J. Aust. Math. Soc. **100** (2016), 182–191
doi:10.1017/S1446788715000440

REPRESENTATIONS OF INTEGERS BY THE BINARY QUADRATIC FORM $x^2 + xy + ny^2$

BUMKYU CHO

(Received 19 October 2014; accepted 19 August 2015; first published online 17 November 2015)

Communicated by I. E. Shparlinski

Abstract

In terms of class field theory we give a necessary and sufficient condition for an integer to be representable by the quadratic form $x^2 + xy + ny^2$ ($n \in \mathbb{N}$ arbitrary) under extra conditions $x \equiv 1 \bmod m$, $y \equiv 0 \bmod m$ on the variables. We also give some examples where their extended ring class numbers are less than or equal to 3.

2010 *Mathematics subject classification*: primary 11N32; secondary 11R37, 11F11.

Keywords and phrases: quadratic forms, class field theory.

1. Introduction

As is well known, the principal binary quadratic form of discriminant $D < 0$ is $x^2 - (D/4)y^2$ or $x^2 + xy + ((1 - D)/4)y^2$ for $D \equiv 0$ or $1 \bmod 4$, respectively. Thanks to Cox [5], we are well aware of a necessary and sufficient condition for a prime to be representable by $x^2 - (D/4)y^2$ and his result is described in terms of class field theory. In [3], the author of the present article gave a necessary and sufficient condition for an integer to be representable by the same form. The purpose of this article is to study the same problem for the other principal form $x^2 + xy + ((1 - D)/4)y^2$.

Let $a = 3^l \prod_{i=1}^{s} p_i^{n_i} \prod_{j=1}^{t} q_j^{m_j}$ be the prime factorization of a positive integer a, where $p_i \equiv 1 \bmod 3$ and $q_j \equiv 2 \bmod 3$. It is a classical result that $a = x^2 + xy + y^2$ for some integers x, y if and only if each m_j is even. There are similar results for the binary forms $x^2 + xy + ny^2$ with some small positive integers n (see, for example, [6, Ch. I]). In the present article we will give a generalization of those results for arbitrary $n \in \mathbb{N}$. Actually, we will consider the problem under the congruence conditions $x \equiv 1 \bmod m$ and $y \equiv 0 \bmod m$ on the variables, and the result will be described in terms of extended

The author was supported by NRF-2015R1C1A1A02037526 and the Dongguk University Research Fund of 2015.

ring class fields. When the extended ring class number is less than or equal to 3, we can give a more down-to-earth characterization. Some examples are given in Section 3.

2. Statements and proofs of results

We begin by briefly reviewing some properties of extended ring class fields. For more details the reader may refer to [2] or [5, Section 15].

Let $\mathcal{O}_K$ be the ring of integers in an imaginary quadratic field K, $\mathfrak{m}$ an ideal of $\mathcal{O}_K$, $\mathcal{O}$ an order of conductor f in K, and $I_K(\mathfrak{m})$ the group of all fractional ideals of K relatively prime to $\mathfrak{m}$. We denote by $P_{K,1}(\mathfrak{m})$ the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv 1 \bmod \mathfrak{m}$. Moreover, we define the subgroup $P_{\mathfrak{m},\mathcal{O}}$ of $I_K(\mathfrak{m}(f))$ by

$$P_{\mathfrak{m},\mathcal{O}} = \langle\{(\alpha) \in I_K(\mathfrak{m}(f)) \mid \alpha \in \mathcal{O}_K, \alpha \equiv a \bmod \mathfrak{m}(f) \text{ for some } a \in \mathbb{Z} \\ \text{with } (a, f) = 1, a \equiv 1 \bmod \mathfrak{m}\}\rangle.$$

Note that $P_{K,1}(\mathfrak{m}(f)) \subset P_{\mathfrak{m},\mathcal{O}} \subset I_K(\mathfrak{m}(f))$, and hence we may define the extended ring class field $K_{\mathfrak{m},\mathcal{O}}$ to be the class field of K corresponding to $P_{\mathfrak{m},\mathcal{O}}$. Then the Galois group of $K_{\mathfrak{m},\mathcal{O}}$ over K is isomorphic to the ideal class group $I_K(\mathfrak{m}(f))/P_{\mathfrak{m},\mathcal{O}}$ via the Artin map. By definition, $K_{\mathcal{O}_K,\mathcal{O}}$ equals the ring class field of the order $\mathcal{O}$ and $K_{\mathfrak{m},\mathcal{O}_K}$ equals the ray class field of K with modulus $\mathfrak{m}$. Of course, $K_{\mathcal{O}_K,\mathcal{O}_K}$ is nothing but the Hilbert class field of K.

Let $\rho : \mathbb{C} \to \mathbb{C}$ be complex conjugation. Then $\rho(K_{\mathfrak{m},\mathcal{O}})$ is abelian over $\rho(K) = K$ with the Galois group $\rho\mathrm{Gal}(K_{\mathfrak{m},\mathcal{O}}/K)\rho^{-1}$. If we assume $\mathfrak{m} = \rho(\mathfrak{m})$, then $\rho(P_{\mathfrak{m},\mathcal{O}}) = P_{\mathfrak{m},\mathcal{O}}$ implies $\rho(K_{\mathfrak{m},\mathcal{O}}) = K_{\mathfrak{m},\mathcal{O}}$ by the same argument as in the proof of [5, Lemma 9.3]. Thus, $K_{\mathfrak{m},\mathcal{O}}$ is Galois over $\mathbb{Q}$, and consequently there exists a real algebraic integer ε such that $K_{\mathfrak{m},\mathcal{O}} = K(\varepsilon)$ (see [5, Proposition 5.29(i)]). If we let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of ε over K and p a rational prime relatively prime to the discriminant of $f(X)$, then by [5, Proposition 5.29(ii)] we have that p splits completely in $K_{\mathfrak{m},\mathcal{O}}$ if and only if $(d_K/p) = 1$ and $f(X) \equiv 0 \bmod p$ has an integer solution.

Throughout the rest of this article, let n, m denote positive integers, $D = 1 - 4n$, $K = \mathbb{Q}(\sqrt{D})$, $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{D})/2]$, and let f denote the conductor of the order $\mathcal{O}$. Then $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ and $D = f^2 d_K$, where d_K is the discriminant of K.

Lemma 2.1. *Let $p \in \mathbb{N}$ be a prime with $(p, 2Dm) = 1$. Then p is of the form $x^2 + xy + ny^2$ with $x \equiv 1 \bmod m$, $y \equiv 0 \bmod m$ if and only if $(D/p) = 1$ and $\mathfrak{p} \in P_{(m),\mathcal{O}}$, where $\mathfrak{p}$ is any prime ideal of $\mathcal{O}_K$ lying over p.*

Proof. Suppose that p is representable by the form described in the assumption. Since $(p, y) = 1$, we infer from $(2x + y)^2 - Dy^2 \equiv 0 \bmod p$ that $(D/p) = 1$. Setting $\mathfrak{p} = (x + ((1 + \sqrt{D})/2)y)\mathcal{O}_K$, we have a factorization $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Now it is straightforward to deduce $\mathfrak{p} \in P_{(m),\mathcal{O}}$ from

$$\mathfrak{p} = \Big(x + \frac{1-f}{2}y + \frac{1+\sqrt{d_K}}{2}fy\Big)\mathcal{O}_K, \quad \Big(f, x + \frac{1-f}{2}y\Big) = 1, \quad (f, p) = 1.$$

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

For the converse, we may put $\mathfrak{p} = (u + mv + mw((1 + \sqrt{D})/2))\mathcal{O}_K$ for some $u, v, w \in \mathbb{Z}$ with $(u, f) = 1$, $u \equiv 1 \bmod m$. Then

$$p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} = ((u + mv)^2 + (u + mv)mw + n(mw)^2)\mathcal{O}_K,$$

and hence $p = ((u + mv)^2 + (u + mv)mw + n(mw)^2)\alpha$ for some unit $\alpha \in \mathcal{O}_K^\times$. The only possibility is $\alpha = 1$. □

Lemma 2.2. *Let $q \in \mathbb{N}$ be a prime with $(q, 2Dm) = 1$ and $(D/q) = -1$. Then $q \equiv \pm 1 \bmod m$ if and only if $q\mathcal{O}_K \in P_{(m),\mathcal{O}}$.*

Proof. If $q \equiv \pm 1 \bmod m$, then $\pm q \equiv 1 \bmod m$ with the same sign. Thus we have $q\mathcal{O}_K = (\pm q) \in P_{(m),\mathcal{O}}$.

For the converse, we may put $q\mathcal{O}_K = (u + mv + mw((1 + \sqrt{D})/2))\mathcal{O}_K$ for some $u, v, w \in \mathbb{Z}$ with $(u, f) = 1$, $u \equiv 1 \bmod m$. Then

$$q = \Big(u + mv + mw\frac{1 + \sqrt{D}}{2}\Big)\alpha$$

for some unit $\alpha \in \mathcal{O}_K^\times$. It is tedious to verify that $\alpha = \pm 1$ and $w = 0$. □

Proposition 2.3. *Let $p \in \mathbb{N}$ be a prime such that $(p, 2Dm) = 1$. Then*

$$\begin{pmatrix} p = x^2 + xy + ny^2 \\ x \equiv 1 \bmod m,\ y \equiv 0 \bmod m \end{pmatrix} \Longleftrightarrow p \text{ splits completely in } K_{(m),\mathcal{O}}.$$

Let $f_{n,m}(X) \in \mathbb{Z}[X]$ be the minimal polynomial of a real algebraic integer which generates $K_{(m),\mathcal{O}}$ over K. Assuming further that p is relatively prime to the discriminant of $f_{n,m}(X)$,

$$\begin{pmatrix} p = x^2 + xy + ny^2 \\ x \equiv 1 \bmod m,\ y \equiv 0 \bmod m \end{pmatrix} \Longleftrightarrow \begin{pmatrix} \left(\frac{D}{p}\right) = 1 \text{ and } f_{n,m}(X) \equiv 0 \bmod p \\ \text{has an integer solution} \end{pmatrix}.$$

Proof. By Lemma 2.1,

$$p = x^2 + xy + ny^2 \quad x \equiv 1\ (m), \quad y \equiv 0\ (m) \Longleftrightarrow \left(\frac{D}{p}\right) = 1 \quad \mathfrak{p} \in P_{(m),\mathcal{O}}$$

where $\mathfrak{p}$ is any prime ideal lying over p. Since $K_{(m),\mathcal{O}} \subset K_{(mf)}$ and $(mf, p) = 1$, $\mathfrak{p}$ is unramified in $K_{(m),\mathcal{O}}$. Hence, by class field theory,

$$\mathfrak{p} \in P_{(m),\mathcal{O}} \Longleftrightarrow \mathfrak{p} \text{ splits completely in } K_{(m),\mathcal{O}}.$$

Since $K_{(m),\mathcal{O}}$ is Galois over $\mathbb{Q}$,

$$\left(\frac{D}{p}\right) = 1, \quad \mathfrak{p} \in P_{(m),\mathcal{O}} \Longleftrightarrow p \text{ splits completely in } K_{(m),\mathcal{O}}.$$

Now, by means of [5, Proposition 5.29], we conclude that p splits completely in $K_{(m),\mathcal{O}}$ if and only if $(d_K/p) = 1$ and $f_{n,m}(X) \equiv 0 \bmod p$ has an integer solution. This completes the proof. □

Let $P(n, m)$ (respectively, $P^*(n, m)$) denote the set of all primes p such that $(p, 2Dm) = 1$, $(D/p) = 1$, and p is (respectively, is not) of the form $x^2 + xy + ny^2$ with $x \equiv 1 \bmod m$ and $y \equiv 0 \bmod m$. Further, let $Q(n, m)$ (respectively, $Q^*(n, m)$) denote the

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

set of all primes q such that $(q, 2Dm) = 1$, $(D/q) = -1$, and q is (respectively, is not) congruent to ± 1 modulo m. Then we see from Lemmas 2.1 and 2.2 that

$$p \in P(n,m) \iff \mathfrak{p} \in P_{(m),O},$$
$$q \in Q(n,m) \iff qO_K \in P_{(m),O}$$

where $\mathfrak{p}$ is any prime ideal of O_K lying over p. Assume further that p is relatively prime to the discriminant of $f_{n,m}(X)$. Appealing to Proposition 2.3,

$$p \in P(n,m) \iff f_{n,m}(X) \equiv 0 \bmod p \text{ is solvable in } \mathbb{Z}.$$

There are several articles describing methods of finding generators of $K_{(m),O}$ and their minimal polynomials $f_{n,m}(X)$. See [1, 2, 4, 5, 7, 8, 10–12] for references. Explicit descriptions of $P(n,m)$ for certain n, m will be given in Section 3.

We now state our main theorem.

Theorem 2.4. *Let*

$$a = p_1 \cdots p_t p_{t+1}^{k_{t+1}} \cdots p_r^{k_r} q_1^{l_1} \cdots q_u^{l_u} q_{u+1}^{l_{u+1}} \cdots q_s^{l_s}$$

be a positive integer relatively prime to $2Dm$, *where* $r, s \geq 0$, $k_i, l_j > 0$ *and* $p_1, \ldots, p_t \in P^*(n,m)$, $p_{t+1}, \ldots, p_r \in P(n,m)$, $q_1, \ldots, q_u \in Q^*(n,m)$, $q_{u+1}, \ldots, q_s \in Q(n,m)$. *Here* $p_1, \ldots, p_t$ *are primes, not necessarily distinct; the other primes are mutually distinct. Then* $a = x^2 + xy + ny^2$ *for some* $x, y \in \mathbb{Z}$ *with* $x \equiv 1 \bmod m$, $y \equiv 0 \bmod m$ *if and only if:*

(1) l_j *is even for each* $j = 1, \ldots, s$;
(2) *there exist prime ideals* $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ *of* O_K *lying over* $p_1, \ldots, p_t$, *respectively, such that* $\prod_{i=1}^t \mathfrak{p}_i \prod_{j=1}^u (q_j O_K)^{l_j/2} \in P_{(m),O}$.

Remark 2.5. The prime ideals $\mathfrak{p}_i, \mathfrak{p}_j$ of O_K in the preceding theorem need not be equal even when $p_i = p_j$ with $i \neq j$.

The primes q_j for which the discriminant D is a quadratic nonresidue must appear to even coefficients l_j in the factoring of an a that is represented by the principal form. If, further, $m = 1$, then $Q^*(n, 1)$ is empty and hence the part $q_j^{l_j}$ of the representation is inherently imprimitive. Namely, the primes q_j for which D is not a quadratic residue are irrelevant because they appear only in the imprimitive representation and hence we can concentrate on $p_1, \ldots, p_t \in P(n, 1)$ as follows.

Corollary 2.6. *Let*

$$a = p_1 \cdots p_t p_{t+1}^{k_{t+1}} \cdots p_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}$$

be a positive integer relatively prime to $2D$, *where* $r, s \geq 0$, $k_i, l_j > 0$ *and* $p_1, \ldots, p_t \in P^*(n, 1)$, $p_{t+1}, \ldots, p_r \in P(n, 1)$, $(D/q_j) = -1$. *Here* $p_1, \ldots, p_t$ *are primes, not necessarily distinct; the other primes are mutually distinct. Then* $a = x^2 + xy + ny^2$ *for some* $x, y \in \mathbb{Z}$ *if and only if:*

(1) l_j *is even for each* $j = 1, \ldots, s$;
(2) *there exist prime ideals* $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ *of* O_K *lying over* $p_1, \ldots, p_t$, *respectively, such that* $\prod_{i=1}^t \mathfrak{p}_i \in P_{(1),O}$.

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

Proof of Theorem 2.4. Let $a = \prod_{i=1}^r p_i \prod_{j=1}^s q_j^{l_j}$ be a positive integer relatively prime to $2Dm$, where $r, s \geq 0$, $l_j > 0$, the p_i are primes, not necessarily distinct, with $(D/p_i) = 1$, and the q_j are mutually distinct primes with $(D/q_j) = -1$. We need to show that $a = x^2 + xy + ny^2$ for some $x, y \in \mathbb{Z}$ with $x \equiv 1 \bmod m$, $y \equiv 0 \bmod m$ if and only if:

(i) l_j is even for each $1 \leq j \leq s$;
(ii) there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of O_K lying over $p_1, \dots, p_r$, respectively, such that $\prod_{i=1}^r \mathfrak{p}_i \prod_{j=1}^s (q_j O_K)^{l_j/2} \in P_{(m),O}$.

Suppose that a satisfies conditions (i) and (ii). Put $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i \prod_{j=1}^s (q_j O_K)^{l_j/2}$. Since $\mathfrak{a} \in P_{(m),O}$, we may put $\mathfrak{a} = (u + mv + mw((1 + \sqrt{D})/2))O_K$ for some $u, v, w \in \mathbb{Z}$ with $(u, f) = 1$, $u \equiv 1 \bmod m$. Then

$$aO_K = \mathfrak{a}\bar{\mathfrak{a}} = ((u + mv)^2 + (u + mv)mw + n(mw)^2)O_K,$$

and hence $a = ((u + mv)^2 + (u + mv)mw + n(mw)^2)\alpha$ for some unit $\alpha \in O_K^\times$. Because $a > 0$, α must be 1.

Now we prove the other direction. If $q_j \nmid y$ for some j, then we can infer from $(2x + y)^2 - Dy^2 \equiv 0 \bmod q_j$ that $(D/q_j) = 1$, which is a contradiction. So $q_j | y$ and hence $q_j | x$ for all j. Applying the same argument to $a/(q_1^2 \cdots q_s^2)$, we can deduce that $2 | l_j$ for all j. Observe that

$$\begin{aligned} a &= \Big(x + \frac{1 + \sqrt{D}}{2} y\Big)\Big(x + \frac{1 - \sqrt{D}}{2} y\Big) \\ &= \Big(x + \frac{1 - f}{2} y + \frac{1 + \sqrt{d_K}}{2} fy\Big)\Big(x + \frac{1 - f}{2} y + \frac{1 - \sqrt{d_K}}{2} fy\Big). \end{aligned}$$

Set $\mathfrak{b} := (x + ((1 - f)/2)y + ((1 + \sqrt{d_K})/2)fy)O_K$. Since $(a, D) = 1$, we deduce that $(\mathfrak{b}, f) = 1$, and hence $(x + ((1 - f)/2)y, f) = 1$. This shows that $\mathfrak{b} \in P_{(m),O}$. Since q_j is inert in K, we can infer from $aO_K = \mathfrak{b}\bar{\mathfrak{b}}$ that $(q_j O_K)^{l_j/2}$ divides $\mathfrak{b}$ for all j. Because p_i splits completely in K, we can choose prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of O_K lying over $p_1, \dots, p_r$, respectively, so that

$$\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i \prod_{j=1}^s (q_j O_K)^{l_j/2}.$$

This completes the proof. □

Let $h(n, m)$ denote the order of the ideal class group $I_K(mf)/P_{(m),O}$. If the extended ring class number $h(n, m)$ is small, we can obtain more down-to-earth statements as corollaries.

Corollary 2.7. *Suppose that $h(n, m) = 1$. Let $a = p_1 \cdots p_r b^2$ be a positive integer relatively prime to $2Dm$, where the p_i are mutually distinct primes. Then $a = x^2 + xy + ny^2$ for some $x, y \in \mathbb{Z}$ with $x \equiv 1 \bmod m$ and $y \equiv 0 \bmod m$ if and only if $(D/p_i) = 1$ for all i.*

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

Proof. Condition (2) of Theorem 2.4 holds trivially because $h(n, m) = 1$. □

Corollary 2.8. *Suppose that $h(n, m) = 2$. Let*

$$a = p_1^{k_1} \cdots p_t^{k_t} p_{t+1}^{k_{t+1}} \cdots p_r^{k_r} q_1^{l_1} \cdots q_u^{l_u} q_{u+1}^{l_{u+1}} \cdots q_s^{l_s}$$

be a positive integer relatively prime to $2Dm$, where the p_i and q_j are mutually distinct primes with $p_1, \ldots, p_t \in P^*(n, m)$, $p_{t+1}, \ldots, p_r \in P(n, m)$, $q_1, \ldots, q_u \in Q^*(n, m)$, $q_{u+1}, \ldots, q_s \in Q(n, m)$. Then $a = x^2 + xy + ny^2$ for some $x \equiv 1 \bmod m$, $y \equiv 0 \bmod m$ if and only if:

(1) *l_j is even for each $j = 1, \ldots, s$;*
(2) $\sum_{i=1}^{t} k_i + \frac{1}{2} \sum_{j=1}^{u} l_j \equiv 0 \bmod 2$.

Proof. Let $\mathfrak{p}_i$ $(1 \le i \le t)$ be a prime ideal of O_K lying over p_i. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_t, q_1 O_K, \ldots, q_u O_K$ are not contained in $P_{(m),O}$. Since $h(n, m) = 2$, $\mathfrak{p}_i P_{(m),O} = \overline{\mathfrak{p}_i} P_{(m),O}$, and the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t, q_1 O_K, \ldots, q_u O_K$ represent the same nonidentity element in the ideal class group $I_K(mf)/P_{(m),O}$ of order 2. Therefore, condition (2) of Theorem 2.4 is equivalent to $\sum_{i=1}^{t} k_i + \frac{1}{2} \sum_{j=1}^{u} l_j \equiv 0 \bmod 2$. □

Corollary 2.9. *Suppose that $h(n, 1) = 3$. Let*

$$a = p_1 \cdots p_t p_{t+1}^{k_{t+1}} \cdots p_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}$$

be a positive integer relatively prime to $2D$ with $p_1, \ldots, p_t \in P^*(n, 1)$, $p_{t+1}, \ldots, p_r \in P(n, 1)$, $(D/q_j) = -1$. Here $p_1, \ldots, p_t$ are primes, not necessarily distinct. Then $a = x^2 + xy + ny^2$ for some $x, y \in \mathbb{Z}$ if and only if:

(1) *l_j is even for each $j = 1, \ldots, s$;*
(2) *$t = 0$ or $t \ge 2$.*

Proof. Let $\mathfrak{p}_i$ $(1 \le i \le t)$ be a prime ideal of O_K lying over p_i. Because $\mathfrak{p}_i \overline{\mathfrak{p}_i} = p_i O_K \in P_{(1),O}$, the ideal class $\overline{\mathfrak{p}_i} P_{(1),O}$ is the inverse of $\mathfrak{p}_i P_{(1),O}$ and hence the ideal classes $\mathfrak{p}_i P_{(1),O}$ and $\overline{\mathfrak{p}_i} P_{(1),O}$ are exactly the two nonidentity elements of the ideal class group $I_K(f)/P_{(1),O}$ of order 3 for each i. Therefore, we can take $\mathfrak{p}_i$ (or $\overline{\mathfrak{p}_i}$ if necessary) lying above p_i so that $\mathfrak{p}_1 \cdots \mathfrak{p}_t \in P_{(1),O}$ whenever $t \ne 1$. This demonstrates condition (2) of Corollary 2.6. □

For completeness we need a formula for $h(n, m)$, which is given in [3, Theorem 2.9].

Proposition 2.10. *Let h_K be the class number of K and*

$$O_{K,m,f}^{\times} = \{\alpha \in O_K^{\times} \mid \alpha \equiv a \bmod mfO_K \text{ for some } a \in \mathbb{Z} \text{ with } a \equiv 1 \bmod m\}.$$

Then

$$h(n, m) = \frac{h_K m^2 f}{[O_K^{\times} : O_{K,m,f}^{\times}]} \prod_{p \mid m} \Big(1 - \frac{1}{p}\Big)\Big(1 - \Big(\frac{d_K}{p}\Big)\frac{1}{p}\Big) \prod_{\substack{p \mid f \\ p \nmid m}} \Big(1 - \Big(\frac{d_K}{p}\Big)\frac{1}{p}\Big).$$

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

REMARK 2.11. By direct computation and known results about imaginary quadratic fields of small class number,

$$\begin{aligned} h(n,m) = 1 &\iff (n,m) = (1,1),(1,2),(1,3),(2,1),(2,2),(3,1),(5,1), \\ &\qquad (7,1),(11,1),(17,1), \text{ or } (41,1), \\ h(n,m) = 2 &\iff (n,m) = (1,4),(2,4),(3,3),(4,1),(4,2),(9,1),(13,1), \\ &\qquad (19,1),(23,1),(25,1),(29,1),(31,1),(37,1),(47,1), \\ &\qquad (59,1),(67,1),(101,1), \text{ or } (107,1), \\ h(n,1) = 3 &\iff n = 6,8,15,21,27,35,53,61,71,77,83,95,125,137,161, \\ &\qquad 221, \text{ or } 227. \end{aligned}$$

3. Examples

When we deal with primes dividing $2Dm$, the following lemmas will turn out to be useful in some cases (see Examples 3.3 and 3.4).

LEMMA 3.1. *If*

$$a = x^2 + xy + ny^2 \quad x \equiv 1 \bmod m,\ y \equiv 0 \bmod m$$

and

$$b = z^2 + zw + nw^2 \quad z \equiv 1 \bmod m,\ w \equiv 0 \bmod m$$

then

$$ab = (xz - nyw)^2 + (xz - nyw)(xw + yz + yw) + n(xw + yz + yw)^2.$$

Moreover, $xz - nyw \equiv 1 \bmod m$ *and* $xw + yz + yw \equiv 0 \bmod m$*.*

LEMMA 3.2. *If*

$$a = x^2 + xy + ny^2 \quad x \equiv 1 \bmod m,\ y \equiv 0 \bmod m$$

and if

$$p = z^2 + zw + nw^2 \quad z \equiv 1 \bmod m,\ w \equiv 0 \bmod m$$

is a prime divisor of a*, then*

$$\frac{a}{p} = (x')^2 + x'y' + n(y')^2$$

for some $x', y' \in \mathbb{Z}$ *with* $x' \equiv 1 \bmod m$ *and* $y' \equiv 0 \bmod m$*.*

PROOF. Since $aw^2 - py^2 = (xw - yz)(xw + yz + yw)$, p divides $xw - yz$ or $xw + yz + yw$. By exchanging z and w with $z + w$ and $-w$, respectively, we may assume that p divides $xw - yz$. From the identity $w(xw + xz + nyw) = (xw - yz)(z + w) + py$ we also see that p divides $xw + xz + nyw$. Now the asserted statement follows immediately by setting $x' = (xw + xz + nyw)/p$ and $y' = -(xw - yz)/p$. □

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

Example 3.3. Consider the case $(n, m) = (2, 2)$. Let $a = p_1 \cdots p_r b^2$ be a positive integer where the p_i are mutually distinct primes. Corollary 2.7 implies that if $(a, 14) = 1$ then

$$a = x^2 + xy + 2y^2 \quad x \equiv 1 \bmod 2, \quad y \equiv 0 \bmod 2 \iff p_i \equiv 1, 2, 4 \bmod 7 \text{ for each } i.$$

Since 2 and 7 are also representable by the given form, we deduce from Lemmas 3.1 and 3.2 that for a arbitrary,

$$a = x^2 + xy + 2y^2 \quad x \equiv 1 \bmod 2, \quad y \equiv 0 \bmod 2 \iff p_i \equiv 0, 1, 2, 4 \bmod 7 \text{ for each } i.$$

Example 3.4. Let $(n, m) = (7, 1)$ and let $a = p_1 \cdots p_r b^2$ be a positive integer, where the p_i are mutually distinct primes. If $(a, 6) = 1$, then

$$a = x^2 + xy + 7y^2 \iff p_i \equiv 1 \bmod 3 \text{ for each } i$$

by Corollary 2.7. Note that neither 2 nor 3 is representable by the given form. We claim that for a arbitrary, $a = x^2 + xy + 7y^2$ if and only if:

(1) $p_i \neq 2$ and $p_i \equiv 0, 1 \bmod 3$ for each i;
(2) if $p_i = 3$ for some i, then b is divisible by 3.

First assume that conditions (1) and (2) hold true. Since 3^3 is representable by the given form, we can deduce from Lemma 3.1 that a can be expressed by the given form.

Now we prove the other direction. Dividing x and y by $d := (x, y)$,

$$a' := p_1 \cdots p_r (b/d)^2 = (x')^2 + x'y' + 7(y')^2,$$

where $x' = x/d$ and $y' = y/d$. Observe that a' must be odd. Let p be any prime divisor of a' not equal to 3. Then we deduce $(-3/p) = 1$ from $(2x' + y')^2 + 27(y')^2 \equiv 0 \bmod p$ and $(p, y') = 1$, so, in particular, we obtain condition (1). Furthermore, if $p_i = 3$ for some i but $3 \nmid b$, then we divide a' by all the prime divisors of a' except 3 and deduce from Lemma 3.2 that $3 = z^2 + zw + 7w^2$ for some $z, w \in \mathbb{Z}$. This is a contradiction.

Example 3.5. Let $(n, m) = (3, 3)$. Then $K = \mathbb{Q}(\sqrt{-11})$, $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-11})/2] = \mathcal{O}_K$, and $K_{(3),\mathcal{O}}$ equals the ray class field of K with modulus (3). By means of [2, Corollary 6] and [1, page 289] we can take the class polynomial $f_{3,3}(X)$ as

$$f_{3,3}(X) = X^2 + 33534X + 3^{12}.$$

The discriminant of $f_{3,3}(X)$ is $2^6 \cdot 3^{13} \cdot 11$ and for any prime $p \neq 2, 3, 11$ we deduce from Proposition 2.3 that

$$p = x^2 + xy + 3y^2 \quad x \equiv 1 \bmod 3, \; y \equiv 0 \bmod 3 \iff p \equiv 1, 4, 16, 25, 31 \bmod 33,$$

and hence

$$P(3, 3) = \{p \mid p \equiv 1, 4, 16, 25, 31 \bmod 33\},$$
$$P^*(3, 3) = \{p \mid p \equiv 5, 14, 20, 23, 26 \bmod 33\}.$$

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

Let $a = p_1^{k_1} \cdots p_t^{k_t} p_{t+1}^{k_{t+1}} \cdots p_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}$ be a positive integer relatively prime to 66, where the p_i and q_j are mutually distinct primes such that

$$p_1, \ldots, p_t \equiv 5, 14, 20, 23, 26 \bmod 33,$$
$$p_{t+1}, \ldots, p_r \equiv 1, 4, 16, 25, 31 \bmod 33,$$
$$q_1, \ldots, q_s \equiv 2, 6, 7, 8, 10 \bmod 11.$$

By Corollary 2.8,

$$a = x^2 + xy + 3y^2 \quad x \equiv 1 \bmod 3,\ y \equiv 0 \bmod 3$$

if and only if:

(1) l_j is even for each j;
(2) $k_1 + \cdots + k_t \equiv 0 \bmod 2$.

Example 3.6. Now we deal with an example of class number 3. Let $(n, m) = (6, 1)$. Then $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-23})/2] = \mathcal{O}_K$, and $K_{(1),\mathcal{O}}$ is the Hilbert class field of K. We remark that Hasse [10] has shown that the Hilbert class field of K is

$$K\Big(\sqrt[3]{(25 + 3\sqrt{69})/2} + \sqrt[3]{(25 - 3\sqrt{69})/2}\Big).$$

Hence, we can compute its class polynomial as

$$f_{6,1}(X) = X^3 - 3X - 25$$

with discriminant $-3^6 \cdot 23$. Using this, we may compute $P(6, 1)$ and $P^*(6, 1)$. But a more explicit and useful condition for the prime p to be represented by $x^2 + xy + ((1 - D)/4)y^2$ (or $x^2 - (D/4)y^2$) is given by Gurak [9] for $D = -23$ and by Williams and Hudson [12, Theorem 3] for all D with class number 3. The necessary and sufficient condition is described in terms of certain integer sequences: Let $p > 3$ be a prime such that $(-23/p) = 1$. We define the sequence $\{u_n\}_{n=0,1,2,\ldots}$ of integers by $u_0 = 2$, $u_1 = 25$, $u_{n+2} = 25u_{n+1} - u_n$ $(n = 0, 1, 2, \ldots)$. Then p is represented by $x^2 + xy + 6y^2$ if and only if

$$u_{(p-(p/3))/3} \equiv 2 \bmod p.$$

Thanks to this result we easily compute $P(6, 1)$ and $P^*(6, 1)$ as

$$P(6, 1) = \{59, 101, 167, 173, 211, 223, 271, 307, 317, 347, \ldots\},$$
$$P^*(6, 1) = \{13, 29, 31, 41, 47, 71, 73, 127, 131, 139, 151, 163, \ldots\}.$$

Let $a = p_1 \cdots p_t p_{t+1} \cdots p_r q_1^{l_1} \cdots q_s^{l_s}$ be a positive integer relatively prime to $2 \cdot 3 \cdot 23$, where the p_i are primes, not necessarily distinct, with $p_{t+1}, \cdots, p_r \in P(6, 1)$, $p_1, \cdots, p_t \in P^*(6, 1)$, and the q_j are mutually distinct primes with $(-23/q_j) = -1$. From Corollary 2.9, $a = x^2 + xy + 6y^2$ if and only if:

(1) l_j is even for each j;
(2) $t = 0$ or $t \geq 2$.

We further claim that $a = 2x^2 + xy + 3y^2$ if:

(1) l_j is even for each j;
(2) $t \geq 1$.

https://doi.org/10.1017/S1446788715000440 Published online by Cambridge University Press

Since the class number is 3, there is only one genus, and thus any odd prime p for which -23 is a quadratic residue is represented by either the form $x^2 + xy + 6y^2$ or the forms $2x^2 \pm xy + 3y^2$. In other words, every prime $p \in P(6, 1)$ (respectively, $p \in P^*(6, 1)$) with $p \neq 2, 3, 23$ is represented by the form $x^2 + xy + 6y^2$ (respectively, $2x^2 \pm xy + 3y^2$). Since the form class group $\{x^2 + xy + 6y^2, 2x^2 \pm xy + 3y^2\}$ is isomorphic to the cyclic group of order 3, we easily infer from the composition law of form class group that a is representable as $2x^2 + xy + 3y^2$ under the given conditions.

Acknowledgement

The author would like to express sincere thanks to the anonymous referee for very useful and worthy comments on the manuscript.

References

[1] I. Chen and N. Yui, 'Singular values of Thompson series', in: *Groups, Difference Sets, and The Monster (Columbus, OH, 1993)*, Ohio State University Mathematical Research Institute Publications, 4 (eds. K. T. Arasu, J. F. Dillon, K. Harada, S. Sehgal and R. Solomon) (de Gruyter, Berlin, 1996), 255–326.

[2] B. Cho, 'Primes of the form $x^2 + ny^2$ with conditions $x \equiv 1 \bmod N$, $y \equiv 0 \bmod N$', *J. Number Theory* **130** (2010), 852–861.

[3] B. Cho, 'Integers of the form $x^2 + ny^2$', *Monatsh. Math.* **174** (2014), 195–204.

[4] B. Cho and J. K. Koo, 'Construction of class fields over imaginary quadratic fields and applications', *Q. J. Math.* **61** (2010), 199–216.

[5] D. Cox, *Primes of the Form $x^2 + ny^2$*, 2nd edn (Wiley, Hoboken, NJ, 2013).

[6] L. E. Dickson, *History of the Theory of Numbers, Volume III: Quadratic and Higher Forms* (Dover Publications, New York, 2005).

[7] I. S. Eum, J. K. Koo and D. H. Shin, 'Primitive generators of certain class fields', *J. Number Theory* **155** (2015), 46–62.

[8] A. Gee, 'Class invariants by Shimura's reciprocity law', *J. Théor. Nombres Bordeaux* **11** (1999), 45–72.

[9] S. Gurak, 'On the representation theory for full decomposable forms', *J. Number Theory* **13** (1981), 421–442.

[10] H. Hasse, 'Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante −47', *Acta Arith.* **9** (1964), 419–434.

[11] P. Stevenhagen, 'Hilbert's 12th problem, complex multiplication, and Shimura reciprocity', in: *Class Field Theory—Its Centenary and Prospect*, Advanced Studies in Pure Mathematics, 30 (ed. K. Miyake) (Mathematical Society of Japan, Tokyo, 2001), 161–176.

[12] K. S. Williams and R. H. Hudson, 'Representation of primes by the principal form of discriminant $-D$ when the classnumber $h(-D)$ is 3', *Acta Arith.* **57** (1991), 131–153.

BUMKYU CHO, Department of Mathematics, Dongguk University-Seoul,
30 Pildong-ro 1-gil, Jung-gu, Seoul 100-715, Republic of Korea
e-mail: bam@dongguk.edu