(Published in Research in Number Theory 8, no. 3, (2022))

EUCLIDEAN IDEAL CLASSES IN GALOIS NUMBER FIELDS OF ODD PRIME DEGREE

V. KUMAR MURTY AND J. SIVARAMAN

ABSTRACT. Weinberger [16] in 1972, proved that the ring of integers of a number field with unit rank at least 1 is a principal ideal domain if and only if it is a Euclidean domain, provided the generalised Riemann hypothesis holds. Lenstra [13], extended the notion of Euclidean domains in order to capture Dedekind domains with finite cyclic class group and proved an analogous theorem in this setup. More precisely, he showed that the class group of the ring of integers of a number field with unit rank at least 1 is cyclic if and only if it has a Euclidean ideal class, provided the generalised Riemann hypothesis holds. The aim of this paper is to show the following. Suppose that $\mathbf{K}_1$ and $\mathbf{K}_2$ are two Galois number fields of odd prime degree with cyclic class groups and Hilbert class fields that are abelian over $\mathbb{Q}$. If $\mathbf{K}_1\mathbf{K}_2$ is ramified over $\mathbf{K}_i$, then at least one $\mathbf{K}_i$ ($i \in \{1, 2\}$) must have a Euclidean ideal class.

1. INTRODUCTION

A well known result of Weinberger [16] from 1972 states that the ring of integers of a number field $\mathbf{K}$ with unit rank at least 1, has class number 1 if and only if it is a Euclidean domain, provided we assume that the generalised Riemann hypothesis (Riemann hypothesis for all Dedekind zeta functions) holds. In 1977, this result was extended by Lenstra [12]. He showed that if the ring of S-integers of a number field with $|S| \geq 2$ is a principal ideal domain, it is Euclidean, again provided we assume the generalised Reimann hypothesis.

The first unconditional result on this problem came in a paper of the first author, Gupta and Ram Murty [7] in 1985. Using the techniques introduced in the famous work of Gupta and Ram Murty on Artin's conjecture [4], the authors of [7] were able to show unconditionally that rings of S-integers in certain Galois number fields $\mathbf{K}$ have trivial S-class group if and only if they are Euclidean when $|S| \geq \max\{5, 2[\mathbf{K} : \mathbb{Q}] - 3\}$.

In 1995, Clark and Ram Murty [2] were able to extend this result to rings of integers of totally real Galois number fields of degree atleast 4 with an additional property. At this juncture, the case of lower degree had still not been addressed.

In 2004, Harper in his thesis, showed that the ring $\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain [8]. This was immediately followed by a paper of Harper and Ram Murty who introduced some important new ideas to show unconditionally that the ring of integers of a Galois number field with unit

2010 *Mathematics Subject Classification.* 11A05, 13F07, 11R04, 11R37, 11N36 .

Key words and phrases. Euclidean ideal classes, Genus fields, Hilbert class fields, Application of sieve methods.

rank atleast 4 is Euclidean if and only if it has class number 1 [9]. Further in the case of abelian number fields they were able to extend the same result to the case of unit rank 3. Narkiewicz [15] in 2007, used some of the ideas from the works of Harper [8], Harper and Ram Murty [9] and Heath-Brown [10] to address the case of lower unit rank in greater detail. He showed that for Galois cubic fields with class number 1, there is atmost 1 whose ring of integers is not a Euclidean domain and in case of real quadratic fields with class number 1 there are atmost 2 whose rings of integers are not Euclidean domains.

On the other hand, in 1979, Lenstra [13] extended the notion of Euclidean domains to cover a larger family of Dedekind domains with finite cyclic class groups, thereby extending the notion beyond class number 1. In order to do so he defined Euclidean ideal classes. We state the definition of Euclidean ideal classes below while assuming that the ambient ring is the ring of integers of a number field.

Definition 1. *Let $\mathcal{O}_{\mathbf{K}}$ be the ring of integers of a number field $\mathbf{K}$, E be the set of all non-zero integral ideals of $\mathcal{O}_{\mathbf{K}}$ and W be a well-ordered set. Given a map*

$$\psi : E \to W,$$

we say that a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbf{K}}$ is Euclidean for ψ if for each non-zero ideal $\mathfrak{b}$ of $\mathcal{O}_{\mathbf{K}}$ and any $x \in \mathfrak{b}^{-1}\mathfrak{a} - \mathfrak{a}$, there exists $y \in \mathfrak{a}$ such that

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

Further the class $[\mathfrak{a}]$ is called a Euclidean ideal class of $\mathcal{O}_{\mathbf{K}}$.

Lenstra's arguments show that if $\mathcal{O}_{\mathbf{K}}$ has a Euclidean ideal class, it must have a finite cyclic class group which is in fact generated by the Euclidean ideal class. He goes on to show that for number fields with unit rank atleast 1, if the class group is cyclic it must have a Euclidean ideal class, provided the generalised Riemann hypothesis holds.

The first unconditional result in the Euclidean ideal class setup was shown by Graves and Ram Murty [4]. Their precise result is stated below.

Theorem 1. (Graves and Ram Murty [4]) *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 atleast 4, then the class group $\mathrm{Cl}_{\mathbf{K}} = \langle [C] \rangle$ if and only if $[C]$ is a Euclidean ideal class.*

The result was extended to a family of number fields with unit rank 3 by Deshouillers, Gun and Sivaraman [3]. We state the precise result below.

Theorem 2. (Deshouillers, Gun and Sivaraman [3]) *Suppose that $\mathbf{K}$ is a number field with unit rank greater than or equal to 3 and its Hilbert class field $\mathbf{H}(\mathbf{K})$ is abelian over $\mathbb{Q}$. Also suppose that the*

conductor of $\mathbf{K}$ *(that is, the least positive integer* n *for which* $\mathbf{K} \subset \mathbb{Q}(\zeta_n)$*) is* f *and* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$ *is cyclic. Then the class group* $\mathrm{Cl}_{\mathbf{K}}$ *is cyclic if and only if it has a Euclidean ideal class.*

Investigations have also been carried out in number fields of lower unit rank. The theorem of Narkiewicz [15] was extended to this setup under certain conditions by Gun and Sivaraman [5]. We state below the result of Gun and Sivaraman [5] in the case of Galois cubic fields.

Let $\mathbf{K}_1$ and $\mathbf{K}_2$ be number fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$ (abelian over $\mathbb{Q}$) respectively. Also let f_1 and f_2 be the conductors of $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$ respectively. Set f to be the least common multiple of 16, f_1 and f_2. Further, $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where ζ_f is a primitive fth root of unity. In this set up, the result is as follows.

Theorem 3. (Gun and Sivaraman [5]) *Let* $\mathbf{K}_1, \mathbf{K}_2$ *be distinct Galois 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* $\ell = 4$*. If*

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

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

In this paper we extend the above result by removing the condition $G \not\subset \bigcup_\ell G_\ell$ where ℓ is either an odd prime dividing f or $\ell = 4$. The precise result is stated below.

Theorem 4. *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be distinct Galois number fields of odd prime degree with cyclic class groups, such that the Hilbert class fields are abelian over* $\mathbb{Q}$*. If* $\mathbf{K}_1\mathbf{K}_2$ *is ramified over* $\mathbf{K}_i$*, then at least one* $\mathbf{K}_i$ *for* $i \in \{1, 2\}$ *has a Euclidean ideal class.*

The rest of the paper is organised as follows. In the preliminaries, we state some results which will be used in due course of the main proof. This will be followed by a section on choosing a residue class modulo f. In the next section, we give the proof of Theorem 4 using this choice of residue class. In the penultimate section, we give some examples of fields for which our theorem holds and the final section consists of the data availability statement.

2. PRELIMINARIES

We state below some definitions and theorems required to complete the proof of our theorem. We first state the definition of a genus field of an abelian number field $\mathbf{K}$.

Definition 2. *For an abelian number field* $\mathbf{K}$*, the maximal extension* $\mathbf{G}(\mathbf{K})$ *of* $\mathbf{K}$*, abelian over* $\mathbb{Q}$*, which is unramified at all the finite places of* $\mathbf{K}$ *is called the genus field of* $\mathbf{K}$*. Further* $[\mathbf{G}(\mathbf{K}) : \mathbf{K}]$ *is called the genus number of* $\mathbf{K}$*, denoted* $g_{\mathbf{K}}$*.*

The first theorem we state here is due to Leopoldt stated as a corollary in Section 5 of [14].

Theorem 5. (Leopoldt [14], Pg 52 [11]) *For an abelian number field* $\mathbf{K}$ *the genus number* $g_{\mathbf{K}}$ *is given by*

$$g_{\mathbf{K}} = \frac{\prod_q e(q)}{[\mathbf{K} : \mathbb{Q}]}$$

where the product runs over rational primes q *and* $e(q)$ *is the ramification index of* q *with respect to the field* $\mathbf{K}$.

We now introduce the definition of the Hilbert class field of a number field $\mathbf{K}$.

Definition 3. *For a number field* $\mathbf{K}$, *the Hilbert class field* $\mathbf{H}(\mathbf{K})$ *is the maximal extension of* $\mathbf{K}$, *abelian over* $\mathbf{K}$, *which is unramified at all the places of* $\mathbf{K}$. *The degree* $[\mathbf{H}(\mathbf{K}) : \mathbf{K}]$ *is denoted by* $h_{\mathbf{K}}$.

Remark 2.1. *We note that if the Hilbert class field* $\mathbf{H}(\mathbf{K})$ *is abelian over* $\mathbb{Q}$, *then it is an abelian number field containing* $\mathbf{K}$ *and unramified at all the finite places of* $\mathbf{K}$. *Therefore* $\mathbf{H}(\mathbf{K}) \subset \mathbf{G}(\mathbf{K})$ *and therefore* $h_{\mathbf{K}} \mid g_{\mathbf{K}}$. *In particular for a field* $\mathbf{K}$ *of odd prime degree* p *whose* $\mathbf{H}(\mathbf{K})$ *is abelian over* $\mathbb{Q}$, *the ramification indices* $e(q) \mid p$ *for all rational primes* q. *Therefore* $h_{\mathbf{K}}$ *is a non-negative power of* p *(by Theorem 5). This fact will be used crucially in the proof of Lemma 9.*

The next theorem is Theorem 14 of Gun and Sivaraman [5], on Euclidean ideal classes in quadratic and cubic fields.

Theorem 6. (Gun and Sivaraman [5]) *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*

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

then $[\mathfrak{a}]$ *is a Euclidean ideal class of* $\mathcal{O}_{\mathbf{K}}$.

The next is Lemma 3 of Heath-Brown's paper on Artin's conjecture [10].

Lemma 7. (Heath-Brown [10]) *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 $a, b \in (\frac{1}{4}, \frac{1}{2})$ *with* $a < b$ *such that for any* $\epsilon > 0$, *the set*

$$\begin{aligned} P(X) \quad := \quad & \{p \equiv u \bmod v \,:\, p \in (X^{1-\epsilon}, X) \text{ such that } \frac{p-1}{2} \text{ is either prime or} \\ & \text{is a product of primes } q_1 q_2 \text{ with } X^a \leq q_1 \leq X^b\} \end{aligned}$$

has cardinality $\gg X/\log^2 X$.

The final lemma is Lemma 2 of Narkiewicz's paper [15], on counting units in residue classes of number fields.

Lemma 8 (Narkiewicz [15]). *Let $\mathbf{K}$ be an arbitrary algebraic number field and 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 1 in $\mathbf{K}$ and $\mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p})$ denotes the absolute norm of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$. Suppose that T has the following properties;*

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

$$|T(x_n) := \{\mathfrak{p} \in T \ : \ \mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) \leq x_n\}| \ > \ cx_n/\log^2 x_n \ \text{ for all } n.$$

(2) *there exist $\alpha, \beta \in (1/4, 1/2)$ with $\alpha < \beta$ such that if $\mathfrak{p} \in T$ and $p := \mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p})$, then either $p - 1 = 2q$ or $p - 1 = 2q_1q_2$ where q, q_1 and q_2 are primes such that $p^\alpha < q_1 < p^\beta$.*
(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_is is a primitive root for at least $(c - \epsilon)y_m/\log^2 y_m$ elements of $T(y_m)$.

In the next section, we will construct an appropriate residue class before we proceed to the proof of the main theorem.

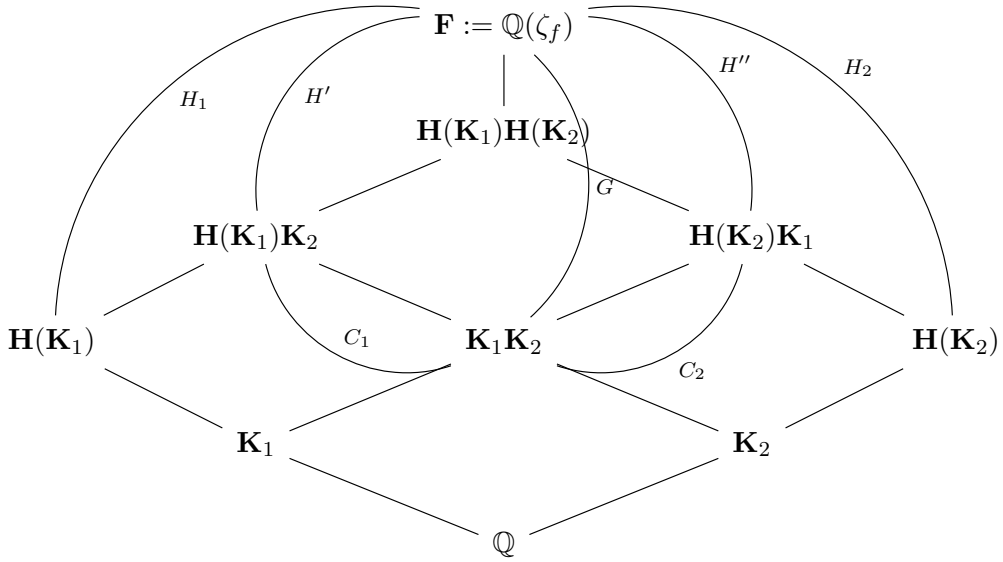
3. Choosing a residue class

We briefly state some notation that will be used in this section. Let $\mathbf{K}_1$ and $\mathbf{K}_2$ be distinct fields of degree p_1 and p_2 (odd primes), with cyclic class groups and Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$ (assumed abelian over $\mathbb{Q}$) respectively. Also let f_1 and f_2 be the conductors of $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$ respectively. Set f to be the least common multiple of 16, f_1 and f_2. Further let $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where ζ_f is a primitive fth root of unity. Let G be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$.

Lemma 9. *If $\mathbf{K}_1\mathbf{K}_2$ is ramified over $\mathbf{K}_i$, then there exists a residue class $d \bmod f \in G$ such that the image of $d \bmod f$ in $Gal(\mathbf{H}(\mathbf{K}_i)/\mathbf{K}_i)$ is a generator of the group and $d \bmod f \notin Gal(\mathbf{F}/\mathbb{Q}(\zeta_\ell))$ for any odd prime $\ell \mid f$ or $\ell = 4$.*

Proof. If $h_{\mathbf{K}_i} \neq 1$ and $\mathbf{K}_1\mathbf{K}_2$ is ramified over $\mathbf{K}_i$, it follows that $\mathbf{H}(\mathbf{K}_i) \cap \mathbf{K}_1\mathbf{K}_2 = \mathbf{K}_i$. If $h_{\mathbf{K}_i} = 1$ we still have $\mathbf{H}(\mathbf{K}_i) \cap \mathbf{K}_1\mathbf{K}_2 = \mathbf{K}_i$. Therefore we have the following diagram when $\mathbf{H}(\mathbf{K}_i) \neq \mathbf{K}_i$

for $i \in \{1, 2\}$.



Consider a $c \bmod f \in G$ which restricts to a generator of C_1 (Galois group of $\mathbf{H}(\mathbf{K}_1)\mathbf{K}_2/\mathbf{K}_1\mathbf{K}_2$) and C_2 (Galois group of $\mathbf{H}(\mathbf{K}_2)\mathbf{K}_1/\mathbf{K}_1\mathbf{K}_2$). Note that these groups are non-trivial and isomorphic to the class groups of $\mathbf{K}_1$ and $\mathbf{K}_2$, respectively and cyclic by our assumptions. This also implies that $1 \not\equiv c \bmod f$.

Claim: We may assume that the order of $c \bmod f$ is odd.
If not, we may replace $c \bmod f$ with $c' \equiv c^{2^m} \bmod f$ where the 2-adic valuation of the order of $c \bmod f$ is m. Such a $c' \bmod f$ is still in G and since the class numbers are powers of the odd primes p_1 and p_2 (by the remarks after Definition 3), it will still restrict to a generator of C_1 and C_2.

Let H_i be the Galois group of $\mathbb{Q}(\zeta_f)/H(\mathbf{K}_i)$, H' the Galois group of $\mathbb{Q}(\zeta_f)/H(\mathbf{K}_1)\mathbf{K}_2$ and H'' the Galois group of $\mathbb{Q}(\zeta_f)/H(\mathbf{K}_2)\mathbf{K}_1$. Further, since the $\mathbf{K}_i$ are totally real, $-1 \bmod f \in H_1 \cap H_2 \cap G = H' \cap H''$. This implies that $\bar{c}H' = -\bar{c}H'$ and $\bar{c}H'' = -\bar{c}H''$. So we consider the element $-c \bmod f \in G$ such that

(1) $c \bmod f$ has odd order;
(2) $c \bmod f$ restricts to a generator of C_1 and C_2 and therefore so does $-c \bmod f$.

We observe that $(-c \bmod f)^{ord(c \bmod f)} \equiv -1 \bmod f$. This implies that

$$-1 \bmod f \in \langle -c \bmod f \rangle.$$

This implies that $-c \bmod f \notin Gal(\mathbf{F}/\mathbb{Q}(\zeta_\ell))$ for any odd prime $\ell \mid f$ or $\ell = 4$. In other words $\left(\frac{-c-1}{2}, f\right) = 1$.

If only one of the class groups is trivial then we can find a $c \bmod f$ which corresponds to a generator of the non-trivial class group with the above two properties.

The resulting congruence class $-c \bmod f$ is in G and therefore corresponds to a generator for both class groups.

If both the class groups are trivial then $c \equiv -1 \bmod f$ will satisfy the required conditions. $\square$

4. Proof of Theorem 4

Throughout this subsection, let $\mathbf{K}_1$ and $\mathbf{K}_2$ be Galois fields of odd prime degree with Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$, abelian over $\mathbb{Q}$ respectively. Also let f_1 and f_2 be their conductors. Set f to be the least common multiple of $16, f_1, f_2$. Choose a positive integer u_1 such that it satisfies $u_1 \equiv d \bmod f$. It follows from Lemma 7 and Lemma 9 that there exist $a, b \in (\frac{1}{4}, \frac{1}{2})$ with $a < b$ such that for any $\epsilon > 0$

$$\begin{aligned} |J_\epsilon(X) \;:=\; \{&p \equiv u_1 \bmod f \;:\; p \text{ rational prime, } p \in (X^{1-\epsilon}, X) \text{ such that} \\ &\frac{p-1}{2} \text{ is either a rational prime or a product of rational} \\ &\text{primes } q_1 q_2 \text{ with } X^a < q_1 < X^b\}| \gg \frac{X}{\log^2 X}. \end{aligned}$$

Next set $\mathbf{K} = \mathbf{K}_1\mathbf{K}_2$. Note that any prime $p \in \mathbb{Z}$ which is congruent to $u_1 \bmod f$ splits in $\mathbf{K}_1\mathbf{K}_2$. Since $\left(\frac{u_1-1}{2}, f\right) = 1$, we note that $u_1 \equiv 3 \bmod 4$. Choose ϵ such that $a < \frac{b}{1-\epsilon} < \frac{1}{2}$. Consider the set

$$\begin{aligned} M_\epsilon \;:=\; \{&\mathfrak{p} \;:\; \mathfrak{p} \text{ is a prime ideal in } \mathcal{O}_{\mathbf{K}},\ \mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) = p \text{ rational prime }, p \equiv u_1 \bmod f, \\ &\frac{p-1}{2} \text{ is either a rational prime or a product of} \\ &\text{rational primes } q_1 q_2 \text{ with } p^a < q_1 < p^{\frac{b}{1-\epsilon}}\}; \end{aligned}$$

and also the set $M_\epsilon(X) := \{\mathfrak{p} \in M_\epsilon : \mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) \leq X\}$ for any real number $X > 0$. It follows that $M_\epsilon(X) \gg \frac{X}{\log^2 X}$. Suppose that ϵ_1, ϵ_2 and ϵ_3 are fundamental units from $\mathbf{K}_i$ with atleast one from each $\mathbf{K}_i$ for $i \in \{1, 2\}$.

Following the proof of Lemma 16 in [5], we write $M_\epsilon = \cup_{n=1}^{8} M_n$. where each M_n corresponds to a tuple (c_1, c_2, c_3) with entries in ± 1 such that $\left(\frac{\epsilon_i}{\mathfrak{p}}\right) = -c_i$ for all $\mathfrak{p} \in M_n$. Here $\left(\frac{\cdot}{\mathfrak{p}}\right)$ is used to denote the second power residue symbol.

Since $M_\epsilon(X) \gg \frac{X}{\log^2 X}$, we claim that there exists an increasing unbounded sequence of positive real numbers $\{x_m\}_{m \in \mathbb{N}}$ and a $c > 0$ such that

$$M_{n_0}(x_m) > c\frac{x_m}{\log^2 x_m} \text{ for some } 1 \leq n_0 \leq 8.$$

Suppose not, then for any $1 \leq n \leq 8$, we have

$$\limsup_{X\to\infty} \frac{M_n(X)}{X/\log^2 X} = 0 \quad \text{and} \quad \liminf_{X\to\infty} \frac{M_n(X)}{X/\log^2 X} = 0.$$

This implies $M_\epsilon(X) = o\left(\frac{X}{\log^2 X}\right)$, which is a contradiction.

Further since $u_1 \equiv 3 \bmod 4$, it follows that $\left(\frac{-1}{\mathfrak{p}}\right) = -1$. For the tuple (c_1, c_2, c_3) corresponding to M_{n_0}, $c_i\epsilon_i$ is a quadratic non-residue modulo any prime $\mathfrak{p} \in M_{n_0}$. Now, on applying Lemma 8 with $T = M_{n_0}$ there exists a subsequence $\{y_l\}_{l\in\mathbb{N}}$ of $\{x_m\}_{m\in\mathbb{N}}$ such that one of the elements $\pm\epsilon_1, \pm\epsilon_2, \pm\epsilon_3$ is a primitive root modulo $\mathfrak{p}$ for atleast $(c-\epsilon)y_l/\log^2 y_l$ elements of $M_{n_0}(y_l)$ for any $0 < \epsilon < c$. We denote this subset of elements of M_{n_0} by Q and the primitive root by η.

For Q and η as above, it follows that $\eta \in \mathbf{K}_s$ for some $s \in \{1, 2\}$. Further we have a sequence $\{y_l\}_{l\in\mathbb{N}}$ such that

$$Q(y_l) \geq (c-\epsilon)\frac{y_l}{\log^2 y_l} \quad \text{where} \quad Q(X) := \{\mathfrak{p} \in Q : \mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) \leq X\}.$$

Since every $\mathfrak{p} \in Q$ has degree 1, η generates $(\mathcal{O}_{\mathbf{K}_s}/\mathfrak{r})^\times$ where $\mathfrak{r} = \mathfrak{p} \cap \mathbf{K}_s$. Note $\mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) = p$ and $p \equiv u_1 \bmod f$, $u_1 \bmod f$ restricts to a generator of C_s (by Lemma 9) and therefore to a generator of $Gal(\mathbf{H}(\mathbf{K}_s)/\mathbf{K}_s)$ and is trivial on $\mathbf{K}_s$.

Therefore for all the primes in $\mathbf{K}_s$ below the ones in Q, the Artin symbol with respect to $Gal(\mathbf{H}(\mathbf{K}_s)/\mathbf{K}_s)$ corresponds to a generator of C_s. By the isomorphism between said Galois group and the class group of $\mathbf{K}_s$ and by Theorem 6, we see that this class must be a Euclidean ideal class. This completes the proof of Theorem 4.

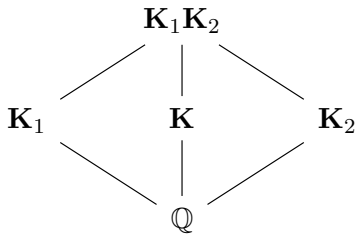
5. Examples

In this section, we provide some examples as an application of Theorem 4.

Lemma 10. *Let p and q be two distinct primes which are $1 \bmod 3$. The cyclotomic field $\mathbb{Q}(\zeta_{pq})$ contains four subfields of degree 3. If the class number of a subfield not contained in both $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$ is 3, then the Hilbert class field of the subfield is abelian over $\mathbb{Q}$.*

Proof. The cyclotomic fields $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$ have each a unique subfield of degree 3. Consider the compositum of these fields. This is a subfield of $\mathbb{Q}(\zeta_{pq})$ of degree 9 with Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This gives rise to four subfields of degree 3, two of which are contained in $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$. Conversely any element of order 3 in the Galois group of $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}$ must be in the unique subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ in the Galois group of of $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}$ and therefore these are the only degree 3 subfields. For the two abelian cubic fields which are not contained in $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$, the conductor is pq. Therefore both p and q ramify in these fields. Now

consider the following diagram.



Suppose that $\mathbf{K}_1 \subset \mathbb{Q}(\zeta_p)$, $\mathbf{K}_2 \subset \mathbb{Q}(\zeta_q)$ and $\mathbf{K}$ is one of the other two subfields. Then p ramifies in $\mathbf{K}_1$ and not $\mathbf{K}_2$ and therefore has ramification index 3 with respect to $\mathbf{K}_1\mathbf{K}_2$. Similarly q ramifies in $\mathbf{K}_2$ and not $\mathbf{K}_1$ and therefore has ramification index 3 with respect to $\mathbf{K}_1\mathbf{K}_2$. Since both p and q have ramification index 3 with respect to $\mathbf{K}$, the extension $\mathbf{K}_1\mathbf{K}_2/\mathbf{K}$ is unramified at all places of $\mathbf{K}$. If the class number of $\mathbf{K}$ is 3 then the Hilbert class field of $\mathbf{K}$ must be $\mathbf{K}_1\mathbf{K}_2$ and is therefore abelian over $\mathbb{Q}$. □

Corollary 11. *Consider four distinct primes p_1, q_1, p_2 and q_2, all of which are $1 \bmod 3$. Suppose that either $\mathbf{K}_1$ is a cubic subfield of $\mathbb{Q}(\zeta_{p_1q_1})$ not contained in $\mathbb{Q}(\zeta_{p_1})$ or $\mathbb{Q}(\zeta_{q_1})$ with class number 3 or it is a cubic subfield with class number 1. Similarly either $\mathbf{K}_2$ is a cubic subfield of $\mathbb{Q}(\zeta_{p_2q_2})$ not contained in $\mathbb{Q}(\zeta_{p_2})$ or $\mathbb{Q}(\zeta_{q_2})$ with class number 3 or it is a cubic subfield with class number 1. Then at least one $\mathbf{K}_i$ must have a Euclidean ideal class.*

Proof. Since the conductors of $\mathbf{K}_1$ and $\mathbf{K}_2$ are co-prime to each other, it follows that $\mathbf{K}_1\mathbf{K}_2$ over $\mathbf{K}_i$ must be ramified for $i \in \{1, 2\}$. By Lemma 10, the Hilbert class field of each $\mathbf{K}_i$ is abelian over $\mathbb{Q}$. Therefore from Theorem 4 we have the corollary. □

Remark 5.1. *We would like to remark here that if the Hilbert class field is abelian over $\mathbb{Q}$ and the class number is a power of 3 greater than or equal to 9, the class group will no longer be cyclic (see* [11]*, Corollary to Theorem 5, Page 64-65).*

The following table contains examples of fields satisfying the hypothesis of Corollary 11 (generated using SAGE).

TABLE 1. Examples of cubic subfields with class number 1 in $\mathbb{Q}(\zeta_{pq})$.

Serial	p	q	Defining polynomial of the subfield	Class number of the ring of integers
1	7	13	$x^3 - x^2 - 2x + 1$	1
2	7	13	$x^3 - x^2 - 4x - 1$	1
3	7	19	$x^3 - x^2 - 2x + 1$	1
4	7	19	$x^3 - x^2 - 6x + 7$	1

Serial	p	q	Defining polynomial of the subfield	Class number of the ring of integers
5	7	31	$x^3 - x^2 - 2x + 1$	1
6	7	31	$x^3 - x^2 - 10x + 8$	1
7	7	37	$x^3 - x^2 - 2x + 1$	1
8	7	37	$x^3 - x^2 - 12x - 11$	1
9	7	43	$x^3 - x^2 - 2x + 1$	1
10	7	43	$x^3 - x^2 - 14x - 8$	1
11	7	61	$x^3 - x^2 - 2x + 1$	1
12	7	61	$x^3 - x^2 - 20x + 9$	1
13	7	67	$x^3 - x^2 - 2x + 1$	1
14	7	67	$x^3 - x^2 - 22x - 5$	1
15	13	19	$x^3 - x^2 - 6x + 7$	1

TABLE 2. Examples of cubic subfields with class number 3 in $\mathbb{Q}(\zeta_{pq})$. (not contained in $\mathbb{Q}(\zeta_p)$ or $\mathbb{Q}(\zeta_q)$)

Serial	p	q	Defining polynomial of the subfield	Class number of the ring of integers
1	7	13	$x^3 - x^2 - 30x - 27$	3
2	7	13	$x^3 - x^2 - 30x + 64$	3
3	7	19	$x^3 - x^2 - 44x - 69$	3
4	7	19	$x^3 - x^2 - 44x + 64$	3
5	7	31	$x^3 - x^2 - 72x - 209$	3
6	7	31	$x^3 - x^2 - 72x + 225$	3
7	7	37	$x^3 - x^2 - 86x + 211$	3
8	7	37	$x^3 - x^2 - 86x - 48$	3
9	7	43	$x^3 - x^2 - 100x + 379$	3
10	7	43	$x^3 - x^2 - 100x - 223$	3
11	7	61	$x^3 - x^2 - 142x + 680$	3
12	7	61	$x^3 - x^2 - 142x - 601$	3
13	7	67	$x^3 - x^2 - 156x - 608$	3
14	7	67	$x^3 - x^2 - 156x + 799$	3
15	13	19	$x^3 - x^2 - 82x + 64$	3

6. DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

REFERENCES

[1] *The shaping of arithmetic after C. F. Gauss's Disquisitiones arithmeticae,* Edited by C. Goldstein, N. Schappacher and J. Schwermer, Springer, Berlin (2007).

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

[3] J.-M. Deshouillers, S. Gun and J. Sivaraman, *On Euclidean ideal classes in certain Abelian extensions,* Mathematische Z. **296** (2020), 847– 859.

[4] H. Graves and M. Ram 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.

[5] S. Gun and J. Sivaraman, *On Existence of Euclidean Ideal Classes in Real Cubic and Quadratic Fields with Cyclic Class Group,* Michigan Math. J. **69**, Issue 2 (2020), 429 – 448.

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

[7] R. Gupta, V. Kumar Murty and M. Ram Murty, *The Euclidean algorithm for S-integers*, Number Theory (Montreal 1985), CMS Conf. Proc. 7, American Mathematical Society, Providence (1987), 189–201.

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

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

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

[11] M. Ishida, *The genus fields of algebraic number fields*, Lecture notes in Mathematics - 555, Springer-Verlag Berlin Heidelberg (1976).

[12] H. W. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent Math **42**, 201–224 (1977).

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

[14] H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkorpern,* Math. Nachr. **9** (1953), 350-362

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

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

(V. Kumar Murty) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, 40 ST. GEORGE STREET, TORONTO, ON, CANADA, M5S 2E4.

Email address: murty@math.toronto.edu

(J. Sivaraman) CHENNAI MATHEMATICAL INSTITUTE, H1, SIPCOT IT PARK, SIRUSERI, KELAMBAKKAM, INDIA, 603103.

Email address: jyothsnaas@cmi.ac.in