ある2次多項式で与えられる整数がもつ素因子の個数による虚2次体の類数の特徴付け

名古屋大学　大学院　数理情報学専攻
山川実佑子 (Miyuko YAMAKAWA) *

Abstract

虚 2 次体 $\mathbb{Q}(\sqrt{m})$ の類数が 1 であるための条件は, オイラーの素数生成多項式：$f(X) = X^2 + X + q$ $(m = 1 - 4q)$ を用いて言い表すことができることはよく知られている. また, 類数が 2 であるための条件も, 別の素数生成多項式を用いることにより, 定式化できることが知られている. 本講演では, オイラーの素数生成多項式 $f(X)$ に $n = 0, 1, ..., q-2$ を代入したときの各 $f(n)$ の重複を許した素因子の個数に着目し, その最大値 R_q と類数との関係を明らかにする. 主結果は一般リーマン予想の仮定の下で以下のとおりである. 平方因子をもたない負の整数 m に対して,

$$h_K = 3 \iff m = 1 - 4q \text{ は有理素数かつ } R_q = 3$$

1　序論

平方因子をもたない負の有理整数 $m = 1 - 4q$ $(q \geq 1)$ に対して,[1]

(1) 虚 2 次体 $\mathbb{Q}(\sqrt{m})$ の類数は 1 である.

(2) オイラーの素数生成多項式：$f(X) = X^2 + X + q$ $(m = 1 - 4q)$ に連続する $q - 1$ 個の有理整数 $n = 0, 1, \ldots, q-2$ を代入したとき, $f(n)$ は有理素数である.

は同値である. (1)⇒(2) は 1912 年に**フロベニウス (Ferdinand Georg Frobenius)[4]** により証明され, その 1 年後, **ラビノヴィッチ (Von Herrn Georg Rabinowitch)[6]** が (1)⇔(2) を証明した. 一方, 1952 年に, **ベイカー (Aalan Baker)[2], ヘーグナー (Kurt Heegner)[5], スターク (Harold Mead Stark)[9, 10]** により, 平方因子をもたない負の有理整数 m に対して, 虚 2 次体の $\mathbb{Q}(\sqrt{m})$ の類数が 1 であるのは,

$$m = -1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163$$

の 9 個に限ることが証明された. これらのうち, 上記の条件 $m = 1 - 4q$ $(q \geq 1)$ をみたすのは, $m = -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163$ の 7 個である. 残りの $m = -1,\ -2$ は, $m \equiv 2,\ 3 \pmod 4$ をみたす. 1986 年に, **佐々木 (Ryuji Sasaki)[7]** は, $m \equiv 2,\ 3 \pmod 4$ のとき，オイラーの素数生成多項式の代わりに新たに $f(X) = X^2 + q$ $(m = -q)$ を用いることにより，(1)⇔(2) を証明した. さらに, **佐々木**は, 上記で定めた $f(X)$ に $n = 0, 1, \ldots, q-2$ を代入したときの $f(n)$ の重複を許した素因子の個数に着目し, その最大値 R_q（ただし, $R_1 = 1$ と定義する）と $\mathbb{Q}(\sqrt{m})$ の類数と

*yamami1129@icloud.com

[1] $q = 1$ すなわち $m = -3$ のとき, 条件 (2) の n が存在しないので条件 (2) は成立している.

の関係を考察し, 以下の同値性を証明した:

平方因子をもたない負の有理整数 m に対して,

$$f(X) = \begin{cases} X^2 + X + q & (m \equiv 1 \pmod 4,\ m = 1 - 4q) \\ X^2 + q & (m \equiv 2,\ 3 \pmod 4,\ m = -q) \end{cases}$$

とすれば, 虚 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の類数 h_K に対して, 以下はそれぞれ同値である.

(I) $h_K = 1 \iff R_q = 1$

(II) $h_K = 2 \iff R_q = 2$

虚 2 次体の類数が 3 以上の奇数であるためには種の理論より, $m = 1 - 4q$ は有理素数でなければならない. 本論文の主定理は以下の通りである.

主定理. 一般リーマン予想[2]を仮定して, 平方因子をもたない負の整数 m に対して,

$$h_K = 3 \iff m = 1 - 4q \text{ は有理素数かつ } R_q = 3$$

が成り立つ[3].

1.1 群論からの準備

補題 1.1. G を可換群とし, $a_i \in G\ (1 \le i \le n)$ とする. 任意の $k\ (1 \le k \le n)$ に対して, $a_{n_1} \cdots a_{n_k} \neq e$ ならば, G の部分群 $\langle a_1, \ldots, a_n \rangle$ の位数は n よりも大きい. ただし, $1 \le n_1 < \cdots < n_k \le n$ であり, また, e は G の単位元である.

Proof. n 個の元：$a_1,\ a_1a_2, \ldots, a_1a_2 \cdots a_n$ は仮定よりすべて異なる. よって, 部分群の位数は単位元を入れて $n + 1$ 以上である. □

2 2 次体

2.1 2 次体のノルムとトレース

定義 2.1. m を平方数でない有理整数とする. 有理数体 $\mathbb{Q}$ と $\sqrt{m}$ を含む最小の体を $\mathbb{Q}(\sqrt{m})$ で表す. 体 $\mathbb{Q}(\sqrt{m})$ を 2 次体と呼ぶ. 特に, $m > 0$ のとき, 実 2 次体, $m < 0$ のとき, 虚 2 次体と呼ぶ.

定義 2.2. 2 次体 $\mathbb{Q}(\sqrt{m})$ の元 $\alpha = a + b\sqrt{m}\ (a,\ b \in \mathbb{Q})$ に対して, $\alpha' = a - b\sqrt{m}$ とおき, α' を α の **共役**と呼ぶ.

定義 2.3. 2 次体 $\mathbb{Q}\,(\sqrt{m})$ の元 $\alpha = a + b\sqrt{m}\ (a,\ b \in \mathbb{Q})$ に対して, α のノルム $\mathrm{N}(\alpha)$ とトレース $\mathrm{T}(\alpha)$ を, $\mathrm{N}(\alpha) = \alpha\alpha' = a^2 - mb^2,\ \ \mathrm{T}(\alpha) = \alpha + \alpha' = 2a$ により定義する. 定義より, $\mathrm{N}(\alpha),\ \mathrm{T}(\alpha) \in \mathbb{Q}$ である.

---

[2] 一般リーマン予想（GRH）と拡張リーマン予想（ERH）を区別して用いることもあるが, 本論文ではどちらも一般リーマン予想と述べる.

[3] $\Leftarrow$ の証明で一般 Riemann 予想の成立を仮定している.

2.2　2 次体 $\mathbb{Q}(\sqrt{m})$ の整数

定義 2.4. 2 次体 $K=\mathbb{Q}(\sqrt{m})$ に対して, $O_K := \left\{\alpha \in K \;\middle|\; \mathrm{T}(\alpha)\in\mathbb{Z} \text{ かつ } \mathrm{N}(\alpha)\in\mathbb{Z}\right\}$ を K の**整数環**と呼び, O_K の元を K の**整数**と呼ぶ.

定義 2.5. m を平方因子を含まない有理整数とする. このとき, 2 次体 $K=\mathbb{Q}(\sqrt{m})$ の**判別式** d_K を,

$$d_K = \begin{cases} m & (m\equiv 1 \pmod 4) \\ 4m & (m\equiv 2,\ 3 \pmod 4) \end{cases}$$

により定義する. 定義より, $d_K \equiv 0,\ 1 \pmod 4$ である.

命題 2.1. m を平方因子をもたない有理整数とするとき, 2 次体 $K=\mathbb{Q}(\sqrt{m})$ の整数 $\omega\in O_K$ を次で定義する.

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & (m\equiv 1 \pmod 4) \\ \sqrt{m} & (m\equiv 2,\ 3 \pmod 4) \end{cases}$$

このとき, $O_K=\mathbb{Z}[\omega]=\{a+b\omega \mid a,\ b\in\mathbb{Z}\}$ である.

3　素イデアル分解の一意性

定義 3.1 (素イデアル)**.** 可換環 R のイデアル $\mathfrak{p}\neq R$ が以下をみたすとき, $\mathfrak{p}$ を R の素イデアルという.

$$\alpha\beta\in\mathfrak{p}\ (\alpha,\ \beta\in R) \Rightarrow\ \alpha\in\mathfrak{p} \text{ または } \beta\in\mathfrak{p}$$

命題 3.1 (素イデアル分解の一意性)**.** (0) と (1) 以外の O_K の任意のイデアルは素イデアルの積に一意的に分解できる.

3.1　イデアルのノルム

代数体の特筆すべき性質として, 剰余環の有限性を挙げることができる.

命題 3.2. O_K のイデアル $\mathfrak{a}\neq(0)$ に対して, 剰余環 $O_K/\mathfrak{a}$ は有限環である.

定義 3.2. O_K の任意のイデアル $\mathfrak{a}$ に対して, ある有理整数 $n\geq 0$ が存在して, $\mathfrak{a}\mathfrak{a}'=(n)$ となる. この有理整数 n を $\mathfrak{a}$ の**ノルム**と呼び, $\mathrm{N}(\mathfrak{a})$ で表す.

命題 3.3. O_K の (0) でない任意のイデアル $\mathfrak{a}$ に対し, $|O_K/\mathfrak{a}| = \mathrm{N}(\mathfrak{a})$ が成り立つ. 特に, 任意の $\mu\in O_K\backslash\{0\}$ に対して, $N((\mu))=|\mathrm{N}(\mu)|$ である.

3.2　原始的イデアルとその性質

イデアルの定義より, 整数環 O_K の任意のイデアルは加法群として O_K の部分加群である. O_K の元 $\alpha,\ \beta$ に対して, 加法群 O_K において $\alpha,\ \beta$ で生成される部分加群を, $[\alpha,\beta]=\{\alpha x+\beta y \mid x,\ y\in\mathbb{Z}\}$ で表す. 更に, 任意の $c\in\mathbb{Z}$ に対して, $[c\alpha,c\beta]=c[\alpha,\beta]$ と表す.

定義 3.3. O_K のイデアル $\mathfrak{a}\neq(0)$ において, $\mathfrak{a}$ のすべての元を割り切る有理整数が ±1 に限るとき, $\mathfrak{a}$ を**原始的イデアル**と呼ぶ

補題 3.1. O_K の任意のイデアル $\mathfrak{a}\neq(0)$ に対し, $\mathfrak{a}\cap\mathbb{Z}=a\mathbb{Z}$ となる $a\in\mathbb{N}$ が存在する.

命題 3.4. O_K の任意の原始的イデアル $\mathfrak{a} \neq (0)$ に対して, $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ $(a \in \mathbb{N})$ とすると,

$$\mathfrak{a} = [a, b+\omega], \quad a \mid \mathrm{N}(b+\omega)$$

となる有理整数 b が存在する. ここで, a は $\mathfrak{a}$ に対して一意的に定まり, b は a を法として一意的に定まる. 逆に, $a \mid \mathrm{N}(b+\omega)$ をみたす任意の有理整数 a, b に対して, $[a, b+\omega]$ は O_K の原始的イデアルである.

定義 3.4. O_K のイデアル $\mathfrak{a}$ を, 原始的イデアル $\mathfrak{a}_1$ と自然数 c を用いて, $\mathfrak{a} = c\mathfrak{a}_1 = c[a, b+\omega]$ $(a \mid \mathrm{N}(b+\omega))$ と表したとき, $\{ac,\ c(b+\omega)\}$ を $\mathfrak{a}$ の**標準基底**と呼ぶ.

命題 3.5. O_K のイデアル $\mathfrak{a} \neq (0)$ を標準基底で $\mathfrak{a} = c[a, b+\omega]$ と表したとき, $\mathrm{N}(\mathfrak{a}) = |a|c^2$ である.

定義 3.5. 平方因子をもたない負の有理整数 m に対して,

$$f(X) = \begin{cases} X^2 + X + q & (m \equiv 1 \pmod 4,\ m = 1 - 4q) \\ X^2 + q & (m \equiv 2,\ 3 \pmod 4,\ m = -q) \end{cases}$$

と定める.

平方因子をもたない負の有理整数 m が与えられたとき, 特に断りがなければ, 本論文では $f(X)$ および q はそれぞれ上で定義された多項式および自然数を意味するものとする.

補題 3.2. 平方因子をもたない負の有理整数 m に対して, $0 < a \mid f(n)$ のとき, $\mathfrak{a} = [a, n+\omega]$ とすれば, $\mathfrak{a}$ は a を割る O_K の原始的イデアルであり, もし単項ならば,

$$\mathrm{N}(\mathfrak{a}) = a \geq q$$

である.

補題 3.3. 平方因子をもたない負の有理整数 m に対して, $ab \mid f(n)$ $(a, b \in \mathbb{Z})$ ならば, 以下が成り立つ.

$$[a, n+\omega][b, n+\omega] = [ab, n+\omega]$$

補題 3.4. 平方因子をもたない負の有理整数 m に対して, $0 < a \mid f(n)$ のとき, $a = f(b), \quad n \equiv b \pmod a$ をみたす b が存在するとき, かつそのときに限り, $[a, n+\omega] = (b+\omega)$ と表すことができる.

補題 3.5. 平方因子をもたない負の有理整数 m に対して,

$$|k| \leq \begin{cases} 2q-2 & (m \equiv 1 \pmod 4,\ m = 1 - 4q) \\ 2q-3 & (m \equiv 2,\ 3 \pmod 4,\ m = -q) \end{cases}$$

のとき, $f(n) \equiv 0 \pmod k$ をみたす n は存在すれば, $0 \leq n \leq q-2$ の範囲からとることができる.

4 イデアル類群

4.1 指標

定義 4.1. 判別式 $d = d_K$ と有理素数 p に対して, χ_d を

$$\chi_d(p) = \begin{cases} \left(\frac{d}{p}\right) & (p \nmid 2d \text{ のとき}) \\ \left(\frac{2}{|d|}\right) & (p = 2 \text{ かつ } 2 \nmid d \text{ のとき}) \\ 0 & (p \mid d \text{ のとき}) \end{cases}$$

により定義し, これを乗法的に拡張する. χ_d を K に附随する指標という.

命題 4.1. 2 次体 $K=\mathbb{Q}(\sqrt{m})$ の判別式を d とすれば, 有理素数 p で生成される O_K のイデアル (p) の素イデアル分解は次で与えられる.

(1) $\chi_d(p)=1$ のとき, $(p)=\mathfrak{p}\mathfrak{p}'$ と分解する. ここで, $\mathfrak{p}$, $\mathfrak{p}'$ は素イデアルであり, $\mathfrak{p}\neq\mathfrak{p}'$ をみたす. このとき, p は K で**「完全分解する」**という.

(2) $\chi_d(p)=-1$ のとき, (p) は素イデアルである. このとき, p は K で**「惰性する」**という.

(3) $\chi_d(p)=0$ のとき, $(p)=\mathfrak{p}^2$ と分解する. ここで, $\mathfrak{p}$ は素イデアルであり, $\mathfrak{p}=\mathfrak{p}'$ をみたす. このとき, p は K で**「完全分岐する」**という.

4.2 イデアル類群

定義 4.2. O_K のイデアル $\mathfrak{a}\neq(0)$ および $\alpha\in K^\times$ に対して, $\alpha\mathfrak{a}:=\{\alpha\gamma\mid\gamma\in\mathfrak{a}\}$ を K の分数イデアルと呼び, K の分数イデアル全体を $\mathcal{I}_K$ で表す. $\mathcal{I}_K$ は乗法群であり, 分数イデアル群という. 特に, 分数イデアル $(\alpha):=\alpha O_K$ を単項分数イデアルと呼び, 単項分数イデアル全体を $\mathcal{P}_K$ で表す. $\mathcal{P}_K$ は $\mathcal{I}_K$ の部分群である.

定義 4.3 (ミンコフスキー定数)**.** 2 次体 K の判別式を d として,

$$M_K=\begin{cases}\frac{\sqrt{d}}{2} & (d>0\text{ のとき})\\ \sqrt{\frac{|d|}{3}} & (d<0\text{ のとき})\end{cases}$$

と定義する.

今後, この論文を通して, 分数イデアル $\mathfrak{i}$ の $\mathcal{I}_K/\mathcal{P}_K$ における類を $[\mathfrak{i}]$ で表す.

命題 4.2. 剰余群 $\mathcal{I}_K/\mathcal{P}_K$ の各類の中に, ノルムが M_K 以下の原始的な整イデアルが存在する.

定義 4.4. 剰余群 $\mathcal{I}_K/\mathcal{P}_K$ を K のイデアル類群と呼び, $\mathcal{C}_K$ で表す. また, その位数 $|\mathcal{C}_K|$ を K の**類数**と呼び, h_K で表す.

定義 4.5. 有理素数の有限集合 S_K を,

$$S_K:=\{p\mid p\text{ は, }p\leq M_K\text{かつ}\chi_d(p)\neq-1\text{ をみたす正の有理素数 }\}$$

で定義する.

命題 4.3. イデアル類群 $\mathcal{C}_K$ は, S_K に属する有理素数を割る素イデアルの類により生成される. 特に, $S_K=\emptyset$ ならば, $h_K=1$ である.

4.3 その他の重要な補題

補題 4.1. 平方因子をもたない負の有理整数 m に対して, $K=\mathbb{Q}(\sqrt{m})$ の素イデアル $\mathfrak{p}$ が惰性しないとき, $\mathfrak{p}=[p,n+\omega]$ となる有理素数 p と有理整数 n が存在し, 次が成り立つ.

$$\mathfrak{p}\text{ は完全分岐する }\iff f'(n)\equiv0\pmod p$$

補題 4.2. 平方因子をもたない負の有理整数 m に対して, $S_K\neq\emptyset$ ならば, 任意の $p\in S_K$ に対して, $f(n)\equiv0\pmod p$ をみたす有理整数 $0\leq n\leq q-2$ が存在する. 特に, p が完全分解すれば, $f(n)\equiv0\pmod{p^2}$ をみたす有理整数 $0\leq n\leq q-2$ が存在する. さらに, $|S_K|\geq2$ のとき, p_1, $p_2\in S_K$ $(p_1\neq p_2)$ に対して, $f(n)\equiv0\pmod{p_1p_2}$ をみたす有理整数 $0\leq n\leq q-2$ が存在する.

5　類数 1 の虚 2 次体の特徴付け

類数が 1 の虚 2 次体は, 以下の定理により完全に決定されている.

定理 5.1 (**ベイカー・ヘーグナー・スタークの定理**)**.** 平方因子をもたない負の有理整数 m に対して, 虚 2 次体 $\mathbb{Q}(\sqrt{m})$ の類数が 1 であるのは, $m=-1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163$ の 9 個に限る.

定義 5.1. 自然数 $q\geq 2$ に対して, $f(n)=\sum_{i=1}^{r}p_i^{e_i}\ (0\leq n\leq q-2)$ を素因数分解とするとき,

$$R_1=1,\quad R_q=\max_{0\leq n\leq q-2}\left\{\sum_{i=1}^{r}e_i\right\}$$

と定める.

命題 5.1. m が平方因子をもたないとき, $h_K\geq R_q$ が成立する.

Proof. $R_1=1$ であるから, $q\geq 2$ の場合を示せばよい. このとき, $0\leq n\leq q-2$ に対して, $f(n)$ の重複を許した素因子の個数を R としたとき, $R\geq 2$ ならば, $h_K\geq R$ を示せばよい. $f(n)=p_1\cdots p_R$ とすれば, $R-1$ 個の原始的素イデアル $[p_i,n+\omega]\ (1\leq i\leq R-1)$ から任意に $r\ (\leq R-1)$ 個を選んだとき, その積は単項でない. 実際, $f(n)=kl$ と任意の非自明な分解を考えれば, $[kl,n+\omega]=[k,n+\omega][l,n+\omega]$ は単項であるから, $[k,n+\omega]$ と $[l,n+\omega]$ は共に単項であるか, または共に単項でない. 共に単項とすれば, ノルムはそれぞれ q 以上であるから, $q^2\leq f(n)<f(q-1)\leq q^2$ となり, 矛盾する. よって, 補題 1.1 の条件が成立し, イデアル類 $[[p_i,n+\omega]]\ (1\leq i\leq R)$ が生成する部分群の位数は R 以上である. すなわち, $h_K\geq R$ が成立する. □

5.1　$m\equiv 1\pmod 4$ の場合

定理 5.2 (**フロベニウス・ラビノヴィッチ**)**.** 自然数 $q\geq 1$ に対し, $f(X)=X^2+X+q$ および $m=1-4q$ とするとき, 次の 2 つの条件は同値である.

(1) m は平方因子をもたず, 虚 2 次体 $K=\mathbb{Q}(\sqrt{m})$ の類数は 1 である.

(2) 連続する $q-1$ 個の有理整数 $n=0,1,\ldots,q-2$ に対して, $f(n)$ は有理素数である.

Proof. $q=1$ のとき, (1) および (2) はともに成立しているから, $q\geq 2$ の場合を示せばよい. 命題 5.1 より, (1) $\Rightarrow$ (2) は明らかである. (2) $\Rightarrow$ (1) の証明: $q=2$ のとき, $f(X)=X^2+X+2$ で, $n=0$ より, $f(0)=2$ は有理素数である. また, $m=1-8=-7$ で, 定理 5.1 より, 類数は 1 であるから, (1) が成り立つ. 以下, $q>2$ とする. (2) の仮定の下で, m が平方因子をもつとする. $-m=l^2m_1\ (l>1,\ m_1\geq 1)$ おくと, m は奇数なので l^2 も奇数となり, l が 3 以上の奇数であることが分かり, さらに, $m\equiv 1\pmod 4$ であるから, $m_1\equiv 3\pmod 4$ でなければならない. よって, m_1 も 3 以上の奇数である. ここで, $n=\frac{lm_1-1}{2}$ とすると, $0\leq n\leq q-2$ である. 実際, $4q-1=-m=l^2m_1$ であるから,

$$n\leq q-2\iff\frac{lm_1-1}{2}\leq\frac{l^2m_1+1}{4}-2\iff 0\leq m_1(l-1)^2-m_1-5$$

であり, $m_1,\ l\geq 3$ より, 上記の不等式は成立する. このとき,

$$f(n)=n^2+n+q=\left(\frac{lm_1-1}{2}\right)^2+\frac{lm_1-1}{2}+\frac{1+l^2m_1}{4}=\frac{l^2m_1(m_1+1)}{4}$$

となり, これは合成数である[4] ($\because l$ は奇数). よって, m は平方因子をもたない. 続いて, (2) を仮定したとき, 虚二次体 $\mathbb{Q}(\sqrt{m})$ の類数が 1 であることを示す. 任意の $p \in S_K$ に対して, 補題 4.2 より, $f(n) \equiv 0 \pmod{p}$ となる $0 \leq n \leq q-2$ が存在する. ここで, $R_q = 1$ より, $f(n) = p$ である. よって, イデアル類群の生成元 $[p, n+\omega]$ は補題 3.4 より, 単項イデアルである. 従って, $h_K = 1$ である.

□

5.2 $m \equiv 2, 3 \pmod 4$ の場合

定理 5.3 (**佐々木**)**.** 自然数 $q \neq 3$ に対して, $f(X) = X^2 + q$ および $m = -q$ とするとき, 次の 2 つの条件は同値である.

(1) $m \equiv 2,\ 3 \pmod 4$ であり, m は平方因子をもたず, 虚 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の類数は 1 である.

(2) $R_q = 1$ である.

6 類数 2 の虚 2 次体の特徴付け

6.1 $m \equiv 1 \pmod 4$ の場合

定理 6.1 (**佐々木**)**.** 自然数 q に対して, $f(X) = X^2 + X + q$ および $m = 1 - 4q$ とするとき, 次の 2 つの条件は同値である.

(1) m は平方因子をもたず, 虚 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の類数は 2 である.

(2) $R_q = 2$ である.

注意 6.1. m が平方因子をもたない負の有理整数のとき, 虚 2 次体 $K = Q(\sqrt{m})$ に対して, $h_K = 2$ となる m は 18 個存在する. その m を法 4 で分類すると,

(1) $m \equiv 1 \pmod 4$ は, $-15,\ -35,\ -51,\ -91,\ -115,\ -123,\ -187,\ -235,\ -267,\ -403,\ -427$

(2) $m \equiv 2 \pmod 4$ は, $-6,\ -10,\ -22,\ -58$

(3) $m \equiv 3 \pmod 4$ は, $-5,\ -13,\ -37$

であり, これらすべての K に対して, $|S_K| = 1$ であることを確かめることができる. 逆に $|S_K| = 1$ のとき, その 1 つの元を p とし, もし p が K で完全分岐すれば, $h_K = 2$ である. これら 18 個の中でこの条件をみたす K は 13 個あり, 残りの 5 個の m と対応する p の組は,

$$(-15, 2),\ (-35, 3),\ (-91, 5),\ (-187, 7),\ (-403, 11)$$

である. この 5 個の K に対して, $h_K = 2$ となる理由の 1 つが $R_q = 2$ であるということができる.

定理 6.1 の証明. $h_K = 1 \iff R_q = 1$ および命題 5.1 より, (1) $\Rightarrow$ (2) は明らかである. (2) $\Rightarrow$ (1) の証明: m が平方因子をもたないことは, 定理 5.2 の証明がそのまま適用できる. 続いて, 類数が 2 であることを示す.

(i) イデアル類群 $\mathcal{C}_K$ が巡回群であること: そのためには, $|S_K| \geq 2$ の場合に示せば十分である. $S_K \ni p_i$ $(i = 1, 2,\ p_1 \neq p_2)$ に対して, 補題 4.2 より, $f(n) \equiv 0 \pmod{p_1 p_2}$ をみたす有理整数 $0 \leq n \leq q-2$ が存在する. 仮定:$R_q = 2$ より, $p_1 p_2 = f(n)$ である. よって, 原始イデアル $[p_1 p_2, n+\omega] = (n+\omega)$ は単項であるから, $\mathcal{C}_K$ は 1 つのイデアル類で生成される. すなわち, $\mathcal{C}_K$ は巡回群である.

[4]実際には, 3 個以上の素因子をもつ. 従って, この証明は, 定理 6.1 の証明でも適用できる.

(ii) $\mathfrak{p}^2$ $(\mathfrak{p} \mid p \in S_K)$ が単項であること: p が K で完全分岐すれば, $\mathfrak{p}^2 = (p)$ である. 一方, p が K で完全分岐しなければ, p は K で完全分解するから, 補題 4.2 より, $f(n) \equiv 0 \pmod{p^2}$ をみたす有理整数 $0 \leq n \leq q-2$ が存在する. 再び仮定:$R_q = 2$ より, $p^2 = f(n)$ である. よって, $\mathfrak{p} = [p, n+\omega]$ とすれば, $\mathfrak{p}^2 = [p^2, n+\omega] = (n+\omega)$ は単項である.

従って, $h_K = 2$ であるから, 定理 6.1 の (1) と (2) は同値である. □

6.2 $m \equiv 2,\ 3 \pmod 4$ の場合

定理 6.2 (**佐々木**)**.** 自然数 q $(\neq 3)$ に対して, $f(X) = X^2 + q$ および $m = -q$ とするとき, 次の 2 つの条件は同値である

(1) $m \equiv 2,\ 3 \pmod 4$ であり, m は平方因子をもたず, 虚 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の類数は 2 である.

(2) $R_q = 2$ である.

7 類数 3 の虚 2 次体の特徴付け

本論文では, 一般リーマン予想の仮定の下で類数 3 の虚 2 次体を特徴付けることに成功した.

定理 7.1 (**山川**)**.** 一般リーマン予想を仮定して, 平方因子をもたない負の整数 m に対して, 次の 2 つの条件は同値である

(1) 虚 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の類数は 3 である.

(2) $m = 1 - 4q$ は有理素数かつ $R_q = 3$ である.

Proof. $h_K = 1 \iff R_q = 1$, $h_K = 2 \iff R_q = 2$ および命題 5.1 より, (1) $\Rightarrow$ (2) は明らかである. (2) $\Rightarrow$(1) の証明:**西来路 (Fumio Sairaiji) と清水 (Kenichi Shimizu)**[8] は, 一般リーマン予想を仮定した**バッハ (Eric Bach)**[3] の結果:

$$\min S_K \leq 6 \log^2 |d_K|$$

を用いて,

$$R_q \geq \frac{\log\log 163}{\log 163} \frac{\log |d_K|}{\log\log |d_K|}$$

を示した. よって, $R_q = 3$ のとき, $q \leq 4.169\cdots \times 10^{13}$ でなければならない. したがって, この範囲で $4q-1$ が有理素数のとき, $R_q = 3$ ならば $h_K = 3$ であることを確かめればよい. 実際, PariGP による計算では成立している. □

8 一般リーマン予想下での検証

前節の考察では, $q \leq 4.169\cdots \times 10^{13}$ の範囲の q を検証する必要があるが, q の範囲を狭めることができる. 具体的には, もし, $\min S_K = p$ ならば, p 未満の有理素数 p' に対して, $\chi_{d_K}(p') = -1$ であるから, $q \leq 4.169\cdots \times 10^{13}$ の範囲の q で $2 \leq \min S_K \leq 19$ をみたす場合を予め検証しておき, その後は, 公差 $\prod_{2 \leq p \leq 19} p$ の等差数列上の q のみを検証する. ただし, 初項の選び方は, $\varphi(2) \prod_{3 \leq p \leq 19} \frac{\varphi(p)}{2}$ 通りあるので, この数だけの等差数列を扱うことになる. この方法により, 検証すべき q を約 1000 分の 1 にすることができる.

補題 8.1 (**一般リーマン予想下**)**.** $m = 1 - 4q$ が有理素数のとき，$h_K \geq 4$ ならば[5]，$R_q \geq 4$ である．

Proof. $d_K = m$ が有理素数であるから，完全分岐する有理素数は m のみである．しかし，$|m| = 4q - 1 > M_K$ より，$|m| \notin S_K$ であるから，S_K に属する有理素数はすべて K で完全分解する．よって，$p \in S_K$ に対して，

$$p \in S_K \iff \chi_{d_K}(p) = 1 \iff \begin{cases} \left(\frac{2}{d_K}\right) = 1 \iff d_K \equiv 1 \bmod 2^3 & (p = 2) \\ \left(\frac{d_K}{p}\right) = 1 & (p \neq 2) \end{cases}$$

であるから，

$$f(n) \equiv 0 \bmod p^3 \iff \begin{cases} 4f(n) \equiv 0 \bmod 2^5 \iff (2n+1)^2 \equiv d_K \bmod 2^5 & (p = 2) \\ 4f(n) \equiv 0 \bmod p^3 \iff (2n+1)^2 \equiv d_K \bmod p^3 & (p \neq 2) \end{cases}$$

をみたす整数 n が存在する．以下，$\min S_K = p$ とすれば，$h_K \geq 4$ であるから，$q \geq 12$ であることに注意して，p^3 と $q < 2q - 2$ の大小比較により 3 通りの場合分けをして

(i) $p^3 < q$ のとき，$0 \leq n \leq q - 2$ とすることができ，$f(n) \geq f(0) = q > p^3$ であるから，$f(n)$ は重複を許して 4 個以上の素因子をもつ．すなわち，$R_q \geq 4$ である．

(ii) $q \leq p^3 \leq 2(q-1)$ のとき，補題 3.5 より，$0 \leq n \leq q - 2$ とすることができる．ここで，もし，$f(n) \neq p^3$ ならば，$f(n)$ は重複を許して 4 個以上の素因子をもつ．すなわち，$R_q \geq 4$ である．また，もし，$f(n) = p^3$ ならば，重複を許して 4 個以上の素因子をもつ $f(n')$ $(0 \leq n' \leq q - 2)$ を探す必要がある．

(iii) $2(q-1) < p^3$ のとき，重複を許して 4 個以上の素因子をもつ $f(n')$ $(0 \leq n' \leq q - 2)$ を探す必要がある．

である．以上より，

(1) $2 \leq p \leq 19$ のとき, $1 - 4q$ が素数で $h_K \geq 4$ ならば, $R_q \geq 4$ であることを, $q \leq p^3$ の範囲の q に対して検証する．

(2) $p \geq 23$ のとき，

$$\chi_{d_K}(2) = \chi_{d_K}(3) = \chi_{d_K}(5) = \chi_{d_K}(7) = \chi_{d_K}(11) = \chi_{d_K}(13) = \chi_{d_K}(17) = \chi_{d_K}(19) = -1$$

であるから，q は法 $\displaystyle\prod_{2 \leq p \leq 19} p = 9699690$ で $\varphi(2) \displaystyle\prod_{3 \leq p \leq 19} \frac{\varphi(p)}{2} = 12960$ 通り定まる．ここで，一般 Riemann 予想を仮定すれば，

$$R_q \geq \frac{\log\log 163}{\log 163} \frac{\log |d_K|}{\log\log |d_K|}$$

であるから，$R_q = 3$ ならば，$q \leq 4.16952\cdots \times 10^{13}$ でなければならない．よって，この範囲の q に対して，$m = 1 - 4q$ が素数で $h_K \geq 4$ ならば，$R_q \geq 4$ であることを確かめればよい．さらに上の考察により，対象の q を $\dfrac{12960}{9699690} = 1.33612\cdots \times 10^{-3}$ 倍に減らすことができる．この検証の中で見つかった (i) をみたさない素数 p は以下の $23 \leq p \leq 43$ である．

□

[5] $m = 1 - 4q$ が有理素数ならば，h_K は奇数であるから，必然的に $h_K \geq 5$ である．

Table 1: $d_K = 1 - 4q$ が素数で $h_K \geq 4$ をみたす q

$p = \min S_K$	(iii) $2(q-1) < p^3$	(ii) $q \leq p^3 \leq 2(q-1)$	(i) $p^3 < q$
$p = 2$	—	—	$12 \sim$
$p = 3$	—	—	$33 \sim$
$p = 5$	—	—	$143 \sim$
$p = 7$	131	197, 281	$371 \sim$
$p = 11$	431	671, 797, 977, 1061, 1091	$1637 \sim$
$p = 13$	521, 767, 1007	1151, 1361, 1691, 1931, 2141	$2351 \sim$
$p = 17$	437, 587, 1511, 1607	2657, 3587	$5177 \sim$
$p = 19$	1277, 1481	3671, 4241, 6551	$6971 \sim$
$p = 23$	2201, 2267, 3317, 5501	9131	$14741 \sim$
$p = 29$	2747, 3527, 3917	22271	$27737 \sim$
$p = 31$	8081, 8621	—	$40121 \sim$
$p = 37$	9281, 22697	—	$93881 \sim$
$p = 41$	—	63377	$247757 \sim$
$p = 43$	—	55661	$619517 \sim$
$p \geq 47$	—	—	$\forall q$

重複を許して 4 個以上の素因子をもつ $f(n)$ $(0 \leq n \leq q-2)$ を探す必要のある q を赤字で記した.

References

[1] 青木昇, 素数と 2 次体の整数論, 共立出版 *(2012)*.

[2] A. Baker, Linear forms in the logarithms of algebraic numbers, *Mathematika 13 (1966), 204–216*.

[3] E. Bach, Explicit bounds for primality testing and related problems, *Math. Computation, vol. 55, number 191 (1990), 355–380*.

[4] F. G. Frobenius, Über quadratische Formen die viele Primzahlen darstellen, *Sitz. Akad. Wissen., Berlin (1912), 966–980*.

[5] K. Heegner, Diophantische analysis und modulfunktionen, *Mathematische Zeitschrift, 56 (1952), 227–253*.

[6] V. H. G. Rabinowitsch, Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern, *J. Reine Angew. Math., vol. 142 (1913), 153–164*.

[7] R. Sakaki, On a Lower Bound for the Class Number of an Imaginary Quadratic Field, *Proc. Japan Acad., vol. 62, Ser. A (1986), 37–39*.

[8] F. Sairaiji and K. Shimizu, On a Lower Bound for the Class Number of an Imaginary Quadratic Field, *Proc. Japan Acad., vol. 78, Ser. A (2002), 105–108*.

[9] H. M. Stark, A complete determination of the complex quadratic fields of class number one. *Mich. Math. J., vol. 14 (1967), 1–27*.

[10] ———, On the "Gap" in a Theorem of Heegner, *J. Number Theory 1 (1969), 16–27*.