極小型実2次体と2つの有名予想

河本 史紀 (学習院大学)　冨田 耕史 (名城大学)

目 次

1　はじめに

これは 2 講演

「極小型実 2 次体と Ankeny-Artin-Chowla 予想 ～橋本竜太氏の仕事の紹介～」

「極小型実 2 次体と Gauss 予想」

の報告書であるが, 標題のように 1 つにまとめて書かせていただく.

数値実験を行うために Section 2 において, 任意の平方でない自然数 d に対して, 実 2 次体のある整環を対応させて, d の導手, 判別式, 基本単数, 横井不変量, 類数を定義する. d が平方因子をもたないとき, これらは実 2 次体 $\mathbb{Q}(\sqrt{d})$ の対応する不変量と一致する. 不変量の拡張をする動機については脚注 2.2 を参照してほしい. 基本性質として, まず Siegel の定理の拡張 (Proposition 2.2) が成り立つことがわかる. 次に, 横井の定理の拡張 (Proposition 2.3) が成り立つことから, 後で定義を述べる横井不変量は基本単数の大雑把な大きさを与えることが

わかる. したがって, 実 2 次体の場合 (d: square-free) と同じく, d の類数が 1 ならばその基本単数は比較的大きく, 横井不変量も比較的大きい.

Section 3 では, Friesen and Halter-Koch の定理を使って [13] で導入された極小型自然数および極小型実 2 次体を定義する. この概念に着目すると, d が極小型でないとき, その横井不変量は高々 3 の値しか取らない (Proposition 3.2). よって, d が極小型のときに横井不変量の値は大きい可能性がある.

Section 4 では, Ankeny-Artin-Chowla 予想 (実 2 次体 $\mathbb{Q}(\sqrt{p})$, $p \equiv 1 \mod 4$ の基本単数に関する予想) に対する橋本竜太氏の仕事 [10] の主結果を極小型実 2 次体のことばで再定式化し, その位置付けを行う. この予想の解決にはまだ手が届かないことが納得できる. 定式化の違いは Section 4.1 で説明する.

Section 5 では, 類数 1 の実 2 次体は無限に多く存在するだろうと主張する Gauss 予想 (Gauss [8, Article 304]) について論じる. その正当性を見るために極小型自然数に着目し, 連分数による数値実験を行った. その結果を報告し, 予想を立てる. 講演では 2 億の範囲のデータを紹介したが, ここでは 3 億の範囲のデータを述べる. 予想の変更はない. これが報告書の主目的で, 連分数による類数 1 の実 2 次体の無限族の抽出方法を提唱する (Section 5.1). その予想を解くための取り組みについても述べる (Section 5.2). 我々の予想は単純ですぐにわかるから, その 1 つを始めに書く. d を $4 \nmid d$ をみたす任意の平方でない自然数とし, $\ell = \ell(d)$ により $d \equiv 1 \bmod 4$ のとき $(1+\sqrt{d})/2$ の単純な (simple) 連分数展開の周期を, $d \equiv 2, 3 \bmod 4$ のときは $\sqrt{d}$ の単純な連分数展開の周期を表わす. 各周期 ℓ ごとに小さい順に d の値をいくつか並べる:

表 1.1: 各周期における d の値

ℓ	d					
1	2	5	10	13	26	…
2	3	6	11	15	18	…
3	17	37	61	65	101	…
4	7	14	23	33	34	…
5	41	74	149	157	181	…
6	19	22	54	57	59	…
7	58	89	109	113	137	…
8	31	71	91	135	153	…
9	73	97	106	233	277	…
10	43	67	86	115	118	…
11	265	298	541	554	593	…
12	46	103	127	177	209	…
13	421	746	757	778	1021	…
14	134	179	190	201	251	…
15	193	281	481	1066	1417	…
16	94	191	217	249	302	…
⋮	…	…	…	…	…	…

表 1.1 の第 1 列目における最小の自然数 d に着目する. それが平方因子をもたないとき実 2 次体 $\mathbb{Q}(\sqrt{d})$ を与える. 数値実験の結果に基づき, その類数 h_d は, 6 個の例外を除くと $h_d = 1$ となることを予想する (Conjecture 1).

Sections 6, 7 では, それぞれ Propositions 2.2, 2.3 を証明する. Section 8 では, Proposition 5.1 の証明の概略を書き, Friesen and Halter-Koch の定理の使用例を提示する.

2 不変量の導入と基本性質

d を任意の平方でない自然数とする. d を

$$d = d_1 d_2^2, \quad d_1, d_2 \in \mathbb{N},\ d_1 \text{ は平方因子をもたない} \tag{2.1}$$

の形に分解して (よって, $d_1 > 1$), **平方でない自然数 d の導手**を

$$f = f_d := \begin{cases} d_2/2, & \text{if } 4 \mid d \text{ かつ } d_1 \equiv 2, 3 \mod 4, \\ d_2, & \text{otherwise} \end{cases} \tag{2.2}$$

により定義する. 実 2 次体 $K = \mathbb{Q}(\sqrt{d_1})$ を考え, $\mathcal{O}_f$ を導手 f の K の整環とする. それは, 有限指数 $(\mathcal{O}_K : \mathcal{O}_f) = f$ をもつ, K の整数環 $\mathcal{O}_K$ の 1 を含む部分環である. (Cox [5, p.133], Borevich-Shafarevich [2, p.88, Definition] を参照.) 具体的には,

$$\tilde{\omega} = \tilde{\omega}(d) := \begin{cases} (1 + \sqrt{d_1})/2, & \text{if } d_1 \equiv 1 \mod 4, \\ \sqrt{d_1}, & \text{if } d_1 \equiv 2, 3 \mod 4 \end{cases}$$

とおくと, $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z} f\tilde{\omega}$ と書くことができる. (Cox [5, Lemma 7.2] を参照.) $\mathcal{O}_f$ の判別式を D_d で表わすと,

$$D_d := \begin{vmatrix} 1 & f\tilde{\omega} \\ 1 & (f\tilde{\omega})' \end{vmatrix}^2 = D_{d_1} f^2. \tag{2.3}$$

ここで $(f\tilde{\omega})'$ は $f\tilde{\omega}$ の自明でない共役, D_{d_1} は実 2 次体 K の判別式である. D_d を **d の判別式**と簡単に呼ぶ. 導手 f_d の定義により次がわかる:

Lemma 2.1. *上の設定の下で, $d \equiv 0, 1 \mod 4$ のとき, $D_d = d$. $d \equiv 2, 3 \mod 4$ のときは, $D_d = 4d$ となる.*

Proof. (i) $4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$ のとき, $D_{d_1} = 4d_1$. $f = d_2/2$ だから, (2.3) により, $D_d = d$.

(ii) $4 \mid d$ かつ $d_1 \equiv 1 \mod 4$ のとき, $D_{d_1} = d_1$. $f = d_2$ だから, $D_d = d$.

(iii) $d \equiv 1 \bmod 4$ のとき, 分解 $d = d_1 d_2^2$ により $d_1 \equiv 1 \bmod 4$ だから, $D_{d_1} = d_1$. $f = d_2$ だから, $D_d = d$.

(iv) $d \equiv 2, 3 \bmod 4$ のとき, $4 \nmid d$, $d = d_1 d_2^2$ により d_2 は奇数. したがって, $d_1 \equiv 2, 3 \bmod 4$ だから, $D_{d_1} = 4d_1$. $f = d_2$ だから, $D_d = 4d$. □

このように d に対して, $d \equiv 0, 1 \mod 4$ のとき判別式 d の整環を, $d \equiv 2, 3 \mod 4$ のときは判別式 $4d$ の整環を対応させている.[2.1] $E_d > 1$ を整環 $\mathcal{O}_f$ の基本単数とし, E_d を **d の基本単数**と簡単に呼ぶ.

[2.1] 拡張された不変量の位置付けに関する説明は [15, Remark 2.4] にある.

Definition 2.1. E_d は $\mathcal{O}_K$ の元で $E_d > 1$ だから, $E_d = (t + u\sqrt{d_1})/2$, $t \equiv u \mod 2$ をみたす自然数 t, u が一意的に存在し, さらに $E_d \in \mathcal{O}_f$ より $f \mid u$ だから, $E_d = \{t + (u/f)f\sqrt{d_1}\}/2$ と書ける. そこで, d **の横井不変量** m_d を

$$m_d := \left[\frac{(u/f)^2}{t}\right] = \left[\frac{u^2}{tf^2}\right] \ (\geq 0)$$

により定義する. ここで, 実数 x に対して $[x]$ は x 以下の最大の整数を表わす.

Remark 2.1. d が平方因子をもたないとき, $f = 1$ だから, m_d は元の $\mathcal{O}_K = \mathcal{O}_1$ の横井不変量と一致する.[2.2]

$\mathcal{O}_f$ の invertible な分数イデアル全体の集合 $I(\mathcal{O}_f)$ を考える (Cox [5, Proposition 7.4] を参照). $I(\mathcal{O}_f)$ はイデアルの積により Abel 群をなし, 単項イデアル全体の集合 $P(\mathcal{O}_f)$ はその部分群になる. 商群 $Cl(\mathcal{O}_f) := I(\mathcal{O}_f)/P(\mathcal{O}_f)$ は $\mathcal{O}_f$ のイデアル類群と呼ばれ, 有限 Abel 群となり, その位数を

$$h_d := |Cl(\mathcal{O}_f)|$$

で表わす. これを d **の類数**と簡単に呼ぶことにする.

$$e_f := (\mathcal{O}_K^\times : \mathcal{O}_f^\times), \qquad a_f := \prod_{p \mid f}\left(1 - \frac{\chi_{d_1}(p)}{p}\right)$$

とおく. ここで, p は f のすべての素因数を動き, χ_{d_1} は $\mathbb{Q}(\sqrt{d_1})$ に対応する Kronecker 指標である. 整環の類数公式 (Cox [5, Theorem 7.24]) により, fa_f/e_f は自然数となり,

$$h_d = h_{d_1} \cdot (fa_f/e_f) \tag{2.4}$$

をみたす. h_{d_1} は実 2 次体 $\mathbb{Q}(\sqrt{d_1})$ の (広義の) 類数である. ([5, Theorem 7.24] では K を虚 2 次体と仮定しているが, その証明は実 2 次体にも働く.)

いま定義した不変量の基本性質を 3 つ述べる. まず, 平方でない自然数に関する Siegel の定理が成り立つ:

Proposition 2.2. *上の設定の下で,*

$$\lim_{d\to\infty} \frac{\log(h_d \log E_d)}{\log D_d} = \frac{1}{2}$$

が成り立つ. ここで d は平方でないすべての自然数を動く.

Remark 2.2. $d \to \infty$ のとき, Lemma 2.1 により $D_d \to \infty$ となる. 類数 h_d が小さいならば, Proposition 2.2 により基本単数 E_d は比較的大きいことがわかる ([17, Section 3] を参照). Section 6 において, イデアルのことば (整環の類数公式) と実 2 次体に関する Siegel [24] の結果を使って Proposition 2.2 を証明する. なお, 2 次形式に関する Siegel の定理 (Hua [11, Theorem 12.15.4]; 狭義のイデアル類群に対応する) から導くこともできる.

[2.2] [14, Definition 3.1] では, $4 \nmid d$ のとき連分数のことばで横井不変量を定義したが, 後述の Proposition 7.3 により, それは我々の m_d の値と一致する. [14, Tables 2 and 3], [17, Section 8] における数値例から, d が平方因子をもつか否かにかかわらず横井不変量 m_d の値は一定になることが観察できる. それで任意の平方でない自然数へ不変量を拡張して, それらの値を, とくに横井不変量と類数の値の変化を観察するのが得策であると考えた. これが不変量の拡張をする動機である.

上の設定の下で, $T := t$, $U := u/f$ とおくと T, U は自然数で, 導手 $f = f_d$ の定義により,

$$E_d = \begin{cases} (T+U\sqrt{d/4})/2, & \text{if } 4 \mid d \text{ かつ } d_1 \equiv 2, 3 \mod 4, \\ (T+U\sqrt{d})/2, & \text{otherwise} \end{cases} \tag{2.5}$$

をみたす. また,

$$\omega = \omega(d) := \begin{cases} \sqrt{d/4}, & \text{if } d \equiv 0 \mod 4, \\ (1+\sqrt{d})/2, & \text{if } d \equiv 1 \mod 4, \\ \sqrt{d}, & \text{if } d \equiv 2, 3 \mod 4 \end{cases} \tag{2.6}$$

とおく. そのとき, $\omega(d)$ は循環連分数になることがよく知られている:

$$\omega(d) = [a_0, \overline{a_1, \ldots, a_{\ell-1}, a_\ell}].$$

ここで ℓ は(最小)周期を表わす. さらに部分商 $a_1, \ldots, a_{\ell-1}$ は対称性: $a_n = a_{\ell-n}$, $1 \leq n \leq \ell-1$ をみたし, $\omega(d) = (1+\sqrt{d})/2$ のとき $a_\ell = 2a_0 - 1$, $\omega(d) = \sqrt{d/4}$ または $\sqrt{d}$ のときは $a_\ell = 2a_0$ をみたすことが知られている. また文献には見られないが, この特殊な形の 2 次無理数 $\omega(d)$ に関して, 対称部分 $a_1, \ldots, a_{\ell-1}$ のどの数字も末尾の数字 a_ℓ より小さいことがわかる ([13, p.878, Lines 13-8↑]). 次に, 平方でない自然数に関する横井の定理が成り立つ:

Proposition 2.3. 上の設定の下で次が成り立つ.

[A] 「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」の場合, $d > 12$ のとき $T \geq 5$. さらに

$$m_d = [T/(d/4)] = [U/\sqrt{d/4}] = [E_d/(d/4)].$$

[B] そうでない場合, 次が成り立つ.

(i) $d > 13$ かつ $d \neq 20$ のとき, $T \geq 5$.

以下, $d > 13$ と仮定する.

(ii) ℓ が偶数のとき,

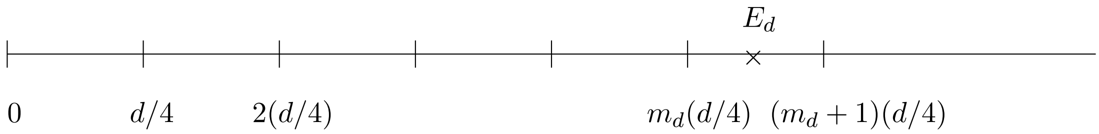
$$m_d d \leq T - 1 < U\sqrt{d} < E_d < T < (m_d+1)d. \tag{2.7}$$

(iii) ℓ が奇数のとき,

$$m_d d < T < E_d < U\sqrt{d} < T + 1 \leq (m_d+1)d. \tag{2.8}$$

(2.7) と (2.8) の両辺を d で割って, $m_d = [T/d] = [U/\sqrt{d}] = [E_d/d]$ を得る.

Remark 2.3. d が平方因子をもたないとき, $f = 1$. そして $d > 13$ ならば, Proposition 2.3 [B] により $m_d = [E_d/d]$, つまり「$m_d d < E_d < (m_d+1)d$」が成り立つ. よって, Yokoi の結果 [27, Theorem 1.1] を得る. このように Proposition 2.3 により, 「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」かそうでないかに従って, 横井不変量 m_d は $d/4$ または d に対する基本単数 E_d の大きさを測る量であることがわかる. [A] の場合:



m_d の値は, 単数基準 $\log E_d$ の代わりに E_d の大雑把な大きさを与えている. m_d が大きいとき E_d は原点 0 から遠ざかるから, 基本単数は大きいと考えてよい. Section 7 において Proposition 2.3 を証明する.

$\ell(d)$ を 2 次無理数 $\omega(d)$ の連分数展開の周期とする. 最後に, 平方でない自然数に関する Sasaki-Lachaud の定理が成り立つ. 証明は [23, Theorem 1] のそれと同じで良い.

Proposition 2.4 (Sasaki [23], Theorem 1; Lachaud [19], Theorem 2.2 を参照). ℓ, h を任意の自然数とする. このとき, $\ell = \ell(d)$ かつ $h = h_d$ をみたす平方でない自然数 d は有限個しか存在しない. すなわち, 各周期 ℓ において, 類数 h の平方でない自然数は有限個である.

Proof. 証明の概略を書く. Sasaki [23, Lemma 2] と同じ方針により,

$$(3/2)^{\ell(d)-2}\sqrt{d} < E_d < (2\sqrt{d})^{\ell(d)}$$

が示せる (後述の Proposition 7.3 と [13, Lemma 2.2] を参照). Lemma 2.1 により, $d \to \infty$ のとき $\sqrt{D_d} \to \infty$ だから, ある自然数 d_0 が存在して,

$$\frac{\log\log(3/2)}{\log D_d} < \frac{\log\left(\frac{1}{\ell(d)}\log E_d\right)}{\log D_d} < \frac{\log\log(2\sqrt{D_d})}{\log D_d} \qquad (\forall d \geq d_0)$$

となり,

$$\lim_{d\to\infty} \frac{\log\left(\frac{1}{\ell(d)}\log E_d\right)}{\log D_d} = 0 \tag{2.9}$$

が成り立つ. $h_d \log E_d = h_d \ell(d) \frac{1}{\ell(d)} \log E_d$ により,

$$\frac{\log(h_d \log E_d)}{\log D_d} = \frac{\log(h_d \ell(d))}{\log D_d} + \frac{\log\left(\frac{1}{\ell(d)}\log E_d\right)}{\log D_d}. \tag{2.10}$$

いま $\ell = \ell(d)$ かつ $h = h_d$ をみたす平方でない自然数 d は無限個存在すると仮定し, $\ell = \ell(d_n)$ かつ $h = h_{d_n}$ をみたす平方でない自然数の狭義単調増加列 $\{d_n\}_{n\geq 1}$ を取り出す. そのとき, (2.10) と (2.9) により,

$$\lim_{n\to\infty} \frac{\log(h_{d_n} \log E_{d_n})}{\log D_{d_n}} = \lim_{n\to\infty} \frac{\log(h\ell)}{\log D_{d_n}} = 0.$$

これは Siegel の定理 (Proposition 2.2) に反する. このように主張がわかる. □

Remark 2.4. (2.10) と (2.9) により,

$$\lim_{d\to\infty} \frac{\log(h_d \log E_d)}{\log D_d} = \lim_{d\to\infty} \frac{\log(h_d \ell(d))}{\log D_d}.$$

したがって,

$$\lim_{d\to\infty} \frac{\log(h_d \ell(d))}{\log D_d} = \frac{1}{2} \tag{2.11}$$

は Proposition 2.2 と同値となり, それゆえ (2.11) は成り立つ.

3　極小型自然数と極小型実 2 次体

d を平方でない自然数とし, (2.1) のように d を $d = d_1 d_2^2$ と分解する．(2.6) のような 2 次無理数の連分数展開: $\omega = \omega(d) = [a_0, \overline{a_1, \ldots, a_{\ell-1}, a_\ell}]$ を考える．その対称部分 $a_1, \ldots, a_{\ell-1}$ から漸化式

$$\begin{cases} p_0 = 1,\ p_1 = a_0,\ p_n = a_{n-1}p_{n-1} + p_{n-2}, \\ q_0 = 0,\ q_1 = 1,\ q_n = a_{n-1}q_{n-1} + q_{n-2}, \qquad n \geq 2 \\ r_0 = 1,\ r_1 = 0,\ r_n = a_{n-1}r_{n-1} + r_{n-2}, \end{cases} \tag{3.1}$$

により,

$$A := q_\ell, \quad B := q_{\ell-1}, \quad C := r_{\ell-1}$$

を計算し, 整数係数 1 次多項式 $g(x)$, $h(x)$ と整数係数 2 次多項式 $f(x)$ を

$$g(x) := Ax - (-1)^\ell BC; \quad h(x) := Bx - (-1)^\ell C^2; \quad f(x) := g(x)^2 + 4h(x)$$

により定める．(p_n の漸化式は下で使う.) さらに s_0 を $g(s) > 0$, つまり, $s > (-1)^\ell BC/A$ をみたす最小の整数 s とする．このとき, $d \equiv 0$ (resp. $d \equiv 1$, $d \equiv 2, 3$) mod 4 に従って, $d/4 = f(s)/4$ (resp. $d = f(s)$, $d = f(s)/4$) をみたす整数 $s \geq s_0$ が唯 1 つ存在する．これは Friesen and Halter-Koch の定理 ([13, Theorem 3.1] の主張 [B]) によりわかる．それは Friesen [7] と Halter-Koch [9] による結果の改善である．ここで, もし $s = s_0$ ならば $d/4$ (resp. d, d) は $\sqrt{d/4}$ **(resp.** $(1+\sqrt{d})/2$**,** $\sqrt{d}$**) に関する周期** ℓ **の極小型自然数**という ([13, Definition 3.1])．$d > 1$ が平方因子をもたないとき実 2 次体 $\mathbb{Q}(\sqrt{d})$ を考える．そのとき, $d \equiv 1, 2, 3$ mod 4. $d \equiv 1$ (resp. $d \equiv 2, 3$) mod 4 のとき d が $(1+\sqrt{d})/2$ (resp. $\sqrt{d}$) に関する周期 ℓ の極小型自然数ならば $\mathbb{Q}(\sqrt{d})$ を**周期** ℓ **の極小型実 2 次体**と呼ぶ．横井不変量 m_d の別の表示を導入する．簡単のために

$$\lambda := \frac{A^2}{g(s)A + 2B}$$

とおく．

Lemma 3.1. *上の設定の下で,「$4 \mid d$ かつ $d_1 \equiv 1 \mod 4$」または $d \equiv 1 \mod 4$ のとき, $m_d = [\lambda]$.「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」または $d \equiv 2, 3 \mod 4$ のときは, $m_d = [4\lambda]$ が成り立つ.*

Proof. $d \not\equiv 1 \mod 4$ ならば, 後述の表 7.1 の G_ℓ と Q_0 の定義により, $p_\ell = G_\ell/Q_0$. よって, $p_\ell = a_0 q_\ell + r_\ell$ から,

$$a_\ell q_\ell = 2a_0 q_\ell = 2((G_\ell/Q_0) - r_\ell).$$

$d \equiv 1 \mod 4$ ならば, 同様に $Q_0 = 2$ だから,

$$a_\ell q_\ell = (2a_0 - 1)q_\ell = 2((G_\ell/Q_0) - r_\ell)$$

を得る．したがって, $g(s) = a_\ell$ ([13] の等式 (3.4)), $q_{\ell-1} = r_\ell$ ([13, Lemma 2.1] の等式 (2.5)) により,

$$g(s)A + 2B = a_\ell q_\ell + 2q_{\ell-1} = 2((G_\ell/Q_0) - r_\ell) + 2q_{\ell-1} = 2(G_\ell/Q_0).$$

ゆえに, $\lambda = q_\ell^2/(2(G_\ell/Q_0))$. 始めに,「$4 \mid d$ かつ $d_1 \equiv 1 \mod 4$」または $d \equiv 1 \mod 4$ の場合を考える．$Q_0 = 2$ だから, $\lambda = q_\ell^2/G_\ell = (2q_\ell^2)/(G_\ell Q_0)$. よって, 後述の Proposition 7.3 は

$[\lambda]=m_d$ を導く．次に，「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」または $d \equiv 2, 3 \mod 4$ の場合を考える．$Q_0=1$ だから，$4\lambda=(2q_\ell^2)/G_\ell=(2q_\ell^2)/(G_\ell Q_0)$．よって，後述の Proposition 7.3 は $[4\lambda]=m_d$ を導く． □

Lemma 3.1 を使って，[13, Proposition 4.2] とまったく同じ計算により次がわかる．

Proposition 3.2. $d \equiv 0$ (resp. $d \equiv 1$, $d \equiv 2, 3$) $\mod 4$ に従って，$d/4$ (resp. d, d) は $\sqrt{d/4}$ (resp. $(1+\sqrt{d})/2$, $\sqrt{d}$) に関する周期 ℓ の極小型でない自然数であると仮定する．このとき，「$4 \mid d$ かつ $d_1 \equiv 1 \mod 4$」または $d \equiv 1 \mod 4$ ならば，$m_d=0$．「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」または $d \equiv 2, 3 \mod 4$ ならば，$0 \le m_d \le 3$ が成り立つ．

このように極小型でない自然数 d の横井不変量 m_d の値は小さい．

Friesen and Halter-Koch の定理により上の逆が成り立つことが重要である．すなわち，任意に $\ell-1$ 個の対称な自然数の列 $a_1,\ldots,a_{\ell-1}$ が与えられたとき，それを連分数展開の対称部分にもつ 2 次無理数 $\omega(d)$ を作ることができる．そのために上と同じ手順で整数 A, B, C を計算して，次の 3 つの場合分けを考える:

$$\text{(I) } A \equiv 1 \mod 2,\quad \text{(II) } (A,C) \equiv (0,0) \mod 2,\quad \text{(III) } (A,C) \equiv (0,1) \mod 2.$$

Theorem 3.3 (Friesen, Halter-Koch; [13] Theorem 3.1). 自然数 ℓ を固定し，$a_1,\ldots,a_{\ell-1}$ を任意の対称な自然数の列とする．

(i) *Case* (I) または *Case* (III) が起こるときに限り，次の手順で $d \equiv 1 \mod 4$ をみたす $(1+\sqrt{d})/2$ の連分数展開 (3.3) を作ることができる：s を s_0 以上の任意の整数とし，$d := f(s)$, $a_0 := (g(s)+1)/2$ とおく．ここで $\ell \ge 2$ のとき

$$g(s) > a_1,\ldots,a_{\ell-1} \tag{3.2}$$

が成り立つと仮定し，*Case* (I) のときにはさらに s を奇数として取る．このとき，d, a_0 は自然数，d は平方数でなく，$d \equiv 1 \mod 4$, $a_0=[(1+\sqrt{d})/2]$ をみたし，

$$(1+\sqrt{d})/2=[a_0,\overline{a_1,\ldots,a_{\ell-1},2a_0-1}] \tag{3.3}$$

は $(1+\sqrt{d})/2$ の周期 ℓ の連分数展開となる．

(ii) *Case* (I) または *Case* (II) が起こるときに限り，次の手順で $\sqrt{d}$ の連分数展開 (3.4) を作ることができる：s を s_0 以上の任意の整数とし，$d := f(s)/4$, $a_0 := g(s)/2$ とおく．ここで $\ell \ge 2$ のとき (3.2) が成り立つと仮定し，*Case* (I) のときにはさらに s を偶数として取る．このとき，d, a_0 は自然数，d は平方数でなく，$a_0=[\sqrt{d}]$ をみたし，

$$\sqrt{d}=[a_0,\overline{a_1,\ldots,a_{\ell-1},2a_0}] \tag{3.4}$$

は $\sqrt{d}$ の周期 ℓ の連分数展開となる．

条件 (3.2) は，対称部分 $a_1,\ldots,a_{\ell-1}$ のどの数字も末尾の数字 $g(s)$ より小さいことを表現している．これにより上の連分数展開の最小周期が ℓ となることがわかる．なお，$s>s_0$ のときには条件 (3.2) は自動的にみたされるので確かめる必要はない ([14, Remark 2.2] を参照)．この Friesen and Halter-Koch の定理は具体例を計算してみると実感がわく．

極小型実 2 次体の作り方

$\ell=4$ とし，3 個の対称な自然数の列 $2,1,2$ を考える．

			2	1	2
n	0	1	2	3	4
q_n	0	1	2	$B=3$	$A=8$
r_n	1	0	1	$C=1$	3

$(A,C)\equiv(0,1) \mod 2$ だから, Case (III) が起こる.

$$(-1)^\ell\frac{BC}{A}=\frac{3\cdot 1}{8}=\frac{3}{8}$$

により, $s_0=1$. また, $g(x)=8x-3\cdot 1=8x-3,\ \ h(x)=3x-1^2=3x-1$.

そこで始めに, $s=1$ と取る. そのとき, $g(1)=8-3=5>2,1,\ \ h(1)=3-1=2$. $a_0:=(g(1)+1)/2=3,\ \ d:=f(1)=5^2+4\cdot 2=25+8=33$ ($\equiv 1 \mod 4$) とおくと, Theorem 3.3 (i) により $(1+\sqrt{33})/2=[3,\overline{2,1,2,5}]$ が成り立つ. $\mathbb{Q}(\sqrt{33})$ は周期 4 の極小型実 2 次体となる. さらに $s=2,3,\ldots$ を代入して行くと, 周期 4 の極小型でない実 2 次体が現れる.

s	1	2	3	4	5	$\ldots$
d	33	189	473	885	1425	$\ldots$
d の素因数分解	$3\cdot 11$	$3^3\cdot 7$	$11\cdot 43$	$3\cdot 5\cdot 59$	$3\cdot 5^2\cdot 19$	$\ldots$
h_d	1	1	3	2	6	$\ldots$
m_d	1	0	0	0	0	$\ldots$

$\mathbb{Q}(\sqrt{473})$, $\mathbb{Q}(\sqrt{885})$ は周期 4 の極小型でない実 2 次体となる. この表では Section 2 で定義した d の類数 h_d と横井不変量 m_d も計算している.

[14] では特殊な対称な自然数の列を取り, ℓ が $8\nmid\ell$ をみたす 4 以上の偶数のとき, 周期 ℓ の極小型自然数を構成し, 与えられた任意の自然数より大きな類数をもち, かつ与えられた任意の正の値より大きな横井不変量をもつ周期 ℓ の極小型実 2 次体の無限族が構成されている. 極小型自然数に関する基本的未解決問題については Section 5.3 で述べる.

4 Ankeny-Artin-Chowla 予想

この Section では $\mathbb{Q}(\sqrt{d})$ を任意の実 2 次体とする. ここで $d>1$ は平方因子をもたない自然数である: $d=d_1$. ε_d $(=E_{d_1})>1$ をその基本単数とし, ある自然数 t_d, u_d を使って $\varepsilon_d=(t_d+u_d\sqrt{d})/2$ と一意的に書く. 次の予想を扱う Hashimoto [10] の解説をする.

Ankeny-Artin-Chowla 予想 (AAC 予想と略す). p は $p\equiv 1 \mod 4$ をみたす素数とする. このとき, 実 2 次体 $\mathbb{Q}(\sqrt{p})$ について, $p\nmid u_p$ が成り立つ.

ここで $\mathbb{Q}(\sqrt{p})$ は奇数周期 (基本単数のノルムが -1) の体となる (Remark 5.1 を参照). $p\equiv 3 \mod 4$ の場合, $\mathbb{Q}(\sqrt{p})$ は偶数周期の体で, t_p, u_p は共に偶数になるが, $p\nmid(u_p/2)$ が成り立つと考えられているようである. [10] の主結果は異なる定式化をしているが, 極小型実 2 次体のことばを使うと次のように明解に再定式化できる. 定式化の違いは Section 4.1 で説明する. Section 3 のように 2 次無理数 $\omega(d)$ の連分数展開の対称部分から整数 A, B, C, s, s_0 と整数係数多項式 $g(x)$, $h(x)$, $f(x)$ を計算する.[4.1]

[4.1] [10] では, q_n, r_n の番号 n は -1 から始まり, 0 から始める我々のものとは 1 つずれていることに注意.

Proposition 4.1 (Hashimoto [10], Theorem 3.4). 上の設定の下で, $\mathbb{Q}(\sqrt{d})$ は周期 ℓ の極小型でない実 2 次体であると仮定する．このとき, $d \equiv 1 \mod 4$ ならば, $d > u_d$. $d \equiv 2, 3 \mod 4$ ならば, $d > u_d/2$ が成り立つ.

Remark 4.1. $\ell \le 5$ のときは上の結論がいつも ($\mathbb{Q}(\sqrt{d})$ が極小型でも) 成り立つことがわかる.

Proof of Proposition 4.1. $A > 0$ より 1 次関数 $g(x)$ は狭義単調増加である．仮定により $s > s_0$ だから,

$$g(s) \ge g(s_0+1) = A(s_0+1) - (-1)^\ell BC > A \cdot (-1)^\ell BC/A + A - (-1)^\ell BC = A.$$

よって, $g(s) \ge A+1$. また $h(s) > 0$ ([13] の等式 (3.7)) が成り立つ．連分数に慣れるためにこれを示してみる．n に関する帰納法により,

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{\ell-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_\ell & q_{\ell-1} \\ r_\ell & r_{\ell-1} \end{pmatrix}$$

が成り立つことがわかる．$a_1, \ldots, a_{\ell-1}$ は対称な自然数の列だから, 上の左辺は対称行列となる．したがって, $q_{\ell-1} = r_\ell$. 両辺の行列式を取ると,

$$(-1)^{\ell-1} = q_\ell r_{\ell-1} - q_{\ell-1} r_\ell = q_\ell r_{\ell-1} - q_{\ell-1}^2,$$

それで, $B^2 - AC = (-1)^\ell$ を得る．よって $s \ge s_0 > (-1)^\ell BC/A$ により,

$$\begin{aligned} h(s) &> B \cdot (-1)^\ell BC/A - (-1)^\ell C^2 = (-1)^\ell \frac{C}{A}(B^2 - AC) \\ &= (-1)^\ell \frac{C}{A} \cdot (-1)^\ell = \frac{C}{A} \ge 0. \end{aligned}$$

このように, $h(s) > 0$ がわかる．ゆえに,

$$f(s) = g(s)^2 + 4h(s) > g(s)^2 \ge (A+1)^2. \tag{4.1}$$

Section 7 で見るように, 連分数による (整環の) 基本単数の計算方法が知られている．Proposition 7.3 の証明 (等式 (7.1)) により, $d \equiv 1$ (resp. $d \equiv 2, 3$) mod 4 ならば, $\varepsilon_d = (2p_\ell - q_\ell + q_\ell\sqrt{D_d})/2$ (resp., $= (2p_\ell + q_\ell\sqrt{D_d})/2$) となる．Lemma 2.1 により $D_d = d$ (resp., $= 4d$) だから, $u_d = q_\ell$ (resp., $= 2q_\ell$) がわかる．始めに, $d \equiv 1 \mod 4$ を仮定する. $d = f(s)$ だから, (4.1) により $d > (A+1)^2 > A$. $A = q_\ell = u_d$ により, $d > u_d$ を得る．次に $d \equiv 2, 3 \mod 4$ を仮定し, $d > A$ を示す.

• $\ell = 1$ のとき．$A = q_1 = 1$ だから, $d > 1 = A$.

• $\ell = 2$ のとき．[13, Example 3.5] で見たように, $A = a_1$, $B = 1$, $C = 0$, $s_0 = 1$. よって, $f(x) = g(x)^2 + 4h(x) = (a_1x)^2 + 4x$. d は $\sqrt{d}$ に関して極小型でないから, $s \ge 2$. $4d = f(s)$ だから, $4d = f(s) = (a_1s)^2 + 4s > 4a_1$. よって, $d > A$.

• $\ell = 3$ のとき．[13, Example 3.5] で見たように, $A = a_1^2 + 1$, $B = a_1$, $C = 1$, $s_0 = 0$. よって, $f(x) = g(x)^2 + 4h(x) = \{(a_1^2+1)x + a_1\}^2 + 4(a_1x + 1)$. a_1 が偶数ならば Case (I) が起こり, a_1 が奇数なら Case (III) が起こる．d は $\sqrt{d}$ に関して極小型でないから, $s \ge 1$. Friesen and Halter-Koch の定理 ([13, Theorem 3.1] の主張 [B, A-i]) により, Case (I) が起こり, s は偶数．したがって $s \ge 2$ だから,

$$4d = f(s) > \{2(a_1^2+1) + a_1\}^2 > 4(a_1^2+1).$$

よって, $d > A$.

• $\ell \geq 4$ のとき. $A = q_\ell \geq q_4 = a_3(a_2a_1+1)+a_1 \geq 3$. $4d = f(s)$ だから, (4.1) により, $4d > (A+1)^2 \geq 4(A+1) > 4A$. よって, $d > A$.

以上からいつも $d > A$ が成り立つ. $A = q_\ell = u_d/2$ だから, $d > u_d/2$ を得る. □

Remark 4.2. 一般に任意の平方でない自然数 d に対して, $d \equiv 0$ (resp. $d \equiv 1$, $d \equiv 2, 3$) mod 4 に従って, $d/4$ (resp. d, d) は $\sqrt{d/4}$ (resp. $(1+\sqrt{d})/2$, $\sqrt{d}$) に関する周期 ℓ の極小型でない自然数であると仮定する. このとき, 「$4 \mid d$ かつ $d_1 \equiv 1 \mod 4$」または $d \equiv 1 \mod 4$ ならば, $d > U$. 「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」ならば, $d/4 > U/2$. $d \equiv 2, 3 \mod 4$ ならば, $d > U/2$ が成り立つ. ここで, 「$4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$」のとき $E_d = (T + U\sqrt{d/4})/2$. そうでないときは, $E_d = (T + U\sqrt{d})/2$. E_d は d の基本単数である. 証明は Proposition 4.1 のそれと同じで, Proposition 7.3 を使えば良い.

このように極小型でない実 2 次体 $\mathbb{Q}(\sqrt{d})$ の不変量 u_d の値は比較的小さいことがわかる. なお, 各周期において極小型でない実 2 次体は無限個存在することが知られている. (Friesen と Halter-Koch による結果. [13, Section 8.1], [17, Section 3] を参照.) $p \equiv 1 \mod 4$ のとき, $\mathbb{Q}(\sqrt{p})$ が極小型でない実 2 次体ならば, $p > u_p$ だから $p \nmid u_p$, すなわち AAC 予想は正しい. $p \equiv 3 \mod 4$ のときは, $\mathbb{Q}(\sqrt{p})$ が極小型でない実 2 次体ならば, $p > u_p/2$ だから $p \nmid (u_p/2)$ が成り立つ. 一方 Cohen and Lenstra [4] によると, 実 2 次体の無限族 $\mathbb{Q}(\sqrt{p})$, $p \equiv 1 \mod 4$ のうち約 75 パーセントの体の類数は 1 になるだろうと試算している. そして [13, Proposition 4.4] により, 類数 1 の極小型でない実 2 次体は, 1 つの例外を除くと 51 個の体に限る. したがって, この無限族の中の極小型でない実 2 次体の割合は約 25 パーセント以下であると試算される. よって, Proposition 4.1 により, 残された多くの極小型の体に対して AAC 予想の正当性を確かめなければならない. この予想の解決にはまだ手が届かないことが納得できる.

Example 4.1. e を任意の自然数とする. $d > u_d$ をみたす周期 $4(2e+1)$ の極小型実 2 次体 $\mathbb{Q}(\sqrt{d})$, $d \equiv 1 \mod 4$ は無限個存在することがわかる ([14] における Proposition 4.3 と Proposition 4.5 の証明を参照). また, $d > u_d/2$ をみたす周期 $2(2e+1)$ の極小型実 2 次体 $\mathbb{Q}(\sqrt{d})$, $d \equiv 2, 3 \mod 4$ も無限個存在することがわかる ([14] における Proposition 4.1 と Proposition 4.4 の証明 (i) を参照). 一方 $d = 89\,(\equiv 1)$ と取ると, $d < u_d = 106$ かつ $89 \nmid u_{89}$ ($\underline{\ell = 7}$). $d = 19\,(\equiv 3)$ と取ると, $d < u_d/2 = 39$ かつ $19 \nmid (u_{19}/2)$ ($\underline{\ell = 6}$). このように $\ell = 7$, 6 ではそれぞれ $d < u_d$, $d < u_d/2$ となる例がある. また, $d = 4801\,(\equiv 1)$ と取ると,

$$d < u_d = 19130659731728835141354500676990161829234916493 0$$

かつ $4801 \nmid u_{4801}$ ($\ell = 101$). $d = 2566 = 2 \cdot 1283\,(\equiv 2)$ と取ると,

$$d < u_d/2 = 3374781873712813288079701917958005584807887406 58$$

($\ell = 102$). このように d に比べて u_d の値が極端に大きくなることもある.

4.1 主結果 [10, Theorem 3.4] の再定式化

橋本氏の主結果 [10, Theorem 3.4] (および [10, p.145]) には「one possible exception」ということばが現れるが, そのことばの定義はない. そこで極小型自然数のことばを使ってその主結果の再定式化を行う. [10] では, AAC 予想を扱うために $a_1, \ldots, a_L$ を $L\,(\geq 1)$ 個の任意

の自然数とし, $\ell := 2L+1$ とおく. $\ell-1\,(=2L)$ 個の対称な自然数の列 $a_1,\dots,a_L,a_L,\dots,a_1$ に対して集合

$$\begin{aligned} S(\ell;a_1,\dots,a_L) := \{&d : \text{平方でない自然数} \mid d\equiv 1 \mod 4,\\ &a_0 := [(1+\sqrt{d})/2],\ (1+\sqrt{d})/2 = [a_0,\overline{a_1,\dots,a_L,a_L,\dots,a_1,2a_0-1}]\} \end{aligned}$$

を考えている. 上の連分数展開は ℓ が最小周期となることを想定していないことに注意する ([10, Remark 2.5] を参照). 集合 $S(\ell;a_1,\dots,a_L)$ を周期 ℓ によって定めるためには, 対称部分のどの数字も末尾の数字より小さいという条件 (3.2) が必要である. (この性質は, $(1+\sqrt{7})/2=[1,\overline{1,4,1,1}]$ のような例があるから,「$\omega(d)=(1+\sqrt{d})/2$ かつ $d\equiv 3 \mod 4$」の場合には崩れる.) [10] では性質 (3.2) の重要性が意識されなかった. そこで改めて,

$$\begin{aligned} \tilde{S}(\ell;a_1,\dots,a_L) := \{&d : \text{平方でない自然数} \mid d\equiv 1 \mod 4,\\ &a_0 := [(1+\sqrt{d})/2],\ (1+\sqrt{d})/2 = [a_0,\overline{a_1,\dots,a_L,a_L,\dots,a_1,2a_0-1}]\ (\ell\ \text{は最小周期})\ \} \end{aligned}$$

という集合を考えることにする. すなわち $\tilde{S}(\ell;a_1,\dots,a_L)$ は, $d\equiv 1 \mod 4$ かつ

$$(1+\sqrt{d})/2 = [a_0,\overline{a_1,\dots,a_L,a_L,\dots,a_1,2a_0-1}]$$

が $(1+\sqrt{d})/2$ の (最小) 周期 ℓ の連分数展開となる平方でない自然数 d 全体の集合である. ここで $a_0 := [(1+\sqrt{d})/2]$ とおく. さらに我々の Case 分けはなされていないが ([10, Proposition 3.1] を参照), それに相当する条件が [10, Proposition 4.1] で述べられている.

$\ell-1$ 個の対称な自然数の列 $a_1,\dots,a_L,a_L,\dots,a_1$ から漸化式 (3.1) により, 非負整数 $A:=q_\ell$, $B:=q_{\ell-1}$, $C:=r_{\ell-1}$ を計算し, 整数係数 1 次多項式 $g(x)$, $h(x)$ と整数係数 2 次多項式 $f(x)$, 整数 s_0 を定める. $\ell\ (\geq 3)$ は奇数だから, [14, Lemma 2.3] により, この対称な自然数の列に関して Case (I) または Case (III) が起こる. Theorem 3.3 (i) と [14, Remark 2.2] から, $\tilde{S}(\ell;a_1,\dots,a_L)$ は空でないことがわかる ([10, Proposition 4.1] を参照). ($s>s_0$ をみたす (適切な) 整数 s を取れば, [14, Remark 2.2] により性質 (3.2) がみたされ, ℓ が $(1+\sqrt{d})/2$ の連分数展開の最小周期となる平方でない自然数 d が作れる. 実際は $\tilde{S}(\ell;a_1,\dots,a_L)$ は無限集合である.) したがって, $\tilde{S}(\ell;a_1,\dots,a_L)$ の最小元 d_0 が存在する:

$$d_0 := \min \tilde{S}(\ell;a_1,\dots,a_L).$$

さらに 2 次関数 $f(x)$ は区間 $[s_0,\infty)$ で狭義単調増加であることに注意する ([13, p.878, Lines 6-10↓]). 主結果の内容を次のように解釈する:

Proposition 4.2 (Hashimoto [10], Theorem 3.4). 上の設定の下で次が成り立つ.

(i) p を $p\in\tilde{S}(\ell;a_1,\dots,a_L)$ をみたす任意の素数とする. このとき, p が $(1+\sqrt{p})/2$ に関する周期 ℓ の極小型でない自然数ならば $p>u_p$ が成り立つ. とくに, $d_0<p$ ならば $p>u_p$.

(ii) 最小元 d_0 は素数であると仮定し, $p:=d_0$ とおく. さらに p は $(1+\sqrt{p})/2$ に関する周期 ℓ の極小型自然数であると仮定する. このとき,

$$p=(As+BC)^2+4(Bs+C^2)$$

と書ける. ここで非負整数 A, B, C は, $(1+\sqrt{p})/2$ の連分数展開の対称部分から求まる $A=q_\ell$, $B=q_{\ell-1}$, $C=r_{\ell-1}$ である. また, s は $-BC/A$ 以上の 最小の整数である.

Proof. Friesen and Halter-Koch の定理と Proposition 4.1 を使って証明する．$d \in \tilde{S}(\ell; a_1, \ldots, a_L)$ とする．Friesen and Halter-Koch の定理 ([13], Theorem 3.1 [B]) により, $d = f(s)$ をみたす整数 $s \geq s_0$ が唯 1 つある．Case (I) が起こっていれば s は奇数でなければならない ([13, p.878, Lines 12-20↓])．最小元 d_0 について見る．

• Case (I) が起こるとき．s_0 が奇数ならば, Theorem 3.3 (i) により, $f(s_0) \in \tilde{S}(\ell; a_1, \ldots, a_L)$ かつ $d_0 = f(s_0)$ となる．s_0 が偶数ならば, $f(s_0) \notin \tilde{S}(\ell; a_1, \ldots, a_L)$, $f(s_0+1) \in \tilde{S}(\ell; a_1, \ldots, a_L)$. 2 次関数 $f(x)$ は区間 $[s_0, \infty)$ で狭義単調増加であるから, $d_0 = f(s_0 + 1)$. (このように d_0 は極小型自然数ではない．Example 4.2 を参照.)

• Case (III) が起こるとき．Theorem 3.3 (i) により, $f(s_0) \in \tilde{S}(\ell; a_1, \ldots, a_L)$ かつ $d_0 = f(s_0)$ となる．

(i) p を $p \in \tilde{S}(\ell; a_1, \ldots, a_L)$ をみたす任意の素数とする．Friesen and Halter-Koch の定理 ([13], Theorem 3.1 [B]) により, $p = f(s)$ をみたす整数 $s \geq s_0$ が唯 1 つある．p が極小型でない, すなわち, $s_0 < s$ ならばProposition 4.1 により $p > u_p$ が成り立つ．また上で見たように $d_0 = f(s_0)$ または $d_0 = f(s_0 + 1)$ だから, もし $d_0 < p$ ならば $s_0 < s$ を得る．(2 次関数 $f(x)$ は区間 $[s_0, \infty)$ で狭義単調増加である.) よって, p は極小型でないから, Proposition 4.1 により $p > u_p$ が成り立つ.

(ii) d_0 は素数であると仮定し, $p := d_0$, $a_0 := [(1 + \sqrt{p})/2]$ とおく．$p \in \tilde{S}(\ell; a_1, \ldots, a_L)$ だから, 周期 ℓ の連分数展開

$$(1 + \sqrt{p})/2 = [a_0, \overline{a_1, \ldots, a_L, a_L, \ldots, a_1, 2a_0 - 1}]$$

をもつ．p は極小型であるから, $p = f(s_0)$ と書ける．ここで,

$$f(x) := (Ax - (-1)^\ell BC)^2 + 4(Bx - (-1)^\ell C^2).$$

$\ell \geq 3$ だから, $(-1)^\ell BC/A$ は整数でないことを主張する．これは次のように示せる: n に関する帰納法により, $n \geq 4$ のとき $r_{n-1} < q_{n-1}$ がわかる．これから $\ell \geq 2$ のとき $C = r_{\ell-1} < q_\ell = A$ を得る．$(-1)^\ell BC/A$ は整数であると仮定する．よって, $A \mid BC$. Proposition 4.1 の証明で見た等式 $B^2 - AC = (-1)^\ell$ により A と B は互いに素だから, $A \mid C$. $\ell \geq 3$ により C は 0 ではない．ゆえに $A \leq C$ となり, $C < A$ に反する．このように $(-1)^\ell BC/A$ は整数でない．したがって ℓ は奇数だから, 整数 s は $(-1)^\ell BC/A$ より大きい最小の整数となる．よって s_0 の定義により, $s_0 = s$. このように主張 (ii) がわかる．($\ell = 1$, 2 のとき $(-1)^\ell BC/A = 0$, $s_0 = 1$ となる.) □

Example 4.2. $L = 3$, $a_1 = 3$, $a_2 = 4$, $a_3 = 7$ と取ると, $A = 9005$, $B = 2778$, $C = 857$, $s_0 = -264$, Case (I) が起こる．$s_0 = -264$ は奇数ではないから, $\tilde{S}(7; 3, 4, 7)$ の最小元 d_0 は, $d_0 = f(s_0 + 1) = f(-263) = 154545101$ となる．また小さい順に元を並べると,

$$\tilde{S}(7; 3, 4, 7) = \{154545101, 926692045, 2347559189, 4417146533, 7135454077, \ldots\}.$$

$p := d_0 = 154545101$ は素数で, p は $(1 + \sqrt{p})/2$ に関する周期 7 の極小型でない自然数である．Proposition 4.2 (i) により $p > u_p$. 確かに, $p = 154545101 > 9005 = A = u_p$ が成り立つ.

参考のために [10] の他結果の再定式化を述べる.

Proposition 4.3 (Hashimoto [10], Theorem 4.2). $\mathbb{Q}(\sqrt{d})$ を実 2 次体とし, $d \equiv 1 \bmod 4$, $A = q_\ell$ は奇数, s_0 は偶数であると仮定する．このとき, $\mathbb{Q}(\sqrt{d})$ は周期 ℓ の極小型でない実 2 次体であり, $d > u_d$ が成り立つ.

Proof. A が奇数だから, 対称な自然数の列 $a_1, \ldots, a_{\ell-1}$ に関して Case (I) が起こっている．したがって s は奇数でなければならない ([13, p.878, Lines 12-20↓]). s_0 は偶数だから, $s > s_0$. よって, $\mathbb{Q}(\sqrt{d})$ は極小型でない実 2 次体であり, Proposition 4.1 により $d > u_d$. □

Proposition 4.4 (Hashimoto [10], Corollary 5.1). $\mathbb{Q}(\sqrt{d})$ を $\omega(d)$ の連分数展開の対称部分が一定 $(a_1 = \cdots = a_{\ell-1})$ の実 2 次体とする．このとき, $d \equiv 1 \mod 4$ ならば, $d > u_d$. $d \equiv 2, 3 \mod 4$ ならば, $d > u_d/2$ が成り立つ.

Proof. 対称部分が一定の体は Louboutin [20, Section 5] で扱われている．対称部分が一定だから, $\mathbb{Q}(\sqrt{d})$ は周期 ℓ の極小型でない実 2 次体になる ([13, Example 3.5] を参照). よって Proposition 4.1 から主張がわかる． □

5 Gauss 予想

実 2 次体の類数を調べるために d を $4 \nmid d$ をみたす平方でない自然数とし, 簡単のために (2.6) における 2 次無理数 $\omega(d)$ の連分数展開の周期を $\ell(d)$ で表わす. 大雑把な推測により各周期における最小元に注目する ([18, Section 3.1] を参照). それに基づく数値実験の結果を報告する．任意の自然数 ℓ と $\delta = 1, 2, 3$ に対して,

$$\mathrm{CF}_{\ell,\delta} := \{d : \text{平方でない自然数} \mid \ell = \ell(d) \text{ かつ } d \equiv \delta \mod 4\},$$

すなわち, $\ell = \ell(d)$ かつ $d \equiv \delta \mod 4$ をみたす平方でない自然数 d 全体の集合を考え,

$$\mathrm{CF}_\ell := \mathrm{CF}_{\ell,1} \cup \mathrm{CF}_{\ell,2} \cup \mathrm{CF}_{\ell,3}$$

とおく．CF_ℓ は $\ell = \ell(d)$ かつ $4 \nmid d$ をみたす平方でない自然数 d 全体の集合である．よく知られているように, $d \equiv 3 \mod 4$ のとき $\sqrt{d}$ の連分数展開の周期 $\ell(d)$ は偶数になる. ($d \equiv 3 \mod 4$ だから $p \equiv 3 \mod 4$ をみたす d の素因数 p がある．$p_\ell^2 - dq_\ell^2 = (-1)^{\ell(d)}$ が成り立つ ([14, Lemma 2.7] を参照). これより $\ell(d)$ が奇数ならば, -1 は mod p で平方剰余となり矛盾を得る.) よって, ℓ が奇数ならば $\mathrm{CF}_{\ell,3}$ は空集合である: $\mathrm{CF}_{\ell,3} = \emptyset$. それで以下では, $\delta = 3$ のとき ℓ は偶数であると仮定する．そのとき, 任意の自然数 ℓ と $\delta = 1, 2, 3$ に対して, 次の Proposition 5.1 により

$$\mathrm{CF}_{\ell,\delta} \neq \emptyset, \quad \text{したがって, } \mathrm{CF}_\ell \neq \emptyset$$

がわかる．

$$\begin{cases} c_0 = 0,\ c_1 = 1,\ c_n = 4c_{n-1} + c_{n-2}, \\ e_0 = 0,\ e_1 = 1,\ e_n = 2e_{n-1} + e_{n-2}, & \qquad n \geq 2 \\ f_0 = 0,\ f_1 = 1,\ f_n = f_{n-1} + f_{n-2}, \end{cases}$$

により数列 $\{c_n\}_{n\geq 0}, \{e_n\}_{n\geq 0}, \{f_n\}_{n\geq 0}$ を定める．$\{f_n\}_{n\geq 0}$ は Fibonacci 数列である. Proposition 5.1 [I-ii], [II-iii], [III-ii] は Tomita and Yamamuro [26, Theorems 2, 3] で証明されている．証明の概略については Section 8 で触れる．自然数 $N_{\ell,\delta}$ はすべて極小型ではなく ([13, Example 3.5] を参照), 比較的大きい.

Proposition 5.1. ℓ を任意の自然数とする．$\delta = 1, 2, 3$ に対して, 下のように自然数 $N = N_{\ell,\delta}$ を定める.

[I] 次のように自然数 $N = N_{\ell,1}$ を定めると $N \equiv 1 \mod 4$ をみたし, $(1+\sqrt{N})/2$ の周期 ℓ の連分数展開を得ることができる.

(i) $3 \mid \ell$ のとき, $N := (f_\ell + 1)^2 + 4(f_{\ell-1} + 1)$ とおくと,

$$(1+\sqrt{N})/2 = [(f_\ell + 2)/2, \overline{1, 1, \ldots, 1, f_\ell + 1}\,].$$

(ii) $3 \nmid \ell$ のとき, $N := (2f_\ell + 1)^2 + 4(2f_{\ell-1} + 1)$ とおくと,

$$(1+\sqrt{N})/2 = [f_\ell + 1, \overline{1, 1, \ldots, 1, 2f_\ell + 1}\,].$$

[II] 次のように自然数 $N = N_{\ell,2}$ を定めると $N \equiv 2 \mod 4$ をみたし, $\sqrt{N}$ の周期 ℓ の連分数展開を得ることができる.

(i) $\ell \equiv 0 \mod 4$ または $\ell \equiv 3, 7, 9 \mod 12$ のとき, $N := (2e_\ell + 1)^2 + 4e_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [2e_\ell + 1, \overline{2, 2, \ldots, 2, 4e_\ell + 2}\,].$$

(ii) $\ell \equiv 2 \mod 4$ のとき, $N := ((e_\ell + 2)/2)^2 + e_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [(e_\ell + 2)/2, \overline{2, 2, \ldots, 2, e_\ell + 2}\,].$$

(iii) $\ell \equiv 1 \mod 12$ のとき, $N := ((f_\ell + 1)/2)^2 + f_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [(f_\ell + 1)/2, \overline{1, 1, \ldots, 1, f_\ell + 1}\,].$$

(iv) $\ell \equiv 5, 11 \mod 12$ のとき, $N := ((3f_\ell + 1)/2)^2 + 3f_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [(3f_\ell + 1)/2, \overline{1, 1, \ldots, 1, 3f_\ell + 1}\,].$$

[III] $\ell \geq 2$ を偶数とする. 次のように自然数 $N = N_{\ell,3}$ を定めると $N \equiv 3 \mod 4$ をみたし, $\sqrt{N}$ の周期 ℓ の連分数展開を得ることができる.

(i) $\ell \equiv 0 \mod 4$ のとき, $N := ((e_\ell + 2)/2)^2 + e_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [(e_\ell + 2)/2, \overline{2, 2, \ldots, 2, e_\ell + 2}\,].$$

(ii) $\ell \equiv 2, 10 \mod 12$ のとき, $N := ((f_\ell + 1)/2)^2 + f_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [(f_\ell + 1)/2, \overline{1, 1, \ldots, 1, f_\ell + 1}\,].$$

(iii) $\ell \equiv 6 \mod 12$ のとき, $N := (c_\ell + 2)^2 + 2c_{\ell-1} + 1$ とおくと,

$$\sqrt{N} = [c_\ell + 2, \overline{4, 4, \ldots, 4, 2c_\ell + 4}\,].$$

5.1 予想と Question

いまから

$$X := \{d : \text{平方でない自然数} \mid 4 \nmid d \text{ かつ } 2 \le d \le 3 \times 10^8\}$$

とおき, 始めに集合 $\mathrm{CF}_\ell \cap X$ を考える. X は 224991340 個の元をもつ. $\alpha_X := \max\{\ell(d) \mid d \in X\}$ とすると, $\alpha_X = 52702$, $\min \mathrm{CF}_{\alpha_X} = 299553094$. また, 連続する周期 $\ell(d)$, $d \in X$ の最大値を β_X とすると, $\beta_X = 38298$, $\min \mathrm{CF}_{\beta_X} = 209637334$. これは任意の ℓ, $1 \le \ell \le \beta_X$ に対して $\mathrm{CF}_\ell \cap X \ne \emptyset$, しかし, $\mathrm{CF}_{\beta_X+1} \cap X = \emptyset$ となることを意味する. そこで, $1 \le \ell \le \beta_X$ のとき, d_ℓ を $\mathrm{CF}_\ell \cap X$ の最小元とする: $d_\ell = \min(\mathrm{CF}_\ell \cap X)$. 表 1.1 により, $d_1 = 2$, $d_2 = 3$, $d_3 = 17$, $d_4 = 7, \ldots$. 始めに, $1 \le \ell \le \beta_X = 38298$ とする. このとき, $\ell \ne 7, 11, 49, 225, 299$ ならばいつも $h_{d_\ell} = 1$ が成り立つ. ($\ell = 7, 11, 49, 225, 299$ のとき, それぞれ $d_\ell = 58, 265, 2746, 40954, 64234$ となり, そのときいつも $h_{d_\ell} = 2$ が成り立っている.) 次に, $\beta_X < \ell \le \alpha_X = 52702$ とする. このとき, もし $\mathrm{CF}_\ell \cap X \ne \emptyset$ ならば $h_{d_\ell} = 1$ が成り立っている. さらに, $1 \le \ell \le \alpha_X$ の範囲で $\ell = 1032$ のときのみ, d_ℓ は平方因子をもつ ([18, 表 3] を参照). また, $d \in \mathrm{CF}_\ell$ が $d_\ell = \min \mathrm{CF}_\ell$ に近いとき, 類数 h_d は比較的小さいことが観察できる ([18, 表 2, 3] を参照). ゆえに, 我々は次の予想を立てる:

Conjecture 1. ℓ を任意の自然数とし, d_ℓ を CF_ℓ の最小元とする: $d_\ell = \min \mathrm{CF}_\ell$. このとき, $\ell \ne 7, 11, 49, 225, 299, 1032$ ならば, d_ℓ は平方因子をもたず, かつ $h_{d_\ell} = 1$ が成り立つ.

Remark 5.1. $d > 1$ を平方因子をもたない自然数とする. 種の理論により, もし類数 h_d が奇数ならば d の形は, $d = q$, $2q$, q_1q_2, p, または 2 となることが知られている. ここで, q, q_i は 4 を法として 3 に合同な素数, p は 4 を法として 1 に合同な素数である. さらに始めの 3 つの周期 $\ell(d)$ は偶数, 後ろの 2 つの周期は奇数である.

ℓ を $\ell \ne 1, 7, 11, 49, 225, 299, 1032$ をみたす自然数とし, Conjecture 1 が正しいと仮定する (注意: $d_1 = 2$). このとき, ℓ が偶数のとき, $d_\ell \equiv 1$ (resp., $\equiv 2, 3$) mod 4 ならば d_ℓ の形は, $d_\ell = q_1q_2$ (resp., $= 2q$, $= q$) となる. ℓ が奇数のときは, d_ℓ は $d_\ell \equiv 1 \mod 4$ をみたす素数である.

次に集合 $\mathrm{CF}_{\ell,\delta} \cap X$ を考える.

$$\alpha_{X,\delta} := \max\{\ell(d) \mid d \in X \text{ かつ } d \equiv \delta \mod 4\}$$

とし, $\beta_{X,\delta}$ で連続する周期 $\ell(d)$, $d \in X$, $d \equiv \delta \mod 4$ の最大値を表わす. 始めに, $\delta = 1$ とする. そのとき, $\alpha_{X,1} = 49588$, $\min \mathrm{CF}_{\alpha_{X,1},1} = 298258321$. また, $\beta_{X,1} = 37785$, $\min \mathrm{CF}_{\beta_{X,1},1} = 227147449$. $1 \le \ell \le \beta_{X,1}$ のとき $\mathrm{CF}_{\ell,1} \cap X \ne \emptyset$ だから, $d_{\ell,1}$ を $\mathrm{CF}_{\ell,1} \cap X$ の最小元とする: $d_{\ell,1} = \min(\mathrm{CF}_{\ell,1} \cap X)$. そのとき, $d_\ell \le d_{\ell,1}$. 表 1.1 により, $d_5 = d_{5,1} = 41$; $d_6 = 19$, $d_{6,1} = 57$. 始めに, $1 \le \ell \le \beta_{X,1} = 37785$ とする. このとき, $\ell \ne 11, 20, 49$ ならばいつも $h_{d_{\ell,1}} = 1$ が成り立つ. ($\ell = 11, 20, 49$ のとき, それぞれ $d_{\ell,1} = 265, 1065, 3649$ となり, そのときいつも $h_{d_{\ell,1}} = 2$ が成り立っている.) 次に, $\beta_{X,1} < \ell \le \alpha_{X,1} = 49588$ とする. このとき, もし $\mathrm{CF}_{\ell,1} \cap X \ne \emptyset$ ならば $h_{d_{\ell,1}} = 1$ が成り立っている. さらに, $1 \le \ell \le \alpha_{X,1}$ の範囲で, $d_{\ell,1}$ が平方因子をもつような 42 個の周期 ℓ が存在し, それらはすべて偶数である. そのような 42 個の周期の最小値は, $\ell = 8$ ($d_{\ell,1} = 153 = 3^2 \cdot 17$) になる. 最大値については下の表 5.2 を見よ. よって次の予想を立てる:

Conjecture 2. ℓ を任意の自然数とし, $d_{\ell,1}$ を $\mathrm{CF}_{\ell,1}$ の最小元とする: $d_{\ell,1} = \min \mathrm{CF}_{\ell,1}$ ($\ge d_\ell$). このとき, $\ell \ne 11, 20, 49$ ならばいつも $h_{d_{\ell,1}} = 1$. さらに ℓ が奇数ならば $d_{\ell,1}$ は平方因子をもたない.

Remark 5.2. ℓ を $\ell \neq 1, 7, 11, 49, 225, 299$ をみたす奇数と仮定する．もし Conjecture 1 と 2 が正しければ, 種の理論により $d_{\ell,1} = d_\ell$, また, $d_{\ell,1}$ は $d_{\ell,1} \equiv 1 \mod 4$ をみたす素数になる.

Conjecture 2 で例外となった周期 49 において, 小さい順に d の値を 10 個, 下の表 5.1 に並べる．そこでは d の素因数分解が与えられている．また, d が $\omega(d)$ に関して極小型自然数であるとき `mtype` $:= 1$ とおき, そうでないときは `mtype`$:= 0$ とおく (Section 3 の始めを参照). 表 5.1 から, 3 番目の $d = 4337$ は $h_d = 1$ をみたすことがわかる.

表 5.1: 例外周期 49 における d の 10 個の値

d	d mod 4	Factorization of d	h_d	`mtype`
3649	1	$41 \cdot 89$	2	1
3961	1	$17 \cdot 233$	2	1
4337	1	4337	1	1
4789	1	4789	1	1
5581	1	5581	1	1
6421	1	6421	1	1
6473	1	6473	1	1
6569	1	6569	1	1
7433	1	7433	1	1
8081	1	8081	1	1

上で述べた 42 個の周期 ℓ を小さい順に並べたときの最後の 10 個を表 5.2 におく.

表 5.2: 平方因子をもつ $d_{\ell,1}$ の値

ℓ	$d_{\ell,1}$	$d_{\ell,1}$ mod 4	Factorization of $d_{\ell,1}$	$h_{d_{\ell,1}}$	`mtype`
16680	56453881	1	$11^2 \cdot 466561$	1	1
17060	68190409	1	$7^2 \cdot 1391641$	1	1
17492	63012481	1	$7^2 \cdot 1285969$	1	1
19524	73114129	1	$11^2 \cdot 604249$	1	1
20304	81837889	1	$7^2 \cdot 1670161$	1	1
26376	136299361	1	$11^2 \cdot 1126441$	1	1
26508	158520769	1	$11^3 \cdot 119099$	1	1
26780	135195841	1	$11^2 \cdot 1117321$	1	1
28424	168055969	1	$19^2 \cdot 465529$	1	1
38752	263471329	1	$11^2 \cdot 2177449$	1	1

次に, $\delta = 2$ とする．そのとき, $\alpha_{X,2} = 52702$, $\min \mathrm{CF}_{\alpha_{X,2},2} = 299553094$. また, $\beta_{X,2} = 19236$, $\min \mathrm{CF}_{\beta_{X,2},2} = 67105054$. $1 \leq \ell \leq \beta_{X,2}$ のとき $\mathrm{CF}_{\ell,2} \cap X \neq \emptyset$ だから, $d_{\ell,2}$ を $\mathrm{CF}_{\ell,2} \cap X$ の最小元とする: $d_{\ell,2} = \min(\mathrm{CF}_{\ell,2} \cap X)$. 始めに, $1 \leq \ell \leq \beta_{X,2} = 19236$ とする．このとき, ℓ

が偶数で $\ell \neq 18, 20, 30, 42, 62, 90, 92, 120, 204$ ならばいつも $h_{d_{\ell,2}} = 1$ が成り立つ. ($\ell = 18$, 20, 30, 42, 62, 90, 92, 120, 204 のとき, それぞれ $d_{\ell,2} = 562, 606, 946, 1786, 3886, 6526, 7294$, 13066, 30286 となり, そのときいつも $h_{d_{\ell,2}} = 2$ が成り立っている.) 一方, ℓ が奇数で $\ell \neq 1, 3$, 15, 117 ならば, いつも $h_{d_{\ell,2}} = 2$ が成り立つ. ($d_{1,2} = 2$ かつ $h_{d_{1,2}} = 1$. $\ell = 3, 15, 117$ のとき, それぞれ $d_{\ell,2} = 130, 1066, 57586$ となり, そのときいつも $h_{d_{\ell,2}} = 4$ が成り立っている.) さらに, $d_{\ell,2}$ はいつも平方因子をもたない. 次に, $\beta_{X,2} < \ell \leq \alpha_{X,2} = 52702$ かつ $\mathrm{CF}_{\ell,2} \cap X \neq \emptyset$ とする. このとき, ℓ が偶数ならば $h_{d_{\ell,2}} = 1$ が成り立つ. 一方, ℓ が奇数ならば $h_{d_{\ell,2}} = 2$ が成り立っている. さらに, $d_{\ell,2}$ はいつも平方因子をもたない. よって次の疑問をもつ:

Question 1. ℓ を任意の自然数とし, $d_{\ell,2}$ を $\mathrm{CF}_{\ell,2}$ の最小元とする: $d_{\ell,2} = \min \mathrm{CF}_{\ell,2}\ (\geq d_\ell)$.

(i) ℓ は偶数かつ $\ell \neq 18, 20, 30, 42, 62, 90, 92, 120, 204$ とする. このとき, $d_{\ell,2}$ は平方因子をもたず, いつも $h_{d_{\ell,2}} = 1$ が成り立つか?

(ii) ℓ は奇数かつ $\ell \neq 1, 3, 15, 117$ とする. このとき, $d_{\ell,2}$ は平方因子をもたず, いつも $h_{d_{\ell,2}} = 2$ が成り立つか?

Remark 5.3. ℓ を $\ell \neq 18, 20, 30, 42, 62, 90, 92, 120, 204$ をみたす偶数とし, Question 1 (i) の答えは正しいと仮定する. このとき, 種の理論により $d_{\ell,2}$ の形は, $d_{\ell,2} = 2q$ となる.

Question 1 (ii) で例外となった周期 15 において, 小さい順に d の値を 10 個, 下の表 5.3 に並べる. 表 5.3 から, 2 番目の $d = 1466$ は $h_d = 2$ をみたすことがわかる.

表 5.3: 例外周期 15 における d の 10 個の値

d	d mod 4	Factorization of d	h_d	`mtype`
1066	2	$2 \cdot 13 \cdot 41$	4	1
1466	2	$2 \cdot 733$	2	1
2290	2	$2 \cdot 5 \cdot 229$	4	1
2738	2	$2 \cdot 37^2$	2	1
2858	2	$2 \cdot 1429$	2	1
3314	2	$2 \cdot 1657$	4	1
3562	2	$2 \cdot 13 \cdot 137$	4	1
4498	2	$2 \cdot 13 \cdot 173$	4	1
4538	2	$2 \cdot 2269$	2	1
4570	2	$2 \cdot 5 \cdot 457$	4	1

Conjectures 1, 2, Question 1 (i) (resp. Question 1 (ii)) におけるどの例外周期においても, 何番目かの d の値は, $h_d = 1$ (resp. $h_d = 2$) をみたしている.

最後に, $\delta = 3$ とする. そのとき, $\alpha_{X,3} = 52474$, $\min \mathrm{CF}_{\alpha_{X,3},3} = 292011619$. また, $\beta_{X,3} = 41004$, $\min \mathrm{CF}_{\beta_{X,3},3} = 221088319$. ℓ が偶数で $2 \leq \ell \leq \beta_{X,3}$ のとき $\mathrm{CF}_{\ell,3} \cap X \neq \emptyset$ だから, $d_{\ell,3}$ を $\mathrm{CF}_{\ell,3} \cap X$ の最小元とする: $d_{\ell,3} = \min(\mathrm{CF}_{\ell,3} \cap X)$. 始めに, ℓ は偶数で, $2 \leq \ell \leq \beta_{X,3} = 41004$ をみたすとする. このとき, $d_{\ell,3}$ は平方因子をもたず, いつも $h_{d_{\ell,3}} = 1$ が成り立つ. 次に, ℓ は偶数で, $\beta_{X,3} < \ell \leq \alpha_{X,3} = 52474$ をみたすとする. このとき, もし $\mathrm{CF}_{\ell,3} \cap X \neq \emptyset$ ならば, $d_{\ell,3}$ は平方因子をもたず $h_{d_{\ell,3}} = 1$ が成り立っている. よって次の予想を立てる:

Conjecture 3. ℓ を任意の正の偶数とし, $d_{\ell,3}$ を $\mathrm{CF}_{\ell,3}$ の最小元とする: $d_{\ell,3} = \min \mathrm{CF}_{\ell,3}$ ($\geq d_\ell$). このとき, $d_{\ell,3}$ は平方因子をもたず, かつ $h_{d_{\ell,3}} = 1$ が成り立つ.

Remark 5.4. ℓ を任意の正の偶数とし, Conjecture 3 は正しいと仮定する. このとき, 種の理論により $d_{\ell,3}$ は素数である.

さらに連分数展開の周期に基づく類数 1 の自然数の分布を見ると, 各周期において類数 1 の (平方でない) 自然数は最小元近くに集中していることが観察できる ([18, Section 3.2] の図 1, 2 を参照). 以上で述べた d が 3 億の範囲における最大周期 α_X, $\alpha_{X,\delta}$ と連続する最大周期 β_X, $\beta_{X,\delta}$ のリストを挙げる. ここで, $X := \{d :$ 平方でない自然数 $\mid 4 \nmid d$ かつ $2 \leq d \leq 3 \times 10^8\}$, $|X| = 224991340$.

α_X	$\min \mathrm{CF}_{\alpha_X}$	$\alpha_{X,1}$	$\min \mathrm{CF}_{\alpha_{X,1},1}$
52702	299553094	49588	298258321
β_X	$\min \mathrm{CF}_{\beta_X}$	$\beta_{X,1}$	$\min \mathrm{CF}_{\beta_{X,1},1}$
38298	209637334	37785	227147449

$\alpha_{X,2}$	$\min \mathrm{CF}_{\alpha_{X,2},2}$	$\alpha_{X,3}$	$\min \mathrm{CF}_{\alpha_{X,3},3}$
52702	299553094	52474	292011619
$\beta_{X,2}$	$\min \mathrm{CF}_{\beta_{X,2},2}$	$\beta_{X,3}$	$\min \mathrm{CF}_{\beta_{X,3},3}$
19236	67105054	41004	221088319

5.2 予想への取り組み

Conjectures 1, 2, 3 (または Question 1) は, 類数 1 の実 2 次体は無限個存在することを期待させる. 我々の予想を解くために知られている結果をまとめる. $N_{\ell,\delta}$ を Proposition 5.1 で与えた自然数とする. そのとき, 我々は粗い上からの評価

$$\min \mathrm{CF}_\ell \leq \min\{N_{\ell,1},\, N_{\ell,2},\, N_{\ell,3}\}, \qquad \min \mathrm{CF}_{\ell,\delta} \leq N_{\ell,\delta}\ (\delta = 1, 2, 3)$$

をもつ. 類数 1 の実 2 次体をたくさん見つけるには, [13, Proposition 4.4] により, 我々は極小型実 2 次体 (または極小型自然数) を構成しなければならないことを知っている. そして, $\omega(d)$ に関する周期 ℓ の極小型自然数 d はすべて, Friesen and Halter-Koch の定理を使って原理的に計算される (Section 3). この方法により, 上の最小元のより良い上からの評価を得るのは可能であると考える. 一方 Louboutin [20] は実 2 次体の類数が 1 となるための必要十分条件を与えている. その条件は, $\omega(d)$ の連分数展開と (Minkowski 定数以下の) ある素数の有限集合の情報を含む. $\mathbb{Q}(\sqrt{d})$ を実 2 次体とする. ここで $d > 1$ は平方因子をもたない自然数である. Section 2 のように, χ_d を $\mathbb{Q}(\sqrt{d})$ に対応する Kronecker 指標とする ($d = d_1$). $\omega = \omega(d)$ を (2.6) のような 2 次無理数とし, 簡単のために $\omega = (P_0 + \sqrt{d})/Q_0$ と書く. ここで, $d \equiv 1 \mod 4$ のとき $P_0 := 1$, $Q_0 := 2$, $d \equiv 2, 3 \mod 4$ のときは $P_0 := 0$, $Q_0 := 1$ とおく. 各自然数 $n \geq 1$ に対して

$$\omega_0 := \omega, \quad \omega_n = a_n + \frac{1}{\omega_{n+1}}, \quad a_n = [\omega_n]$$

により 2 次無理数 ω_{n+1} が定まり, 自然数 P_n, Q_n があって $\omega_n = (P_n + \sqrt{d})/Q_n$ と書ける. Q_n/Q_0 は自然数になる ([13, Lemma 2.2] を参照).

Theorem 5.2 (Louboutin [20] Theorem 3). 上の設定の下で,

$$\mathcal{S}_d := \{p \mid p \text{ は素数},\ p < \sqrt{D_d}/2,\ \chi_d(p) \neq -1\}$$

とおく. このとき $h_d = 1$ となるための必要十分条件は, 任意の $p \in \mathcal{S}_d$ に対して, $p = Q_n/Q_0$ をみたす番号 n, $1 \leq n \leq [\ell/2]$ が存在することである.

別の条件として, Lu [21], Dubois and Levesque [6, Section 1] の結果もある. これらの事実が, Conjectures 1, 2, 3 を将来解くために, 役に立つことを (筆者たちは) 希望している. Gauss の類数問題への別のアプローチとして, Takhtajan and Vinogradov [25] の仕事がある.

5.3 極小型自然数に関する基本的未解決問題

[18, Section 3.3] で述べた, 現在考えられる基本的な未解決問題を再提示する.

- 任意の自然数 $\ell \geq 4$ に対して, $d \in \mathrm{CF}_\ell$ をみたす $\omega(d)$ に関する極小型自然数 d は無限個存在することを示せ.

- 任意の自然数 $\ell \geq 4$ に対して, $d \in \mathrm{CF}_\ell$ をみたす平方因子をもたなく, かつ $\omega(d)$ に関する極小型自然数 d, すなわち, 極小型実 2 次体 $\mathbb{Q}(\sqrt{d})$ が無限個存在することを示せ.

[解説]. 周期 1 の極小型自然数は ($(1+\sqrt{5})/2$ の連分数展開に関する) $d = 5$ のみで, 周期 2, 3 の極小型自然数は存在しない ([13, Examples 3.4, 3.5]). $\ell \geq 4$ が偶数かつ $8 \nmid \ell$ のとき, $d \in \mathrm{CF}_\ell$ をみたす平方因子をもたなく, かつ $\omega(d)$ に関する極小型自然数 d は無限個あることが示されている ([14]). しかし, その具体的に構成された d の形から, 最小元の上からのかなり粗い評価にしかならないことがわかる. また, このことはその類数が比較的大きいことからも納得できる. 現在, 奇数周期の極小型実 2 次体の無限性に関する情報はない. (周期 5 の極小型自然数が無限個あることはわかりますが, 周期 5 の極小型実 2 次体の無限性はわかっていません. 奇数周期は, 偶数周期に比べて取り扱いが困難であるように思えます.)

一方, 任意の自然数 ℓ と $\delta = 1, 2, 3$ に対して, $d \in \mathrm{CF}_{\ell,\delta}$ をみたす平方因子をもたなく, かつ $\omega(d)$ に関する極小型でない自然数 d は無限個存在することがわかっている (Friesen と Halter-Koch の結果, [13, Section 8.1] を参照). ただし, Section 5 の始めにおいて断ったように, $\delta = 3$ のとき ℓ は偶数であると仮定する.

上の 2 つの問題において, 条件「$d \in \mathrm{CF}_\ell$」を「$d \in \mathrm{CF}_{\ell,\delta}$」に置き換えて, より精密な結果を得ても良い.

各周期の最小元は高々2 つの素数の積になることが予想されるので, 次の問いをするのは意味があるし, また興味深い.

- 任意の自然数 ℓ に対して, $p \in \mathrm{CF}_\ell$ をみたす素数 p が少なくとも 1 つ存在することを示せ.

- 任意の自然数 ℓ に対して, $p \in \mathrm{CF}_\ell$ をみたす素数 p が無限個存在することを示せ.

[解説]. 前者の問題は解けるかもしれない. 後者の素数の無限性の証明は難問になると思われる. 例えば $\ell = 1$ として, 集合 CF_1 を考える. [13, p.875, Lines 10–11↓] で見たように, $A = q_1 = 1$ は奇数だから Case (I) が起こり, $s_0 = 1$, $g(x) = x$, $h(x) = 1$, $f(x) = x^2 + 4$ となる. これと

Friesen and Halter-Koch の定理 ([13, Theorem 3.1] の主張 [B]) により, $d \in \mathrm{CF}_1$ ならば, ある自然数 t が存在して $d = t^2 + 1$ (そのとき, $\sqrt{d} = [t, \overline{2t}]$) となるか, またはある正の奇数 t が存在して $d = t^2 + 4$ と書ける (そのとき, $(1+\sqrt{d})/2 = [(t+1)/2, \overline{t}]$). 自然数 t を動かすとき, 2 次式 $t^2 + 1$ の値に無限個の素数が現れることが期待されている. Hardy-Littlewood によるそのような素数の (正の) 密度予想もあるが, まだ証明はされていない. このように後者の問題における素数の無限性の難しさがわかる.

これらは基本的な問題である. そしていずれの問題においても, (構成方法に依存するけれども) 各周期における最小元のより良い上からの評価が得られる可能性のある点がとても大事になる.

6 Siegel の定理の拡張: Proposition 2.2 の証明

この Section では Proposition 2.2 を証明する. 簡単のために, $\kappa_d := \log(h_d \log E_d)/\log D_d$ とおく. また, 平方でない任意の自然数 d に対して, $r_d := 2h_d \log E_d/\sqrt{D_d}$ とおく. $E_d, E_{d_1} > 1$ はそれぞれ整環 $\mathcal{O}_f$, $\mathcal{O}_1$ の基本単数だから, 群指数 e_f の定義により $E_d = E_{d_1}^{e_f}$, したがって, $\log E_d = e_f \log E_{d_1}$. (2.4) より $h_d = h_{d_1} f a_f / e_f$ だから, よって, $h_d \log E_d = f a_f h_{d_1} \log E_{d_1}$. また (2.3) により, $f = \sqrt{D_d}/\sqrt{D_{d_1}}$. したがって,

$$h_d \log E_d = \frac{\sqrt{D_d} a_f h_{d_1} \log E_{d_1}}{\sqrt{D_{d_1}}}$$

となるから,

$$r_d = a_f r_{d_1}. \tag{6.1}$$

Dirichlet の L-関数 $L(s, \chi_{d_1}) := \sum_{n=1}^{\infty} \chi_{d_1}(n)/n^s$ の $s = 1$ での値はよく知られているように, $r_{d_1} = L(1, \chi_{d_1})$ となる (Narkiewicz [22, Theorem 8.6]). (r_{d_1} は実 2 次体 $\mathbb{Q}(\sqrt{d_1})$ の Dedekind ゼータ関数 $\zeta_{\mathbb{Q}(\sqrt{d_1})}(s)$ の $s = 1$ における留数である.) Proposition 2.2 の証明のためには, 元の Siegel の定理 [24] ([22, Theorem 8.14]) の証明で使われている, r_{d_1} の上からの評価 (Lemma 6.1) と下からの評価 (Proposition 6.2) が必要である.

Lemma 6.1 ([22] Lemma 8.16). $r_{d_1} = L(1, \chi_{d_1}) < 3 \log D_{d_1}$.

Proposition 6.2 ([22] Lemma 8.17). $\varepsilon > 0$ を任意の正の数とする. このとき, ある正の数 $B_1 = B_1(\varepsilon) > 0$ が存在して, 任意の平方因子をもたない自然数 $d_1 > 1$ に対して $r_{d_1} \geq B_1 D_{d_1}^{-\varepsilon}$.

さらに, a_f の上からの評価が必要である. 任意の自然数 n に対して,

$$\phi(n) := \prod_{p|n} \left(1 + \frac{1}{p}\right)$$

とおく. ここで p は n の相異なるすべての素因数を動く. $\chi_{d_1}(p) \in \{-1, 0, 1\}$ だから, $a_f \leq \phi(f)$. したがって, a_f の上からの評価を得るには $\phi(n)$ の上からの評価が必要である:

Proposition 6.3. ある実数 $c > 0$ が存在して, 任意の自然数 $n \geq 3$ に対して $\phi(n) < c \log\log n$.

$\varphi(n)$ を Euler 関数とすると,

$$\frac{n}{\varphi(n)} = \prod_{p|n}\left(1-\frac{1}{p}\right)^{-1} = \prod_{p|n}\left(\sum_{k=0}^{\infty}\frac{1}{p^k}\right) \geq \phi(n)$$

だから, 次の Proposition 6.4 は Proposition 6.3 を導く.

Proposition 6.4 (Apostol [1], Theorem 13.14 (a)). ある実数 $c > 0$ が存在して, 任意の自然数 $n \geq 3$ に対して $\varphi(n) > cn/\log\log n$.

Proof of Proposition 2.2. r_d の定義と (6.1) により,

$$h_d \log E_d = r_d\sqrt{D_d}/2 = a_f r_{d_1}\sqrt{D_d}/2. \tag{6.2}$$

始めに, κ_d の上からの評価を行う. $D_d = D_{d_1}f^2$ だから, $D_d \geq D_{d_1}$. Lemma 6.1 により,

$$r_{d_1} < 3\log D_{d_1} \leq 3\log D_d.$$

(6.2) により,

$$h_d \log E_d < (3a_f/2)\cdot(\log D_d)\sqrt{D_d}.$$

$D_d \geq 3$ に注意する. そのとき,

$$\log(h_d \log E_d) < \log(3a_f/2) + \log\log D_d + \frac{1}{2}\log D_d.$$

ゆえに,

$$\kappa_d < \frac{\log(3a_f/2)}{\log D_d} + \frac{\log\log D_d}{\log D_d} + \frac{1}{2}.$$

$c > 0$ を Proposition 6.3 のような正の数とする. そのとき, $3f \geq 3$ だから, $\phi(3f) < c\log\log(3f)$. また, $D_d = D_{d_1}f^2$ より $D_d > f^2$ だから, $f < \sqrt{D_d}$. したがって, $\phi(n)$ の定義により,

$$a_f \leq \phi(f) \leq \phi(3f) < c\log\log(3f) < c\log\log(3\sqrt{D_d}). \tag{6.3}$$

一方, $c' > 0$ を Proposition 6.4 のような正の数とする. $\chi_{d_1}(p) \in \{-1, 0, 1\}$ と $f \mid D_d$ は

$$a_f \geq \prod_{p|f}\left(1-\frac{1}{p}\right) \geq \prod_{p|D_d}\left(1-\frac{1}{p}\right) = \varphi(D_d)/D_d > \frac{c'}{\log\log D_d} \tag{6.4}$$

を導く. (6.3) と (6.4) により,

$$\frac{\log(3c'/2)}{\log D_d} - \frac{\log\log\log D_d}{\log D_d} < \frac{\log(3a_f/2)}{\log D_d} < \frac{\log\{3c\log\log(3\sqrt{D_d})/2\}}{\log D_d}.$$

よって, $d \to \infty$ のとき, Lemma 2.1 により $D_d \to \infty$ だから,

$$\frac{\log(3a_f/2)}{\log D_d} \longrightarrow 0, \quad \text{また,} \quad \frac{\log\log D_d}{\log D_d} \longrightarrow 0.$$

次に, κ_d の下からの評価を行う. $\varepsilon > 0$ を任意の正の数とする. $B_1 = B_1(\varepsilon) > 0$ を Proposition 6.2 のような正の数とする. そのとき, $r_{d_1} \geq B_1 D_{d_1}^{-\varepsilon}$. $D_d \geq D_{d_1} > 1$ だから, $D_{d_1}^{-\varepsilon} \geq D_d^{-\varepsilon}$. したがって, $r_{d_1} \geq B_1 D_d^{-\varepsilon}$. (6.2) により,

$$h_d \log E_d \geq a_f(B_1/2)D_d^{1/2-\varepsilon}.$$

よって,

$$\log(h_d \log E_d) \geq \log a_f + \log(B_1/2) + (1/2 - \varepsilon) \log D_d.$$

ゆえに,

$$\kappa_d \geq \frac{\log a_f}{\log D_d} + \frac{\log(B_1/2)}{\log D_d} + \frac{1}{2} - \varepsilon.$$

$d \to \infty$ のとき, $\log(3a_f/2)/\log D_d \to 0$ だから,

$$\frac{\log a_f}{\log D_d} \longrightarrow 0, \quad \text{また}, \quad \frac{\log(B_1/2)}{\log D_d} \longrightarrow 0.$$

$\varepsilon > 0$ は任意だから, 以上から, $d \to \infty$ のとき $\kappa_d \to 1/2$ となる. □

7 横井の定理の拡張: Proposition 2.3 の証明

Proposition 2.3 の証明のために, 連分数による整環の基本単数の計算方法を復習する. Δ を $\Delta \equiv 0, 1 \mod 4$ をみたす平方でない自然数とし, $\mathcal{O}$ を判別式 Δ の 2 次整環とする. (x_1, y_1) を Pell 方程式 $X^2 - \Delta Y^2 = \pm 4$ の最小自然数解とし, $\epsilon_\Delta := (x_1 + y_1\sqrt{\Delta})/2 > 1$ とおく. ϵ_Δ は $\mathcal{O}$ の基本単数を与えることが知られている (Buchmann and Vollmer [3, Theorem 8.3.5], Jacobson and Williams [12, pp.81–82] を参照).

Lemma 7.1. *上の設定の下で, $\mathcal{O}^\times = \langle -1, \epsilon_\Delta \rangle$ が成り立つ. つまり, ϵ_Δ は整環 $\mathcal{O}$ の基本単数になる.*

次に, D を平方でない自然数とし, 2 次無理数 $\delta(D)$ を

$$\delta = \delta(D) := \begin{cases} \sqrt{D}/2, & \text{if } D \equiv 0 \mod 4, \\ (1+\sqrt{D})/2, & \text{if } D \equiv 1 \mod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \mod 4 \end{cases}$$

により定義する. 簡単のために, $\delta(D) = (q + \sqrt{D})/s$ と書く. もし (x_1, y_1) が Pell 方程式 $X^2 - DY^2 = \pm 4$ の最小自然数解ならば, それは δ の周期 ℓ の連分数展開 $\delta = [a_0, \overline{a_1, \ldots, a_{\ell-1}, a_\ell}]$ から次の手順で計算されることが知られている. 部分商 $a_0, a_1, \ldots, a_{\ell-1}$ から漸化式 (3.1) により自然数 p_ℓ, q_ℓ を計算する.

Proposition 7.2 (Jacobson and Williams [12], pp.57–59). *$\epsilon_D := (x_1 + y_1\sqrt{D})/2$ とおく. 上の設定の下で, $\epsilon_D = (sp_\ell - qq_\ell + q_\ell\sqrt{D})/s$ が成り立つ. すなわち, $x_1 = 2(sp_\ell - qq_\ell)/s$, $y_1 = 2q_\ell/s$.*

いまから d を平方でない自然数とする. $d = d_1 d_2^2$ を (2.1) のような分解とし, 実 2 次体 $K = \mathbb{Q}(\sqrt{d_1})$ を考える. f_d を (2.2) で定義された d の導手とし, $E_d > 1$ を K における整環 $\mathcal{O}_{f_d}$ の基本単数とする. $\omega = \omega(d)$ を (2.6) のような 2 次無理数とし, 周期 ℓ の連分数展開 $\omega = [a_0, \overline{a_1, \ldots, a_{\ell-1}, a_\ell}]$ を考える. 部分商 $a_0, a_1, \ldots, a_{\ell-1}$ から漸化式 (3.1) により自然数 p_ℓ, q_ℓ を計算する. 整数 P_0, Q_0 を表 7.1 のように決め,

$$G_\ell := Q_0 p_\ell - P_0 q_\ell$$

とおく. $\omega = (1 + \sqrt{d})/2$ のとき, $p_\ell = a_0 q_\ell + r_\ell$ だから, $G_\ell = (2a_0 - 1)p_\ell + 2r_\ell > 0$. このように, G_ℓ はいつも自然数となる.

表 7.1: P_0, Q_0, G_ℓ の定義

d (d_1) mod 4	$\omega(d)$	P_0	Q_0	G_ℓ	T	U	U^2/T
0 (1 mod 4)	$\sqrt{d}/2$	0	2	$2p_\ell$	$2p_\ell$	q_ℓ	$q_\ell^2/(2p_\ell)$
0 (2, 3 mod 4)	$\sqrt{d/4}$	0	1	p_ℓ	$2p_\ell$	$2q_\ell$	$2q_\ell^2/p_\ell$
1	$(1+\sqrt{d})/2$	1	2	$2p_\ell - q_\ell$	G_ℓ	q_ℓ	q_ℓ^2/G_ℓ
2, 3	$\sqrt{d}$	0	1	p_ℓ	$2p_\ell$	$2q_\ell$	$2q_\ell^2/p_\ell$

Proposition 7.3. d の基本単数 E_d と横井不変量 m_d は (2.6) で定義された 2 次無理数 $\omega(d)$ の連分数展開を使って計算される. すなわち,

$$T = 2G_\ell/Q_0, \quad U = 2q_\ell/Q_0, \quad m_d = \left[\frac{U^2}{T}\right] = \left[\frac{2q_\ell^2}{G_\ell Q_0}\right].$$

Proof. Lemma 2.1 により

$$D_d = \begin{cases} d, & \text{if } d \equiv 0, 1 \mod 4, \\ 4d, & \text{if } d \equiv 2, 3 \mod 4 \end{cases}$$

だから, $d \not\equiv 1 \mod 4$ のとき $D_d \equiv 0 \mod 4$, $d \equiv 1 \mod 4$ のとき $D_d \equiv 1 \mod 4$. また $\omega(d)$ は,

$$\omega(d) = \begin{cases} \sqrt{D_d}/2, & \text{if } d \not\equiv 1 \mod 4, \\ (1+\sqrt{D_d})/2, & \text{if } d \equiv 1 \mod 4 \end{cases}$$

と書けるから, $\omega(d) = \delta(D_d)$ となる. (x_1, y_1) を Pell 方程式 $X^2 - D_d Y^2 = \pm 4$ の最小自然数解とする. Lemma 7.1 により $(x_1 + y_1\sqrt{D_d})/2 > 1$ は判別式 D_d の整環 $\mathcal{O}_{f_d}$ の基本単数だから, $E_d = (x_1 + y_1\sqrt{D_d})/2$ となる. Proposition 7.2 により, $d \not\equiv 1 \mod 4$ のとき $x_1 = 2p_\ell$, $y_1 = q_\ell$; $d \equiv 1 \mod 4$ のとき $x_1 = 2p_\ell - q_\ell$, $y_1 = q_\ell$ を得る. したがって,

$$E_d = \begin{cases} (2p_\ell + q_\ell\sqrt{D_d})/2, & \text{if } d \not\equiv 1 \mod 4, \\ (2p_\ell - q_\ell + q_\ell\sqrt{D_d})/2, & \text{if } d \equiv 1 \mod 4. \end{cases} \tag{7.1}$$

T, U の定義により, $m_d = [U^2/T]$. 4 つの場合分けをする.

(i) $4 \mid d$ かつ $d_1 \equiv 1 \mod 4$ の場合. $D_d = d$ だから, (7.1) により, $E_d = (2p_\ell + q_\ell\sqrt{d})/2$. よって, $T = 2p_\ell$, $U = q_\ell$. G_ℓ, Q_0 の定義により, $T = 2G_\ell/Q_0$, $U = 2q_\ell/Q_0$ を得る. ゆえに, $m_d = [2q_\ell^2/(G_\ell Q_0)]$.

(ii) $4 \mid d$ かつ $d_1 \equiv 2, 3 \mod 4$ の場合. $D_d = d$ だから, $E_d = (2p_\ell + 2q_\ell\sqrt{d/4})/2$. よって, $T = 2p_\ell = 2G_\ell/Q_0$, $U = 2q_\ell = 2q_\ell/Q_0$.

(iii) $d \equiv 1 \mod 4$ の場合. $D_d = d$ だから, $E_d = (2p_\ell - q_\ell + q_\ell\sqrt{d})/2$. よって, $T = 2p_\ell - q_\ell = 2G_\ell/Q_0$, $U = q_\ell = 2q_\ell/Q_0$.

(iv) $d \equiv 2, 3 \mod 4$ の場合. $D_d = 4d$ だから, $E_d = (2p_\ell + 2q_\ell\sqrt{d})/2$. よって, $T = 2p_\ell = 2G_\ell/Q_0$, $U = 2q_\ell = 2q_\ell/Q_0$. □

Proposition 7.3 を使って, Proposition 2.3 の証明で必要ないくつかの T の値を計算する:

Example 7.1.

d	2	3	5	6	7	8	10	11	12	13	14	15
T	2	4	1	10	16	2	6	20	4	3	30	8
U	2	2	1	4	6	2	2	6	2	1	8	2

d	17	18	19	20	21	22	23	24	26	27	28
T	8	34	340	4	5	394	48	10	10	52	16
U	2	8	78	1	1	84	10	4	2	10	6

Proof of Proposition 2.3. $\omega=\sqrt{d/4}$ の場合 $p_\ell^2-(d/4)q_\ell^2=(-1)^\ell$, $\omega=(1+\sqrt{d})/2$ の場合 $G_\ell^2-dq_\ell^2=(-1)^\ell Q_0^2$, $\omega=\sqrt{d}$ の場合 $p_\ell^2-dq_\ell^2=(-1)^\ell$ が成り立つことが知られている ([14, Lemma 2.7] を参照). ゆえに,

$$E'_d:=\begin{cases}(T-U\sqrt{d/4})/2, & \text{if } 4\mid d \text{ かつ } d_1\equiv 2,3 \mod 4,\\ (T-U\sqrt{d})/2, & \text{otherwise}\end{cases}$$

とおくと, Proposition 7.3, G_ℓ と Q_0 の定義, (2.5) により, $E_dE'_d=(-1)^\ell$, すなわち,

$$\text{[A]:}\quad T^2-\frac{d}{4}U^2=(-1)^\ell 4, \tag{7.2}$$

$$\text{[B]:}\quad T^2-dU^2=(-1)^\ell 4 \tag{7.3}$$

を得る. 簡単のために $m:=m_d$, $E:=E_d$, $E':=E'_d$ とおく. 始めに主張 [B] を示す.

[B-i] $d\geq 29$ ならば, (7.3) により

$$29\leq d\leq dU^2=T^2-(-1)^\ell 4\leq T^2+4.$$

したがって, $T\geq 5$. また, $13<d<29$ かつ $d\neq 20$ ならば, Example 7.1 より $T\geq 5$ を得る.

[B-ii, iii] $d>13$ と仮定する. $d=20$ のとき, $\sqrt{d/4}=\sqrt{5}=[2,\overline{4}]$ だから, Proposition 7.3 により, $T=2p_1=4$, $U=q_1=1$. よって, $E=(4+\sqrt{20})/2=2+\sqrt{5}$, $m_{20}=[1^2/4]=0$. したがって,

$$m_{20}\cdot 20=0<T<E=4.2\cdots<U\sqrt{20}=4.4\cdots<T+1\leq(m_{20}+1)\cdot 20=20.$$

このように (2.8):

$$md<T<E<U\sqrt{d}<T+1\leq(m+1)d$$

が成り立つ. それで, 以下 $d\neq 20$ と仮定してよい. そのとき, [B-i] により $T\geq 5$. U^2 を T で割ったときの余りを r とすると, $m=[U^2/T]$ だから,

$$U^2=Tm+r,\quad 0\leq r<T.$$

$r=0$ と仮定すると, $U^2=Tm$. これを (7.3) に代入して, $T(T-dm)=(-1)^\ell 4$. よって, $T\mid 4$; それで, $T\leq 4$. これは $T\geq 5$ に矛盾する. ゆえに, $r>0$. したがって,

$$T-md=\frac{1}{T}(T^2-mdT)=\frac{1}{T}\{T^2-d(U^2-r)\}=\frac{1}{T}(dr+(-1)^\ell 4)\quad(\because (7.3))$$

だから, $T-md \geq \frac{1}{T}(d+(-1)^\ell 4) > 0$. よって, $md < T$. これは (2.7):

$$md \leq T-1 < U\sqrt{d} < E < T < (m+1)d$$

と (2.8) の第 1 番目の不等式を導く. また,

$$\begin{aligned}(m+1)d - T &= \frac{1}{T}(dT + dTm - T^2) = \frac{1}{T}\{dT + d(U^2 - r) - T^2\} \\ &= \frac{1}{T}\{d(T-r) + dU^2 - T^2\} = \frac{1}{T}(d(T-r) - (-1)^\ell 4) \quad (\because (7.3))\end{aligned}$$

だから, $T-r \geq 1$ により, $(m+1)d - T \geq \frac{1}{T}(d-(-1)^\ell 4) > 0$. よって, $T < (m+1)d$. これは (2.7) と (2.8) の最後の不等式を与える. 残りの不等式を示すために次の等式を使う:

$$E - U\sqrt{d} = (T - U\sqrt{d})/2 = E', \tag{7.4}$$

$$E - T = (-T + U\sqrt{d})/2 = -E'. \tag{7.5}$$

(I) ℓ が偶数のとき. $EE' = 1$, $E > 0$ だから, $E' > 0$. よって, (7.4) により $U\sqrt{d} < E$. また, (7.5) により $E < T$. このように (2.7) の第 3, 4 番目の不等式が成り立つ. (7.3) により, $T^2 - 4 = dU^2$. $T \geq 5$ だからこの左辺は正で, $\sqrt{T^2-4} = U\sqrt{d}$ を得る.

$$\sqrt{T^2-4}^2 - (T-1)^2 = 2T - 5 \geq 5 > 0$$

だから, $U\sqrt{d} = \sqrt{T^2-4} > T-1$. (2.7) の第 2 番目の不等式が成り立つ.

(II) ℓ が奇数のとき. $EE' = -1$, $E > 0$ だから, $E' < 0$. よって, (7.4) により $E < U\sqrt{d}$. また, (7.5) により $T < E$. このように (2.8) の第 2, 3 番目の不等式が成り立つ. (7.3) により, $T^2 + 4 = dU^2$. したがって, $\sqrt{T^2+4} = U\sqrt{d}$.

$$(T+1)^2 - \sqrt{T^2+4}^2 = 2T - 3 \geq 7 > 0$$

だから, $T+1 > \sqrt{T^2+4} = U\sqrt{d}$. (2.8) の第 4 番目の不等式が成り立つ. このように主張 [B] を得る.

[A] d を $d/4$ で置き換えて, (7.3) の代わりに (7.2) を使って [B] と同じ議論をする. 始めに, $d > 12$ のとき $T \geq 5$ を示す. [B-i] の議論により, $d/4 \geq 29$ のとき $T \geq 5$ がわかる. $3 < d/4 \leq 28$ とする. Proposition 7.3 により, $\omega = \sqrt{d/4}$ の連分数展開を使って T の値を計算できる. いま $d/4$ は平方数でなく, $d/4 = d_1(d_2/2)^2$ で $d_1 \equiv 2, 3 \mod 4$ をみたしているから,

$$d/4 = 6, 7, 8, 10, 11, 12, 14, 15, 18, 19, 22, 23, 24, 26, 27, 28$$

のときに T の値を計算すればよい. $4 \nmid (d/4)$ のとき, $d_2/2$ は奇数だから $d/4 \equiv d_1 \equiv 2, 3 \mod 4$. よって T の値は, Proposition 7.3 (表 7.1) により, Example 7.1 ですでに求められていることがわかる. したがって, $T \geq 5$. $4 \mid (d/4)$ のときは次の表を得る:

$d/4$	8	12	24	28
$T = 2p_\ell$	6	14	10	254
$U = 2q_\ell$	2	4	2	48

よって, $T \geq 5$. このように, $d > 12$ のとき $T \geq 5$ が成り立つ. 次に, (7.2) を使うことにより, d を $d/4$ で置き換えた [B-ii, iii] の議論は主張 [A] を導く. □

8 Proposition 5.1 の証明の概略

主張 [I-ii], [II-iii] において周期が $\ell = 1$ となる. $N = 13$; $(1+\sqrt{13})/2 = [2, \overline{3}]$ ([I-ii]), $N = 2$; $\sqrt{2} = [1, \overline{2}]$ ([II-iii]) だから主張の正当性がわかる. そこで以下, $\ell \geq 2$ と仮定する. 主張 [I] と [II] の証明は [18, Section 4] を参照. 主張 [III] のみを確かめる.

$\ell - 1$ 個の対称な自然数の列 $a, \ldots, a$ を考え, Friesen and Halter-Koch の定理 (Theorem 3.3) を使う. [13, Example 3.5] で見たように, $s_0 = (-1)^\ell r_{\ell-2}$, $g(s_0) = a$ が成り立つ. t を任意の自然数とし,

$$s := s_0 + t = (-1)^\ell r_{\ell-2} + t$$

とおく. そのとき [18, Section 4] で見たように, $g(s) > a$, $f(s) = (q_\ell t + a)^2 + 4(q_{\ell-1} t + 1)$ となる. $0 \leq n \leq \ell$ とする. a が偶数のとき, n が偶数のときに限り q_n は偶数. a が奇数のときは, $n \equiv 0 \mod 3 \Leftrightarrow q_n \equiv 0 \mod 2$ が成り立つことがすぐに確かめられる. そして, $(A, B, C) = (q_\ell, q_{\ell-1}, q_{\ell-2})$; $\ell = 2$ のとき, $s \equiv 1 + t \mod 2$, $\ell > 2$ のときは, $s \equiv q_{\ell-3} + t \mod 2$ がわかる. また, a が偶数のとき $k \geq 0$ に対して, $q_{4k+1} \equiv 1$, $q_{4k+2} \equiv a$, $q_{4k+3} \equiv 1$, $q_{4k} \equiv 0 \mod 4$. a が奇数のときは, $q_{6k+1} \equiv 1$, $q_{6k+2} \equiv a$, $q_{6k+3} \equiv 2$, $q_{6k+4} \equiv a+2$, $q_{6k+5} \equiv 1$, $q_{6k} \equiv 0 \mod 4$ がすぐに確かめられる.

[III-i] $\ell \equiv 0 \mod 4$ と仮定し, $a = 2$ と取る. そのとき, $q_n = e_n$, $(A, B, C) \equiv (0, 1, 0) \mod 2$. よって, Case (II) が起こる. $t = 1$ と取り, $N := f(s)/4 = ((e_\ell + 2)/2)^2 + e_{\ell-1} + 1$ とおくと, Theorem 3.3 (ii) により,

$$\sqrt{N} = [(e_\ell + 2)/2, \overline{2, 2, \ldots, 2, e_\ell + 2}\,]$$

は $\sqrt{N}$ の周期 ℓ の連分数展開になる. $\ell \equiv 0 \mod 4$ により, $e_\ell \equiv 0 \mod 4$ だから $(e_\ell + 2)/2$ は奇数. また, $e_{\ell-1} \equiv 1 \mod 4$. よって, $N \equiv 1 + 1 + 1 = 3 \mod 4$.

[III-ii] $\ell \equiv 2, 10 \mod 12$ と仮定し, $a = 1$ と取る. そのとき, $q_n = f_n$, $3 \nmid \ell$ だから $A \equiv 1 \mod 2$. よって, Case (I) が起こる. $t = 1$ と取る. $\ell = 2$ のとき, $s \equiv 1+1 \equiv 0 \mod 2$. $\ell > 2$ のときは, $3 \nmid \ell$ だから, $s \equiv q_{\ell-3} + 1 \equiv 0 \mod 2$. そこで, $N := f(s)/4 = ((f_\ell + 1)/2)^2 + f_{\ell-1} + 1$ とおくと, Theorem 3.3 (ii) により,

$$\sqrt{N} = [(f_\ell + 1)/2, \overline{1, 1, \ldots, 1, f_\ell + 1}\,]$$

は $\sqrt{N}$ の周期 ℓ の連分数展開になる. $\ell \equiv 2 \mod 12$ ならば $f_\ell \equiv 1 \mod 4$ だから, $(f_\ell + 1)/2$ は奇数. また, $f_{\ell-1} \equiv 1 \mod 4$. よって, $N \equiv 1 + 1 + 1 = 3 \mod 4$. $\ell \equiv 10 \mod 12$ ならば $f_\ell \equiv 1 + 2 = 3 \mod 4$ だから, $(f_\ell + 1)/2$ は偶数. また, $f_{\ell-1} \equiv 2 \mod 4$. よって, $N \equiv 0 + 2 + 1 = 3 \mod 4$.

[III-iii] $\ell \equiv 6 \mod 12$ と仮定し, $a = 4$ と取る. そのとき, $q_n = c_n$, $(A, B, C) \equiv (0, 1, 0) \mod 2$. よって, Case (II) が起こる. $t = 2$ と取り, $N := f(s)/4 = (c_\ell + 2)^2 + 2c_{\ell-1} + 1$ とおくと, Theorem 3.3 (ii) により,

$$\sqrt{N} = [c_\ell + 2, \overline{4, 4, \ldots, 4, 2c_\ell + 4}\,]$$

は $\sqrt{N}$ の周期 ℓ の連分数展開になる. c_ℓ は偶数で $c_{\ell-1}$ は奇数だから, $N \equiv 0 + 2 + 1 = 3 \mod 4$.

参考文献

[1] T. Apostol, Introduction to analytic number theory, Springer-Verlag, New York Heidelberg Berlin, 1976.

[2] Z. I. Borevich and I. R. Shafarevich, Number theory, Academic Press, New York, 1966.

[3] J. Buchmann and U. Vollmer, Binary quadratic forms: An algorithmic approach, Algorithms and Computation in Mathematics Vol. 20, Springer-Verlag, Berlin Heidelberg, 2007.

[4] H. Cohen and H. W. Jr. Lenstra, Heuristic on class group of number fields, in: Number Theory, Noordwijkerhout 1983, 33-62, Lectute Notes in Math., **1068**, Spinger 1984.

[5] D. A. Cox, Primes of the form $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[6] E. Dubois and C. Levesque, On determining certain real quadratic fields with class number one and relating this property to continued fractions and primality properties, Nagoya Math. J. **124** (1991), 157–180.

[7] C. Friesen, On continued fractions of given period, Proc. Amer. Math. Soc. **103** (1988), 9–14.

[8] C. F. Gauss, Disquisitiones Arithmeticae, Göttingen 1801. (The Springer edition in 1986 of English translation by A. A. Clarke.)

[9] F. Halter-Koch, Continued fractions of given symmetric period, Fibonacci Quart. **29** (1991), 298–303.

[10] R. Hashimoto, Ankeny-Artin-Chowla conjecture and continued fraction expansion, J. Number Theory **90** (2001), 143–153.

[11] L. K. Hua, Introduction to number theory, Springer-Verlag, Berlin Heidelberg New York, 1982.

[12] M. J. Jacobson, Jr. and H. C. Williams, Solving the Pell equation, CMS Books in Mathematics, Springer Science+Business Media, LLC, 2009.

[13] F. Kawamoto and K. Tomita, Continued fractions and certain real quadratic fields of minimal type, J. Math. Soc. Japan **60** No.3 (2008), 865–903.

[14] F. Kawamoto and K. Tomita, Continued fractions with even period and an infinite family of real quadratic fields of minimal type, Osaka J. Math. **46** No.4 (2009), 949–993.

[15] F. Kawamoto and K. Tomita, Continued fractions and Gauss' class number problem for real quadratic fields, preprint.

[16] 河本史紀, 与えられた連分数展開をもつ 2 次無理数の Friesen による構成法, 早稲田大学整数論研究集会 2005 報告集, 147–160.

[17] 河本史紀, 冨田耕史, Gauss 予想 (類数 1 問題) は難しい, 早稲田大学整数論研究集会 2008 報告集, 99–114.

[18] 河本史紀, 冨田耕史, 連分数と実 2 次体に関する Gauss の類数問題, 早稲田大学整数論研究集会 2010 報告集, 15pp. 印刷中.

[19] G. Lachaud, On real quadratic fields, Bull. Amer. Math. Soc. (New Series) **17** No.2 (1987), 307–311.

[20] S. Louboutin, Continued fractions and real quadratic fields, J. Number Theory **30** (1988), 167–176.

[21] H. Lu, On the class number of real quadratic fields, Scientia Sinica, Special Issue **2** (1979), 118–130.

[22] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Springer-Verlag Berlin Heidelberg, 3rd ed. 2004.

[23] R. Sasaki, A characterization of certain real quadratic fields, Proc. Japan Acad. **62A** (1986), 97–100.

[24] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, Acta Arith. **1** (1935), 83–86.

[25] L. A. Takhtajan and A. I. Vinogradov, The Gauss-Hasse hypothesis on real quadratic fields with class number one, J. Reine Angew. Math. **335** (1982), 40–86.

[26] K. Tomita and K. Yamamuro, Lower bounds for fundamental units of real quadratic fields, Nagoya Math. J. **166** (2002), 29–37.

[27] H. Yokoi, New invariants and class number problem in real quadratic fields, Nagoya Math. J. **132** (1993), 175–197.