TAMKANG JOURNAL OF MATHEMATICS
Volume 25, Number 4, Winter 1994

REPRESENTATION OF PRIMES BY THE PRINCIPAL FORM OF NEGATIVE DISCRIMINANT Δ WHEN $h(\Delta)$ IS 4

KENNETH S. WILLIAMS * AND D. LIU

Abstract. Let Δ be a negative integer which is congruent to 0 or 1 (mod 4). Let $H(\Delta)$ denote the form class group of classes of positive-definite, primitive integral binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant Δ. If $H(\Delta)$ is a cyclic group of order 4, an explicit quartic polynomial $\rho_\Delta(x)$ of the form $x^4 - bx^2 + d$ with integral coefficients is determined such that for an odd prime p not dividing Δ, p is represented by the principal form of discriminant Δ if and only if the congruence $\rho_\Delta(x) \equiv 0 \pmod p$ has four solutions.

1. Notation and a preliminary result

Let Δ be a negative integer which is congruent to 0 or 1 (mod 4). Let $H(\Delta)$ denote the form class group of classes of positive-definite, primitive integral binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant Δ. It is well known that $H(\Delta)$ is a finite Abelian group. The order of $H(\Delta)$ is called the classnumber of forms of discriminant Δ and is denoted by $h(\Delta)$. The principal form of discriminant Δ is the form 1_Δ given by

$$1_\Delta = \begin{cases} (1, 0, -\Delta/4), & \text{if } \Delta \equiv 0 \pmod 4, \\ (1, 1, (1-\Delta)/4), & \text{if } \Delta \equiv 1 \pmod 4. \end{cases}$$

In this paper we are concerned with the representability of a prime by the principal form 1_Δ of discriminant Δ when $h(\Delta) = 4$.

Recent work of Steven Arno has determined all the imaginary quadratic fields with classnumber 4 [1: Theorem 7], namely, the 54 fields $Q(\sqrt{-n})$ with

$$\begin{aligned} n = {} & 14, 17, 21, 30, 33, 34, 39, 42, 46, 55, 57, 70, 73, 78, 82, 85, 93, 97, \\ & 102, 130, 133, 142, 155, 177, 190, 193, 195, 203, 219, 253, 259, 291, \\ & 323, 355, 435, 483, 555, 595, 627, 667, 715, 723, 763, 795, 955, \\ & 1003, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555. \end{aligned}$$

Received June 14, 1993.
1991 *Mathematics Subject Classification.* 11E16, 11R11, 11R29, 11R37.
Key words and phrases. Form class group, ideal class group, ring class field.
* Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

The complete list of all imaginary quadratic fields $Q(\sqrt{-n})$ with classnumber 1 or 2 has been known for some time:

$$h(-n) = 1: \quad n = 1, 2, 3, 7, 11, 19, 43, 67, 163 \quad \text{(9 fields)}$$
$$h(-n) = 2: \quad n = 5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427. \quad \text{(18 fields)}$$

From these results we can deduce

Proposition 1.1. *$h(\Delta) = 4$ if and only if $-\Delta$ has one of the following 84 values:*

$$39, 55, 56, 63, 68, 80, 84, 96, 120, 128, 132, 136, 144, 155, 156, 160, 168, 171, 180,$$
$$184, 192, 195, 196, 203, 208, 219, 220, 228, 240, 252, 256, 259, 275, 280, 288, 291,$$
$$292, 312, 315, 323, 328, 340, 352, 355, 363, 372, 387, 388, 400, 408, 435, 448, 475,$$
$$483, 507, 520, 532, 555, 568, 592, 595, 603, 627, 667, 708, 715, 723, 760, 763, 772,$$
$$795, 928, 955, 1003, 1012, 1027, 1227, 1243, 1387, 1411, 1435, 1467, 1507, 1555.$$

Proof. Let d be the discriminant of the imaginary quadratic field given uniquely by

$$\Delta = f^2 d,$$

where f is a positive integer. Then, by a formula of Gauss, we have

$$h(\Delta) = h(f^2 d) = h(d)\phi_d(f)/u,$$

where

$$\phi_d(f) = f \prod_{q|f} \left(1 - \left(\frac{d}{q}\right)\frac{1}{q}\right)$$

and

$$u = \begin{cases} 3, & \text{if } d = -3, \\ 2, & \text{if } d = -4, \\ 1, & \text{if } d < -4. \end{cases}$$

Note that q runs through the distinct primes dividing f and $\left(\frac{d}{q}\right)$ is the Kronecker symbol. As $\phi_d(f)/u$ is a positive integer, we see that

$$h(\Delta) = 4 \iff \begin{cases} (a) & h(d) = 4 & \text{and } \phi_d(f)/u = 1, & \text{or} \\ (b) & h(d) = 2 & \text{and } \phi_d(f)/u = 2, & \text{or} \\ (c) & h(d) = 1 & \text{and } \phi_d(f)/u = 4. \end{cases} \quad (1)$$

For case (a), we have $\phi_d(f) = 1$, which occurs if and only if $f = 1$ or $d \equiv 1 \pmod 8$ and $f = 2$. Then appealing to the list of imaginary quadratic fields with classnumber 4, we deduce that (a) occurs if and only if $-\Delta$ has one of the following 56 values:

$$39, 55, 56, 68, 84, 120, 132, 136, 155, 156, 168, 184, 195, 203, 219, 220, 228,$$
$$259, 280, 291, 292, 312, 323, 328, 340, 355, 372, 388, 408, 435, 483, 520, 532,$$
$$555, 568, 595, 627, 667, 708, 715, 723, 760, 763, 772, 795, 955, 1003, 1012,$$
$$1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555.$$

For case (b), we have $\phi_d(f) = 2$, which occurs if and only if $d \equiv 0 \pmod 4$ and $f = 2$ or $d \equiv 1 \pmod 8$ and $f = 4$ or $d \equiv 1 \pmod 3$ and $f = 3$. Then appealing to the list of imaginary quadratic fields with classnumber 2, we deduce that (b) occurs if and only if $-\Delta$ has one of the following 10 values:

$$80,\ 96,\ 160,\ 180,\ 208,\ 240,\ 315,\ 352,\ 592,\ 928.$$

For case (c), we consider the following three subcases: (c1): $d < -4$; (c2): $d = -4$; (c3): $d = -3$. For case (c1), we have $\phi_d(f) = 4$, which occurs if and only if

$$\begin{aligned}
d \equiv & 0 \pmod 4 \text{ and } f = 4 \text{ or} \\
d \equiv & 1, 4 \pmod 5 \text{ and } f = 5 \text{ or} \\
d \equiv & 2 \pmod 3 \text{ and } f = 3 \text{ or} \\
d = & -7 \text{ and } f = 6, 8 \text{ or} \\
d = & -8 \text{ and } f = 4, 6.
\end{aligned}$$

Then appealing to the list of imaginary quadratic fields with classnumber 1, we deduce that (c1) occurs if and only if $-\Delta$ has one of the following 11 values:

$$63, 128, 171, 252, 275, 288, 387, 448, 475, 603, 1467.$$

For case (c2), we have $\phi_{-4}(f)/2 = 4$, which occurs if and only if $f = 6, 7, 8$ or 10, that is if and only if $-\Delta$ has one of the following 4 values:

$$144, 196, 256, 400.$$

For case (c3), we have $\phi_{-3}(f)/3 = 4$, which occurs if and only if $f = 8, 11$ or 13, that is if and only if $-\Delta$ has one of the following 3 values:

$$192, 363, 507.$$

2. Introduction and a preliminary result

Gauss [2] showed that an odd prime p is represented by the quadratic form $x^2 + 64y^2$ (the principal form of discriminant -256) if and only if the congruence $x^4 - 2 \equiv 0 \pmod{p}$ has four solutions. In this paper we extend this result of Gauss to all negative discriminants Δ for which $H(\Delta) \simeq Z_4$ (see Theorem 4.1). The case $H(\Delta) \simeq Z_3$ was treated by K.S. Williams and R.H. Hudson [9].

Let K be an imaginary quadratic field, and let $\mathcal{O}_K$ denote the ring of algebraic integers of K. We define for any nonzero ideal $\mathcal{M}$ of $\mathcal{O}_K$ the group $I_K(\mathcal{M})$, and its subgroups $P_{K,1}(\mathcal{M})$ and $P_{K,Z}(\mathcal{M})$, by

$I_K(\mathcal{M})$ = group of all fractional $\mathcal{O}_K$-ideals which are relatively prime to $\mathcal{M}$,

$P_{K,1}(\mathcal{M})$ = subgroup of $I_K(\mathcal{M})$ generated by principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv 1 \pmod{\mathcal{M}}$,

$P_{K,Z}(\mathcal{M})$ = subgroup of $I_K(\mathcal{M})$ generated by principal ideals $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K$ and $\alpha \equiv a \pmod{\mathcal{M}}$ for some integer a coprime with $\mathcal{M}$.

If $\mathcal{M} = \alpha\mathcal{O}_K$ we write $I_K(\alpha)$ for $I_K(\alpha\mathcal{O}_K)$, $P_{K,Z}(\alpha)$ for $P_{K,Z}(\alpha\mathcal{O}_K)$, and $P_{K,1}(\alpha)$ for $P_{K,1}(\alpha\mathcal{O}_K)$. Let f be a positive integer and let $\mathcal{O}_f$ denote the order of conductor f in a quadratic field K. We also let $C(\mathcal{O}_f)$ denote the ideal class group of the order $\mathcal{O}_f$ and $F_f(K)$ the ring class field of the order $\mathcal{O}_f$. The genus field of the ring class field $F_f(K)$ is denoted by $K(f)$ and is the largest subfield of $F_f(K)$ such that $K(f)$ is an Abelian extension of Q.

Theorem 2.1. *Let $\Delta \equiv 0, 1 \pmod 4$ be a negative integer. Set $K = Q(\sqrt{\Delta})$. Let N be a subgroup of $H(\Delta)$. Then there exists a unique dihedral extension M of Q such that if p is unramified in M then p is represented by a form in N if and only if p splits completely in M. In particular, p is represented by the principal form 1_Δ if and only if p splits completely in $F_f(K)$, where $f = \sqrt{\Delta/d_K}$.*

Proof. As $\Delta \equiv 0, 1 \pmod 4$, there is a positive integer f such that $\Delta = d_K f^2$, where d_K denotes the discriminant of K. We have the isomorphisms

$$H(\Delta) \simeq C(\mathcal{O}_f) \simeq I_K(f)/P_{K,Z}(f).$$

Under the above isomorphisms, as $N \subset H(\Delta)$, there exists a unique subgroup H with

$$P_{K,Z}(f) \subset H \subset I_K(f) \tag{2}$$

such that $N \simeq H/P_{K,Z}(f)$. By the existence theorem of class field theory, (2) determines a unique Abelian extension M of K such that

$$I_K(f)/H \simeq Gal(M/K).$$

Further, we have that

$$Gal(M/K) \simeq I_K(f)/H \simeq (I_K(f)/P_{K,Z}(f))/(H/P_{K,Z}(f)) \simeq H(\Delta)/N.$$

Now appealing to [5: Theorem 3.6], the assertion of the theorem follows. In particular, if $N = \{1_\Delta\}$, then we have $M = F_f(K)$ so that the last assertion of the theorem follows.

For $h(\Delta) = 4$, as $H(\Delta)$ is either a Klein-4 group or a cyclic-4 group, we have the following result.

Theorem 2.2. *Suppose $h(\Delta) = 4$. Set $K = Q(\sqrt{\Delta})$ and let $f = \sqrt{\Delta/d_K}$.*

(i) *If $H(\Delta) \simeq Z_2 \times Z_2$, then $F_f(K)$ is the composite field of its three quadratic fields, say, k, k' and k'', so that for a prime p not dividing Δ,*

$$p \quad \text{is represented by } 1_\Delta \Longleftrightarrow \left(\frac{d_k}{p}\right) = \left(\frac{d_{k'}}{p}\right) = \left(\frac{d_{k''}}{p}\right) = 1.$$

(ii) *If $H(\Delta) \simeq Z_4$, then there is an irreducible quartic $\rho(x) = x^4 - bx^2 + d \in Z[x]$ such that $F_f(K)$ is the splitting field of $\rho(x)$ so that, for an odd prime p not dividing disc(ρ),*

$$p \quad \text{is represented by } 1_\Delta \Longleftrightarrow \begin{cases} \left(\frac{d_K}{p}\right) = 1 \text{ and } \rho(x) \equiv 0 \pmod{p} \\ \text{has a solution,} \end{cases} \tag{3}$$

$$\Longleftrightarrow \left(\frac{d}{p}\right) = \left(\frac{b^2 - 4d}{p}\right) = \left(\frac{(b + \sqrt{b^2 - 4d})/2}{p}\right) = 1, \tag{4}$$

$$\Longleftrightarrow \left(\frac{d}{p}\right) = \left(\frac{b^2 - 4d}{p}\right) = \left(\frac{b + 2\sqrt{d}}{p}\right) = 1, \tag{5}$$

$$\Longleftrightarrow v_{(p-1)/2} \equiv 2 \pmod{p}, \tag{6}$$

where the $v_n (n = 0, 1, 2, \ldots)$ are given by the recurrence relation

$$v_{n+2} = bv_{n+1} - dv_n, \quad v_0 = 2, \quad v_1 = b.$$

Proof. For the case (i), as $F_f(K)$ is the composite field of the fields k, k' and k'', p splits completely in $F_f(K)$ if and only if p splits completely in all the three quadratic fields. Then the assertion of the theorem follows from the last assertion of Theorem 2.1. For the case (ii), as $Gal(F_f(K)/K) \simeq H(\Delta)$, we have $Gal(F_f(K)/K)$ is a cyclic group of order 4 so that $Gal(F_f(K)/Q) \simeq D_4$. By [5: Lemma 2.4] and [7: Theorem 4.2], the quartic $\rho(x)$ stated in the theorem exists. Now we prove the assertion (3). As $F_f(K)$ is the splitting field of $\rho(x)$, we have, for a prime p not dividing disc(ρ), that p splits completely in M if and only if the congruence

$$x^4 - bx^2 + d \equiv 0 \pmod{p}$$

has four solutions. Then the assertion (3) follows from [8: Theorem 2.16 (i)]. The assertions (4), (5) and (6) follow from [8: Theorem 2.1, Lemma 2.4 and Lemma 2.3] respectively.

For the case $H(\Delta) \simeq Z_2 \times Z_2$, as $F_f(K) = K(f)$, applying [6: Theorem 4.1] we have no difficulty in determining k, k' and k''. The following table gives all the 34 discriminants satisfying Theorem 2.2(i).

Δ	d_k	$d_{k'}$	$d_{k''}$	Δ	d_k	$d_{k'}$	$d_{k''}$
-84	-4	-3	-7	-96	-4	8	-3
-120	8	-3	5	-132	8	-3	-11
-160	-4	8	5	-168	-8	-3	-7
-180	-4	-3	5	-192	-4	8	-3
-195	-3	5	13	-228	8	-3	-19
-240	-4	-3	5	-280	8	5	-7
-288	-4	8	-3	-312	8	-3	13
-315	-3	5	-7	-340	-4	5	17
-352	-4	8	-11	-372	8	-3	-31
-408	8	-3	17	-435	-3	5	29
-448	-4	8	-7	-483	-3	-7	-23
-520	-8	5	13	-532	8	-7	-19
-555	-3	5	37	-595	5	-7	17
-627	-3	-11	-19	-708	8	-3	-59
-715	5	-11	13	-760	8	5	-19
-795	-3	5	53	-928	-4	-8	29
-1012	8	-11	-23	-1435	5	-7	41

3. Determination of $\rho(x)$ when $H(\Delta) \simeq Z_4$

In order to apply Theorem 2.2 (ii), for each $\Delta = df^2$, where d is a fundamental discriminant, we have to determine a quartic $\rho(x) = x^4 - bx^2 + d \in Z[x]$ such that the ring class field $F_f(Q(\sqrt{d}))$ is the splitting field of $\rho(x)$. We divide the remaining 50 values of Δ into nine sets as follows:

(A) $-\Delta = 39, 55, 155, 156, 203, 219, 220, 259, 291, 323, 355, 667, 723, 763, 955,$
$1003, 1027, 1227, 1243, 1387, 1411, 1507, 1555$ (see Lemma 3.2)
(B) $-\Delta =$ 63, 171, 252, 387, 603, 1467(see Lemma 3.3)
(C) $-\Delta =$ 68, 292, 388, 772(see Lemma 3.4)
(D) $-\Delta =$ 80, 208, 592(see Lemma 3.5)
(E) $-\Delta =$ 56, 136, 184, 328, 568(see Lemma 3.6)
(F) $-\Delta =$ 363, 507(see Lemma 3.7)
(G) $-\Delta =$ 144, 196, 256, 400(see Lemma 3.8)
(H) $-\Delta =$ 275, 475(see Lemma 3.9)
(I) $-\Delta =$ 128(see Lemma 3.10)

Lemma 3.1. *Let M be a dihedral extension with $Gal(M/Q) \simeq D_4$. Let K be the unique quadratic field in M such that $Gal(M/K) \simeq Z_4$, and let k be a quadratic* *field in M different from K. Let $K = Q(\sqrt{D})$, $k = Q(\sqrt{d})$, where both D and d are squarefree. Then there are nonzero integers a, b, c with $gcd(a, b)$ squarefree such that $c^2 D = (a^2 - b^2 d)d$.*

Proof. As $\mathrm{Gal}(M/Q) \simeq D_4$, there is a quartic field in M containing k such that the normal closure of L is M. As $[L : k] = 2$, there are integers a, b with $\gcd(a, b)$ squarefree such that $L = Q(\sqrt{a + b\sqrt{d}})$. It is clear that $\sqrt{a + b\sqrt{d}}$ is a root of $f(x) = x^4 - 2ax^2 + a^2 - b^2 d$ and M is the splitting field of $f(x)$. By [7: Lemma 3.3], we have $K = Q(\sqrt{D}) = Q(\sqrt{(a^2 - b^2 d)d})$. As D is squarefree, there is an integer c such that $c^2 D = (a^2 - b^2 d)d$.

Lemma 3.2. *Let p_1 and p_2 be two primes with $p_1 \equiv 3 \pmod 4$, $p_2 \equiv 1 \pmod 4$. Let $K = Q(\sqrt{-p_1 p_2})$. Then $h(-p_1 p_2) \equiv 0 \pmod 4$ if and only if there are integers a, b and c such that*

$$c^2 p_2 = a^2 + b^2 p_1,$$

where a and b satisfy

$$\gcd(a, b) = \gcd(a, b, p_1 p_2), a \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2, a + b \equiv 1 \pmod 4. \quad (1)$$

Further, if $h(-p_1 p_2) \equiv 0 \pmod 4$, set

$$\rho(x) = (x^2 - a)^2 + p_1 b^2 = x^4 - 2ax^2 + c^2 p_2,$$

where a and b are given as above. Then the splitting field M of $\rho(x)$ over Q satisfies

$$K \subset M \subset F_1(K).$$

In particular, if $h(-p_1 p_2) = 4$ then $M = F_1(K)$.

Proof. By [6: Theorem 4.1], the ring class field $F_1(K)$ of K contains the genus field

$$K(1) = Q(\sqrt{-p_1}, \sqrt{p_2}).$$

This implies that the 2-part of $\mathrm{Gal}(F_1(K)/K)$ is a cyclic group of order 2^r, $r \geq 1$. Now suppose that $h(\mathcal{O}_K) \equiv 0 \pmod 4$. By Galois theory there is an extension $K \subset K(1) \subset M \subset F_1(K)$ with $\mathrm{Gal}(M/K) \simeq Z_4$. Let $k = Q(\sqrt{-p_1})$. By Lemma 3.1, there are integers a, b, c with $\gcd(a, b)$ squarefree such that $p_2 c^2 = a^2 + b^2 p_1$. Set

$$\rho(x) = (x^2 - a)^2 + p_1 b^2 = x^4 - 2ax^2 + c^2 p_2,$$

Then M is the splitting field of $\rho(x)$ and M contains $L = k(\sqrt{a + b\sqrt{-p_1}})$. By [3: Theorem 2], we have

$$d_L = 2^e p_1^2 p_2 \Big(\frac{(a, b)}{(a, b, p_1 p_2)} \Big)^2, \quad (2)$$

where e is an even integer given by [3: TABLES C and D]. On the other hand, by [6: Theorem 3.12], we have

$$d_L = d_k d_K f_0(M/K)^2 = p_1^2 p_2 f_0(M/K)^2, \tag{3}$$

where $f_0(M/K)$ denotes the finite part of the conductor of the extension M/K. Hence we obtain

$$f_0(M/K) = 2^{e/2}\Big(\frac{(a,b)}{(a,b,p_1p_2)}\Big).$$

Noting that as $M \subset F_1(K)$, we have, by [5: Theorem 3.9], that $f_0(M/K) = 1$ so that $e = 0$ and $\gcd(a,b) = \gcd(a,b,p_1p_2)$. By [3: TABLES C and D], we obtain the condition (1).

Conversely, suppose that the conditions involving a and b of the lemma are satisfied. Set $\rho(x) = (x^2-a)^2 + p_1b^2$. Let M be the splitting field of $\rho(x)$ so that $\mathrm{Gal}(M/Q) \simeq D_4$ and $\mathrm{Gal}(M/K) \simeq Z_4$. Let $k = Q(\sqrt{-p_1})$, $L = Q(\sqrt{a+b\sqrt{-p_1}})$. By [3: Theorem 2], we have

$$d_L = p_1^2 p_2.$$

and then, by (3), we have $f_0(M/K) = 1$ so that $M \subset F_1(K)$, which implies that $h(-p_1p_2) \equiv 0 \pmod 4$.

Lemma 3.3. *Let $K = Q(\sqrt{-p})$, where $p = 7, 19, 43, 67, 163$ so that $h(\mathcal{O}_3) = 4$. There are integers a and b such that $p = a^2 + 3b^2$ and*

$$b \equiv \begin{cases} 3 \pmod 4), & \text{if } a \equiv 0 \pmod 4), \\ 1 \pmod 4), & \text{if } a \equiv 2 \pmod 4), \end{cases} \tag{4}$$

Set $\rho(x) = x^4 - 6b^2x^2 + 3p$. Then $F_3(K)$ is the splitting field of $\rho(x)$.

Proof. As $p \equiv 1 \pmod 3$, there are integers a and b such that $p = a^2+3b^2$. Modulo 4 we obtain $a \equiv 0 \pmod 2$, $b \equiv 1 \pmod 2$. Replacing b by $-b$ if necessary we obtain (4). Let M be the splitting field of $\rho(x)$. By [4: Theorem 3], $\mathrm{Gal}(M/Q) \simeq D_4$. By [7: Lemma 3.3], M contains $k = Q(\sqrt{-3})$ and K, and $\mathrm{Gal}(M/K) \simeq Z_4$. Let $L = k(\sqrt{3b + a\sqrt{-3}})$. As $\sqrt{3b+a\sqrt{-3}}$ is a root of $\rho(x)$, M is the normal closure of L. Now by [6: Theorem 3.12],

$$d_L = d_k d_K f_0(M/K)^2 = 3p f_0(M/K)^2.$$

By [3: Theorem 2], we have

$$d_L = 3^3 p,$$

so that $f_0(M/K) = 3$. Finally, by [5: Theorem 3.9], we obtain $M = F_3(K)$.

Lemma 3.4. *Let p be a prime which is congruent to 1 modulo 4. Set $K = Q(\sqrt{-p})$. Then*

$$h(\mathcal{O}_K) \equiv 0 \pmod 4) \text{ if and only if } p \equiv 1 \pmod 8). \tag{5}$$

Further, if $p \equiv 1 \pmod 8$, then p can be expressed in the form

$$p = a^2 + b^2,$$

where $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$. Set

$$\rho(x) = x^4 - 2ax^2 + p.$$

Then the splitting field M of $\rho(x)$ over Q satisfies

$$K \subset M \subset F_1(K).$$

In particular, if $h(\mathcal{O}_K) = 4$ then $M = F_1(K)$.

Proof. By [6: Theorem 4.1], the Hilbert class field $F_1(K)$ of K contains

$$K(1) = Q(\sqrt{-1}, \sqrt{p}).$$

This implies that the 2-rank of $\mathrm{Gal}(F_1(K)/K)$ is 1, so that $h(\mathcal{O}_K) \equiv 0 \pmod 2$. Further, suppose that $h(\mathcal{O}_K) \equiv 0 \pmod 4$. Then $F_1(K)$ contains a 4-cyclic extension M of K. It is obvious that $K(1) \subset M$. Set $k = Q(\sqrt{-1})$. By Lemma 3.1, there are integers a, b, c with $\gcd(a, b)$ squarefree such that $pc^2 = a^2 + b^2$. Set

$$\rho(x) = (x^2 - a)^2 + b^2 = x^4 - 2ax^2 + c^2 p.$$

Then M is the splitting field of $\rho(x)$ and M contains $L = k(\sqrt{a + b\sqrt{-1}})$. By [3: Theorem 2], we have

$$d_L = 2^e p \Big(\frac{(a,b)}{(a,b,p)} \Big)^2. \tag{6}$$

On the other hand, by [6: Theorem 3.12], we have

$$d_L = d_k d_K f_0(M/K)^2 = 2^4 p f_0(M/K)^2, \tag{7}$$

Hence we obtain

$$f_0(M/K) = 2^{(e-4)/2} \Big(\frac{(a,b)}{(a,b,p)} \Big).$$

Noting that as $M \subset F_1(K)$, we have, by [5: Theorem 3.9], that $f_0(M/K) = 1$ so that $e = 4$ and $\gcd(a, b) = \gcd(a, b, p)$. This, by [3: TABLE B], implies $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 4$ so that $p \equiv 1 \pmod 8$.

Conversely, suppose $p \equiv 1 \pmod 8$. Then there are integers a, b with $b \equiv 0 \pmod 4$ such that $p = a^2 + b^2$. Set $\rho(x) = (x^2 - a)^2 + b^2$. Let M be the splitting field of $\rho(x)$ so that $\mathrm{Gal}(M/Q) \simeq D_4$ and $\mathrm{Gal}(M/K) \simeq Z_4$. Let $k = Q(\sqrt{-1})$, $L = Q(\sqrt{a + b\sqrt{-1}})$. By [3: TABLE B] we have

$$d_L = 2^4 p.$$

Then, by (7), we have $f_0(M/K) = 1$ so that $M \subset F_1(K)$, which implies that $h(d_K) \equiv 0 \pmod 4$.

Lemma 3.5. *Let p be a prime which is congruent to 5 modulo 8 so that there are integers a, b such that*

$$p = a^2 + b^2, \quad a \equiv 1 \pmod 2, \quad b \equiv 2 \pmod 4.$$

Set $K = Q(\sqrt{-p})$. Then $h(\mathcal{O}_2) \equiv 4 \pmod 8$. Set

$$\rho(x) = x^4 - 2ax^2 + p.$$

Then the splitting field M of $\rho(x)$ over Q satisfies

$$K \subset M \subset F_2(K).$$

In particular, if $h(\mathcal{O}_2) = 4$ then $M = F_2(K)$.

Proof. By Lemma 3.4, we have $h(O_K) \equiv 2 \pmod 4$. Then appealing to Gauss's formula, $h(O_2) = 2h(O_K) \equiv 4 \pmod 8$.

Let M be the splitting field of $\rho(x)$, let $k = Q(\sqrt{-1})$, $L = k(\sqrt{a + b\sqrt{-1}})$. By [3: Theorem 2], we have

$$d_L = 2^6 p. \tag{8}$$

On the other hand, by [6: Theorem 3.12], we have

$$d_L = d_k d_K f_0(M/K)^2 = 2^4 p f_0(M/K)^2. \tag{9}$$

where $f_0(M/K)$ denotes the finite part of the conductor of the extension M/K. Hence we obtain $f_0(M/K) = 2$ so that, by [5: Theorem 3.9], $M \subset F_2(K)$.

Lemma 3.6 *Let p be an odd prime and let $K = Q(\sqrt{-2p})$. Then*

$$h(\mathcal{O}_K) \equiv \begin{cases} 2 \pmod 4, & \text{if } \left(\frac{2}{p}\right) = -1, \\ 0 \pmod 4, & \text{if } \left(\frac{2}{p}\right) = 1. \end{cases}$$

Further, suppose that $\left(\frac{2}{p}\right) = 1$, that is, $p = \pm 1 \pmod 8$. Then p can be expressed in the form

$$p = \begin{cases} -a^2 + 2b^2, & \text{if } p \equiv -1 \pmod 8, \\ a^2 + 2b^2, & \text{if } p \equiv 1 \pmod 8, \end{cases}$$

where the integers a and b satisfy

$$a \equiv \begin{cases} 1 \pmod 4, & \text{if } b \equiv 0 \pmod 4, \\ -1 \pmod 4, & \text{if } b \equiv 2 \pmod 4. \end{cases} \tag{10}$$

Set

$$\rho(x) = \begin{cases} (x^2-a)^2 - 2b^2 = x^4 - 2ax^2 - p, & \text{if } p \equiv -1 \pmod 8, \\ (x^2-a)^2 + 2b^2 = x^4 - 2ax^2 + p, & \text{if } p \equiv 1 \pmod 8. \end{cases} \tag{11}$$

Then the splitting field M of $\rho(x)$ over Q satisfies

$$K \subset M \subset F_1(K).$$

In particular, if $h(\mathcal{O}_K) = 4$ then $M = F_1(K)$.

Proof. We just treat the case when $p \equiv 1 \pmod 4$. The case when $p \equiv 3 \pmod 4$ can be handled similarly. By [6: Theorem 4.1] the Hilbert class field $F_1(K)$ contains the genus field

$$K(1) = Q(\sqrt{-2}, \sqrt{p}),$$

so that $[K(1) : K] = 2$. This implies that the 2-rank of $\mathrm{Gal}(F_1(K)/K)$ is 1, so that $h(\mathcal{O}_K) \equiv 0 \pmod 2$. We now show that

$$h(\mathcal{O}_K) \equiv 0 \pmod 4 \text{ if and only if } p \equiv 1 \pmod 8.$$

Suppose first that $h(\mathcal{O}_K) \equiv 0 \pmod 4$. Then $F_1(K)$ contains a cyclic-4 extension M of K. It is obvious that $K(1) \subset M$. Set $k = Q(\sqrt{-2})$. By Lemma 3.1, there are integers a, b, c such that $c^2 p = a^2 + 2b^2$ so that $p \equiv 1 \pmod 8$.

Conversely, suppose that $p \equiv 1 \pmod 8$. Then there are integers a, b satisfying (10) such that $p = a^2 + 2b^2$. Set $k = Q(\sqrt{-2})$. Set

$$\rho(x) = x^4 - 2ax + p.$$

Let M be the splitting field of $\rho(x)$ so that $\mathrm{Gal}(M/Q) \simeq D_4$. Let $k = Q(\sqrt{-2})$ and let $L = Q(\sqrt{a + b\sqrt{-2}})$ so that M is the normal closure of L. By [7: Theorem 3.12],

$$d_L = d_K d_k f_0(M/K)^2 = -2^6 p f_0(M/K)^2.$$

On the other hand, as a and b satisfy (10), from [3: TABLE A] we have

$$d_L = -2^6 p,$$

so that $f_0(M/K) = 1$. Thus, the extension $K \subset M$ is unramified, so that $M \subset F_1(K)$, which implies $h(\mathcal{O}_K) \equiv 0 \pmod 4$. In particular, if $h(\mathcal{O}_K) = 4$, then $M = F_1(K)$.

Lemma 3.7. *Let $K = Q(\sqrt{-3})$ and $f = 11, 13$. Set*

$$\rho_f(x) = \begin{cases} x^4 - 22x^2 + 297, & \text{if } f = 11, \\ x^4 - 36x^2 - 39, & \text{if } f = 13. \end{cases}$$

Then the splitting field of $\rho_f(x)$ is $F_f(K)$.

Proof. We just prove the result when $f = 13$. The case when $f = 11$ can be treated similarly. Let M be the splitting field of $\rho_f(x)$. Let $k = Q(\sqrt{13})$, $L = Q(\sqrt{13+4\sqrt{13}})$. By [7: Theorem 3.12],

$$d_L = d_K d_k f_0(M/K)^2 = -39 f_0(M/K)^2.$$

On the other hand, by [3: Theorem 2]

$$d_L = -39 \cdot 13^2,$$

so that $f_0(M/K) = 13$. By [5: Theorem 3.9], $M = F_{13}(K)$.

Lemma 3.8. *Let $K = Q(\sqrt{-4})$ and $f = 6, 7, 8, 10$. Set*

$$\rho_f(x) = \begin{cases} x^4+3, & \text{if } f=6,\\ x^4+7, & \text{if } f=7,\\ x^4-2, & \text{if } f=8,\\ x^4-5, & \text{if } f=10.\end{cases}$$

Then the splitting field of $\rho_f(x)$ is $F_f(K)$.

Proof. We just prove the result when $f = 6$. The other cases can be treated similarly. Let M be the splitting field of $\rho_f(x)$. Let $k = Q(\sqrt{-3})$, $L = Q(\sqrt[4]{-3})$. By [7: Theorem 3.12],

$$d_L = d_K d_k f_0(M/K)^2 = 12 f_0(M/K)^2.$$

On the other hand, by [3: Theorem 2]

$$d_L = 2^4 \cdot 3^3,$$

so that $f_0(M/K) = 6$. By [5: Theorem 3.9], $M = F_6(K)$.

Lemma 3.9. *Let $K = Q(\sqrt{d})$, where $d = -11$ or -19. Set*

$$\rho(x) = \begin{cases} x^4-10x^2-55, & \text{if } d=-11,\\ x^4+30x^2-95, & \text{if } d=-19.\end{cases}$$

Then the splitting field of $\rho(x)$ is $F_5(K)$.

Proof. We just prove the result when $K = Q(\sqrt{-11})$. The case when $K = Q(\sqrt{-19})$ can be treated similarly. Let M be the splitting field of $\rho(x)$. Let $k = Q(\sqrt{5})$, $L = Q(\sqrt{5+4\sqrt{5}})$. By [7: Theorem 3.12],

$$d_L = d_K d_k f_0(M/K)^2 = -11 \cdot 5 f_0(M/K)^2.$$

On the other hand, by [3: TABLE C]

$$d_L = -11 \cdot 5^3,$$

so that $f_0(M/K) = 5$. By [5: Theorem 3.9], $M = F_5(K)$.

Lemma 3.10. *Let $K = Q(\sqrt{-8})$. Set $\rho(x) = x^4 - 2x^2 + 2$. Then the splitting field of $\rho(x)$ is $F_4(K)$.*

Proof. Let M be the splitting field of $\rho(x)$. Let $k = Q(\sqrt{-1})$, $L = Q(\sqrt{1+\sqrt{-1}})$. By [7: Theorem 3.12],

$$d_L = d_K d_k f_0(M/K)^2 = 2^5 f_0(M/K)^2.$$

On the other hand, by [3: Theorem 2]

$$d_L = 2^9,$$

so that $f_0(M/K) = 4$. By [5: Theorem 3.9], $M = F_4(K)$.

4. The main result

Appealing to Theorem 2.2 and Lemmas 3.2-3.10, we obtain the following result.

Theorem 4.1. *Let Δ be one of the 50 discriminants such that $h(\Delta) = 4$ and $H(\Delta) \simeq Z_4$. Then the prime p $(p > 3, p \nmid \Delta)$ is represented by the principal form 1_Δ of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = +1$ and $\rho_\Delta(x)$ is congruent to the product of four distinct linear polynomials (mod p), where $\rho_\Delta(x)$ is the monic biquadratic polynomial with integral coefficients listed in the following table.*

Table

Δ	ρ_Δ	Δ	ρ_Δ
39	$x^4 + 2x^2 + 13$	55	$x^4 + 2x^2 + 45$
56	$x^4 + 2x^2 - 7$	63	$x^4 + 6x^2 + 21$
68	$x^4 - 2x^2 + 17$	80	$x^4 - 2x^2 + 5$
128	$x^4 - 2x^2 + 2$	136	$x^4 - 6x^2 + 17$
144	$x^4 + 3$	155	$x^4 + 2x^2 + 125$
156	$x^4 + 2x^2 + 13$	171	$x^4 + 6x^2 + 57$
184	$x^4 + 6x^2 - 23$	196	$x^4 + 7$
203	$x^4 + 2x^2 + 29$	208	$x^4 - 6x^2 + 13$
219	$x^4 - 10x^2 + 73$	220	$x^4 + 2x^2 + 45$
252	$x^4 + 6x^2 + 21$	256	$x^4 - 2$
259	$x^4 - 6x^2 + 37$	275	$x^4 - 10x^2 - 55$
291	$x^4 + 14x^2 + 97$	292	$x^4 + 6x^2 + 73$
323	$x^4 + 22x^2 + 425$	328	$x^4 + 6x^2 + 41$
355	$x^4 - 22x^2 + 405$	363	$x^4 - 22x^2 + 297$
387	$x^4 - 18x^2 + 129$	388	$x^4 - 18x^2 + 97$

400	$x^4 - 5$	475	$x^4 + 30x^2 - 95$
507	$x^4 - 36x^2 - 39$	568	$x^4 + 2x^2 - 71$
592	$x^4 - 2x^2 + 37$	603	$x^4 + 6x^2 + 201$
667	$x^4 + 26x^2 + 261$	723	$x^4 + 14x^2 + 241$
763	$x^4 + 18x^2 + 109$	772	$x^4 + 14x^2 + 193$
955	$x^4 + 18x^2 + 845$	1003	$x^4 + 14x^2 + 3825$
1027	$x^4 - 6x^2 + 325$	1227	$x^4 + 38x^2 + 409$
1243	$x^4 + 6x^2 + 2825$	1411	$x^4 + 14x^2 + 1377$
1387	$x^4 + 78x^2 + 1825$	1467	$x^4 - 42x^2 + 489$
1507	$x^4 + 46x^2 + 1233$	1555	$x^4 - 62x^2 + 2205$

References

[1] Steven Arno, "The imaginary quadratic fields of class number 4," *Acta Arith.*, 60 (1992), 321-334.

[2] C. F. Gauss, "Theoria Residuorum Biquadraticorum," *Commentatio Prima, in Werke,* II (1876), 65-92.

[3] J. G. Huard, B. K. Spearman and K. S. Williams, "Integral bases for quartic fields with quadratic subfields," *Carleton-Ottawa Mathematical Lecture Note Series*, Number 4, June 1991.

[4] L-C. Kappe and B. Warren, "An elementary test for the Galois group of a quartic polynomial," *Amer. Math. Monthly*, 96 (1989), 133-137.

[5] D. Liu, "Dihedral polynomial congruences and binary quadratic forms," submitted for publication.

[6] D. Liu, "Evaluation of the conductor $f_0(M/K) - II$," submitted for publication.

[7] D. Liu, "Some properties of dihedral polynomials," submitted for publication.

[8] D. Liu, "Evaluation of the Legendre symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$," submitted for publication.

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

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada, K1S 5B6.