On integers simultaneously represented by integral binary quadratic forms of a given discriminant

Hiroki Murata

The study of the problem of representing integers by quadratic forms with integral coefficients is one of the classical themes in number theory for a long time. Since Gauss's foundation for the theory of quadratic forms in the early 1800s, many researchers have been studying this subject until recent years. In a recent study, Donnay et al. considered the problem of whether there exists an integer that can be simultaneously represented by all primitive positive-definite integral binary quadratic forms of a given discriminant and conditionally solved it in 2017.

The first aim of this paper is to extend their results and to present a criterion for determining whether there exists an integer that is simultaneously represented by all primitive positive-definite binary quadratic forms of a given discriminant. The second aim is to examine several variants of the problem studied by Donnay et al. and give answers to them. Moreover, we present some interesting examples of the main results.

与えられた判別式をもつ整係数 2 元 2 次形式が同時に表現する整数について

村田　弘樹

概要

整数論において，2 次形式が表現する整数は長年に渡り研究されてきた古典的テーマの一つである．これに関する系統立てた研究の由来は，1800 年代初頭に提唱された Gauss の 2 次形式論に遡る．それ以降，Dedekind により発見された 2 次体の整数論との対応をはじめ，近年に至るまでこのテーマについて，数多くの研究が行われてきた．このテーマについて最近行われた研究の一例として，Donnay らは 2017 年に，与えられた判別式をもつ原始的整係数 2 元 2 次形式が同時に表現する正の整数が存在するか否か，という問題について，対応する 2 次体の類数が奇数の場合には存在し，類数が偶数かつ与えられた判別式が基本判別式の場合には存在しないことを明らかにした．本論文では，この結果を拡張し，与えられた判別式をもつ原始的正定値整係数 2 元 2 次形式が同時に表現する正の整数が存在するか否かを判定する方法を述べる．さらに，派生した問題として，この問題の条件を様々に変化させた問題を考察する．

1　序文

整数論において，整係数 2 元 2 次形式 $Q(x,y)=ax^2+bxy+cy^2$ が表現する整数は長年に渡り研究されてきた古典的テーマの一つである．1640 年，Fermat は 2 次形式 x^2+y^2 が表現する正の整数はどのようなものかを明らかにした．

定理 1.1 (Fermat の 2 平方和定理) 正の整数 n に対し，次の 2 つの命題は同値である．

(i) 2 次形式 x^2+y^2 は n を表現する．
(ii) n の素因数のうち，4 を法として 3 に合同なものの冪指数が全て偶数である．

ただし，2 次形式 $Q(x,y)$ が整数 n を表現するとは，$n=Q(x,y)$ となるような整数 x,y が存在することを意味する．

この 2 平方和定理は，整数論の中でも最も基本的で有名な定理の一つであり，現代数学の立場では，類体論における素イデアル分解法則の応用例である．

このような個々の 2 次形式がどのような整数を表現するかといった問題を越えて，Gauss (1777-1855) は 2 次形式全体を研究の対象とした．1801 年，Gauss はその著作「Disquisitiones Arithmeticae」において，2 元 2 次形式の理論を作り上げた．具体的には，彼は 2 次形式の間に対等という同値関係を導入し，この同値関係で判別式が不変であることや任意の 2 次形式がある簡約 2 次形式に対等であることを示し，これより同じ判別式をもつ 2 次形式が有限個の同値類に分類されることを示した．さらに，同じ判別式をもつ 2 次形式の同値類の全体に，合成という一種の群演算を定義した（第 2 節参照）．Gauss は 2 次形式論の創始者であり，彼の理論により 2 次形式がどのような整数を表し得るかといった問題が見通しよく解決できるようになった．

Gauss の 2 次形式論は後の数学者たちによって様々な改良がなされた．1863 年, Dirichlet (1805-1859) は自身の整数論の講義に基づいて「Vorlesungen über Zahlentheorie」を著した．これは Gauss の「Disquisitiones Arithmeticae」の紹介を主な目的としており，2 次形式の合成や種の理論の簡易化が含まれている．1871 年，Dedekind (1831-1916) は Dirichlet の「Vorlesungen über Zahlentheorie」の第 2 版の付録の中で，2 次体のイデアル論を用いれば Gauss の 2 次形式の理論を 2 次体の理論から説明できることを示した．Dedekind はイデアルという新しい概念を導入することにより，Kummer (1810-1893) の円分体における理想数の理論を一般の有限次代数体にまで拡張し，代数的整数の理論の基礎を築いた．この理論を用いると，2 次体のイデアル類と 2 次形式の同値類を対応させることができ，2 次形式がどのような整数を表し得るかといった問題を 2 次体の理論の中で表現できるようになった（第 6 節参照）．

Dedekind 以降も 2 次形式論に関する重要な進展があった．例えば，19 世紀末以降，Minkowski (1864-1909) や Hasse (1898-1979) らによって，体上の n 元 2 次形式の理論が発達した．特に，1923 年に発表された Minkowski–Hasse の定理は，当時できたばかりの p 進数の理論を，Hensel (1861-1941) の示唆のもとに利用したもので，Hasse 原理の最初の例という意味で数学的に重要であるばかりか，歴史的にも重要である．他にも，Cox [1] にあるように，類体論や保型形式といった，現在の整数論における基本的な概念を用いて，2 次形式の表現する整数が考察できるようになったが，この論文の主たる関心事とは方向性が異なるため，ここでは詳細は述べない．

このように，近年に至るまでこのテーマについて，数多くの研究が行われてきた．その中でも，本論文において考察する対象は，複数の 2 次形式が同時に表現する整数である．これについて，判別式の異なる 2 つの 2 次形式が同時に表現する整数の研究は Voight [9] などが興味深い結果を残しているが，本論文では同じ判別式をもつ 2 次形式が同時に表現する整数の研究を行う．本論文の主な目的は，与えられた判別式を持つ全ての 2 次形式が同時に表現する整数の研究において，新しく得られた結果を報告することである．

議論の出発点として，複数の 2 次形式が同時に表現する整数に関する問題をいきなり考えることは不自然であるし，問題の要点も捉え難くなるため，まずは最も単純な場合として，一つの 2 次形式が表現する素数に関する問題である，次の問題 1 を考える．

問題 1 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D のある原始的正定値整係数 2 元 2 次形式が表現する素数はどのようなものか．

この問題 1 は，表現する素数を判別式 D を割り切らない奇素数のみに限れば，Gauss の 2 次形式論を用いて次のように解決することができる．

定理 1.2 ([1, Theorem 2.16]) $D \equiv 0, 1 \pmod 4$ である負の整数 D と D を割り切らない奇素数 p に対し，次の 2 つの命題は同値である．

(i) D を判別式にもつある原始的正定値整係数 2 元 2 次形式が p を表現する．
(ii) D は p を法とする平方剰余である．

ただし，整係数 2 元 2 次形式 $Q(x, y) = ax^2 + bxy + cy^2$ について，Q の各単項式の係数 a, b, c の最大公約数が 1 であるとき，Q は原始的であるといい，Q が負の整数を表現し得ないとき，Q は正定値であるという．

問題 1 の文言において，「ある」の部分を「全ての」に変えるとどうなるかを実験してみると，そもそも共通して表現する素数がない場合があることが分かる．そこで，この文言において「どのようなものか」の部分を「存在するか」に変えると次の問題 2 になる．

問題 2 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D の全ての原始的正定値整係数 2 元 2 次形式が表現する素数が存在するか．

この問題 2 は第 3 節で示すように，類体論を用いて得られる「原始的正定値整係数 2 元 2 次形式は無限に多くの素数を表現する」という事実（補題 3.3）と，Gauss の 2 次形式論を用いて次のように解決される．

定理 1.3 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する素数が存在する．
(ii) 判別式 D の原始的正定値整係数 2 元 2 次形式の対等による同値類の個数（類数 $h(D)$）が 1 である．

この定理 1.3 において，「同じ同値類に属している 2 次形式が表現する整数の集合は等しい」という事実（定義 2.2 (2) 参照）を考え合わせると，与えられた判別式をもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する素数が存在するのは自明な場合のみであることが分かる．そこで，この問題 2 の文言において，「素数」の部分を「正の整数」に変えることにより，条件を弱めた次の問題 3 を考察する．

問題 3 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D の全ての原始的正定値整係数 2 元 2 次形式が表現する正の整数が存在するか．

この問題 3 について，2017 年，Donnay らは論文 [3] を発表し，部分的な解決を行った．[3] の Theorem 4 では類数 $h(D)$ が奇数の場合，そして Theorem 2 (Fundamental Discriminant Theorem) では D が基本判別式かつ類数 $h(D)$ が偶数の場合の解答を与えた．詳しくは以下の通りである．

定理 1.4 ([3], Theorem 4) $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，類数 $h(D)$ が奇数ならば，D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在する．

定理 1.5 ([3], Theorem 2) $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，D が基本判別式かつ類数 $h(D)$ が偶数ならば，D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数は存在しない．

ところが，定理 1.4 にはちょっとした誤植があり，定理 1.5 には証明に本質的な誤りがある．そこで，第 4 節と第 5 節では，基本的にはこの論文に沿いながらも，これらの定理を，筆者が修正した証明と共に述べる．

これらの結果から，与えられた判別式をもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在するか否かを判定する上で，類数の偶奇に着目することが肝要であると分かる．一方，定理 1.5 では，D が基本判別式という条件が付いているが，D が基本判別式でないものでかつ類数 $h(D)$ が偶数の場合にどうなるかを実験してみると，共通して表現する正の整数が存在するときと存在しないときのどちらもあることが分かる．

筆者は，この定理 1.4 と定理 1.5 を拡張して，与えられた判別式をもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在するか否かを判定する具体的な基準を与えることに成功した．それを述べる前に，一つ記号の説明を行う．「$D \equiv 0, 1 \pmod 4$ なる負の整数 D に対し，$\widetilde{D}$ が基本判別式かつ $D/\widetilde{D}$ が平方数となるような整数 $\widetilde{D}$ がただ一つ存在する」という事実を第 7 節で述べる．この $\widetilde{D}$ を用いて，本論文の主結果の一つである主定理 1 は次のように述べることができる．

主定理 1 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在する．
(ii) $h(\widetilde{D})$ が奇数である．

つまり，D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在するか否かは，$h(\widetilde{D})$ の偶奇によって判定できる．

この主定理 1 において，特筆すべきは，「D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在するか否か」と，「$\widetilde{D}$ を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在するか否か」という 2 つの問題に対する解答が一致してしまうことである．この事実を踏まえて，主定理 1 の証明は，定理 1.4 と定理 1.5 で明らかにされていない D が基本判別式でないものでかつ類数 $h(D)$ が偶数の場合を，基本判別式 $\widetilde{D}$ の場合に帰着させることにより行われる．

さらに，関連する問題として，この問題 3 の条件を様々に変化させた問題を考える．まず，問題 3 の条件を強めて，原始的でない 2 次形式も考察の対象に含めたものが次の問題 4 である．

問題 4 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D の全ての正定値整係数 2 元 2 次形式が表現する正の整数が存在するか．

次に，問題 3 の条件を別の観点から強めて，2 次形式による表現を原始的な表現のみに制限したものが次の問題 5 である．

問題 5 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D の全ての原始的正定値整係数 2 元 2 次形式が原始的に表現する正の整数が存在するか．

最後に，問題 4 と問題 5 の制約条件を合わせて考えたものが次の問題 6 である．

問題 6 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D の全ての正定値整係数 2 元 2 次形式が原始的に表現する正の整数が存在するか．

これらの問題群について，問題 4 に対しては完全な解答，問題 5 に対しては部分的な解答を得ることができた．より詳しくは，主定理 1 に次ぐ本論文の主結果として，以下の主定理 2 と主定理 3 を得た．

主定理 2 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) D を判別式にもつ正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在する．
(ii) $h(\widetilde{D})$ が奇数であり，かつ $D/\widetilde{D}$ の各素因子を表現するような判別式 $\widetilde{D}$ の原始的正定値整係数 2 元 2 次形式が存在する．

主定理 3 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題を考える．

(i) D を判別式にもつ原始的正定値整係数 2 元 2 次形式全てが同時に原始的に表現する正の整数が存在する．
(ii) $h(\widetilde{D})$ が奇数であり，かつ $D/\widetilde{D}$ の各素因子を表現するような判別式 $\widetilde{D}$ の原始的正定値整係数 2 元 2 次形式が存在する．

このとき，(ii) が成り立つならば (i) も成り立つ．

主定理 2 は，与えられた判別式をもつ正定値整係数 2 元 2 次形式全てが同時に表現する正の整数が存在する

ための必要十分条件を与えている．主定理 3 は，与えられた判別式をもつ正定値整係数 2 元 2 次形式全てが同時に原始的に表現する正の整数が存在するための十分条件を与えている．主定理 2 と主定理 3 において，命題 (ii) が一致していることに着目すれば，問題 5 よりも問題 4 の方が条件をより強めていることが分かる．このような問題の間の関係について，第 10 節では問題 3 から問題 6 までの各問題の関係をより詳しく述べる．

ところで，正定値とは限らない整係数 2 元 2 次形式の表現する整数についても扱った Elia [10] や，2 元とは限らない正定値 n 元 2 次形式の表現する整数について述べた Conway [11] などのように，対象を広げて研究することも考えられる．しかしながら，正定値整係数 2 元 2 次形式に限っても，充分に豊富な内容が存在するため，本論文では正定値整係数 2 元 2 次形式の表現する整数のみを取り扱うこととした．

序文の最後に，本論文の構成を述べる．第 2 節と第 6 節では，主結果を証明するための準備として，それぞれ，古典的な 2 次形式論と虚 2 次体の整数論におけるいくつかの事柄を，本論文で用いる最小限の範囲で述べる．第 3 節では定理 1.3 を証明し，問題 1 に対する完全な解答を与える．第 4 節と第 5 節では，問題 3 に対する部分的な解答である定理 1.4 と定理 1.5 を [3] に沿って与える．第 7 節では主定理 1 を証明し，問題 3 に対する完全な解答を与える．第 8 節では主定理 2 を証明し，問題 4 に対する完全な解答を与える．第 9 節では主定理 3 を証明し，問題 5 に対する部分的な解答を与える．第 10 節では問題 3 から問題 6 までの各問題の関係を整理する．

2　2 次形式

本節では，主定理を証明するための準備として，2 次形式の基本的な定義や性質のうち，後の議論に関連しているものを簡単に述べる．本節で述べる事柄はいずれも整数論において基本的な事柄であるため，証明はほとんど述べず，必要な文献を挙げるに留める．なお，前半の 2 次形式の内容は [3, §2] を，後半の Dirichlet 積の内容は [1, §3-A] を参考にした．

整数全体の集合を $\mathbf{Z}$，素数全体の集合を $\mathbf{P}$ で表す．整数 a, b, c に対し，$ax^2+bxy+cy^2$ の形の斉次多項式を整係数 2 元 2 次形式という．これにより定まる写像 $Q : \mathbf{Z}^2 \to \mathbf{Z},\ (x, y) \mapsto ax^2+bxy+cy^2$ と $ax^2+bxy+cy^2$ を同一視する．この Q を，$Q = \langle a, b, c\rangle$ とかく．さらに，

$$Q(x, y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

であることに注目して，整係数 2 元 2 次形式 $\langle a, b, c\rangle$ と行列 $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ を同一視することもある．

整係数 2 元 2 次形式 $Q = \langle a, b, c\rangle$ に対し，いくつかの概念や用語を用意する．ただし「2 次形式」のように，この論文では記述の簡明さのために一般的な用語の使い方とは必ずしも一致しない使い方をする用語もあるので注意して欲しい．

定義 2.1 整係数 2 元 2 次形式 $Q = \langle a, b, c\rangle$ について，以下のように定義する．

(1) Q が整数 m を表現するとは，$m = Q(x, y)$ となる整数 x, y が存在することである．Q は斉次であるから，Q は常に 0 を表現する．
(2) Q が整数 m を原始的に表現するとは，$m = Q(x, y)$ となる互いに素な整数 x, y が存在することである．
(3) Q が表現する整数全体のなす集合から 0 を除いた集合を $R(Q)$，Q が原始的に表現する整数全体のなす集

合から 0 を除いた集合を $R'(Q)$ とかく．

(4) 任意の $(x,y) \in \mathbf{Z}^2 \setminus \{(0,0)\}$ に対し $Q(x,y) > 0$ が成立するとき，Q は正定値であるという．Q が正定値ならば，Q が表現する正の整数全体のなす集合は $R(Q)$，Q が原始的に表現する正の整数全体のなす集合は $R'(Q)$ である．

(5) $\gcd(a,b,c) = 1$ が成立するとき，Q は原始的であるという．

(6) Q が正定値整係数 2 元 2 次形式であるとき，Q を単に 2 次形式とよぶ．

(7) Q が原始的正定値整係数 2 元 2 次形式であるとき，Q を単に原始的 2 次形式とよぶ．

(8) $D = b^2 - 4ac$ を Q の判別式という．Q が正定値ならば，D は $D \equiv 0, 1 \pmod 4$ である負の整数である．逆に，$D \equiv 0, 1 \pmod 4$ である負の整数 D を判別式に持つ Q が必ず存在する．

さらに，負の判別式 D に対し，いくつかの概念や用語を用意する．

定義 2.2 $D \equiv 0, 1 \pmod 4$ である負の整数 D について，以下のように定義する．

(1) 判別式 D をもつ 2 次形式全体のなす集合を $F(D)$，判別式 D をもつ原始的 2 次形式全体のなす集合を $F'(D)$ とかく．

(2) 2 次形式 Q_1, Q_2 に対し，$Q_1(x,y) = Q_2(sx+ty, ux+vy)$ となる $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ が存在するとき，Q_1, Q_2 は対等であるといい，$Q_1 \sim Q_2$ とかく．$Q_1 \sim Q_2$ ならば，Q_1, Q_2 の判別式は等しく，$R(Q_1) = R(Q_2)$, $R'(Q_1) = R'(Q_2)$ が成り立つ．この二項関係 $\sim$ は $F(D)$, $F'(D)$ における同値関係になっている．このとき，2 次形式 Q を含む同値類を $[Q]$ とかく．なお，Q_1, Q_2 を行列と同一視すると，Q_1, Q_2 が対等であるとは，$Q_1 = {}^tMQ_2M$ となる $M \in \mathrm{SL}(2,\mathbf{Z})$ が存在することである．

(3) 判別式 D をもつ 2 次形式 $Q = \langle a,b,c \rangle$ が

$$c > a \geq b > -a \quad \text{または} \quad c = a \geq b \geq 0$$

を満たすとき，Q は簡約であるという．

(4) $F(D)$ のうち簡約であるもの全体のなす集合を $F_{\mathrm{red}}(D)$，$F'(D)$ のうち簡約であるもの全体のなす集合を $F'_{\mathrm{red}}(D)$ とかく．$F_{\mathrm{red}}(D)$, $F'_{\mathrm{red}}(D)$ は有限集合であり，それぞれ同値関係 $\sim$ による $F(D)$, $F'(D)$ の商集合 $F(D)/\!\sim$, $F'(D)/\!\sim$ の代表元の集合の一つになっている．

(5) 判別式 D が次の (i), (ii) のいずれかを満たすとき，D は基本判別式，または単に D は基本であるという．

(i) $D \equiv 1 \pmod 4$ かつ D が平方因子をもたない．

(ii) $D \equiv 0 \pmod 4$ かつ $D/4 \equiv 2, 3 \pmod 4$ かつ $D/4$ が平方因子をもたない．

第 1 節で述べたように，本論文の目的の一つは，「与えられた D を判別式にもつ 2 次形式または原始的 2 次形式全てが同時に表現する正の整数が存在するか否かを判定すること」であったが，このことを定義 2.1 や 2.2 で述べた記号を用いて表すと，「$D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，$S = F(D), F'(D)$ のとき $\bigcap_{Q \in S} R(Q) \neq \emptyset$ となるか否かを判定すること」と言い換えることができる．この集合 $\bigcap_{Q \in S} R(Q)$ について，基本的な性質をいくつか述べる．

命題 2.3 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題が成り立つ．

(i) $\bigcap_{Q \in F(D)} R(Q)$, $\bigcap_{Q \in F'(D)} R(Q)$ は空集合または無限集合である．

(ii) $\displaystyle\bigcap_{Q\in F(D)} R(Q) = \bigcap_{Q\in F_{\mathrm{red}}(D)} R(Q),\quad \bigcap_{Q\in F'(D)} R(Q) = \bigcap_{Q\in F'_{\mathrm{red}}(D)} R(Q).$

証明

(i) もし $\displaystyle\bigcap_{Q\in F(D)} R(Q) \neq \emptyset$ であれば，$m \in \displaystyle\bigcap_{Q\in F(D)} R(Q)$ がとれる．各 $Q \in F(D)$ に対し $m = Q(x, y)$ となる整数 x, y をとれば，任意の正の整数 l に対し $l^2 m = Q(lx, ly)$ となって $l^2 m \in R(Q)$ が成立するから，$l^2 m \in \displaystyle\bigcap_{Q\in F(D)} R(Q)$ も成立する．従って，$\displaystyle\bigcap_{Q\in F(D)} R(Q)$ が空集合でないならば，$\displaystyle\bigcap_{Q\in F(D)} R(Q)$ は無限集合となり，$\displaystyle\bigcap_{Q\in F(D)} R(Q)$ が空でない有限集合になることはない．$F'(D)$ のときも同様に示せる．

(ii) $Q, Q' \in F(D)$ に対し，$Q \sim Q'$ ならば $R(Q) = R(Q')$ であるから，$\displaystyle\bigcap_{Q'\in[Q]} R(Q') = R(Q)$ となる．このことと，$F_{\mathrm{red}}(D)$ は商集合 $F(D)/\!\sim$ の代表元の集合の一つになっていることより，$\displaystyle\bigcap_{Q\in F(D)} R(Q) = \bigcap_{Q\in F_{\mathrm{red}}(D)} R(Q)$ が成り立つ．$F'(D)$ のときも同様に示せる． □

命題 2.3 (ii) より，第 1 節で述べた問題 2 から問題 4 までの各問題は，簡約な 2 次形式または原始的 2 次形式全体に制限して考えれば良いことが分かる．したがって，無限集合である $F(D), F'(D)$ から有限集合である $F_{\mathrm{red}}(D), F'_{\mathrm{red}}(D)$ へと考える対象を狭めることができる．2 次形式による表現を原始的な表現のみに制限した問題 5 と問題 6 についても，「2 つの対等な 2 次形式が原始的に表現する正の整数の集合は等しい」という事実（定義 2.2 (2) 参照）から，全く同じように考えることができる．

さて，負の判別式 D に対し，原始的 2 次形式の集合 $F'(D)$ を定義したが，この $F'(D)$ に Dirichlet 積 $\circ$ を導入する．$Q_1 = \langle a_1, b_1, c_1\rangle, Q_2 = \langle a_2, b_2, c_2\rangle \in F'(D)$ に対し，$Q_3 = \langle a_3, b_3, c_3\rangle = Q_1 \circ Q_2 \in F'(D)$ を以下で定める：

- $\gcd(a_1, a_2, (b_1 + b_2)/2) = 1$ のとき，$a_j B \equiv a_j b_j \pmod{2a_1a_2}\,(j = 1, 2)$ かつ $\frac{b_1+b_2}{2} B \equiv \frac{b_1b_2+D}{2} \pmod{2a_1a_2}$ となる整数 B を一つとり，$a_3 = a_1a_2$, $b_3 = B$, $c_3 = (B^2 - D)/(4a_3)$ とする．

- $\gcd(a_1, a_2, (b_1+b_2)/2) = d\,(> 1)$ のとき，$\frac{a_j}{d} B \equiv \frac{a_j}{d} b_j \pmod{\frac{2a_1a_2}{d}}\,(j = 1, 2)$ かつ $\frac{b_1+b_2}{2d} B \equiv \frac{b_1b_2+D}{2d} \pmod{\frac{2a_1a_2}{d}}$ となる整数 B を一つとり，$a_3 = a_1a_2/d^2$, $b_3 = B$, $c_3 = (B^2 - D)/(4a_3)$ とする．

2 つの同値類 $[Q_1], [Q_2] \in F'(D)/\!\sim$ に対し $[Q_1] \cdot [Q_2] = [Q_1 \circ Q_2] \in F'(D)/\!\sim$ によって積を定めると，この演算は well-defined であり，この演算によって $F'(D)/\!\sim$ は有限 Abel 群となる．この群を $C(D)$ と表す．群 $C(D)$ の位数を類数とよび，$h(D)$ と表す．定義 2.2 (4) により，類数は常に有限である．群 $C(D)$ において，単位元は $D \equiv 0 \pmod 4$ のとき $[\langle 1, 0, -D/4\rangle]$ であり，$D \equiv 1 \pmod 4$ のとき $[\langle 1, 1, (1 - D)/4\rangle]$ である．$C(D)$ の単位元となる同値類のうち，簡約である原始的 2 次形式を基本形式とよぶ．また，$[Q] = [\langle a, b, c\rangle]$ の逆元は $[Q]^{-1} = [\langle a, -b, c\rangle]$ である．

3 問題 2 の解答

本節では，問題 2 の解答，すなわち負の判別式 D に対し，D を判別式にもつ原始的 2 次形式全てが同時に表現する素数が存在するか否かについての判定法を与える．

補題 3.1 ([1, Lemma 2.3]). 原始的 2 次形式 Q が整数 m を原始的に表現するならば，ある整数 b, c が存在し

て，Q は $\langle m,b,c\rangle$ と対等である．

証明 m が互いに素な整数 s,u により $m=Q(s,u)$ と表現されているものとする．このとき，$sv-tu=1$ を満たす整数 t,v をとれば，$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ であり，$Q(x,y)\sim Q(sx+ty,ux+vy)$ が成り立つ．この右辺を $Q'(x,y)$ とおけば，$Q'(x,y)$ の x^2 の係数が $Q(s,u)=m$ となるから，整数 b,c を用いて，$Q'=\langle m,b,c\rangle$ とできる． □

注意 3.2 補題 3.1 の証明において，$\begin{pmatrix} s & t \\ u & v \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ に対し，$Q''(x,y)=Q'(sx+ty,ux+vy)$ とおくと，$Q'\sim Q''$ かつ $Q''=\langle c,b,m\rangle$ となることに注意すれば，次も成り立つ：原始的 2 次形式 Q が整数 m を原始的に表現するならば，ある整数 a,b が存在して，Q は $\langle a,b,m\rangle$ と対等である．

補題 3.3 原始的 2 次形式 Q に対し，$R(Q)\cap\mathbf{P}$ は無限集合である．つまり，原始的 2 次形式は無限に多くの素数を表現する．

証明 [1, Theorem 9.12] の一部であるが，証明は本論文の主旨から外れるため，省略する． □

命題 3.4 $D\equiv 0,1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) $\left(\bigcap_{Q\in F'(D)} R(Q)\right)\cap\mathbf{P}\neq\emptyset$,
(ii) $h(D)=1$.

つまり，D を判別式にもつ原始的 2 次形式全てが同時に表現する素数が存在するための必要十分条件は，判別式 D の原始的 2 次形式が全て判別式 D の基本形式と対等であることである．

証明 [1, Exercise 2.27(a)] の誘導に従って証明する．$h(D)=1$ のときは，$F'_{\mathrm{red}}(D)=\{Q\}$（$Q$ は $F'(D)$ の基本形式）となるから，補題 3.3 より (i) が成立する．以下，$h(D)\geq 2$ とする．このとき，$[Q_1]\neq[Q_2]$ かつ $[Q_1]\neq[Q_2]^{-1}$ となるような $Q_1,Q_2\in F'(D)$ がとれる．実際，位数が 2 以上の $F'_{\mathrm{red}}(D)$ から基本形式とそれとは異なる元をとり，それらを Q_1,Q_2 とすればよい．このとき，(i) が成り立っていると仮定すると， (i) の左辺の集合に属す素数 p が取れる．すると，p の取り方より $p\in R(Q_1), p\in R(Q_2)$ であり，素数 p の Q_1,Q_2 による表現は原始的であるから，補題 3.1 から，ある整数 $b_i,c_i\,(i=1,2)$ が存在して，$Q_1\sim\langle p,b_1,c_1\rangle$, $Q_2\sim\langle p,b_2,c_2\rangle$ とできる．対等な原始的 2 次形式の判別式は等しいため，$D=b_1^2-4pc_1=b_2^2-4pc_2$ が成立し，特に $D\equiv b_1^2\equiv b_2^2 \pmod{4p}$, $(b_1+b_2)(b_1-b_2)\equiv 0 \pmod{4p}$ が成立する．$p=2$ のとき，$(b_1+b_2)(b_1-b_2)\equiv 0 \pmod 8$ となるため，b_1+b_2, b_1-b_2 のどちらかは $4(=2p)$ で割り切れる．p が奇素数のとき，$(b_1-b_2)(b_1+b_2)\equiv 0 \pmod 4$ と b_1-b_2, b_1+b_2 の偶奇が一致することより，b_1-b_2, b_1+b_2 はどちらも偶数であり，さらに，$(b_1-b_2)(b_1+b_2)\equiv 0 \pmod p$ より b_1-b_2, b_1+b_2 のどちらかは p で割り切れるため，b_1-b_2, b_1+b_2 のどちらかは $2p$ で割り切れる．いま，$Q'_1=\langle p,b_1,c_1\rangle$, $Q'_2=\langle p,b_2,c_2\rangle$ とおき，b_1-b_2, b_1+b_2 のどちらが $2p$ の倍数かで場合分けを行う．

$2p\mid b_1-b_2$ のとき，整数 k を用いて $b_1-b_2=2pk$ と表すと，$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\in\mathrm{SL}(2,\mathbf{Z})$ に対し，$Q'_1(x,y)=Q'_2(x+ky,y)$ が成立するから，$Q'_1\sim Q'_2$ となる．対等は同値関係であったから，推移律より $Q_1\sim Q_2$ だが，これは $Q_1\not\sim Q_2$ に矛盾する．

$2p \mid b_1+b_2$ のとき，整数 k を用いて $b_1+b_2=2pk$ と表すと，$Q_2''=\langle p,-b_2,c_2\rangle \in [Q_2']^{-1}=[Q_2]^{-1}$，$\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ に対し，$Q_1'(x,y)=Q_2''(x+ky,y)$ が成立するから，$Q_1' \sim Q_2''$ となる．対等は同値関係であったから，推移律より $Q_1 \sim Q_2''$ だが，これは $[Q_1] \neq [Q_2]^{-1}$ に矛盾する．

以上により，$h(D) \geq 2$ のとき，(i) が成り立たないことが分かった． □

系 3.5 $D \equiv 0,1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) $\left(\bigcap_{Q\in F'(D)} R(Q)\right) \cap \mathbf{P} \neq \emptyset$,

(ii) $D=-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163$.

証明 命題 3.4 と [1, Theorem 7.30] より成り立つ．証明は本論文の主旨から外れるため，省略する． □

4 問題 3 の解答：類数が奇数の場合

本節では，類数 $h(D)$ が奇数となるような D に対し，問題 3 を考える．その解答として，命題 4.2 で，そのような判別式 D の 2 次形式全てが表現する正の整数が存在することを述べ，それを $\bigcap_{Q\in F'_{\mathrm{red}}(D)} R(Q)$ の具体的な元を求めることにより証明する．

命題 4.1 判別式 D の原始的 2 次形式 Q_1,Q_2 に対し，$m_1 \in R(Q_1)$ かつ $m_2 \in R(Q_2)$ ならば，$m_1m_2 \in R(Q_1\circ Q_2)$ である．

証明 $m_1 \in R(Q_1)$ かつ $m_2 \in R(Q_2)$ より，整数 $x_i,y_i\,(i=1,2)$ を用いて $m_1=Q_1(x_1,y_1)$, $m_2=Q_2(x_2,y_2)$ と表せる．$g_i=\gcd(x_i,y_i)$, $m_i'=m_i/g_i^2$, $x_i'=x_i/g_i$, $y_i'=y_i/g_i\,(i=1,2)$ とおけば，$m_1'=Q_1(x_1',y_1')$, $m_2'=Q_2(x_2',y_2')$ であるから，Q_1,Q_2 は m_1',m_2' をそれぞれ原始的に表現する．このとき，補題 3.1 よりある整数 $b_i,c_i\,(i=1,2)$ が存在して，$Q_1 \sim \langle m_1',b_1,c_1\rangle, Q_2 \sim \langle m_2',b_2,c_2\rangle$ とできる．

$\gcd(m_1',m_2',\frac{b_1+b_2}{2})=1$ のとき，$Q_1\circ Q_2 \sim \langle m_1',b_1,c_1\rangle \circ \langle m_2',b_2,c_2\rangle = \langle m_1'm_2',*,*\rangle$ より，$m_1'm_2' \in R(Q_1\circ Q_2)$ が成立する．そこで，$Q_3=Q_1\circ Q_2$ とおいて，$m_1'm_2'$ を $m_1'm_2'=Q_3(x_3,y_3)$ と整数 x_3,y_3 を用いて表せば，$x=g_1g_2x_3$, $y=g_1g_2y_3$ に対し $Q_3(x,y)=g_1^2g_2^2\cdot m_1'm_2'=g_1^2g_2^2\cdot\frac{m_1}{g_1^2}\frac{m_2}{g_2^2}=m_1m_2$ より，$m_1m_2 \in R(Q_3)$ が成立する．

$\gcd(m_1',m_2',\frac{b_1+b_2}{2})=d\,(>1)$ のとき，$Q_1\circ Q_2 \sim \langle m_1',b_1,c_1\rangle \circ \langle m_2',b_2,c_2\rangle = \langle \frac{m_1'm_2'}{d^2},*,*\rangle$ より，$\frac{m_1'm_2'}{d^2} \in R(Q_1\circ Q_2)$ が成立する．そこで，$Q_3=Q_1\circ Q_2$ とおいて，$\frac{m_1'm_2'}{d^2}$ を $\frac{m_1'm_2'}{d^2}=Q_3(x_3,y_3)$ と整数 x_3,y_3 を用いて表せば、$x=dg_1g_2x_3$, $y=dg_1g_2y_3$ に対し，$Q_3(x,y)=d^2g_1^2g_2^2\cdot\frac{m_1'm_2'}{d^2}=g_1^2g_2^2\cdot\frac{m_1}{g_1^2}\frac{m_2}{g_2^2}=m_1m_2$ より，$m_1m_2 \in R(Q_3)$ が成立する． □

命題 4.2 $D \equiv 0,1 \pmod 4$ である負の整数 D に対し，$h(D)$ が奇数ならば，$\bigcap_{Q\in F'(D)} R(Q) \neq \emptyset$ が成り立つ．つまり，D を判別式にもつ原始的 2 次形式全てが同時に表現する正の整数が存在する．

証明 $h(D)=1$ のときは，$F'_{\mathrm{red}}(D)=\{Q\}$（$Q$ は $F'(D)$ の基本形式）となるから明らかである．以下，正の整数 n を用いて $h(D)=2n+1$ と表し，$F'_{\mathrm{red}}(D)$ の元を次のように番号付けする：

$$\begin{cases} Q_1 = \langle 1, b_0, c_0 \rangle : \text{基本形式}, \\ Q_2 = \langle a_1, b_1, c_1 \rangle, \\ Q_3 = \langle a_1, -b_1, c_1 \rangle \in [Q_2]^{-1}, \\ \cdots, \\ Q_{2n} = \langle a_n, b_n, c_n \rangle, \\ Q_{2n+1} = \langle a_n, -b_n, c_n \rangle \in [Q_{2n}]^{-1}. \end{cases}$$

ここで，簡約の定義から，$\langle a, b, c \rangle$ が $F'_{\mathrm{red}}(D)$ の元であれば $\langle a, -b, c \rangle$ も $F'_{\mathrm{red}}(D)$ の元であることと，$h(D)$ が奇数より，$Q \in F'_{\mathrm{red}}(D) \setminus \{Q_1\}$ に対し $[Q] \neq [Q]^{-1}$ が成り立つことに注意する．このとき，$h(D)$ が奇数であるから，$[Q] \mapsto [Q]^2$ により定まる $C(D)$ 上の写像は有限集合上の全単射となり，各 $Q_j\,(2 \leq j \leq 2n+1)$ に対し $[Q_k]^2 = [Q_j]$ となる $Q_k \in F'_{\mathrm{red}}(D)\,(2 \leq k \leq 2n+1)$ をただ一つとれる．いま，

$$Q'_j = \begin{cases} Q_2 \circ Q_3 \circ \cdots \circ Q_{k-1} \circ Q_k \circ Q_k \circ Q_{k+2} \circ \cdots \circ Q_{2n} \circ Q_{2n+1} & (k : \text{奇数}) \\ Q_2 \circ Q_3 \circ \cdots \circ Q_{k-2} \circ Q_k \circ Q_k \circ Q_{k+1} \circ \cdots \circ Q_{2n} \circ Q_{2n+1} & (k : \text{偶数}) \end{cases}$$

とおく．すると，$Q'_j \sim Q_1 \circ \cdots \circ Q_1 \circ Q_k \circ Q_k \circ Q_1 \circ \cdots \circ Q_1 \sim Q_k \circ Q_k \sim Q_j$ である．各 $i\,(1 \leq i \leq n)$ に対し $a_i \in R(Q_{2i}),\, c_i \in R(Q_{2i+1})$ であることに注意して，$m = \prod_{i=1}^{n} a_i c_i$ といたとき，命題 4.1 より $m \in R(Q'_j) = R(Q_j)\,(2 \leq j \leq 2n+1)$ が成立する．また，$Q'_1 = Q_2 \circ Q_3 \circ \cdots \circ Q_{2n} \circ Q_{2n+1}$ とおくと，$Q'_1 \sim Q_1 \circ \cdots \circ Q_1 \sim Q_1$ から，命題 4.1 より $m \in R(Q'_1) = R(Q_1)$ が成立する．以上により，この m が判別式 D のすべての原始的 2 次形式で表現されることが分かったから，命題の主張が示された． □

注意 4.3 本証明は [3, Theorem 4] とほとんど同じであるが，[3] では m のおき方に誤植があったため, それらを修正するために証明を記載した．

例 4.4 (命題 4.2 の具体例)

(1) $D = -23$ のとき，$h(D) = 3$ であり，これは奇数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 1, 6 \rangle, Q_2 = \langle 2, 1, 3 \rangle, Q_3 = \langle 2, -1, 3 \rangle\}$ である．すると，命題 4.2 の証明より $2 \cdot 3 = 6$ がこの 3 つの原始的 2 次形式で表現されるはずだが，$6 = Q_1(0, 1) = Q_2(1, 1) = Q_3(1, -1)$ より，これは実際に成立している．しかも，このとき，Q_1, Q_2, Q_3 は 6 を原始的に表現できていることを注意しておく．

(2) $D = -31$ のとき，$h(D) = 3$ であり，これは奇数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 1, 8 \rangle, Q_2 = \langle 2, 1, 4 \rangle, Q_3 = \langle 2, -1, 4 \rangle\}$ である．すると，命題 4.2 の証明より $2 \cdot 4 = 8 \in \bigcap_{Q \in F'(D)} R(Q)$ となるはずだが，$8 = Q_1(0, 1) = Q_2(2, 0) = Q_3(2, 0)$ より，これは実際に成立している．しかしながら，Q_2, Q_3 は 8 を原始的に表現できず，$8 \notin \bigcap_{Q \in F'(D)} R'(Q)$ である．なお，例 9.4 で，Q_1, Q_2, Q_3 全てが同時に原始的に表現する正の整数の例を挙げる．

5 問題 3 の解答：基本判別式かつ類数が偶数の場合

本節では，類数 $h(D)$ が偶数かつ基本判別式であるような D に対し，問題 3 を考える．その解答として，命題 5.4 で，[3] の Theorem 2 (Fundamental Discriminant Theorem) を述べる．この証明は，類数が偶数かつ基本であるような D の形に注目した場合分けを行い，それぞれの場合において命題の主張を示すことによっ

て行う．

本節以降で用いる平方剰余記号 $\left(\frac{a}{p}\right)$ を定義する．なお，本節では p が奇素数である場合のみに平方剰余記号 $\left(\frac{a}{p}\right)$ を用いるが，第 6 節では $p=2$ の場合にも用いる．

定義 5.1 奇素数 p と整数 a に対して，

$$\left(\frac{a}{p}\right)=\begin{cases}0, & p \mid a,\\ 1, & p \nmid a \ \text{ かつ } \ a \text{ が } p \text{ を法とする平方剰余},\\ -1, & p \nmid a \ \text{ かつ } \ a \text{ が } p \text{ を法とする平方非剰余}\end{cases}$$

と定める．また，$p=2$ の場合については，$a \equiv 0,1 \pmod 4$ である整数 a に対して，

$$\left(\frac{a}{2}\right)=\begin{cases}0, & a \equiv 0 \pmod 4,\\ 1, & a \equiv 1 \pmod 8,\\ -1, & a \equiv 5 \pmod 8\end{cases}$$

と定める．

命題 5.2 ([1, Proposition 3.11]). $D \equiv 0,1 \pmod 4$ である負の整数 D に対し，r, μ を以下で定める：

$$r=\#\{p \in \mathbf{P} \setminus \{2\} \mid D \equiv 0 \pmod p\},$$

$$\mu=\begin{cases}r, & D \equiv 1 \pmod 4,\\ r, & D=-4n,\ n \equiv 3 \pmod 4,\\ r+1, & D=-4n,\ n \equiv 1,2 \pmod 4,\\ r+1, & D=-4n,\ n \equiv 4 \pmod 8,\\ r+2, & D=-4n,\ n \equiv 0 \pmod 8.\end{cases}$$

このとき，$C(D)$ の元で位数が 2 以下のものの個数は $2^{\mu-1}$ である．

証明 証明は本論文の主旨から外れるため，省略する． □

補題 5.3 ([3, Lemma 10]). $D=-2^h \cdot p_1 \cdots p_r \equiv 0,1 \pmod 4$ ($p_1, \cdots, p_r$は奇素数, $h \geq 0$) となる負の整数 D と，D を割らない奇素数 q により $Q=\langle q,b,c\rangle$ と表される判別式 D の原始的 2 次形式 Q をとる．このとき，各 $i\,(1 \leq i \leq r)$ に対し次の 2 つの命題が成り立つ．

(i) $\left(\frac{q}{p_i}\right)=1$ かつ $m \in R(Q)$ ならば，$\left(\frac{m}{p_i}\right)=1$ または $p_i \mid m$,
(ii) $\left(\frac{q}{p_i}\right)=-1$ かつ $m \in R(Q)$ ならば，$\left(\frac{m}{p_i}\right)=-1$ または $p_i \mid m$.

証明 補題の仮定の下で $c=(-D+b^2)/(4q)$ であり，これを代入して $Q(x,y)=q(x+\frac{b}{2q}y)^2-\frac{D}{4q}y^2$ を得る．いま，$m=Q(x,y)$ となる整数 x,y をとれば，各 $1 \leq i \leq r$ に対し $\gcd(q,p_i)=1$ より $m \equiv q(x+\frac{b}{2q}y)^2 \pmod{p_i}$ となる．よって，$\left(\frac{m}{p_i}\right)=\left(\frac{q(x+\frac{b}{2q}y)^2}{p_i}\right)$ より，$\left(\frac{m}{p_i}\right)=\left(\frac{q}{p_i}\right)$ または $p_i \mid m$ を得る． □

命題 5.4 ([3, Theorem 2]). $D \equiv 0,1 \pmod 4$ である負の整数 D に対し，D が基本判別式かつ $h(D)$ が偶数ならば，$\bigcap_{Q \in F'(D)} R(Q)=\emptyset$ が成り立つ．つまり，D を判別式にもつ原始的 2 次形式全てが同時に表現する正の整数は存在しない．

証明 命題 5.2 より，$D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，命題 5.2 の μ が 2 以上であるか否かによって類数 $h(D)$ の偶奇を判定することができる．特に，負の基本判別式 D に対し，$h(D)$ が偶数となるのは，D が 2 を割り切る回数に注目すれば，次の (I) から (III) までのいずれかの場合となる：

(I) $D = -p_1 \cdots p_r = -s \equiv 1 \pmod 4$, $r \geq 2$,
(II) $D = -4p_1 \cdots p_r = -4s$, $s \equiv 1 \pmod 4$ のとき $r \geq 1$, $s \equiv 3 \pmod 4$ のとき $r \geq 2$,
(III) $D = -8p_1 \cdots p_r = -8s$, $r \geq 1$.

ただし，$p_1, \cdots, p_r$ は全て異なる奇素数で，各場合共通して，$s = p_1 \cdots p_r$ とおいた．

以下では，この場合分けに従って考える．証明は背理法による．(I), (II), (III) の各場合それぞれにおいて $\bigcap_{Q \in F'(D)} R(Q) \neq \emptyset$ を仮定したとき，ある $F'_{\mathrm{red}}(D)$ の空でない部分集合 S, S' で $S \subset S'$ を満たし，さらに次の (i) と (ii) を満たすようなものがとれることを示す：

(i) $m \in \bigcap_{Q \in S} R(Q)$ ならば，$s|m$,
(ii) $m = s^k l \in \bigcap_{Q \in S'} R(Q)$, $k \geq 1$, $s \nmid l$ ならば，$l \in \bigcap_{Q \in S} R(Q)$.

なお，(I), (II) においては $S = S'$ であるが，(III) においてのみ $S \neq S'$ となっている．すると，$F'_{\mathrm{red}}(D)$, S, S' の包含関係から，(i) に注意して $m = s^k l \in \bigcap_{Q \in S'} R(Q)$, $k \geq 1$, $s \nmid l$ となる m をとることができるが，(ii) より $l \in \bigcap_{Q \in S} R(Q)$ となり，これは (i) に矛盾する．

(I) $D = -p_1 \cdots p_r = -s \equiv 1 \pmod 4$, $r \geq 2$: この場合に (i) を満たす S の取り方を述べる．$D \equiv 1 \pmod 4$ より，基本形式は $Q_1 = \langle 1, 1, \frac{1+s}{4} \rangle$ であり，整数 x, y と各 $1 \leq i \leq r$ に対し $Q_1(x, y) \equiv (x + \frac{y}{2})^2 \pmod{p_i}$ が成立するので，

$$m \in R(Q_1) \quad \text{ならば，} \quad \left(\frac{m}{p_i}\right) = 1 \quad \text{または} \quad p_i | m. \tag{5.1}$$

一方，中国剰余定理と Dirichlet の算術級数定理を用いることにより，各 $1 \leq i \leq r$ に対し $\left(\frac{q}{p_i}\right) = -1$ が成り立ち，かつ $\left(\frac{D}{q}\right) = 1$ を満たす奇素数 q がとれる．$\left(\frac{D}{q}\right) = 1$ より $D \equiv b'^2 \equiv (q - b')^2 \pmod q$ となる整数 b' がとれ，q が奇数であることより b を b' または $q - b'$ にとって $D \equiv b^2 \pmod{4q}$ とできる．さらに，$D = b^2 - 4qc$ となる整数 c をとって，$Q_2 = \langle q, b, c \rangle$ を定める．このとき，補題 5.3 より，

$$m \in R(Q_2) \quad \text{ならば，} \quad \left(\frac{m}{p_i}\right) = -1 \quad \text{または} \quad p_i | m. \tag{5.2}$$

よって，(5.1), (5.2) より，各 $1 \leq i \leq r$ に対し，$m \in R(Q_1) \cap R(Q_2)$ ならば $p_i | m$ である．したがって，$S = \{Q_1, Q_2\}$ とおけば，各 p_i が異なることより (i) を得る．つぎに，$S = S' = \{Q_1, Q_2\}$ に対して (ii) が成り立つことを示す．方針としては，整数 k, l を用いて $m = s^k l$ と表し，s の指数 k を段々と下げていく．

$m = s^k l \in R(Q_1)$, $k \geq 2$, $s \nmid l$ のとき，$m = Q_1(x, y) = (x + \frac{y}{2})^2 + \frac{sy^2}{4}$ となる整数 x, y をとると，

$$\left(x + \frac{y}{2}\right)^2 \equiv 0 \pmod s \quad \text{よって，} \quad -2x \equiv y \pmod s$$

であるから，$x \not\equiv 0$, $y \not\equiv 0 \pmod s$ または $x \equiv y \equiv 0 \pmod s$ となる．整数 h を用いて $y = -2x + hs$ と表せば，

$$m = x^2 + x(-2x + hs) + \frac{1+s}{4}(-2x + hs)^2 \equiv sx^2 \pmod{s^2} \quad \text{よって，} \quad s^k l \equiv sx^2 \pmod{s^2}$$

であるから，$x \equiv y \equiv 0 \pmod{s}$ となり，整数 i, j を用いて $x = is$, $y = js$ と表せる．このとき，

$$m = \left(is + \frac{js}{2}\right)^2 + \frac{s}{4}(js)^2 \quad \text{よって，} \quad \frac{m}{s^2} = \left(i + \frac{j}{2}\right)^2 + \frac{sj^2}{4}$$

であるから，

$$m = s^k l \in R(Q_1),\ k \geq 2,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s^2} \in R(Q_1). \tag{5.3}$$

一方，$s = Q_1(-1, 2)$ より $s \in R(Q_1)$ が成り立つので，命題 4.1 より $\frac{m}{s^2} \cdot s = \frac{m}{s} \in R(Q_1 \circ Q_1) = R(Q_1)$ となるから，

$$m = s^k l \in R(Q_1),\ k \geq 2,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s} \in R(Q_1). \tag{5.4}$$

$m = s^k l \in R(Q_2),\ k \geq 2,\ s \nmid l$ のとき，$m = Q_2(x, y) = q(x + \frac{by}{2q})^2 + \frac{sy^2}{4q}$ となる整数 x, y をとると，

$$q\left(x + \frac{by}{2q}\right)^2 \equiv 0 \pmod{s} \quad \text{よって，} \quad -2qx \equiv by \pmod{s}$$

であるから，$x \not\equiv 0,\ y \not\equiv 0 \pmod{s}$ または $x \equiv y \equiv 0 \pmod{s}$ となる．整数 h を用いて $by = -2qx + hs$ と表せば，

$$m = q\{x + \frac{1}{2q}(-2qx + hs)\}^2 + \frac{s}{4qb^2}(-2qx + hs)^2 \equiv s\frac{qx^2}{b^2} \pmod{s^2} \quad \text{よって，} \quad s^k l \equiv \frac{qx^2}{b^2} \pmod{s^2}$$

であるから，$x \equiv y \equiv 0 \pmod{s}$ となり，整数 i, j を用いて $x = is$, $y = js$ と表せる．このとき，

$$m = q\left(is + \frac{jbs}{2q}\right)^2 + \frac{s}{4q}(js)^2 \quad \text{よって，} \quad \frac{m}{s^2} = q\left(i + \frac{jb}{2q}\right)^2 + \frac{sj^2}{4q}$$

であるから，

$$m = s^k l \in R(Q_2),\ k \geq 2,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s^2} \in R(Q_2). \tag{5.5}$$

一方，$s = Q_1(-1, 2)$ より $s \in R(Q_1)$ が成り立つので，命題 4.1 より $\frac{m}{s^2} \cdot s = \frac{m}{s} \in R(Q_2 \circ Q_1) = R(Q_2)$ となるから，

$$m = s^k l \in R(Q_2),\ k \geq 2,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s} \in R(Q_2). \tag{5.6}$$

以下，m が s を割り切る回数によって二つに場合分けして，各場合において (ii) が成り立つことを確認する．

$m = s^k l \in \bigcap_{Q \in S} R(Q),\ k \geq 2,\ s \nmid l$ の場合，$s^k l \in R(Q_1)$ かつ $s^k l \in R(Q_2)$ である．前者について，(5.4) を繰り返し用いると $s^2 l \in R(Q_1)$ となり，これに (5.3) を用いれば，$l \in R(Q_1)$ が成り立つ．後者について，(5.6) を繰り返し用いると $s^2 l \in R(Q_2)$ となり，これに (5.5) を用いれば，$l \in R(Q_2)$ が成り立つ．よって，$l \in \bigcap_{Q \in S} R(Q)$ が従う．

$m = sl \in \bigcap_{Q \in S} R(Q),\ s \nmid l$ の場合，$sl = Q_1(x_1, y_1) = Q_2(x_2, y_2)$ となる整数 $x_i, y_i\,(i = 1, 2)$ をとると，$s^3 l = Q_1(sx_1, sy_1) = Q_2(sx_2, sy_2)$ より $s^3 l \in \bigcap_{Q \in S} R(Q)$ となり，$s^3 l$ は s を 2 回以上割り切るため，もう一つの場合に帰着される．

(II) $D=-4p_1\cdots p_r=-4s$, $s\equiv 1 \pmod 4$ のとき $r\geq 1$, $s\equiv 3 \pmod 4$ のとき $r\geq 2$ ：この場合に (i) を満たす S の取り方を述べる．$D\equiv 0 \pmod 4$ より，基本形式は $Q_3=\langle 1,0,s\rangle$ であり，整数 x,y と各 $1\leq i\leq r$ に対し $Q_3(x,y)\equiv x^2 \pmod{p_i}$ が成立するので，

$$m\in R(Q_3) \quad \text{ならば，} \quad \left(\frac{m}{p_i}\right)=1 \quad \text{または} \quad p_i|m. \tag{5.7}$$

一方，(I) と同様に，各 $1\leq i\leq r$ に対し $\left(\frac{q}{p_i}\right)=-1$ が成り立ち，かつ $\left(\frac{D}{q}\right)=1$ を満たす奇素数 q と $D=b^2-4qc$ となる整数 b,c をとって，$Q_4=\langle q,b,c\rangle$ を定める．このとき，補題 5.3 より，

$$m\in R(Q_4) \quad \text{ならば，} \quad \left(\frac{m}{p_i}\right)=-1 \quad \text{または} \quad p_i|m. \tag{5.8}$$

よって，(5.7), (5.8) より，各 $1\leq i\leq r$ に対し，$m\in R(Q_3)\cap R(Q_3)$ ならば $p_i|m$ である．$S=\{Q_3,Q_4\}$ とおけば，各 p_i が異なることより (i) を得る．つぎに， $S=S'=\{Q_3,Q_4\}$ に対して (ii) が成り立つことを示す．これは，s の指数 k の値に注意すれば (I) の (ii) とほとんど同様にできる．

$m=s^kl\in R(Q_3)$, $k\geq 1$, $s\nmid l$ のとき，$m=Q_3(x,y)=x^2+sy^2$ となる整数 x,y をとると，

$$x^2\equiv 0 \pmod s \quad \text{よって，} \quad x\equiv 0 \pmod s$$

であるから、整数 i を用いて $x=is$ と表せる．このとき，

$$m=(is)^2+sy^2 \quad \text{よって，} \quad \frac{m}{s}=si^2+y^2$$

であるから，

$$m=s^kl\in R(Q_3),\ k\geq 1,\ s\nmid l \quad \text{ならば，} \quad \frac{m}{s}\in R(Q_3). \tag{5.9}$$

$m=s^kl\in R(Q_4)$, $k\geq 2$, $s\nmid l$ のとき，(I) と同様にして，

$$m=s^kl\in R(Q_4),\ k\geq 2,\ s\nmid l \quad \text{ならば，} \quad \frac{m}{s^2}\in R(Q_4). \tag{5.10}$$

一方，$s=Q_3(0,1)$ より $s\in R(Q_3)$ が成り立つので，命題 4.1 より $\frac{m}{s^2}\cdot s=\frac{m}{s}\in R(Q_4\circ Q_3)=R(Q_4)$ となるから，

$$m=s^kl\in R(Q_4),\ k\geq 2,\ s\nmid l \quad \text{ならば，} \quad \frac{m}{s}\in R(Q_4). \tag{5.11}$$

以下，(I) と同様にして，m が s を割り切る回数によって二つ場合分けして，各場合において (ii) が成り立つことを確認する．

$m=s^kl\in \bigcap_{Q\in S} R(Q)$, $k\geq 2$, $s\nmid l$ の場合，$s^kl\in R(Q_3)$ かつ $s^kl\in R(Q_4)$ である．前者について，(5.9) を繰り返し用いて，$l\in R(Q_3)$ が成り立つ．後者について，(5.11) を繰り返し用いると $s^2l\in R(Q_4)$ となり，これに (5.10) を用いれば，$l\in R(Q_4)$ が成り立つ．よって，$l\in \bigcap_{Q\in S} R(Q)$ が従う．

$m=sl\in \bigcap_{Q\in S} R(Q)$, $s\nmid l$ の場合，(I) と同様にして，もう一つの場合に帰着される．

(III) $D=-8p_1\cdots p_r=-8s$, $r\geq 1$: この場合に (i) を満たす S の取り方を述べる．$D\equiv 0 \pmod 4$ より，基本形式は $Q_5=\langle 1,0,2s\rangle$ であり，整数 x,y と各 $1\leq i\leq r$ に対し $Q_5(x,y)\equiv x^2 \pmod{p_i}$ が成立するので，

$$m\in R(Q_5) \quad \text{ならば，} \quad \left(\frac{m}{p_i}\right)=1 \quad \text{または} \quad p_i|m. \tag{5.12}$$

一方，(I) と同様に，各 $1 \leq i \leq r$ に対し $\left(\frac{q}{p_i}\right) = -1$ が成り立ち，かつ $\left(\frac{D}{q}\right) = 1$ を満たす奇素数 q と $D = b^2 - 4qc$ となる整数 b, c をとって，$Q_6 = \langle q, b, c\rangle$ を定める．このとき，補題 5.3 より，

$$m \in R(Q_6) \quad \text{ならば，} \quad \left(\frac{m}{p_i}\right) = -1 \quad \text{または} \quad p_i | m. \tag{5.13}$$

よって，(5.12), (5.13) より，各 $1 \leq i \leq r$ に対し，$m \in R(Q_5) \cap R(Q_6)$ ならば $p_i | m$ である．$S = \{Q_5, Q_6\}$ とおけば，各 p_i が異なることより (i) を得る．次に， $S = \{Q_5, Q_6\}$ に対して適した S' をとって (ii) が成り立つことを示すが，その際に $Q_5' = \langle 2, 0, s\rangle \in F'(D)$ についても考える必要がある．

$m = s^k l \in R(Q_5)$, $k \geq 1$, $s \nmid l$ のとき，$m = Q_5(x, y) = x^2 + 2sy^2$ となる整数 x, y をとると，

$$x^2 \equiv 0 \pmod{s} \quad \text{よって，} \quad x \equiv 0 \pmod{s}$$

であるから，整数 i を用いて $x = is$ と表せる．このとき，

$$m = (is)^2 + 2sy^2 \quad \text{よって，} \quad \frac{m}{s} = si^2 + 2y^2$$

であるから，

$$m = s^k l \in R(Q_5),\ k \geq 1,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s} \in D(Q_5'). \tag{5.14}$$

$m = s^k l \in R(Q_5'),\ k \geq 1,\ s \nmid l$ のとき，$m = Q_5'(x, y) = 2x^2 + sy^2$ となる整数 x, y をとると，

$$2x^2 \equiv 0 \pmod{s} \quad \text{よって，} \quad x \equiv 0 \pmod{s}$$

であるから，整数 i を用いて $x = is$ と表せる．このとき，

$$m = 2(is)^2 + sy^2 \quad \text{よって，} \quad \frac{m}{s} = 2si^2 + y^2$$

であるから，

$$m = s^k l \in R(Q_5'),\ k \geq 1,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s} \in R(Q_5). \tag{5.15}$$

よって，(5.14), (5.15) より，

$$m = s^k l \in R(Q_5) \cap R(Q_5'),\ k \geq 1,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s} \in R(Q_5) \cap R(Q_5'). \tag{5.16}$$

以下，Q_5', Q_6 が対等か否かによってさらに場合分けを行う．

- $Q_5' \sim Q_6$ のとき，$S' = S = \{Q_5, Q_6\}$ とする．$m = s^k l \in \bigcap_{Q \in S} R(Q) = R(Q_5) \cap R(Q_5')$, $k \geq 1$, $s \nmid l$ に対し，(5.16) を繰り返し用いると，$l \in R(Q_5) \cap R(Q_5') = \bigcap_{Q \in S} R(Q)$ が成り立つ．

- $Q_5' \nsim Q_6$ のとき，さらに $Q_6' = Q_6 \circ Q_5'$ も考え，$S' = \{Q_5, Q_5', Q_6, Q_6'\}$ とする．

  $m = s^k l \in R(Q_6)$, $k \geq 2$, $s \nmid l$ のとき，(I) と同様にして，

  $$m = s^k l \in R(Q_6),\ k \geq 2,\ s \nmid l \quad \text{ならば，} \quad \frac{m}{s^2} \in R(Q_6). \tag{5.17}$$

  $m = s^k l \in R(Q_6')$, $k \geq 2$, $s \nmid l$ のとき，$s = Q_5'(0, 1)$ より $s \in R(Q_5')$ が成り立つので，命題 4.1 より $ms \in R(Q_6' \circ Q_5') = R(Q_6 \circ Q_5' \circ Q_5') = R(Q_6)$ となるから，

  $$m = s^k l \in R(Q_6'),\ k \geq 1,\ s \nmid l \quad \text{ならば，} \quad ms \in R(Q_6). \tag{5.18}$$

ここで，$Q_5' = \langle 2, 0, s\rangle$ ゆえ，$[Q_5']^{-1} = [\langle 2, 0, s\rangle] = [Q_5']$ であるから，$Q_5' \circ Q_5'$ は基本形式 Q_5 と対等であることを用いた．

$m = s^k l \in \bigcap_{Q\in S} R(Q) = R(Q_5)\cap R(Q_5')\cap R(Q_6)\cap R(Q_6')$, $k \geq 1$, $s \nmid l$ のとき，$s^k l \in R(Q_5)\cap R(Q_5')$ かつ $s^k l \in R(Q_6) \cap R(Q_6')$ である．前者について，(5.16) を繰り返し用いると，$l \in R(Q_5) \cap R(Q_5')$ が成り立つ．後者について，k が偶数のとき，$s^k l \in R(Q_6)$ に (5.17) を繰り返し用いると，$l \in R(Q_6)$ が成り立つ．k が奇数のとき，$s^k l \in R(Q_6')$ に (5.18) を用いて，$s^{k+1} l \in R(Q_6)$ となり，これに (5.17) を繰り返し用いると，$l \in R(Q_6)$ が成り立つ．したがって，$l \in R(Q_5) \cap R(Q_5') \cap R(Q_6) \subset \bigcap_{Q\in S} R(Q)$ が従う． □

注意 5.5 本証明の方針は [3, Theorem 2] に沿ったものであるが，[3, Theorem 2] の証明は (III) の場合において，基本形式 $Q_5 = \langle 1, 0, 2s\rangle$ は s を表現するなどと記述しており，これは s が平方数でないことと $s < 2s$ であることから明らかに間違いである．また，[3, Theorem 2] の証明では，全ての場合で集合 S, S' を同じものとして取っているため，(III) の場合に議論が行き詰まってしまう．そこで，本論文では，(III) の場合に $S = \{Q_5, Q_6\}$, $S' = \{Q_5, Q_5', Q_6, Q_6'\}$ と異なる集合をとることによって誤りを修正した．

例 5.6 (命題 5.4 の具体例) $D = -24$ のとき，$h(D) = 2$ であり，これは偶数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 0, 6\rangle, Q_2 = \langle 2, 0, 3\rangle\}$ である．すると，$D/4 = 6$ が平方因子を持たないため $D = -24$ が基本判別式であることに注意すると，命題 5.3 より判別式が -24 の全ての原始的 2 次形式により表現される正の整数は存在しない．

6 虚 2 次体

本節では，主定理を証明するための準備として，虚 2 次体の基本的な定義や性質のうち，後の主定理の証明の議論に関連しているものを簡単に述べた後，2 次形式を虚 2 次体の中で考えることで得られる，2 次形式が表現する整数に関するいくつかの性質を述べる．これを行うにあたり，代数的整数論の基本的な知識は前提として，用語の定義などを詳しく書かない事もあるが，そのような用語については，例えば [1] を参照して頂きたい．本節は本論文において，「異なる判別式の原始的 2 次形式が表現する整数の関係を明らかにする」という，主定理の証明のアイデアを担っており，非常に重要である．なお，前半の原始的 2 次形式の同値類全体がなす群 $C(D)$（第 2 節参照）と虚 2 次体の整環のイデアル類群の対応については [1, §7] を，後半の異なる判別式の原始的 2 次形式が表現する整数の関係については [2, §8] を参考にした．

有理数全体のなす集合を $\mathbf{Q}$，虚部が正である複素数全体のなす集合を $\boldsymbol{H}$ で表す．平方因子をもたない負の整数 N が与えられたとき，$\mathbf{Q}(\sqrt{N})$ の形をした体を虚 2 次体という．虚 2 次体 $K = \mathbf{Q}(\sqrt{N})$ に対し，いくつかの概念や用語を用意する．

定義 6.1 虚 2 次体 $K = \mathbf{Q}(\sqrt{N})$ について，以下のように定義する．

(1) K の元で $\mathbf{Z}$ 上整であるもの全体の集合を K の整数環といい，$\mathcal{O}_K$ とかく．整数環 $\mathcal{O}_K$ は Dedekind 環で

あり，階数が 2 の $\mathbf{Z}$ 上の自由加群である．より詳しくは，与えられた N に対し，

$$\mathcal{O}_K = \begin{cases} \left\langle 1, \frac{1+\sqrt{N}}{2} \right\rangle_{\mathbf{Z}}, & N \equiv 1 \pmod 4, \\ \langle 1, \sqrt{N} \rangle_{\mathbf{Z}}, & N \equiv 2, 3 \pmod 4 \end{cases}$$

とかける．ここで，$\alpha, \beta \in \mathcal{O}_K$ に対し，$\langle \alpha, \beta \rangle_{\mathbf{Z}}$ は $\mathbf{Z}$ 加群 $\alpha\mathbf{Z} + \beta\mathbf{Z}$ を表す．さらに，$w_K = \frac{d_K + \sqrt{d_K}}{2}$ を用いれば，$\mathcal{O}_K = \langle 1, w_K \rangle_{\mathbf{Z}}$ と表せる．

(2) $\mathcal{O}_K$ を $\mathbf{Z}$ 上の自由加群とみて，その基底の一つを $\{\alpha, \beta\}$ としたとき，$d_K = \left| \begin{array}{cc} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{array} \right|^2$ を K の判別式という．ここで，K の元 x に対し，x の共役を $\overline{x}$ と表す．判別式 d_K は基底の取り方によらず一意に定まる．より詳しくは，

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

と表せる．d_K は基本判別式である．また，負の基本判別式は，ある虚 2 次体の判別式になっている．

(3) $\mathcal{O}_K$ の部分環で $\mathbf{Z}$ 加群として階数 2 の自由加群をなすものを，K の整環という．$\mathcal{O}_K$ は K の整環で極大なものである．

また，K の整環 $\mathcal{O}$ に対し，いくつかの概念や用語を用意する．

定義 6.2 K の整環 $\mathcal{O}$ について，以下のように定義する．

(1) $\mathcal{O}$ は $\mathcal{O}_K$ の部分加群であり，その指数 $f = [\mathcal{O}_K : \mathcal{O}]$ を $\mathcal{O}$ のコンダクターという．この f を用いれば，$\mathcal{O} = \mathbf{Z} + f\mathcal{O}_K = \langle 1, f w_K \rangle_{\mathbf{Z}}$ と表せる．

(2) $\mathcal{O}$ を $\mathbf{Z}$ 上の自由加群とみて，その基底の組の一つを $\{\alpha, \beta\}$ としたとき，$D = \left| \begin{array}{cc} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{array} \right|^2$ を $\mathcal{O}$ の判別式という．これは基底の取り方によらず一意に定まり，$D = f^2 d_K$ と表せる．このとき，D は $D \equiv 0, 1 \pmod 4$ である負の整数である．

命題 6.3 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，判別式が D である虚 2 次体の整環 $\mathcal{O}$ がただ一つ存在する．

証明 与えられた D に対し，$K = \mathbf{Q}(\sqrt{D})$ として，d_K が定まる．$f = \sqrt{D/d_K}$ とおけば，整環 $\mathcal{O} = \langle 1, f w_K \rangle_{\mathbf{Z}}$ の判別式は $f^2 d_K = D$ である． □

零でない K の部分 $\mathcal{O}$ 加群で，$\mathcal{O}$ 加群として有限生成なものを $\mathcal{O}$ の分数イデアルという．整環 $\mathcal{O}$ の分数イデアル $\mathfrak{a}$ に対し，いくつかの概念や用語を用意する．

定義 6.4 K の整環 $\mathcal{O}$ の分数イデアル $\mathfrak{a}$ について，以下のように定義する．

(1) $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ となる $\mathcal{O}$ の分数イデアル $\mathfrak{b}$ が存在するとき，$\mathfrak{a}$ は可逆であるという．

(2) $\mathcal{O} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{a}\}$ が成立するとき，$\mathfrak{a}$ は固有であるという．

補題 6.5 ([1, Lemma 7.5]). $K = \mathbf{Q}(\tau)$ を虚 2 次体，$ax^2 + bx + c$ を $\gcd(a, b, c) = 1$ となる τ の最小多項式とする．このとき，$\mathcal{O} = \langle 1, a\tau \rangle_{\mathbf{Z}}$ は K の整環であり，$\langle 1, \tau \rangle_{\mathbf{Z}}$ は $\mathcal{O}$ の固有イデアルである．

証明 $a\tau \in \mathcal{O}_K$ であるから，$\langle 1, a\tau\rangle_{\mathbf{Z}}$ は K の整環となる．このとき，任意の $\beta \in K$ に対し，$\beta\langle 1,\tau\rangle_{\mathbf{Z}} \subset \langle 1,\tau\rangle_{\mathbf{Z}}$ となるための必要十分条件は，$\beta\cdot 1 \in \langle 1,\tau\rangle_{\mathbf{Z}}$ かつ $\beta\cdot\tau \in \langle 1,\tau\rangle_{\mathbf{Z}}$ である．$\beta \in \langle 1,\tau\rangle_{\mathbf{Z}}$ より $\beta = m + n\tau$ となる整数 m, n がとれる．すると，

$$\beta\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau - c) = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau$$

より，$\gcd(a,b,c) = 1$ に注意すれば，$\beta\tau \in \langle 1,\tau\rangle_{\mathbf{Z}}$ は $a \mid n$ と同値である．従って，$\mathcal{O} = \{\beta \in K \mid \beta\langle 1,\tau\rangle_{\mathbf{Z}} \subset \langle 1,\tau\rangle_{\mathbf{Z}}\} = \langle 1, a\tau\rangle_{\mathbf{Z}}$ となって，補題の主張が示された． □

命題 6.6 ([1, Proposition 7.4]). 整環 $\mathcal{O}$ の分数イデアル $\mathfrak{a}$ に対し，$\mathfrak{a}$ が可逆であることと $\mathfrak{a}$ が固有であることは同値である．

証明 $\mathcal{O}$ の可逆イデアル $\mathfrak{a}$ に対し，$\mathfrak{b}$ を $\mathfrak{ab} = \mathcal{O}$ となる分数イデアルとする．$\mathcal{O} \subset \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}$ は常に成り立つので、逆の包含関係を示せばよい．$\beta \in K$ を $\beta\mathfrak{a} \subset \mathfrak{a}$ となるものとする．このとき，$\beta\mathcal{O} = \beta\mathfrak{ab} \subset \mathfrak{ab} = \mathcal{O}$ より $\beta \subset \mathcal{O}$ となるので $\mathfrak{a}$ は固有イデアルである．

一方，$\mathcal{O}$ の固有イデアル $\mathfrak{a}$ に対し，$\mathfrak{a} = \alpha\mathfrak{b}$ となる $\alpha \in K$ と $\mathcal{O}$ のイデアル $\mathfrak{b}$ をとる．$\mathcal{O}/\mathfrak{b}$ は有限であるから，$\mathfrak{a}$ は階数 2 の $\mathbf{Z}$ 上の自由加群であり，$\beta, \gamma \in K$ を用いて $\mathfrak{a} = \langle\beta,\gamma\rangle_{\mathbf{Z}}$ とかける．$\tau = \gamma/\beta$ とおけば，$\mathfrak{a} = \beta\langle 1,\tau\rangle_{\mathbf{Z}}$ であり，$ax^2 + bx + c$ を $\gcd(a,b,c) = 1$ となる τ の最小多項式とすれば，固有イデアルの定義に注意して，補題 6.5 の証明より $\mathcal{O} = \langle 1, a\tau\rangle_{\mathbf{Z}}$ が成り立つ．$\overline{\tau}$ は $ax^2 + bx + c$ のもう一方の根となるから，補題 6.5 より $\overline{\mathfrak{a}} = \overline{\beta}\langle 1,\overline{\tau}\rangle_{\mathbf{Z}}$ は $\langle 1, a\overline{\tau}\rangle_{\mathbf{Z}} = \langle 1, a\tau\rangle_{\mathbf{Z}} = \mathcal{O}$ の固有イデアルである．解と係数の関係より $\tau + \overline{\tau} = -b/a$, $\tau\overline{\tau} = c/a$ が成り立つことと $\gcd(a,b,c) = 1$ であることに注意すると，

$$a\mathfrak{a}\overline{\mathfrak{a}} = a\beta\langle 1,\tau\rangle_{\mathbf{Z}}\overline{\beta}\langle 1,\overline{\tau}\rangle_{\mathbf{Z}} = N(\beta)\langle a, a\tau, a\overline{\tau}, a\tau\overline{\tau}\rangle_{\mathbf{Z}} = N(\beta)\langle a, a\tau, -b, c\rangle_{\mathbf{Z}} = N(\beta)\langle 1, a\tau\rangle_{\mathbf{Z}} = N(\beta)\mathcal{O}$$

となるから，$\mathfrak{a}$ は可逆イデアルである． □

命題 6.7 ([1, Lemma 7.14]). 整環 $\mathcal{O}$ の固有イデアル $\mathfrak{a}, \mathfrak{b}$ に対し，$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$ が成り立つ．

証明 命題 6.6 の証明と同様に，$\mathfrak{a} = \beta\langle 1,\tau\rangle_{\mathbf{Z}}$ とおいて，$ax^2 + bx + c$ を $\gcd(a,b,c) = 1$ となる τ の最小多項式としたときに，$\mathcal{O} = \langle 1, a\tau\rangle_{\mathbf{Z}}$ となる．このとき，$\langle a, a\tau\rangle_{\mathbf{Z}}$ の $\langle 1, a\tau\rangle_{\mathbf{Z}}$ における指数は明らかに a であるから，

$$N(\mathfrak{a}) = N\left(\frac{\beta}{a}\langle a, a\tau\rangle_{\mathbf{Z}}\right) = \frac{N(\beta)}{a^2}N(\langle a, a\tau\rangle_{\mathbf{Z}}) = \frac{N(\beta)}{a}$$

が成り立つ．よって，命題 6.6 の証明より $a\mathfrak{a}\overline{\mathfrak{a}} = N(\beta)\mathcal{O}$ が成り立つことと合わせて，$\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$ が従う．さらに，

$$N(\mathfrak{ab})\mathcal{O} = \mathfrak{ab}\cdot\overline{\mathfrak{ab}} = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{b}\overline{\mathfrak{b}} = N(\mathfrak{a})\mathcal{O}\cdot N(\mathfrak{b})\mathcal{O} = N(\mathfrak{a})N(\mathfrak{b})\mathcal{O}$$

より $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ が従う． □

K の整環 $\mathcal{O}$ に対し，$I(\mathcal{O})$ を $\mathcal{O}$ の固有イデアル全体のなす群，$P(\mathcal{O})$ を $\mathcal{O}$ の単項分数イデアル全体のなす群とする．このとき，$P(\mathcal{O})$ は $I(\mathcal{O})$ の部分群であり，商群 $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ を $\mathcal{O}$ のイデアル類群という．このとき，$\mathcal{O}$ の固有イデアル $\mathfrak{a}$ に対し，$\mathfrak{a}$ を含む $C(\mathcal{O})$ の元を $[\mathfrak{a}]$ とかく．

ここで，原始的 2 次形式の同値類全体のなす群 $C(D)$ と虚 2 次体の整環のイデアル類群 $C(\mathcal{O})$ の対応を見る．第 2 節で説明した Dirichlet 積は $D \equiv 0, 1 \pmod 4$ である任意の整数 D に対し導入できるが，第 2 節

において負の整数に限定したのは，本節のように 2 次形式を虚 2 次体の中で議論ができるようにするためである．

命題 6.8 ([1, Theorem 7.7]). $\mathcal{O}$ を判別式 D をもつ虚 2 次体の整環とするとき，次の 3 つの命題が成り立つ．

(i) $Q = \langle a, b, c\rangle \in F'(D)$ に対し，$\langle a, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}}$ は $\mathcal{O}$ の固有イデアルである．

(ii) (i) の $\langle a, b, c\rangle \in F'(D)$ から $\langle a, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}} \in I(\mathcal{O})$ への対応は，$C(D)$ から $C(\mathcal{O})$ への同型を導く．

(iii) 正の整数 m と $Q \in F'(D)$ に対し， $m \in R(Q)$ となることと，Q に対応する固有イデアルと同じ類に含まれる固有イデアル $\mathfrak{a}$ で $m = N(\mathfrak{a})$ となるものが存在することは同値である．

証明 (i) を示す．$D < 0$ ゆえ，$Q(x, 1) = ax^2 + bx + c$ は実根を持たず，$Q(\tau, 1) = 0$ となる $\tau \in \boldsymbol{H}$ がとれる．$a > 0$ に注意すれば，$\tau = (-b+\sqrt{D})/(2a)$ であり，$\langle a, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}} = \langle a, a\tau\rangle_{\mathbf{Z}} = a\langle 1, \tau\rangle_{\mathbf{Z}}$ となる．このとき，Q が原始的であるから $\gcd(a, b, c) = 1$ となることに注意すれば，補題 6.5 より $\mathcal{O}' = \langle 1, a\tau\rangle_{\mathbf{Z}}$ は整環であり，$a\langle 1, \tau\rangle_{\mathbf{Z}} \subset \mathcal{O}'$ は固有イデアルとなる．f を $\mathcal{O}'$ のコンダクターとすると，$D = f^2 d_K$ であるから，

$$a\tau = \frac{-b+\sqrt{D}}{2} = \frac{-b+f\sqrt{d_K}}{2} = -\frac{b+fd_K}{2} + f\frac{d_K+\sqrt{d_K}}{2} = -\frac{b+fd_K}{2} + fw_K$$

となる．$D = b^2 - 4ac$ と $D = f^2 d_K$ より fd_K, b の偶奇は一致するので，$(b + fd_K)/2$ は整数となる．よって，$\langle 1, a\tau\rangle_{\mathbf{Z}} = \langle 1, fw_K\rangle_{\mathbf{Z}}$ より $\mathcal{O}' = \mathcal{O}$ となるから，$\langle a, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}} = a\langle 1, \tau\rangle_{\mathbf{Z}}$ は $\mathcal{O}' = \mathcal{O}$ の固有イデアルである．

(ii) を示す．写像 $\phi : C(D) \to C(\mathcal{O})$, $[\langle a, b, c\rangle] \mapsto [\langle a, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}}]$ について，ϕ が同型であることを以下のように何段階かに分けて示す．

まず，ϕ が well-defined であることを示す．$Q_1 = \langle a_1, b_1, c_1\rangle$, $Q_2 = \langle a_2, b_2, c_2\rangle \in F'(D)$ に対し，$Q_1(\tau_1, 1) = Q_2(\tau_2, 1) = 0$ となる $\tau_1, \tau_2 \in \boldsymbol{H}$ をとると，Q_1, Q_2 はそれぞれ $a_1\langle 1, \tau_1\rangle_{\mathbf{Z}}, a_2\langle 1, \tau_2\rangle_{\mathbf{Z}}$ に対応する．いま，$Q_1 \sim Q_2$ であるとして，$Q_1(x, y) = Q_2(sx + ty, ux + vy)$ となる $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ をとる．すると，

$$0 = Q_1(\tau_1, 1) = Q_2(s\tau_1 + t, u\tau_1 + v) = (u\tau_1 + v)^2 Q_2\left(\frac{s\tau_1 + t}{u\tau_1 + v}, 1\right)$$

となるが，$\tau_1 \in \boldsymbol{H}$ かつ $\mathrm{Im}\left(\dfrac{s\tau_1 + t}{u\tau_1 + v}\right) = |u\tau_1 + v|^{-2}\mathrm{Im}(\tau_1)$ より $\dfrac{s\tau_1 + t}{u\tau_1 + v} \in \boldsymbol{H}$ に注意すれば，$\tau_2 = \dfrac{s\tau_1 + t}{u\tau_1 + v}$ が分かる．さらに，$\lambda = u\tau_1 + v \in K$ とおくと，$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ に注意して，

$$\lambda\langle 1, \tau_2\rangle_{\mathbf{Z}} = (u\tau_1 + v)\left\langle 1, \frac{s\tau_1 + t}{u\tau_1 + v}\right\rangle_{\mathbf{Z}} = \langle u\tau_1 + v, s\tau_1 + t\rangle_{\mathbf{Z}} = \langle 1, \tau_1\rangle_{\mathbf{Z}}$$

がいえるので，$a_1\langle 1, \tau_1\rangle_{\mathbf{Z}}$, $a_2\langle 1, \tau_2\rangle_{\mathbf{Z}}$ は $C(\mathcal{O})$ の同じ類に含まれる．

次に，ϕ が単射であることを示す．いま，$a_1\langle 1, \tau_1\rangle_{\mathbf{Z}}$, $a_2\langle 1, \tau_2\rangle_{\mathbf{Z}}$ が $C(\mathcal{O})$ の同じ類に含まれるものと仮定して，$\langle 1, \tau_1\rangle_{\mathbf{Z}} = \lambda\langle 1, \tau_2\rangle_{\mathbf{Z}}$ を満たす $\lambda \in K$ をとる．すると，$\langle 1, \tau_1\rangle_{\mathbf{Z}} = \langle \lambda, \lambda\tau_2\rangle_{\mathbf{Z}}$ より $\lambda\tau_2 = s\tau_1 + t$ かつ $\lambda = u\tau_1 + v$ となる $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{GL}(2, \mathbf{Z})$ がとれる．このとき，$\tau_2 = \dfrac{s\tau_1 + t}{u\tau_1 + v}$ と表せ，$\tau_1, \tau_2 \in \boldsymbol{H}$ かつ $\mathrm{Im}\left(\dfrac{s\tau_1 + t}{u\tau_1 + v}\right) = |u\tau_1 + v|^{-2}\mathrm{Im}(\tau_1)$ より $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ である．さらに，$0 = Q_1(\tau_1, 1) =$

$Q_2(\tau_2,1)=Q_2(s\tau_1+t,u\tau_1+v)$ より $Q_1(x,1)$, $Q_2(sx+t,ux+v)$ は同じ根 $\tau_1,\overline{\tau_1}$ を持ち，Q_1,Q_2 が原始的ゆえ $Q_1(x,y)=Q_2(sx+ty,ux+vy)$ が分かる．

さらに，ϕ が全射であることを示す．$\mathcal{O}$ の固有イデアル $\mathfrak{a}$ に対し，命題 6.6 の証明と同様に，$\mathfrak{a}$ を $\beta\in K,\tau\in\boldsymbol{H}$ を用いて $\mathfrak{a}=\beta\langle 1,\tau\rangle_{\mathbf{Z}}$ と表し，ax^2+bx+c を $a>0$ かつ $\gcd(a,b,c)=1$ となる τ の最小多項式とすれば，$\mathcal{O}=\langle 1,a\tau\rangle_{\mathbf{Z}}$ が成り立つ．このとき，$Q=\langle a,b,c\rangle$ とおき，Q の判別式を D' とすると，$\tau=(-b+\sqrt{D'})/(2a)$ と表せて，

$$D=\begin{vmatrix}1 & a\tau\\ 1 & a\overline{\tau}\end{vmatrix}^2=a^2(\overline{\tau}-\tau)^2=a^2\cdot\frac{D'}{a^2}=D'$$

より $Q\in F'(D)$ となり，Q は $a\langle 1,\tau\rangle_{\mathbf{Z}}$ に対応する．

最後に，ϕ が準同型であることを示す．$Q_1=\langle a_1,b_1,c_1\rangle, Q_2=\langle a_2,b_2,c_2\rangle\in F'(D)$ に対し，$Q_3=\langle a_3,b_3,c_3\rangle=Q_1\circ Q_2\in F'(D)$ は，$\gcd(a_1,a_2,(b_1+b_2)/2)=1$ の場合，$a_3=a_1a_2, b_3=B, c_3=(B^2-D)/(4a_3)$ となる．ただし，整数 B は $a_jB\equiv a_jb_j\pmod{2a_1a_2}\,(j=1,2)$ かつ $\frac{b_1+b_2}{2}B\equiv\frac{b_1b_2+D}{2}\pmod{2a_1a_2}$ を満たすようにとる．このとき，Q_1,Q_2,Q_3 はそれぞれ $\langle a_1,(-b_1+\sqrt{D})/2\rangle_{\mathbf{Z}}$, $\langle a_2,(-b_2+\sqrt{D})/2\rangle_{\mathbf{Z}}$, $\langle a_1a_2,(-B+\sqrt{D})/2\rangle_{\mathbf{Z}}$ に対応する．$d=(-B+\sqrt{D})/2$ とおくと，$B\equiv b_j\pmod{2a_j}\,(j=1,2)$ に注意すれば，

$$\langle a_1,(-b_1+\sqrt{D})/2\rangle_{\mathbf{Z}}=\langle a_1,d\rangle_{\mathbf{Z}}\text{ かつ }\langle a_2,(-b_2+\sqrt{D})/2\rangle_{\mathbf{Z}}=\langle a_2,d\rangle_{\mathbf{Z}}$$

が成り立つ．$B\equiv b_j\pmod{2a_j}\,(j=1,2)$ かつ $(b_1+b_2)B\equiv b_1b_2+D\pmod{2a_1a_2}$ ゆえ，$D\equiv(b_1+b_2)B-b_1b_2=B^2-(B-b_1)(B-b_2)\equiv B^2\pmod{4a_1a_2}$ であるから，

$$d^2+dB=d(d+B)=(-B+\sqrt{D})(B+\sqrt{D})/4=(D-B^2)/4\equiv 0\pmod{a_1a_2}$$

となる．よって，$\gcd(a_1,a_2)=1$ かつ $B\equiv b_j\pmod{2a_j}\,(j=1,2)$ ゆえ，$\gcd(a_1,a_2,B)=1$ となることに注意すれば，

$$\langle a_1,d\rangle_{\mathbf{Z}}\langle a_2,d\rangle_{\mathbf{Z}}=\langle a_1a_2,a_1d,a_2d,d^2\rangle_{\mathbf{Z}}=\langle a_1a_2,a_1d,a_2d,-Bd\rangle_{\mathbf{Z}}=\langle a_1a_2,d\rangle_{\mathbf{Z}}$$

が成り立つ．$\gcd(a_1,a_2,(b_1+b_2)/2)>1$ の場合は，$Q_2\sim Q_2'$ となる $Q_2'=\langle a_2',b_2',c_2'\rangle\in F'(D)$ で $\gcd(a_1,a_2',(b_1+b_2')/2)=1$ を満たすものを考えて，上の場合に帰着させる．補題 3.3 より $\gcd(a_1,Q_2(s,u))=\gcd(s,u)=1$ となる整数 s,u が存在する．このとき，$sv-tu=1$ となる整数 t,v をとれば，$\begin{pmatrix}s & t\\ u & v\end{pmatrix}\in\mathrm{SL}(2,\mathbf{Z})$ となり，$Q_2'(x,y)=Q_2(sx+ty,ux+vy)$ によって $Q_2'\in F'(D)$ を定めれば，$\gcd(a_1,a_2')=\gcd(a_1,Q_2(s,u))=1$ より $\gcd(a_1,a_2',(b_1+b_2')/2)=1$ が成り立つ．

(iii) を示す．$m\in R(Q)$ に対し $m=d^2a$ となる正の整数 d と $a\in R'(Q)$ がとれる．すると，補題 3.1 より $Q\sim Q'=\langle a,b,c\rangle$ となる整数 b,c がとれて，(ii) によって Q' が対応する固有イデアルを $\mathfrak{a}$ とすると，(i) の証明により $N(\mathfrak{a})=a$ となり，$N(d\mathfrak{a})=d^2a=m$ が従う．

一方，$N(\mathfrak{a})=m$ とすると，$\mathfrak{a}\subset\mathcal{O}$ であり，$\mathfrak{a}=\beta\langle 1,\tau\rangle_{\mathbf{Z}}$ となる $\beta\in K,\tau\in\boldsymbol{H}$ がとれる．このとき，命題 6.6 の証明と同様に，ax^2+bx+c を $\gcd(a,b,c)=1$ かつ $a>0$ となる τ の最小多項式として，$Q=\langle a,b,c\rangle$ とおくと，(ii) の ϕ が全射であることの証明より，Q は $a\langle 1,\tau\rangle_{\mathbf{Z}}$ に対応する．すると，命題 6.7 の証明より $m=N(\mathfrak{a})=\frac{N(\beta)}{a}$ だが，$\beta\langle 1,\tau\rangle_{\mathbf{Z}}=\mathfrak{a}\subset\mathcal{O}=\langle 1,a\tau\rangle_{\mathbf{Z}}$ ゆえ，$\beta=s+ta\tau$, $\beta\tau=u+va\tau$ となる整数 s,t,u,v がとれる．すると，$(s+ta\tau)\tau=u+va\tau$ かつ $a\tau^2=-b\tau-c$ より，$s=av+bt$ を得る．よって，解と係数

の関係より $\tau+\overline{\tau}=-b/a$, $\tau\overline{\tau}=c/a$ に注意すると，

$$\begin{aligned} m =& \frac{N(\beta)}{a} = \frac{1}{a}(s+ta\tau)(s+ta\overline{\tau}) = \frac{1}{a}(s^2+ast(\tau+\overline{\tau})+at^2\tau\overline{\tau}) \\ =& \frac{1}{a}(s^2-bst+act^2) = \frac{1}{a}((av+bt)^2-b(av+bt)t+act^2) \\ =& \frac{1}{a}(a^2v^2+abvt+act^2) = av^2+bvt+ct^2 = Q(v,t) \end{aligned}$$

が成り立つため，$m \in R(Q)$ となる．□

命題 6.8 (ii) により，負の基本判別式をもつ原始的 2 次形式 Q が正の整数 m を表現するための必要十分条件を，系 6.11(ii) として求めることができる．この系 6.11 は主定理 2 の証明に必要である．

補題 6.9 ([1, Proposition 5.16]). 素数 p に対し，$\mathcal{O}_K$ のイデアル $p\mathcal{O}_K$ は以下のように素イデアル分解される．

(i) $\left(\frac{d_K}{p}\right)=0$ のとき，$p\mathcal{O}_K=\mathfrak{p}^2$ が成り立つ．ここで，$\mathfrak{p}$ は $\mathcal{O}_K$ の素イデアルであり，$N(\mathfrak{p})=p$ となる．
(ii) $\left(\frac{d_K}{p}\right)=1$ のとき，$p\mathcal{O}_K=\mathfrak{p}\overline{\mathfrak{p}}$ が成り立つ．ここで，$\mathfrak{p}, \overline{\mathfrak{p}}$ は異なる $\mathcal{O}_K$ の素イデアルであり，$N(\mathfrak{p})=N(\overline{\mathfrak{p}})=p$ となる．
(iii) $\left(\frac{d_K}{p}\right)=-1$ のとき，$p\mathcal{O}_K$ は素イデアルであり，$N(p\mathcal{O}_K)=p^2$ となる．

証明 証明は本論文の主旨から外れるため，省略する．□

命題 6.10 ([2, Theorem 2.4]). $\mathfrak{a}$ を $\mathcal{O}_K$ のイデアル，m を正の整数とする．いま，m を $m=p_1\cdots p_r\cdot q_1^{e_1}\cdots q_s^{e_s}$ と表す．ただし，$p_1,\cdots,p_r, q_1,\cdots,q_s$ は素数であり，$q_1,\cdots,q_s$ は全て異なるものとする．また，$1\leq i\leq r$ となる i に対し $\left(\frac{d_K}{p_i}\right)=0,1$ が，$1\leq j\leq s$ となる j に対し $\left(\frac{d_K}{q_j}\right)=-1$ が成り立つものとする．このとき，次の 2 つの命題は同値である．

(i) $N(\mathfrak{a})=m$,
(ii) 各 e_j が偶数であり，かつ各 i に対し $N(\mathfrak{p}_i)=p_i$ となる $\mathcal{O}_K$ のイデアル $\mathfrak{p}_i$ が存在し，$\mathfrak{a}=\mathfrak{p}_1\cdots\mathfrak{p}_r\cdot(q_1\mathcal{O}_K)^{\frac{e_1}{2}}\cdots(q_s\mathcal{O}_K)^{\frac{e_s}{2}}$ が成り立つ．

証明 (i) を仮定すれば (ii) が成り立つことを示す．補題 6.9 より，Dedekind 環 $\mathcal{O}_K$ のイデアル $\mathfrak{a}$ は，$\mathfrak{a}=\mathfrak{p}_1\cdots\mathfrak{p}_r\cdot(q_1\mathcal{O}_K)^{f_1}\cdots(q_s\mathcal{O}_K)^{f_s}$ と素イデアル分解できる．ただし，$1\leq i\leq r$ となる i と $1\leq j\leq s$ となる j に対し，$N(\mathfrak{p}_i)=p_i$, $f_j>0$ である．よって，

$$p_1\cdots p_r\cdot q_1^{e_1}\cdots q_s^{e_s}=m=N(\mathfrak{a})=N(\mathfrak{p}_1)\cdots N(\mathfrak{p}_r)\cdot N(q_1\mathcal{O}_K)^{f_1}\cdots N(q_s\mathcal{O}_K)^{f_s}=p_1\cdots p_r\cdot q_1^{2f_1}\cdots q_s^{2f_s}$$

ゆえ $e_j=2f_j$ となり，各 e_j は偶数となる．逆は明らかに成り立つ．□

系 6.11 $D\equiv 0,1 \pmod 4$ となる基本である負の整数 D に対し，$Q\in F'(D)$ をとる．いま，正の整数 m を $m=p_1\cdots p_r\cdot q_1^{e_1}\cdots q_s^{e_s}$ と表す．ただし，$p_1,\cdots,p_r, q_1,\cdots,q_s$ は素数であり，$q_1,\cdots,q_s$ は全て異なるものとする．また，$1\leq i\leq r$ となる i に対し $\left(\frac{D}{p_i}\right)=0,1$ が，$1\leq j\leq s$ となる j に対し $\left(\frac{D}{q_j}\right)=-1$ が成り立つものとする．このとき，次の 2 つの命題は同値である．

(i) $m\in R(Q)$,

(ii) 各 e_j が偶数であり，かつ各 i に対し $p_i \in R(Q_i)$ となる $Q_i \in F'(D)$ が存在し，$Q \sim Q_1 \circ \cdots \circ Q_r$ が成り立つ．

証明 [2, Theorem 2.1] で $f = 1$ とした場合そのものだが，証明を述べておく．まず，(i) を仮定すれば (ii) が成り立つことを示す．$K = \mathbf{Q}(\sqrt{D})$ に対し d_K を K の判別式とすると，D が基本であるから $d_K = D$ となる．命題 6.8 (iii) より，Q に対応する固有イデアルと同じ類に含まれる固有イデアル $\mathfrak{a}$ で $m = N(\mathfrak{a})$ を満たすものがとれ，それに命題 6.10 を適用すれば，各 e_j が偶数であり，かつ各 i に対し $N(\mathfrak{p}_i) = p_i$ なる $\mathcal{O}_K$ のイデアル $\mathfrak{p}_i$ が存在し，$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot (q_1\mathcal{O}_K)^{\frac{e_1}{2}} \cdots (q_s\mathcal{O}_K)^{\frac{e_s}{2}}$ が成立する．このとき，$q_1\mathcal{O}_K, \cdots, q_s\mathcal{O}_K \in P(\mathcal{O}_K)$ であるから，$C(\mathcal{O}_K)$ の元として，$[\mathfrak{a}] = [\mathfrak{p}_1] \cdots [\mathfrak{p}_r]$ となる．命題 6.8 (ii) より，各 $\mathfrak{p}_i$ に対応する $Q_i \in F'(D)$ をとれば，$p_i \in R(Q_i)$ であり，$Q \sim Q_1 \circ \cdots \circ Q_r$ が成り立つ．

次に，(ii) を仮定すれば (i) が成り立つことを示す．各 i に対し $p_i \in R(Q_i)$ であるから，命題 4.1 より $p_1 \cdots p_r \in R(Q_1 \circ \cdots \circ Q_r) = R(Q)$ が成り立つ．よって，$Q(x, y) = p_1 \cdots p_r$ となる整数 x, y がとれ，各 e_j が偶数であることに注意して，$Q({q_1}^{\frac{e_1}{2}} \cdots {q_s}^{\frac{e_s}{2}} x, {q_1}^{\frac{e_1}{2}} \cdots {q_s}^{\frac{e_s}{2}} y) = p_1 \cdots p_r \cdot {q_1}^{e_1} \cdots {q_s}^{e_s} = m$ より，$m \in R(Q)$ が成り立つ． □

注意 6.12 命題 6.10 と系 6.11 の仮定において，q_j が相異なるのに対し，p_i は重複を許している．この仮定で，p_i, q_j を全て相異なる素数として, $m = p_1^{e_1} \ldots p_r^{e_r} q_1^{e_{r+1}} \ldots q_s^{e_{r+s}}$ と表記しても良いのだが，ここでは [2] の表記に従った．

以下，本節では，K を虚 2 次体，$\mathcal{O}$ を K の整環，$f = |\mathcal{O}_K/\mathcal{O}|$ を $\mathcal{O}$ のコンダクター，D を $\mathcal{O}$ の判別式，$\widetilde{D}$ を K の判別式とする．このとき，定義 6.2 (2) より $D = f^2 d_K$ であるから，$f = \sqrt{D/d_K} = \sqrt{D/\widetilde{D}}$ が成り立つ．

命題 6.13 ([2, Proposition 5.1]). $\mathcal{O}$ のイデアル $\mathfrak{a}, \mathfrak{b}$ に対し，$(\mathfrak{ab})\mathcal{O}_K = (\mathfrak{a}\mathcal{O}_K)(\mathfrak{b}\mathcal{O}_K)$ が成り立つ．

証明 整環の定義から直ちに従う． □

命題 6.14 ([2, Proposition 5.2, 5.3]). $\mathcal{O}$ の固有イデアル $\mathfrak{a}$ に対し，次の 2 つの命題が成り立つ．

(i) $\mathfrak{a}\mathcal{O}_K$ は $\mathcal{O}_K$ の固有イデアルである,
(ii) $N(\mathfrak{a}) = N(\mathfrak{a}\mathcal{O}_K)$.

証明 (i) を示す．命題 6.7 より，

$$(\mathfrak{a}\mathcal{O}_K)(\overline{\mathfrak{a}\mathcal{O}_K}) = (\mathfrak{a}\overline{\mathfrak{a}})\mathcal{O}_K = (N(\mathfrak{a})\mathcal{O})\mathcal{O}_K = N(\mathfrak{a})\mathcal{O}_K$$

であるから，$(\mathfrak{a}\mathcal{O}_K) \cdot \frac{1}{N(\mathfrak{a})}(\overline{\mathfrak{a}\mathcal{O}_K}) = \mathcal{O}_K$ より $\mathfrak{a}\mathcal{O}_K$ は $\mathcal{O}_K$ の可逆イデアルであり，命題 6.6 により固有である．
(ii) を示す．命題 6.7 より，

$$N(\mathfrak{a}\mathcal{O}_K)\mathcal{O}_K = (\mathfrak{a}\mathcal{O}_K)(\overline{\mathfrak{a}\mathcal{O}_K}) = (\mathfrak{a}\overline{\mathfrak{a}})\mathcal{O}_K = (N(\mathfrak{a})\mathcal{O})\mathcal{O}_K = N(\mathfrak{a})\mathcal{O}_K$$

であるから，$N(\mathfrak{a}) = N(\mathfrak{a}\mathcal{O}_K)$ となる． □

命題 6.15 ([2, Proposition 5.4, Lemma 5.5]). f と互いに素な $\mathcal{O}_K$ のイデアル $\mathfrak{a}$ に対し，次の 2 つの命題が成り立つ．

(i) $N(\mathfrak{a} \cap \mathcal{O}) = N(\mathfrak{a})$ であり，$\mathfrak{a} \cap \mathcal{O}$ は f と互いに素なイデアルである．

(ii) $(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K=\mathfrak{a}$.

証明 (i) を示す．自然な単射 $\phi\colon \mathcal{O}/\mathfrak{a}\cap\mathcal{O}\hookrightarrow\mathcal{O}_K/\mathfrak{a}$，$f$ 倍写像 $\psi\colon \mathcal{O}_K/\mathfrak{a}\to\mathcal{O}_K/\mathfrak{a}$ を考える．2 つの写像 ϕ,ψ を満たすいくつかの性質を述べる．まず，有限アーベル群の基本定理と $\gcd(f,N(\mathfrak{a}))=1$ より，ψ は同型である．次に，$f\mathcal{O}_K\subset\mathcal{O}$ ゆえ，$x\in\mathcal{O}_K$ に対し $fx\in\mathcal{O}$ であり，$\psi^{-1}\circ\phi(fx+\mathfrak{a}\cap\mathcal{O})=\psi^{-1}(fx+\mathfrak{a})=x+\mathfrak{a}$ が成り立つため，$\psi^{-1}\circ\phi$ は全射である．最後に，$\psi^{-1}\circ\phi$ が全射かつ ψ^{-1} が単射ゆえ，ϕ は全射となり，写像 ϕ が同型であることが分かった．よって，$N(\mathfrak{a}\cap\mathcal{O})=|\mathcal{O}/\mathfrak{a}\cap\mathcal{O}|=|\mathcal{O}/\mathfrak{a}|=N(\mathfrak{a})$ となり，$\gcd(f,N(\mathfrak{a}\cap\mathcal{O}))=1$ から $\mathfrak{a}\cap\mathcal{O}$ は $\mathcal{O}$ の f と互いに素なイデアルである．

(ii) を示す．$\mathfrak{a}\cap\mathcal{O}$ は $\mathcal{O}$ の f と互いに素なイデアルであるから，$\mathfrak{a}\cap\mathcal{O}+f\mathcal{O}=\mathcal{O}$ が成り立つ．よって，

$$\mathfrak{a}=\mathfrak{a}\mathcal{O}=\mathfrak{a}(\mathfrak{a}\cap\mathcal{O}+f\mathcal{O})=\mathfrak{a}(\mathfrak{a}\cap\mathcal{O})+f\mathfrak{a}\mathcal{O}\subset\mathcal{O}_K(\mathfrak{a}\cap\mathcal{O})+f\mathfrak{a}\mathcal{O}=(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K+f\mathfrak{a}$$

が成り立つ．さらに，$f\mathfrak{a}\subset f\mathcal{O}_K\subset\mathcal{O}$ より，

$$f\mathfrak{a}=\mathfrak{a}\cap f\mathfrak{a}\subset\mathfrak{a}\cap\mathcal{O}\subset(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K$$

となる．したがって，

$$\mathfrak{a}\subset(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K+(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K=(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K$$

より $(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K\supset\mathfrak{a}$ が成り立つ．一方，この逆の包含は明らかに成り立つ． □

命題 6.16 ([1, Corollary 8.6]). 正の整数 N に対し，$C(\mathcal{O})$ の各類は N と互いに素な固有イデアルを含む．

証明 $\mathcal{O}$ の判別式 D に対し，補題 3.3 より，任意の $Q\in F'(D)$ は N と互いに素である整数を表現することが分かる．このとき，命題 6.8 の (ii) と (iii) より，$C(\mathcal{O})$ の各類は N と互いに素な固有イデアルを含む． □

命題 6.17 ([2, Proposition 8.2]). 写像 $\rho\colon C(\mathcal{O})\to C(\mathcal{O}_K),\ [\mathfrak{a}]\mapsto[\mathfrak{a}\mathcal{O}_K]$ は全射準同型である．

証明 命題 6.16 より，$C(\mathcal{O}_K)$ の各類について f と互いに素な固有イデアルがとれ，さらに K の元をかけることにより f と互いに素な $\mathcal{O}_K$ のイデアル $\mathfrak{a}$ がとれる．すると，命題 6.15 (ii) より，$(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K=\mathfrak{a}$ であるから，写像 ρ により $[\mathfrak{a}\cap\mathcal{O}]\in C(\mathcal{O})$ は $[\mathfrak{a}]\in C(\mathcal{O}_K)$ に対応し，全射性がいえる．また，ρ が準同型であることは明らかである． □

命題 6.17 の全射準同型 $\rho\colon C(\mathcal{O})\twoheadrightarrow C(\mathcal{O}_K)$ と命題 6.8 (ii) の同型 $C(D)\simeq C(\mathcal{O}),\ C(\widetilde{D})\simeq C(\mathcal{O}_K)$ を合わせると，異なる判別式に対する原始的 2 次形式の同値類全体がなす群の間の全射準同型

$$\pi\colon C(D)\simeq C(\mathcal{O})\twoheadrightarrow C(\mathcal{O}_K)\simeq C(\widetilde{D}) \tag{6.1}$$

を得る．

以下では，異なる判別式を持つ 2 次形式の表現する整数について，虚 2 次体を用いて議論する．[2] に従って，整環のコンダクターを利用することで整環同士の関係を明確に出来る．命題 6.18 と命題 6.20 は主定理 1, 2 どちらの証明にも本質的に用いられるため，本論文の要である．

命題 6.18 ([2, Proposition 8.4]). $Q\in F'(D),\ \widetilde{Q}\in F'(\widetilde{D})$ に対し，これらの類が (6.1) の準同型によって $\pi\colon [Q]\mapsto[\widetilde{Q}]$ と対応するとき，$m\in R(Q)$ ならば $m\in R(\widetilde{Q})$ である．

証明 $m\in R(Q)$ であるから，命題 6.8 (iii) より，Q に対応する $\mathcal{O}$ の固有イデアルと同じ類に含まれる固有イデアル $\mathfrak{a}$ で，$m=N(\mathfrak{a})$ となるものが存在する．命題 6.16 の準同型 $\rho\colon [\mathfrak{a}]\mapsto[\mathfrak{a}\mathcal{O}_K]$ において，命題 6.14 (ii)

より $N(\mathfrak{a}\mathcal{O}_K) = N(\mathfrak{a}) = m$ であるから，$\widetilde{Q}$ に対応する $\mathcal{O}_K$ の固有イデアルが $\mathfrak{a}\mathcal{O}_K$ と同じ類に含まれることに注意すれば，再び命題 6.8 (iii) より $\widetilde{Q}$ は m を表現する．□

命題 6.19 ([2, Lemma 8.6]). $Q \in F'(D)$, $\widetilde{Q} \in F'(\widetilde{D})$ に対し，これらの類が (6.1) の準同型によって $\pi\colon [Q] \mapsto [\widetilde{Q}]$ と対応するとき，$Q(x,y) = \widetilde{Q}(sx+ty, ux+vy)$ かつ $\det \begin{pmatrix} s & t \\ u & v \end{pmatrix} = \pm f$ となる $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{M}(2, \mathbf{Z})$ が存在する．

証明 補題 3.3 より，$\#(R(Q) \cap \mathbf{P}) = \infty$ であるから，$p \nmid \widetilde{D}$ となる $p \in R(Q) \cap \mathbf{P}$ がとれる．すると，p が素数ゆえ Q は p を原始的に表現するため，補題 3.1 より，Q の類は $[\langle p, b, c\rangle]$ と整数 b, c を用いて表せる．命題 6.18 より，$p \in R'(\widetilde{Q})$ であるから，再び補題 3.1 より，$\widetilde{Q}$ の類は $[\langle p, B, C\rangle]$ と整数 B, C を用いて表せる．命題 6.8 (ii) の同型によって，これらの原始的 2 次形式の類は次のようなイデアル類群の元に対応する：

$$C(D) \ni [\langle p, b, c\rangle] \mapsto [\langle p, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}}] \in C(\mathcal{O}),$$
$$C(\widetilde{D}) \ni [\langle p, B, C\rangle] \mapsto [\langle p, (-B+\sqrt{D})/2\rangle_{\mathbf{Z}}] \in C(\mathcal{O}_K).$$

さらに，命題 6.17 の写像 ρ によって，これらのイデアル類群の元は次のように対応する：

$$C(\mathcal{O}) \ni [\langle p, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}}] \mapsto [\langle p, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}}\mathcal{O}_K] = [\langle p, (-B+\sqrt{D})/2\rangle_{\mathbf{Z}}] \in C(\mathcal{O}_K).$$

ここで，$\mathcal{O}_K$ のイデアルでノルムが素数 p であるものは 2 つしかないため，$\langle p, (-b+\sqrt{D})/2\rangle_{\mathbf{Z}}\mathcal{O}_K = \langle p, \left(-B \pm \sqrt{\widetilde{D}}\right)/2\rangle_{\mathbf{Z}}$ となり，整数 s, t を用いて $(-b+\sqrt{D})/2 = sp + t(-B \pm \sqrt{\widetilde{D}})/2$ と表せる．$D = f^2\widetilde{D}$ ゆえ，$-b + f\sqrt{\widetilde{D}} = 2sp - tB \pm t\sqrt{\widetilde{D}}$ となるから，$b = -2sp + tB$ かつ $\pm f = t$ が成り立つ．いま，$Q' = \langle p, b, c\rangle$, $\widetilde{Q}' = \langle p, B, C\rangle$ とおいて，$\widetilde{Q}'(x - sy, ty)$ を計算すると，

$$\begin{aligned}
\widetilde{Q}'(x-sy, ty) =& p(x-sy)^2 + B(x-sy)(ty) + C(ty)^2 \\
=& \begin{pmatrix} x-sy & ty \end{pmatrix} \begin{pmatrix} p & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x-sy \\ ty \end{pmatrix} \\
=& \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -s & t \end{pmatrix} \begin{pmatrix} p & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} 1 & -s \\ 0 & t \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
=& \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & -sp + t(B/2) \\ -sp + t(B/2) & ps^2 - Bst + Ct^2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
=& px^2 + (-2sp + tB)xy + (ps^2 - Bst + Ct^2)y^2 \\
=& px^2 + bxy + (ps^2 - Bst + Ct^2)y^2
\end{aligned}$$

となる．この最右辺の 2 次形式 $px^2 + bxy + (ps^2 - Bst + Ct^2)y^2$ の判別式は，

$$-4 \cdot \det\left\{ \begin{pmatrix} 1 & 0 \\ -s & t \end{pmatrix} \begin{pmatrix} p & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} 1 & -s \\ 0 & t \end{pmatrix} \right\} = t^2(B^2 - 4pC) = f^2\widetilde{D} = D$$

であり，Q' の判別式も D ゆえ，$\widetilde{Q}'(x-sy, ty) = Q'(x, y)$ が成り立つ．また，$\begin{pmatrix} 1 & -s \\ 0 & t \end{pmatrix} = t = \pm f$ である．

以上より，これらと $Q \sim Q'$, $\widetilde{Q} \sim \widetilde{Q}'$ であることを合わせれば，命題の主張が示される．□

命題 6.20 ([2, Proposition 8.7]). $Q \in F'(D)$, $\widetilde{Q} \in F'(\widetilde{D})$ に対し，これらの類が (6.1) の準同型によって $\pi\colon [Q] \mapsto [\widetilde{Q}]$ と対応するとき，$m \in R(\widetilde{Q})$ ならば $f^2 m \in R(Q)$ である．

証明 命題 6.19 より，$Q(x,y)=\widetilde{Q}(sx+ty,ux+vy)$ かつ $\det\begin{pmatrix}s & t\\ u & v\end{pmatrix}=\pm f$ となる $\begin{pmatrix}s & t\\ u & v\end{pmatrix}\in \mathrm{M}(2,\mathbf{Z})$ をとれば，$Q(vx-ty,-ux+sy)=\widetilde{Q}(\pm fx,\pm fy)=f^2\widetilde{Q}(x,y)$ であるから，m が整数 p,q によって $m=\widetilde{Q}(p,q)$ と表されるものとすれば，$f^2m=Q(vp-tq,-up+sq)$ となる． □

7 問題 3 の解答

本節では，問題 3 の解答，すなわち $D\equiv 0,1 \pmod 4$ である負の整数 D に対し，D を判別式にもつ原始的 2 次形式全てが同時に表現する正の整数が存在するか否かについての判定法を与える．

補題 7.1 $D\equiv 0,1 \pmod 4$ である負の整数 D に対し，$\widetilde{D}$ が基本判別式かつ $D/\widetilde{D}$ が平方数となるような整数 $\widetilde{D}$ がただ一つ存在する．

証明 $D\equiv 0,1 \pmod 4$ である負の整数 D に対し，虚 2 次体 $\mathbf{Q}(\sqrt{D})$ の判別式を $\widetilde{D}$ といたとき，$\widetilde{D}$ は基本判別式であり，判別式の定義から $D/\widetilde{D}$ は明らかに平方数となる．以上により，条件を満たす $\widetilde{D}$ は存在する．一意性は，基本判別式の定義から明らかに成り立つ． □

以下では，$D\equiv 0,1 \pmod 4$ である負の整数 D に対し，$\widetilde{D}$ を補題 7.1 によって定まる $\widetilde{D}$ とする．また，本節と第 8 節において，$f=\sqrt{D/\widetilde{D}}$ とおく．なお，$\widetilde{D}$ は第 6 節にも現れているが，その対応を述べておく．$D\equiv 0,1 \pmod 4$ である負の整数 D に対し，命題 6.3 より，判別式が D となる虚 2 次体 K の整環 $\mathcal{O}$ がただ一つ存在する．このとき，K の整数環を $\mathcal{O}_K$，判別式を d_K とすると，$\mathcal{O}$ のコンダクターは f となり，$D=f^2d_K$ が成り立つ．d_K は基本判別式かつ $D/d_K=f^2$ が平方数となることから，d_K が $\widetilde{D}$ に他ならない．

命題 7.2 $D\equiv 0,1 \pmod 4$ である負の整数 D に対し，$h(D)$ が奇数ならば，$h(\widetilde{D})$ も奇数である．

証明 (6.1) の全射準同型 $\pi\colon C(D)\twoheadrightarrow C(\widetilde{D})$ を考えれば，$h(\widetilde{D})$ は $h(D)$ を割り切ることが分かるので, 命題の主張が成り立つ． □

定理 7.3 (主定理 1) $D\equiv 0,1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) $\displaystyle\bigcap_{Q\in F'(D)} R(Q)\neq\emptyset$,
(ii) $h(\widetilde{D})$ が奇数である．

証明 $h(D)$ が奇数のとき，命題 4.2 より (i) が成り立ち，命題 7.2 より，(ii) も成り立っているので，定理の主張は正しい．以下，$h(D)$ が偶数のときを考える．

D が基本判別式であれば，命題 5.4 から (ii) は成り立たない．

D が基本判別式でなく，かつ $h(\widetilde{D})$ が奇数であれば，命題 4.2 より集合 $\displaystyle\bigcap_{Q\in F'(\widetilde{D})} R(Q)$ に属す整数 m をとることができる．任意の $Q\in F'(D)$ に対し，(6.1) の準同型により $\pi\colon [Q]\mapsto[\widetilde{Q}]$ となる $\widetilde{Q}\in F'(D)$ をとると，$m\in\displaystyle\bigcap_{Q\in F'(\widetilde{D})} R(Q)\subset R(\widetilde{Q})$ に注意すれば，命題 6.20 より，$f^2m\in R(Q)$ が成立する．よって，(i) の左辺の集合に属す整数として f^2m がとれるため，(i) が成立する．

D が基本判別式でなく，かつ $h(\widetilde{D})$ が偶数であれば，命題 5.4 から $\displaystyle\bigcap_{Q\in F'(\widetilde{D})} R(Q)=\emptyset$ となる．このとき，

任意の正の整数 m に対し，$m \notin R(\widetilde{Q})$ となる $\widetilde{Q} \in F'(\widetilde{D})$ がとれる．(6.1) の準同型 $\pi\colon C(D) \twoheadrightarrow C(\widetilde{D})$ が全射ゆえ $\pi\colon [Q] \mapsto [\widetilde{Q}]$ となる $Q \in F'(D)$ をとれば，命題 6.18 の対偶より $m \notin R(Q)$ となるので，(ii) は成り立たない．

以上により，(ii) から (i) が従うことと，その対偶が示されたので，定理の主張が成り立つ． □

系 7.4 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) $\displaystyle\bigcap_{Q \in F'(D)} R(Q) \neq \emptyset$,

(ii) $D = -2^h \cdot p^e \cdot {q_1}^{e_1} \cdots {q_s}^{e_s}$ とかける．ただし，$p, q_1, \cdots, q_s$ は全て異なる奇素数で $p \equiv 3 \pmod 4$ を満たし，さらに，$h, e_1, \cdots, e_s \geq 0$ は偶数，$e \geq 0$ は奇数とする．

系 7.4 により，$D \equiv 0, 1 \pmod 4$ である負の整数 D が与えられたとき，D を素因数分解して形を調べることで，D を判別式にもつ原始的 2 次形式全てが同時に表現する正の整数が存在するか否かを判定することができる．

例 7.5 (主定理 1 の具体例)

(1) $D = -207$ のとき，$h(D) = 6$ であり，これは偶数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 1, 52\rangle, Q_2 = \langle 2, 1, 26\rangle, Q_3 = \langle 2, -1, 26\rangle, Q_4 = \langle 4, 1, 13\rangle, Q_5 = \langle 4, -1, 13\rangle, Q_6 = \langle 8, 7, 8\rangle\}$ である．一方，$\widetilde{D} = -23$, $f = 3$ で $h(\widetilde{D}) = 3$ は奇数である．すると，例 4.4 (1) と定理 7.3 の証明より $3^2 \cdot 6 = 54 \in \displaystyle\bigcap_{Q \in F'(D)} R(Q)$ となるはずだが，$54 = Q_1(1, 1) = Q_2(4, -1) = Q_3(4, 1) = Q_4(1, -2) = Q_5(1, 2) = Q_6(1, 2)$ より，これは実際に成立する．

(2) $D = -216$ のとき，$h(D) = 6$ であり，これは偶数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 0, 54\rangle, Q_2 = \langle 2, 0, 27\rangle, Q_3 = \langle 5, 2, 11\rangle, Q_4 = \langle 5, -2, 11\rangle, Q_5 = \langle 7, 6, 9\rangle, Q_6 = \langle 7, -6, 9\rangle\}$ である．一方，$\widetilde{D} = -24$, $f = 3$ で $h(\widetilde{D}) = 2$ は偶数であり，定理 7.3 より $\displaystyle\bigcap_{Q \in F'(D)} R(Q) = \emptyset$ が成立する．

8 問題 4 の解答

本節では，問題 4 の解答，すなわち $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，D を判別式にもつ 2 次形式全てが同時に表現する正の整数が存在するか否かについての判定法を与える．

補題 8.1 $D \equiv 0, 1 \pmod 4$ である負の整数 D が $\displaystyle\bigcap_{Q \in F'(D)} R(Q) \neq \emptyset$ を満たすとき，$d \in \displaystyle\bigcup_{Q \in F'(D)} R(Q)$, $m \in \displaystyle\bigcap_{Q \in F'(D)} R(Q)$ に対し，$dm \in \displaystyle\bigcap_{Q \in F'(D)} R(Q)$ が成立する．

証明 $d \in \displaystyle\bigcup_{Q \in F'(D)} R(Q)$ より，$d \in R(Q')$ を満たす $Q' \in F'(D)$ をとることができる．任意の $Q \in F'(D)$ に対し，$[Q''] = [Q']^{-1} \cdot [Q]$ を満たす $Q'' \in F'(D)$ をとれば，$m \in \displaystyle\bigcap_{Q \in F'(D)} R(Q) \subset R(Q'')$ に注意して，命題 4.1 より，$dm \in R(Q' \circ Q'') = R(Q)$ を得るので，$dm \in \displaystyle\bigcap_{Q \in F'(D)} R(Q)$ となる． □

定理 8.2 (主定理 2) $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) $\bigcap_{Q\in F(D)} R(Q)\neq\emptyset$,

(ii) $h(\widetilde{D})$ が奇数であり，かつ $D/\widetilde{D}$ の各素因子が $\bigcup_{Q\in F'(\widetilde{D})} R(Q)$ の元である．

証明 まず，(ii) が成り立つならば (i) が成り立つことを示す．$h(\widetilde{D})$ が奇数であるから，命題 4.2 より $m\in\bigcap_{Q\in F'(\widetilde{D})} R(Q)$ がとれる．このとき，定理 7.3 の証明より，$f^2m\in\bigcap_{Q\in F'(D)} R(Q)$ であるから，任意の $Q'\in F(D)\setminus F'(D)$ に対して $f^2m\in R(Q')$ をいえば，$f^2m\in\bigcap_{Q\in F(D)} R(Q)$，特に (i) が成立する．この $Q'=\langle a,b,c\rangle$ は原始的ではないから，$d=\gcd(a,b,c)>1$ である．$D'=D/d^2$ とおけば，$Q''=\langle a/d,b/d,c/d\rangle\in F'(D')$ となる．d の各素因子は $\bigcup_{Q\in F'(\widetilde{D})} R(Q)$ の元であり，しかも $m\in\bigcap_{Q\in F'(\widetilde{D})} R(Q)$ であるから，補題 8.1 を繰り返し用いることにより，$dm\in\bigcap_{Q\in F'(\widetilde{D})} R(Q)$ であることが分かる．したがって，再び定理 7.3 の証明より，$\frac{D'}{\widetilde{D}}\cdot dm\in\bigcap_{Q\in F'(D')} R(Q)\subset R(Q'')$ となる．$dQ'(x,y)=Q''(x,y)$ に注意すれば，$f^2m=\frac{D}{\widetilde{D}}m=d\cdot\frac{D'}{\widetilde{D}}\cdot dm\in R(Q')$ も成立する．

次に，(i) が成り立つならば (ii) が成り立つ，という命題の対偶を示す．$h(\widetilde{D})$ が偶数であるなら，定理 7.3 より $\bigcap_{Q\in F'(D)} R(Q)=\emptyset$ となるから，包含関係 $F'(D)\subset F(D)$ に注意すれば，(i) が成り立たないことが分かる．以下，$h(\widetilde{D})$ が奇数であり，かつ $p\mid f$ を満たす $p\in\mathbf{P}\setminus\bigcup_{Q\in F'(\widetilde{D})} R(Q)$ がとれたとする．いま，(i) が成り立つと仮定して矛盾を導く．$m\in\bigcap_{Q\in F(D)} R(Q)$ をとると，再び包含関係 $F'(D)\subset F(D)$ に注意すれば，$m\in\bigcap_{Q\in F'(D)} R(Q)$ であり，命題 6.18 と (6.1) の写像 π の全射性より，$m\in\bigcap_{Q\in F'(\widetilde{D})} R(Q)$ が成立する．$D'=D/p^2$ とおけば，定理 7.3 の証明より $\frac{D'}{\widetilde{D}}\cdot m=\frac{D}{p^2}\cdot\frac{f^2}{\widetilde{D}}\cdot m=\frac{f^2m^2}{p^2}\in\bigcap_{Q\in F'(D')} R(Q)$ となるから，再び命題 6.18 と (6.1) の写像 π の全射性より，$\frac{f^2m^2}{p^2}\in\bigcap_{Q\in F'(\widetilde{D})} R(Q)$ が成立する．これと $p\in\mathbf{P}\setminus\bigcup_{Q\in F'(\widetilde{D})} R(Q)$ によって，系 6.11 を用いれば $\frac{f^2m^2}{p^2}\cdot p=\frac{f^2m^2}{p}\notin\bigcup_{Q\in F'(\widetilde{D})} R(Q)$ が分かる．すると，命題 6.18 の対偶から $\frac{f^2m^2}{p}\notin\bigcup_{Q\in F'(D')} R(Q)$ である．したがって，任意に $Q\in F'(D')$ をとれば，$\bigcup_{Q\in F'(D')} R(Q)\subset R(Q)$ より $\frac{f^2m^2}{p}\notin R(Q)$ であり，$Q=\langle a,b,c\rangle$ に対し $pQ=\langle pa,pb,pc\rangle$ とかけば，$p\cdot\frac{f^2m^2}{p}=f^2m\notin R(pQ)$ となる．しかしながら，一方で $pQ\in F(D)$ より，$m\in R(pQ)$ となるが，このとき，$f^2\cdot pQ(x,y)=pQ(fx,fy)$ に注意すれば，$f^2m\in R(pQ)$ も成立するため，矛盾が生ずる． □

系 8.3 $D\equiv 0,1\pmod 4$ である負の整数 D に対し，次の 2 つの命題は同値である．

(i) $\bigcap_{Q\in F(D)} R(Q)\neq\emptyset$,

(ii) $D=-2^h\cdot p^e\cdot {q_1}^{e_1}\cdots {q_s}^{e_s}$ とかける．ただし，$p,q_1,\cdots,q_s$ は全て異なる奇素数で，$p\equiv 3\pmod 4$ かつ $q_i\in\bigcup_{Q\in F'(\widetilde{D})} R(Q)\,(1\leq i\leq s)$ を満たし，さらに，$h,e_1,\cdots,e_s\geq 0$ は偶数，$e\geq 0$ は奇数とする．

次の命題 8.4 は，第 1 節で述べた定理 1.2 を第 2 節の記法で書き直したものである．これは以下の注意 8.5 を述べる際に必要となるため，証明を追記した上で再掲する．

命題 8.4 ([1, Theorem 2.16])．$D \equiv 0, 1 \pmod 4$ である負の整数 D と D を割り切らない奇素数 p に対し，次の 2 つの命題は同値である．

(i) $p \in \bigcup_{Q \in F'(D)} R(Q)$,
(ii) $\left(\frac{D}{p}\right) = 1$.

証明 まず, (i) から (ii) が従うことを示す．$p \in R(Q)$ となる $Q \in F'(D)$ をとる．p が素数ゆえ, p の Q による表現は原始的であるから，補題 3.1 より $Q \sim \langle p, b, c\rangle$ となる整数 b, c がとれる．このとき，$D = b^2 - 4pc \equiv b^2 \pmod p$ であるから，$\left(\frac{D}{p}\right) = 1$ が成り立つ．

次に，(ii) から (i) が従うことを示す．$\left(\frac{D}{p}\right) = 1$ とすると，$D \equiv b^2 \pmod p$ となる整数 b がとれる．p が奇数であるから，必要ならば b を $b + p$ と取り替えることにより，$D \equiv b^2 \pmod{4p}$ とできる．このとき，$D = b^2 - 4pc$ となる整数 c がとれ，$p \nmid D$ ゆえ $Q = \langle p, b, c\rangle$ に対し $Q \in F'(D)$ であり，$p = Q(1, 0)$ より $p \in R(Q)$ が成り立つ． □

注意 8.5 命題 8.4 により，定理 8.2 (ii) は，$\widetilde{D}$ の値で場合分けすることにより，以下のように書き換えられる：

(I) $\widetilde{D} = -4$ のとき，$D/\widetilde{D}$ の各素因子 p が $p = 2$ または $p \equiv 1 \pmod 4$ を満たす．
(II) $\widetilde{D} = -8$ のとき，$D/\widetilde{D}$ の各素因子 p が $p = 2$ または $p \equiv 1, 3 \pmod 8$ を満たす．
(III) $\widetilde{D} = -q$ (q は素数) のとき，$D/\widetilde{D}$ の各素因子 p が $p = q$ または $\left(\frac{p}{q}\right) = 1$ を満たす．

系 8.3 と注意 8.5 により，$D \equiv 0, 1 \pmod 4$ である負の整数 D が与えられたとき，D を素因数分解して形を調べることで，D を判別式にもつ 2 次形式全てが同時に表現する正の整数が存在するか否かを判定することができる．

例 8.6 (主定理 2 の具体例)

(1) $D = -207$ のとき，$\widetilde{D} = -23$, $f = 3$ であり，$h(\widetilde{D}) = 3$ は奇数である．また，$F_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 1, 52\rangle, Q_2 = \langle 2, 1, 26\rangle, Q_3 = \langle 2, -1, 26\rangle, Q_4 = \langle 4, 1, 13\rangle, Q_5 = \langle 4, -1, 13\rangle, Q_6 = \langle 8, 7, 8\rangle, Q_7 = \langle 3, 3, 18\rangle, Q_8 = \langle 6, 3, 9\rangle, Q_9 = \langle 6, -3, 9\rangle\}$，$F'_{\mathrm{red}}(\widetilde{D}) = \{\widetilde{Q}_1 = \langle 1, 1, 6\rangle, \widetilde{Q}_2 = \langle 2, 1, 3\rangle, \widetilde{Q}_3 = \langle 2, -1, 3\rangle\}$ である．一方，$D/\widetilde{D} = 9$ の素因子は 3 のみであり，$3 = \widetilde{Q}_2(0, 1)$ より $3 \in R(\widetilde{Q}_2) \subset \bigcup_{Q \in F'(\widetilde{D})} R(Q)$ となる．よって，例 4.4 (1) と定理 8.2 の証明より $3^2 \cdot 6 = 54 \in \bigcap_{Q \in F'(D)} R(Q)$ となるはずだが，$54 = Q_1(1, 1) = Q_2(4, -1) = Q_3(4, 1) = Q_4(1, -2) = Q_5(1, 2) = Q_6(1, 2) = Q_7(3, 1) = Q_8(3, 0) = Q_9(3, 0)$ より，これは実際に成立する．

(2) $D = -20700 = -2^2 \cdot 3^2 \cdot 5^2 \cdot 23$ のとき，$\widetilde{D} = -23$, $f = 30$ であり，$h(\widetilde{D}) = 3$ は奇数である．このとき，$D/\widetilde{D} = 900$ の素因子は $2, 3, 5$ だが, $5 \neq 23$ かつ $\left(\frac{5}{23}\right) = -1$ であるから，注意 8.5 より $5 \notin \bigcup_{Q \in F'(\widetilde{D})} R(Q)$ となる．よって，定理 8.2 より $\bigcap_{Q \in F(D)} R(Q) = \emptyset$ が成立する．

9　問題 5 の部分的な解答

本節では，問題 5 の部分的な解答として，$D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，D を判別式にもつ 2 次形式全てが同時に表現する正の整数が存在するならば，D を判別式にもつ原始的 2 次形式全てが同時に原始的に表現する正の整数が存在することを示す．

まず，類数 $h(D)$ が奇数となるような D に対し，問題 5 を考える．命題 9.3 では，$\bigcap_{Q \in F'(D)} R'(Q) \neq \emptyset$ であることを，$\bigcap_{Q \in F'(D)} R'(Q)$ の具体的な元を求めることで証明している．これから述べる命題 9.1，補題 9.2，および命題 9.3 は，それぞれ命題 4.1，補題 8.1，および命題 4.2 を原始的な表現で考えたものであり，証明の流れはほとんど同じである．

命題 9.1 $Q_1, Q_2 \in F'(D)$ に対し，$m_1 \in R'(Q_1)$ かつ $m_2 \in R'(Q_2)$ かつ $\gcd(m_1, m_2) = 1$ ならば，$m_1 m_2 \in R'(Q_1 \circ Q_2)$ である．

証明 $m_1 \in R'(Q_1)$ かつ $m_2 \in R'(Q_2)$ より，m_1, m_2 は $\gcd(x_i, y_i) = 1$ を満たす整数 $x_i, y_i \, (i = 1, 2)$ を用いて，$m_1 = Q_1(x_1, y_1)$, $m_2 = Q_2(x_2, y_2)$ と表せる．このとき，補題 3.1 よりある整数 $b_i, c_i \, (i = 1, 2)$ が存在して，$Q_1 \sim \langle m_1, b_1, c_1 \rangle$, $Q_2 \sim \langle m_2, b_2, c_2 \rangle$ とできて，$\gcd(m_1, m_2, \frac{b_1 + b_2}{2}) | \gcd(m_1, m_2)$ かつ $\gcd(m_1, m_2) = 1$ より，$\gcd(m_1, m_2, \frac{b_1 + b_2}{2}) = 1$ となるから，$Q_1 \circ Q_2 \sim \langle m_1, b_1, c_1 \rangle \circ \langle m_2, b_2, c_2 \rangle = \langle m_1 m_2, *, * \rangle$ となる．すると，$m_1 m_2 = Q_3(1, 0)$ より，$m_1 m_2 \in R'(Q_3)$ が成立する． □

補題 9.2 $D \equiv 0, 1 \pmod 4$ である負の整数 D が $\bigcap_{Q \in F'(D)} R'(Q) \neq \emptyset$ を満たすとき，$d \in \bigcup_{Q \in F'(D)} R'(Q)$, $m \in \bigcap_{Q \in F'(D)} R'(Q)$ に対し，$\gcd(d, m) = 1$ ならば，$dm \in \bigcap_{Q \in F'(D)} R'(Q)$ が成立する．

証明 命題 9.1 を用いれば，補題 8.1 とほとんど同様に証明することができる．$d \in \bigcup_{Q \in F'(D)} R'(Q)$ より，$d \in R'(Q')$ となる $Q' \in F'(D)$ をとることができる．任意の $Q \in F'(D)$ に対し，$[Q''] = [Q']^{-1} \cdot [Q]$ を満たす $Q'' \in F'(D)$ をとれば，$m \in \bigcap_{Q \in F'(D)} R'(Q) \subset R'(Q'')$ と $\gcd(d, m) = 1$ に注意して，命題 9.1 より，$dm \in R'(Q' \circ Q'') = R'(Q)$ を得るので，$dm \in \bigcap_{Q \in F'(D)} R'(Q)$ となる． □

命題 9.3 $D \equiv 0, 1 \pmod 4$ である負の整数 D に対し，$h(D)$ が奇数ならば，$\bigcap_{Q \in F'(D)} R'(Q) \neq \emptyset$ が成立する．

証明 $h(D) = 1$ のときは，$F'_{\mathrm{red}}(D) = \{Q\}$ (Q は $F'(D)$ の基本形式) となるから明らかである．以下，正の整数 n を用いて $h(D) = 2n + 1$ と表し，$F'_{\mathrm{red}}(D)$ の元を次のように番号付けする：

$$\begin{cases} Q_1 = \langle 1, b_0, c_0 \rangle : \text{基本形式}, \\ Q_2 = \langle a_1, b_1, c_1 \rangle, \\ Q_3 = \langle a_1, -b_1, c_1 \rangle \in [Q_2]^{-1}, \\ \cdots, \\ Q_{2n} = \langle a_n, b_n, c_n \rangle, \\ Q_{2n+1} = \langle a_n, -b_n, c_n \rangle \in [Q_{2n}]^{-1}. \end{cases}$$

このとき，命題 4.2 の証明と同様に，各 $Q_j\,(2 \leq j \leq 2n+1)$ に対し $[Q_k]^2 = [Q_j]$ となるただ一つの $Q_k \in F'_{\mathrm{red}}(D)\,(2 \leq k \leq 2n+1)$ をとって，

$$Q'_j = \begin{cases} Q_2 \circ Q_3 \circ \cdots \circ Q_{k-1} \circ Q_k \circ Q_k \circ Q_{k+2} \circ \cdots \circ Q_{2n} \circ Q_{2n+1} & (k : \text{奇数}) \\ Q_2 \circ Q_3 \circ \cdots \circ Q_{k-2} \circ Q_k \circ Q_k \circ Q_{k+1} \circ \cdots \circ Q_{2n} \circ Q_{2n+1} & (k : \text{偶数}) \end{cases}$$

とおくと，$Q'_j \sim Q_j$ が成り立つ．ここで，補題 3.3 より，各 $i\,(1 \leq i \leq n)$ に対し $d_{2i-1}, d_{2i} \in R'(Q_{2i})$ を $\gcd(d_{2i-1}, d_{2i}) = 1$ となるようにとることができる．いま，$m = \prod_{l=1}^{2n} d_l$ とおいたとき，命題 9.1 より $m \in R'(Q'_j) = R'(Q_j)\,(2 \leq j \leq 2n+1)$ が成立する．また，命題 4.2 の証明と同様に，$Q'_1 = Q_2 \circ Q_3 \circ \cdots \circ Q_{2n} \circ Q_{2n+1}$ とおけば，$Q'_1 \sim Q_1$ が成り立つから，命題 9.1 より $m \in R'(Q'_1) = R'(Q_1)$ が成立する．以上により，$m \in \bigcap_{Q \in F'(D)} R'(Q)$ がいえたので，$\bigcap_{Q \in F'(D)} R'(Q) \neq \emptyset$ が示された． □

例 9.4 (命題 9.3 の具体例) $D = -31$ のとき $h(D) = 3$ であり，これは奇数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 1, 8 \rangle, Q_2 = \langle 2, 1, 4 \rangle, Q_3 = \langle 2, -1, 4 \rangle\}$ である．このとき，互いに素な 2 つの整数 $2, 5$ について，$2 = Q_2(1, 0)$, $5 = Q_2(-1, 1)$ より $2, 5 \in R'(Q_2)$ であるから，命題 9.3 の証明より $2 \cdot 5 = 10 \in \bigcap_{Q \in F'(D)} R'(Q)$ となるはずだが，$10 = Q_1(1, 1) = Q_2(-2, 1) = Q_3(2, 1)$ よりこれは実際に成立する．

次に，[4, §7] を参考にして，$D \equiv 0, 1 \pmod 4$ である負の整数 D と素数 p に対し，$F'(p^2 D)$ の元と $F'(D)$ の元の関係について議論する．特に補題 9.11 は主定理 3 の証明の要であり，異なる判別式の 2 次形式が表現する整数の関係を明らかにするだけでなく，その表現が原始的か否かを明らかにすることができるという意味で非常に重要である．

以下，本節では，D を $D \equiv 0, 1 \pmod 4$ である負の整数，p を素数とする．また，簡単のため，ここでのみ用いる記号 $\mathrm{M}_p(2, \mathbf{Z})$ を，$\mathrm{M}_p(2, \mathbf{Z}) = \{K \in \mathrm{M}(2, \mathbf{Z}) \mid \det K = p\}$ と定める．

補題 9.5 任意の $Q \in F'(p^2 D)$ に対し，$Q \sim \langle a, bp, cp^2 \rangle$ となる整数 a, b, c が存在する．

証明 補題 3.3 より，$\gcd(a, p) = 1$ となる $a \in R'(Q)$ がとれる．すると，補題 3.1 より $Q \sim \langle a, B, C \rangle$ となる整数 B, C が存在するので，それを $Q' = \langle a, B, C \rangle$ とおく．ここで，$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ に対し $Q''(x, y) = Q'(x + ky, y)$ とおけば，$Q'' \sim Q'$ である．これを $Q'' = \langle a, B', C' \rangle$ とおく．このとき，$B' = B + 2ak$ とかけることに注意する．以下，p の偶奇によって場合分けする．

p が奇数の場合，$\gcd(a, p) = 1$ より $\gcd(-2a, p) = 1$ であるから，$-2ak + pl = B$ となる整数 k, l がとれる．すると，$B' = B + 2ak = pl \equiv 0 \pmod p$ となるから，判別式が $p^2 D = B'^2 - 4aC'$ であることに注目すれば $C' \equiv 0 \pmod{p^2}$ を得る．よって，$b = B'/p, c = C'/p^2$ とすればよい．

p が偶数の場合，判別式が $p^2 D = B'^2 - 4aC'$ であることに注目して B' が偶数となるから，$B' = B + 2ak$

より B も偶数である．$\gcd(a,p)=1$ より $\gcd(-2a,p)=2$ であるから，B が偶数ゆえ $-2ak+pl=B$ となる整数 k,l がとれる．あとは，p が奇数の場合と同様に示すことができる． □

命題 9.6 ([4, Proposition 7.1]). 任意の $Q\in F'(p^2D)$ に対し，$Q={}^tNQ'N$ が成り立つような $Q'\in F'(D)$, $N\in \mathrm{M}_p(2,\mathbf{Z})$ が存在する．ただし，ここでは 2 次形式 Q,Q' を行列と同一視している．

証明 この証明中では，2 次形式を行列と同一視する．$Q\in F(p^2D)$ に対し，$Q\sim\langle a,bp,cp^2\rangle$ となる整数 a,b,c が存在する．このとき，$Q'=\langle a,b,c\rangle$, $Q''=\langle a,bp,cp^2\rangle$ とおいて $Q={}^tMQ''M$ となる $M\in\mathrm{SL}(2,\mathbf{Z})$ をとると，$N=\begin{pmatrix}1&0\\0&p\end{pmatrix}M$ に対し，${}^tNQ'N={}^tM\begin{pmatrix}1&0\\0&p\end{pmatrix}Q'\begin{pmatrix}1&0\\0&p\end{pmatrix}M={}^tNQ''N=Q$ が成り立つ． □

注意 9.7 補題 9.5 と命題 9.6 の主張は，素数 p を任意の正の整数 f としても成り立っている．実際，補題 9.5 と命題 9.6 の証明の中では，p が素数である事実を一切使っていない．したがって，正の整数 f と $Q\in F'(f^2D)$ に対し，$Q(x,y)=Q'(sx+ty,ux+vy)$ かつ $\det\begin{pmatrix}s&t\\u&v\end{pmatrix}=f$ となる $Q'\in F'(D)$ と $\begin{pmatrix}s&t\\u&v\end{pmatrix}\in\mathrm{M}(2,\mathbf{Z})$ が存在する．このとき，命題 6.20 の証明と同様にして，$Q(vx-ty,-ux+sy)=Q'(fx,fy)=f^2Q'(x,y)$ であるから，$m\in R(Q')$ ならば $f^2m\in R(Q)$ となる．この事実より，

$$m\in\bigcap_{Q\in F'(D)}R(Q)\quad\text{ならば，}\quad f^2m\in\bigcap_{Q\in F'(f^2D)}R(Q)$$

が成り立つため，命題 6.20 の代わりにこれを用いて主定理 1 を示すこともできる．

命題 9.8 任意の $K\in\mathrm{M}_p(2,\mathbf{Z})$ に対し，$K=K_hL$ を満たす $0\le h\le p$, $L\in\mathrm{SL}(2,\mathbf{Z})$ が存在する．ただし，$K_h=\begin{pmatrix}p&h\\0&1\end{pmatrix}$ $(0\le h<p)$, $K_p=\begin{pmatrix}1&0\\0&p\end{pmatrix}$ とする．

証明 [4, Proposition 7.2] を参照する．$K=\begin{pmatrix}s&t\\u&v\end{pmatrix}\in\mathrm{M}_p(2,\mathbf{Z})$ をとると，$sv-tu=p$ は素数であるから，$\gcd(u,v)$ は 1 または p である．以下，$\gcd(u,v)$ の値によって場合分けを行う．

$\gcd(u,v)=1$ のとき，$t'u+vv'=1$ となる整数 t',v' をとる．K の右から $\begin{pmatrix}v&t'\\-u&v'\end{pmatrix}\in\mathrm{SL}(2,\mathbf{Z})$ をかけた行列は，

$$\begin{pmatrix}s&t\\u&v\end{pmatrix}\begin{pmatrix}v&t'\\-u&v'\end{pmatrix}=\begin{pmatrix}sv-tu&st'+tv'\\uv-vu&t'u+vv'\end{pmatrix}=\begin{pmatrix}p&pk+h\\0&1\end{pmatrix}$$

のように整数 k と $0\le h<p$ を用いて表せる．さらに右から $\begin{pmatrix}1&-k\\0&1\end{pmatrix}\in\mathrm{SL}(2,\mathbf{Z})$ をかけることにより，

$$\begin{pmatrix}p&pk+h\\0&1\end{pmatrix}\begin{pmatrix}1&-k\\0&1\end{pmatrix}=\begin{pmatrix}p&h\\0&1\end{pmatrix}=K_h$$

を得る．このとき，$L=\begin{pmatrix}1&k\\0&1\end{pmatrix}\begin{pmatrix}v'&-t'\\u&v\end{pmatrix}\in\mathrm{SL}(2,\mathbf{Z})$ とすればよい．

$\gcd(u,v)=p$ のとき，整数 u'',v'' を用いて $u=pu''$, $v=pv''$ と表し，$t'u''+v'v''=1$ となる整数 t',v' を

とる．K の右から $\begin{pmatrix} v'' & t' \\ -u'' & v' \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ をかけた行列は，

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix}\begin{pmatrix} v'' & t' \\ -u'' & v' \end{pmatrix} = \begin{pmatrix} sv''-tu'' & st'+tv' \\ uv''-vu'' & t'u+vv' \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$$

のように整数 k を用いて表せる．さらに右から $\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ をかけて，

$$\begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = K_p$$

を得る．このとき，$L = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} v' & -t' \\ u'' & v'' \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ とすればよい． □

命題 9.9 $D \equiv 0,1 \pmod 4$ である負の整数 D と素数 p に対し，任意の $Q \in F'(p^2D)$ は集合 $\bigcup_{\langle a,b,c\rangle \in F'_{\mathrm{red}}(D)} \{Q_h \mid 0 \le h \le p\}$ のいずれかの元と対等である．ただし，各 $\langle a,b,c\rangle \in F'_{\mathrm{red}}(D)$ に対し，$Q_h = \langle ap^2, (b+2ah)p, (b+ah)h+c\rangle\ (0 \le h < p)$, $Q_p = \langle a, bp, cp^2\rangle$ とする．

証明 [4, Chapter 7] を参照する．この証明中では，2 次形式を行列と同一視する．任意に $Q \in F'(p^2D)$ をとると，命題 9.6 より，$Q = {}^tNQ'N$ を満たす $Q' \in F'(D)$, $N \in \mathrm{M}_p(2,\mathbf{Z})$ がとれる．$Q'' \sim Q'$ となる $Q'' \in F'_{\mathrm{red}}(D)$ をとると，対等の定義より $Q'' = {}^tMQ'M$ を満たす $M \in \mathrm{SL}(2,\mathbf{Z})$ が存在する．このとき，

$$Q = {}^tNQ'N = {}^tN\left({}^tM\right)^{-1}{}^tMQ'MM^{-1}N = {}^t(M^{-1}N)Q''(M^{-1}N)$$

となる．すると，$M^{-1}N \in \mathrm{M}_p(2,\mathbf{Z})$ であるから，命題 9.8 より $M^{-1}N = K_hL$ となる $0 \le h \le p$, $L \in \mathrm{SL}(2,\mathbf{Z})$ が存在する．よって，これを代入すれば，

$$Q = {}^t(K_hL)Q''K_hL = {}^tL{}^tK_hQ''K_hL \sim {}^tK_hQ''K_h$$

が成り立つ．$Q'' = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ と表せば，${}^tK_hQ''K_h = \begin{pmatrix} ap^2 & (b+2ah)p/2 \\ (b+2ah)p/2 & (b+ah)h+c \end{pmatrix} = Q_h\ (0 \le h < p)$, ${}^tK_pQ''K_p = \begin{pmatrix} a & bp/2 \\ bp/2 & cp^2 \end{pmatrix} = Q_p$ となることと合わせて，$Q \sim Q_h$ が示された． □

注意 9.10 命題 9.9 の集合は $F'_{\mathrm{red}}(D)$ にわたる和集合であるが，この $F'_{\mathrm{red}}(D)$ は $C(D)$ の代表元の集合であればどれでも成り立つ．実際，命題 9.9 の証明の中で，$Q'' \sim Q'$ となる $Q'' \in F'_{\mathrm{red}}(D)$ をとっていたが，Q' が簡約である必要は一切ない．

補題 9.11 $D \equiv 0,1 \pmod 4$ である負の整数 D と $p \in \left(\bigcup_{Q\in F'(D)} R(Q)\right) \cap \mathbf{P}$ に対し，$p \mid m$ となる $m \in \bigcap_{Q\in F'(D)} R'(Q)$ がとれるとき，$mp^2 \in \bigcap_{Q\in F'(p^2D)} R'(Q)$ が成り立つ．

証明 任意に $Q \in F'(D)$ をとると，$m \in \bigcap_{Q\in F'(D)} R'(Q)$ であるから，$m \in R'(Q)$ となる．このとき，注意 3.2 より．ある整数 a,b が存在して，$Q \sim \langle a,b,m\rangle$ とできる．すると，命題 9.9 における $Q_h = \langle ap^2, (b+$

$2ah)p, (b+ah)h+m\rangle$, $Q_p = \langle a, bp, mp^2\rangle \in F'(p^2D)\,(0 \le h < p)$ について，$mp^2 = Q_h(-h,p) = Q_p(0,1)$ であるから，各 $Q_h\,(1 \le h \le p)$ は mp^2 を原始的に表現する．ここで，$h = 0$ のとき $Q_0 = \langle ap^2, bp, m\rangle$ であるが，$p \mid m$ に注意すると $Q_0 \notin F'(p^2D)$ である．よって，$Q_h\,(0 \le h \le p)$ の中で原始的なものは全て mp^2 を原始的に表現することが分かった．$Q \in F'(D)$ は任意であったので，命題 9.9 と注意 9.10 より，$mp^2 \in \bigcap_{Q\in F'(p^2D)} R'(Q)$ が成り立つ． □

定理 9.12 (主定理 3) $D \equiv 0,1 \pmod 4$ である負の整数 D に対し，$h(\widetilde{D})$ が奇数であり，かつ $D/\widetilde{D}$ の各素因子が $\bigcup_{Q\in F'(\widetilde{D})} R(Q)$ の元であるならば，$\bigcap_{Q\in F'(D)} R'(Q) \neq \emptyset$ が成り立つ．

証明 $h(\widetilde{D})$ が奇数であるから，命題 9.3 より $m \in \bigcap_{Q\in F'(\widetilde{D})} R'(Q)$ がとれる．$D/\widetilde{D}$ のある素因子 p について，$p \nmid m$ ならば，$\gcd(p,m) = 1$ に注意すれば補題 9.2 より $pm \in \bigcap_{Q\in F'(\widetilde{D})} R'(Q)$ が成り立つ．これより，必要ならば m の値を取り替えることにより，m が $D/\widetilde{D}$ の各素因子を割り切ると仮定しても一般性を失わない．このとき，$D/\widetilde{D}$ の各素因子に対し補題 9.11 を繰り返し用いることにより，$mD/\widetilde{D} \in \bigcap_{Q\in F'(D)} R'(Q)$ が成り立つ． □

例 9.13 (主定理 3 の具体例) $D = -775$ のとき，$h(D) = 12$ であり，これは偶数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1,1,194\rangle, Q_2 = \langle 2,1,97\rangle, Q_3 = \langle 2,-1,97\rangle, Q_4 = \langle 4,3,49\rangle, Q_5 = \langle 4,-3,49\rangle, Q_6 = \langle 7,3,28\rangle, Q_7 = \langle 7,-3,28\rangle, Q_8 = \langle 8,5,25\rangle, Q_9 = \langle 8,-5,25\rangle, Q_{10} = \langle 14,3,14\rangle, Q_{11} = \langle 14,11,16\rangle, Q_{12} = \langle 14,-11,16\rangle\}$ である．一方，$\widetilde{D} = -31$ で $h(\widetilde{D}) = 3$ は奇数である．このとき，例 9.4 より $10 \in \bigcap_{Q\in F'(\widetilde{D})} R'(Q)$ をとると，$D/\widetilde{D} = 25 = 5^2$ より 10 は $D/\widetilde{D}$ の素因子 5 を割り切る．すると，例 9.4 より $5 \in \bigcup_{Q\in F'(\widetilde{D})} R(Q)$ であることに注意すれば，定理 9.12 の証明により $10 \cdot 25 = 250 \in \bigcap_{Q\in F'(D)} R'(Q)$ となるはずだが，$250 = Q_1(7,1) = Q_2(-9,1) = Q_3(9,1) = Q_4(3,2) = Q_5(-3,2) = Q_6(-1,3) = Q_7(1,3) = Q_8(5,1) = Q_9(-5,1) = Q_{10}(1,4) = Q_{11}(-3,4) = Q_{12}(3,4)$ より，これは実際に成立する．

10 問題 3 から問題 6 までの関係について

これまで，問題 3 から問題 5 までについて独立に考察を進めてきた．それらに対し，本節では，各問題の相互の関係に着目した議論を行う．つまり，$D \equiv 0,1 \pmod 4$ である負の整数 D に対し，各問題に対応する次の条件 3 から条件 6 までの関係について考える．

条件 3 判別式が D の全ての原始的 2 次形式が表現する正の整数が存在する．

条件 4 判別式が D の全ての 2 次形式が表現する正の整数が存在する．

条件 5 判別式が D の全ての原始的 2 次形式が原始的に表現する正の整数が存在する．

条件 6 判別式が D の全ての 2 次形式が原始的に表現する正の整数が存在する．

分かりやすくするため，$D \equiv 0,1 \pmod 4$ である負の整数 D のうち，条件 3，条件 4，条件 5，条件 6 を満たすもの全体のなす集合をそれぞれ，$\Delta_3, \Delta_4, \Delta_5, \Delta_6$ とおく．このとき系 7.4 と系 8.3 より，Δ_3 と Δ_4 は具体的に元を書き出すことができる．

いま，この 4 つの集合の包含関係を調べる．まず，原始的 2 次形式の定義より，$\Delta_3 \supset \Delta_4$, $\Delta_5 \supset \Delta_6$ が成り立つ．次に，原始的な表現の定義より，$\Delta_3 \supset \Delta_5$, $\Delta_4 \supset \Delta_6$ が成り立つ．最後に，主定理 2 と主定理 3 により，条件 4 が満たされるならば条件 5 も満たされるから，$\Delta_5 \supset \Delta_4$ が成り立つ．以上より，

$$\Delta_3 \supset \Delta_5 \supset \Delta_4 \supset \Delta_6$$

という包含関係があることが分かる．

以下では，より詳しく，

$$\Delta_3 \supset \Delta_5 \supsetneq \Delta_4 \supsetneq \Delta_6 \neq \emptyset$$

という関係が成り立っていることを見る．そのために，Δ_6, $\Delta_4 \setminus \Delta_6$, $\Delta_5 \setminus \Delta_4$ の元をそれぞれ具体的に挙げる．

まず，Δ_6 の元を具体的に挙げることは容易である．実際，基本判別式の定義と命題 9.3 より，類数が奇数である基本判別式 D は条件 6 を満たすことが直ちに分かる．例えば，例 9.4 では $D = -31$ を扱っているが，この D が条件 5 を満たしていることと，$F(D) = F'(D)$ であることから，この D は条件 6 も満たしていることがいえる．よって，$-31 \in \Delta_6$ であり，$\Delta_6 \neq \emptyset$ が示された．

次に，$\Delta_4 \setminus \Delta_6$ の元を具体的に挙げる．

命題 10.1 $D \equiv 0,1 \pmod 4$ である負の整数 D と奇素数 p に対し，$p \mid \widetilde{D}$ かつ $D/\widetilde{D} = p^4$ ならば，$\bigcap_{Q \in F(D)} R'(Q) = \emptyset$ である．

証明 p が奇素数であることと，基本判別式の定義から，$p^2 \nmid \widetilde{D}$ であることに注意する．以下，$\widetilde{D}$ の偶奇で場合分けする．

$\widetilde{D}$ が偶数の場合，正の整数 n を用いて $\widetilde{D} = -4n$ とかける．$F(D)$ の元として，$Q_1 = \langle 1, 0, np^4 \rangle$, $Q_2 = \langle p, 0, np^3 \rangle$, $Q_3 = \langle p^2, 0, np^2 \rangle$ がとれる．いま，$m \in \bigcap_{Q \in F(D)} R'(Q)$ が存在すると仮定すると，$\{Q_1, Q_2, Q_3\} \subset F(D)$ に注意すれば，$\gcd(x_i, y_i) = 1$ を満たす整数 $x_i, y_i \, (i = 1,2,3)$ を用いて $m = Q_1(x_1, y_1) = Q_2(x_2, y_2) = Q_3(x_3, y_3)$ と表せる．このとき，$\gcd(x_3, y_3) > 1$ が示されれば矛盾が生ずるので，したがって，$\bigcap_{Q \in F(D)} R'(Q) = \emptyset$ が成り立つ．そこで，以下で $\gcd(x_3, y_3) > 1$ を示す．まず，$m = Q_3(x_3, y_3) = p^2(x_3^2 + ny_3^2)$ より，$p^2 \mid m$ が成り立つ．これと $m = Q_1(x_1, y_1) = x_1^2 + np^4 y_1^2$, $m = Q_2(x_2, y_2) = p(x_2^2 + np^2 y_2^2)$ より，$p \mid x_1, x_2$ が成り立ち，$p \mid x_2$ と $m = p(x_2^2 + np^2 y_2^2)$ から $p^3 \mid m$ となる．次に，$p^3 \mid m$ と $m = x_1^2 + np^4 y_1^2$ から $p^2 \mid x_1$ となり，$p^4 \mid m$ が成り立つ．これと $m = p^2(x_3^2 + ny_3^2)$ より，$p \mid \widetilde{D}$ から $p \mid n$ であることに注意すれば，$p \mid x_3$ を得る．しかし，$p^2 \nmid \widetilde{D}$ より $p^2 \nmid n$ であるから，$p \mid x_3$ と合わせて $p \mid y_3$ を得る．よって，$p \mid \gcd(x_3, y_3)$ より $\gcd(x_3, y_3) > 1$ が示された．

$\widetilde{D}$ が奇数の場合，正の整数 n を用いて $\widetilde{D} = 1 - 4n$ とかける．$F(D)$ の元として，$Q_1 = \langle 1, p^2, np^4 \rangle$, $Q_2 = \langle p, p^2, np^3 \rangle$, $Q_3 = \langle np^2, -p^2\widetilde{D}, -p^2\widetilde{D} \rangle$ がとれる．$\widetilde{D}$ が偶数の場合と同様に，$m \in \bigcap_{Q \in F(D)} R'(Q)$ が存在すると仮定し，$\gcd(x_i, y_i) = 1$ を満たす整数 $x_i, y_i \, (i = 1,2,3)$ を用いて $m = Q_1(x_1, y_1) = Q_2(x_2, y_2) = Q_3(x_3, y_3)$ と表すと，$\widetilde{D}$ が偶数の場合と同様の議論により $p^4 \mid m$ がいえる．これと $m = Q_3(x_3, y_3) = p^2(nx_3^2 - \widetilde{D}x_3y_3 - \widetilde{D}y_3^2)$ より，$p \mid \widetilde{D}, p \nmid n$ に注意すれば，$p \mid x_3$ を得る．しかし，$p^2 \nmid \widetilde{D}$ であるから，

$p \mid x_3$, $p^2\widetilde{D}y_3^2 = -m + p^2nx_3^2 + p^2\widetilde{D}x_3y_3$ と合わせると $p \mid y_3$ が得られ，したがって $\gcd(x_3, y_3) > 1$ が成り立つから，矛盾が生ずる．□

例 10.2 (命題 10.1 の具体例) $D = -243$ のとき，$h(D) = 3$ であり，これは奇数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 1, 61\rangle, Q_2 = \langle 7, 3, 9\rangle, Q_3 = \langle 7, -3, 9\rangle\}$ である．さらに，$\widetilde{D} = -3$ となり，$h(\widetilde{D}) = 1$ である．このとき，$h(D)$ が奇数であるから，命題 9.3 より $\bigcap_{Q\in F'(D)} R'(Q) \neq \emptyset$ が成り立つ．一方，$D/\widetilde{D} = 81 = 3^4$ であり，かつ 3 が $\widetilde{D}$ を割り切る奇素数なので，命題 10.1 より $\bigcap_{Q\in F(D)} R'(Q) = \emptyset$ である．よって，$-243 \in \Delta_4 \setminus \Delta_6$ となり，$\Delta_4 \supsetneq \Delta_6$ が示された．

最後に，$\Delta_5 \setminus \Delta_4$ の元を具体的に挙げる．

命題 10.3 $D \equiv 0, 1 \pmod 4$ である負の整数 D と奇素数 p に対し，$h(\widetilde{D}) = 1$ かつ $D/\widetilde{D} = p^2$ ならば，$\bigcap_{Q\in F'(D)} R'(Q) \neq \emptyset$ である．

証明 $h(\widetilde{D}) = 1$ より，$F'_{\mathrm{red}}(\widetilde{D}) = \{Q\}$ (Q は $F'(\widetilde{D})$ の基本形式) である．以下，$\widetilde{D}$ の偶奇で場合分けする．

$\widetilde{D}$ が偶数のとき，正の整数 n を用いて $Q = \langle 1, 0, n\rangle$ とかける．すると，命題 9.9 より，任意の $F'(D)$ の元は，$Q_h = \langle p^2, 2hp, h^2 + n\rangle\ (0 \le h < p)$, $Q_p = \langle 1, 0, np^2\rangle \in F'(D)$ のいずれかと対等である．ここで，$(n+1)p^2 = Q_h(-h+1, p) = Q_h(-h-1, p) = Q_p(0, 1)$ であり，$\gcd(-h+1, -h-1) = \gcd(-h+1, 2)$ が 2 を割り切ることと p が奇素数であることより，$\gcd(-h+1, p) = 1$ または $\gcd(-h-1, p) = 1$ であることに注意すれば，$Q_h\ (0 \le h \le p)$ は $(n+1)p^2$ を原始的に表現し，$(n+1)p^2 \in \bigcap_{Q\in F'(D)} R'(Q)$ が成り立つ．

$\widetilde{D}$ が奇数のとき，正の整数 n を用いて $Q = \langle 1, 1, n\rangle$ とかける．すると，命題 9.9 より，任意の $F'(D)$ の元は，$Q_h = \langle p^2, (1+2h)p, (1+h)h+n\rangle\ (0 \le h < p)$, $Q_p = \langle 1, p, np^2\rangle \in F'(D)$ のいずれかと対等である．ここで，$np^2 = Q_h(-h, p) = Q_h(-h-1, p) = Q_p(0, 1)$ であり，$\gcd(-h, -h-1) = 1$ より $\gcd(-h, p) = 1$ または $\gcd(-h-1, p) = 1$ であることに注意すれば，$Q_h\ (0 \le h \le p)$ は np^2 を原始的に表現し，$np^2 \in \bigcap_{Q\in F'(D)} R'(Q)$ が成り立つ．□

例 10.4 (命題 10.3 の具体例) $D = -200$ のとき，$h(D) = 6$ であり，これは偶数である．また，$F'_{\mathrm{red}}(D) = \{Q_1 = \langle 1, 0, 50\rangle, Q_2 = \langle 2, 0, 25\rangle, Q_3 = \langle 3, 2, 17\rangle, Q_4 = \langle 3, -2, 17\rangle, Q_5 = \langle 6, 4, 9\rangle, Q_6 = \langle 6, -4, 9\rangle\}$ である．さらに，$\widetilde{D} = -8$ となり，$h(\widetilde{D}) = 1$ である．このとき，$D/\widetilde{D} = 25 = 5^2$ であり，$\left(\frac{\widetilde{D}}{p}\right) = \left(\frac{-8}{5}\right) = -1$ ゆえ，命題 8.4 から $5 \notin \bigcup_{Q\in F'(\widetilde{D})} R(Q)$ となる．すると，定理 8.2 から $\bigcap_{Q\in F(D)} R(Q) = \emptyset$ が成り立つ．一方，$h(\widetilde{D}) = 1$ かつ 5 が奇素数なので，命題 10.3 の証明により $(1+2)\cdot 5^2 = 75 \in \bigcap_{Q\in F'(D)} R'(Q)$ となるはずだが，$75 = Q_1(5, 1) = Q_2(5, 1) = Q_3(1, 2) = Q_4(-1, 2) = Q_5(3, 1) = Q_6(-3, 1)$ より，これは実際に成立する．以上より，$-200 \in \Delta_5 \setminus \Delta_4$ となり，$\Delta_5 \supsetneq \Delta_4$ が示された．

謝辞

本論文作成において，学部生のときからお世話になっております，指導教官の鈴木正俊先生には，丁寧かつ熱心なご指導と多大なご協力をいただき，大変感謝しております．誠にありがとうございました．この場をお借りして厚く御礼を申し上げます．

参考文献

[1] D. A. Cox, Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[2] N. Uchida, Integers of the Form $ax^2 + bxy + cy^2$, preprint, arXiv:2001.11632v3.

[3] C. Donnay, H. Ellers, K. O'Connor, K. Thompson, E. Wood, Numbers represented by a Finite Set of Binary Quadratic Forms, preprint, arXiv:1708.04877v1.

[4] D. A. Buell, Binary quadratic forms. Classical theory and modern computations. Springer-Verlag, New York, 1989.

[5] 河田敬義, 数学の歴史 7a 19 世紀の数学 整数論, 共立出版, 1992.

[6] 河田敬義, 数論：古典数論から類体論へ, 岩波書店, 1992.

[7] 高瀬正仁, 数学史叢書 ガウス整数論, 朝倉書店, 1995.

[8] 酒井孝一, 現代数学の系譜 5 ディリクレ デデキント 整数論講義, 共立出版, 1970.

[9] J. Voight, Quadratic forms that represent almost the same primes. Math. Comp. 76, 2007.

[10] M. Elia, F. Pintore, On the Representation of Primes by Binary Quadratic Forms, and Elliptic Curves, preprint, arXiv:1604.06586v1.

[11] J. H. Conway, Universal quadratic forms and the fifteen theorem. Quadratic forms and their applications (Dublin, 1999), 23–26, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.