Michigan Math. J. 69 (2020), 429–448

On Existence of Euclidean Ideal Classes in Real Cubic and Quadratic Fields with Cyclic Class Group

Sanoli Gun & Jyothsnaa Sivaraman

Abstract. Lenstra introduced the notion of Euclidean ideal classes for number fields to study cyclicity of their class groups. In particular, he showed that the class group of a number field with unit rank greater than or equal to one is cyclic if and only if it has a Euclidean ideal class. The only if part in the above result is conditional on the extended Riemann hypothesis. Graves and Murty showed that one does not require the extended Riemann hypothesis if the unit rank of the number field is greater than or equal to four and its Hilbert class field is abelian over rationals. In this article, we study real cubic and quadratic fields with cyclic class groups and show that they have a Euclidean ideal class under certain conditions.

1. Introduction

Throughout the paper $\mathbf{K}$ denotes a number field and $\mathcal{O}_{\mathbf{K}}$ denotes its ring of integers. One of the problems in algebraic number theory, which has been studied extensively, is to determine number fields $\mathbf{K}$ for which $\mathcal{O}_{\mathbf{K}}$ is Euclidean. In 1972, Weinberger [17] showed that the generalized Riemann hypothesis implies that $\mathcal{O}_{\mathbf{K}}$ is a principal ideal domain (PID) if and only if it is Euclidean provided the unit rank of $\mathcal{O}_{\mathbf{K}}$ is greater than or equal to one. In 1987, Gupta, Murty, and Murty [7] showed that the above result holds unconditionally for rings of S-integers of certain number fields. Then Clark and Murty [1] proved Weinberger's theorem without any hypothesis for certain totally real quartic extensions of $\mathbb{Q}$. This introduced a new ingredient, namely the notion of admissible primes, into these investigations. Later Harper and Murty [10] proved that if a number field $\mathbf{K}$ is Galois and its unit rank is greater than or equal to 4, then it is a PID if and only if it is Euclidean. They also showed that one can prove a similar result for abelian number fields $\mathbf{K}$ with unit rank greater than or equal to 3. In the meantime, Lenstra [12] introduced the notion of Euclidean ideal classes to study cyclicity of the class groups of number fields. Before proceeding further, let us introduce some definitions.

Definition 1. An integral domain R is said to be a Euclidean domain if there exists a map

$$\phi : R \setminus \{0\} \to \mathbb{N}$$

Received June 7, 2018. Revision received October 23, 2019.

such that, for all $s, t \in R$, $t \neq 0$, there exists $q \in R$ such that either $s = tq$ or

$$\phi(s - tq) < \phi(t).$$

It is easy to see that if R is a Euclidean domain, then there exists a Euclidean algorithm on R such that

$$\phi(su) = \phi(s) \quad \text{for any unit } u \in R \text{ and all } s \in R \setminus \{0\}.$$

For a proof of the above, we refer the reader to page 8 of [13]. From the above observation we note that, given a Euclidean algorithm on R, we can define a map on the set of integral ideals of R. Therefore the definition of a Euclidean domain given as above in terms of elements can now be rewritten in terms of ideals in the case of Dedekind domains, as we shall see in what follows.

DEFINITION 2. Let R be a Dedekind domain, E be the set of all nonzero integral ideals of R, and W be a well-ordered set. Suppose that there is a map

$$\psi : E \to W.$$

We say that R is Euclidean for ψ if R is a PID, and for each nonzero ideal $\mathfrak{b}$ of R and any $x \in \mathfrak{b}^{-1}R - R$, there exists $y \in R$ such that

$$\psi(\mathfrak{b}(x - y)) < \psi(\mathfrak{b}).$$

In case of Dedekind domains, it is easily seen that the two definitions above are equivalent. In order to prove that Definition 1 is equivalent to Definition 2, we just need to observe that if $\mathfrak{b} = bR$, then put $s = bx$, $t = b$, and $y = q$. This new interpretation of the usual definition of Euclidean domains now motivates the definition of Euclidean ideal classes.

DEFINITION 3. Let R be a Dedekind domain, E be the set of all nonzero integral ideals of R, and W be a well-ordered set. Suppose that there is a map

$$\psi : E \to W.$$

We say that a nonzero ideal $\mathfrak{a}$ of R is Euclidean for ψ if, for each nonzero ideal $\mathfrak{b}$ of R and any $x \in \mathfrak{b}^{-1}\mathfrak{a} - \mathfrak{a}$, there exists $y \in \mathfrak{a}$ such that

$$\psi(\mathfrak{a}^{-1}\mathfrak{b}(x - y)) < \psi(\mathfrak{b}).$$

Thus the second definition generalizes the notion of a Euclidean algorithm in a number field. Also if a number field $\mathbf{K}$ has a Euclidean ideal $\mathfrak{a}$ for some ψ, then every element of the class $[\mathfrak{a}]$ is a Euclidean ideal for ψ, and from now on we shall call such a class a Euclidean ideal class of $\mathbf{K}$.

After introducing the concept of Euclidean ideal, Lenstra showed that under the extended Riemann hypothesis, a number field with unit rank greater than or equal to one has cyclic class group if and only if it has a Euclidean ideal class. In a recent work, Graves and Murty [6] showed that if the unit rank of a number field $\mathbf{K}$ is greater than 4, then under certain conditions one can show that a cyclic class group implies the existence of a Euclidean ideal class. In particular, they proved the following.

THEOREM 1 (Graves and Murty [6]). *Let* $\mathbf{K}$ *be a number field with ring of integers* $\mathcal{O}_{\mathbf{K}}$ *and cyclic class group* $Cl_{\mathbf{K}}$. *If its Hilbert class field* $\mathbf{H}(\mathbf{K})$ *has an abelian Galois group over* $\mathbb{Q}$ *and if the unit rank of* $\mathcal{O}_{\mathbf{K}}^{\times}$ *is greater than or equal to* 4, *then* $\mathrm{Cl}_{\mathbf{K}} = \langle [C] \rangle$ *if and only if* $[C]$ *is a Euclidean ideal class.*

The above theorem can be compared to the result of Harper and Murty [10] in the context of existence of Euclidean algorithm. Later Narkiewicz [16] proved that there are at most two quadratic fields and at most one Galois cubic field of class number one which are not Euclidean. In this article, we prove an analogous result in the setup of Euclidean ideal classes. In particular, we investigate the question of existence of a Euclidean ideal class in real quadratic and cubic fields when their class groups are cyclic.

Before we state our results, we introduce some notation. Let $\mathbf{K}_1$, $\mathbf{K}_2$, and $\mathbf{K}_3$ be number fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, and $\mathbf{H}(\mathbf{K}_3)$ respectively, all of which are abelian over $\mathbb{Q}$. Also let f_1, f_2, and f_3 be their conductors, that is, $\mathbb{Q}(\zeta_{f_1})$, $\mathbb{Q}(\zeta_{f_2})$, and $\mathbb{Q}(\zeta_{f_3})$ be the smallest cyclotomic fields containing $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, and $\mathbf{H}(\mathbf{K}_3)$ respectively. Here ζ_{f_1}, ζ_{f_2}, and ζ_{f_3} are primitive f_1, f_2, and f_3th roots of unity respectively. Set f to be the least common multiple of 16, f_1, f_2, f_3 if $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$ are real quadratic and the least common multiple of 16, f_1, f_2 if $\mathbf{K}_1$, $\mathbf{K}_2$ are real cubic. Further put $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where ζ_f is a primitive fth root of unity. In this set up, we have the following theorems.

THEOREM 2. *Let* $\mathbf{K}_1, \mathbf{K}_2$ *be distinct real cubic fields with prime class numbers and* $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2), \mathbf{F}$, f *be as above. Also let* G *be the Galois group of* $\mathbf{F}$ *over* $\mathbf{K}_1\mathbf{K}_2$, G_ℓ *be the Galois group of* $\mathbf{F}$ *over* $\mathbb{Q}(\zeta_\ell)$, *where either* ℓ *is an odd prime dividing* f *or* $\ell = 4$, *and* $\mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ *be the Galois group of* $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ *for* $i = 1, 2$. *If*

$$G \not\subset \bigcup_{\ell} G_\ell \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

then at least one of $\mathbf{K}_1, \mathbf{K}_2$ *has a Euclidean ideal class.*

We also have an analogous result in the quadratic case.

THEOREM 3. *Let* $\mathbf{K}_1, \mathbf{K}_2$, *and* $\mathbf{K}_3$ *be distinct real quadratic fields with prime class numbers and* $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2), \mathbf{H}(\mathbf{K}_3), \mathbf{F}$, f *be as above. Also let* G *be the Galois group of* $\mathbf{F}$ *over* $\mathbf{K}_1\mathbf{K}_2\mathbf{K}_3$, G_ℓ *be the Galois group of* $\mathbf{F}$ *over* $\mathbb{Q}(\zeta_\ell)$, *where either* ℓ *is an odd prime dividing* f *or* $\ell = 4$, *and* $\mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ *be the Galois group of* $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ *for* $i = 1, 2, 3$. *If*

$$G \not\subset \bigcup_{\ell} G_\ell \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)) \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_3)),$$

then at least one of $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ *has a Euclidean ideal class.*

Now if we assume the Elliott and Halberstam conjecture (see Section 2), we can strengthen Theorem 3.

THEOREM 4. *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be distinct real quadratic fields with prime class numbers and* $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, $\mathbf{F}$, *and* f *be as above. Also let* G *be the Galois group of* $\mathbf{F}$ *over* $\mathbf{K}_1\mathbf{K}_2$, G_ℓ *be the Galois group of* $\mathbf{F}$ *over* $\mathbb{Q}(\zeta_\ell)$, *where either* ℓ *is an odd prime dividing* f *or* $\ell = 4$, *and* $\mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ *be the Galois group of* $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ *for* $i = 1, 2$. *If*

$$G \not\subset \bigcup_{\ell} G_\ell \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

then at least one of $\mathbf{K}_1$, $\mathbf{K}_2$ *has a Euclidean ideal class provided the Elliott and Halberstam conjecture holds.*

The paper is structured as follows. In Section 2, we list some preliminaries that are relevant for our work. In the next section, we prove a sequential generalization of Harper's criterion [9] in the setup of Euclidean ideal classes. In the penultimate section and in Section 4, we provide the proofs of our theorems. In the final section, we give some explicit examples for which our theorems apply.

2. Preliminaries

In this section, we state the theorems which are required to complete the proofs of our theorems. We start with a lemma of Heath-Brown which uses the idea of well factorable weights [4].

LEMMA 5 (Heath-Brown [11]). *Suppose that* u *and* v *are natural numbers with the following properties*:

$$(u, v) = 1, \quad v \equiv 0 \bmod 16, \quad \text{and} \quad \left(\frac{u-1}{2}, v\right) = 1.$$

Then there exist $a, b \in (1/4, 1/2)$ *with* $a < b$ *such that, for any* $\epsilon > 0$, *the cardinality of the set*

$$P(X) := \left\{ p \equiv u \bmod v : p \in (X^{1-\epsilon}, X) \text{ such that } \frac{p-1}{2} \text{ is either prime or} \right.$$
$$\left. \text{is a product of primes } q_1 q_2 \text{ with } X^a \le q_1 \le X^b \right\}$$

is $\gg X/\log^2 X$.

The other important ingredient is the following lemma by Narkiewicz [14] which revolves around primitive roots.

LEMMA 6 (Narkiewicz [14]). *Let* a_1, a_2, *and* a_3 *be multiplicatively independent elements of* $\mathbf{K}^\times$, T *be a set of prime ideals of degree one in* $\mathbf{K}$, *and* $\mathfrak{N}(\mathfrak{p})$ *denote the absolute norm of a prime ideal* $\mathfrak{p}$ *of* $\mathcal{O}_{\mathbf{K}}$. *Suppose that* T *has the following properties*:

(1) *There exist a constant* $c > 0$ *and an unbounded increasing sequence* $\{x_n\}_{n\in\mathbb{N}}$ *such that*

$$|T(x_n) := \{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \le x_n\}| > \frac{cx_n}{\log^2 x_n} \quad \text{for all } n.$$

(2) *There exist* $\alpha, \beta \in (1/4, 1/2)$ *with* $\alpha < \beta$ *such that, if* $\mathfrak{p} \in T$ *and* $p := \mathfrak{N}(\mathfrak{p})$, *then either* $p - 1 = 2q$ *or* $p - 1 = 2q_1q_2$, q, q_1, *and* q_2 *are primes and* $p^\alpha < q_1 < p^\beta$.

(3) *The numbers* a_1, a_2, *and* a_3 *are quadratic non-residues with respect to every prime in* T.

Then, for any $0 < \epsilon < c$, *there exists a subsequence* $\{y_m\}_{m\in\mathbb{N}}$ *of* $\{x_n\}_{n\in\mathbb{N}}$ *such that one of the* a_i*s is a primitive root for at least* $(c-\epsilon)y_m/\log^2 y_m$ *elements of* $T(y_m)$.

A proof of an analogous statement will be presented in Section 5. We now move on to some results on Euclidean ideal classes. For an integral ideal $\mathfrak{a}$ of $\mathbf{K}$, let us define

$$\begin{aligned} B_{0,\mathfrak{a}} &:= \{\mathcal{O}_{\mathbf{K}}\} \quad \text{and} \quad \text{for } i \ge 1, \\ B_{i,\mathfrak{a}} &:= \{\mathfrak{p} : \mathfrak{p} \text{ prime}, \forall x \in \mathfrak{p}^{-1}\mathfrak{a} - \mathfrak{a}, \exists y \in \mathfrak{a} \text{ such that } \mathfrak{a}^{-1}\mathfrak{p}(x-y) \in B_{i-1,\mathfrak{a}}\} \\ &\quad \cup B_{i-1,\mathfrak{a}}. \end{aligned} \tag{1}$$

Note that $B_{i,\mathfrak{a}} \setminus B_{i-1,\mathfrak{a}} \subset [\mathfrak{a}^i]$, the class of $\mathfrak{a}^i$. In this set-up, Graves [5] proved the following theorem.

THEOREM 7 (Graves [5]). *If* $\mathfrak{a}$ *is a nonzero integral ideal of* $\mathbf{K}$, *then*

$$\begin{aligned} B_{1,\mathfrak{a}} = \{\mathfrak{p} : \mathfrak{p} \textit{ is prime}, [\mathfrak{p}] = [\mathfrak{a}], \textit{every residue class of } (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^\times \textit{ contains a unit}\} \\ \cup \{\mathcal{O}_{\mathbf{K}}\}. \end{aligned}$$

Further let $B_{\mathfrak{a}} = \bigcup_i B_{i,\mathfrak{a}}$. *If* $B_{\mathfrak{a}}$ *contains all prime ideals of* $\mathbf{K}$, *then* $\mathfrak{a}$ *is a Euclidean ideal.*

The above theorem can be thought of as a generalization of a result of Clark and Murty [1]. Now let

$$B_{1,\mathfrak{a}}(X) := \{\mathfrak{p} \in B_{1,\mathfrak{a}} : \mathfrak{N}(\mathfrak{p}) \le X\} \cup \{\mathcal{O}_{\mathbf{K}}\}.$$

Graves [5] showed that to prove Theorem 7, it is sufficient to prove the following theorem.

THEOREM 8 (Graves [5]). *Suppose that* $\mathbf{K}$ *is a number field with unit rank greater than or equal to one, and* $\mathfrak{a}$ *is an integral ideal of* $\mathbf{K}$ *such that* $[\mathfrak{a}]$ *generates the class group. Further suppose that*

$$|B_{1,\mathfrak{a}}(X)| \gg \frac{X}{\log^2 X},$$

then $\mathfrak{a}$ *is a Euclidean ideal.*

The above theorem is a generalization of a result of Harper [9]. We will deduce a sequential variant of Graves theorem in the next section. In order to do that, we need to fix a few more definitions and results from [5].

DEFINITION 4. Suppose that $\mathfrak{a}$ is a nonzero integral ideal of $\mathbf{K}$ such that $[\mathfrak{a}]$ generates the class group of $\mathbf{K}$. Let $A \subset E$ be a finite set of ideals in the same equivalence class of the class group. If $\mathfrak{p}$ is a prime ideal such that $[\mathfrak{p}] = [I\mathfrak{a}]$ for any $I \in A$ and if $x \in \mathfrak{p}^{-1}\mathfrak{a}$, we define

$$Z_A(x, \mathfrak{p}, \mathfrak{a}) := \begin{cases} |\{H \in A : \text{ there exists some } y \in \mathfrak{a} \text{ such that} \\ \quad (x-y)\mathfrak{p}\mathfrak{a}^{-1} = H\}| \quad \text{if } x \notin \mathfrak{a}; \\ f(\mathfrak{p}) \times |\{H \in A : \text{ there exists some } y \in \mathfrak{a} \text{ such that} \\ \quad (x-y)\mathfrak{p}\mathfrak{a}^{-1} = H\}| \quad \text{if } x \in \mathfrak{a}. \end{cases} \tag{2}$$

The next theorem we state from [5] is a variant of Dirichlet's theorem on arithmetic progressions for ideals.

THEOREM 9 (Graves [5]). *Suppose that $\mathfrak{a}$ is a fractional ideal of $\mathbf{K}$ and $\mathfrak{b}$ is a nonzero integral ideal of $\mathbf{K}$ with $\mathfrak{b} \neq \mathcal{O}_{\mathbf{K}}$. If x is an element of $\mathfrak{a}\mathfrak{b}^{-1}$ and $x + \mathfrak{a} = \mathfrak{a}\mathfrak{b}^{-1}$, then there is a set of primes $\mathfrak{p}$ with positive density such that*

$$\mathfrak{p} = \mathfrak{b}(x-y)\mathfrak{a}^{-1}$$

for some y in $\mathfrak{a}$.

We also need the following lemma.

LEMMA 10 (Graves [5]). *Suppose that $\mathfrak{p}$, $\mathfrak{a}$ are ideals in $\mathbf{K}$ with $\mathfrak{p}$ prime such that $[\mathfrak{p}] = [\mathfrak{a}^2]$ and $[\mathfrak{a}]$ generates the class group of $\mathbf{K}$. Also suppose that $x_{\mathfrak{p}}$ is a generator of $\mathfrak{p}\mathfrak{a}^{h-2}$, where h is the class number of $\mathbf{K}$. Then the map $\phi : \mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a} \to \mathfrak{a}^{h-1}/\mathfrak{p}\mathfrak{a}^{h-1}$ defined by $\alpha + \mathfrak{a} \mapsto \alpha x_{\mathfrak{p}} + \mathfrak{p}\mathfrak{a}^{h-1}$ is an isomorphism.*

Finally we list some consequences of the large sieve inequality.

DEFINITION 5. Let $\mathfrak{a}$ be a nonzero integral ideal of $\mathbf{K}$ such that $[\mathfrak{a}]$ generates the class group of $\mathbf{K}$, and let, for some natural number n,

$$A_{\mathfrak{a}} \subset \{I : I \in E \text{ and } [I] = [\mathfrak{a}^n]\}$$

be a finite set. Then we define, for $\mathfrak{p} \in [\mathfrak{a}^{n+1}]$,

$$\omega(\mathfrak{p}, \mathfrak{a}, A_{\mathfrak{a}}) := |\{[\alpha] \in \mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a} : Z_{A_{\mathfrak{a}}}(\alpha, \mathfrak{p}, \mathfrak{a}) = 0\}|. \tag{3}$$

LEMMA 11 (Graves [5]). *Let $\mathfrak{a}$ be an integral ideal of $\mathbf{K}$ such that $[\mathfrak{a}]$ generates the class group of $\mathbf{K}$. Also let A and P be finite sets of integral ideals with $A \subset E \cap \{I : I \in [\mathfrak{a}^n]\}$ and*

$$P \subset \{\mathfrak{p} : \mathfrak{p} \text{ is prime}, [\mathfrak{p}] = [\mathfrak{a}^{n+1}]\},$$

where n is a natural number. If $X = \max_{I \in A} \mathfrak{N}(I)$ and $Q = \max_{\mathfrak{p} \in P} \mathfrak{N}(\mathfrak{p})$, then

$$\sum_{\mathfrak{p} \in P} \frac{\omega(\mathfrak{p}, \mathfrak{a}, A)}{\mathfrak{N}(\mathfrak{p})} \ll \frac{Q^2 + X}{|A|},$$

where the implied constant depends only on $\mathbf{K}$, $\mathfrak{a}$, and n.

We shall also use the result of Gupta and Murty [8] as given in Harper and Murty [10].

LEMMA 12 (Gupta and Murty [8]). *Let K be a number field with unit rank $r \geq 1$ and P_K be the set of prime ideals in $\mathcal{O}_K$. For $\mathfrak{p} \in P_K$, if $f(\mathfrak{p})$ denotes the cardinality of the set $\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^{\times}\}$, then*

$$|\{\mathfrak{p} \in P_K : f(\mathfrak{p}) \leq Y\}| \ll Y^{1+1/r}.$$

We can improve our Theorem 3 if we assume the following conjecture of Elliott and Halberstam.

CONJECTURE 1 (Elliott and Halberstam conjecture [3]). *Let a, q be natural numbers, ϕ be the Euler totient function, $\pi(Y, q, a) := \{p \leq Y : p \text{ prime in } \mathbb{Q}, p \equiv a \bmod q\}$, and $\mathrm{li}(Y) := \int_2^Y \frac{1}{\log t}\, dt$. For every real number $\theta < 1$ and for every positive integer $e > 0$, one has*

$$\sum_{q \leq X^{\theta}} \max_{Y \leq X} \max_{(a,q)=1} \left| \pi(Y, q, a) - \frac{\mathrm{li}(Y)}{\phi(q)} \right| \ll \frac{X}{\log^e X}$$

for all real numbers $X > 2$.

Under the above conjecture, one can prove the following theorem.

THEOREM 13 (Deshouillers, Gun, and Sivaraman [2]). *Suppose that the Elliott and Halberstam conjecture is true. Let $\mathbf{K}$ be a number field such that its Hilbert class field $\mathbf{H}(\mathbf{K})$ is abelian over $\mathbb{Q}$. Also let f be the conductor of $\mathbf{H}(\mathbf{K})$ and $d := \max\{n : \mathbb{Q}(\zeta_n) \subseteq \mathbf{K}\}$. Set*

$$\mathcal{A} := \left\{ \frac{\ell - 1}{d} : \ell \in \mathbb{N} \text{ is prime}, \ell \leq X \text{ and } \ell \equiv b \bmod f \right\},$$

where $b \bmod f$ is an element of the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ such that $((b-1)/d, f/d) = 1$. Then, for any real number $\eta < 1/2$, one has

$$|\{u \in \mathcal{A} : p \text{ prime}, p|u \implies p > X^{\eta}\}| \gg \frac{X}{\log^2 X},$$

where the implied constant depends on η.

REMARK 2.1. We first observe that in [2] the authors assumed that f is the conductor of $\mathbf{K}$. However, the proof holds if f is replaced by any multiple of f, say for $16f$, in the statement.

3. Sequential Variant of Theorem 8

In this section we prove a sequential variant of the criterion given by Graves in [5]. This criterion can be thought of as a generalization of Narkiewicz's result (see p. 239, Lemma 2 of [14]).

THEOREM 14. *Suppose that* $\mathbf{K}$ *is a number field with unit rank greater than or equal to one and its class group* $\mathrm{Cl}_{\mathbf{K}} = \langle [\mathfrak{a}] \rangle$. *If there exists an unbounded increasing sequence* $\{x_n\}_{n\in\mathbb{N}}$ *such that*

$$|\{\mathfrak{p} : \mathfrak{p} \text{ is prime}, [\mathfrak{p}] = [\mathfrak{a}], \mathfrak{N}(\mathfrak{p}) \le x_n, \text{ every residue class of } (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times} \text{ contains a unit}\}| \gg \frac{x_n}{\log^2 x_n},$$

then $[\mathfrak{a}]$ *is a Euclidean ideal class.*

Proof. We apply Theorem 7 to prove Theorem 14. Since every ideal class $[\mathfrak{a}]$ contains infinitely many prime ideals, to show that $[\mathfrak{a}]$ is a Euclidean ideal class, it is sufficient to show that any prime ideal in $[\mathfrak{a}]$ is a Euclidean ideal. From now onwards, we shall assume that $\mathfrak{a}$ is a prime ideal.

For $i \in \mathbb{N}$, let $B_{i,\mathfrak{a}}$ be as in (1) and $B_{\mathfrak{a}} := \bigcup_i B_{i,\mathfrak{a}}$. In order to complete the proof of Theorem 14, we need to show that all prime ideals of $\mathcal{O}_{\mathbf{K}}$ are in $B_{\mathfrak{a}}$. We start with the following definition. For $i \in \mathbb{N}$, let $B_{i,\mathfrak{a}}(X) := \{\mathfrak{p} \in B_{i,\mathfrak{a}} : \mathfrak{N}(\mathfrak{p}) \le X\}$. We claim that, for any $i \ge 1$ and for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$, if

$$\mathfrak{p} \in [\mathfrak{a}^{i+2}], \quad \text{then } \mathfrak{p} \in B_{i+2,\mathfrak{a}}. \tag{4}$$

We prove this claim by induction on i. Set

$$\begin{aligned} &A := B_{1,\mathfrak{a}}(x_n^2) \setminus B_{0,\mathfrak{a}}, \qquad P := \{\mathfrak{p} : \mathfrak{p} \in [\mathfrak{a}^2]\} \setminus B_{2,\mathfrak{a}} \quad \text{and} \\ &P(x_n) := \{\mathfrak{p} : \mathfrak{p} \in [\mathfrak{a}^2], \mathfrak{N}(\mathfrak{p}) \le x_n\} \setminus B_{2,\mathfrak{a}}(x_n). \end{aligned} \tag{5}$$

By the given hypothesis, we have

$$|B_{1,\mathfrak{a}}(x_n^2)| \gg \frac{x_n^2}{\log^2(x_n^2)}.$$

Let $\omega(\mathfrak{p}, \mathfrak{a}, A)$ be as in (3). Then, applying Lemma 11, we get

$$\sum_{p\in P(x_n)} \frac{\omega(\mathfrak{p}, \mathfrak{a}, A)}{\mathfrak{N}(\mathfrak{p})} \ll \frac{x_n^2}{|A|} \ll \frac{x_n^2}{x_n^2/\log^2(x_n^2)} \ll \log^2 x_n.$$

If $\mathfrak{p} \in P$, then there exists $x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}$ such that

$$\mathfrak{a}^{-1}\mathfrak{p}(x - q) \notin B_{1,\mathfrak{a}}$$

for all $q \in \mathfrak{a}$. This implies that $Z_A(x, \mathfrak{p}, \mathfrak{a}) = 0$ for $Z_A(x, \mathfrak{p}, \mathfrak{a})$ is as defined in (2). Therefore, for any unit u of $\mathcal{O}_{\mathbf{K}}$, we have

$$\mathfrak{a}^{-1}\mathfrak{p}(ux - q') \notin B_{1,\mathfrak{a}}$$

for all $q' \in \mathfrak{a}$. This implies that, for any unit $u \in \mathcal{O}_{\mathbf{K}}^{\times}$, one has $Z_A(ux, \mathfrak{p}, \mathfrak{a}) = 0$. Now suppose that $u_1, u_2 \in \mathcal{O}_{\mathbf{K}}^{\times}$. We now show that if u_1 and u_2 are distinct modulo

$\mathfrak{p}$, then xu_1 and xu_2 are distinct elements in $\mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a}$. Let h be the order of $\mathrm{Cl}_{\mathbf{K}}$. Then $\mathfrak{p}\mathfrak{a}^{h-2}$ is a principal ideal as $\mathfrak{p} \in P \subset [\mathfrak{a}^2]$. Let $x_{\mathfrak{p}}$ be a generator of $\mathfrak{p}\mathfrak{a}^{h-2}$. Consider the map

$$\begin{aligned}\psi_1 : \mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a} &\to \mathfrak{a}^{h-1}/\mathfrak{a}^{h-1}\mathfrak{p}\\ \alpha \bmod \mathfrak{a} &\mapsto \alpha x_{\mathfrak{p}} \bmod \mathfrak{a}^{h-1}\mathfrak{p},\end{aligned}$$

which is well defined as $x_{\mathfrak{p}}\mathfrak{a} = \mathfrak{p}\mathfrak{a}^{h-2} \cdot \mathfrak{a} = \mathfrak{a}^{h-1}\mathfrak{p}$. Also consider the map

$$\begin{aligned}\psi_2 : \mathfrak{a}^{h-1}/\mathfrak{a}^{h-1}\mathfrak{p} &\to \mathcal{O}_{\mathbf{K}}/\mathfrak{p}\\ \beta \bmod \mathfrak{a}^{h-1}\mathfrak{p} &\mapsto \beta \bmod \mathfrak{p},\end{aligned}$$

which is well defined as $\mathfrak{a}$ is an integral ideal and hence $\mathfrak{a}^{h-1}\mathfrak{p} \subset \mathfrak{p}$. We know by Lemma 10 that ψ_1 is an isomorphism. Also it is easy to check that ψ_2 is an injective group homomorphism as $\mathfrak{a}$ is a prime ideal which is co-prime to $\mathfrak{p}$. Since $x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}$, we see that $x_{\mathfrak{p}}x \bmod \mathfrak{p}$ is a nonzero element in $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$, that is, $x_{\mathfrak{p}}x \notin \mathfrak{p}$. This implies that $x_{\mathfrak{p}}x(u_1 - u_2) \in \mathfrak{p}$ if and only if $u_1 - u_2 \in \mathfrak{p}$, as required. Let

$$f(\mathfrak{p}) := |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\}|.$$

Thus if $\mathfrak{p} \in P$, then $\omega(\mathfrak{p}, \mathfrak{a}, A) \geq f(\mathfrak{p})$. Therefore

$$\begin{aligned}\log^2 x_n \gg \sum_{\mathfrak{p}\in P(x_n)} \frac{\omega(\mathfrak{p},\mathfrak{a},A)}{\mathfrak{N}(\mathcal{P})} \geq \sum_{\mathfrak{p}\in P(x_n)} \frac{f(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})} \geq \sum_{\substack{p\in P(x_n)\\ f(\mathfrak{p})\geq \mathfrak{N}(\mathfrak{p})^{1/2-\epsilon}}} \frac{1}{\mathfrak{N}(\mathfrak{p})^{1/2+\epsilon}}\\ > \frac{|\{\mathfrak{p} \in P(x_n) : f(\mathfrak{p}) > \mathfrak{N}(\mathfrak{p})^{1/2-\epsilon}\}|}{x_n^{1/2+\epsilon}}.\end{aligned}$$

Multiplying both sides by $x_n^{1/2+\epsilon}$, we get that

$$|\{\mathfrak{p} \in P(x_n) : f(\mathfrak{p}) > \mathfrak{N}(\mathfrak{p})^{1/2-\epsilon}\}| = o\left(\frac{x_n}{\log x_n}\right).$$

On the other hand, by the Gupta–Murty lemma [6] (see also [10]), we have

$$|\{\mathfrak{p} \in P(x_n) : f(\mathfrak{p}) \leq \mathfrak{N}(\mathfrak{p})^{1/2-\epsilon}\}| \ll x_n^{1-2\epsilon}.$$

Hence

$$|P(x_n)| = o\left(\frac{x_n}{\log x_n}\right). \tag{6}$$

Now, for any $\mathfrak{p} \in [\mathfrak{a}^3]$ and any $x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}$, we have $(x) = \mathfrak{p}^{-1}\mathfrak{a}\mathfrak{a}_1$ for some integral ideal $\mathfrak{a}_1$. Note that $\mathfrak{a}_1 \not\subset \mathfrak{p}$ as $x \notin \mathfrak{a}$ and hence

$$(x) + \mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}(\mathfrak{p} + \mathfrak{a}_1) = \mathfrak{p}^{-1}\mathfrak{a}.$$

Then, by Theorem 9, the set $\overline{P}$ of prime ideals $\mathfrak{q}$ in $\mathcal{O}_{\mathbf{K}}$ such that

$$\mathfrak{q} = (x - y)\mathfrak{p}\mathfrak{a}^{-1}$$

for some $y \in \mathfrak{a}$ has positive density. Note that $\overline{P} \subset [\mathfrak{a}^2]$ and it has positive density. Since by (6) P has zero density, it follows that $\overline{P}$ cannot be contained in P. Therefore there exists $y_0 \in \mathfrak{a}$ such that

$$\mathfrak{q}_0 = (x - y_0)\mathfrak{p}\mathfrak{a}^{-1} \in B_{2,\mathfrak{a}}.$$

This implies that $\mathfrak{p} \in B_{3,\mathfrak{a}}$ and hence by definition all prime ideals $\mathfrak{p}$ for which $[\mathfrak{p}] = [\mathfrak{a}^3]$ are in $B_{3,\mathfrak{a}}$. This proves claim (4) for $i = 1$. Suppose that the claim is true for $i = m$. This implies that if $\mathfrak{p} \in [\mathfrak{a}^{m+2}]$, then $\mathfrak{p} \in B_{m+2,\mathfrak{a}}$. Now let $\mathfrak{p} \in [\mathfrak{a}^{m+3}]$. Then arguing exactly as before we see that, for any $x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}$, we have $(x) + \mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$. Now, by Theorem 9, there exists a prime ideal $\mathfrak{q}$ such that

$$\mathfrak{q} = (x - y)\mathfrak{p}\mathfrak{a}^{-1}$$

for some $y \in \mathfrak{a}$. Since $\mathfrak{p} \in [\mathfrak{a}^{m+3}]$, we have $\mathfrak{q} \in [\mathfrak{a}^{m+2}]$. Then, by induction hypothesis, we have $\mathfrak{q} \in B_{m+2,\mathfrak{a}}$ and hence by definition $\mathfrak{p} \in B_{m+3,\mathfrak{a}}$, as required. This implies that every prime ideal of $\mathcal{O}_{\mathbf{K}}$ is in $B_{h+2,\mathfrak{a}}$ and hence in $B_{\mathfrak{a}}$. Thus $\mathfrak{a}$ is a Euclidean ideal. □

4. Proof of Theorem 2 and Theorem 3

In this section, we give a proof for Theorem 2 and then outline a proof for Theorem 3 as the arguments are similar.

4.1. Proof of Theorem 2

We start by proving some lemmas which are required to prove Theorem 2. Throughout this subsection, let $\mathbf{K}_1$, $\mathbf{K}_2$ be abelian cubic fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, both of which are abelian over $\mathbb{Q}$. Also let f_1 and f_2 be their conductors. Set f to be the least common multiple of 16, f_1, f_2 and $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where ζ_f is a primitive fth root of unity.

LEMMA 15. *Suppose that the Galois group G of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$ satisfies the hypothesis of Theorem 2. Then there exists a co-prime residue class modulo f, say $t \bmod f$, such that any rational prime that belongs to this residue class splits completely in $\mathbf{K}_1\mathbf{K}_2$ but does not split completely in $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$. Further, there exist $a, b \in (1/4, 1/2)$ such that, for any $X, \epsilon > 0$, we have*

$$\left| J_\epsilon(X) := \left\{ p \equiv t \bmod f : p \text{ rational prime}, \right.\right.$$
$$\left. p \in (X^{1-\epsilon}, X) \text{ such that } \frac{p-1}{2} \text{ is either a rational prime or} \right.$$
$$\left.\left. \text{a product of rational primes } q_1 q_2 \text{ with } X^a < q_1 < X^b \right\} \right| \gg \frac{X}{\log^2 X}.$$

Proof. By the given hypothesis, we have

$$G \not\subset \bigcup_{\ell} G_\ell \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \cup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)).$$

This implies that there exists a co-prime residue class modulo f, say $t \bmod f$ such that $((t-1)/2, f) = 1$, such that every rational prime in this class splits completely in $\mathbf{K}_1\mathbf{K}_2$ but not in $\mathbf{H}(K_1)$ and $\mathbf{H}(\mathbf{K}_2)$.

We can now apply Lemma 5 for $u = t$ and $v = f$, which gives us that, for some $a, b \in (1/4, 1/2)$ and any $\epsilon > 0$,

$$|J_\epsilon(X)| \gg \frac{X}{\log^2 X}.$$

This completes the proof of the lemma. □

Next set $\mathbf{K} = \mathbf{K}_1\mathbf{K}_2$ and let $t \bmod f$ be as in Lemma 15. Since $(t, f) = 1$ and $((t-1)/2, f) = 1$, we note that $t \equiv 3 \bmod 4$. For a and b as in the previous lemma, choose ϵ such that $a < b/(1-\epsilon) < 1/2$. Consider the set

$$M_\epsilon := \Bigg\{ \mathfrak{p} : \mathfrak{p} \text{ is a prime ideal, } \mathfrak{N}\mathfrak{p} = p \text{ rational prime, } p \equiv t \bmod f, \\ \frac{p-1}{2} \text{ is either a rational prime or} \\ \text{a product of rational primes } q_1 q_2 \text{ with } p^a < q_1 < p^{b/(1-\epsilon)} \Bigg\};$$

and also the set $M_\epsilon(X) := \{\mathfrak{p} \in M_\epsilon : \mathfrak{N}(\mathfrak{p}) \le X\}$ for any real number $X > 0$. In this set-up, we have the following lemma.

LEMMA 16. *Let $\mathbf{K}$ be as above and e_1, e_2, e_3 be multiplicatively independent elements in $\mathbf{K}^\times$. Then, for some $i \in \{1, 2, 3\}$, either e_i or $-e_i$ is a primitive root mod $\mathfrak{p}$ for infinitely many ideals in the set M_ϵ. Let this set of prime ideals be called P, and let $P(X)$ denote the set of elements in P of norm less than or equal to X. Then there exists an increasing unbounded sequence $\{x_n\}_{n\in\mathbb{N}}$ such that*

$$|P(x_n)| \gg \frac{x_n}{\log^2 x_n}.$$

Proof. For any real number $X > 0$, let $J_\epsilon(X)$ be as in Lemma 15. Since for every rational prime $p \in J_\epsilon$ there exists a prime ideal $\mathfrak{p} \in M_\epsilon$ such that $\mathfrak{N}(\mathfrak{p}) = p$ and by Lemma 15, we know that

$$|J_\epsilon(X)| \gg \frac{X}{\log^2 X},$$

it follows that

$$|M_\epsilon(X)| \gg \frac{X}{\log^2 X}. \tag{7}$$

For any multiplicatively independent elements e_1, e_2, and e_3 in $\mathcal{O}_K$, we can partition the set $M_\epsilon = \bigcup_{j=1}^{8} M_j$, where each M_j corresponds to a tuple (c_1, c_2, c_3) with entries in $\{\pm 1\}$ such that

$$\left(\frac{e_i}{\mathfrak{p}}\right) = -c_i$$

for all $\mathfrak{p} \in M_j$. See page 394 of [15] for the definition of second power residue symbol $(e_i/\mathfrak{p})$. We now claim that there exist an increasing unbounded sequence $\{x_n\}_{n\in\mathbb{N}}$ and $1 \le j_0 \le 8$ such that

$$|M_{j_0}(x_n)| \gg \frac{x_n}{\log^2 x_n}.$$

Suppose that our claim is not true, in other words, none of the M_j have such a sequence. Then

$$\limsup_{X\to\infty} |M_j(X)| \Big/ \left(\frac{X}{\log^2 X}\right) = 0.$$

However, since

$$\liminf_{X\to\infty} |M_j(X)| \Big/ \left(\frac{X}{\log^2 X}\right) = 0,$$

we have

$$|M_j(X)| = o\left(\frac{X}{\log^2 X}\right)$$

for all $1 \le j \le 8$. This implies that

$$|M_\epsilon(X)| = o\left(\frac{X}{\log^2 X}\right),$$

a contradiction to (7). Since $t \equiv 3 \bmod 4$, any $\mathfrak{p} \in M_\epsilon$ has the property that $(\frac{-1}{\mathfrak{p}}) = -1$. Now, by applying Lemma 6 with $T = M_{j_0}$ and noting that, for any $i \in \{1, 2, 3\}$, the elements $c_i e_i$ are quadratic non-residues modulo any prime ideal $\mathfrak{p} \in M_{j_0}$, we get our lemma. □

REMARK 4.1. Note that ± 1 cannot be a subset of a multiplicatively independent set. Also both $e_i \bmod \mathfrak{p}$ and $-e_i \bmod \mathfrak{p}$ for any $\mathfrak{p} \in M_\epsilon$ cannot simultaneously be quadratic residues as $(\frac{-1}{\mathfrak{p}}) = -1$. Therefore the usual exclusion of ± 1 and perfect squares for Artin's primitive root conjecture does not appear in Lemma 16.

We now complete the proof of Theorem 2. Since $\mathbf{K}_1, \mathbf{K}_2$ are real cubic, their compositum $\mathbf{K}$ contains three multiplicatively independent units, say ϵ_1, ϵ_2, and ϵ_3. Let P be as in Lemma 16 and η be one of the elements $\pm\epsilon_1, \pm\epsilon_2, \pm\epsilon_3$ that generates $(\mathcal{O}_\mathbf{K}/\mathfrak{p})^\times$ for all $\mathfrak{p} \in P$. Then $\eta \in \mathbf{K}_s$, where $s \in \{1, 2\}$, and by Lemma 16 we have a sequence $\{x_n\}_{n\in\mathbb{N}}$ such that

$$|P(x_n)| \ge \frac{cx_n}{\log^2 x_n}.$$

Since every $\mathfrak{p} \in P$ has degree one, η generates $(\mathcal{O}_{\mathbf{K}_s}/\mathfrak{r})^\times$ where $\mathfrak{r} = \mathfrak{p} \cap K_s$. Since there are only finitely many ideal classes, arguing as in Lemma 16, there exists some ideal class $[\mathfrak{f}]$ in the class group of $\mathbf{K}_s$ so that

$$|\{\mathfrak{q} \cap \mathbf{K}_s \in [\mathfrak{f}] : \mathfrak{q} \in P, \mathfrak{N}(\mathfrak{q} \cap \mathbf{K}_s) \leq y_n\}| \gg \frac{y_n}{h_{K_s} \log^2 y_n}$$

for a subsequence $\{y_n\}_{n\in\mathbb{N}}$ of $\{x_n\}_{n\in\mathbb{N}}$. Here $h_{\mathbf{K}_s}$ is used to denote the class number of $\mathbf{K}_s$. Since $P \subset M_\epsilon$, our choice of t (see Lemma 15) ensures that none of the elements of P lie above any ideal in the trivial class of $\mathbf{K}_s$. Since $h_{\mathbf{K}_s}$ is prime, the ideal class $[\mathfrak{f}]$ must generate the ideal class group. Therefore, by Theorem 14, we see that $[\mathfrak{f}]$ is a Euclidean ideal class. This completes the proof of Theorem 2.

4.2. Proof of Theorem 3

In this subsection, we outline the proof of Theorem 3. Throughout this subsection, let $\mathbf{K}_1$, $\mathbf{K}_2$, and $\mathbf{K}_3$ be real quadratic fields with abelian Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, and $\mathbf{H}(\mathbf{K}_3)$ respectively. Also let f_1, f_2, and f_3 be their conductors. Set f to be the least common multiple of 16, f_1, f_2, f_3, and $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where ζ_f is a primitive fth root of unity. Also set $\mathbf{K} = \mathbf{K}_1\mathbf{K}_2\mathbf{K}_3$. For the sake of completeness, we now state two lemmas required to prove Theorem 3. Their proofs follow by arguing exactly as in Lemma 15 and Lemma 16.

LEMMA 17. *Suppose that the Galois group G of $\mathbf{F}$ over $\mathbf{K}$ satisfies the hypothesis of Theorem 3. Then there exists a co-prime residue class modulo f, say $t \bmod f$, such that any rational prime that belongs to this residue class splits completely in $\mathbf{K}$ but does not split completely in $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, and $\mathbf{H}(\mathbf{K}_3)$. Further, there exist $a, b \in (1/4, 1/2)$ such that, for any $X, \epsilon > 0$, we have*

$$\Bigg| J_\epsilon(X) := \Bigg\{ p \equiv t \bmod f : p \text{ rational prime}, p \in (X^{1-\epsilon}, X) \text{ such that } \frac{p-1}{2} \text{ is either a rational prime or a product of rational primes } q_1q_2 \text{ with } X^a < q_1 < X^b \Bigg\} \Bigg| \gg \frac{X}{\log^2 X}.$$

For a and b as in Lemma 17, choose $\epsilon > 0$ such that $a < b/(1-\epsilon) < 1/2$. Consider the sets

$$M_\epsilon := \Bigg\{ \mathfrak{p} : \mathfrak{p} \text{ is a prime ideal}, \mathfrak{N}\mathfrak{p} = p \text{ rational prime}, p \equiv t \bmod f, \frac{p-1}{2} \text{ is either a rational prime or a product of rational primes } q_1q_2 \text{ with } p^a < q_1 < p^{b/(1-\epsilon)} \Bigg\};$$

and $M_\epsilon(X) := \{\mathfrak{p} \in M_\epsilon : \mathfrak{N}(\mathfrak{p}) \leq X\}$ for any real number $X > 0$. In this set-up, we have the following lemma.

LEMMA 18. *Let e_1, e_2, e_3 be multiplicatively independent elements in $\mathbf{K}^\times$. Then, for some $i \in \{1,2,3\}$, either e_i or $-e_i$ is a primitive root mod $\mathfrak{p}$ for infinitely many ideals in the set M_ϵ. Let this set of prime ideals be called P, and let $P(X)$ denote the set of elements in P of norm less than or equal to X. Then there exists an increasing unbounded sequence $\{x_n\}_{n\in\mathbb{N}}$ such that*

$$|P(x_n)| \gg \frac{x_n}{\log^2 x_n}.$$

This completes the proof of Theorem 3.

5. Consequences of Elliott and Halberstam Conjecture

We first note the following improvement of Lemma 6.

LEMMA 19. *Let a_1 and a_2 be multiplicatively independent elements of $\mathbf{K}^\times$, T be a set of prime ideals of degree one in $\mathbf{K}$, and $\mathfrak{N}(\mathfrak{p})$ denote the absolute norm of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathbf{K}$. Suppose that T has the following properties*:

(1) *There exist a constant $c > 0$ and an unbounded increasing sequence $\{x_n\}_{n\in\mathbb{N}}$ such that*
$$|T(x_n) := \{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \le x_n\}| \gg \frac{x_n}{\log^2 x_n};$$
(2) *There exists $\alpha < \beta$ in the open interval $(1/3, 1/2)$ such that if $\mathfrak{p}$ is an element of T and $p = \mathfrak{N}(\mathfrak{p})$, then $(p-1)/2$ is either a prime q or a product of primes q_1q_2, with $p^\alpha < q_1 < p^\beta$;*
(3) *The numbers a_1 and a_2 are both quadratic non-residues with respect to every prime in T.*

Then, for any $c > \epsilon > 0$, there exists a subsequence $\{y_m\}_{m\in\mathbb{N}}$ of $\{x_n\}_{n\in\mathbb{N}}$ such that one of the a_is is a primitive root for at least $(c-\epsilon)y_m/\log^2 y_m$ elements of $T(y_m)$.

Proof. If the order of a_1 or a_2 is two in $\mathcal{O}_\mathbf{K}/\mathfrak{p}$, then $a_i^2 - 1 \in \mathfrak{p}$ and hence there are only finitely many such prime ideals $\mathfrak{p}$ in $\mathcal{O}_\mathbf{K}$. Without loss of generality, we can assume that neither a_1 nor a_2 has order two in $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ with $\mathfrak{N}(\mathfrak{p})$ sufficiently large.

From now onwards assume that $\mathfrak{p} \in T$ with $\mathfrak{N}(\mathfrak{p}) = p$ such that neither a_1 nor a_2 has order two in $\mathcal{O}_\mathbf{K}/\mathfrak{p}$. Also we shall denote the order of any element a in $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ by $o_\mathfrak{p}(a)$. By the given hypothesis, $p = 1 + 2q$ for a prime q or $p = 1 + 2q_1q_2$, with q_1, q_2 primes such that $p^\alpha < q_1 < p^\beta$. If both a_1 and a_2 are not primitive roots modulo $\mathfrak{p}$, then they have order q when $p - 1 = 2q$ or they have order $q_1, q_2, 2q_1, 2q_2, q_1q_2$ when $p - 1 = 2q_1q_2$. Again by the given hypothesis, a_1, a_2 are quadratic non-residues modulo $\mathfrak{p}$ and hence $o_\mathfrak{p}(a_1)$, $o_\mathfrak{p}(a_2)$ must be divisible by 2. This implies that there are no primes p with $p - 1 = 2q$ for which both a_1 and a_2 are not primitive roots modulo $\mathfrak{p}$. When $p - 1 = 2q_1q_2$ and both a_1 and a_2 are not primitive roots modulo $\mathfrak{p}$, then $o_\mathfrak{p}(a_1)$ is equal to $2q_1$ or $2q_2$ and same is true for $o_\mathfrak{p}(a_2)$. Now suppose that at least one of $o_\mathfrak{p}(a_1), o_\mathfrak{p}(a_2)$ is equal

to $2q_1$. Then, for any $i = 1, 2$, we have

$$\begin{aligned}&|\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \le X, o_{\mathfrak{p}}(a_i) := e \le 2X^{\beta}\}| \\ &\le \sum_{e \le 2X^{\beta}} |\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \le X, \mathfrak{p} | (a_i^e - 1)\}|,\end{aligned}$$

where β is as in the hypothesis. Taking norms, we get

$$\begin{aligned}\sum_{e \le 2X^{\beta}} |\{p \le X : p | \mathfrak{N}(a_i^e - 1)\}| &\ll \sum_{e \le 2X^{\beta}} \log |\mathfrak{N}(a_i^e - 1)| \\ &= \sum_{e \le 2X^{\beta}} \log\left(\prod_{\sigma} |\sigma(a_i^e) - 1|\right) \\ &\ll \sum_{e \le 2X^{\beta}} \log\left(\prod_{\sigma} (|\sigma(a_i)| + 1)^e\right) \\ &\ll \sum_{e \le 2X^{\beta}} e \ll X^{2\beta} = o\left(\frac{X}{\log^2 X}\right).\end{aligned}$$

If both $o_{\mathfrak{p}}(a_1), o_{\mathfrak{p}}(a_2)$ are equal to $2q_2$, we claim that

$$|\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \le X, o_{\mathfrak{p}}(a_1) = 2q_2 = o_{\mathfrak{p}}(a_2)\}| = o\left(\frac{X}{\log^2 X}\right).$$

To prove this, we show that there exists a set S of tuples $(r, s) \in \mathbb{N} \times \mathbb{N}$ such that

$$\begin{aligned}&\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \le X, o_{\mathfrak{p}}(a_1) = 2q_2 = o_{\mathfrak{p}}(a_2)\} \\ &\quad \subset \{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) := p \le X, p | \mathfrak{N}(a_1^r a_2^s - 1) \text{ for some } (r, s) \in S\}. \qquad (8)\end{aligned}$$

Consider the set

$$\tilde{S} := \{(r, s) \in \mathbb{N} \times \mathbb{N} : 0 \le r, s \le 2X^{(1-\alpha)/2}\}.$$

Note that when $o_{\mathfrak{p}}(a_1) = 2q_2 = o_{\mathfrak{p}}(a_2)$ for some $\mathfrak{p} \in T$, then $(a_1^r a_2^s)^{2q_2} \equiv 1 \bmod \mathfrak{p}$ for any $(r, s) \in \tilde{S}$. Since $|\tilde{S}|$ is $4X^{1-\alpha} \ge 4p^{1-\alpha} \ge 4q_2$ and the fact that the polynomial $Y^{2q_2} - 1$ over $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ can have at most $2q_2$ roots, we have by the pigeonhole principle that there exists $(r, s) \in S$, where $S := \{(r, s) \in \mathbb{Z} \times \mathbb{Z} : (|r|, |s|) \in \tilde{S}\}$ such that $a_1^r a_2^s - 1 \in \mathfrak{p}$. Let the numerator of $a_1^r a_2^s - 1$ be $M_{r,s}$. Clearly $M_{r,s} \ne 0$ as a_1 and a_2 are multiplicatively independent. Then the number of prime divisors of the numerator $\mathfrak{N}(M_{r,s})$ is $\log |\mathfrak{N}(M_{r,s})| \ll X^{(1-\alpha)/2}$. Hence

$$|\{p \le X : p | \mathfrak{N}(M_{r,s}) \text{ for some } (r, s) \in S\}| \ll X^{1-\alpha} \times X^{(1-\alpha)/2} = o\left(\frac{X}{\log^2 X}\right)$$

as $\alpha > 1/3$. Thus

$$|\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) := p \le X, p | \mathfrak{N}(a_1^r a_2^s - 1) \text{ for some } (r, s) \in S\}| = o\left(\frac{X}{\log^2 X}\right).$$

Therefore there exists a subsequence $\{y_m\}_{m \in \mathbb{N}}$ such that one of the a_is is a primitive root for at least $(c - \epsilon) y_m / \log^2 y_m$ primes for any $\epsilon > 0$. □

We now complete the proof of Theorem 4.

Proof. Let $\mathbf{K} := \mathbf{K}_1\mathbf{K}_2$ be the compositum of the real quadratic fields $\mathbf{K}_1$ and $\mathbf{K}_2$ and $f := [16, f_1, f_2]$, where f_1 and f_2 denote the conductors of $\mathbf{K}_1$ and $\mathbf{K}_2$ respectively. By the given hypothesis, there exists an element $b \bmod f$ in the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ such that $((b-1)/2, f/2) = 1$. Since $16|f$, we have $b \equiv 3 \bmod 4$. We can now apply Theorem 13 to see that the set

$$\tilde{T}(X) := \left\{ \ell \le X : \ell \text{ rational prime}, \ell \equiv b \bmod f, \frac{\ell-1}{2} \text{ is either a rational prime} \right.$$
$$\left. \text{or a product of rational primes } q_1q_2 \text{ with } X^{1/2-\delta} < q_1 < X^{1/2} \right\}$$

has cardinality $\gg X/\log^2 X$ for any $\delta < 1/6$. If we set

$$T(X) := \{\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}} : \mathfrak{p} \text{ is a prime ideal of degree one}, \mathfrak{N}(\mathfrak{p}) \in \tilde{T}(X)\},$$

then we have

$$|T(X)| \gg \frac{X}{\log^2 X}.$$

Let $a_1 \in \mathbf{K}_1$ and $a_2 \in \mathbf{K}_2$ be two fundamental units. By arguing as in Theorem 16, it follows that there exist an increasing unbounded sequence $\{x_n\}_{n\in\mathbb{N}}$ and a choice of tuple (c_1, c_2) with entries in $\{\pm 1\}$ such that

$$\left(\frac{a_i}{\mathfrak{p}}\right) = -c_i$$

for at least $\gg x_n/\log^2 x_n$ primes in $T(x_n)$. Let the set of these primes be called $A_1(x_n)$. Since $b \equiv 3 \bmod 4$, each c_ia_i is a quadratic non-residue modulo all primes in $A_1(x_n)$, $n \ge 1$. Now, by applying Lemma 19, there exists $a \in \{\pm a_1, \pm a_2\}$ in K_s for $s \in \{1, 2\}$, which is a primitive root for every element of a subset $P_1(x_n)$ of $A_1(x_n)$. Further there exists an unbounded increasing sequence $\{y_m\}_{m\in\mathbb{N}}$ such that

$$|P_1(y_m)| \gg \frac{y_m}{\log^2 y_m}.$$

Since $\mathfrak{p} \in P_1(y_m)$ is of degree one, a generates $(\mathcal{O}_{\mathbf{K}_s}/\mathfrak{q})^\times$, where $\mathfrak{q} = \mathfrak{p} \cap \mathbf{K}_s$. Since there are only finitely many ideal classes in $\mathbf{K}_s$, by arguing as in Theorem 16, there exist an ideal class $[\mathfrak{f}]$ and a subsequence $\{z_r\}_{r\in\mathbb{N}}$ of $\{y_m\}_{m\in\mathbb{N}}$ such that

$$|\{\mathfrak{q} \cap \mathbf{K}_s \in [\mathfrak{f}] : \mathfrak{q} \in P_1(z_r)\}| \gg \frac{z_r}{\log^2 z_r}.$$

By the given hypothesis, none of the primes in $P_1(z_r)$ split completely in $\mathbf{H}(\mathbf{K}_s)$. Thus $[\mathfrak{f}]$ must generate the ideal class group $\mathbf{K}_s$. Therefore, by Theorem 14, we see that $[\mathfrak{f}]$ is a Euclidean ideal class. □

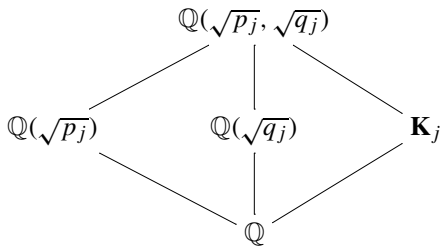
6. Concluding Remarks

In this section, we construct some explicit examples for which the hypotheses of our main theorems hold. We start with real quadratic fields.

COROLLARY 20. *Let $p_1, q_1, p_2, q_2, p_3, q_3$ be six distinct primes that are congruent to* 1 mod 4. *For $j \in \{1,2,3\}$, if each $\mathbf{K}_j := \mathbb{Q}(\sqrt{p_j q_j})$ has class number* 2, *then at least one of them has a Euclidean ideal class.*

Proof. Since p_j and q_j are all congruent to 1 mod 4, we note that the conductor of $\mathbf{K}_j$ is $p_j q_j$ for all $j \in \{1,2,3\}$. To see this, we first observe that if $\mathbb{Q}(\zeta_r)$ is the conductor, then r must be a multiple of p_j and q_j since both of these numbers ramify in $\mathbf{K}_j$. However, $\mathbb{Q}(\zeta_{p_j q_j})$ contains $\mathbb{Q}(\zeta_{p_j})$ and $\mathbb{Q}(\zeta_{q_j})$. Since both p_j and q_j are congruent to 1 mod 4, we have $\mathbb{Q}(\sqrt{p_j})$ and $\mathbb{Q}(\sqrt{q_j})$ are contained in $\mathbb{Q}(\zeta_{p_j})$ and $\mathbb{Q}(\zeta_{q_j})$ respectively. Therefore $\mathbb{Q}(\zeta_{p_j q_j})$ is the smallest cyclotomic field containing $\mathbf{K}_j$.

The next observation we would like to make is that $\mathbf{H}(\mathbf{K}_j) = \mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$. Since the class number of the quadratic field $\mathbf{K}_j$ is two, degree of the extension $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ over $\mathbb{Q}$ is four, and both these fields are totally real, it suffices to show that $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is an unramified extension of $\mathbf{K}_j$. Consider the following diagram:



The prime p_j does not ramify in $\mathbb{Q}(\sqrt{q_j})$ and hence its ramification index in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is 2. Similarly the ramification index of q_j in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is also 2. Note that the discriminant of $\mathbf{K}_j$ is equal to $p_j q_j$ (as p_j, q_j are 1 mod 4) and hence both p_j and q_j ramify in $\mathbf{K}_j$. Since both p_j and q_j have ramification index 2 in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$, the primes in $\mathbf{K}_j$ lying above p_j, q_j do not ramify in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$. Thus $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is unramified over $\mathbf{K}_j$ as the discriminant of $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is $p_j^2 q_j^2$.

Note that $f = 16 p_1 p_2 p_3 q_1 q_2 q_3$ and $\mathbf{K} := \mathbb{Q}(\sqrt{p_1 q_1}, \sqrt{p_2 q_2}, \sqrt{p_3 q_3})$ is the compositum of $\mathbf{K}_j$ for $j \in \{1,2,3\}$. We claim that there exists an element σ in the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ such that

$$\sigma(\iota) = -\iota, \qquad \sigma\left(\sqrt{p_j}\right) = -\sqrt{p_j} \quad \text{and} \quad \sigma\left(\sqrt{q_j}\right) = -\sqrt{q_j}$$

for $j = 1,2,3$. Here $\iota \in \mathbf{C}$ is such that $\iota^2 = -1$. To see this, we first observe that since the discriminant of $\mathbb{Q}(\iota, \sqrt{p_2}, \ldots, \sqrt{q_3})$ is co-prime to p_1, $\sqrt{p_1}$ is not contained in $\mathbb{Q}(\iota, \sqrt{p_2}, \ldots, \sqrt{q_3})$. So there exists a Galois element in $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ that takes $\sqrt{p_1}$ to $-\sqrt{p_1}$ while fixing the other six elements. The same argument can be applied to the other six elements. The composition of all these Galois isomorphisms will give us the required isomorphism σ. This isomorphism in fact belongs to the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$. Since σ does not fix the unique quadratic subfield of $\mathbb{Q}(\zeta_\ell)$ for any odd prime $\ell | f$ or $\ell = 4$, it follows that σ does not belong to the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}(\zeta_\ell)$ for all odd primes $\ell | f$

or $\ell = 4$. Also σ does not belong to the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{H}(K_j)$ for $j \in \{1, 2, 3\}$. This is because it does not fix the quadratic subfields $\mathbb{Q}(\sqrt{p_j})$ or $\mathbb{Q}(\sqrt{q_j})$ of $\mathbf{H}(K_j)$ for all $j \in \{1, 2, 3\}$. Therefore we can now apply Theorem 3 to this set of three real quadratic fields to conclude that at least one of them must have a Euclidean ideal class. □

Arguing exactly as in Theorem 3 and using Theorem 4, we get the following corollary.

COROLLARY 21. *Let p_1, q_1, p_2, q_2 be distinct primes that are congruent to* 1 mod 4. *If $\mathbb{Q}(\sqrt{p_j q_j})$ for $j \in \{1, 2\}$ have class number* 2, *then at least one of them must contain a Euclidean ideal class provided the Elliott and Halberstam conjecture is true.*

To provide an example for the real Galois cubic fields, we consider the following construction. Let p_1, q_1, p_2, q_2 be four distinct primes that are congruent to 1 mod 12. Let $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3, \mathbf{K}_4$ denote the unique degree three subfields of $\mathbb{Q}(\zeta_{p_1})$, $\mathbb{Q}(\zeta_{q_1})$, $\mathbb{Q}(\zeta_{p_2})$, and $\mathbb{Q}(\zeta_{q_2})$. Consider a degree three subfield of $\mathbf{K}_1\mathbf{K}_2$ that is distinct from $\mathbf{K}_1$ and $\mathbf{K}_2$. This is possible since the Galois group of $\mathbf{K}_1\mathbf{K}_2$ over $\mathbb{Q}$ is $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and this group contains more than two subgroups of order three. Let us denote this field by $\mathbf{K}$. Similarly, we consider a degree three subfield of $\mathbf{K}_3\mathbf{K}_4$, distinct from $\mathbf{K}_3$, $\mathbf{K}_4$, and denote it by $\tilde{\mathbf{K}}$.

COROLLARY 22. *If $\mathbf{K}$ and $\tilde{\mathbf{K}}$ have class number* 3, *then one of $\mathbf{K}$ or $\tilde{\mathbf{K}}$ must have a Euclidean ideal class.*

Proof. We note that $\mathbf{K}$ is not contained in $\mathbb{Q}(\zeta_{p_1})$ or $\mathbb{Q}(\zeta_{q_1})$, but it is contained in $\mathbb{Q}(\zeta_{p_1 q_1})$. Therefore, the conductor of $\mathbf{K}$ must be $p_1 q_1$. Similarly the conductor of $\tilde{\mathbf{K}}$ is $p_2 q_2$. If $\mathbf{K}$ and $\tilde{\mathbf{K}}$ have class number 3, then the Hilbert class field of $\mathbf{H}(\mathbf{K})$ of $\mathbf{K}$ and the Hilbert class field of $\mathbf{H}(\tilde{\mathbf{K}})$ of $\tilde{\mathbf{K}}$ are $\mathbf{K}_1\mathbf{K}_2$ and $\mathbf{K}_3\mathbf{K}_4$ respectively. This follows from an argument similar to that of Corollary 20 and the fact that the conductors of $\mathbf{K}$ and $\tilde{\mathbf{K}}$ are $p_1 q_1$ and $p_2 q_2$, respectively. Now let $\mathbf{K}_1 = \mathbb{Q}(\alpha_1)$ and $\mathbf{K}_3 = \mathbb{Q}(\tilde{\alpha_1})$. We first claim that $\alpha_1 \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. Suppose not, then

$$\mathbf{K}\tilde{\mathbf{K}}(\alpha_1) \subset \mathbf{K}\tilde{\mathbf{K}}\big(\tilde{\alpha_1}, \iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}\big).$$

This implies that

$$\mathbf{K}\tilde{\mathbf{K}}\mathbf{K}_1 \subset \mathbf{K}\tilde{\mathbf{K}}\mathbf{K}_3\big(\iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}\big).$$

Note that $\mathbf{K}\mathbf{K}_1 = \mathbf{K}_1\mathbf{K}_2$ and $\tilde{\mathbf{K}}\mathbf{K}_3 = \mathbf{K}_3\mathbf{K}_4$. So we have

$$\tilde{\mathbf{K}}\mathbf{K}_1\mathbf{K}_2 \subset \mathbf{K}\mathbf{K}_3\mathbf{K}_4\big(\iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}\big).$$

We first note that $\mathbf{K}$, $\mathbf{K}_3$, and $\mathbf{K}_4$ have co-prime conductors. Therefore the degree of the field $\mathbf{K}\mathbf{K}_3\mathbf{K}_4(\iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ is 27×2^n for some positive natural number n. But since the Galois group of this field is abelian, it has a unique

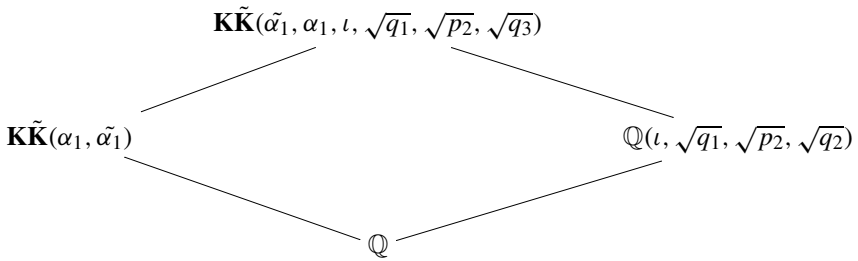
Sylow-2 subgroup. Therefore it has a unique subfield of degree 27. This implies that

$$\mathbf{K}_1\mathbf{K}_2\tilde{\mathbf{K}} = \mathbf{K}\mathbf{K}_3\mathbf{K}_4.$$

But composing with $\mathbf{K}_3$ on both sides, we get

$$\mathbf{K}_1\mathbf{K}_2\mathbf{K}_3\mathbf{K}_4 = \mathbf{K}\mathbf{K}_3\mathbf{K}_4,$$

which is not possible as seen by a degree argument and the fact that all the $\mathbf{K}_i$s have distinct prime conductors. Further $\iota \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ since the field under consideration is totally real. And finally $\sqrt{p_1} \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. To see this, consider the following diagram:



The degree of $\mathbf{K}\tilde{\mathbf{K}}(\alpha_1, \tilde{\alpha_1}) = \mathbf{K}_1\mathbf{K}_2\mathbf{K}_3\mathbf{K}_4$ is a power of three. Note that p_1 does not ramify in $\mathbb{Q}(\iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. Since the degree of $\mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_3})$ over $\mathbb{Q}(\iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ is a power of three, the ramification index of p_1 in $\mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ is a power of three, but the ramification index of p_1 in $\mathbb{Q}(\sqrt{p_1})$ is divisible by two. Therefore $\sqrt{p_1} \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. Similar arguments work for $\sqrt{q_1}$, $\sqrt{p_2}$, and $\sqrt{q_2}$. Arguing as in Corollary 20, we can choose a Galois isomorphism of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}$, where $f = 16p_1q_1p_2q_2$, which fixes $\mathbf{K}\tilde{\mathbf{K}}$ but not any of $\alpha_1, \tilde{\alpha_1}, \iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}$, and $\sqrt{q_2}$. This shows that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbf{K}\tilde{\mathbf{K}}) \not\subset \bigcup G_\ell \cup \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbf{K}_1\mathbf{K}_2) \cup \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbf{K}_3\mathbf{K}_4),$$

where ℓ is either an odd prime dividing f or 4 and G_ℓ is the Galois group of $\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_\ell)$. Now, applying Theorem 2, we have that one of $\mathbf{K}$ or $\tilde{\mathbf{K}}$ has a Euclidean ideal class. □

REMARK 6.1. Let p_1, q_1, p_2, q_2 be distinct primes. Corollary 22 is also true if we assume that some of the primes p_1, q_1, p_2, q_2 are congruent to 1 mod 12 and some of them are congruent to 7 mod 12. It can be seen by replacing p_i or q_i for $i = 1, 2$ by $-p_i$ or $-q_i$ when p_i or q_i are congruent to 7 mod 12 in the proof of Corollary 22.

ACKNOWLEDGMENTS. The authors would like to thank the referee for very careful reading and a number of relevant suggestions, which improved the exposition of the paper.

References

[1] D. A. Clark and M. R. Murty, *The Euclidean algorithm for Galois extensions of* $\mathbb{Q}$, J. Reine Angew. Math. 459 (1995), 151–162.

[2] J.-M. Deshouillers, S. Gun, and J. Sivaraman, *On Euclidean ideal classes in certain Abelian extensions,* Math. Z. (2019), doi:10.1007/s00209-019-02434-2.

[3] P. D. T. A. Elliott and H. Halberstam, *A conjecture in prime number theory,* Symposia mathematica, vol. IV (INDAM, Rome, 1968/69), pp. 59–72, Academic Press, London, 1970.

[4] E. Fouvry and H. Iwaniec, *Primes in arithmetic progressions,* Acta Arith. 42 (1983), no. 2, 197–218.

[5] H. Graves, *Growth results and Euclidean ideals,* J. Number Theory 133 (2013), 2756–2769.

[6] H. Graves and M. R. Murty, *A family of number fields with unit rank at least* 4 *which has Euclidean ideals,* Proc. Amer. Math. Soc. 141 (2013), no. 9, 2979–2990.

[7] R. Gupta, M. R. Murty, and V. K. Murty, *The Euclidean algorithm for S-integers,* Number theory (Montreal, Que., 1985), Conf. Proc., Can. Math. Soc., 7, pp. 189–201, American Mathematical Society, Providence, 1987.

[8] R. Gupta and R. M. Murty, *A remark on Artin's conjecture,* Invent. Math. 78 (1984), no. 1, 127–130.

[9] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean,* Canad. J. Math. 56 (2004), no. 1, 55–70.

[10] M. Harper and M. R. Murty, *Euclidean rings of algebraic integers,* Canad. J. Math. 56 (2004), no. 1, 71–76.

[11] D. R. Heath-Brown, *Artin's conjecture for primitive roots,* Quart. J. Math. Oxford Ser. (2) 37 (1986), no. 145, 27–38.

[12] H. W. Lenstra, *Euclidean ideal classes,* Astérisque 61 (1979), 121–131.

[13] ———, *Lectures on Euclidean rings,* Fakultät für Mathematik, Universität Bielefeld.

[14] W. Narkiewicz, *Units in residue classes,* Arch. Math. 51 (1988), 238–241.

[15] ———, *Elementary and analytic theory of algebraic numbers,* Springer-Verlag, Berlin, 1990.

[16] ———, *Euclidean algorithm in small Abelian fields,* Funct. Approx. Comment. Math. 37 (2007), no. 2, 337–340.

[17] P. J. Weinberger, *On Euclidean rings of algebraic integers,* Proc. Sympos. Pure Math. 24 (1972), 321–332.

S. Gun
Institute of Mathematical Sciences
HBNI, C.I.T Campus
Taramani
Chennai 600 113
India

sanoli@imsc.res.in

J. Sivaraman
Institute of Mathematical Sciences
HBNI, C.I.T Campus
Taramani
Chennai 600 113
India

jyothsnaa@imsc.res.in