假设前述条件以及 $\left[\frac{p_i}{q_j}\right] = 0, \forall i, j$.
- 假设存在分解 $P = f_1 \cdots f_r$ 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, $i \neq j$;
  - $\left[\frac{\gamma_i}{f_j}\right] = 0, \forall i \neq j$; $\left[\frac{\gamma_i}{f_i}\right] = h_8(-f_i)$,

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

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

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

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

- 相应的 Cassels 配对对应矩阵

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

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

$$\boldsymbol{C} = \operatorname{diag}\Big\{\Big[\frac{\sqrt{2}+1}{f_1}\Big], \ldots, \Big[\frac{\sqrt{2}+1}{f_r}\Big]\Big\} = \operatorname{diag}\{1 - h_8(-f_1), \ldots, 1 - h_8(-f_r)\}.$$

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

- 相应的 Cassels 配对对应矩阵

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

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

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

- 因此 $\boldsymbol{X}=\begin{pmatrix} * & \boldsymbol{I} \\ \boldsymbol{I} & \boldsymbol{O} \end{pmatrix}$ 可逆, Cassels 配对非退化.
- 从而 n 是非同余数且 $Ш(E_n)[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^{2r}$.

- 若 $Q = 2, n = 2P$, 则

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

- 若 $Q = 2, n = 2P$, 则

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

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

- 若 $Q = 2, n = 2P$, 则

$$\boldsymbol{R}_{-2P} = \mathrm{diag}\{\boldsymbol{A}_n, 0\} = \mathrm{diag}\{\boldsymbol{A}_{f_1}, \cdots \boldsymbol{A}_{f_r}, 0\}.$$

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

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

推论: $s_2(n) \geqslant 2, Q = 1, 2$ 情形

- 若 $Q = 2, n = 2P$, 则

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

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

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

- 条件 $\left[\frac{\gamma_i}{f_j}\right] = 0, \forall i \neq j$; $\left[\frac{\gamma_i}{f_i}\right] = h_8(-f_i)$ 等价于 $h_8(-f_i) = 0$.

推论: $s_2(n) \geqslant 2, Q = 1, 2$ 情形

- 若 $Q = 2, n = 2P$, 则

$$\boldsymbol{R}_{-2P} = \mathrm{diag}\{\boldsymbol{A}_n, 0\} = \mathrm{diag}\{\boldsymbol{A}_{f_1}, \cdots \boldsymbol{A}_{f_r}, 0\}.$$

- 所以 $h_4(-2P) = r$ 且 $\mathcal{A}_{-2P}[2] \cap \mathcal{A}^2_{-2P}$ 由 $\theta_{-2P}(f_1), \ldots, \theta_{-2P}(f_{r-1})$ 生成.
- 若 $h_8(-2P) = r$, 则它们都属于 $\mathcal{A}^4_{-2P}$. 从而 $\boldsymbol{b}_{P,\gamma_i} \in \mathrm{Im}\, \boldsymbol{A}_P$,

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

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

  则 $2P$ 是非同余数且 $Ш(E_{2P})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$.

推论: $s_2(n) \geqslant 2, Q = 1, 2$ 情形

- 若 $Q = 2, n = 2P$, 则

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

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

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

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

  则 $2P$ 是非同余数且 $\text{Ш}(E_{2P})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$. $Q = 1$ 情形类似.


济 南
中国城市地标插画系列
谢 谢