关于奇素因子模 8 余 ±1 的非同余数

张神星

2021 年四川大学青年数论论坛
四川 成都

2021 年 11 月 26 日

同余数与同余椭圆曲线

设 n 是一个平方自由的正整数. 如果 n 可以表为一个有理边长直角三角形的面积, 则称 n 是一个同余数. 这等价于椭圆曲线

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

的 Mordell-Weil 秩至少为 1. 记 $\mathrm{Sel}_2(E)$ 为 $E/\mathbb{Q}$ 的 2-Selmer 群,

$$s_2(n) := \dim_{\mathbb{F}_2}\left(\frac{\mathrm{Sel}_2(E)}{E(\mathbb{Q})[2]}\right) = \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E) - 2.$$

由长正合列

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

可知

$$s_2(n) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \dim_{\mathbb{F}_2} \text{Ш}(E/\mathbb{Q})[2].$$

已知的结果

Monsky 证明了 $n \equiv 1, 2, 3 \bmod 8$ 时, $s_2(n)$ 总是偶数. 显然 $s_2(n) = 0$ 时, n 是非同余数. 该情形由田野-袁新意-张寿武 (2017) 和 Smith (2016) 完全刻画.

我们来考虑何时 n 是非同余数且 $s_2(n) = 2$. 记 $h_{2^a}(m)$ 为 $\mathbb{Q}(\sqrt{m})$ 的缩理想类群的 2^a 阶秩. 如果 n 的素因子均模 4 余 1, 王章结证明了:

定理 (王章结, 2016)

设 $n = p_1 \cdots p_k \equiv 1 \bmod 8$ 的素因子均模 4 余 1, 则下述等价:

(i) $h_4(-n) = 1, h_8(-n) \equiv (d-1)/4 \pmod 2$;

(ii) $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0, Ш(E_n/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

这里, 要么 $d \neq 1$, n 是满足 $(d, -n)_v = 1, \forall v$ 的 n 的正因子; 要么 d 是满足 $(2d, -n)_v = 1, \forall v$ 的 n 的正因子.

主要结果：奇数情形

定理

设 $n = p_1 \cdots p_k \equiv 1 \bmod 8$ 的素因子均模 8 余 ± 1，则下述等价：

(i) $h_4(-n) = 1, h_4(n) = 0, \left(\frac{-\mu}{d}\right) = -1$;

(ii) $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0, \text{Ш}(E_n/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

这里，$d \neq 1$ 是满足 $(d, n)_v = 1, \forall v$ 的 n 的正因子，$n = 2\mu^2 - \tau^2$，其中 $\mu \equiv d \bmod 4$.

推论

设 $n = p_1 \cdots p_k \equiv 1 \bmod 8$ 的素因子均模 8 余 1，则下述等价：

(i) $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 0$;

(ii) $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0, \text{Ш}(E_n/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

秦厚荣的结果

定理 (秦厚荣, 2021)

设素数 $p \equiv 1 \mod 8$. 如果 $r_8(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{p})}) = 0$, 则 p 是非同余数.

实际上, 该情形下可以证明完整的 BSD 猜想成立.

主要结果：偶数情形

定理

设 $n = 2p_1 \cdots p_k \equiv 1 \bmod 8$ 的奇素因子均模 8 余 ± 1，则下述等价：

(i) $h_4(-n/2) = 1, \left(\frac{2-\sqrt{2}}{|d|}\right) = -1$;

(ii) $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0, Ш(E_n/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

这里，$d \neq 1$ 是满足 $(d, n)_v = 1, \forall v$ 的 n 的模 8 余 1 的因子.

推论

设 $n = 2p_1 \cdots p_k \equiv 1 \bmod 8$ 的奇素因子均模 8 余 1，则下述等价：

(i) $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}) = 0$;

(ii) $\mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0, Ш(E_n/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Selmer 群与齐性空间

我们来回顾下 Monsky 矩阵 [HeathBrown1994]. $\mathrm{Sel}_2(E_n)$ 可以表为

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

其中

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

$$O \mapsto (1,1,1) \qquad (n,0) \mapsto (2, 2n, n)$$

$$(-n, 0) \mapsto (-2n, 2, -n) \qquad (0,0) \mapsto (-n, n, -1)$$

$$(x, y) \mapsto (x - n, x + n, x)$$

辅助矩阵和向量

记 $n' = n/(2,n) = p_1 \cdots p_k$. 记 $[a,b]_v, \left[\frac{a}{b}\right] \in \mathbb{F}_2$ 分别为加性希尔伯特符号和雅克比符号. 定义

$$\mathbf{A} = \mathbf{A}_{n'} = (a_{ij})_{k\times k} \quad 其中 \quad a_{ij} = [p_j, -n']_{p_i} = \begin{cases} \left[\frac{p_j}{p_i}\right], & i \neq j; \\ \left[\frac{n'/p_i}{p_i}\right], & i = j, \end{cases}$$

$$\mathbf{D}_\varepsilon = \mathrm{diag}\left\{\left[\frac{\varepsilon}{p_1}\right], \ldots, \left[\frac{\varepsilon}{p_k}\right]\right\} \qquad \mathbf{b}_\varepsilon = \mathbf{D}_\varepsilon \mathbf{1}.$$

则 $\mathbf{A1} = \mathbf{0}, \mathrm{rank}(\mathbf{A}) \leq k-1.$

Monsky 矩阵：奇数情形

当 n 为奇数时, $\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ 中元素可表为 (d_1, d_2, d_3), 其中 d_1, d_2 均为 n 的正因子. 于是 D_Λ 局部处处可解等价于特定的希尔伯特符号的条件. 我们有同构

$$\begin{aligned}\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2] &\longrightarrow \mathrm{Ker}\,\mathbf{M}_n \\ (d_1, d_2, d_3) &\longmapsto \begin{pmatrix} \psi^{-1}(d_2) \\ \psi^{-1}(d_1) \end{pmatrix},\end{aligned}$$

其中

$$\psi\left((\delta_1, \ldots, \delta_k)^{\mathrm{T}}\right) = \prod_{\delta_j = 1} p_j,$$

$$\mathbf{M}_n = \begin{pmatrix} \mathbf{A} + \mathbf{D}_2 & \mathbf{D}_2 \\ \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_{-2} \end{pmatrix}.$$

Monsky 矩阵: 偶数情形

类似地, 当 n 为偶数时, $\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ 中元素可表为 (d_1, d_2, d_3), 其中 d_2, d_3 均为 n 的因子, $d_2 > 0, d_3 \equiv 1 \bmod 4$. 我们有同构

$$\begin{aligned}\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2] &\longrightarrow \mathrm{Ker}\,\mathbf{M}_n\\ (d_1, d_2, d_3) &\longmapsto \begin{pmatrix}\psi^{-1}(|d_3|)\\ \psi^{-1}(d_2)\end{pmatrix},\end{aligned}$$

其中

$$\mathbf{M}_n = \begin{pmatrix}\mathbf{A}^{\mathrm{T}} + \mathbf{D}_2 & \mathbf{D}_{-1}\\ \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_2\end{pmatrix}.$$

特别地,

$$s_2(n) = 2k - \mathrm{rank}(\mathbf{M}_n), \qquad \forall n.$$

Cassels 配对

Cassels 在 $\mathbb{F}_2$ 线性空间 $\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ 上定义了一个 (反) 对称双线性型. 对于 Λ, Λ', 选择 $P = (P_v) \in D_\Lambda(\mathbb{A})$, $Q_i \in H_i(\mathbb{Q})$. 令 L_i 为定义了 H_i 在 Q_i 处切平面的线性型, 定义

$$\langle \Lambda, \Lambda' \rangle = \prod_v \langle \Lambda, \Lambda' \rangle_v, \qquad \text{其中 } \langle \Lambda, \Lambda' \rangle_v = \prod_{i=1}^{3} \left(L_i(P_v), d_i'\right)_v.$$

它不依赖 P 和 Q_i 的选择.

引理 (Cassels1998, Lemma 7.2)

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

类群与 Rédei 矩阵

设 $m \neq 0, 1$ 为无平方因子整数，$F = \mathbb{Q}(\sqrt{m})$，$C(F)$ 为缩理想类群. 我们将其判别式进行分解

$$D = p_1^* \cdots p_t^*, \qquad p^* = (-1)^{\frac{p-1}{2}} p \equiv 1 \bmod 4,\ \ 2^* = -4, 8, -8.$$

高斯型理论告诉我们

$$h_2(m) = t - 1.$$

Rédei 证明了

$$\theta : \{D \text{ 的平方自由且属于 } \mathrm{N}F \text{ 的正因子}\} \longrightarrow C(F)[2] \cap C(F)^2$$
$$d \longmapsto \mathrm{cl}[\mathfrak{d}]$$

是 $2:1$ 的满射，其中 $(d) = \mathfrak{d}^2$. 将其用矩阵语言表达，则

$$h_4(m) = t - 1 - \mathrm{rank}(\mathbf{R}_m), \qquad \mathbf{R}_m = ([p_j, m]_{p_i})_{ij}.$$

温核 $K_2\mathcal{O}_F$

记 $K_2\mathcal{O}_F$ 为 $\mathcal{O}_F$ 的 K_2 群, 则我们有正合列

$$1 \to K_2\mathcal{O}_F \to K_2F \to \prod_p \mathbb{F}_p^\times \to 1,$$

其中第二个箭头是温剩余符号: $(a,b)_p = (-1)^{v(a)v(b)} b^{v(a)} a^{-v(b)} \bmod p.$

Browkin-Schinzel (1982) 证明了 $K_2\mathcal{O}_F[2]$ 可由如下 Steinberg 符号生成:

- $\{-1, d\}, d \mid m$;
- $\{-1, u+\sqrt{m}\}$, 其中 $m = u^2 - cw^2, c = -1, \pm 2, u, w \in \mathbb{N}$.

温核的 4 阶秩

设 $r_4 = r_4(K_2\mathcal{O}_F)$. 秦厚荣 (1995) 证明了如下结果:

(i) $m > 0$ 时, $2^{r_4+1} = \#V_1 + \#V_2$, 其中

$$V_1 = \{\psi(\mathbf{d}) : \mathbf{Bd} = \mathbf{b}_{\pm 1}, \mathbf{b}_{\pm 2}\}, \qquad V_2 = \{\psi(\mathbf{d}) : \mathbf{Bd} = \mathbf{b}_{\pm \mu}\}.$$

(ii) $m < 0$ 时, $2^{r_4+2} = \#V_1 + \#V_2$, 其中

$$V_1 = \{\psi(\mathbf{d}) : \mathbf{Bd} = \mathbf{0}, \mathbf{b}_2\} \cup \{-\psi(\mathbf{d}) : \mathbf{Bd} = \mathbf{b}_{-1}, \mathbf{b}_{-2}\},$$
$$V_2 = \{\psi(\mathbf{d}) : \mathbf{Bd} = \mathbf{b}_{\mu}\} \cup \{-\psi(\mathbf{d}) : \mathbf{Bd} = \mathbf{b}_{-\mu}\}.$$

这里 $\mathbf{B} = \mathbf{A}_{m'} + \mathbf{D}_{m/m'}$, $m' = \frac{|m|}{(2,m)}$, $m = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$.

约化到 Cassels 配对非退化

设 $s_2(n)=2$. 正合列

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

诱导了

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

于是

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

当且仅当 $\#\mathrm{Sel}_2(E)=\#\mathrm{Sel}_4(E)$, 即 $\#\mathrm{Im}\,\mathrm{Sel}_4(E)=\#E(\mathbb{Q})[2]$. 而 Cassels 配对的核是 $\mathrm{Im}\,\mathrm{Sel}_4(E)/E(\mathbb{Q})[2]$, 因此我们只需刻画何时 Cassels 配对非退化.

奇数情形: $s_2(n) = 2$

设 n 的素因子均模 8 余 ± 1, 此时

$$\mathbf{D}_2 = \mathbf{O} \qquad \mathbf{M}_n = \begin{pmatrix} \mathbf{A} & \\ & \mathbf{A} + \mathbf{D}_{-1} \end{pmatrix}.$$

由于 $\mathbf{A}\mathbf{1} = (\mathbf{A}^{\mathrm{T}} + \mathbf{D}_{-1})\mathbf{1} = \mathbf{0}$, 我们有

$$\operatorname{rank}(\mathbf{A}) \le k - 1, \quad \operatorname{rank}(\mathbf{A} + \mathbf{D}_{-1}) \le k - 1.$$

而

$$\mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{b}_{-1}^{\mathrm{T}} & 0 \end{pmatrix}, \quad \mathbf{R}_n = \mathbf{A} + \mathbf{D}_{-1}$$

且 $\mathbf{1}^{\mathrm{T}}\mathbf{A} = \mathbf{b}_{-1}^{\mathrm{T}}$, 因此 $s_2(n) = 2 \iff h_4(-n) = 1, h_4(n) = 0.$

奇数情形: 齐性空间

设 $d \neq 1$ 是唯一满足 $(d, n)_v = 1, \forall v$ 的 n 的正因子. 换言之, $(\mathbf{A} + \mathbf{D}_{-1})\psi^{-1}(d) = \mathbf{0}$. 于是 E_n 的纯 2-Selmer 群为

$$\{(1,1,1), \Lambda = (1, n, n), \Lambda' = (d, 1, d), (d, n, nd)\}.$$

$$D_\Lambda = \begin{cases} H_1: & -t^2 + u_2^2 - u_3^2 = 0, \\ H_2: & -nt^2 + nu_3^2 - u_1^2 = 0, \\ H_3: & 2nt^2 + u_1^2 - nu_2^2 = 0. \end{cases}$$

令 $n = 2\mu^2 - \tau^2$, 则 μ 是奇数且 $n = u^2 - 2w^2$, $u = 2\mu - \tau, w = -\mu + \tau$. 选择

$$\begin{aligned} Q_1 &= (0, 1, 1) \in H_1(\mathbb{Q}), & L_1 &= u_2 - u_3, \\ Q_3 &= (w, n, u) \in H_3(\mathbb{Q}), & L_3 &= 2wt + u_1 - uu_2. \end{aligned}$$

奇数情形: Cassels 配对

对于 $p \mid n$, 取 $(t, u_1, u_2, u_3) = (1, 0, \sqrt{2}, 1)$, 其中 $\sqrt{2} \equiv -u/w \bmod p$,

$$L_1 L_3(P_p) = (\sqrt{2}-1)(2w - \sqrt{2}u) \equiv 4(\sqrt{2}-1)w \equiv -4\mu \bmod p,$$

$$\big(L_1 L_3(P_p), d\big)_p = (-\mu, d)_p.$$

对于 $p = 2$, 取 $(t, u_1, u_2, u_3) = (0, \sqrt{n}, 1, -1)$,

$$\big(L_1 L_3(P_2), d\big)_2 = \big(2(\sqrt{n}-u), d\big)_2 = (-\sqrt{n}-u, d)_2 = (-\mu, d)_2.$$

由于 $\mu \equiv d \bmod 4$, 于是我们有 $(-\mu, d)_2 = 1$,

$$\langle \Lambda, \Lambda' \rangle = \prod_{p \mid d} (-\mu, d)_p = \left(\frac{-\mu}{d}\right).$$

奇数情形: 推论

如果所有的 $p_i \equiv 1 \bmod 8$, 则 $\mathbf{D}_{\pm 1} = \mathbf{D}_{\pm 2} = \mathbf{O}$, $d = n$. 令 $F = \mathbb{Q}(\sqrt{n})$, 则

$$2^{r_4(K_2\mathcal{O}_F)+1} = \#\{\mathbf{d} : \mathbf{A}\mathbf{d} = \mathbf{0}\} + \#\left\{\mathbf{d} : \mathbf{A}\mathbf{d} = \mathbf{b}_{|\mu|} = \mathbf{b}_\mu\right\}.$$

由于 $\operatorname{Ker}\mathbf{A} \supseteq \{\mathbf{0}, \mathbf{1}\}$, 因此 $r_4(K_2\mathcal{O}_F) = 0$ 当且仅当 $\operatorname{rank}(\mathbf{A}) = k - 1$ 且 $\mathbf{b}_\mu \notin \operatorname{Im}\mathbf{A}$. 但此时

$$\operatorname{Im}\mathbf{A} = \left\{\mathbf{d} : \mathbf{1}^{\mathrm{T}}\mathbf{d} = \mathbf{0}\right\},$$

因此 $\left(\frac{\mu}{n}\right) = -1$.

偶数情形: $s_2(n) = 2$

设 $n = 2n'$ 的奇素因子均模 8 余 ± 1, 此时

$$\mathbf{D}_2 = \mathbf{O} \qquad \mathbf{M}_n = \begin{pmatrix} \mathbf{A}^{\mathrm{T}} & \mathbf{D}_{-1} \\ & \mathbf{A} \end{pmatrix}.$$

由于 $\mathbf{A1} = \mathbf{0}$, 我们有 $\operatorname{rank}(\mathbf{A}) \leq k - 1$. 方程 $\mathbf{M}_n \left(\begin{smallmatrix} \mathbf{x} \\ \mathbf{y} \end{smallmatrix}\right) = \mathbf{0}$ 等价于

$$\mathbf{A}^{\mathrm{T}}\mathbf{x} = \mathbf{D}_{-1}\mathbf{y}, \quad \mathbf{A}\mathbf{y} = \mathbf{0}.$$

若 $\mathbf{y} = \mathbf{0}$, 则 $\mathbf{A}^{\mathrm{T}}\mathbf{x} = \mathbf{0}$ 至少有两个解. 若 $\mathbf{y} = \mathbf{1}$, 则 $\mathbf{A}^{\mathrm{T}}(\mathbf{x} + \mathbf{1}) = \mathbf{0}$ 至少有两个解. 因此 $s_2(n) = \dim_{\mathbb{F}_2} \operatorname{Ker} \mathbf{M}_n \geq 2$ 且

$$s_2(n) = 2 \iff \operatorname{rank}(\mathbf{A}) = k - 1 \iff h_4(-n/2) = 1.$$

偶数情形：齐性空间

设 $d \neq 1$ 是唯一满足 $(d,n)_v = 1, \forall v$ 的 n 的模 8 余 1 的因子. 换言之, $\mathbf{A}^{\mathrm{T}}\psi^{-1}(|d|) = \mathbf{0}$. 于是 E_n 的纯 2-Selmer 群为

$$\{(1,1,1), \Lambda = (1,n',n'), \Lambda' = (d,1,d), (d,n',n'd)\}.$$

$$D_\Lambda = \begin{cases} H_1: & -2t^2 + u_2^2 - u_3^2 = 0, \\ H_2: & -2n't^2 + n'u_3^2 - u_1^2 = 0, \\ H_3: & 4n't^2 + u_1^2 - n'u_2^2 = 0. \end{cases}$$

选择

$$Q_1 = (0,1,1) \in H_1(\mathbb{Q}), \qquad L_1 = u_2 - u_3,$$
$$Q_3 = (n'-1, 4n', 2n'+2) \in H_3(\mathbb{Q}), \qquad L_3 = 2(n'-1)t + 2u_1 - (n'+1)u_2.$$

偶数情形: Cassels 配对

对于 $p \mid n$, 取 $(t, u_1, u_2, u_3) = (1, 0, 2, \sqrt{2})$,

$$\big(L_1L_3(P_p), d\big)_p = \big(-2(2-\sqrt{2}), d\big)_p = (\sqrt{2}-2, d)_p.$$

对于 $p = 2$, 取 $(t, u_1, u_2, u_3) = (0, \sqrt{n'}, 1, -1)$,

$$L_1L_3(P_2) = 2(2\sqrt{n'} - n' - 1) = -2(\sqrt{n'}-1)^2,$$

$$\big(L_1L_3(P_2), d\big)_2 = (-2, d)_2 = (-1, d)_2.$$

因此

$$\langle \Lambda, \Lambda' \rangle = (-1, d)_2 \prod_{p \mid d} (\sqrt{2}-2, d)_p = \left(\frac{2-\sqrt{2}}{|d|}\right).$$

偶数情形: 推论

如果所有的 $p_i \equiv 1 \bmod 8$, 则 $\mathbf{D}_{\pm 1} = \mathbf{D}_{\pm 2} = \mathbf{O}$, $d = n'$. 令 $F = \mathbb{Q}(\sqrt{-n})$, $-n = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$, 则

$$2^{r_4(K_2\mathcal{O}_F)+2} = 2\#\{\mathbf{d} : \mathbf{A}\mathbf{d} = \mathbf{0}\} + 2\#\{\mathbf{d} : \mathbf{A}\mathbf{d} = \mathbf{b}_\mu\}.$$

由于 $\mathrm{Ker}\,\mathbf{A} \supseteq \{\mathbf{0}, \mathbf{1}\}$, 因此 $r_4(K_2\mathcal{O}_F) = 0$ 当且仅当 $\mathrm{rank}(\mathbf{A}) = k - 1$ 且 $\mathbf{b}_\mu \notin \mathrm{Im}\,\mathbf{A}$. 但此时

$$\mathrm{Im}\,\mathbf{A} = \left\{\mathbf{d} : \mathbf{1}^{\mathrm{T}}\mathbf{d} = \mathbf{0}\right\},$$

因此 $\left(\frac{\mu}{n'}\right) = -1$. 记 $u = \lambda - \mu, w = -\lambda/2 + \mu$, 则 $n' = u^2 - 2w^2$,

$$\left(\frac{w}{n'}\right) = \left(\frac{n'}{w'}\right) = \left(\frac{u^2 - 2w^2}{w'}\right) = \left(\frac{u^2}{w'}\right) = 1,$$

$$\left(\frac{\mu}{n'}\right) = \left(\frac{u + 2w}{n'}\right) = \left(\frac{(2 \pm \sqrt{2})w}{n'}\right) = \left(\frac{2 \pm \sqrt{2}}{n'}\right).$$

感谢各位的倾听!