数理解析研究所講究録
第1710巻 2010年 101-112

On the divisibility of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{3^{2e}-4q^n})$ and some Diophantine equations

伊東 杏希子 (名古屋大学大学院多元数理科学研究科 D1)

10月15日

本稿ではまず, Generalized Ramanujan-Nagell 方程式の解の個数に関する先行研究をいくつか述べる (1章). 次にこの方程式に関連して, $Dx^2 \pm 1 = ck^n$ (D, k, c は正の整数でかつ $gcd(D, ck) = 1$ を満たすとする) の形の方程式の整数解 (x, n) $(n > 0)$ の個数についての考察結果を述べる (2章 § 2.1). 最後に応用として, Generalized Ramanujan-Nagell 方程式の解の個数の結果から判定できる, ある虚二次体の類数の可除性についての考察結果を述べる (2章 § 2.2).

1 Introduction

1.1 Ramanujan-Nagell 方程式

次の方程式を考える ;

$$\frac{x^m-1}{x-1} = \frac{y^n-1}{y-1} \qquad (x>1, y>1, m>2, n>2 \text{ with } x>y). \tag{1}$$

方程式 (1) の整数解 (x, y, m, n) として $(5, 2, 3, 5)$, $(90, 2, 3, 13)$ が取れる. 実際,

$$31 = \frac{5^3-1}{5-1} = \frac{2^5-1}{2-1}, \qquad 8191 = \frac{90^3-1}{90-1} = \frac{2^{13}-1}{2-1}$$

である. この方程式について次の予想が知られている.

Conjecture 1. 方程式 (1) の整数解は $(x, y, m, n) = (5, 2, 3, 5)$, $(90, 2, 3, 13)$ の二つのみである.

Baker, Davenport, Lewis, Schinzel, Shorey, Tijdeman などにより, x, y, m, n のうちのどれか二つを固定すれば解 (x, y, m, n) は有限個しか存在しないことが示されている. x, y, m, n のうちのどれか一つのみを固定した時にも解

(x,y,m,n) が有限個しか存在しないかどうかについては特定の場合の結果がいくつか知られている ([Le1], [Le3], [Yu1], [He] など) が, 一般の場合には未解決である ([Sh], [Le1] 参照). ここで, $y=2$, $m=3$ の時を考える. (1) に $y=2$, $m=3$ を代入すると

$$x^2+x+1=\frac{x^3-1}{x-1}=\frac{2^n-1}{2-1}=2^n-1 \qquad (x>2,\ n>2)$$

なので

$$\left(x+\frac{1}{2}\right)^2+\frac{7}{4}=x^2+x+2=2^n$$

となる. よって,

$$(2x+1)^2+7=2^{n+2}$$

となるので, $y=2$, $m=3$ での方程式 (1) の解 (x,n) の考察は方程式

$$X^2+7=2^N \qquad (X>5,\ N>4)$$

の整数解 (X,N) の考察に帰着される.

Theorem 1. (Nagell, [Na]). 方程式

$$x^2+7=2^n \qquad (x,\ n>0) \tag{2}$$

の整数解は $(x,n)=(1,3),\ (3,4),\ (5,5),\ (11,7),\ (181,15)$ の 5 個である.

この定理は Ramanujan により予想され, Nagell により証明された. 方程式 (2) を Ramanujan-Nagell 方程式という. Theorem 1 により $y=2$, $m=3$ の時, 方程式 (1) の解は $(x,y,m,n)=(5,2,3,5),(90,2,3,13)$ のみであることが分かる.

1.2 Generalized Ramanujan-Nagell 方程式

D_1, D_2 を互いに素な正整数, $D:=D_1D_2$, $k\geq 2$ を D と互いに素な整数とする. Ramanujan-Nagell 方程式の一般化として次の方程式を考える ;

$$D_1x^2+D_2=\lambda^2k^n \qquad (x,n\in\mathbb{Z},\ x\geq 1, n\geq 1). \tag{3}$$

ただし, $\lambda\in\{1,\sqrt{2},2\}$ とし, k が偶数の時は $\lambda=2$, $\lambda\in\{\sqrt{2},2\}$ の時は D_2 を奇数とする. この方程式を (ここでは) Generalized Ramanujan-Nagell 方程式という.

Remark 1. 方程式 (3) には

$$D_1x^2+D_2=\lambda'^2k^n \qquad (x,n\in\mathbb{Z},\ x\geq 1, n\geq 1), \tag{4}$$

$$\text{ただし,} \qquad \lambda'=\begin{cases} 1 & k:\text{odd} \\ 2 & k:\text{even} \end{cases}$$

の場合が含まれている. 方程式 (4) のことを通常は Generalized Ramanujan-Nagell 方程式とよぶ ([BS] 参照).

1.3 Generalized Ramanujan-Nagell 方程式の解の個数

方程式 (3) の整数解の個数を $\mathcal{N}(\lambda, D_1, D_2, k)$ と書く. この節では Generalized Ramanujan-Nagell 方程式の解の個数に関する先行研究をいくつか紹介する ([BS] 参照). 与えられた (λ, D_1, D_2, k) に対して, 方程式 (3) の整数解は高々有限個しか存在しないことが Mahler により示され, その後 Apéry, Nagell, Beukers, Le Maohua, Bender, Herzberg, Heuberger([HL]) などにより, k が素数の場合について多くの結果が示された.

Theorem 2. (Le Maohua, [Le2], [Le3], Leu and Li, [LL]). $\mathcal{N}(2,1,7,2)=5$, $\mathcal{N}(2,3,5,2)=\mathcal{N}(2,1,11,3)=\mathcal{N}(2,1,19,5)=\mathcal{N}(1,2,1,3)=3$ を除いて, $\mathcal{N}(\lambda, D_1, D_2, p)\leq 2$ となる. ただし, p は素数とする.

Theorem 2 に対して, $\mathcal{N}(\lambda, D_1, D_2, p)>1$ となる (λ, D_1, D_2, p) を具体的に決定したのが Bugeaud-Shorey による次の結果である.

Theorem 3. (Bugeaud and Shorey, [BS]). 集合 $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}_\lambda\subset\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ を以下のように定義する;

$$\mathcal{F}:=\{(F_{k-2\varepsilon}, L_{k+\varepsilon}, F_k)\mid k\geq 2, \varepsilon\in\{\pm 1\}\},$$

$$\mathcal{G}:=\{(1, 4k^r-1, k)\mid k\geq 2, r\geq 1\},$$

$$\mathcal{H}_\lambda:=\left\{ (D_1,D_2,k) \;\middle|\; \begin{array}{c} D_1s^2+D_2=\lambda^2k^r \text{ かつ } 3D_1s^2-D_2=\pm\lambda^2 \\ \text{を満たす正の整数 } r,\ s \text{ が存在する.} \end{array} \right\}.$$

ただし, $\{F_n\}$ は Fibonacci 数列 ($F_0:=0, F_1:=1, F_{n+2}:=F_{n+1}+F_n (n\geq 0)$), $\{L_n\}$ は Lucas 数列 ($L_0:=2, L_1:=1, L_{n+2}:=L_{n+1}+L_n (n\geq 0)$) とする.
k が素数の時 (以降 k の代わりに p と書く), 方程式

$$D_1x^2+D_2=\lambda^2p^n \quad x\geq 1,\ n\geq 1$$

の整数解 (x,n) の個数は以下を除いて高々一つ $(\mathcal{N}(\lambda,D_1,D_2,p)\leq 1)$ である;

$$(\lambda,D_1,D_2,p)\in\mathcal{E}:=\left\{\begin{array}{c}(2,13,3,2),(\sqrt{2},7,11,3),(1,2,1,3),(2,7,1,2),\\(\sqrt{2},1,1,5),(\sqrt{2},1,1,13),(2,1,3,7)\end{array}\right\}$$

または

$$(D_1,D_2,p)\in\mathcal{F}\cup\mathcal{G}\cup\mathcal{H}_\lambda.$$

Theorem 3 は主に, $D_1x^2\pm D_2y^2=\lambda^2k^z\quad(\lambda=1,2)$ の解 (x,y,z) に関する Le Mauhua([Le4]) の結果 (主に二次形式の性質を用いて証明されている) と Lucas 数列, Lehmer 数列の primitive divisor に関する Bilu-Hanrot-Voutier の結果 ([BHV]) とから示されている.

2 主結果

2.1 方程式 $Dx^2\pm 1=ck^n$ について

Generalized Ramanujan-Nagell 方程式 $D_1x^2+D_2=\lambda^2k^n$ の自然な一般化として, λ が $1,\sqrt{2},2$ 以外の正の整数の場合を考えることができる. λ が $1,\sqrt{2},2$ 以外の正の整数の場合の最近の結果として, [Yu2](ただし, この論文で扱われている方程式の形は $D_1x^2+D_2y^2=ck^n$ である), [Yu3], [SS] 以外のものがどのくらいあるのか著者はあまり知らない. この節では Yuan の結果 ([Yu3]) とそれに関連した方程式の整数解の個数についての考察結果を述べる.

Yuan により次が示された.

Theorem 4. (Yuan, [Yu3]). c, k を正の整数とし, D を ck と互いに素な正の整数とする. 方程式

$$Dx^2+1=ck^n\qquad(x,n\in\mathbb{Z},\ x\geq 1,n\geq 1)\tag{5}$$

の整数解 (x,n) の個数を $N(D,c,k)$ と書くとする.
(i) 次の場合を除いて $N(D,1,k)\leq 1$ となる;

$$N(2,1,3)=3,\ N(6,1,7)=N(7,1,2)=2,\ N(D,1,b^2-1)=2.$$

ただし, $b>1$ は整数でかつ $Ds^2=b^2-2$ となる整数 s が存在するものとする.
(ii) $D>1$ の時, $N(2,1,3)=3$ の場合を除いて $N(D,c,k)\leq 2$ となる.

この定理は主に, 数列 $\frac{k^n-1}{k-1}$ の性質と Walker の結果 ([Wa]) とから示されている. この手法に基づいて次を示した.

主結果 1. c, k を正の整数とし, $D > 1$ を ck と互いに素な正の整数とする. 方程式

$$Dx^2 - 1 = ck^n \qquad (x, n \in \mathbb{Z},\ x \geq 1, n \geq 1) \tag{6}$$

の整数解 (x, n) の個数を $N'(D, c, k)$ と書くとする.
(i) $k \neq 3$ の時, $N'(D, c, k) \leq 2$ となる.
$N'(D, c, k) = 2$ ならば, 解 (x_1, n_1), (x_2, n_2) に対し $n_1 \not\equiv n_2 \bmod 2$ が成立.
(ii) $k = 3$ の時, $N'(D, c, k) \leq 3$ となる ($c = k = 3$ の時は $N'(D, 3, 3) \leq 2$).
解 (x, n) のうち n が奇数となるものは高々2個, n が偶数となるものは高々1個である.

Remark 2. Theorem 4, 主結果 1 に関する Remark を挙げる. 方程式 (5), (6) で $D = c = 1$ となる場合についてである. $x^2 - \lambda = k^n$ ($\lambda = \pm 1, n > 1$) の整数解 (x, k, n, λ) は Yuan の結果以前から知られていて (cf. [Ca], [Ch]), 解は $(x, k, n, \lambda) = (3, 2, 3, 1)$ のみである.

2.2 Application – 虚二次体の類数の可除性について –

この節では応用例として, Generalized Ramanujan-Nagell 方程式の結果を用いて虚二次体の類数の可除性が判定できる例を紹介する. 与えられた正の整数 n について, 類数が n で割れる虚二次体は無限に存在する (実二次体についても同様の主張が成り立つ). 類数が n で割れる虚二次体の無限族を具体的に構成することにより証明することができ, 多くの証明が知られているが, その中に Ankeny-Chowla, Mollin による結果 ([AC], [Mo]) などがある.

2.2.1 虚二次体 $\mathbb{Q}(\sqrt{2^{2e} - q^n})$, $\mathbb{Q}(\sqrt{3^{2e} - 4q^n})$ の類数の可除性について

類数が n で割れる虚二次体の無限族を構成した結果として次の Ankeny-Chowla によるものが知られている.

Theorem 5. (Ankeny and Chowla, [AC]). $n > 0$ を偶数, x を $2 \mid x$ かつ $0 < x < (2 \cdot 3^{n-1})^{\frac{1}{2}}$ を満たす整数とする. 平方因子を持たない整数 $d := 3^n - x^2$ について $n \mid h(-d)$ である (だだし, $h(-d)$ は $\mathbb{Q}(\sqrt{-d})$ の類数).

この Ankeny-Chowla の結果の一般化として次の Mollin による結果がある. 平方因子を持たない整数 d について, σ を $-d \equiv 1 \bmod 4$ の時は $\sigma = 2$, $-d \equiv 2, 3 \bmod 4$ の時は $\sigma = 1$ として定義する. Mollin により次が示されている.

Theorem 6. (Mollin, [Mo]). 整数 $n > 1$, $k > 1$, $x > 0$ について, $-d := x^2 - \sigma^2 k^n < 0$ を平方因子を持たない整数とする.
(1) n が偶数かつ $x \neq 2k^{\frac{n}{2}} - 1$ ならば, $n \mid h(-d)$ である.

(2) n が奇数かつ $x \neq \lfloor \sigma k^{\frac{n}{2}} \rfloor$ ならば, $n \mid h(-d)$ である.
$\lfloor \cdot \rfloor$ は floor 関数であり, ガウス記号と同じ定義である.

ここで Theorem 5, 6 について, d の仮定から「平方因子を持たない」の条件をはずすことができるかを考える. $\mathbb{Q}(\sqrt{x^2-k^n})$, $\mathbb{Q}(\sqrt{x^2-4k^n})$ の形の虚二次体の類数の可除性を判定する際に (特に, x^2-k^n, x^2-4k^n に「平方因子を持たない」の条件を仮定しない場合に), Generalized Ramanujan-Nagell 方程式の解の個数に問題が帰着されることが多い. ここでは, [BS] の結果 Theorem 3 を用いたものを紹介する ([Ki], [It1], [It2]). Ankeny-Chowla の結果 Theorem 5 に対して, $k=3$ かつ x が 2 べきの場合には, 岸康弘氏による次の結果が知られている.

Theorem 7. (岸, [Ki]). 与えられた正の数 n について e を $2^{2e} < 3^n$ を満たす正の数とする. $(n,e) \neq (3,2)$ を除いて, 虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-3^n})$ の類数は n で割れる.

これに対して, k が奇素数の場合にも同様の定理が成り立つかを考え, 次を示すことができた.

主結果 2. $q>0$ を奇素数とする. 与えられた正の数 n について e を $2^{2e} < q^n$ を満たす正の数とする.
(1) $q \equiv 1 \bmod 4$ の時, 虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-q^n}) \neq \mathbb{Q}(\sqrt{-1})$ の類数は n で割れる.
(2) $q \equiv 7 \bmod 8$ の時, 虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-q^n}) \neq \mathbb{Q}(\sqrt{-3})$ の類数は n で割れる.
(3) $q \equiv 3 \bmod 8$ の時, (i) $e \equiv 1 \bmod 2$ または (ii) $n \not\equiv 3 \bmod 6$ を満たすならば, 虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-q^n}) \neq \mathbb{Q}(\sqrt{-3})$ の類数は n で割れる.

主結果 2 の (3) について, $n \equiv 3 \bmod 6$ かつ $e \equiv 0 \bmod 2$ の時に虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-q^n})$ の類数が n で割れない例を挙げる.

Example 1. $(q,n,e)=(11,3,4)$ の時,

$$2^{2e}-q^n = 2^8 - 11^3 = -1075 = 5^2 \times (-43)$$

となる. $\mathbb{Q}(\sqrt{-43})$ の類数は 1 なので, $n=3$ では割れない.

また, $q \equiv 11 \bmod 12$ の時は $\mathbb{Q}(\sqrt{2^{2e}-q^n}) \neq \mathbb{Q}(\sqrt{-3})$ となる.

系 1. $q \equiv 11 \bmod 12$ を奇素数とする. 与えられた正の数 n について e を $2^{2e} < q^n$ を満たす正の数とする.

(1) $q \equiv 11 \bmod 24$ の時, (i) $e \equiv 1 \bmod 2$ または (ii) $n \not\equiv 3 \bmod 6$ を満たすならば, 虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-q^n})$ の類数は n で割れる.
(2) $q \equiv 23 \bmod 24$ の時, 虚二次体 $\mathbb{Q}(\sqrt{2^{2e}-q^n})$ の類数は n で割れる.

主結果 2 の証明と同様に, $\mathbb{Q}(\sqrt{3^{2e}-4q^n})$ ($q \neq 3$ は素数, $e \geq 1$ は整数) の形の虚二次体に対しても Theorem 3 を用いて次を示すことができた.

主結果 **3.** $q \neq 3$ を素数とし, 整数 $n > 0$, $e \geq 1$ が $3^{2e} < 4q^n$ を満たすとする. $3^{2e} - 4q^n = m^2 D$ (ただし, $D < 0$ は平方因子を持たない整数, $m > 0$) とする.
(1) $q \neq 3$ が奇素数の時, 次が成り立つ.
  (1.1) $n \equiv 2 \bmod 4$ かつ, $2q^{n/2} - 3^e (e \equiv 0 \bmod 2)$ または $2q^{n/2} + 3^e (e \equiv 1 \bmod 2)$ が平方数ならば, $n/2 \mid h(D)$ である.
  (1.2) (1.1) 以外の時は $n \mid h(D)$ である.
(2) $q = 2$ かつ $(n, e) \neq (6, 2)$ の時, 次が成り立つ.
  (2.1) $n \equiv 2 \bmod 4$, $e \equiv 1 \bmod 2$ かつ $2^{(n/2)+1} - 3^e$ が平方数なら, $n/2 \mid h(D)$ である.
  (2.2) (2.1) 以外の時は $n \mid h(D)$ である.
  (*) $(q, n, e) = (2, 6, 2)$ の時は $\mathbb{Q}(\sqrt{3^{2\cdot 2} - 4 \cdot 2^6}) = \mathbb{Q}(\sqrt{-7})$, $6 \nmid h(-7) = 1$.

ここで, 主結果 3 の (1.1), (2.1) について例を挙げる.

Example 2. (1) $(q, n, e) = (5, 2, 2)$ の時, $2q^{n/2} - 3^e = 2 \cdot 5^{2/2} - 3^2 = 1$ より $2q^{n/2} - 3^e$ は平方数である.

$$m^2 D = 3^{2e} - 4q^n = 3^4 - 4 \cdot 5^2 = 1^2 \times (-19)$$

より, $m = 1$, $D = -19$ となるが, $h(-19) = 1$ なので, $2 \nmid h(-19)$ かつ $2/2 = 1 \mid h(-19)$ である.
(2) $(q, n, e) = (2, 2, 1)$ の時, $2^{(n/2)+1} - 3^e = 2^{(2/2)+1} - 3^1 = 1$ より $2^{(n/2)+1} - 3^e$ は平方数である.

$$m^2 D = 3^{2e} - 2^{n+2} = 3^2 - 2^{2+2} = -7$$

より, $m = 1$, $D = -7$ となるが, $h(-7) = 1$ なので, $2 \nmid h(-7)$ かつ $2/2 = 1 \mid h(-7)$ である.

主結果 3 は Mollin の結果 Theorem 6 に対して, $\sigma = 2$, k が素数 かつ x が 3 べきの場合には上の条件のもとで, 扱う二次体の仮定から「平方因子を持たない」の条件をはずすことができることを意味している. 主結果 3 の系として次が成り立つ.

系 2. $q \neq 3$ を素数とし, 整数 $n > 0$, $e \geq 1$ が $3^{2e} < 4q^n$ を満たすとする.
(1) $q \equiv 1 \bmod 3$ または $n \equiv 0, 1, 3 \bmod 4$ ならば, $n \mid h(D)$ である.
(2) $q \equiv 2 \bmod 3$ かつ $n \equiv 2 \bmod 4$ ならば, $n/2 \mid h(D)$ である.

2.2.2 主結果 3 の証明の概略

この節では主結果 3 の証明の概略を述べる.

イデアル類の位数が n となる $O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$ のイデアルを構成することにより主結果 3 は示される.

$$\alpha := \frac{3^e + \sqrt{3^{2e} - 4q^n}}{2} \in \mathbb{Q}(\sqrt{3^{2e} - 4q^n})$$

とおく. ただし, $q \neq 3$ は素数とし, 整数 $n > 0$, $e \geq 1$ が $3^{2e} < 4q^n$ を満たすとする. $\alpha \in O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$ であり, さらに $N(\alpha) = q^n$ かつ $(q, 3^{2e} - 4q^n) = 1$ かつ $q \nmid \alpha$ なので,

$$(\alpha) = \wp^n$$

と書ける. ただし, N はノルムで $\wp$ は (q) の素因子である (q は $\mathbb{Q}(\sqrt{3^{2e} - 4q^n})/\mathbb{Q}$ で完全分解する). 主結果 3 の (1.1), (2.1) の仮定を満たさない (q, n, e) に対して, $\pm\alpha$ が $O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$ の元の p 乗 (p は n の素因数) で書けないことを示せば, イデアル類 $[\wp]$ の位数が n となることが言える. 具体的には次の補題を示す.

Lemma 1. n, eが以下のうちの一つを満たすならば, 任意のnの素因数pに対して$\pm\alpha$は$O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$の元の$p$乗では書けない.
(1) qが奇素数の時,
  (1.1) $n \not\equiv 2 \bmod 4$.
  (1.2) $n \equiv 2 \bmod 4$ かつ $2q^{n/2} - 3^e$ $(e \equiv 0 \bmod 2)$が平方数でない.
  (1.3) $n \equiv 2 \bmod 4$ かつ $2q^{n/2} + 3^e$ $(e \equiv 1 \bmod 2)$が平方数でない.
(2) $q = 2$ かつ $(n, e) \neq (6, 2)$ の時,
  (2.1) $n \not\equiv 2 \bmod 4$.
  (2.2) $n \equiv 2 \bmod 4$ かつ $2^{(n/2)+1} - 3^e (e \equiv 1 \bmod 2)$が平方数でない.

この補題の証明では,

$$\pm\alpha = \left(\frac{a + b\sqrt{D}}{2}\right)^p$$

となる $a, b \in \mathbb{Z}$ が存在する (ただし, $a \equiv b \equiv 1 \bmod 2$) と仮定して矛盾を導く. $p = 2$, $p \geq 3$ と場合分けして考察するが, $\pm\alpha = \left(\frac{a+b\sqrt{D}}{2}\right)^p$ と書けるとすると $p \geq 3$ の時には $a = \pm 3^i (0 \leq i \leq e)$ となる. そこで, $i = e$, $i = 0$, $0 < i < e$ の三

つの場合に分けて考察し, それぞれの場合ごとに矛盾を導く. 特に, $i = e$ の時, $3^{2e} - 4q^n = m^2 D$ かつ $-b^2 D + 3^{2e} = 4q^{n/p}$ となり, 方程式 $-Dx^2 + 3^{2e} = 4q^y$ の正整数解として $(x, y) = (m, n), (|b|, n/p)$ の少なくとも二つが取れることが分かる. しかし, 与えられた素数 q に対して方程式 $D_1 x^2 + 3^{2e} = 4q^y$ ($D_1 > 0$ は奇数) の正整数解 (x, y) の個数は高々一つである. このことは Theorem 3 から分かる ($(2, D_1, 3^{2e}, q) \notin \mathcal{E}$, $(D_1, 3^{2e}, q) \notin \mathcal{F} \cup \mathcal{G} \cup \mathcal{H}_2$ を示せばよい). よって $i = e$ の時, 矛盾が導ける. イデアル類 $[\wp]$ の位数を s と書くとすると $n = sn'$ ($n' > 0 \in \mathbb{Z}$) と書ける. $\wp^s \sim (1)$ より,

$$(\alpha) = \wp^n = (\wp^s)^{n'} = (\beta)^{n'} = (\beta^{n'})$$

を満たす $O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$ の元 β が存在する. $\mathbb{Q}(\sqrt{3^{2e} - 4q^n}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ より

$$O^{\times}_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})} = \{\pm 1\}$$

なので

$$\pm\alpha = \beta^{n'}$$

が言える. Lemma 1 の仮定の下では $\pm\alpha$ は $O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$ の元の p 乗 ($p \mid n$) で書けないので, このことは $n' = 1$, つまり, $n = s$ を意味する. よって, イデアル類の位数が n となる $O_{\mathbb{Q}(\sqrt{3^{2e}-4q^n})}$ のイデアルとして $\wp$ が取れるので主結果 3 が示せる.

2.2.3 虚二次体 $\mathbb{Q}(\sqrt{1 - 4k^n})$ の類数の可除性について

この節では [Le5] の結果に関する Remark として, $\mathbb{Q}(\sqrt{1 - 4k^n})$ の形の虚二次体の類数の可除性について考察した内容を紹介する. 虚二次体 $\mathbb{Q}(\sqrt{1 - 4k^n})$ の類数の可除性について, Le Maohua により次が示されている.

Theorem 8. (Le Maohua, [Le5]). $k > 1$, $n > 0$ を整数とし, $1 - 4k^n = -m^2 D < 0$ とする (ただし $D > 3$ は平方因子を持たない整数, $m > 0$ とする). $(m, D, k, n) \neq (3, 7, 2, 4)$ ならば次が成り立つ.
(1) n が偶数でかつ, ある正の整数 m_1, m_2 が存在して $m = m_1 m_2$, $m_1^2 - D m_2^2 = 2$ または -2 となるならば, $n/2 \mid h(-D)$ である.
(2) (1) 以外の時は $n \mid h(-D)$ である.

Theorem 8 に対して次を得た.

主結果 4. (I, [It2]). $k > 1$ を奇数とし, $n > 0$ とする.
(1) 与えられた $k \neq 5, 13$ に対して, 虚二次体 $\mathbb{Q}(\sqrt{1 - 4k^n})$ の類数は高々一つを除いて n で割れる. 除外される n は 2 または 4 であり, この場合には $\mathbb{Q}(\sqrt{1 - 4k^n})$ の類数は $n/2$ で割れる.

(2) $k=5$ の時, 虚二次体 $\mathbb{Q}(\sqrt{1-4k^n})$ の類数は $n=2,\ 4$ を除いて n で割れる. $\mathbb{Q}(\sqrt{1-4\cdot 5^2})=\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{1-4\cdot 5^4})=\mathbb{Q}(\sqrt{-51})$ の類数はそれぞれ 1, 2 であり, $n/2$ で割れるが n では割れない.

(3) $k=13$ の時, 虚二次体 $\mathbb{Q}(\sqrt{1-4k^n})$ の類数は $n=2,\ 8$ を除いて n で割れる. $\mathbb{Q}(\sqrt{1-4\cdot 13^2})=\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{1-4\cdot 13^8})=\mathbb{Q}(\sqrt{-6347})$ の類数はそれぞれ 1, 28 であり, $n/2$ で割れるが n では割れない.

この定理は, 虚二次体 $\mathbb{Q}(\sqrt{1-4k^n})$ のうち類数が $n/2$ で割れるが n では割れない可能性のあるもの (Theorem 8 (1) に該当するケース) が, 与えられた奇数 $k\neq 5, 13$ に対して高々一つであることを意味している. Theorem 8 (1) での仮定と, $\mathbb{Q}(\sqrt{1-4k^n})$ の整数環 $\mathcal{O}_{\mathbb{Q}(\sqrt{1-4k^n})}$ のある元のノルムに関する事実とを組み合わせることで, k が奇数の時には方程式 $x^2+1=2k^z$ の正整数解 (x,z) の考察に問題が帰着される. より一般に方程式 $x^2+1=2y^z$ の正整数解 (x,y,z) はすでに研究されていて ([Ri], [BS] 参照), $z>1$ が奇数でかつ $y>1$ となる正整数解 (x,y,z) は存在しないこと, $x^2+1=2y^4$ $(y>1)$ を満たす正整数解 (x,y,z) が存在するのは $y=13$ の時のみであること, 方程式 $x^2+1=2y^z$ が二つの正整数解 $(x,y,1)$, $(x',y,2)$ を持つならば $y=1,5$ となることなどが知られている. これらの結果を用いることにより, 類数が $n/2$ で割れるが n では割れない可能性のある整数 n を, k が奇数の場合に具体的に決定することができたのが主結果 4 の内容である.

Remark 3. 主結果 4 についての Remark を挙げる. 奇数 $k\geq 3$ の素因数のうち少なくとも一つが 3 と mod 4 で合同ならば虚二次体 $\mathbb{Q}(\sqrt{1-4k^n})$ の類数は n で割れる. このことは Louboutin により示されている ([Lo] 参照). Louboutin の結果と主結果 4 を合わせると次が分かる ;

与えられた整数 $k>1$ に対して, k の素因数のうち少なくとも一つが 3 と mod 4 で合同ならば $\mathbb{Q}(\sqrt{1-4k^n})$ の類数は ($n=2,\ 4$ の時も) n で割れ, k $(\neq 5, 13)$ の素因数がすべて 1 と mod 4 で合同ならば $\mathbb{Q}(\sqrt{1-4k^n})$ の類数は高々一つを除いて n で割れる. 除外される n は 2 または 4 であり, この場合には $\mathbb{Q}(\sqrt{1-4k^n})$ の類数は $n/2$ で割れる.

謝辞 : RIMS 解析数論研究集会での発表の機会, そして, この原稿を書く機会を下さった津村博文先生, 小森靖先生に感謝申し上げます. また, 二次体の類数の可除性の考察に最初に取り組み始めた時からたくさんのアドバイスを下さった松本耕二先生をはじめ, 貴重なご意見を下さったすべての方に心より感謝申し上げます.

参考文献

[AC] N.C.Ankeny and S.Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math. **5**(1955), 321-324.

[BHV] Yu.Bilu, G.Hanrot and P.M.Voutier with an appendix by M. Mignotte, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math. **539**(2001), 75–122.

[BS] Y.Bugeaud and T.N.Shorey, On the number of solutions of the generalized Ramanujan-Nagell equation, J. Reine Angew. Math. **539**(2001), 55-74.

[Ca] Cao Zhen Fu, The divisibility of the class number of imaginary quadratic fields (Chinese), Chinese Ann. Math. Ser. A. **25**(2004), no. 3, 397–406.

[Ch] Chao Ko, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica **14**(1965), 457–460.

[He] He Bo, A remark on the Diophantine equation $(x^3 - 1)/(x - 1) = (y^n - 1)/(y - 1)$, Glas. Mat. Ser. III. **44**(64) (2009), no. 1, 1–6.

[HL] Heuberger Clemens and Le Maohua, On the generalized Ramanujan-Nagell equation $x^2 + D = p^z$, J. Number Theory. **78**(1999), no. 2, 312–331.

[It1] A.Ito, Remarks on the divisibility of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n})$, preprint.

[It2] A.Ito, Notes on the divisibility of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{3^{2e} - 4q^n})$, preprint.

[Ki] Y.Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields, Glasgow Math. J. **51**(2009), 187-191.

[Le1] Le Maohua, Exceptional solutions of the exponential Diophantine equation $(x^3 - 1)/(x - 1) = (y^n - 1)/(y - 1)$, J. Reine Angew. Math. **543**(2002), 187–192.

[Le2] Le Maohua, A note on the number of solutions of the generalized Ramanujan-Nagell equation $D_1x^2 + D_2 = 4p^n$, J. Number Theory. **62**(1997), no. 1, 100–106.

[Le3] Le Maohua, On the Diophantine equation $(x^3 - 1)/(x - 1) = (y^n - 1)/(y - 1)$, Trans. Amer. Math. Soc. **351**(1999), no. 3, 1063–1074.

[Le4] Le Maohua, Some exponential Diophantine equations. I. The equation $D_1x^2 - D_2y^2 = \lambda k^z$, J. Number Theory. **55**(1995), no. 2, 209–221.

[Le5] Le Maohua, Divisibility of the class numbers of a class of imaginary quadratic fields (Chinese), Kexue Tongbao **32**(1987), no. 10, 724–727.

[LL] Leu Ming-Guang and Li Guan-Wei, The Diophantine equation $2x^2+1 = 3^n$, Proc. Amer. Math. Soc. **131**(2003), no. 12, 3643–3645.

[Lo] Louboutin Stéphane R, On the divisibility of the class number of imaginary quadratic number fields. Proc. Amer. Math. Soc. **137**(2009), no. 12, 4025–4028.

[Mo] R.A.Mollin, Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields, Glasgow Math. J. **38**(1996), 195-197.

[Na] T. Nagell, The diophantine equation $x^2 + 7 = 2^n$, Ark. Math. **4**(1960), 185–187.

[Ri] P.Ribenboim, Catalan's Conjecture, Academic Press, New York 1994.

[Sh] T.N.Shorey, Some exponential diophantine equation, in Number theory and related topics, Bombay (1989), 217-229.

[SS] Saradha. N and Srinivasan. Anitha, Solutions of some generalized Ramanujan-Nagell equations via binary quadratic forms, Publ. Math. Debrecen **71**(2007), no. 3-4, 349–374.

[Yu1] Yuan Pingzhi, On the Diophantine equation $\frac{x^3-1}{x-1} = \frac{y^n-1}{y-1}$. J. Number Theory. **112**(2005), no. 1, 20–25.

[Yu2] Yuan Pingzhi, On the Diophantine equation $ax^2 + by^2 = ck^n$, Indag. Math. (N.S.). **16**(2005), no. 2, 301–320.

[Yu3] Yuan Ping-zhi, On the Diophantine equation $Dx^2 + 1 = ca^n$, Heilongjiang Daxue Ziran Kexue Xuebao **22**(2005), no. 2, 195–197, 203.

[Wa] Walker D. T, On the diophantine equation $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly **74**(1967), 504–513.

Akiko Ito
Graduate School of Mathematics
Nagoya University
Chikusa-ku, Nagoya 464-8602
Japan
Mail: m07004a@math.nagoya-u.ac.jp