名古屋大学　大学院情報学研究科　数理情報学専攻
出口 絢結 (Ayu DEGUCHI) *

概要

虚 2 次体 K の類数 h_K と素数生成多項式の値の素因子の個数 Ω_K との関係は古くからよく知られている（$h_K = 1 \iff \Omega_K = 1$）. この事実は，類数が 2, 3 の場合にも同様の定式化がなされている. 本稿では, 類数が 4 の場合の定式化を試みる．種の理論により，類数が 4 ならば，判別式 d_K のもつ異なる素因子の個数は 2 個または 3 個である．主結果は一般リーマン予想の仮定の下で，d_K が異なる素因子を 3 個もつとき，

$$h_K = 4 \iff \Omega_K = 3$$

である．また，$\Omega_K = 4$ の場合の類数の 3, 5, 7, 8 に関する整除性の予想も述べる．

1　導入

虚 2 次体 K の判別式 d_K を

$$d_K = \begin{cases} 1 - 4q & d_K \equiv 1 \pmod 4 \\ -4q & d_K \not\equiv 1 \pmod 4 \end{cases}$$

と表すことにより, 自然数 q を定め, 素数生成多項式 $f(X)$ を

$$f_K(X) = \begin{cases} X^2 + X + q & d_K \equiv 1 \pmod 4 \\ X^2 + q & d_K \not\equiv 1 \pmod 4 \end{cases}$$

と定める[*1]. Ω_K を

$$\Omega_K = \begin{cases} 1 & (q = 1) \\ \max\limits_{0 \le n \le q-2} \{\Omega(f_K(n))\} & (q \ge 2) \end{cases}$$

と定義する[*2]. ただし, 整数 $n \neq 0$ の重複を許した素因子の個数を $\Omega(n)$ と表す. また, 異なる素因子の個数を $\omega(n)$ と表す. 虚 2 次体の類数 h_K に対して, 以下の結果が古くから知られている:

定理 1.1 (フロベニウス・ラビノヴィッチ)**.** 平方因子をもたない負の有理整数 m に対して,

$$h_K = 1 \iff \Omega_K = 1.$$

は同値である.

* ayu.deguchi@nagoya-u.jp

[*1] 虚 2 次体 K に対して, 特に断りがなければ q および $f_K(X)$ は, 上で定義された自然数および多項式を意味するものとする. また, 体 K が明確であるときは添え字 K を省略する.

[*2] $q = 1$ となる虚 2 次体 K は $\mathbb{Q}(\sqrt{-1})$ または $\mathbb{Q}(\sqrt{-3})$ のみである.

また, 類数 2, 3 の場合も同様の同値性が証明されている:

定理 1.2 (佐々木)**.** 平方因子をもたない負の有理整数 m に対して, $h_K = 2 \iff \Omega_K = 2$.

定理 1.3 (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有理整数 m に対して,

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

西来路と清水 [SS02] は, 一般リーマン予想下でバッハ [Bac90] が証明した：

$$K \text{ で惰性しない最小の有理素数は } 6\log^2 |d_K| \text{ 以下である.}$$

という結果を用いて

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

を示した. これは, $\Omega_K = 3$ ならば $q \leq 4.169\cdots \times 10^{13}$ であることを意味する. したがって, この範囲の q に対して, $4q-1$ が有理素数のとき, $\Omega_K = 3$ ならば $h_K = 3$ であることを確かめることができれば, 定理 1.3 の $\Leftarrow$ ができたことになる. しかし, 実際にはこの検証に膨大な計算量を必要とする. 山川 [山 24] はこの範囲のすべての q を検証する必要はなく特定の q のみを検証すれば良いことを示し計算量を大幅に減らすことに成功し, PARI/GP を用いて検証に成功した. 講演者は山川の技法を拡張し, 一般リーマン予想下での $\Omega_K = 3$ となる虚 2 次体の決定, および類数 4 の一部の場合の定式化に成功したので報告する.

定理 1.4 (主定理)**.** 一般リーマン予想を仮定して, 平方因子をもたない負の有理整数 m に対して, 虚 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の判別式 d_K が 3 つの異なる素因子をもつとき,

$$h_K = 4 \iff \Omega_K = 3.$$

は同値である.

2 準備

定義 2.1. $\mathfrak{a}$ を整数環 $\mathfrak{o}_K$ のイデアルとする. $|\mathfrak{o}_K/\mathfrak{a}|$ をイデアル $\mathfrak{a}$ のノルムといい, $\mathrm{N}\mathfrak{a}$ と表す. また, $K \ni \alpha$ に対して, α のノルムを $\mathrm{N}\alpha = \alpha \cdot \alpha'$ と定義する.

定義 2.2. *(i)* イデアル $\mathfrak{a},\ \mathfrak{b} \subset \mathfrak{o}_K$ に対し

$$\mathfrak{a} \sim \mathfrak{b} \iff (\alpha)\mathfrak{a} = (\beta)\mathfrak{b} \text{ となる } 0 \text{ でない} \alpha,\ \beta \in \mathfrak{o}_K \text{が存在する}$$

と定義する. この同値類をイデアル類という[*3].

(ii) $\mathfrak{o}_K$ のイデアル類の個数を K の類数といい, h_K で表す. $\mathfrak{o}_K$ のイデアル類全体は位数 h_K の群をなす. この群をイデアル類群といい $\mathfrak{C}_K$ で表す.

[*3] $\mathfrak{a} \sim \mathfrak{o}_K = (1)$ のことを $\mathfrak{a} \sim (1)$ と略記する. $\mathfrak{a} \sim (1) \iff \mathfrak{a}$ は単項イデアル.

定義 2.3 (クロネッカー指標)**.** $p \nmid d_K$ に対してクロネッカー指標 $\chi_K(p)$ を平方剰余記号を用いて

$$\chi_K(p) = \begin{cases} \left(\frac{d_K}{p}\right), & p \neq 2 \\ \left(\frac{2}{d_K}\right), & p = 2 \end{cases}$$

と定める. ただし, $p \mid d_K$ に対しては $\chi_K(p) = 0$ とする.

定理 2.1. $K = \mathbb{Q}(\sqrt{m})$ を虚 2 次体とする. 有理素数は次のように分解する*:*

(1) $\chi_K(p) = 0$ のとき, $(p) = \mathfrak{p}^2$ と分解する. $\mathfrak{p}$ は素イデアルであり, p は K で完全分岐する, という.

(2) $\chi_K(p) = 1$ のとき, $(p) = \mathfrak{p}\mathfrak{p}'$ と分解する. $\mathfrak{p}$, $\mathfrak{p}'$ は素イデアルかつ, $\mathfrak{p} \neq \mathfrak{p}'$ をみたす. このとき, p は K で完全分解する, という.

(3) $\chi_K(p) = -1$ 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.

以下, $\omega = \begin{cases} \frac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4 \\ \sqrt{m}, & m \equiv 2,\ 3 \pmod 4 \end{cases}$ とおく.

命題 2.1. $\mathfrak{a} = [a, b+\omega]$ を原始イデアルとする. $a = a_1 \cdot a_2$ を a の任意の分解とすると, $\mathfrak{a}_i = [a_i, b+\omega]$, $i = 1,\ 2$ も原始イデアルで $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2$ が成り立つ.

p が惰性するならば, p 上の素イデアル $\mathfrak{p}$ は単項であるから, イデアル類群の生成元として必要ない. すなわち, イデアル類群の生成元になり得るのは, 完全分岐, または完全分解する p 上の素イデアルのみである. ここで, $f(n) = \prod_i p_i$ とおき, p_i 上の素イデアルを $[p_i, n+\omega]$ とすれば,

$$\prod_i [p_i, n+\omega] \sim (1)$$

を得る. $f(X)$ がもつ素因子は完全分岐, または完全分解するから, $f(n)$ の素因数分解, およびそれから得られるイデアルの関係式を調べることにより, イデアル類群の構造を決定することができる.

補題 2.1. m に対して, $0 < f(n)$ のとき, $\mathfrak{a} = [a, n+\omega]$ とすれば, $\mathfrak{a}$ は a を割る $\mathfrak{o}_K$ 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.

$f(n) = ab, (0 \leq n \leq q-2)$ を非自明な分解とし, $\mathfrak{a} = [a, n+\omega]$, $\mathfrak{b} = [b, n+\omega]$ がそれぞれ単項であったとする. このとき, 補題 2.1より$\mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b} \geq q^2 > f(q-2)$ となり矛盾である. したがって, $f(n)$ の非自明は因子はどれも単項でない.

3 主定理

類数が 4 であるためには, 種の理論より $\omega(d_K) = 2$ または 3 である. また, 類数が 4 であるとき $\Omega_K = 3$ または $\Omega_K = 4$ である. さらに, $\omega(d_K)$ と Ω_K は以下をみたす:

命題 3.1. 任意の虚 2 次体 K に対して, $\omega(d_K) \leq \Omega_K$ が成立する.

Proof. d_K の偶奇により, 場合分けする:

(i) $d_K = 1 - 4q$ のとき，$\omega(d_K) = 1$ のときは明らかであるから, d_K を合成数と仮定して素数 p を用いて $d_K = -p(2n+1)$ と分解する．このとき, $\omega(d_K) = \omega(2n+1) + 1$ であ．ここで,

$$4f(n) = (2n+1)^2 - d_K = (2n+1)(2n+1+p)$$

であり, $2n+1+p$ は 4 の真の倍数であるから, $\Omega(2n+1+p) \geq 3$ である． よって, $\Omega(f(n)) > \Omega(2n+1)$ である．以上より,

$$\omega(d_K) = \omega(2n+1) + 1 \leq \Omega(2n+1) + 1 \leq \Omega(f(n)) \leq \Omega_K$$

が成立する．

(ii) $d_K = -4q$ のとき,

(a) q が偶数のとき, $\omega(d_K) = \omega(-4q) = \omega(q) = \omega(f(0)) \leq \Omega(f(0)) \leq \Omega_K$ である．

(b) q が奇数のとき, $\omega(d_K) = \omega(-4q) = \omega(q) + 1$ である．

i. q が素数のとき, $\omega(d_K) = 2$ であるから, $2 \leq \Omega_K$ ならば, $\omega(d_K) \leq \Omega_K$ である．一方, $\Omega_K = 1$ ならば, $h_K = 1$ であるが, $\omega(d_K) = 2$ のとき, h_K は偶数であるから, 矛盾である．

ii. q が合成数のとき, $q = pa$, ただし p は素数で $3 \leq a$ と分解する．q は平方因子をもたないから, $p \nmid a$ である．よって, $\omega(q) = \omega(a) + 1$ である．一方, $0 \leq a \leq q-2$ であり, $f(a) = a(a+p)$ である．ここで, p と a は奇数であるから, $a+p$ は偶数かつ合成数であるから, $2 \leq \Omega(a+p)$ である．よって,

$$\omega(d_K) = \omega(a) + 2 \leq \Omega(a) + 2 \leq \Omega(f(a)) \leq \Omega_K$$

である．

□

3.1 $\Omega_K = 3$ となる虚 2 次体について

定理 3.1. $\Omega_K = 3$ となる体は 52 個あり, $\omega(d_K)$ の値により, 次の 3 通りに分類される:

(1) d_K が素数となる体は 16 個あり, その全ての類数は 3 である．逆に類数 3 の虚 2 次体 16 個がすべて現れる．

(2) $\omega_(d_K) = 2$ となる体は 12 個あり, うち 11 個の体の類数は 4 であり, $\mathfrak{C}_K$ が位数 4 の巡回群となる虚 2 次体 11 個がすべて現れる．残り 1 個の体は類数 6 である．

(3) $\omega_(d_K) = 3$ となる体は 24 個あり, その全ての類数は 4 である．逆に $\mathfrak{C}_K$ が $[2,2]$ 型の虚 2 次体 24 個がすべて現れる．

Proof. 山川 [山 24] より $\Omega_K = 3$ であるとき, $q \leq 4.169\cdots \times 10^{13}$ でなければならない．したがって, この範囲に q をもつ虚 2 次体 K の Ω_K を調べる．山川が定理 1.3 の証明で述べた議論と同様に, 検証すべき q を減らすことができる．虚 2 次体 K で完全分解する最小の素数を p_K とおく．$d_K = 1 - 4q$

のとき,

$$\chi_K(p_K)=1 \iff \begin{cases} \left(\frac{2}{d_K}\right)=1 \iff d_K\equiv 1 \pmod{2^3} & (p_K=2) \\ \left(\frac{d_K}{p}\right)=1 & (p_K\neq 2) \end{cases}$$

より,

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

をみたす整数 n が存在する. $d_K=-4q$ のときも同様である. ここで, p_K^3 と q の大小比較により 2 通りの場合分けをする.

(i) $p_K^3<q$ のとき, $0\leq n\leq q-2$ とでき, $f(n)\geq f(0)=q>p_K^3$ 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, $\Omega_K\geq 4$ である.
(ii) $q\leq p_K^3$ のとき, それぞれの体の類数, および Ω_K を計算する.

この場合分けにより, $\Omega_K=3$ をみたす K を決定するためには (ii) の場合のみを考察すればよく, 計算量を大幅に減らすことができる. さらに, 計算量を減らすために $2\leq p_K\leq 31$ をみたす K に対して, 予め類数および Ω_K を求めておき, その後は $p_K\geq 37$ となる場合のみを考察する. このとき, $2\leq p\leq 31$ に対して $\chi_K(p)=0$ または -1 であるから, q は公差 $\prod_{2\leq p\leq 31}p=200560490130$ の等差数列上に分布し, 初項は中国の剰余定理により, $\chi_K(p)=0$ または -1 $(2\leq p\leq 31)$ から決定される. さらに, d_K が異なる素因子を高々 3 個もつという条件を考慮することにより考察すべき q の数を判別式が奇数の場合は $\frac{241363902}{200560490130}=0.00120\cdots$, 偶数の場合は $\frac{387943417}{200560490130}=0.00193\cdots$ に減らすことができる. 計算を行った結果, 判別式 d_K が奇数, かつ異なる 2 個の素因子をもつ場合に, $h_K\geq 5 \implies \Omega_K\geq 4$ が唯一の例外 $q=941$ (類数 $6, \Omega_K=3$) を除いて成立していることがわかる. したがって, 定理 1.1, 1.2, および定理 1.3 より, $2\leq\omega(d_K)\leq 3$ かつ $\Omega_K=3$ となる虚 2 次体は $q=941$ の場合を除いて類数 4 であることがわかった. 一方, 類数 4 の虚 2 次体は 54 個あり,

(2) $\omega(d_K)=2$ となる体は 30 個あり, そのうち 11 個が $\Omega_K=3$, 19 個が $\Omega_K=4$ である.
(3) $\omega(d_K)=3$ となる体は 24 個あり, そのすべてが $\Omega_K=3$ である.

であるから, 定理 3.1 が証明された. □

定理 3.1 より, 次の系（本講演の主定理）を得る.

系 3.1. 一般リーマン予想を仮定して, 平方因子をもたない負の有理整数 m に対して, 虚 2 次体 $K=\mathbb{Q}(\sqrt{m})$ の判別式 d_K が 3 つの異なる素因子をもつとき,

$$h_K=4 \iff \Omega_K=3.$$

は同値である.

定理 3.1 における唯一の例外であった $q=941$, $K=\mathbb{Q}(\sqrt{-3763})$ を除外するために $4\mid h_K$ となるための条件を考察する.

定義 3.1. 自然数 $n \geq 2$ の素因数分解が $n = \prod_{i=1}^{k} p_i^{e_i}$ $(e_1 \leq \cdots \leq e_k)$ であるとき, $(e_1, \ldots, e_k)$ を n の型という. また, $\prod_{p_i | d_K} p_i^{e_i}$ を n の分岐部分といい n_r と表す. $n_r \neq 1$ のとき, n は分岐する, または分岐的, 分岐 $(e_1, \ldots, e_k)$ 型という. また, $\prod_{p_i \nmid d_K} p_i^{e_i}$ を n の不分岐部分といい, n_{ur} と表し, $\Omega(n_{ur})$ を n の不分岐重みという. $n_r = 1$ のとき, n は不分岐する, または不分岐的, 不分岐 $(e_1, \ldots, e_k)$ 型という.

補題 3.1. *(i)* $f(n) = ab^2$ $(0 \leq n \leq q-2)$ となる n が存在すれば, $\mathfrak{C}_K$ は 2 基本 *abel* 群ではない.
(ii) $f(n) = ab^2$ $(a \mid d_K,\ 0 \leq n \leq q-2)$ となる n が存在すれば, $4 \mid h_K$

Proof. (i) $\mathfrak{C}_K$ が 2 基本 abel 群ならば, $f(n) = ab^2$ のとき, $[b, n+\omega]^2$ は単項であるから $[a, n+\omega]$ も単項となるが, これは矛盾である.
(ii) $a \mid d_K$ より $[a, n+\omega]^2$ は単項である. よって $[b, n+\omega]^4$ も単項である. 一方, $[b, n+\omega]^2$ は単項でないから, $[b, n+\omega]$ が代表するイデアル類の位数は 4 である.

□

定理 3.1 と補題 3.1 より, 次の定理を得る.

定理 3.2. 一般リーマン予想を仮定して, 平方因子をもたない負の有理整数 m に対して, $K = \mathbb{Q}(\sqrt{m})$ を虚 2 次体とする. $\Omega_K = 3$ であるとき,

(1) 分岐 $(1, 2)$ 型の $f(n)$ が存在する $\iff$ $\mathfrak{C}_K$ は位数 4 の巡回群.
(2) $(1, 2)$ 型の $f(n)$ が存在しない $\iff$ $\mathfrak{C}_K$ は $[2, 2]$ 型の *abel* 群 $\iff$ $\omega(d_K) = 3$.

ただし, n はすべて $0 \leq n \leq q-2$ の範囲とする.

Proof. $\mathfrak{C}_K$ が $[2, 2]$ 型の abel 群となる体において, $\Omega(f_K(n)) = 3$ を与える任意の n に対して $f(n)$ は $(1, 1, 1)$ 型であり, $(1, 2)$ 型の $f(n)$ は存在しない. □

定理 3.3. 一般リーマン予想を仮定して, 平方因子をもたない負の有理整数 m に対して, $K = \mathbb{Q}(\sqrt{m})$ を虚 2 次体とする. $\Omega_K = 3$ かつ d_K が異なる素因子を 2 個もつ体は 12 個存在し,

$$h_K = \begin{cases} 4 & (\text{分岐 } (1,\ 2) \text{ 型の } f(n) \text{ が存在する}) \\ 6 & (\text{分岐 } (1,\ 2) \text{ 型の } f(n) \text{ が存在しない}) \end{cases}$$

である. すなわち, 類数が 4 であるか否かは分岐 $(1, 2)$ 型の $f(n)$ の有無で特徴付けられる.

Proof. $\mathbb{Q}\left(\sqrt{-3763}\right)$ $(q = 941,\ h_K = 6)$ に現れる $(1, 2)$ 型の $f(n)$ はすべて不分岐的である. □

4 $\Omega_K = 4$ となる虚 2 次体について

$-1000000 \leq m \leq -1$ のとき, $\Omega_K = 4$ をみたす虚 2 次体は 186 個存在し, $3, 5, 7, 8$ の倍数となる類数が存在する. 類数 4 の体を特徴づけるため, この節では $3 \mid h_K,\ 5 \mid h_K,\ 7 \mid h_K,\ 8 \mid h_K$ となるための条件について考察する.

補題 4.1. *(i)* $f(k)=ab,\ (a,b)=1$ のとき,

$$n\equiv k \pmod a, \qquad n\equiv \begin{cases} -k-1 & (\bmod b) \quad (m=1-4q) \\ -k & (\bmod b) \quad (m=-q) \end{cases}$$

により n を定めれば, $[a,n+\omega]\sim[b,n+\omega]$ である. さらに, $ab\mid f(n)$ ならば, $f(n)=abc$ とすれば, $[a,n+\omega]^2[c,n+\omega]\sim(1)$ である[*4].

(ii) 正の素数 $a,\ b,\ c\ (a\neq b,\ a\neq c)$ に対して, $f(k)=ab,\ f(l)=ac,\ f(n)=abcd^3\ (0\leq n\leq q-2)$ をみたす非負整数 $d,\ k,\ l$ および n が存在すれば, $3\mid h_K$ である.

例 4.1. 定理 3.3 において, $K=\mathbb{Q}(\sqrt{-3762})\ (q=941,\ d_K=-3762)$ が $\Omega_K=3$, かつ判別式 d_K が合成数であるとき, 類数 $h_K\ (=6)$ が 4 でない唯一の体であった. この補題を用いれば,

$$f(307)=29\cdot 37\cdot 89, \quad f(11)=29\cdot 37, \quad f(40)=29\cdot 89$$

であるから, 補題 4.1*(iii)* より $3\mid h_K$ である.

注意 4.1.

$$f(n)-f(k)=\begin{cases}(n-k)(n+k+1) & (m=1-4q)\\ (n-k)(n+k) & (m=-q)\end{cases}$$

であるから, $p\mid f(n),\ p\mid f(k)$ ならば, $n\equiv k \pmod p$ または $n\equiv -k-\delta \pmod p$ である. ただし, $m=1-4q$ のとき $\delta=1$ であり, $m=-4q$ のとき $\delta=0$ とする. よって, $f(n)$ と $f(k)$ の素因数分解が定めるイデアル類の等式に現れる素イデアル, およびその共役イデアルの現れ方は, 上の合同式により決定される.

注意 4.1 で述べた概念を, 以下で定義する.

定義 4.1 (共役的素因数分解)**.** $f(n),\ f(k)=\prod p^e$ に対して, $p\mid f(n),\ p\mid f(k)$ のとき,

$$\varepsilon_p=\begin{cases}1 & (n\equiv k \pmod p)\\ -1 & (n\not\equiv k \pmod p)\end{cases}$$

とし, $\prod p^{\varepsilon_p e}$ を $f(k)$ の $f(n)$ に対する共役的素因数分解という. 3 個以上の $f(n_i)$ が与えられたときは, 適当に順番を定めて共役的素因数分解を定義する.

定義 4.2 (推移的・原始推移的)**.** $f(n_1)=a_1a_2,\ f(n_2)=a_2a_3,\dots,f(n_{k-1})=a_{k-1}a_k\ (1<k)$ のとき, a_1 と a_k は推移的であるという. 特に $a_1,\dots,a_k$ がすべて素数のとき, a_1 と a_k は原始推移的である, あるいは原始的に推移するという.

補題 4.2. $p,\ q$ が原始的推移すれば, その上の素イデアル $\mathfrak{p},\ \mathfrak{q}$ は $\mathfrak{p}\sim\mathfrak{q}$ または $\mathfrak{p}\sim\bar{\mathfrak{q}}$ をみたす.

定義 4.3 (巡回的・原始巡回的)**.** $f(n_1)=a_1^{s_1}a_2^{t_2},\ f(n_2)=a_2^{s_2}a_3^{t_3},\dots,f(n_k)=a_k^{s_k}a_1^{t_1}$ のとき, a_1 は（したがって各 a_i は）(s,t) 型巡回的であるという. ただし, $s=\prod_{i=1}^k s_i,\ t=\prod_{i=1}^k t_i$ である. ま

[*4] 対称性より, 法を入れ替えても同じ結果が得られる.

た, k を長さという. 特に, $a_1, \ldots, a_k$ がすべて素数のとき, 共役的素因数分解により各 $s_i,\ t_i$ に符号情報を与え, その積をそれぞれ $\bar{s},\ \bar{t}$ とする. すなわち,

$$\bar{s} = s\prod_{i=2}^{k}\varepsilon_i, \quad \varepsilon_i = \begin{cases} 1 & (n_{i-1} \equiv n_i \pmod{a_i}) \\ -1 & (n_{i-1} \not\equiv n_i \pmod{a_i}) \end{cases}, \quad \bar{t} = t\varepsilon_1, \quad \varepsilon_1 = \begin{cases} 1 & (n_1 \equiv n_k \pmod{a_1}) \\ -1 & (n_1 \not\equiv n_k \pmod{a_1}) \end{cases}$$

とし, a_1 は（したがって各 a_i は）原始 $[\bar{s}, \bar{t}]$ 型巡回的である, あるいは原始的に $[\bar{s}, \bar{t}]$ 型巡回するといい, $|\bar{s} + (-1)^{k-1}\bar{t}|$ を巡回の位数という.

補題 4.3. 素数 p が長さ k, 位数 l で原始的に $[\bar{s}, \bar{t}]$ 型巡回すれば, p 上の素イデアル $\mathfrak{p}$ は $\mathfrak{p}^l \sim (1)$, すなわち $\mathfrak{p}^{\bar{s}+(-1)^{k-1}\bar{t}} \sim (1)$ をみたす.

Proof. $p = p_1,\ p_2, \ldots, p_k$ を素数とし, $f(n_1) = p_1^{s_1}p_2^{t_2},\ f(n_2) = p_2^{s_2}p_3^{t_3}, \ldots, f(n_k) = p_k^{s_k}p_1^{t_1}$ とする. さらに, $s_i,\ t_i$ の符号調整後の値をそれぞれ $\bar{s}_i,\ \bar{t}_i$ とする. このとき, $\bar{s} = \prod_{i=1}^{k}\bar{s}_i,\ \bar{t} = \prod_{i=1}^{k}\bar{t}_i = t\varepsilon_1$ であり,

$$\begin{aligned} \mathfrak{p}^{\bar{s}+(-1)^{k-1}\bar{t}} &= \left(\cdots \left(\left(\mathfrak{p}_1^{\bar{s}_1}\mathfrak{p}_2^{\bar{t}_2}\right)^{\bar{s}_2} \left(\mathfrak{p}_2^{\bar{s}_2}\mathfrak{p}_3^{-\bar{t}_2}\right)^{\bar{s}_3} \left(\mathfrak{p}_3^{\bar{s}_3}\mathfrak{p}_4^{\bar{t}_4}\right)^{\bar{t}_2\bar{t}_3} \right) \cdots \right)^{\bar{s}_k} \left(\mathfrak{p}_k^{\bar{s}_k}\mathfrak{p}_1^{\bar{t}_1}\right)^{(-1)^{k-1}\bar{t}_2\bar{t}_3\cdots\bar{t}_{k-1}} \\ &\sim (1) \end{aligned}$$

が成り立つ. □

例 4.2. $q = 281,\ d_K = 1 - 4q = -1123,\ h_K = 5$ のとき,

$$f(72) = 7^2 \cdot 113,\ f(153) = 113 \cdot 211,\ f(268) = 211 \cdot 7^3$$

を選べば, $\bar{s} = s \cdot (-1)^2 = 2, \quad \bar{t} = t \cdot 1 = 3$ と計算できる. したがって, 7 は長さ 3 で原始的に $[2, 3]$ 型巡回する. このとき, 位数は $|2 + (-1)^2 \cdot 3| = 5$ である. よって, 補題 4.3 より $5 \mid h_K$ を得る.

例 4.3. $-1000000 \leq m \leq -1$ の範囲で $\Omega_K = 4$ をみたす K のうち, $5 \mid h_K$ をみたす K は 24 個あり, すべて位数が 5 の原始的に巡回する素数が存在する. また, $7 \mid h_K$ をみたす K は 11 個あり, すべて位数が 7 の原始的に巡回する素数が存在する.

定義 4.4 (a の原始集約的)**.** a の不分岐部分 a_{ur} のすべての素因子が a_{ur} の 1 つに素因子 p に a_{ur} の素因子のみを辿りながら原始的に推移するとき, a は p に原始集約的であるという. さらに, a_{ur} が素べき（指数 1 の場合も含む）のときも原始集約的であるという.

定義 4.5 (w 位集約的)**.** a の不分岐部分を a_{ur} とする. 不分岐重みがすべて w の倍数である原始集約的 a_i $(1 \leq i \leq l)$, および自然数 b を用いて $a_{ur} = a_{1ur}\cdots a_{lur}b^w$ と表示されるとき, a は w 位集約的, あるいは単に集約的であるという[*5]. また, a_i が素数 p_i に集約し, $\Omega(a_i) = we_i$ のとき, a は $\prod p_i^{e_i}b$ に w 位集約するという[*6].

補題 4.4. w 位集約的 $f(n)$ $(0 \leq n \leq q-2)$ が存在するとき, $f(n)$ が不分岐ならば $w \mid h_K$ であり, $f(n)$ が分岐ならば, $2w \mid h_K$ である.

[*5] 任意の自然数 a は a_{ur} に 1 位集約的である.

[*6] 補題 4.1 の (iii) の $f(n)$ は 3 位集約的である.

Proof. $f(n)=a\cdot(a_1)_{ur}\cdots(a_l)_{ur}b^w$, $(a\mid h_K)$ とおく. ただし, a_i は素数 p_i に原始集約的であり, a_i の不分岐重みを we_i とする. このとき,

$$[a,n+\omega]\left(\prod_{i=1}^{l}[p_i,n+\omega]^{e_i}\right)^w[b,n+\omega]^w\sim(1)$$

が成り立つ. ここで, 素数 $p,\ q$ に対して, $pq\mid f(n)$ ならば, $[pq,n+\omega]$ は単項でない. 原始集約的の定義より, 各 p_i に対し, $f(k_i)=p_iq_i$ となる k_i が存在する. よって, 補題 4.2 より $[p_i,n+\omega]\sim[q_i,n+\omega]$ となるから, 左辺の非自明な因子はどれも単項でない. 以上より, 左辺が代表するイデアル類の位数は, $f(n)$ が不分岐ならば w であり, $f(n)$ が分岐するならば, 両辺を 2 乗して位数 $2w$ を得る. □

定義 4.6 (準同型変位・同型変位)**.** 素数 p と q が原始的に推移し,

$$f(n)=ap^s,\quad f(k)=qb^t,\quad (a\mid d_K,\ 2^{1-\delta_{a1}}\mid st,\ 1<t)$$

と表示される $n,\ k$ が存在するとき, $f(n)$ は原始的に変位するという. 特に, $s=t$ のとき, 原始的に準同型変位するといい, さらに $f(n)$ と $f(k)$ が同型のとき, 原始的に同型変位するという.

補題 4.5. $s=t=2$ の準同型変位が存在すれば, すなわち,

(i) 素数 p に対して $f(n)=ap^2(a\mid d_K),\ f(k)=pc^2$ と表示される $n,\ k$ $(0\le n,\ k\le q-2)$ が存在すれば, $\mathfrak{C}_K$ は位数 8 の元をもつ. すなわち $8\mid h_K$ である.

(ii) 素数 p と q が原始的に推移するとき, $f(n)=ap^2(a\mid d_K),\ f(k)=qb^2$ と表示される $n,\ k$ $(0\le n,\ k\le q-2)$ が存在すれば, $\mathfrak{C}_K$ は位数 8 の元をもつ. すなわち $8\mid h_K$ である.

Proof. (i) $f(n)$ の素因数分解より, $[p,n+\omega]^4\sim(1)$ を得る. 注意 4.1 より, $[q,k+\omega]$ は $[p,n+\omega]$ または $\overline{[p,n+\omega]}$ と一致するから, $[q,k+\omega]$ が代表するイデアル類の位数は 4 である. よって, $f(k)$ の素因数分解より $[c,k+\omega]^8\sim(1)$ を得るから $8\mid h_K$.

(ii) 注意 4.1 より, $[p,n+\omega]$ と $[q,k+\omega]$ が代表するイデアル類の位数は等しい. よって, (i) と同様にして $[b,k+\omega]^8\sim(1)$ を得るから, $8\mid h_K$.

□

例 4.4. $q=647, d_K=1-4q=-13\cdot199, h_K=8$ のとき,

$$f(370)=13\cdot103^2,\quad f(464)=23\cdot97^2,\quad f(41)=103\cdot23\ (\text{単純推移})$$

であるから, $f(n)$ は同型変位しており, 補題 4.5 より $8\mid h_K$ である.

以下に述べる予想は虚 2 次体 $K=\mathbb{Q}(\sqrt{m})$ $(-1000000\le m\le-1)$ に対して成立している:

予想 4.1. 一般リーマン予想を仮定して, 平方因子をもたない負の有理整数 m に対して, $K=\mathbb{Q}(\sqrt{m})$ を虚 2 次体とする. また, n はすべて $0\le n\le q-2$ とする. $\Omega_K=4$ であるとき,

(i)

$$3 \mid h_K \iff \begin{cases} (3) \text{ 型の } f(n) \text{ が存在する，または} \\ \text{分岐 } (1,3) \text{ 型の } f(n) \text{ が存在する，または} \\ \text{同じ素因子をもつ } (1,2) \text{ 型の } f(n) \text{ と } (1,1) \text{ 型の } f(k) \text{ が存在する} \end{cases}$$
$$\iff \text{不分岐重み 3 の原始集約的 } f(n) \text{ が存在する}$$

(ii) $5 \mid h_K \iff$ 位数が 5 の倍数の原始的に巡回する素数が存在する

(iii) $7 \mid h_K \iff$ 位数が 7 の倍数の原始的に巡回する素数が存在する

(iv) d_K が異なる素因子を 2 個もつとき，

$$4 \mid h_K \iff \text{分岐 } (1,2) \text{ 型の } f(n) \text{ が存在する}$$

(v) d_K が異なる素因子を 2 個もつとき，

$$8 \mid h_K \iff \text{原始的に同型変位する分岐 } (1,2) \text{ 型の } f(n) \text{ が存在する}$$

(vi) d_K が異なる素因子を 2 個もつとき，

$$h_K = 4 \iff \begin{cases} \text{不分岐重み 3 の原始集約的 } f(n) \text{ が存在しない} \\ \text{位数が 5 の倍数の原始的に巡回する素数が存在しない} \\ \text{分岐 } (1,2) \text{ 型の } f(n) \text{ が存在し，かつどれも原始的に同型変位しない} \end{cases}$$

参考文献

[Bac90] E. Bach. Explicit bounds for primality testing and related problems. *Math. Computation*, 55(191):355–380, 1990.

[Fro12] F. G. Frobenius. Über quadratische formen die viele primzahlen darstellen. *Sitz. Akad.der Wissen.*, pages 966–980, 1912.

[Rab13] V. H. G. Rabinowitsch. Eindeutigkeit der zerlegung in primzahlfaktoren in quadratischen zahlkörpern. *J. Reine Angew. Math.*, 142:153–164, 1913.

[Sas86] R. Sasaki. On a lower bound for the class number of an imaginary quadratic field. *Prod. Japan Acad.*, 62:37–39, 1986. Ser. A.

[SS02] F. Sairaii and K. Shimizu. An inequality between class numbers and ono's numbers associated to imaginary quadratic fields. *Prod. Japan Acad.*, 78:105–108, 2002. Ser. A.

[Wat04] Mark Watkins. Class numbers of imaginary quadratic fields. *Math. Computation*, 73(246):907–938, 2004.

[小 87] 小野 孝. 数論序説. 裳華房, 1987.

[山 24] 山川 実佑子. 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, 2024.

[青 12] 青木 昇. 素数と 2 次体の整数論. 共立出版, 2012.