CUBIC RESIDUACITY OF REAL QUADRATIC INTEGERS

RON EVANS AND MARK VAN VEEN

ABSTRACT. Given a real quadratic integer $u = A + B\sqrt{D}$ with cubic norm, we identify all the classes in a related form class group that represent primes p for which u is a cubic residue mod p. A special case of this result was conjectured in a 2025 paper of Evans, Lemmermeyer, Sun, and Van Veen.

1. INTRODUCTION

For squarefree $D > 1$, write $\mathcal{O}$ for the ring of integers in $\mathbb{Q}(\sqrt{D})$. Let $\mathcal{S}_D$ denote the set consisting of those $u = A + B\sqrt{D}$ with $A, B \in \mathbb{Z}$ such that the norm $N(u)$ is a cube, u itself is not a cube in $\mathcal{O}$, and (A, B) is not divisible by the cube of a prime. A closely related set S_D was introduced in [3, Section 7]. The difference between the two sets S_D and $\mathcal{S}_D$ is that those elements μ in S_D of the form $(x + y\sqrt{D})/2$ with odd x, y have been converted to 8μ in $\mathcal{S}_D$ to ensure integer coefficients without affecting cubic residuacity. Some examples of elements in $\mathcal{S}_D$ for $D \in \{2, 3, 5, 6, 7\}$ are $19+3\sqrt{2}$, $1342+99\sqrt{3}$, $3047+176\sqrt{5}$, $1633+437\sqrt{6}$, $232 + 319\sqrt{7}$, with norms 7^3, 121^3, 209^3, 115^3, -87^3, respectively.

For $u \in \mathcal{S}_D$, define $C = C(u)$ to be the product of the distinct odd primes that divide (A, B) but not D. For example, $C(u) = 5$ for $u = 110 + 10\sqrt{41}$, while $C(u) = 1$ for $u = 25 + 5\sqrt{30}$.

Corresponding to $u \in \mathcal{S}_D$, let $d = -27C^2D$, where $C = C(u)$. Let $H = H(4d)$ be the form class group of discriminant $4d$ consisting of the classes of primitive binary quadratic forms $[a, 2b, c]$ with $a > 0$ and $d = b^2 - ac$.

The primary purpose of this paper is to prove Theorem 1.1 below, which identifies the classes in H that represent primes $p \equiv 1 \pmod 3$ for which $u = A + B\sqrt{D}$ is a cubic residue mod p. Note that $\sqrt{D}$ mod p exists for such p, since d is a square mod p [4, Prop. 12.3.1], [5, Sec. 6.2]. The cubic residuacity of u does not depend on the choice of $\sqrt{D}$ mod p, since $N(u)$ is a cube. Theorem 1.1 is proved in Section 3.

Versions of Theorem 1.1 for fundamental units u are due to Sun [6, Section 5]. The special case of our Theorem 1.1 applied to the principal class in H proves the conjecture in [3, Conj. 7.8]. That conjecture asserted that the real cube root of every $u \in \mathcal{S}_D$ lies in the ring class field for the order $\mathbb{Z}[3C\sqrt{-3D}]$ in $\mathbb{Q}(\sqrt{-3D})$. This means that for primes p of the form $p = x^2 + 27C^2Dy^2$, *every* $u \in \mathcal{S}_D$ with $C(u) = C$ is a cubic residue mod p. We remark that the same is not true for primes p of the forms $p = x^2 + 3C^2Dy^2$, $p = x^2 + 27CDy^2$, or $p = x^2 + 27Dy^2$. For example, $17 + 51\sqrt{2} \in \mathcal{S}_2$ is not cubic mod any of the primes $p = 1759 = 25 + 3C^2D$, $p = 919 = 1 + 27CD$, $p = 79 = 25 + 27D$.

Date: Nov 2025.

2020 *Mathematics Subject Classification.* 11A15, 11E16, 11R29.

Key words and phrases. Artin symbol, Dirichlet composition, Cebotarev density, binary quadratic forms, form class group, real quadratic integers, cubic reciprocity, cubic residuacity.

Define $\omega = (-1 + i\sqrt{3})/2$. Our proof of Theorem 1.1 is based on a modification of an ingenious argument of Sun [7], which invokes properties of the cubic residue symbol $\left(\frac{*}{*}\right)_3$ for the Eisenstein integers $\mathbb{Z}[\omega]$ [1, Ch. 8], [5, Sec. 7.1].

Theorem 1.1. *Let $u = A + B\sqrt{D} \in \mathcal{S}_D$ and let $p \equiv 1 \pmod 3$ be a prime represented by a class $[a, 2b, c] \in H$, so that $p = ax^2 + 2bxy + cy^2$ for some integers x, y. Assume that*

$$(ap, 3N(u)Dy) = 1. \tag{1.1}$$

Write $C = C(u)$. Then u is a cubic residue mod p if and only if

$$\left(\frac{9A - (B/C)b(1 + 2\omega)}{a}\right)_3 = 1. \tag{1.2}$$

Observe that the symbol in (1.2) is independent of the choice of prime p represented by $[a, 2b, c]$.

After the following comments demonstrating the "insignificance" of the restriction (1.1), we provide an example for Theorem 1.1. Let $\mathcal{C}$ be any class in H. By [2, pp. 149–150], $\mathcal{C}$ represents infinitely many primes. Suppose that a is one of these primes with $a > 3|N(u)|D$. Then by [4, eq. 12.1.4], [5, Sec. 6.2], $\mathcal{C}$ can be written as $[a, 2b, c]$ for some integers b, c. Let $p > a$ be a prime with $p = ax^2 + 2bxy + cy^2$. Since $(ax + by)^2 - dy^2 = ap$, we have $(ap, y) = 1$, so that $(ap, 3N(u)Dy) = 1$. In short, there always exists a form $(a, 2b, c) \in \mathcal{C}$ that satisfies (1.1) for infinitely many primes p represented by $\mathcal{C}$.

Example 1.2. *Let $u = 6 + 3\sqrt{7}$, so that $N(u) = -27$, $D = 7$, and $C = 3$. The class group H consists of 36 classes of discriminant $4d = -6804$, half of which represent primes $p \equiv 1 \pmod 3$. Here (1.2) holds for six classes in H, namely*

$$[1, 0, 1701],\ [7, 0, 243],\ [19, \pm 6, 90],\ [22, \pm 18, 81]. \tag{1.3}$$

The classes in (1.3) are precisely those in H that represent primes $p \equiv 1 \pmod 3$ for which u is a cubic residue mod p. As is explained in Section 4, it should come as no surprise that the classes in (1.3) form a subgroup of index 6 in the class group, since the same is true in general for the classes satisfying (1.2).

In the sequel, let $u = A + B\sqrt{D} \in \mathcal{S}_D$, $[a, 2b, c] \in H$ and $f = f(x, y) = ax^2 + 2bxy + cy^2$ for integers x, y (where f need not be prime). We have

$$(ax + by)^2 - dy^2 = af(x, y). \tag{1.4}$$

When $3 \nmid f(x, y)$, define

$$L = L(u) = L(u, f) = \left(\frac{9Ay + (B/C)(ax + by)(1 + 2\omega)}{f(x, y)}\right)_3, \tag{1.5}$$

and when $3 \nmid a$, define

$$R = R(u) = R(u, f) = \left(\frac{9A - (B/C)b(1 + 2\omega)}{a}\right)_3. \tag{1.6}$$

In Theorem 2.4, we prove that $L = R$ whenever

$$(af(x, y), 3N(u)Dy) = 1. \tag{1.7}$$

This result is crucial for the proof of Theorem 1.1.

2. $L = R$

Corresponding to $u = A + B\sqrt{D} \in \mathcal{S}_D$, define $Q := (A, B/C)$. Assume that (1.7) holds. The object of this section is to prove that $L = R$ (see Theorem 2.4). Our proof makes use of the following three well-known properties of the cubic residue symbol for integers m, m', n, n' [5, Sec. 7.1]. When $3 \nmid m$,

$$\left(\frac{1+2\omega}{m+3n\omega}\right)_3 = \omega^{jn}, \quad \text{where } j = \left(\frac{m}{3}\right).$$

When $(n, 3m) = 1$,

$$\left(\frac{m}{n}\right)_3 = 1.$$

When $3 \nmid mm'$,

$$\left(\frac{m+3n\omega}{m'+3n'\omega}\right)_3 = \left(\frac{m'+3n'\omega}{m+3n\omega}\right)_3.$$

We proceed with three lemmas.

Lemma 2.1. *Let q be a prime dividing Q. Write $s = v_q(A)$ and $r = v_q(B/C)$, where $v_q(n)$ denotes the largest power of q dividing n. If either $q > 2$ or $q = 2$ with $2 \mid D$, then $s > r$. If $q = 2$ with $2 \nmid D$, then $s = r$.*

Proof. By definition of q, the integers r, s are positive. Recall that $N(u) = A^2 - B^2D$.

First suppose that $q > 2$. If $q \mid D$ (so that $q \nmid C$), then $v_q(B^2D) = 2r + 1$. If $q \nmid D$ (so that $q \mid C$), then $v_q(B^2D) = 2r + 2$. Suppose for the purpose of contradiction that $s \leq r$. Then $v_q(N(u)) = 2s$. Since $N(u)$ is a cube, $3 \mid s$, so that $r \geq s \geq 3$. Then (A, B) is divisible by q^3, which contradicts the definition of the set $\mathcal{S}_D$. Therefore $s > r$.

Next suppose that $q = 2$, so that $3 \mid v_2(N(u))$. If D is even, then arguing by contradiction as above, we see that $s > r$. If D is odd, then clearly we must have $r = s \leq 2$ (with strict inequality when $D \equiv 3 \pmod 4$).

□

Define $u_2 = (A_2 + B_2\sqrt{D})/T$, where $A_2 = BD^2$, $B_2 = AD$, and T is the largest integer cube dividing (A_2, B_2). We have $u_2 = (\sqrt{D})^3 u/T$ and $N(u_2) = -D^3N(u)/T^2$, so $u_2 \in \mathcal{S}_D$. Note that $C = C(u) = C(u_2)$. By (1.7), $(T, af(x, y)) = 1$, because any prime divisor of T must also divide D.

Lemma 2.2. $R(u) = R(u_2)$.

Proof. Since $b^2 - ac = d = -27C^2D$, we have $b \equiv 3C\sigma \pmod a$, where σ is a square root of $-3D \bmod a$. Then

$$R(u_2) = \left(\frac{9BD - (A/C)b(1+2\omega)}{a}\right)_3 = \left(\frac{9BD - 3A\sigma(1+2\omega)}{a}\right)_3,$$

so that

$$R(u_2) = \left(\frac{\sigma}{a}\right)_3 \left(\frac{-3B\sigma - 3A(1+2\omega)}{a}\right)_3.$$

Since $\left(\frac{\sigma}{a}\right)_3 = 1$ and $\left(\frac{1+2\omega}{a}\right)_3 = 1$, we obtain

$$R(u_2) = \left(\frac{9A - 3B\sigma(1+2\omega)}{a}\right)_3 = \left(\frac{9A - (B/C)b(1+2\omega)}{a}\right)_3 = R(u).$$

□

Lemma 2.3. *$L(u) = L(u_2)$.*

Proof. By (1.4), we have $ax + by \equiv 3yC\tau \pmod{f(x,y)}$, where τ is a square root of $-3D$ mod $f(x,y)$. Then

$$L(u_2) = \left(\frac{9BDy + (A/C)(ax+by)(1+2\omega)}{f(x,y)}\right)_3 = \left(\frac{9BDy + 3Ay\tau(1+2\omega)}{f(x,y)}\right)_3,$$

so that

$$L(u_2) = \left(\frac{\tau}{f(x,y)}\right)_3 \left(\frac{-3By\tau + 3Ay(1+2\omega)}{f(x,y)}\right)_3.$$

Since $\left(\frac{\tau}{f(x,y)}\right)_3 = 1$ and $\left(\frac{(1+2\omega)}{f(x,y)}\right)_3 = 1$, we obtain

$$L(u_2) = \left(\frac{9Ay + 3yB\tau(1+2\omega)}{f(x,y)}\right)_3 = \left(\frac{9Ay + (B/C)(ax+by)(1+2\omega)}{f(x,y)}\right)_3 = L(u). \tag{2.1}$$

□

In preparation for the proof of Theorem 2.4, we'll need the following additional facts. First we show that L and R are nonzero. By (1.4), the norm of the numerator of L in (1.5) is congruent modulo $af(x,y)$ to $81N(u)y^2$, which by (1.7) is coprime with $af(x,y)$. Thus L is nonzero. Since $b^2 = ac + d$ is congruent modulo a to d, the norm of the numerator of R in (1.6) is congruent mod a to $81N(u)$, which is coprime with a. Thus R is nonzero.

Recall that $Q = (A, B/C)$. By (1.7), $(Q, af(x,y)) = 1$, since $Q^2 \mid N(u)$. We proceed to show that

$$(ax + by, 3yQ') = 1, \tag{2.2}$$

where Q' denotes the odd part of Q. If some prime were to divide $(ax+by, 3y)$, then it would also divide $af(x,y)$ by (1.4), contradicting (1.7). Next let q be a prime dividing Q'. If $q \mid D$, then $q \mid d$. If $q \nmid D$, then $q \mid C$, so $q \mid d$ in either case. Therefore $q \nmid (ax + by)$, otherwise q would divide $af(x,y)$ by (1.4), contradicting the fact that $(Q, af(x,y)) = 1$. Thus (2.2) holds.

Theorem 2.4. *Suppose that (1.7) holds. Then $L = R$.*

Proof. Let $\alpha = A/Q$ and $\beta = B/(CQ)$, so that $(\alpha, \beta) = 1$. Let $\gamma = (y, \beta)$, $\beta_1 = \beta/\gamma$, $y_1 = y/\gamma$, so that $(\beta_1, y_1) = 1$. By (1.7), $(\gamma, af(x,y) = 1$. Define M by

$$M = \beta_1(ax + by) - 3y_1\alpha(1+2\omega). \tag{2.3}$$

We now show that $(N(M), af(x,y)) = 1$. Taking the norm of γM, we have

$$\gamma^2 N(M) = \beta^2(ax+by)^2 + 27y^2\alpha^2, \tag{2.4}$$

so by (1.4), $\gamma^2 N(M) = \beta^2 af(x,y) + 27y^2(\alpha^2 - \beta^2 C^2 D)$. Therefore $N(M) \equiv 27y_1^2 N(u)/Q^2 \pmod{af(x,y)}$, so by (1.7), $(N(M), af(x,y)) = 1$.

We next show that

$$(N(M), Q) = 1. \tag{2.5}$$

Let q be a prime dividing Q. If q is odd, then by Lemma 2.1, $q \nmid \beta$ and $q \mid \alpha$, so by (2.2) and (2.4), $(N(M), Q') = 1$. Now suppose that $q = 2$. To prove (2.5), it remains to show that $N(M)$ is odd. Since Q is even, $af(x,y)$ must be odd by (1.7). First suppose that D is even. Then $(ax + by)$ is odd by (1.4). By Lemma 2.1, $2 \nmid \beta$ and $2 \mid \alpha$, so $N(M)$ is odd by (2.4). Next suppose that D is odd. Then d is also odd, since C is odd. By Lemma 2.1, both α and β are odd. Therefore by (1.4), $(ax + by)$ and y have opposite parity. It now follows from (2.4) that $N(M)$ is odd. This completes the proof of (2.5).

Since $(Qy, f(x,y)) = 1$ by (1.7), it follows from (1.5) that

$$L = \left(\frac{M}{f(x,y)}\right)_3 \left(\frac{1+2\omega}{f(x,y)}\right)_3 = \left(\frac{M}{f(x,y)}\right)_3.$$

Also,

$$\left(\frac{M}{a}\right)_3^{-1} = \left(\frac{\beta_1 by + 3y_1\alpha(1+2\omega)}{a}\right)_3 = \left(\frac{\beta by + 3y\alpha(1+2\omega)}{a}\right)_3,$$

so

$$\left(\frac{M}{a}\right)_3^{-1} = \left(\frac{3A(1+2\omega) + b(B/C)}{a}\right)_3 = \left(\frac{1+2\omega)}{a}\right)_3 R = R.$$

Since $L = \left(\frac{M}{af(x,y)}\right)_3 \left(\frac{M}{a}\right)_3^{-1}$, it remains to show that $\left(\frac{M}{af(x,y)}\right)_3 = 1$. This will be done in two cases.

Case 1: $3 \mid Q$ or $3 \nmid (\beta Q)$.

By Lemma 2.1, $3 \nmid \beta$. Since $(\beta_1, 3y_1\alpha) = 1$, we have $(N(M), \beta_1) = 1$ by (2.4). In view of (2.2), we also have $(N(M), 3y_1) = 1$. Cubic reciprocity yields

$$\left(\frac{\beta_1}{M}\right)_3 = \left(\frac{M}{\beta_1}\right)_3 = \left(\frac{1+2\omega}{\beta_1}\right)_3 \left(\frac{3y_1\alpha}{\beta_1}\right)_3 = 1. \tag{2.6}$$

By (1.4) and (2.6),

$$\left(\frac{M}{af(x,y)}\right)_3 = \left(\frac{af(x,y)}{M}\right)_3 = \left(\frac{\beta_1^2(ax+by)^2 - \beta_1^2 y^2 d}{M}\right)_3.$$

By (2.4),

$$\beta_1^2(ax+by)^2 \equiv -27y_1^2\alpha^2 \pmod{N(M)},$$

so since $\beta_1 y = \beta y_1$,

$$\left(\frac{M}{af(x,y)}\right)_3 = \left(\frac{27y_1^2\alpha^2 + \beta^2 y_1^2 d}{M}\right)_3 = \left(\frac{27y_1^2 N(u)/Q^2}{M}\right)_3 = \left(\frac{y_1}{M}\right)_3^2 \left(\frac{Q}{M}\right)_3.$$

We next show that

$$\left(\frac{Q}{M}\right)_3 = 1. \tag{2.7}$$

Let q be a prime factor of Q. If $q = 3$, then

$$\left(\frac{q}{M}\right)_3 = \left(\frac{1+2\omega}{M}\right)_3^2 = \omega^{4\alpha y_1} = 1,$$

since $3 \mid \alpha$ by Lemma 2.1. If $q > 3$, then since $q \mid \alpha$ and $q \nmid \beta$ by Lemma 2.1, and since $q \nmid (ax+by)$ by (2.2), we have

$$\left(\frac{q}{M}\right)_3 = \left(\frac{M}{q}\right)_3 = \left(\frac{\beta_1(ax+by)}{q}\right)_3 = 1. \tag{2.8}$$

Now suppose that $q = 2$. First assume that D is even. Then as in the proof of (2.5), we see that α is even and $\beta(ax+by)$ is odd, so that (2.8) holds for $q = 2$. Next assume that D is odd. Then as in the proof of (2.5), α and β are odd while $(ax+by)$ and y have opposite parity, so that either (2.8) holds for $q = 2$ or else $(ax+by)$ is even and

$$\left(\frac{2}{M}\right)_3 = \left(\frac{3y_1\alpha(1+2\omega)}{2}\right)_3 = 1.$$

Thus $\left(\frac{q}{M}\right)_3 = 1$ for all primes q dividing Q, which completes the proof of (2.7).

To complete the proof for Case 1, it remains to prove that $\left(\frac{y_1}{M}\right)_3 = 1$. Write $y_1 = 3^e y_0$, with $3 \nmid y_0$. Then

$$\left(\frac{y_1}{M}\right)_3 = \left(\frac{3}{M}\right)_3^e \left(\frac{y_0}{M}\right)_3 = \left(\frac{1+2\omega}{M}\right)_3^{2e} \left(\frac{M}{y_0}\right)_3.$$

Thus

$$\left(\frac{y_1}{M}\right)_3 = \omega^{4\alpha y_1 e} \left(\frac{\beta_1(ax+by)}{y_0}\right)_3 = \omega^{4\alpha y_1 e} = 1,$$

since $3 \mid y_1 e$. This completes the proof for Case 1.

Case 2: $3 \nmid Q$ and $3 \mid \beta$.

Since $3 \mid (B/C)$ and $3 \nmid Q$, we have $3 \nmid A$. Recall that $u_2 = (A_2 + B_2\sqrt{D})/T \in \mathcal{S}_D$, where $A_2 = BD^2$, $B_2 = AD$, and T is the largest integer cube dividing (A_2, B_2). Observe that $(3C, T) = 1$, since $3 \nmid A$ and every prime factor of T must divide D.

Define $Q_2 := (A_2, B_2/C)/T$. If $3 \mid D$, then $3 \mid Q_2$. If $3 \nmid D$, then, since $3 \nmid A$, we have $3 \nmid (B_2 Q_2)$. Since (1.7) holds with u_2 in place of u, Case 1 applies to show that $L(u_2) = R(u_2)$. Then by Lemmas 2.2–2.3,

$$L(u) = L(u_2) = R(u_2) = R(u).$$

This completes the proof for Case 2.

□

3. Proof of Theorem 1.1

Proof. Let $u = A + B\sqrt{D} \in \mathcal{S}_D$ and consider a prime

$$p = f(x,y) = ax^2 + 2bxy + cy^2 \equiv 1 \pmod 3$$

with $(ap, 3yN(u)D) = 1$, where the form $[a, 2b, c]$ is in H. In view of Theorem 2.4, (1.2), and (1.6), Theorem 1.1 is equivalent to

$$u \text{ is a cubic residue } \pmod p \iff L(u) = 1. \tag{3.1}$$

By (2.1),

$$L(u) = \left(\frac{E}{p}\right)_3, \quad \text{with } E = 3A + B\tau(1+2\omega), \tag{3.2}$$

where τ is a square root of $-3D$ mod p. Since $p \equiv 1 \pmod 3$, we can write $p = \pi\overline{\pi}$ for Eisenstein primes $\pi, \overline{\pi}$. By definition of the cubic residue symbol,

$$\left(\frac{E}{\overline{\pi}}\right)_3 \equiv E^{(p-1)/3} \pmod{\overline{\pi}}.$$

Thus

$$\left(\frac{E}{\overline{\pi}}\right)_3^{-1} \equiv \overline{E}^{(p-1)/3} \pmod{\pi},$$

so that

$$\left(\frac{E}{\overline{\pi}}\right)_3 \equiv (1/\overline{E})^{(p-1)/3} \pmod{\pi}.$$

Therefore

$$L(u) = \left(\frac{E}{p}\right)_3 = \left(\frac{E}{\pi}\right)_3 \left(\frac{E}{\overline{\pi}}\right)_3 \equiv (E/\overline{E})^{(p-1)/3} \pmod{\pi}.$$

By (3.2), $E \equiv 3A \pm 3B\sqrt{D} \pmod{\pi}$, so that

$$L(u) \equiv (u/u')^{\pm(p-1)/3} \pmod{\pi},$$

where $u' = A - B\sqrt{D}$. Consequently,

$$L(u) = 1 \iff L(u) \equiv 1 \pmod{\pi} \iff (u/u')^{(p-1)/3} \equiv 1 \pmod{\pi}.$$

Since $N(u)^{(p-1)/3} \equiv 1 \pmod{\pi}$,

$$L(u) = 1 \iff (u^2)^{(p-1)/3} \equiv 1 \pmod{\pi} \iff u^{(p-1)/3} \equiv 1 \pmod{p}.$$

Therefore $L(u) = 1$ if and only if u is a cubic residue mod p, as desired. □

4. A homomorphism on H

For $u \in \mathcal{S}_D$, define a map $J : H \to \{1, \omega, \omega^2\}$ by $J(\mathcal{C}) = R(u, f)$, where $f = (a, 2b, c)$ is a form in $\mathcal{C}$ with $(a, 3N(u)D) = 1$. The map J is well-defined on H by the same proof given in [7] except with Theorem 2.4 in place of [7, Theorem 2.1]. Moreover, J is a group homomorphism. To see this, let $\mathcal{C}_i = [a_i, 2b_i, c_i] \in H$ for $i = 1, 2$, where $(a_1a_2, 3N(u)D) = 1$ and $(a_1, a_2) = 1$. Then by Dirichlet composition [2, Prop. 3.8], $\mathcal{C}_1\mathcal{C}_2 = \mathcal{C}_3$, where $\mathcal{C}_3 = [a_3, 2b_3, c_3] \in H$ is given by

$$a_3 = a_1a_2, \quad b_3 \equiv b_1 \pmod{a_1}, \quad b_3 \equiv b_2 \pmod{a_2}. \tag{4.1}$$

By (1.6) and (4.1),

$$J(\mathcal{C}_i) = \left(\frac{9A - (B/C)b_3(1+2\omega)}{a_i}\right)_3, \quad i = 1, 2.$$

Since $a_3 = a_1a_2$, we see that $J(\mathcal{C}_1)J(\mathcal{C}_2) = J(\mathcal{C}_3)$, so J is a homomorphism.

We close with the explanation promised in Example 1.2. Let H_2 denote the subgroup of index 2 in H consisting of the classes that represent primes congruent to 1 mod 3. (To see that H_2 is a group, suppose that $\mathcal{C}_1, \mathcal{C}_2$ lie in H_2. Then $a_1 \equiv a_2 \equiv 1 \pmod 3$, since the right

member of (1.4) is congruent to 1 mod 3. Thus $a_3 = a_1 a_2 \equiv 1 \pmod 3$, so $\mathcal{C}_3 \in H_2$). Let G be the set of classes in H_2 that represent primes p for which u is a cubic residue mod p. By Theorem 1.1, G is the kernel of the homomorphism $J : H_2 \to \{1, \omega, \omega^2\}$. We proceed to show that this map is an epimorphism, i.e.,

$$H_2/G \simeq \{1, \omega, \omega^2\}. \tag{4.2}$$

This will establish the promised result that G is a subgroup of index 6 in H.

To prove (4.2), we will invoke the Cebotarev density theorem [2, Theorem 8.17]. It suffices to show that u is a cubic residue mod p for primes p represented only by one third of the classes in H_2, or put another way, u is a cubic residue mod p for only "a third" of the primes p satisfying $(-3/p) = (d/p) = (D/p) = 1$. Consider the number fields $K = \mathbb{Q}(\omega, \sqrt{D})$ and $L = K(v)$, where v is the real cube root of u. Recall that u is not a cube in $\mathcal{O}$. Thus u cannot be a cube in K, so that $|\mathrm{Gal}(L/K)| = 3$. Let W be the set of first degree prime ideals $\mathfrak{p}$ in K which split completely in L. The Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ is trivial for $\mathfrak{p} \in W$, so by the Cebotarev density theorem, W has Dirichlet density $1/3$. We can now relate W to cubic residuacity, just as in the proof of [3, Theorem 1.6], to conclude that u is a cubic residue mod p for primes p represented only by one third of the classes in H_2.

Acknowledgement

The authors are grateful to Zhi-Hong Sun and Franz Lemmermeyer for helpful suggestions.

References

[1] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, Wiley, New York, 1998.
[2] D. Cox, *Primes of the form $p = x^2 + ny^2$*, 3rd ed., AMS Chelsea, Providence, RI, 2022.
[3] R. Evans, F. Lemmermeyer, Z.-H. Sun, M. Van Veen, Ring class fields and a result of Hasse, J. Number Theory 266 (2025), 33–61.
[4] A. Granville, *Number theory revealed: a masterclass*, AMS, Providence, RI, 2019.
[5] F. Halter-Koch, *Quadratic Irrationals*, CRC Press, Boca Raton, FL, 2013.
[6] Z.-H. Sun, Cubic residues and binary quadratic forms, J. Number Theory 124 (2007), no. 1, 62–104.
[7] Z.-H. Sun, Cubic congruences and binary quadratic forms, arXiv:2503.12861v2

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

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