RING CLASS FIELDS AND A RESULT OF HASSE

RON EVANS, FRANZ LEMMERMEYER, ZHI-HONG SUN, AND MARK VAN VEEN

ABSTRACT. For squarefree $d > 1$, let M denote the ring class field for the order $\mathbb{Z}[\sqrt{-3d}]$ in $F = \mathbb{Q}(\sqrt{-3d})$. Hasse proved that 3 divides the class number of F if and only if there exists a cubic extension E of $\mathbb{Q}$ such that E and F have the same discriminant. Define the real cube roots $v = (a + b\sqrt{d})^{1/3}$ and $v' = (a - b\sqrt{d})^{1/3}$, where $a + b\sqrt{d}$ is the fundamental unit in $\mathbb{Q}(\sqrt{d})$. We prove that E can be taken as $\mathbb{Q}(v + v')$ if and only if $v \in M$. As byproducts of the proof, we give explicit congruences for a and b which hold if and only if $v \in M$, and we also show that the norm of the relative discriminant of $F(v)/F$ lies in $\{1, 3^6\}$ or $\{3^8, 3^{18}\}$ according as $v \in M$ or $v \notin M$. We then prove that v is always in the ring class field for the order $\mathbb{Z}[\sqrt{-27d}]$ in F. Some of the results above are extended for subsets of $\mathbb{Q}(\sqrt{d})$ properly containing the fundamental units $a + b\sqrt{d}$.

1. INTRODUCTION

Write $u = a + b\sqrt{d}$ for the fundamental unit in $\mathbb{Q}(\sqrt{d})$, where $d > 1$ is squarefree. Define the real cube roots $v = (a + b\sqrt{d})^{1/3}$ and $v' = (a - b\sqrt{d})^{1/3}$. Note that $vv' = \pm 1$. Write $t = v + v'$ and $F = \mathbb{Q}(\sqrt{-3d})$. Let M denote the ring class field for the order $\mathbb{Z}[\sqrt{-3d}]$ in F. For number field extensions K/k, write $D(K/k)$ for the relative discriminant and $D(K)$ for the discriminant.

In [5], Hasse proved that 3 divides the class number of F if and only if there exists a cubic extension E of $\mathbb{Q}$ such that $D(E) = D(F)$. When $v \in M$, we prove in Theorems 1.1 and 1.2 below that E can be taken to be $\mathbb{Q}(t)$. Theorems 1.1 and 1.2 address the cases $3 \nmid d$ and $3 \mid d$, respectively. They are proved in Sections 2 and 3.

Theorem 1.1. *Suppose that $3 \nmid d$ and $v \in M$. Then the fields $E = \mathbb{Q}(t)$ and F have the same discriminant.*

Theorem 1.2. *Suppose that $3 \mid d$ and $v \in M$. Then the fields $E = \mathbb{Q}(t)$ and F have the same discriminant.*

Remarks (2A) and (3B) show that $v \in M$ implies that 3 divides the class number of F. However, the converse is false; the smallest counterexample when $3 \nmid d$ is $d = 142$, while the smallest counterexample when $3 \mid d$ is $d = 786$. See [7, 8, 9, 13] for examples of infinite families of d for which 3 divides the class number of F.

When $v \notin M$, then in contrast with the theorems above, the discriminant of $\mathbb{Q}(t)$ does not equal $D(F)$. In fact, when $v \notin M$, Theorems 1.3 and 1.4 show that $D(\mathbb{Q}(t))$ equals $9D(F)$ or $81D(F)$ according as $3 \nmid d$ or $3 \mid d$. The proofs are given in Sections 4 and 5.

Date: April 2024.

2020 *Mathematics Subject Classification.* 11R11, 11R27, 11R29, 11R37.

Key words and phrases. ring class fields, fundamental units, class number, relative discriminants, Artin symbol, cubic residuacity.

Theorem 1.3. *Suppose that $3 \nmid d$ and $v \notin M$. Then the field $E = \mathbb{Q}(t)$ has discriminant $9D(F)$.*

Theorem 1.4. *Suppose that $3 \mid d$ and $v \notin M$. Then the field $E = \mathbb{Q}(t)$ has discriminant $81D(F)$.*

The four proofs will use the following notation: $w = (-1+\sqrt{-3})/2$, $C = \mathbb{Q}(\sqrt{d})$, $B = \mathbb{Q}(\sqrt{-3}, \sqrt{d}) = F(\sqrt{d}) = F(w)$, $k = \mathbb{Q}(t)$, $K = \mathbb{Q}(v) = k(\sqrt{d})$, and $L = F(v) = \mathbb{Q}(w, v) = K(w)$. Note that $|L : B| = |K : C| = |k : \mathbb{Q}| = |F(t) : F| = 3$. We remark in passing that by the Scholz reflection principle, 3 divides the class number of F whenever 3 divides the class number of C [1, Theorem 5]. The Galois extension L/F is cyclic of degree 6; to see this, observe that the automorphism given by

$$v \to v'\bar{w},\ w \to \bar{w},\ \sqrt{d} \to\ -\sqrt{d} \tag{1.1}$$

is a generator of $\mathrm{Gal}(L/F)$ of order 6. This automorphism along with complex conjugation generate the non-abelian group $\mathrm{Gal}(L/\mathbb{Q})$.

As a byproduct of the proofs, Theorem 1.5 gives an evaluation of the norm of $D(L/F)$. For a generalization, see Conjecture 7.7.

Theorem 1.5. *When $v \in M$, the norm of $D(L/F)$ equals 1 or 3^6 according as $3 \nmid d$ or $3 \mid d$; and when $v \notin M$, the norm of $D(L/F)$ equals 3^8 or 3^{18} according as $3 \nmid d$ or $3 \mid d$.*

Proof. See Remarks (2A), (3D), (4F), and (5G), respectively. □

The inclusion $v \in M$ is connected to cubic residuacity of $u = a + b\sqrt{d} \pmod p$, where p is any prime of the form $p = x^2 + 3dy^2$. This is shown in Theorem 1.6 below.

When $d = 2$, we have $\left(\frac{d}{p}\right) = 1$. When d is odd, one of d, p is 1 (mod 4), so that $\left(\frac{d}{p}\right) = \left(\frac{p}{d}\right) = 1$. Thus d is a square (mod p), so that $u = a + b\sqrt{d}$ can be viewed as a rational integer $u_p \pmod p$. For example, if $d \equiv c^2 \pmod p$ for some integer c, then $u_p = a \pm bc \pmod p$. The choice of sign does not affect whether or not u_p is a cubic residue (mod p), since $a^2 - b^2 d = \pm 1$ is a cube.

Theorem 1.6. *$v \in M$ if and only if u_p is a cubic residue mod the primes $p = x^2 + 3dy^2$.*

Proof. Consider the principal prime ideal $\mathfrak{p} = (x + y\sqrt{-3d})$ in F of norm p. By Theorem 1.5, $\mathfrak{p}$ is unramified in L. Let σ denote the Artin symbol $\left(\frac{L/F}{\mathfrak{p}}\right)$, and let $\mathfrak{P}$ be a prime ideal in L above $\mathfrak{p}$. Since $\sigma(v) \equiv v^p \pmod{\mathfrak{P}}$, we see that σ is trivial on L if and only if $v^{p-1} \equiv 1 \pmod{\mathfrak{P}}$. This last congruence is equivalent to $u_p^{(p-1)/3} \equiv 1 \pmod p$. Thus u_p is a cubic residue (mod p) if and only if σ is trivial on L. It remains to show that σ is trivial on L if and only if $L \subset M$.

By [3, Theorem 9.4], the primes p split completely in M. First suppose that $L \subset M$. Then a fortiori the primes p split completely in L, or equivalently, by [3, Corollary 5.21], σ is trivial on L. Conversely, suppose that the primes p split completely in L. Then $L \subset M$ by [3, Theorem 8.19]. □

Let M_c denote the ring class field of F for the order $\mathbb{Z}[\sqrt{-3dc^2}]$. Thus $M_1 = M$ and M_3 is the ring class field of F for the order $\mathbb{Z}[\sqrt{-27d}]$. Mimicking the proof of Theorem 1.6, we see that $v \in M_c$ if and only if u_p is a cubic residue mod the primes $p = x^2 + 3d(cy)^2$.

In Theorem 6.1, we give explicit criteria in terms of a and b for $v = (a + b\sqrt{d})^{1/3}$ to lie in M, where $a + b\sqrt{d}$ is the fundamental unit. Theorem 6.2 shows that every v lies in M_3.

In Section 7, we introduce a large class S_d of integers $r + s\sqrt{d}$ with cubic norms, where S_d properly contains the set of fundamental units $a+b\sqrt{d}$. Under certain conditions, we extend Theorem 6.1 for elements in S_d.

A substantial generalization of Theorem 6.1 is given in Section 8. The proof makes no appeal to class field theory, but instead relies wholly on the methods developed in [11]. As a corollary, we provide congruences for certain Lucas numbers modulo primes $p = x^2 + 3dy^2$.

2. Proof of Theorem 1.1

Assume throughout this section that $v \in M$. The proof of Theorem 1.1 utilizes the following five lemmas.

Lemma 2.1. *When $3 \nmid d$, L/F is unramified.*

Proof. By hypothesis, $L \subset M$. We may assume that $d \equiv 1 \pmod 8$; otherwise, by [3, Thm. 7.24], M is the Hilbert class field of F so that L/F is unramified. Under this assumption, the order $\mathbb{Z}[\sqrt{-3d}]$ has conductor 2, so it suffices to show that 2 is unramified in L. Consider the tower $\mathbb{Q} \subset C \subset K \subset L$. Clearly $C/\mathbb{Q}$ is unramified at 2. Also $K/C = \mathbb{Q}(v)/\mathbb{Q}(\sqrt{d})$ is unramified at 2, since the polynomial $x^3 - v^3$ has discriminant $-27v^6$. Finally, any prime ideal in K above 2 must be unramified in the extension $L = K(w)$, since the minimal polynomial $x^2 + x + 1$ of w over K has discriminant -3. □

Remark (2A). *Let $3 \nmid d$. Since L/F is a cyclic unramified extension of degree 6 when $3 \nmid d$ by Lemma 2.1, the class number of F is divisible by 6, and $D(L/F)$ has (absolute) norm 1. This is in contrast with the case $3 \mid d$; see Remark (3D).*

Lemma 2.2. *When $3 \nmid d$, $D(L/K)$ has norm 9.*

Proof. We need only examine the ramification at 3, since the polynomial $x^2 + x + 1$ has discriminant -3. Note that 3 ramifies in F but there can be no further ramification at 3 in L/F by Lemma 2.1. Thus in the factorization of (3) in L, every prime ideal occurs to the second power.

The minimal polynomial of $t = v + v'$ over $\mathbb{Q}$ is $x^3 - 3\epsilon x - 2a$, where ϵ is the norm of the fundamental unit $v^3 = a + b\sqrt{d}$. This polynomial has discriminant $-108db^2$, in which the exponent of the factor 3 is odd. By [10, Prop. 2.13], 3 divides $D(k)$, so 3 must ramify in k and in K.

The factorization of (3) in C is either $\mathfrak{q}$ or $\mathfrak{p}\mathfrak{p}'$, where $\mathfrak{q}$ has norm 9 and $\mathfrak{p}$, $\mathfrak{p}'$ each have norm 3. Since 3 ramifies in K, we have in K either the prime ideal factorization $(\mathfrak{q}) = \mathfrak{Q}_1^2\mathfrak{Q}$ where the prime factors have norm 9, or $(\mathfrak{p}\mathfrak{p}') = \mathfrak{P}\mathfrak{P}_1^2\mathfrak{P}'\mathfrak{P}_1'^2$ where the prime factors have norm 3. In the first case, $\mathfrak{Q}$ is the factor that ramifies in L, while in the second case, $\mathfrak{P}$ and $\mathfrak{P}'$ are the factors that ramify in L. Since the ramification is tame, $D(L/K)$ equals $\mathfrak{Q}$ or $\mathfrak{P}\mathfrak{P}'$, and in either case $D(L/K)$ has norm 9. □

Lemma 2.3. *When $q \neq 3$ is a rational prime, $(q) \nmid D(K/k)$ in k.*

Proof. Suppose for the purpose of contradiction that (q) divides $D(K/k)$. Since q divides the discriminant of the k-basis $\{1, v\}$ in K, q must divide

$$t^2 - 4 = v^2 + v'^2 - 2. \tag{2.1}$$

Replacing v in (2.1) by its conjugate wv in L, we see that in L, q divides

$$w^2v^2 + wv'^2 - 2. \tag{2.2}$$

Subtracting, we see that q divides

$$(w^2 - 1)v^2 + (w - 1)v'^2. \tag{2.3}$$

Replacing w by w^2 in (2.3), we see that q divides

$$(w - 1)v^2 + (w^2 - 1)v'^2. \tag{2.4}$$

Multiplying (2.3) by $w + 1$ and then subtracting from (2.4), we see that q divides $3wv^2$, which is impossible, since $q \neq 3$. This contradiction proves the lemma. □

Lemma 2.4. *Suppose that $3 \nmid d$. The only rational primes that ramify in L are the ones that divide $D(F)$. If a rational prime q divides $D(C)$, then each prime ideal in the factorizations of (q) in K and L occurs to the second power.*

Proof. If the prime p divides $D(F)$, then p ramifies in F with ramification index 2. Then since L/F is unramified by Lemma 2.1, each prime ideal in the factorization of (p) in L occurs to the second power. If p does not divide $D(F)$, then clearly p does not ramify in L.

Next, suppose that q divides $D(C)$ (so that $q \neq 3$). Then q ramifies in C with ramification index 2. Recall that K/C is unramified at q, since the polynomial $x^3 - v^3$ has discriminant $-27v^6$. Thus each prime ideal factor in the factorization of (q) in K occurs to the second power. □

Lemma 2.5. *When $3 \nmid d$, $D(K) = 9D(C)^3$.*

Proof. By Lemma 2.1 and [10, Prop. 4.15], $D(L) = D(F)^6$. Thus by Lemma 2.2,

$$D(K)^2 = D(L)/9 = D(F)^6/9. \tag{2.5}$$

Since $D(K)$ is positive [10, Prop. 2.15],

$$D(K) = -D(F)^3/3 = 9D(C)^3. \tag{2.6}$$

□

We are now prepared for the proof of Theorem 1.1.

Proof. Consider the set S of rational primes p that divide the discriminant $D(C)$. Note that $3 \notin S$. By Lemma 2.4, each prime ideal in the factorization of (p) in K (as well as in L) occurs to the second power. Each prime ideal in the factorization of (p) in k must occur to either the first or second power, and those occurring to the first power are exactly the ones that ramify in K. Those that ramify tamely in K are the only ones that divide $D(K/k)$ to the first power [10, p. 260].

For $p \in S$, if every prime ideal factor of (p) in k were to occur to the first power, then (p) would divide $D(K/k)$, contradicting Lemma 2.3. Thus p ramifies in k, so there is a unique prime ideal $\mathfrak{p}$ in k that divides (p) to the first power. Note that $\mathfrak{p}$ has norm p. If $p = 2$, then $\mathfrak{p}^e$ exactly divides $D(K/k)$ for some $e \geq 2$ depending on d, while if $p > 3$, then $\mathfrak{p}$ exactly divides $D(K/k)$.

We proceed to say more about the value of e. To distinguish the prime ideal $\mathfrak{p}$ in the case $p = 2$, call it $\mathfrak{p}_2$. The discriminant of the k-basis $\{1, \sqrt{d}\}$ for K is $4d$, so that $D(K/k)$ divides $4d$. First suppose that $d \equiv 3 \pmod 4$. Since $\mathfrak{p}_2$ divides (2) to the first power in k, $\mathfrak{p}_2$ divides $(4d)$ to the second power. Thus $e \leq 2$ in this case, so that $e = 2$. Next suppose that $d \equiv 2 \pmod 4$. Then 8 divides $4d$, so that $e \in \{2, 3\}$ in this case.

So far we have shown that

$$D(K/k) = \mathfrak{p}_2^e \prod_{3<p\in S} \mathfrak{p}, \tag{2.7}$$

where $\mathfrak{p}_2$ is to be interpreted as 1 when $d \equiv 1 \pmod 4$. (No prime ideal above 3 occurs in this product since 3 does not divide $4d$.) Taking absolute norms on both sides of (2.7), we have

$$D(K)/D(k)^2 = \begin{cases} d, & d \equiv 1 \pmod 4 \\ 4d, & d \equiv 3 \pmod 4 \\ 2^{e-1}d, & d \equiv 2 \pmod 4. \end{cases} \tag{2.8}$$

By Lemma 2.5,

$$D(K) = \begin{cases} 9d^3, & d \equiv 1 \pmod 4 \\ 9 \cdot 2^6 d^3, & d \equiv 2, 3 \pmod 4. \end{cases} \tag{2.9}$$

Thus

$$D(k)^2 = \begin{cases} 9d^2, & d \equiv 1 \pmod 4 \\ 9 \cdot 2^4 d^2, & d \equiv 3 \pmod 4 \\ 9 \cdot 2^{7-e} d^2, & d \equiv 2 \pmod 4. \end{cases} \tag{2.10}$$

This shows that e must be odd, so $e = 3$. Finally, since $D(k)$ is negative [10, Prop. 2.15], we obtain the desired result

$$D(k) = \begin{cases} -3d, & d \equiv 1 \pmod 4 \\ -12d, & d \equiv 2, 3 \pmod 4. \end{cases} \tag{2.11}$$

□

3. Proof of Theorem 1.2

Assume throughout this section that $v \in M$. Write $d = 3m$ so that $F = \mathbb{Q}(\sqrt{-m})$. Note that the order $\mathbb{Z}[\sqrt{-3d}] = \mathbb{Z}[3\sqrt{-m}]$ has conductor 3 or 6. The proof of Theorem 1.2 utilizes the following two lemmas.

Lemma 3.1. *When $3 \mid d$, the extension $F(t)/F$ is unramified.*

Proof. Let J denote the ring class field for the order $\mathbb{Z}[\sqrt{-m}]$ in F. Note that this order has conductor 1 or 2. The formula for class numbers of orders [3, Thm. 7.24] shows that the extension M/J has degree 2 or 4. Note that $t \in M$, since $v \in M$.

Since t has degree 3 over $\mathbb{Q}$ and $J(t) \subset M$, we have $|J(t)/J| \leq 2$. Assume for the purpose of contradiction that equality holds. The cubic minimal polynomial of t over $\mathbb{Q}$ is divisible over J by the quadratic minimal polynomial of t over J. Therefore some conjugate of t lies in J, so that $J(t) = J$. Thus the assumption is false, and $t \in J$.

Consider the tower $F \subset F(w) \subset F(v) = L$. The extensions $F(w)/F$ and $L/F(w) = \mathbb{Q}(w)(v)/\mathbb{Q}(w)(\sqrt{d})$ cannot ramify at any rational prime other than 3. Thus the same is true of the extension $F(t)/F$. Since $F(t) \subset J$ and 3 does not divide the conductor of $\mathbb{Z}[\sqrt{-m}]$, the extension $F(t)/F$ must be unramified. □

Remark (3B). *By Lemma 3.1, $F(t)/F$ is a cyclic unramified cubic extension when $3 \mid d$. Thus $F(t)$ lies in the Hilbert class field of F, so that 3 divides the class number of F.*

Remark (3C). *For $d = 3m$, consider the principal prime ideal $\mathfrak{p} = (x + y\sqrt{-m})$ in F of norm p. By Lemma 3.1, the corresponding Artin symbol for the extension L/F fixes t, so it maps v to either v or v'. In the first case, $p \equiv 1 \pmod 3$ and $v^{p-1} \equiv 1 \pmod{\mathfrak{P}}$, while in the second case, since here $vv' = 1$, we have $p \equiv -1 \pmod 3$ and $v^{p+1} \equiv 1 \pmod{\mathfrak{P}}$, where $\mathfrak{P}$ is a prime ideal of L above $\mathfrak{p}$.*

Remark (3D). *When $3 \mid d$ and $v \in M$, $D(L/F)$ has norm 729. To see this, first observe that by Lemma 3.1, $F(t)/Q$ is unramified at 3. Note that $L = F(t)(\sqrt{-3})$. It follows that $D(L/F(t)) = (3)$, since by* [12, p. 685]*, $D(L/F(t))$ is the product of the prime ideals in the factorization of (3) in $F(t)$ which divide (3) to the first power. Taking the norm, we obtain $D(L)/D(F(t))^2 = 3^6$. By Lemma 3.1, $D(F(t)) = D(F)^3$, so that $D(L)/D(F)^6 = 3^6$. This proves that $D(L/F)$ has norm 729.*

Lemma 3.2. *Suppose that $3 \mid d$. The only rational primes that ramify in L are the ones that divide $D(C)$. For a rational prime p dividing $D(C)$, each prime ideal in the factorizations of (p) in K and L occurs to the second power. Consequently the extension K/C is unramified.*

Proof. If p divides $D(C)$, then p ramifies in C with ramification index 2. First assume that $p \neq 3$. Then L/C is unramified at p, since K/C and L/K are unramified at p. Thus each prime ideal in the factorizations of (p) in K and L occurs to the second power. Next consider the case $p = 3$. We know that 3 ramifies in K and in L, because it ramifies in C. By Lemma 3.1, 3 does not ramify in $F(t)$. Since $F(t)$ is a subfield of L of index 2, it follows that each prime ideal in the factorizations of (3) in K and L occurs to the second power. Thus when p divides $D(C)$, there can be no further ramification from C to L, so that L/C and K/C are unramified. □

We are now prepared for the proof of Theorem 1.2.

Proof. Consider the set S of rational primes p that divide the discriminant $D(C)$. Note that $3 \in S$. By Lemma 3.2, each prime ideal in the factorization of (p) in K occurs to the second power. Each prime ideal in the factorization of (p) in k must occur to either the first or second power, and those occurring to the first power are exactly the ones that ramify in K.

Mimicking the proof of (2.7), we obtain

$$D(K/k) = 3\mathfrak{p}_2^e \prod_{3<p\in S} \mathfrak{p}. \tag{3.1}$$

The reason for the factor 3 is as follows. The proof of Theorem 1.1 applies here to show that all primes in S other than 3 ramify in k. However, 3 does not ramify in k; this is due to Lemma 3.1, since $k \subset F(t)$. Consequently each prime ideal in the factorization of (3) in k occurs to the first power, so each ramifies tamely in K. This explains the factor 3 in (3.1).

Taking absolute norms on both sides of (3.1), we have

$$D(K)/D(k)^2 = \begin{cases} 9d, & d \equiv 1 \pmod 4 \\ 4 \cdot 9d, & d \equiv 3 \pmod 4 \\ 2^{e-1}9d, & d \equiv 2 \pmod 4. \end{cases} \tag{3.2}$$

By Lemma 3.2, $D(K) = D(C)^3$ so that

$$D(K) = \begin{cases} d^3, & d \equiv 1 \pmod 4 \\ 2^6 d^3, & d \equiv 2, 3 \pmod 4. \end{cases} \tag{3.3}$$

Thus

$$D(k)^2 = \begin{cases} m^2, & d \equiv 1 \pmod 4 \\ 2^4 m^2, & d \equiv 3 \pmod 4 \\ 2^{7-e} m^2, & d \equiv 2 \pmod 4. \end{cases} \tag{3.4}$$

This shows that e must be odd, so $e = 3$. Finally, since $D(k)$ is negative, we obtain the desired result

$$D(k) = \begin{cases} -m, & d \equiv 1 \pmod 4 \\ -4m, & d \equiv 2, 3 \pmod 4. \end{cases} \tag{3.5}$$

□

4. Proof of Theorem 1.3

Assume throughout this section that $v \notin M$ and $3 \nmid d$. The proof of Theorem 1.3 utilizes the following five lemmas.

Lemma 4.1. *Suppose that $3 \nmid d$. If $D(C)$ is divisible by a prime q, then each prime ideal in the factorizations of (q) in $F(t)$, K, and L occurs to the second power. On the other hand, if $D(C)$ is not divisible by q and $q \neq 3$, then q is unramified in L.*

Proof. First suppose that $q \nmid D(C)$ and $q \neq 3$. The extension $C/\mathbb{Q}$ is unramified at q. The extension K/C is also unramified at q since it can be ramified only at 3, due to the fact that $x^3 - v^3$ has discriminant $-27v^6$. Moreover, L/K can be ramified only at 3, since $L = K(w)$ and $x^2 + x + 1$ has discriminant -3. Thus q is unramified in L.

Next suppose that q divides $D(C)$. Then q ramifies in C and in F, but there can be no further ramification in the extension L/C, since $q \neq 3$. Thus each prime ideal in the factorizations of (q) in $F(t)$, K, and L occurs to the second power. □

Lemma 4.2. *When $3 \nmid d$, the extensions $L/F(t)$ and B/F are unramified.*

Proof. Any prime ideal in $F(t)$ ramifying in $L = F(t, w) = F(t, \sqrt{d})$ would have to divide both $F(t)$-basis discriminants $4d$ and -3, which is impossible. The extension B/F is unramified for the same reason. □

Lemma 4.3. *When $3 \nmid d$, the extension L/B ramifies only at 3.*

Proof. In view of Lemmas 4.1 and 4.2, we need only show that the extension L/B is ramified. Suppose for the purpose of contradiction that it isn't. Then by Lemma 4.2, the extension L/F would be unramified. Consequently $L \subset M$, which contradicts $v \notin M$. □

Lemma 4.4. *When $3 \nmid d$, $D(L/B)$ has norm 3^8 and $D(K/C)$ has norm 3^6.*

Proof. We have the prime ideal factorization $(3) = (\sqrt{-3})^2$ in $\mathbb{Q}(\sqrt{-3})$. In B, either $(\sqrt{-3}) = \mathfrak{q}$ or $(\sqrt{-3}) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{q}$ has norm 9 and $\mathfrak{p}, \mathfrak{p}'$ have norm 3. By Lemma 4.3, these prime ideals ramify wildly in the cubic cyclic extension L/B, with ramification index 3. Thus for some integer $s \geq 3$, $D(L/B) = \mathfrak{q}^s$ or $D(L/B) = (\mathfrak{p}\mathfrak{p}')^s$ [10, Corollary 2, p. 260]. Consequently $D(L/B)$ has norm 9^s. Equivalently,

$$D(L) = 9^s D(B)^3. \tag{4.1}$$

We now know that the ramification index of 3 in the Galois extension $L/\mathbb{Q}$ is divisible by 3. In C, either $(3) = \mathfrak{q}$ or $(3) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{q}$ has norm 9 and $\mathfrak{p}, \mathfrak{p}'$ have norm 3. As K/C is a cubic extension, we have wild ramification in K of the form $(3) = \mathfrak{Q}^3$ or $(3) = (\mathfrak{P}\mathfrak{P}')^3$, where $\mathfrak{Q}$ has norm 9 and $\mathfrak{P}, \mathfrak{P}'$ have norm 3. It follows that $D(K/C)$ equals $\mathfrak{q}^r$ or $(\mathfrak{p}\mathfrak{p}')^r$ for some integer $r \geq 3$. Thus $D(K/C)$ has norm 9^r. Moreover, since $D(K/C)$ divides $(27v^6)$, the norm of $D(K/C)$ divides $27^2 = 9^3$. Thus $r = 3$, so that $D(K/C)$ has the desired norm 3^6. Equivalently,

$$D(K) = 3^6 D(C)^3 = -3^3 D(F)^3. \tag{4.2}$$

By Lemma 4.2, $D(B) = D(F)^2$. Thus, by (4.1),

$$D(L) = 9^s D(F)^6. \tag{4.3}$$

Since $L = K(\sqrt{-3})$, $D(L/K)$ equals the product of the prime ideals in the factorization of (3) in K that occur to odd powers [12, p. 685]. Thus, in the notation above, $D(L/K)$ equals $\mathfrak{Q}$ or $\mathfrak{P}\mathfrak{P}'$. Consequently, $D(L/K)$ has norm 9, so that by (4.2),

$$D(L) = 9D(K)^2 = 3^8 D(F)^6. \tag{4.4}$$

Comparing equations (4.3) and (4.4), we see that $s = 4$. Therefore, by (4.1), $D(L/B)$ has the desired norm 3^8. □

Remark (4E). *Since each prime ideal factor of $D(L/B)$ occurs to the power $s = 4$, the corresponding higher ramification groups G_i must be trivial for $i \geq 2$, in view of* [10, p. 265]. *This is because $s = 4 = (|G_0| - 1) + (|G_1| - 1)$, where $G_0 = G_1 = \mathrm{Gal}(L/B)$.*

Lemma 4.5. *When $3 \nmid d$, $D(F(t)) = 3^4 D(F)^3$.*

Proof. By (4.4), $D(L) = 3^8 D(F)^6$. By Lemma 4.2, $D(F(t))^2 = D(L)$, so that $D(F(t)) = 3^4 D(F)^3$. □

Remark (4F). *When $3 \nmid d$ and $v \notin M$, it follows from (4.4) that $D(L/F)$ has norm 3^8. This is in contrast with the case $3 \mid d$; see Remark (5G).*

We are now prepared for the proof of Theorem 1.3.

Proof. Since $F(t) = k(\sqrt{-3d})$, the odd part of $D(F(t)/k)$ is the product of the prime ideals of odd norm in the factorization of $(-3d)$ in k which occur to odd powers [12]. Let p be any odd prime dividing $3d$. By [10, Prop. 2.13], $p|D(k)$, since the minimal polynomial of t over $\mathbb{Q}$ has discriminant $-108db^2$, which p divides to an odd power. Thus p ramifies in k, so that exactly one prime ideal $\mathfrak{p}_p$ in the factorization of (p) in k occurs to an odd power, where $\mathfrak{p}_p$ has norm p. Therefore the odd part of $D(F(t)/k)$ equals $\prod \mathfrak{p}_p$, where p runs through the odd prime factors of $3d$.

We now consider the case where $2 \mid D(C)$, i.e., $d \equiv 2, 3 \pmod 4$. By Lemma 4.1, each prime ideal in the factorizations of (2) in $F(t)$ and K occurs to the second power. Each prime ideal in the factorization of (2) in k must occur to the first or second power, and those occurring to the first power are exactly the ones that ramify in $F(t)$ and in K. If every prime ideal factor of (2) in k were to occur to the first power, then (2) would divide $D(K/k)$, contradicting Lemma 2.3. Thus exactly one prime ideal $\mathfrak{p}_2$ in k divides (2) to the first power, and $\mathfrak{p}_2$ has norm 2. Then $\mathfrak{p}_2^e$ exactly divides $D(F(t)/k)$ for some $e \geq 2$ depending on d.

The discriminant of the k-basis $\{1, \sqrt{-3d}\}$ for $F(t)$ is $-12d$, so that $D(F(t)/k)$ divides $12d$. First suppose that $d \equiv 3 \pmod 4$. Since $\mathfrak{p}_2$ divides (2) to the first power in k, $\mathfrak{p}_2$ divides $(12d)$ to the second power. Thus $e \leq 2$ in this case, so that $e = 2$. Next suppose that $d \equiv 2 \pmod 4$. Then 8 divides $12d$, so that $e \in \{2, 3\}$ in this case.

So far we have shown that

$$D(F(t)/k) = \mathfrak{p}_2^e \prod_p \mathfrak{p}_p, \tag{4.5}$$

where p runs through the odd primes dividing $3d$, and where $\mathfrak{p}_2$ is to be interpreted as 1 when $d \equiv 1 \pmod 4$. Taking norms on both sides of (4.5), we have

$$D(F(t))/D(k)^2 = \begin{cases} -3d, & d \equiv 1 \pmod 4 \\ -12d, & d \equiv 3 \pmod 4 \\ -3d \cdot 2^{e-1}, & d \equiv 2 \pmod 4. \end{cases} \tag{4.6}$$

By (4.6) and Lemma 4.5,

$$D(k)^2 = \begin{cases} 3^6 d^2, & d \equiv 1 \pmod 4 \\ 3^6 \cdot 2^4 d^2, & d \equiv 3 \pmod 4 \\ 3^6 \cdot 2^{7-e} d^2, & d \equiv 2 \pmod 4. \end{cases} \tag{4.7}$$

This shows that e must be odd, so $e = 3$. Finally, since $D(k)$ is negative [10, Prop. 2.15], we obtain the desired result $D(k) = 9D(F)$. □

5. Proof of Theorem 1.4

Assume throughout this section that $v \notin M$ and $d = 3m$. Then $F = \mathbb{Q}(\sqrt{-m})$. Note that the order $\mathbb{Z}[\sqrt{-3d}] = \mathbb{Z}[3\sqrt{-m}]$ in F has conductor 3 or 6. The proof of Theorem 1.4 utilizes the following three lemmas.

Lemma 5.1. *Let p be a prime dividing $D(F)$. Then each prime ideal in the factorizations of (p) in $F(t)$, K, and L occurs to the second power.*

Proof. The prime p ramifies in C and in F with ramification index 2. Since $L = K(w)$ and $x^2 + x + 1$ has discriminant -3 and $p \neq 3$, the extension L/K is unramified at p. Similarly, K/C is unramified at p, since $x^3 - v^3$ has discriminant $-27v^6$. Thus each prime ideal in the factorization of (p) in L occurs to the second power, and the result follows. □

Lemma 5.2. *The extension $F(t)/F$ is ramified at 3.*

Proof. Suppose for the purpose of contradiction that the lemma is false. Then by Lemma 5.1, the cubic cyclic extension $F(t)/F$ is unramified. Consequently, $F(t)$ is contained in the Hilbert class field of F. Thus t is contained in the ring class field J for the order $\mathbb{Z}[\sqrt{-m}]$,

so that the Artin symbol in Remark (3C) fixes t. As noted in Remark (3C), the Artin map fixes v when $p = x^2 + my^2 \equiv 1 \pmod 3$, which occurs for example when $3|y$. It follows that the primes $p = X^2 + 9mY^2$ split completely in L. These are the primes that split completely in M. By [3, Thm. 8.19], we have $L \subset M$, so that $v \in M$, as contradiction. □

Lemma 5.3. *The norm of $D(F(t)/F)$ is equal to 3^8.*

Proof. In F, either $(3) = \mathfrak{q}$ or $(3) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{q}$ has norm 9 and $\mathfrak{p}, \mathfrak{p}'$ have norm 3. By Lemma 5.2, these prime ideals ramify wildly in $F(t)$ with ramification index 3. Thus

$$D(F(t)/F) = \mathfrak{q}^s \text{ or } D(F(t)/F) = (\mathfrak{p}\mathfrak{p}')^s \tag{5.1}$$

for some integer s with $3 \le s \le 5$ [10, pp. 260,262]. In either case, $D(F(t)/F)$ has norm 9^s. Since $F(t)/F$ is a cubic cyclic extension, $D(F(t)/F)$ is equal to the square of an ideal in F [10, Cor. 2, p. 266]. Thus by (5.1), $s = 4$, so $D(F(t)/F)$ has norm 3^8. □

We are now prepared for the proof of Theorem 1.4.

Proof. Let p be a prime dividing $D(F)$. By Lemma 5.1, each prime ideal in the factorization of (p) in k must occur to the first or second power, and those that occur to the first power are exactly the ones that ramify in $F(t)$ and in K. If every prime ideal factor of (p) in k were to occur to the first power, then (p) would divide $D(K/k)$, contradicting Lemma 2.3. Thus p ramifies in k, so that exactly one prime ideal $\mathfrak{p}_p$ in the factorization of (p) in k occurs to an odd power, and $\mathfrak{p}_p$ has norm p. Since $F(t) = k(\sqrt{-m})$, the odd part of $D(F(t)/k)$ is the product of the prime ideals of odd norm in the factorization of (m) in k which occur to odd powers [12]. Thus the odd part of $D(F(t)/k)$ equals $\prod \mathfrak{p}_p$, where p runs through the odd prime factors of m.

Consider now the case when $p = 2$. Since $\mathfrak{p}_2$ ramifies wildly in $F(t)$, $\mathfrak{p}_2^e$ exactly divides $D(F(t)/k)$ for some integer $e \ge 2$. Arguing as in the paragraph above (2.7), we see that $e = 2$ when $d \equiv 3 \pmod 4$ and $e \in \{2, 3\}$ when $d \equiv 2 \pmod 4$. Thus

$$D(F(t)/k) = \mathfrak{p}_2^e \prod_p \mathfrak{p}_p, \tag{5.2}$$

where p runs through the odd prime factors of m, and where $\mathfrak{p}_2$ is to be interpreted as 1 when $d \equiv 1 \pmod 4$.

Taking norms on both sides of (5.2), we have

$$D(F(t))/D(k)^2 = \begin{cases} -m, & d \equiv 1 \pmod 4 \\ -4m, & d \equiv 3 \pmod 4 \\ -2^{e-1}m, & d \equiv 2 \pmod 4. \end{cases} \tag{5.3}$$

By Lemma 5.3,

$$D(F(t)) = 3^8 D(F)^3 = \begin{cases} -m^3 3^8, & d \equiv 1 \pmod 4 \\ -m^3 2^6 3^8, & d \equiv 2, 3 \pmod 4. \end{cases} \tag{5.4}$$

By (5.3) and (5.4),

$$D(k)^2 = \begin{cases} m^2 3^8, & d \equiv 1 \pmod 4 \\ 2^4 m^2 3^8, & d \equiv 3 \pmod 4 \\ 2^{7-e} m^2 3^8, & d \equiv 2 \pmod 4. \end{cases} \tag{5.5}$$

This shows that e must be odd, so $e = 3$. Finally, since $D(k)$ is negative [10, Prop. 2.15], we obtain the desired result $D(k) = 81D(F)$. □

Remark (5G). *When $3 \mid d$ and $v \notin M$, $D(L/F)$ has norm 3^{18}. To see this, note that by the proof of Lemma 5.3, the prime ideal factorization of (3) in $F(t)$ is either $\mathfrak{Q}^3$ or $(\mathfrak{P}\mathfrak{P}')^3$, where $\mathfrak{Q}$ has norm 9 and $\mathfrak{P}, \mathfrak{P}'$ have norm 3. Since these prime ideals occur to the odd power 3, and since $L = F(t)(\sqrt{-3})$, it follows from* [12] *that $D(L/F(t))$ equals $\mathfrak{Q}$ or $\mathfrak{P}\mathfrak{P}'$. In either case, $D(L/F(t))$ has norm 9, so that $D(L) = 9D(F(t))^2$. By Lemma 5.3, $D(F(t)) = 3^8 D(F)^3$. Combining these last two equalities, we obtain the desired result $D(L) = 3^{18}D(F)^6$.*

6. Ring class fields

Recall that v is the real cube root of the fundamental unit $u = a + b\sqrt{d}$. The following theorem gives explicit criteria in terms of a and b for v to lie in the ring class field M.

Theorem 6.1. *We have $v \in M$ if and only if*

$$a \equiv 0 \pmod 9 \quad \text{or} \quad \begin{cases} a \equiv \pm 2 \pmod 9 & \text{when } a^2 - db^2 = -1 \\ a \equiv \pm 1 \pmod{27} & \text{when } a^2 - db^2 = +1. \end{cases} \tag{6.1}$$

Proof. By the proof of [6, Thm. 6], (6.1) holds if and only if $F(t)/F$ is unramified. The result now follows from Lemmas 2.1, 3.1, 4.5, and 5.3. □

Recall that M_3 denotes the ring class field of F for the order $\mathbb{Z}[\sqrt{-27d}]$. It follows from [3, Thm. 7.24] that $|M_3 : M| = 3$. Consider the example $v = (5/2 + \sqrt{21}/2)^{1/3}$ for $d = 21$. By Theorem 6.1, v does not lie in M, since $a = 5/2 \equiv 16 \not\equiv \pm 1 \pmod{27}$. On the other hand, this v does lie in M_3. In fact, Theorem 6.2 shows that $v \in M_3$ for every v, i.e., every u_p is a cubic residue mod the primes $p = x^2 + 27dy^2$. This fact had been conjectured by the first author, and the proof is due to the third author. For an extension of Theorem 6.2, see Conjecture 7.8.

Note that for each squarefree $d > 1$, the fundamental unit u can be written in the form $u = (m + n\sqrt{d})/2$ with nonzero integers m, n such that $m^2 - dn^2 = \pm 4$.

Theorem 6.2. *Every v lies in M_3.*

Proof. We will utilize the integral quadratic forms below when $d \equiv 1 \pmod 4$:

$$p = A^2 + 3dB^2 \Longrightarrow p = x^2 + xy + \frac{3d+1}{4}y^2 \tag{6.2}$$

and

$$p = A^2 + 27dB^2 \Longrightarrow p = x^2 + xy + \frac{27d+1}{4}y^2, \tag{6.3}$$

where $x = A - B$ and $y = 2B$.

Case 1: $m^2 - dn^2 = -4$.

In this case we cannot have $d \equiv 3 \pmod 4$. First assume that $9 \mid m$ and $p = A^2 + 3dB^2$. If $d \equiv 2 \pmod 4$, then $v \in M$ by [11, Thm. 5.1] with $k = 2$. If $d \equiv 1 \pmod 4$, then $v \in M$ by (6.2) and [11, Thm. 5.1] with $k = 1$.

Next assume that $9 \nmid m$ and $p = A^2 + 27dB^2$. If $d \equiv 2 \pmod 4$, then $v \in M_3$ by [11, Thm. 5.1] with $k = 6$. If $d \equiv 1 \pmod 4$, then $v \in M_3$ by (6.3) and [11, Thm. 5.1] with $k = 3$. This completes the proof in Case 1.

Case 2: $m^2 - dn^2 = 4$.
First assume that $9 \mid m$ and $p = A^2 + 3dB^2$. If $d \equiv 2, 3 \pmod 4$, then $v \in M$ by [11, Thm. 5.3] with $k = 2$. If $d \equiv 1 \pmod 4$, then $v \in M$ by (6.2) and [11, Thm. 5.3] with $k = 1$.

Next assume that $9 \nmid m$. Since $(m-2)(m+2) = dn^2$, we may choose the sign of m so that $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$, where ord_3 denotes the 3-adic order. There is no loss of generality in fixing this sign, since the conjugate v' of v satisfies $vv' = \pm 1$. We will consider separately the cases $d \equiv 2, 3 \pmod 4$, $d \equiv 5 \pmod 8$, and $d \equiv 1 \pmod 8$.

If $d \equiv 2, 3 \pmod 4$, $9 \nmid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 27dB^2$, then $v \in M_3$ by [11, Thm. 5.5] with $k = 2 \cdot 3$. If $d \equiv 2, 3 \pmod 4$, $9 \mid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 3dB^2$, then $v \in M$ by [11, Thm. 5.5] with $k = 2 \cdot 1$. (We can ignore the restriction $p \nmid n$ in [11, Thm. 5.5] because $u \equiv 1 \pmod p$ when $p \mid n$.)

If $d \equiv 5 \pmod 8$, $9 \nmid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 27dB^2$, then $v \in M_3$ by (6.3) and [11, Thm. 5.5] with $k = 1 \cdot 3$. If $d \equiv 5 \pmod 8$, $9 \mid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 3dB^2$, then $v \in M$ by (6.2) and [11, Thm. 5.5] with $k = 1 \cdot 1$.

From now on assume that $d \equiv 1 \pmod 8$. Set $r = \mathrm{ord}_2 \frac{4(m-2)}{(m-2,n)^2}$. If $r > 0$, $r \equiv 0, 1 \pmod 3$, $9 \nmid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 27dB^2$, then $v \in M_3$ by [11, Thm. 5.5] with $k = 2 \cdot 3$. If $r > 0$, $r \equiv 0, 1 \pmod 3$, $9 \mid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 3dB^2$, then $v \in M$ by [11, Thm. 5.5] with $k = 2 \cdot 1$.

Finally consider the case where either $r = 0$ or $r \equiv 2 \pmod 3$. If $9 \nmid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 27dB^2$, then $v \in M_3$ by (6.3) and [11, Thm. 5.5] with $k = 1 \cdot 3$. If $9 \mid \frac{m-2}{(m-2,n)}$ and $p = A^2 + 3dB^2$, then $v \in M$ by (6.2) and [11, Thm. 5.5] with $k = 1 \cdot 1$. This completes the proof in Case 2. □

7. Generalizations for integers $u \in \mathbb{Q}(\sqrt{d})$ with cubic norms

For each squarefree $d > 1$, let $\mathcal{O}(d)$ denote the ring of integers in $\mathbb{Q}(\sqrt{d})$, and write $f(d)$ for the fundamental unit in $\mathcal{O}(d)$. Let S_d denote the set of $u \in \mathcal{O}(d)$ for which the norm of u is a cube, u is not the cube of an element in $\mathcal{O}(d)$, and u is not divisible in $\mathcal{O}(d)$ by the cube of a rational prime. (The notation u will no longer be restricted solely for fundamental units.) Denote the norm of u by $N(u) = n^3$, and let ν denote the real cube root $u^{1/3}$.

Let S_d^* denote the subset of $u \in S_d$ such that $p \mid d$ for each rational prime p dividing u. For example, S_d^* contains the fundamental unit $f(d)$. More generally, whenever $\mu \in \mathcal{O}(d)$ is not divisible by a rational prime, S_d^* contains

$$\mu^3 f(d)^{\pm 1}. \tag{7.1}$$

Examples of elements in S_d^* not of the form (7.1) are

$$17 + 2\sqrt{79},\ 13 + \sqrt{142},\ 14 + \sqrt{223},\ (11 + \sqrt{229})/2,\ 28 + 3\sqrt{235},\ 77 + 2\sqrt{254}, \tag{7.2}$$

whose norms are $-27,\ 27, -27, -27, -11^3, 17^3$, respectively.

Let P_d denote the set of $\mu = a+b\sqrt{d} \in \mathcal{O}(d)$ with norm $N(\mu) = n^3$ satisfying the following conditions:

$$\begin{aligned}
n \equiv 2,5,8 \pmod 9 &\implies a \equiv 0, \pm 2, \pm 7, \pm 9, \pm 11 \pmod{27};\\
n \equiv 1 \pmod 9 &\implies a \equiv 0, \pm 1, \pm 9 \pmod{27};\\
n \equiv 4 \pmod 9 &\implies a \equiv 0, \pm 8, \pm 9 \pmod{27};\\
n \equiv 7 \pmod 9 &\implies a \equiv 0, \pm 9, \pm 10 \pmod{27};\\
n \equiv 0 \pmod 9 &\implies a \equiv \pm 4, \pm 5, \pm 13 \pmod{27};\\
n \equiv \pm 3 \pmod 9 &\implies a \equiv 0, \pm 4, \pm 5, \pm 9, \pm 13 \pmod{27}.
\end{aligned}$$

When u is a fundamental unit (so that $n = \pm 1$), it follows from Theorem 6.1 that $v \in M$ if and only if $u \in P_d$. Theorem 7.3 shows that this equivalence holds for a more general set of u under the condition that the class number $h(d)$ is not a multiple of 3. We conjecture that the condition on the class number can be dropped. The proof of Theorem 7.3 depends on the following two lemmas.

Lemma 7.1. *Let $u \in S_d$. Then the principal ideal (u) factors in $\mathcal{O}(d)$ as*

$$(u) = \mathfrak{A}^3 q \mathfrak{Q}, \tag{7.3}$$

where $\mathfrak{A}$ and $\mathfrak{Q}$ are ideals, and q is a squarefree integer with $q = N(\mathfrak{Q})$, where each rational prime factor of q splits in $\mathcal{O}(d)$.

Proof. Let $\mathfrak{p}$ be a prime ideal factor of (u) lying above a rational prime p, so that for some $e \geq 1$, $\mathfrak{p}^e || (u)$. We will use the term "p-part" of (u) to denote the contribution of the ideals above p to the ideal factorization of (u). As $u \in S_d$, we can write $n^3 = N(u) = uu'$, where u' is the conjugate of u in $\mathcal{O}(d)$.

Suppose first that p does not split in $\mathcal{O}(d)$. Then $\mathfrak{p}^{2e}$ exactly divides $(uu') = (n^3)$, so that $3 \mid e$. Thus the p-part of (u) is a cube, which can be absorbed in (7.3) by $\mathfrak{A}^3$.

Now suppose that p splits and write $(p) = \mathfrak{p}\mathfrak{p}'$. Since $\mathfrak{p}^e || (u)$, taking norms yields $p^e \mid n^3$. Moreover, if $\mathfrak{p}' \nmid (u)$, then $p^e || n^3$, so that $3 \mid e$ and again the p-part of (u) is a cube that can be absorbed by $\mathfrak{A}^3$. It remains to consider the case when $\mathfrak{p}' \mid (u)$. In this case, p^i divides u for some $i \in \{1,2\}$ with $e \geq i$. (We cannot have $i > 2$ by definition of S_d.) We may assume that $3 \nmid e$, otherwise we revert back to the previous situations where the p-part is a cube. We have $\mathfrak{p}^{e-i} || (u/p^i)$. By taking norms, $p^{e-i} || (n^3/p^{2i})$. Thus $p^{e+i} || n^3$, so that $3 | (e+i)$. Therefore $e = 2i + 3k$ for some $k \in \mathbb{Z}$. Since $-i \leq e - 2i = 3k$, we must have $k \geq 0$. The p-part of (u) is $p^i \mathfrak{p}^{e-i} = p^i \mathfrak{p}^i \mathfrak{p}^{3k}$. The cube $\mathfrak{p}^{3k}$ can be absorbed by $\mathfrak{A}^3$. Taking the product of the p-parts of (u) over all p, we could obtain (7.3), where $\mathfrak{Q}$ is the product of the $\mathfrak{p}^i$ and $q = N(\mathfrak{Q})$ is the product of the p^i, but we need $i = 1$ for every p in order to ensure that q is squarefree. Fortunately, we can rearrange each product $p^2\mathfrak{p}^2$ so that the exponents equal 1, using $p^2\mathfrak{p}^2 = p\mathfrak{p}'\mathfrak{p}^3$. □

Let R_d be the set of $\beta \in \mathcal{O}(d)$ having the form $\beta = nr + ns\sqrt{d}$, where $r + s\sqrt{d}$ has norm n (so that $N(u) = n^3$). For example, $\beta = (31 + 155\sqrt{5})/2 \in R_5$ with $N(\beta) = -31^3$. An example of an element of S_d that is not in R_d is $u = 1376 + 387\sqrt{79}$, for which $N(u) = -215^3$.

We provide a computer-generated proof via Mathematica for the following lemma.

Lemma 7.2. *Let $\beta, \gamma \in R_d$, $\mu \in \mathcal{O}(d)$, with norms $N(\mu)$ and $N(\gamma)$ both nonzero modulo 3. Then*

$$\beta \in P_d \Longleftrightarrow \beta\mu^3 \in P_d \tag{7.4}$$

and

$$(\beta \in P_d \text{ and } \gamma \in P_d) \Longrightarrow \beta\gamma \in P_d. \tag{7.5}$$

Proof. Write $\mu = x + y\sqrt{d}$ and $\beta = nr + ns\sqrt{d}$ with $n = r^2 - ds^2$, so that $N(\beta) = n^3$. Create in Mathematica the master set of 9,565,938 quintuples (r, s, x, y, d) modulo 27 for which $x^2 - dy^2$ is nonzero modulo 3. Compute the subset of the master set for which $(nr + ns\sqrt{d})(x + y\sqrt{d})^3 \in P_d$. This turns out to be exactly the same subset for which $\beta = nr + ns\sqrt{d} \in P_d$, thereby proving (7.4).

Next, write $\gamma = mx + my\sqrt{d}$ with $m = x^2 - dy^2$, so that $N(\gamma) = m^3$. Using the same master set, compute the subset for which $(nr + ns\sqrt{d})(mx + my\sqrt{d}) \in P_d$. This turns out to contain the subset for which both of these factors lie in P_d, thus proving (7.5). The details of the Mathematica proof are given in [4]. □

For $u \in S_d$, recall that ν denotes the real cube root $u^{1/3}$, n denotes the cube root of the norm of u, and v denotes the real cube root of the fundamental unit $f(d)$.

Theorem 7.3. *Let $u \in S_d^*$ have nonzero norm modulo 3. Assume that $3 \nmid h(d)$. Then $\nu \in M$ if and only if $u \in P_d$.*

Proof. By definition of S_d^*, any rational prime dividing u must ramify in $\mathcal{O}(d)$. Thus, by Lemma 7.1, we have $(u) = \mathfrak{A}^3$ for some ideal $\mathfrak{A}$ in $\mathcal{O}(d)$. Since $3 \nmid h(d)$ and both of $\mathfrak{A}^3$, $\mathfrak{A}^{h(d)}$ are principal, it follows that $\mathfrak{A}$ is principal. This shows that $(u) = (\mu^3)$ for some $\mu \in \mathcal{O}(d)$, so that u has the form (7.1). Without loss of generality, we will assume the plus sign in (7.1), and we write $u = f(d)(x + y\sqrt{d})^3$, where $(x + y\sqrt{d})$ is an element of $\mathcal{O}(d)$ whose norm is not divisible by 3.

Clearly $\nu = v(x + y\sqrt{d}) \in M$ if and only if $v \in M$. As noted above Lemma 7.1, $v \in M$ if and only if $f(d) \in P_d$. Thus $\nu \in M$ if and only if $f(d) \in P_d$. It remains to prove that

$$f(d) \in P_d \Longleftrightarrow f(d)(x + y\sqrt{d})^3 \in P_d. \tag{7.6}$$

This follows from the special case $\beta = f(d)$ of Lemma 7.2. □

Let M_e denote the ring class field for the order $\mathbb{Z}[e\sqrt{-3d}]$ in $F = \mathbb{Q}(\sqrt{-3d})$. In particular, $M_1 = M$. For $u \in \mathcal{O}(d)$, let $c = c(u)$ be the product of the distinct rational primes which divide u but not d. Note that for $u \in S_d$, we have $c(u) = 1$ if and only if $u \in S_d^*$.

Theorem 7.5 below extends Theorem 7.3. Just as for Theorem 7.3, we conjecture that the condition on the class number can be dropped. The proof of Theorem 7.5 is conditional on the following conjecture.

Conjecture 7.4. *Let $\beta \in \mathcal{O}(d)$ have a cubic norm with $3 \nmid N(\beta)$. Then $\beta^{1/3} \in M_c$ if and only if $\beta \in P_d$, where $c = c(\beta)$. In particular, this equivalence holds for every $\beta \in R_d$ with $3 \nmid N(\beta)$.*

Remark (7I). *Let $\beta, \gamma \in R_d$ with $3 \nmid N(\beta\gamma)$. If $\beta^{1/3} \in M_{c(\beta)}$ and $\gamma^{1/3} \in M_{c(\gamma)}$, then by definition of $M_{c(u)}$, we have $(\beta\gamma)^{1/3} \in M_{c(\beta\gamma)}$. This demonstrates that (7.5) is consistent with Conjecture 7.4.*

Theorem 7.5. *Let $u \in S_d$ have nonzero norm modulo 3. Assume that Conjecture 7.4 holds and that $3 \nmid h(d)$. Then $\nu \in M_c$ if and only if $u \in P_d$, where $c = c(u)$.*

Proof. Let $T \in \{h(d), 2h(d)\}$ be chosen such that $3 \mid (T-1)$. By (7.3),

$$(u^T) = (\mathfrak{A}^T)^3 q^T \mathfrak{Q}^T. \tag{7.7}$$

Since $\mathfrak{Q}^T$ is a principal ideal of norm q^T, we have $(q^T\mathfrak{Q}^T) = (\gamma)$ with $\gamma \in R_d$. By (7.7), $q = c$, where $c = c(u) = c(\gamma)$. Since $\mathfrak{A}^T$ is principal, we have $u^T = \mu_0^3\beta$ for some $\mu_0 \in \mathcal{O}(d)$ and $\beta \in R_d$. Therefore $u^{3k}u = \mu_0^3\beta$ for some k. Multiplying by the conjugate u'^{3k}, we obtain

$$j^3 u = \mu^3 \beta \tag{7.8}$$

for some $\mu \in \mathcal{O}(d)$, where $j = N(u)^k$ is not divisible by 3. Consequently

$$j\nu = \mu\beta^{1/3}. \tag{7.9}$$

Since $j, \mu \in M \subset M_c$,

$$\nu \in M_c \Longleftrightarrow \beta^{1/3} \in M_c \Longleftrightarrow \beta \in P_d, \tag{7.10}$$

where the first equivalence follows from (7.9) and the second follows from Conjecture 7.4. By Lemma 7.2 and (7.8),

$$\beta \in P_d \Longleftrightarrow \mu^3\beta \in P_d \Longleftrightarrow j^3 u \in P_d \Longleftrightarrow u \in P_d. \tag{7.11}$$

The result now follows from (7.10) and (7.11). □

Some numerical examples supporting Theorem 7.5 with $3 \mid h(d)$ are given in the last section of [4].

Theorem 7.6. *Let $u \in \mathcal{O}(d)$ have a cubic norm and write $\nu = u^{1/3}$. Then $\nu \in M_c$ if and only if $\nu \in M_{c'}$, where $c' = c'(u)$ denotes the odd part of $c = c(u)$.*

Proof. It suffices to prove that $\nu \in M_c$ implies $\nu \in M_{c'}$ for even c. Assume for the purpose of contradiction that $\nu \in M_c$ but $\nu \notin M_{c'}$. By [3, Thm. 7.24], M_c has degree 2 over $M_{c'}$. Thus the minimal polynomial of ν over $M_{c'}$ is quadratic. Since this quadratic polynomial must divide the cubic polynomial $x^3 - u = x^3 - \nu^3$ over $M_{c'}$, it follows that this cubic polynomial has a linear factor over $M_{c'}$. Since the cube roots of unity lie in M, we obtain the desired contradiction $\nu \in M_{c'}$. □

We close this section with two conjectures. When u is a fundamental unit, Conjecture 7.7 reduces to Theorem 1.5, while Conjecture 7.8 reduces to Theorem 6.2. Extensive numerical evidence for Conjectures 7.4, 7.7, and 7.8 is given in [4].

Conjecture 7.7. *Let $u \in S_d$ and let $c' = c'(u)$ denote the odd part of $c = c(u)$. When $\nu \in M_c$, the norm of $D(F(\nu)/F)c^{-4}$ equals 1 or 3^6 according as $3 \nmid d$ or $3 \mid d$, and when $\nu \notin M_c$, the norm of $D(F(\nu)/F)c^{-4}$ equals 3^8 or 3^{18} according as $3 \nmid d$ or $3 \mid d$, except that when $d \equiv 3 \pmod 4$, each c^{-4} is to be replaced by c'^{-4}.*

Conjecture 7.8. *For every $u \in S_d$, we have $\nu \in M_{3c}$, where $c = c(u)$.*

8. Generalization of Theorem 6.1

Let $d > 1$ be squarefree. In this section, we compute the value of $(\frac{m+n\sqrt{d}}{2})^{\frac{p-1}{3}} \pmod p$ for the primes $p = x^2 + 3dy^2$, where $m^2 - dn^2 = \pm 4$. Of course the value is $1 \pmod p$ if and only if $\frac{m+n\sqrt{d}}{2}$ is a cubic residue for these p. Theorem 6.2 shows that the value is $1 \pmod p$ whenever $3 \mid y$, so throughout this section, it will be assumed that $3 \nmid y$. The signs of x and y will be chosen such that $3 \mid (x - y)$. Theorems 8.1 and 8.2 address the cases when $m^2 - dn^2 = -4$ and $m^2 - dn^2 = 4$, respectively. In the latter case, we may assume that $p \nmid n$, since otherwise $m \equiv \pm 2 \pmod p$ so that $\frac{m+n\sqrt{d}}{2}$ is a cubic residue for p.

Set $\omega = \frac{-1+\sqrt{-3}}{2}$. We will utilize properties (8.1)–(8.4) for the cubic Jacobi symbol [11, p. 63]. For integers a, b, c, d with $3 \nmid c$, $(d, c) = 1$, and $a - 2 \equiv b \equiv 0 \pmod 3$,

$$\Big(\frac{\omega}{a+b\omega}\Big)_3 = \omega^{\frac{a+b+1}{3}}, \quad \Big(\frac{1-\omega}{a+b\omega}\Big)_3 = \omega^{\frac{2(a+1)}{3}}, \quad \Big(\frac{d}{c}\Big)_3 = 1. \tag{8.1}$$

By the cubic reciprocity law,

$$\Big(\frac{a+b\omega}{c+d\omega}\Big)_3 = \Big(\frac{c+d\omega}{a+b\omega}\Big)_3, \quad \text{when} \quad b \equiv d \equiv 0 \pmod 3, \ \ 3 \nmid ac. \tag{8.2}$$

When $a - 2 \equiv b \equiv 0 \pmod 3$, it follows from (8.1) that

$$\Big(\frac{1+2\omega}{a+b\omega}\Big)_3 = \Big(\frac{\omega(1-\omega)}{a+b\omega}\Big)_3 = \omega^{\frac{b}{3}}, \quad \Big(\frac{3}{a+b\omega}\Big)_3 = \Big(\frac{-\omega^2(1-\omega)^2}{a+b\omega}\Big)_3 = \omega^{\frac{2b}{3}}. \tag{8.3}$$

If $3 \nmid a$ and $(a^2, c^2 + 3d^2) = 1$, we have

$$\Big(\frac{c+d(1+2\omega)}{a}\Big)_3\Big(\frac{-c+d(1+2\omega)}{a}\Big)_3 = \Big(\frac{-c^2-3d^2}{a}\Big)_3 = 1,$$

and so

$$\Big(\frac{-c+d(1+2\omega)}{a}\Big)_3 = \Big(\frac{c+d(1+2\omega)}{a}\Big)_3^{-1}. \tag{8.4}$$

We will also need

$$\Big(\frac{m+n}{2} + m\omega\Big)\Big(\frac{m+n}{2} + m\omega^2\Big) = \frac{3m^2+n^2}{4}. \tag{8.5}$$

Theorem 8.1. *Suppose that $m^2 - dn^2 = -4$. Then modulo $p = x^2 + 3dy^2$, we have*

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-1}{3}} \equiv \begin{cases} 1 & \text{if } m \equiv 0, \pm 4 \pmod 9, \\ \frac{1}{2}\big(-1 + (\frac{mn/3}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv \pm 3 \pmod 9, \\ \frac{1}{2}\big(-1 - (\frac{mn}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv \pm 1 \pmod 9, \\ \frac{1}{2}\big(-1 + (\frac{mn}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv \pm 2 \pmod 9, \end{cases} \tag{8.6}$$

where $\big(\frac{\cdot}{3}\big)$ is the Legendre symbol.

Proof. When $9 \mid m$, (8.6) follows from Case 1 for Theorem 6.2, so assume from now on that $9 \nmid m$. Since $3 \nmid n$, we may choose the signs of m, n so that $m \equiv n \equiv 1 \pmod 3$ when $3 \nmid m$, and $n \equiv m/3 \equiv 1 \pmod 3$ when $3 \mid m$. It suffices to prove (8.6) for this choice of signs, since if the sign of m or n is reversed, one can take conjugates in (8.6). Observe that the Legendre symbol $\left(\dfrac{mn}{3}\right)$ equals 1 when $3 \nmid m$ and $\left(\dfrac{mn/3}{3}\right)$ equals 1 when $3 \mid m$.

Case 1: $d \equiv 2 \pmod 4$
In this case, $m_2 := m/2$ and $n_2 := n/2$ are relatively prime integers. Set $x_1 = y$ and $y_1 = \frac{y-x}{3}$. Then

$$p = (1+3d)x_1^2 - 6x_1y_1 + 9y_1^2 \tag{8.7}$$

and

$$\frac{2(1+3d)x_1 - 6y_1}{6dy_1} \equiv \frac{x}{dy} \pmod p. \tag{8.8}$$

First suppose that $3 \mid m$. Using (8.1)-(8.3) and (8.5), we deduce that

$$\begin{aligned}\Big(\frac{-6n-6m(1+2\omega)}{1+3d}\Big)_3 &= \Big(\frac{m_2+n_2+m\omega}{1+3d}\Big)_3 = \Big(\frac{m_2+n_2+m\omega}{(1+3d)n_2^2}\Big)_3\Big(\frac{m_2+n_2+m\omega}{n_2}\Big)_3\\ &= \Big(\frac{(1+3d)n_2^2}{m_2+n_2+m\omega}\Big)_3\Big(\frac{1+2\omega}{n_2}\Big)_3 = \Big(\frac{3+3m_2^2+n_2^2}{m_2+n_2+m\omega}\Big)_3\\ &= \Big(\frac{3}{m_2+n_2+m\omega}\Big)_3 = \omega^{\frac{2m}{3}}.\end{aligned}$$

Appealing to [11, Theorem 5.1] with the quadratic form (8.7), we obtain, using (8.8),

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-1}{3}} \equiv \frac{1}{2}\Big(-1+\frac{x}{dy}\sqrt{d}\Big) \pmod p,$$

as desired.

Now assume that $3 \nmid m$. Observe that $d \equiv dn^2 = m^2+4 \equiv 2 \pmod 3$. Using (8.1)-(8.3) and (8.5), we deduce that

$$\begin{aligned}&\Big(\frac{-6n-6m(1+2\omega)}{1+3d}\Big)_3\\ &= \Big(\frac{m_2+n_2+m\omega}{1+3d}\Big)_3 = \Big(\frac{-\omega^2}{1+3d}\Big)_3\Big(\frac{m+(m_2-n_2)\omega}{1+3d}\Big)_3\\ &= \Big(\frac{\omega}{-1-3d}\Big)_3^2\Big(\frac{m+(m_2-n_2)\omega}{1+3d}\Big)_3 = \omega^{-2d}\Big(\frac{m+(m_2-n_2)\omega}{n_2}\Big)_3\Big(\frac{m+(m_2-n_2)\omega}{(1+3d)n_2^2}\Big)_3\\ &= \omega^d\Big(\frac{2+\omega}{n_2}\Big)_3\Big(\frac{(1+3d)n_2^2}{m+(m_2-n_2)\omega}\Big)_3 = \omega^2\Big(\frac{-\omega^2(1-\omega)}{n_2}\Big)_3\Big(\frac{3+3m_2^2+n_2^2}{m+(m_2-n_2)\omega}\Big)_3\\ &= \omega^2\Big(\frac{\omega}{n_2}\Big)_3\Big(\frac{3}{m+(m_2-n_2)\omega}\Big)_3 = \omega^2\cdot\omega^{\frac{n_2+1}{3}}\Big(\frac{3}{-m-(m_2-n_2)\omega}\Big)_3\\ &= \omega^2\cdot\omega^{\frac{n_2+1}{3}}\cdot\omega^{-\frac{m-n}{3}} = \omega^{\frac{4-m}{3}}.\end{aligned}$$

Appealing again to [11, Theorem 5.1] with the quadratic form (8.7), we obtain (8.6).

Case 2: $d \equiv 1 \pmod 4$
In this case, m and n have the same parity. Set $x_1 = \frac{x-y}{3}$ and $y_1 = \frac{2x+4y}{3}$. Then

$$p = (3d+4)x_1^2 - (3d-2)x_1y_1 + \frac{3d+1}{4}y_1^2. \tag{8.9}$$

First suppose that $3 \mid m$. Write $n_2 = n/(n,2)$ and $m_2 = m/(n,2)$. Using (8.1)-(8.3) and also (8.5) with n replaced by $-2n$, we deduce that

$$\begin{aligned}
&\Big(\frac{-(3d-2)n - 3m(1+2\omega)}{3d+4}\Big)_3 \\
&= \Big(\frac{6n - 3m(1+2\omega)}{3d+4}\Big)_3 = \Big(\frac{m - 2n + 2m\omega}{3d+4}\Big)_3 \\
&= \Big(\frac{m_2 - 2n_2 + 2m_2\omega}{3d+4}\Big)_3 = \Big(\frac{m_2 - 2n_2 + 2m_2\omega}{n_2}\Big)_3 \Big(\frac{m_2 - 2n_2 + 2m_2\omega}{(3d+4)n_2^2}\Big)_3 \\
&= \Big(\frac{1+2\omega}{n_2}\Big)_3 \Big(\frac{(3d+4)n_2^2}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 = \Big(\frac{3m_2^2 + 4n_2^2 + 12/(n,2)^2}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 \\
&= \Big(\frac{12/(n,2)^2}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 = \Big(\frac{3}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 \Big(\frac{4/(n,2)^2}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 \\
&= \Big(\frac{3}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 \Big(\frac{m_2 - 2n_2 + 2m_2\omega}{2/(2,n)}\Big)_3^2 = \Big(\frac{3}{m_2 - 2n_2 + 2m_2\omega}\Big)_3 = \omega^{\frac{2m}{3}} = \omega^2.
\end{aligned}$$

Appealing to [11, Theorem 5.1] with the quadratic form (8.9), we obtain (8.6) in the case $3 \mid m$.

Next suppose that $3 \nmid m$. Note that $d = (m^2+4)/n^2 \equiv 2 \pmod 3$. From (8.1)–(8.3),

$$\begin{aligned}
&\Big(\frac{-(3d-2)n - 3m(1+2\omega)}{3d+4}\Big)_3 \\
&= \Big(\frac{6n - 3m(1+2\omega)}{3d+4}\Big)_3 = \Big(\frac{m - 2n + 2m\omega}{3d+4}\Big)_3 \\
&= \Big(\frac{-\omega^2}{3d+4}\Big)_3 \Big(\frac{-\omega(m - 2n + 2m\omega)}{3d+4}\Big)_3 = \Big(\frac{\omega^2}{3d+4}\Big)_3 \Big(\frac{2m + (m+2n)\omega}{3d+4}\Big)_3 \\
&= \Big(\frac{\omega}{-4-3d}\Big)_3^2 \Big(\frac{2m_2 + (m_2+2n_2)\omega}{3d+4}\Big)_3 \\
&= \omega^{\frac{1-4-3d}{3}} \Big(\frac{2m_2 + (m_2+2n_2)\omega}{n_2}\Big)_3 \Big(\frac{2m_2 + (m_2+2n_2)\omega}{(3d+4)n_2^2}\Big)_3 \\
&= \omega^{-d-1} \Big(\frac{2+\omega}{n_2}\Big)_3 \Big(\frac{(3d+4)n_2^2}{2m_2 + (m_2+2n_2)\omega}\Big)_3 \\
&= \Big(\frac{-\omega^2(1-\omega)}{n_2}\Big)_3 \Big(\frac{3m_2^2 + 4n_2^2 + 12/(2,n)^2}{2m_2 + (m_2+2n_2)\omega}\Big)_3 = \Big(\frac{\omega}{n_2}\Big)_3 \Big(\frac{12/(n,2)^2}{2m_2 + (m_2+2n_2)\omega}\Big)_3 \\
&= \Big(\frac{\omega}{n_2}\Big)_3 \Big(\frac{3}{2m_2 + (m_2+2n_2)\omega}\Big)_3 \Big(\frac{2/(n,2)}{2m_2 + (m_2+2n_2)\omega}\Big)_3^2 \\
&= \Big(\frac{\omega}{n_2}\Big)_3 \Big(\frac{3}{2m_2 + (m_2+2n_2)\omega}\Big)_3 \Big(\frac{2m_2 + (m_2+2n_2)\omega}{2/(n,2)}\Big)_3^2 \\
&= \Big(\frac{\omega}{n_2}\Big)_3 \Big(\frac{3}{2m_2 + (m_2+2n_2)\omega}\Big)_3 \Big(\frac{\omega}{2/(n,2)}\Big)_3^2 = \omega^{\frac{4-m}{3}}.
\end{aligned}$$

Appealing once again to [11, Theorem 5.1] with the quadratic form (8.9), we obtain (8.6) in the case $3 \nmid m$, which completes the proof. □

From now on let $m^2 - dn^2 = 4$, so that $(m-2)(m+2) = dn^2$. Always choose a sign of m so that $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. Set $m_1 = \frac{m-2}{(m-2,n)}$ and $n_1 = \frac{n}{(m-2,n)}$. Then $(m_1, n_1) = 1$ and $3 \nmid n_1$. Fix the sign of n so that $n_1 \equiv 1 \pmod 3$. For brevity, define $\alpha = \mathrm{ord}_3(m-2)$, $\beta = \mathrm{ord}_3 n$, and $\gamma = \mathrm{ord}_3 d$. From the formula for dn^2, we have $\alpha = \gamma + 2\beta$ when $\beta > 0$. If $3 \nmid m_1$ and $\beta > 0$, then $\beta = \alpha = \gamma + 2\beta$, which is impossible. Thus

$$3 \nmid m_1 \Longleftrightarrow 3 \nmid (m-2)n. \tag{8.10}$$

Let $m_4 = 4m_1/(m-2,n)$, which is an integer since $m_4 = dn_1^2 - m_1^2$. Let m_0 denote the odd part of m_4. We have $m_0 \mid m_1$, so m_0 is relatively prime with n_1. Also m_0 divides $m_4(m+2) = 4dn_1^2$. Thus

$$m_0 \mid d. \tag{8.11}$$

Consequently $(m_4, 3d+1) = 1$ when $2 \mid d$ and $(m_4, 3d+4) = 1$ when $2 \nmid d$.

We claim that

$$9 \mid m_1 \Longleftrightarrow m \equiv 2 \pmod{27}. \tag{8.12}$$

To see this, observe that (8.12) is equivalent to

$$\alpha - \beta \geq 2 \Longleftrightarrow \alpha \geq 3. \tag{8.13}$$

If $\beta = 0$, then $\alpha \leq 1$, so both sides of (8.13) are false. If $\beta > 0$, then (8.13) is equivalent to

$$\gamma + \beta \geq 2 \Longleftrightarrow \gamma + 2\beta \geq 3. \tag{8.14}$$

Since $\gamma = 0$ or $\gamma = 1$, (8.14) holds, so (8.12) is proved.

In view of (8.12), the proof in Case 2 of Theorem 6.2 shows that if either $9 \mid m$ or $m \equiv 2 \pmod{27}$, then $\frac{m+n\sqrt{d}}{2}$ is a cubic residue of the primes $p = x^2 + 3dy^2$. The converse is a consequence of the following technical theorem.

Theorem 8.2. *Suppose that $m^2 - dn^2 = 4$, $9 \nmid m$, $27 \nmid (m-2)$, and $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. Then modulo $p = x^2 + 3dy^2$, we have*

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-1}{3}} \equiv \begin{cases} \frac{1}{2}\big(-1 + (\frac{(m-2)n/3}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv 5, 8 \pmod 9, \\ \frac{1}{2}\big(-1 - (\frac{(m-2)n/27}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv 11, 20 \pmod{27}, \\ \frac{1}{2}\big(-1 + (\frac{mn/3}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv 0 \pmod 3, \\ \frac{1}{2}\big(-1 + (\frac{(m+2)n/3}{3})\frac{x}{dy}\sqrt{d}\big) & \text{if } m \equiv 1 \pmod 3, \end{cases} \tag{8.15}$$

where $\big(\frac{\cdot}{3}\big)$ is the Legendre symbol.

Proof. Note that $9 \nmid n$, otherwise 27 would divide $m-2$. When $3 \mid (m-2)$, we have $3 \parallel m_1$ by (8.10) and (8.12).

Case 1: $2 \mid d$.

In this case $(m,n)=2$. Suppose first that $3 \mid (m-2)$, so that either $m \equiv 5,8 \pmod 9$ or $m \equiv 11,20 \pmod{27}$. Using (8.1)–(8.3) and (8.5), we see that

$$\begin{aligned}
&\Big(\frac{-6n_1+6m_1(1+2\omega)}{3d+1}\Big)_3 \\
&= \Big(\frac{m_1-n_1+2m_1\omega}{3d+1}\Big)_3 = \Big(\frac{m_1-n_1+2m_1\omega}{n_1}\Big)_3\Big(\frac{m_1-n_1+2m_1\omega}{(3d+1)n_1^2}\Big)_3 \\
&= \Big(\frac{1+2\omega}{3d+1}\Big)_3\Big(\frac{(3d+1)n_1^2}{m_1-n_1+2m_1\omega}\Big)_3 = \Big(\frac{3m_1^2+n_1^2+3m_4}{m_1-n_1+2m_1\omega}\Big)_3 \\
&= \Big(\frac{3m_4}{m_1-n_1+2m_1\omega}\Big)_3 = \Big(\frac{3}{m_1-n_1+2m_1\omega}\Big)_3\Big(\frac{m_4}{m_1-n_1+2m_1\omega}\Big)_3.
\end{aligned}$$

Assume that $m \equiv 5,8 \pmod 9$. Then $3 \parallel m_1$, $3 \nmid n$ and $3 \parallel \frac{m-2}{(m-2,n)^2}$. From the above we deduce that

$$\begin{aligned}
&\Big(\frac{-6n_1+6m_1(1+2\omega)}{3d+1}\Big)_3 \\
&= \Big(\frac{3^2}{m_1-n_1+2m_1\omega}\Big)_3\Big(\frac{m_4/3}{m_1-n_1+2m_1\omega}\Big)_3 \\
&= \omega^{\frac{2m_1}{3}}\Big(\frac{m_1-n_1+2m_1\omega}{m_4/3}\Big)_3 \\
&= \omega^{\frac{2m_1}{3}}\Big(\frac{-n_1}{m_4/3}\Big)_3 = \omega^{\frac{2m_1}{3}} = \omega^{2(\frac{(m-2)n/3}{3})},
\end{aligned}$$

where the last equality follows because $(m-2,n)^2 \equiv 1 \pmod 3$.

Applying [11, Thm. 5.5] with the quadratic form (8.7), and using (8.8), we obtain the first line in (8.15).

Next assume $m \equiv 11,20 \pmod{27}$. Then $9 \parallel m-2$. By (8.10) and (8.12), $3 \parallel m_1$. Hence $3 \parallel n$ and $3 \nmid m_4$. This time

$$\begin{aligned}
&\Big(\frac{-6n_1+6m_1(1+2\omega)}{3d+1}\Big)_3 \\
&= \Big(\frac{3}{m_1-n_1+2m_1\omega}\Big)_3\Big(\frac{m_4}{m_1-n_1+2m_1\omega}\Big)_3 \\
&= \omega^{\frac{m_1}{3}}\Big(\frac{m_1-n_1+2m_1\omega}{m_4}\Big)_3 = \omega^{\frac{m_1}{3}}\Big(\frac{-n_1}{m_4}\Big)_3 = \omega^{\frac{m_1}{3}} = \omega^{(\frac{(m-2)n/27}{3})},
\end{aligned}$$

where the last equality follows because $(m-2,n)^2 \equiv 0 \pmod 9$.

Applying [11, Thm. 5.5] with the quadratic form (8.7), and using (8.8),we obtain the second line in (8.15).

Finally assume that $m \equiv 0,1 \pmod 3$. We have $9 \nmid m$, $3 \nmid m-2$ and $3 \nmid n$ since $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. Hence $3 \nmid m_1 n_1$ and so $4(2-m) \equiv m_4 = m_1^2 - dn_1^2 \equiv 1-d \pmod 3$. This implies $d \equiv m-1 \pmod 3$.

First assume $m_1 \equiv n_1 \pmod 3$. Then

$$\begin{aligned}
&\Big(\frac{-6n_1+6m_1(1+2\omega)}{3d+1}\Big)_3\\
&=\Big(\frac{m_1-n_1+2m_1\omega}{3d+1}\Big)_3=\Big(\frac{\omega}{3d+1}\Big)_3\Big(\frac{m_1+n_1-(m_1-n_1)\omega}{3d+1}\Big)_3\\
&=\omega^{-d}\Big(\frac{m_1+n_1-(m_1-n_1)\omega}{n_1}\Big)_3\Big(\frac{m_1+n_1-(m_1-n_1)\omega}{(3d+1)n_1^2}\Big)_3\\
&=\omega^{-d}\Big(\frac{1-\omega}{n_1}\Big)_3\Big(\frac{(3d+1)n_1^2}{m_1+n_1-(m_1-n_1)\omega}\Big)_3\\
&=\omega^{-d}\Big(\frac{1-\omega}{n_1}\Big)_3\Big(\frac{3m_1^2+n_1^2+3m_4}{m_1+n_1-(m_1-n_1)\omega}\Big)_3\\
&=\omega^{-d}\Big(\frac{1-\omega}{-n_1}\Big)_3\Big(\frac{3m_4}{m_1+n_1-(m_1-n_1)\omega}\Big)_3\\
&=\omega^{-d}\cdot\omega^{\frac{2(1-n_1)}{3}}\Big(\frac{3}{m_1+n_1-(m_1-n_1)\omega}\Big)_3\Big(\frac{m_4}{m_1+n_1-(m_1-n_1)\omega}\Big)_3\\
&=\omega^{\frac{2(1-n_1)}{3}-d}\Big(\frac{3}{m_1+n_1-(m_1-n_1)\omega}\Big)_3\Big(\frac{m_1+n_1-(m_1-n_1)\omega}{m_4}\Big)_3\\
&=\omega^{\frac{2(1-n_1)}{3}-d}\cdot\omega^{\frac{2(n_1-m_1)}{3}}\Big(\frac{1+\omega}{m_4}\Big)_3=\omega^{\frac{2(1-m_1)}{3}-d}\Big(\frac{-\omega^2}{m_4}\Big)_3\\
&=\omega^{\frac{m_1-1}{3}+(1-m)}\Big(\frac{\omega}{-m_4^2}\Big)_3=\omega^{\frac{1-(m+1)(\frac{m-2}{3})}{3}},
\end{aligned}$$

where the last equality follows (after a tedious calculation) using the congruence $m-2 \equiv (m-2,n) \pmod 3$.

If on the other hand $m_1 \equiv -n_1 \pmod 3$, then by (8.4),

$$\Big(\frac{-6n_1+6m_1(1+2\omega)}{3d+1}\Big)_3=\Big(\frac{-6(-n_1)+6m_1(1+2\omega)}{3d+1}\Big)_3^{-1}=\omega^{-\frac{1-(m+1)(\frac{m-2}{3})}{3}}.$$

Since $m_1 \equiv (\frac{(m-2)n}{3})n_1 \pmod 3$, we have in either case

$$\Big(\frac{-6n_1+6m_1(1+2\omega)}{3d+1}\Big)_3=\omega^{(\frac{(m-2)n}{3})\frac{1-(m+1)(\frac{m-2}{3})}{3}}=\omega^{(\frac{n}{3})\frac{(\frac{m-2}{3})-(m+1)}{3}}.$$

The rightmost member equals $\omega^{-(\frac{mn/3}{3})}$ or $\omega^{-(\frac{(m+2)n/3}{3})}$ according as m is congruent to 0 or 1 mod 3. Applying [11, Theorem 5.5] with the quadratic form (8.7), and using (8.8), we obtain the last two lines of (8.15).

Case 2: $2 \nmid d$.

Setting $x_1 = y$ and $y_1 = \frac{x+2y}{3}$, we have

$$p=(3d+4)x_1^2-12x_1y_1+9y_1^2, \tag{8.16}$$

and setting $x_2 = \frac{x-y}{3}$ and $y_2 = -\frac{2x+4y}{3}$, we get

$$p=(3d+4)x_2^2+(3d-2)x_2y_2+\frac{3d+1}{4}y_2^2 \quad \text{for} \quad d\equiv 1 \pmod 4. \tag{8.17}$$

Note that

$$\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3=\Big(\frac{(3d-2)n_1+3m_1(1+2\omega)}{3d+4}\Big)_3. \tag{8.18}$$

It is easy to check that

$$\frac{2(3d+4)x_1-12y_1}{6dy_1}=\frac{2(3d+4)x_2+(3d-2)y_2}{3dy_2}\equiv-\frac{x}{dy}\pmod p \tag{8.19}$$

and

$$(m_1-2n_1+2m_1\omega)(m_1-2n_1+2m_1\omega^2)=3m_1^2+4n_1^2=(3d+4)n_1^2-3m_4. \tag{8.20}$$

Formulas (8.17)–(8.19) will be needed later when applying [11, Theorem 5.5] for the case $d\equiv 1 \pmod 4$.

Suppose first that $3\mid(m-2)$, so that either $m\equiv 5,8 \pmod 9$ or $m\equiv 11,20 \pmod{27}$. Using (8.1)–(8.3) and (8.20), we see that

$$\begin{aligned}&\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3\\&=\Big(\frac{m_1-2n_1+2m_1\omega}{3d+4}\Big)_3=\Big(\frac{m_1-2n_1+2m_1\omega}{n_1}\Big)_3\Big(\frac{m_1-2n_1+2m_1\omega}{(3d+4)n_1^2}\Big)_3\\&=\Big(\frac{1+2\omega}{n_1}\Big)_3\Big(\frac{(3d+4)n_1^2}{m_1-2n_1+2m_1\omega}\Big)_3\\&=\Big(\frac{3m_1^2+4n_1^2+3m_4}{m_1-2n_1+2m_1\omega}\Big)_3=\Big(\frac{3^2\cdot m_4/3}{m_1-2n_1+2m_1\omega}\Big)_3.\end{aligned}$$

Assume that $m\equiv 5,8 \pmod 9$. Then $3\parallel m_1$, $3\nmid n$ and $3\parallel m_4$. We have

$$\begin{aligned}&\Big(\frac{m_4/3}{m_1-2n_1+2m_1\omega}\Big)_3=\Big(\frac{m_1-2n_1+2m_1\omega}{m_4/3}\Big)_3\\&=\Big(\frac{m_1-2n_1+2m_1\omega}{m_0/3}\Big)_3=\Big(\frac{-2n_1}{m_0/3}\Big)_3=1.\end{aligned}$$

Hence,

$$\begin{aligned}&\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3=\Big(\frac{3}{-m_1+2n_1-2m_1\omega}\Big)_3^2\\&=\omega^{\frac{m_1}{3}}=\omega^{(\frac{m_1n_1/3}{3})}=\omega^{(\frac{(m-2)n/3}{3})}.\end{aligned}$$

Applying [11, Thm. 5.5] with the quadratic forms (8.16),(8.17) and using (8.19), we obtain the first line in (8.15).

Next assume $m\equiv 11,20 \pmod{27}$. Then $9\parallel m-2$. By (8.10) and (8.12), $3\parallel m_1$. Hence $3\parallel n$ and $3\nmid m_4$. We have

$$\begin{aligned}&\Big(\frac{m_4}{m_1-2n_1+2m_1\omega}\Big)_3=\Big(\frac{m_1-2n_1+2m_1\omega}{m_4}\Big)_3\\&=\Big(\frac{m_1-2n_1+2m_1\omega}{m_0}\Big)_3=\Big(\frac{-2n_1}{m_0}\Big)_3=1.\end{aligned}$$

Hence,

$$\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3=\Big(\frac{3}{-m_1+2n_1-2m_1\omega}\Big)_3$$
$$=\omega^{\frac{2m_1}{3}}=\omega^{(\frac{2m_1n_1/3}{3})}=\omega^{(\frac{2(m-2)n/27}{3})}.$$

Applying [11, Thm. 5.5] with the quadratic forms (8.16),(8.17) and using (8.19), we obtain the second line in (8.15).

Finally assume that $m\equiv 0,1 \pmod 3$. As in Case 1, we have $9\nmid m$, $3\nmid m-2$ and $3\nmid n$. Hence $3\nmid m_1n_1$ and so $4(2-m)\equiv m_4=m_1^2-dn_1^2\equiv 1-d \pmod 3$. This implies $d\equiv m-1 \pmod 3$.

First assume $m_1\equiv n_1 \pmod 3$. Then

$$\begin{aligned}
&\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3\\
&=\Big(\frac{m_1-2n_1+2m_1\omega}{3d+4}\Big)_3=\Big(\frac{-\omega^2}{3d+4}\Big)_3\Big(\frac{2m_1+(m_1+2n_1)\omega}{3d+4}\Big)_3\\
&=\Big(\frac{\omega}{-4-3d}\Big)_3^2\Big(\frac{2m_1+(m_1+2n_1)\omega}{n_1}\Big)_3\Big(\frac{2m_1+(m_1+2n_1)\omega}{(3d+4)n_1^2}\Big)_3\\
&=\omega^{\frac{2(1-4-3d)}{3}}\Big(\frac{2+\omega}{n_1}\Big)_3\Big(\frac{(3d+4)n_1^2}{2m_1+(m_1+2n_1)\omega}\Big)_3\\
&=\omega^{d+1}\Big(\frac{-\omega^2(1-\omega)}{n_1}\Big)_3\Big(\frac{3m_1^2+4n_1^2+3m_4}{2m_1+(m_1+2n_1)\omega}\Big)_3\\
&=\omega^{m}\Big(\frac{\omega^2(1-\omega)}{-n_1}\Big)_3\Big(\frac{3m_4}{2m_1+(m_1+2n_1)\omega}\Big)_3\\
&=\omega^{m}\cdot\omega^{\frac{4(1-n_1)}{3}}\Big(\frac{3}{2m_1+(m_1+2n_1)\omega}\Big)_3\Big(\frac{2m_1+(m_1+2n_1)\omega}{m_4}\Big)_3\\
&=\omega^{m}\cdot\omega^{\frac{4(1-n_1)}{3}}\cdot\omega^{\frac{2(m_1+2n_1)}{3}}\Big(\frac{\omega}{m_4}\Big)_3
\end{aligned}$$

because $m_0\mid m_1$ and m_4 equals m_0 times a power of 2. Therefore

$$\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3=\omega^{m+\frac{4-4n_1+2m_1+4n_1+1-(\frac{m-2}{3})m_4}{3}}=\omega^{\frac{(m+1)(\frac{m-2}{3})-1}{3}},$$

where the last equality follows (after a tedious calculation) using the congruence $m-2\equiv(m-2,n) \pmod 3$.

If on the other hand $m_1\equiv -n_1 \pmod 3$, then by (8.4),

$$\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+4}\Big)_3=\Big(\frac{-12(-n_1)+6m_1(1+2\omega)}{3d+1}\Big)_3^{-1}=\omega^{-\frac{(m+1)(\frac{m-2}{3})-1}{3}}.$$

Since $m_1\equiv(\frac{(m-2)n}{3})n_1 \pmod 3$, we have in either case

$$\Big(\frac{-12n_1+6m_1(1+2\omega)}{3d+1}\Big)_3=\omega^{(\frac{(m-2)n}{3})\frac{(m+1)(\frac{m-2}{3})-1}{3}}=\omega^{(\frac{n}{3})\frac{m+1-(\frac{m-2}{3})}{3}}.$$

The rightmost member equals $\omega^{(\frac{mn/3}{3})}$ or $\omega^{(\frac{(m+2)n/3}{3})}$ according as m is congruent to 0 or 1 mod 3. Applying [11, Theorem 5.5] with the quadratic forms (8.16),(8.17) and using (8.19), we obtain the last two lines of (8.15). $\square$

For real b, c, let $\{U_k(b,c)\}$ be the Lucas sequence defined by

$$U_0 = 0,\ U_1 = 1, \quad U_{k+1} = bU_k - cU_{k-1} \quad (k = 1, 2, 3, \ldots).$$

It is well known that for $b^2 - 4c \neq 0$ and $k \geq 0$,

$$U_k(b,c) = \frac{1}{\sqrt{b^2-4c}}\Big(\Big(\frac{b+\sqrt{b^2-4c}}{2}\Big)^k - \Big(\frac{b-\sqrt{b^2-4c}}{2}\Big)^k\Big).$$

For squarefree $d > 1$, nonzero integers m, n, and $\varepsilon = \pm 1$, write $m^2 - dn^2 = 4\varepsilon$. Then

$$U_k(m,\varepsilon) = \frac{1}{n\sqrt{d}}\Big(\Big(\frac{m+n\sqrt{d}}{2}\Big)^k - \Big(\frac{m-n\sqrt{d}}{2}\Big)^k\Big).$$

The two corollaries below evaluate the Lucas numbers $U_{\frac{p-1}{3}}(m,\varepsilon) \pmod p$ for primes $p = x^2 + 3dy^2$ with $p \nmid n$. When $3 \mid y$, it follows from Theorem 6.2 that $\frac{m+n\sqrt{d}}{2}$ is a cubic residue mod p, so that $U_{\frac{p-1}{3}}(m,\varepsilon) \equiv 0 \pmod p$. Thus we assume that $3 \nmid y$. Fix the signs of x, y so that $x \equiv y \pmod 3$. From Theorems 6.1, 8.1 and 8.2, we deduce:

Corollary 8.3. *Suppose that $m^2 - dn^2 = -4$. Then*

$$U_{\frac{p-1}{3}}(m,-1) \equiv \begin{cases} 0 \pmod p & \text{if } m \equiv 0, \pm 4 \pmod 9, \\ \big(\frac{mn/3}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv \pm 3 \pmod 9, \\ -\big(\frac{mn}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv \pm 1 \pmod 9, \\ \big(\frac{mn}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv \pm 2 \pmod 9. \end{cases}$$

Corollary 8.4. *Suppose that $m^2 - dn^2 = 4$ with a sign of m chosen such that $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. Then*

$$U_{\frac{p-1}{3}}(m,1) \equiv \begin{cases} 0 \pmod p & \text{if } m \equiv 2 \pmod{27}, \\ \big(\frac{(m-2)n/3}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv 5, 8 \pmod 9, \\ -\big(\frac{(m-2)n/27}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv 11, 20 \pmod{27}, \\ \big(\frac{mn/3}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv 0 \pmod 3, \\ \big(\frac{(m+2)n/3}{3}\big)\frac{x}{dny} \pmod p & \text{if } m \equiv 1 \pmod 3. \end{cases}$$

Example. *Take $m = 2t$, so that $\{U_k(m,1)\}$ is a sequence of Chebyshev polynomials of the second kind in the argument t. First suppose that t is an integer multiple of 3. Choose $s \equiv 1 \pmod 3$ such that $(t^2-1)/s^2$ is squarefree. Then by Corollary 8.4 with $n = 2s$ and $d = (t^2-1)/s^2$, we have $U_{\frac{p-1}{3}}(m,1) \equiv \big(\frac{t/3}{3}\big)\frac{xs}{2y(t^2-1)} \pmod p$. For example, with $t = 21$, $s = -2$, $d = 110$, $x = y = 1$, and $p = 331$, we have $U_{110}(m,1) \equiv 249 \pmod{331}$. Next suppose that $t \equiv 2 \pmod 3$. Note that $9 \nmid (t^2-1)$, otherwise $3 \mid n$, contradicting $\mathrm{ord}_3(m-2) = 0$. With s, d, and n as above, it follows from Corollary 8.4 that $U_{\frac{p-1}{3}}(m,1) \equiv \big(\frac{(t+1)/3}{3}\big)\frac{xs}{2y(t^2-1)} \pmod p$.*

References

[1] S. Cortés-Gómez, Higher composition laws, integral trace forms and an alternative proof for the Scholz reflection principle, (2018)
https://repositorio.uniandes.edu.co/server/api/core/bitstreams/dc1e4d53-2886-49ee-a625-f03665bf831b/content

[2] N. Childress, *Class Field Theory*, Springer, New York, 2009.

[3] D. Cox, *Primes of the form* $p = x^2 + ny^2$, 3rd ed., AMS Chelsea, Providence, 2022.

[4] R. Evans, M. Van Veen, Mathematica notebook, (2024)
https://math.ucsd.edu/~revans/CubicData.nb

[5] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Z. 31 (1930), 565–582.

[6] C. Herz, Construction of class fields. In: Seminar on Complex Multiplication. Lecture Notes in Mathematics, vol 21 (1957, revised Nov. 1965) pp. 71–91, Springer, Berlin, Heidelberg.

[7] A. Hogue, K. Chakraborty, Divisibility of class numbers of certain families of quadratic fields, J. Ramanujan Math. Soc. 34 (2019), 281–289.

[8] A.Ito, On the 3-divisibility of class numbers of pairs of quadratic fields with splitting conditions, Functiones et Approx. 60(1) (2019), 61–76.

[9] S. Krishnamoorthy, R. Muneeswaran, Divisibility of the class number of the imaginary quadratic fields $\mathbb{Q}(\sqrt{1-2m^k})$, (2024)
https://arxiv.org/pdf/2111.04387v4.pdf

[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, Berlin, 2004.

[11] Z.-H. Sun, Cubic residues and binary quadratic forms, J. Number Theory 124 (2007), 62–104.

[12] T. Vaughn, The discriminant of a quadratic extension of an algebraic field, Math. Comp. 40 (1983), 685–707.

[13] J. Xie, K. Chao, A note on 3-divisibility of class number of quadratic field, Chin. Ann. Math. Ser. B 43(2) (2022), 307–318.

Department of Mathematics, UCSD, La Jolla, CA 92093-0112
Email address: revans@ucsd.edu
URL: https://mathweb.ucsd.edu/~revans

Mörikeweg 1, 73489 Jagstzell, Germany
Email address: hb3@uni-heidelberg.de
URL: https://www.mathi.uni-heidelberg.de/~flemmermeyer

School of Mathematics and Statistics,
Huaiyin Normal University,
Huaian, Jiangsu 223300, P.R. China
Email address: zhsun@hytc.edu.cn
URL: http://maths.hytc.edu.cn/szh1.htm

2138 Edinburg Avenue, Cardiff by the Sea, CA 92007
Email address: mavanveen@ucsd.edu