TWO CLASSES OF NUMBER FIELDS WITH A NON-PRINCIPAL EUCLIDEAN IDEAL

CATHERINE HSU

ABSTRACT. This paper introduces two classes of totally real quartic number fields, one of biquadratic extensions and one of cyclic extensions, each of which has a non-principal Euclidean ideal. It generalizes techniques of Graves used to prove that the number field $\mathbb{Q}(\sqrt{2}, \sqrt{35})$ has a non-principal Euclidean ideal.

1. INTRODUCTION

1.1. **Notation.** Given a number field K, we will denote its ring of integers $\mathcal{O}_K$, its class group Cl_K, its class number h_K, and its conductor $f(K)$. When $K/\mathbb{Q}$ is abelian, we will denote its Hilbert class field over $\mathbb{Q}$ by $H/\mathbb{Q}$. In this situation, for a rational prime $p \in \mathbb{Z}$, we will use $\mathfrak{p}$ to denote a prime in $\mathcal{O}_K$ lying over (p) and $\mathfrak{P}$ to denote a prime in $\mathcal{O}_H$ lying over $\mathfrak{p}$.

1.2. **Background and Main Results.** In 1979, Lenstra [8] defined the Euclidean ideal, a generalization of the Euclidean algorithm:

Definition 1. Suppose R is a Dedekind domain and that E is the set of fractional ideals that contain R. If C is an ideal of R, it is *Euclidean* if there exists a function $\psi : E \to W$, W a well-ordered set, such that for all $I \in E$ and all $x \in IC \setminus C$, there exists some $y \in C$ such that

$$\psi((x+y)^{-1}IC) < \psi(I).$$

We say ψ is a Euclidean algorithm for C and C is a Euclidean ideal.

While the existence of a Euclidean ideal C in a ring of integers $\mathcal{O}_K$ does not give a method for computing greatest common divisors as a Euclidean algorithm would, it does guarantee that the class group has a certain structure, namely $\mathrm{Cl}_K = \langle [C] \rangle$.

One method that can be used in certain situations to produce a Euclidean algorithm for an ideal C is a Motzkin-type construction for ideals [2]. As its name suggests, this method is a generalization of Motzkin's construction [10], which can be used to find a Euclidean algorithm on certain integral domains. Before we can give an explicit example of such a Euclidean algorithm for C, we need to recall the definition from [2] of a Motzkin-type construction for ideals:

The author's research is partially supported by a GAANN Fellowship.

Definition 2. Given a non-zero ideal C in R, we define

$$A_{0,C} := \{R\}$$

$$A_{i,C} := A_{i-1,C} \cup \left\{ I \in E \,\middle|\, \begin{array}{c} \forall x \in IC \setminus C,\, \exists y \in C \text{ such} \\ \text{that } (x+y)^{-1}IC \in A_{i-1,C} \end{array} \right\} \text{ for } i > 0,$$

and $A_C := \bigcup_{i=0}^{\infty} A_{i,C}$.

Note that the $A_{i,C}$'s are nested sets.

Given this definition, Graves [2] proves that if $A_C = E$, where E is the set fractional ideals containing R, we can construct a Euclidean algorithm for C via the function $\psi_C : E \to \mathbb{N}$ defined by

$$\psi_C(I) = i, \qquad \text{if } I \in A_{i,C} \setminus A_{i-1,C}.$$

Indeed, if I is an ideal in E and $x \in IC \setminus C$, then since $I \in A_C$, there exists some $y \in C$ such that $(x+y)^{-1}IC$ is an element of $A_{\psi_C(I)-1,C}$, and hence, for this $y \in C$,

$$\psi_C((x+y)^{-1}IC) \leq \psi_C(I) - 1 < \psi_C(I).$$

Now, just as the existence of a Euclidean algorithm for the ring of integers $\mathcal{O}_K$ in a number field K implies a trivial class group, the existence of a Euclidean ideal C in $\mathcal{O}_K$ implies a cyclic class group with generator $[C]$. In fact, Lenstra proves a much stronger result:

Theorem 1. *[8] (Lenstra, 1979) Suppose K is a number field, $|\mathcal{O}_K^\times| = \infty$, and C is an ideal of $\mathcal{O}_K$. If one assumes the Generalized Riemann Hypothesis, then C is a Euclidean ideal if and only if $\mathrm{Cl}_K = \langle [C] \rangle$.*

By generalizing the work of Harper and Murty [5, 6] on Euclidean rings to the Euclidean ideal case, Graves [2] proves that under certain conditions, Theorem 1 holds without assuming the Generalized Riemann Hypothesis:

Theorem 2. *[2] (Graves, 2013) If K is a number field such that $|\mathcal{O}_K^\times| = \infty$, if $[C]$ generates Cl_K, and if*

$$\left| \left\{ \begin{array}{c} \textit{prime ideals} \\ \mathfrak{p} \subset \mathcal{O}_K \end{array} \,\middle|\, \mathrm{Nm}(\mathfrak{p}) \leq x,\, [\mathfrak{p}] = [C],\, \mathcal{O}_K^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p})^\times \right\} \right| \gg \frac{x}{\log^2 x},$$

then C is a Euclidean ideal.

In order to use the growth result given in Theorem 2 to find explicit examples of number fields with a Euclidean ideal, we require the following theorem which Graves stated in [1] by utilizing results from [7, 11]:

Theorem 3. *If K is a totally real number field with conductor $f(K)$, if $\{e_1, e_2, e_3\}$ is a multiplicatively independent set contained in $\mathcal{O}_K^\times$, if $\ell = \mathrm{lcm}(16, f(K))$, and if $(u, \ell) = \left(\frac{u-1}{2}, \ell\right) = 1$, then*

$$\left| \left\{ \begin{array}{c} \textit{prime ideals } \mathfrak{p} \\ \textit{of first degree} \end{array} \,\middle|\, \begin{array}{c} \mathrm{Nm}(\mathfrak{p}) \equiv u \pmod{\ell}, \\ \mathrm{Nm}(\mathfrak{p}) \leq x, \langle -1, e_i \rangle \twoheadrightarrow (\mathcal{O}/\mathfrak{p})^\times \end{array} \right\} \right| \gg \frac{x}{\log^2 x},$$

for at least one i.

In [1], Graves uses Theorems 2 and 3 to prove that $\mathbb{Q}(\sqrt{2}, \sqrt{35})$ has a non-principal Euclidean ideal. In this paper, we generalize Graves' work to prove our first main result that a certain class of biquadratic number fields have a non-principal Euclidean ideal. The first main result is:

Theorem 4. *If a number field K is of the form $\mathbb{Q}(\sqrt{q}, \sqrt{k \cdot r})$, where $q, k, r \geq 29$ are distinct rational primes satisfying $q, k, r \equiv 1 \pmod 4$, and if $h_K = 2$, then K has a non-principal Euclidean ideal.*

Then by slightly modifying the techniques used to prove Theorem 4, we obtain our second main result that a certain class of cyclic number fields also have a non-principal Euclidean ideal. The second main result is:

Theorem 5. *If a number field K is of the form*

$$\mathbb{Q}\left(\sqrt{q(k + b\sqrt{k})}\right),$$

where $q, k \geq 17$ are distinct rational primes satisfying $q, k \equiv 1 \pmod 4$ and $b > 0$ is an integer satisfying $b \equiv 0 \pmod 4$, if $k - b^2 > 0$ is a perfect square, and if $h_K = 2$, then K has a non-principal Euclidean ideal.

Remark 1. The significance of these results is that while Graves introduced one number field with a non-principal Euclidean ideal, we give conditions that provide two new classes of examples of number fields, each of which contains a non-principal Euclidean ideal. In particular, Murty and Graves [3] provide the only other examples of number fields with a non-principal Euclidean ideal found without assuming the Generalized Riemann Hypothesis. Their results require unit rank at least 4; our results do not require this condition.

Remark 2. Using PARI [4], the author has found hundreds of number fields satisfying the conditions given in Theorems 4 and 5, some of which are given in Tables 1 and 2. The author conjectures that both of these classes of number fields with a non-principal Euclidean ideal are in fact infinite.

1.3. **Acknowledgments.** I would like to thank my advisor Ellen Eischen for suggesting this project as well as for providing useful feedback. I would also like to thank Dylan Muckerman for helping me write the Python code used to find explicit examples of number fields with a non-principal Euclidean ideal.

2. Proof of Main Results

In order to prove our main results, we would like to apply Theorem 3 to the number field K in order to obtain a growth result which satisfies the hypotheses of Theorem 2. We will first prove our result in the biquadratic case and then modify this proof to obtain our second result in the cyclic case.

2.1. **Main Result in the Biquadratic Case.** Throughout this section, we will assume that K is a number field satisfying the conditions given in Theorem 4, i.e., $h_K = 2$ and

$$K = \mathbb{Q}(\sqrt{q}, \sqrt{k \cdot r}),$$

where $q, k, r \geq 29$ are distinct rational primes satisfying $q, k, r \equiv 1 \pmod 4$.

Before we can prove Theorem 4, we need the following two lemmas.

Lemma 1. *The conductor $f(K)$ of K is qkr.*

Proof. Since both $q \equiv 1 \pmod 4$ and $k \cdot r \equiv 1 \pmod 4$, the conductors of $\mathbb{Q}(\sqrt{q})$, $\mathbb{Q}(\sqrt{k \cdot r})$ are q and kr, respectively. So, since $\mathbb{Q}(\zeta_{f(K)})$ must contain both of these quadratic fields, the minimality of a conductor implies that

$$\mathbb{Q}(\zeta_q), \mathbb{Q}(\zeta_{kr}) \subseteq \mathbb{Q}(\zeta_{f(K)}).$$

By the theory of cyclotomic fields, both q and kr must divide $f(K)$, and hence, since

$$K \subseteq \mathbb{Q}(\sqrt{q})\mathbb{Q}(\sqrt{k \cdot r}) \subseteq \mathbb{Q}(\zeta_q)\mathbb{Q}(\zeta_{kr}) \subseteq \mathbb{Q}(\zeta_{qkr}),$$

we conclude that $f(K) = qkr$. □

Lemma 2. *The Hilbert class field of* K *over* $\mathbb{Q}$ *is* $H = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$.

Proof. Since $[H : K] = 2$ and K has class number 2 by hypothesis, it is sufficient to show that H/K is an unramified extension. Indeed, since $q, k, r \equiv 1 \pmod 4$, the conductors of $\mathbb{Q}(\sqrt{q})$, $\mathbb{Q}(\sqrt{k})$, $\mathbb{Q}(\sqrt{r})$ are q, k, and r, respectively. Then, as in Lemma 1,

$$\mathbb{Q}(\zeta_q), \mathbb{Q}(\zeta_k), \mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_{f(H)})$$

so that q, k, and r each divides $f(H)$. Hence, since

$$H \subseteq \mathbb{Q}(\sqrt{q})\mathbb{Q}(\sqrt{k})\mathbb{Q}(\sqrt{r}) \subseteq \mathbb{Q}(\zeta_q)\mathbb{Q}(\zeta_k)\mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_{qkr}),$$

we again conclude that $f(H) = qkr$. Therefore, only prime ideals lying over (q), (k), or (r) can ramify in H/K, and we now show that the ramification index of each of these prime ideals is 2 in both $H/\mathbb{Q}$ and $K/\mathbb{Q}$.

Let $F = \mathbb{Q}(\sqrt{k \cdot r})$, $L = \mathbb{Q}(\sqrt{k}, \sqrt{r})$, and suppose that $\mathfrak{q}$, $\mathfrak{Q}$, $\mathfrak{b}$ and $\mathfrak{B}$ lie over (q) in $K/\mathbb{Q}$, $H/\mathbb{Q}$, $F/\mathbb{Q}$, and $L/\mathbb{Q}$, respectively. Since q does not divide k or r, the prime ideal (q) does not ramify in $\mathbb{Q}(\sqrt{k})$ or $\mathbb{Q}(\sqrt{r})$, and hence, since $L = \mathbb{Q}(\sqrt{k})\mathbb{Q}(\sqrt{r})$, we have $e(\mathfrak{B}/q) = 1$. But, since q divides $f(H)$, (q) must ramify in $H/\mathbb{Q}$ so that

$$1 < e(\mathfrak{Q}/q) = e(\mathfrak{Q}/\mathfrak{B}) \cdot e(\mathfrak{B}/q) \leq 2 \cdot 1 \Rightarrow e(\mathfrak{Q}/q) = 2.$$

Now, as $F = \mathbb{Q}(\sqrt{k \cdot r}) \subset L$, the prime ideal (q) also does not ramify in $\mathbb{Q}(\sqrt{k \cdot r})$. But again, since q divides $f(K)$, (q) ramifies in $K/\mathbb{Q}$ so that

$$1 < e(\mathfrak{q}/q) = e(\mathfrak{q}/\mathfrak{b}) \cdot e(\mathfrak{b}/q) \leq 2 \cdot 1 \Rightarrow e(\mathfrak{q}/q) = 2.$$

Thus, since

$$2 = e(\mathfrak{Q}/q) = e(\mathfrak{Q}/\mathfrak{q}) \cdot e(\mathfrak{q}/q) = e(\mathfrak{Q}/\mathfrak{q}) \cdot 2,$$

we conclude that $e(\mathfrak{Q}/\mathfrak{q}) = 1$ so that (q) is unramified in H/K.

To see that the prime ideal (k) is unramified in H/K, we apply the same argument with $F = \mathbb{Q}(\sqrt{q})$ and $L = \mathbb{Q}(\sqrt{q}, \sqrt{r})$, and a similar modification gives that the prime ideal (r) is also unramified in H/K. Hence, since H/K is an unramified extension of degree 2, H is the Hilbert class field of K over $\mathbb{Q}$. □

We are now ready to prove the first main result of this paper:

Proof of Theorem 4. Our goal is to apply Theorem 3 to $K = \mathbb{Q}(\sqrt{q}, \sqrt{k \cdot r})$ in order to obtain the growth result necessary to apply Theorem 2. Since K is a totally real number field of degree 4, Dirichlet's unit theorem gives that we can find a set $\{e_1, e_2, e_3\}$ of multiplicatively independent elements in $\mathcal{O}_K^{\times}$. So, the hypotheses of Theorem 3 will be met if, for $\ell = \mathrm{lcm}(16, f(K)) = 16 \cdot qkr$, we can find some $u \in \mathbb{Z}$ satisfying the following conditions:

(1) $(u, \ell) = 1$;

(2) $\left(\frac{u-1}{2}, \ell\right) = 1$.

To translate the growth result given by Theorem 3 into a growth result satisfying the hypotheses of Theorem 2, we need $u \in \mathbb{Z}$ to satisfy one additional condition:

(3) For primes $\mathfrak{P}, \mathfrak{p}$ lying over any (p) such that $p \equiv u \pmod{qkr}$, we have that $\mathfrak{P}/p$ has residue degree 2 and $\mathfrak{p}/p$ has residue degree 1.

Note that the last condition ensures that $\mathfrak{P}/\mathfrak{p}$ has residue degree 2 so that by Artin reciprocity, any prime ideal $\mathfrak{p}$ satisfying Condition (3) is non-principal.

In order to find such an element $u \in \mathbb{Z}$, we first determine a set of conditions equivalent to Condition (2). Indeed, we have

$$\begin{aligned} u \text{ satisfies Condition (2)} \Leftrightarrow u &\not\equiv 1 \pmod{q}, \\ u &\not\equiv 1 \pmod{k}, \\ u &\not\equiv 1 \pmod{r}, \\ u &\not\equiv 1 \pmod{4}. \end{aligned}$$

So, consider the sets

$$\begin{aligned} A_q &= \{\text{primes } p \in \mathbb{Z} : p = 1 + nq, \ \ n \in \mathbb{Z}\}, \\ A_k &= \{\text{primes } p \in \mathbb{Z} : p = 1 + mk, \ \ m \in \mathbb{Z}\}, \\ A_r &= \{\text{primes } p \in \mathbb{Z} : p = 1 + tr, \ \ t \in \mathbb{Z}\}. \end{aligned}$$

By the prime number theorem for arithmetic progressions, the primes in the set $A = A_q \cup A_k \cup A_r$ have density bounded by

$$\frac{1}{q-1} + \frac{1}{k-1} + \frac{1}{r-1},$$

and this is strictly less than $\frac{1}{8}$ since $q, k, r \geq 29$ by hypothesis.

Next, for Condition (3), we see that

$$\text{primes } \mathfrak{P}, \mathfrak{p} \text{ lying over } (p) \text{ satisfy Condition (3)} \Leftrightarrow \left(\frac{p}{K/\mathbb{Q}}\right) = 1, \left(\frac{p}{H/\mathbb{Q}}\right) \neq 1.$$

By the Chebotarev density theorem, the density of the set

$$T_K = \left\{p \in \mathbb{Z} : \left(\frac{p}{K/\mathbb{Q}}\right) = 1\right\}$$

is $\frac{1}{4}$ while the density of the set

$$T_H = \left\{p \in \mathbb{Z} : \left(\frac{p}{H/\mathbb{Q}}\right) = 1\right\}$$

is $\frac{1}{8}$. So, since any prime in $T_K \backslash T_H$ satisfies Condition (3), the set of primes satisfying Condition (3) is at least $\frac{1}{8}$. Hence, we may choose a prime $s \in T_K \backslash T_H$, distinct from $2, q, k$, and r, that is not contained in A.

It remains to address the condition $u \not\equiv 1 \pmod{4}$ in Condition (2):

- If $s \not\equiv 1 \pmod{4}$, then choose $u = s$.
- If $s \equiv 1 \pmod{4}$, then choose $u = s + 2qkr$.

We now verify our choice of u satisfies the required Conditions (1)-(3):

(1) $(u, \ell) = 1$: Clearly, $2, q, k$, and r are the only primes dividing $\ell = 16 \cdot qkr$. If $u = s$, then since s is a prime distinct from $2, q, k$ and r, this condition is satisfied. If $u = s + 2qkr$, then this condition is also satisfied – if this were not the case, then either $2, q, k$ or r would divide s, a contradiction.

(2) $\left(\frac{u-1}{2}, \ell\right) = 1$: By choice, $u \not\equiv 1 \pmod 4$ so that 2 does not divide $\frac{u-1}{2}$. Since $u \equiv s \pmod{qkr}$, where $s \not\equiv 1 \pmod q$, $s \not\equiv 1 \pmod k$, and $s \not\equiv 1 \pmod r$ by choice, neither q, k, nor r divides $u - 1$ so that this condition is satisfied.

(3) As the Artin map factors through $f(H) = f(K) = qkr$, the choice of s above guarantees that primes $\mathfrak{P}, \mathfrak{p}$ lying over any prime ideal (p) such that

$$p \equiv u \equiv s \pmod{qkr}$$

will satisfy this condition. Note that this step requires that $H/\mathbb{Q}$ is abelian.

Thus, we may apply Theorem 3 with our choice of u to obtain

$$\left|\left\{\begin{array}{c|c} \text{prime ideals } \mathfrak{p} & \mathrm{Nm}(\mathfrak{p}) \equiv u \pmod{\ell}, \\ \text{of first degree} & \mathrm{Nm}(\mathfrak{p}) \leq x, \langle -1, e_i\rangle \twoheadrightarrow (\mathcal{O}/\mathfrak{p})^\times \end{array}\right\}\right| \gg \frac{x}{\log^2 x}$$

so that since $\mathcal{O}_K^\times \twoheadrightarrow \langle -1, e_i\rangle$ for any $e_i \in \mathcal{O}_K^\times$, this implies

$$\left|\left\{\begin{array}{c|c} \text{prime ideals } \mathfrak{p} & \mathrm{Nm}(\mathfrak{p}) \equiv u \pmod{\ell}, \\ \text{of first degree} & \mathrm{Nm}(\mathfrak{p}) \leq x, \mathcal{O}_K^\times \twoheadrightarrow (\mathcal{O}/\mathfrak{p})^\times \end{array}\right\}\right| \gg \frac{x}{\log^2 x}.$$

By Condition (3), each of these primes is non-principal, and hence, if $\mathrm{Cl}_K = \langle [C]\rangle$,

$$\left|\left\{\begin{array}{c|c} \text{prime ideals} & \\ \mathfrak{p} \subset \mathcal{O}_K & \mathrm{Nm}(\mathfrak{p}) \leq x,\ [\mathfrak{p}] = [C],\ \mathcal{O}_K^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p})^\times \end{array}\right\}\right| \gg \frac{x}{\log^2 x}.$$

Hence, by Theorem 2, C is a Euclidean ideal. □

2.2. **Main Result in the Cyclic Case.** We will now assume that K is a number field satisfying the conditions given in Theorem 5, i.e., $h_K = 2$ and

$$K = \mathbb{Q}\left(\sqrt{q(k + b\sqrt{k})}\right),$$

where q, $k \geq 17$ are distinct rational primes satisfying q, $k \equiv 1 \pmod 4$, $b > 0$ is an integer satisfying $b \equiv 0 \pmod 4$, and $k - b^2 > 0$ is a perfect square.

As before, in order to prove Theorem 5, we first need two lemmas which are analogous to Lemmas 1 and 2 in the biquadratic case.

Lemma 3. *The conductor $f(K)$ of K is qk.*

Proof. Since $q, k \geq 17$ are distinct rational primes satisfying q, $k \equiv 1 \pmod 4$, $b > 0$ is an integer satisfying $b \equiv 0 \pmod 4$, and $k - b^2 > 0$ is a perfect square by hypothesis, we have that $f(K) = qk$ by the main result of [13]. □

Lemma 4. *The Hilbert class field of K over $\mathbb{Q}$ is*

$$H = \mathbb{Q}\left(\sqrt{q}, \sqrt{k + b\sqrt{k}}\right).$$

Proof. Since $[H : K] = 2$ and K has class number 2 by hypothesis, it is sufficient to show that H/K is an unramified extension. Indeed, since $q \equiv 1 \pmod 4$, the conductor of $\mathbb{Q}(\sqrt{q})$ is q, and since $k \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$, the main result of [13] gives that the conductor of $\mathbb{Q}(\sqrt{k + b\sqrt{k}})$ is k. Then, as in Lemma 2,

$$\mathbb{Q}(\zeta_q), \mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\zeta_{f(H)})$$

so that q and k each divides $f(H)$. Hence, since

$$H \subseteq \mathbb{Q}(\sqrt{q})\mathbb{Q}\left(\sqrt{k+b\sqrt{k}}\right) \subseteq \mathbb{Q}(\zeta_q)\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\zeta_{qk}),$$

we conclude that $f(H) = qk$. Therefore, only prime ideals lying over (q) or (k) can ramify in H/K, and we now show that the ramification indices of the prime ideals (q) and (k) are 2 and 4, respectively, in both $H/\mathbb{Q}$ and $K/\mathbb{Q}$.

We first show that the prime ideal (q) has ramification index 2 in both $H/\mathbb{Q}$ and $K/\mathbb{Q}$. Let $F = \mathbb{Q}(\sqrt{k})$ and $L = \mathbb{Q}(\sqrt{k+b\sqrt{k}})$, and suppose that $\mathfrak{q}$, $\mathfrak{Q}$, $\mathfrak{b}$ and $\mathfrak{B}$ lie over (q) in $K/\mathbb{Q}$, $H/\mathbb{Q}$, $F/\mathbb{Q}$, and $L/\mathbb{Q}$, respectively. Since q does not divide $f(L) = k$, the prime ideal (q) does not ramify in L so that $e(\mathfrak{B}/q) = 1$. But, since q divides $f(H)$, (q) must ramify in $H/\mathbb{Q}$ so that

$$1 < e(\mathfrak{Q}/q) = e(\mathfrak{Q}/\mathfrak{B}) \cdot e(\mathfrak{B}/q) \leq 2 \cdot 1 \Rightarrow e(\mathfrak{Q}/q) = 2.$$

Now, as $F = \mathbb{Q}(\sqrt{k}) \subset K$ also has conductor k, the prime ideal (q) also does not ramify in $\mathbb{Q}(\sqrt{k})$. But again, since q divides $f(K)$, (q) ramifies in $K/\mathbb{Q}$ so that

$$1 < e(\mathfrak{q}/q) = e(\mathfrak{q}/\mathfrak{b}) \cdot e(\mathfrak{b}/q) \leq 2 \cdot 1 \Rightarrow e(\mathfrak{q}/q) = 2.$$

Thus, since

$$2 = e(\mathfrak{Q}/q) = e(\mathfrak{Q}/\mathfrak{q}) \cdot e(\mathfrak{q}/q) = e(\mathfrak{Q}/\mathfrak{q}) \cdot 2,$$

we conclude that $e(\mathfrak{Q}/\mathfrak{q}) = 1$ so that (q) is unramified in H/K.

It remains to show that the prime ideal (k) has ramification index 4 in both $H/\mathbb{Q}$ and $K/\mathbb{Q}$. In addition to the fields defined above, let $F' = \mathbb{Q}(\sqrt{q})$, and suppose that $\mathfrak{k}$, $\mathfrak{K}$, $\mathfrak{c}$ and $\mathfrak{c}'$ lie over (k) in $K/\mathbb{Q}$, $H/\mathbb{Q}$, $F/\mathbb{Q}$ and $F'/\mathbb{Q}$, respectively. Since k divides $f(F) = k$, we see that $e(\mathfrak{c}/k) = 2$. Moreover, we have $K = \mathbb{Q}(\alpha)$, where

$$\alpha = \sqrt{q(k+b\sqrt{k})}$$

has minimal polynomial $f(x) = x^2 - q(k+b\sqrt{k})$ over F. Since $f(x) \in \mathcal{O}_F[x]$ is an Eisenstein polynomial at the prime ideal $(\sqrt{k})$, we see that $e(\mathfrak{k}/\mathfrak{c}) = 2$, and hence,

$$e(\mathfrak{k}/k) = e(\mathfrak{k}/\mathfrak{c}) \cdot e(\mathfrak{c}/k) = 2 \cdot 2 = 4.$$

Lastly, since k does not divide $f(F') = q$, the prime ideal (k) does not ramify in F' so that $e(\mathfrak{c}'/k) = 1$. But, since $K \subset H$, we see that $e(\mathfrak{k}/k) = 4$ implies

$$4 \leq e(\mathfrak{K}/k) = e(\mathfrak{K}/\mathfrak{c}') \cdot e(\mathfrak{c}'/k) \leq 4 \cdot 1 \Rightarrow e(\mathfrak{K}/k) = 4.$$

Thus, since

$$4 = e(\mathfrak{K}/k) = e(\mathfrak{K}/\mathfrak{k}) \cdot e(\mathfrak{k}/k) = e(\mathfrak{K}/\mathfrak{k}) \cdot 4,$$

we conclude that $e(\mathfrak{K}/\mathfrak{k}) = 1$ so that (k) is unramified in H/K. Hence, since H/K is an unramified extension of degree 2, H is the Hilbert class field of K over $\mathbb{Q}$. □

Once we have these two key lemmas, the proof of Theorem 5 follows exactly as in the proof of Theorem 4. In particular, recall that to satisfy Condition (3) in this proof, the Hilbert class field of K over $\mathbb{Q}$ must be abelian over $\mathbb{Q}$; Lemma 4 implies that $\mathrm{Gal}(H/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Also, note that since $f(K)$ has only two prime divisors in the cyclic case, the density conditions which guarantee the existence of $s \in \mathbb{Z}$ in the proof of Theorem 4 will be met as long as q, $k \geq 17$.

3. Examples

We now present several new examples of number fields which satisfy the hypotheses of Theorems 4 or 5 and therefore have a Euclidean ideal. Note that the lists of examples presented in Tables 1 and 2 are not exhaustive – due to space limitations, the author included only a small selection of examples in each case.

As the conditions in Theorems 4 and 5 force the discriminant of K in both cases to be rather large, these results do not apply to any of the number fields given in the table [12] of totally real quartic number fields with class number 2 and discriminant $\leq 600,000$. However, using PARI [4], we can construct new examples of number fields to which Theorems 4 and 5 do apply.[1]

3.1. **Examples in the Biquadratic Case.** We first list all biquadratic number fields of the form $K = \mathbb{Q}(\sqrt{q}, \sqrt{k \cdot r})$, with $29 \leq q \leq 41$ and $29 \leq k, r \leq 100$, which satisfy the hypotheses of Theorem 4. When $h_K = 2$, we give explicit minimal polynomials $f(y)$, $g(x)$ of α, β, respectively, where $H = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r}) = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\beta)$. Indeed, we have

$$f(y) = \left[\left(y^2 - S_1\right)^2 - 4S_2\right]^2 - 64S_3y^2,$$
$$g(x) = \left[x^2 - (q + kr)\right]^2 - 4qkr,$$

for symmetric polynomials $S_1 = q + k + r$, $S_2 = qk + qr + kr$, and $S_3 = qkr$.

With this information, we can use PARI [4] to find the integers (s, u) required to apply Theorems 2 and 3 as in the proof of Theorem 4 above.

Remark 3. Note that a straightforward application of the algorithm given by Lezowski [9] determines whether the fields in Table 1 have a norm-Euclidean ideal.

Remark 4. When $h_K > 2$ in Table 1, we should be able to modify the hypotheses of Theorem 4 in order to obtain similar results. However, it is not clear how to modify Condition (3) in the proof of Theorem 4 - this modification is necessary because when $h_K > 2$, the ideal $\mathfrak{p}$ being non-principal no longer implies that $[\mathfrak{p}] = [C]$.

Table 1: New examples of non-principal biquadratic number fields with a Euclidean ideal

(q,k,r)	h_K	Respective minimal polynomials $f(y)$, $g(x)$ of α, β such that $H = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\beta)$	(s,u)
$(29,37,41)$	2	$y^8 - 428y^6 + 38462y^4 - 1246076y^2 + 13446889$ $x^4 - 3092x^2 + 2214144$	$(13,87999)$
$(29,37,53)$	16		
$(29,37,61)$	2	$y^8 - 508y^6 + 55982y^4 - 2021356y^2 + 18207289$ $x^4 - 4572x^2 + 4963984$	$(23,23)$
$(29,37,73)$	2	$y^8 - 556y^6 + 68798y^4 - 2653948y^2 + 18003049$ $x^4 - 5460x^2 + 7139584$	$(5,156663)$
$(29,37,89)$	2	$y^8 - 620y^6 + 88574y^4 - 3778748y^2 + 14160169$ $x^4 - 6644x^2 + 10653696$	$(13,191007)$
$(29,37,97)$	4		
$(29,41,53)$	2	$y^8 - 492y^6 + 51582y^4 - 1835324y^2 + 19954089$ $x^4 - 4404x^2 + 4596736$	$(67,67)$
$(29,41,61)$	4		

Continued on next page

[1]The code used here can be found at `http://blogs.uoregon.edu/catherinehsu/research`.

Table 1 – *Continued from previous page*

(q,k,r)	h_K	Respective minimal polynomials $f(y)$, $g(x)$ of α, β such that $H=\mathbb{Q}(\alpha)$ and $K=\mathbb{Q}(\beta)$	(s,u)
$(29,41,73)$	6		
$(29,41,89)$	4		
$(29,41,97)$	2	$y^8-668y^6+103502y^4-4691276y^2+16216729$ $x^4-8012x^2+15586704$	$(7,7)$
$(29,53,61)$	2	$y^8-572y^6+70382y^4-2736044y^2+32569849$ $x^4-6524x^2+10265616$	$(23,23)$
$(29,53,73)$	2	$y^8-620y^6+83966y^4-3419324y^2+36808489$ $x^4-7796x^2+14745600$	$(5,224407)$
$(29,53,89)$	4		
$(29,53,97)$	4		
$(29,61,73)$	2	$y^8-652y^6+92702y^4-3839644y^2+46063369$ $x^4-8964x^2+19571776$	$(7,7)$
$(29,61,89)$	2	$y^8-716y^6+114014y^4-5010524y^2+50055625$ $x^4-10916x^2+29160000$	$(7,7)$
$(29,61,97)$	2	$y^8-748y^6+125822y^4-5725756y^2+49378729$ $x^4-11892x^2+34668544$	$(7,7)$
$(29,73,89)$	12		
$(29,73,97)$	2	$y^8-796y^6+141518y^4-6421708y^2+71284249$ $x^4-14220x^2+49730704$	$(5,410703)$
$(29,89,97)$	10		
$(37,29,41)$	2	$y^8-428y^6+38462y^4-1246076y^2+13446889$ $x^4-2452x^2+1327104$	$(3,3)$
$(37,29,53)$	16		
$(37,29,61)$	2	$y^8-508y^6+55982y^4-2021356y^2+18207289$ $x^4-3612x^2+2999824$	$(11,11)$
$(37,29,73)$	2	$y^8-556y^6+68798y^4-2653948y^2+18003049$ $x^4-4308x^2+4326400$	$(11,11)$
$(37,29,89)$	2	$y^8-620y^6+88574y^4-3778748y^2+14160169$ $x^4-5236x^2+6471936$	$(3,3)$
$(37,29,97)$	4		
$(37,41,53)$	4		
$(37,41,61)$	4		
$(37,41,73)$	48		
$(37,41,89)$	2	$y^8-668y^6+99662y^4-4668236y^2+35366809$ $x^4-7372x^2+13046544$	$(3,3)$
$(37,41,97)$	6		
$(37,53,61)$	2	$y^8-604y^6+77198y^4-3425932y^2+49042009$ $x^4-6540x^2+10214416$	$(67,67)$
$(37,53,73)$	4		
$(37,53,89)$	4		
$(37,53,97)$	4		
$(37,61,73)$	4		
$(37,61,89)$	2	$y^8-748y^6+121982y^4-6163516y^2+80048809$ $x^4-10932x^2+29073664$	$(7,7)$
$(37,61,97)$	2	$y^8-780y^6+134046y^4-6970396y^2+81486729$ $x^4-11908x^2+34574400$	$(7,7)$
$(37,73,89)$	8		
$(37,73,97)$	4		

Continued on next page

Table 1 – *Continued from previous page*

(q,k,r)	h_K	Respective minimal polynomials $f(y)$, $g(x)$ of α, β such that $H=\mathbb{Q}(\alpha)$ and $K=\mathbb{Q}(\beta)$	(s,u)
$(37,89,97)$	2	$y^8-892y^6+174254y^4-9443692y^2+152053561$ $x^4-17340x^2+73891216$	$(7,7)$
$(41,29,37)$	2	$y^8-428y^6+38462y^4-1246076y^2+13446889$ $x^4-2228x^2+1065024$	$(31,31)$
$(41,29,53)$	2	$y^8-492y^6+51582y^4-1835324y^2+19954089$ $x^4-3156x^2+2238016$	$(31,31)$
$(41,29,61)$	4		
$(41,29,73)$	2	$y^8-572y^6+72302y^4-2839724y^2+22534009$ $x^4-4316x^2+4309776$	$(31,31)$
$(41,29,89)$	4		
$(41,29,97)$	2	$y^8-668y^6+103502y^4-4691276y^2+16216729$ $x^4-5708x^2+7683984$	$(37,230703)$
$(41,37,53)$	4		
$(41,37,61)$	4		
$(41,37,73)$	16		
$(41,37,89)$	2	$y^8-668y^6+99662y^4-4668236y^2+35366809$ $x^4-6668x^2+10575504$	$(23,23)$
$(41,37,97)$	6		
$(41,53,61)$	4		
$(41,53,73)$	2	$y^8-668y^6+95054y^4-4640588y^2+68079001$ $x^4-7820x^2+14653584$	$(5,317263)$
$(41,53,89)$	6		
$(41,53,97)$	2	$y^8-764y^6+128558y^4-6856172y^2+75394489$ $x^4-10364x^2+26010000$	$(5,421567)$
$(41,61,73)$	8		
$(41,61,89)$	4		
$(41,61,97)$	4		
$(41,73,89)$	8		
$(41,73,97)$	4		
$(41,89,97)$	2	$y^8-908y^6+179102y^4-10388636y^2+182439049$ $x^4-17348x^2+73822464$	$(23,23)$

3.2. **Examples in the Cyclic Case.** Now we list all cyclic number fields

$$K=\mathbb{Q}\left(\sqrt{q(k+b\sqrt{k})}\right),$$

with $17\le q\le 41$, $41\le k\le 337$, and $4\le b\le 16$, which satisfy the hypotheses of Theorem 5. Again, when $h_K=2$, we give explicit minimal polynomials $f(y)$, $g(x)$ of α, β, respectively, where $H=\mathbb{Q}(\sqrt{q},\sqrt{k+b\sqrt{k}})=\mathbb{Q}(\alpha)$ and $K=\mathbb{Q}(\beta)$. Indeed, we have

$$f(y)=\left[\left(y^2-(q+\alpha_+)\right)^2-4q(\alpha_+)\right]^2\left[\left(y^2-(q+\alpha_-)\right)^2-4q(\alpha_-)\right]^2,$$
$$g(x)=x^4-2qkx^2+q^2k(k-b^2),$$

for $\alpha_+=k+b\sqrt{k}$ and $\alpha_-=k-b\sqrt{k}$.

With this information, we can use PARI [4] to find the integers (s,u) required to apply Theorems 2 and 3 as in the proof of Theorem 4 above.

Table 2: New examples of non-principal cyclic number fields with a Euclidean ideal

(q,k,b)	h_K	Respective minimal polynomials $f(y)$, $g(x)$ of α, β such that $H=\mathbb{Q}(\alpha)$ and $K=\mathbb{Q}(\beta)$	(s,u)
$(17,41,4)$	2	$y^8-232y^6+13296y^4-159872y^2+6400$ $x^4-1394x^2+296225$	$(5,1399)$
$(17,97,4)$	2	$y^8-456y^6+61680y^4-2632832y^2+23503104$ $x^4-3298x^2+2270673$	$(3,3)$
$(17,73,8)$	2	$y^8-360y^6+29328y^4-717824y^2+2359296$ $x^4-2482x^2+189873$	$(3,3)$
$(17,89,8)$	26		
$(17,113,8)$	2	$y^8-520y^6+71568y^4-2998784y^2+3936256$ $x^4-3842x^2+1600193$	$(11,11)$
$(17,193,12)$	2	$y^8-840y^6+182768y^4-10233984y^2+10137856$ $x^4-6562x^2+2733073$	$(23,23)$
$(17,257,16)$	6		
$(17,281,16)$	4		
$(17,337,16)$	2	$y^8-1416y^6+533520y^4-46303232y^2+260112384$ $x^4-11458x^2+7888833$	$(3,3)$
$(29,17,4)$	2	$y^8-184y^6+8208y^4-102656y^2+16384$ $x^4-986x^2+14297$	$(19,19)$
$(29,41,4)$	2	$y^8-280y^6+18576y^4-161024y^2+262144$ $x^4-2378x^2+862025$	$(43,43)$
$(29,97,4)$	2	$y^8-504y^6+69648y^4-2268416y^2+9437184$ $x^4-5626x^2+6607737$	$(3,3)$
$(29,73,8)$	2	$y^8-408y^6+36144y^4-1051520y^2+7485696$ $x^4-4234x^2+552537$	$(3,3)$
$(29,89,8)$	2	$y^8-472y^6+51504y^4-1653632y^2+4393216$ $x^4-5162x^2+1871225$	$(17,5179)$
$(29,113,8)$	2	$y^8-568y^6+80304y^4-3255680y^2+30976$ $x^4-6554x^2+4656617$	$(11,11)$
$(29,193,12)$	2	$y^8-888y^6+195344y^4-12099840y^2+802816$ $x^4-11194x^2+7953337$	$(31,31)$
$(29,257,16)$	6		
$(29,281,16)$	4		
$(29,337,16)$	10		
$(37,17,4)$	10		
$(37,41,4)$	2	$y^8-312y^6+23056y^4-188672y^2+409600$ $x^4-3034x^2+1403225$	$(5,3039)$
$(37,97,4)$	2	$y^8-536y^6+75920y^4-2016512y^2+4194304$ $x^4-7178x^2+10756233$	$(31,31)$
$(37,73,8)$	2	$y^8-440y^6+41648y^4-1280384y^2+11397376$ $x^4-5402x^2+899433$	$(19,19)$
$(37,89,8)$	2	$y^8-504y^6+57520y^4-1864064y^2+8952064$ $x^4-6586x^2+3046025$	$(5,6591)$
$(37,113,8)$	2	$y^8-600y^6+87088y^4-3407744y^2+2119936$ $x^4-8362x^2+7580153$	$(13,8375)$
$(37,193,12)$	26		
$(37,257,16)$	6		
$(37,281,16)$	2	$y^8-1272y^6+379696y^4-26813312y^2+153760000$ $x^4-20794x^2+9617225$	$(5,20799)$

Continued on next page

Table 2 – *Continued from previous page*

(q,k,b)	h_K	Respective minimal polynomials $f(y)$, $g(x)$ of α, β such that $H=\mathbb{Q}(\alpha)$ and $K=\mathbb{Q}(\beta)$	(s,u)
$(37,337,16)$	2	$y^8-1496y^6+566960y^4-56650112y^2+13897984$ $x^4-24938x^2+37369593$	$(43,43)$
$(41,17,4)$	2	$y^8-232y^6+14064y^4-248960y^2+92416$ $x^4-1394x^2+28577$	$(19,19)$
$(41,97,4)$	2	$y^8-552y^6+79344y^4-1892480y^2+2509056$ $x^4-7954x^2+13207617$	$(3,3)$
$(41,73,8)$	2	$y^8-456y^6+44688y^4-1401344y^2+13307904$ $x^4-5986x^2+1104417$	$(3,3)$
$(41,89,8)$	10		
$(41,113,8)$	2	$y^8-616y^6+90768y^4-3482624y^2+4194304$ $x^4-9266x^2+9307697$	$(11,11)$
$(41,193,12)$	2	$y^8-936y^6+209648y^4-13843584y^2+21977344$ $x^4-15826x^2+15897217$	$(67,67)$
$(41,257,16)$	6		
$(41,281,16)$	2	$y^8-1288y^6+386064y^4-28725248y^2+205520896$ $x^4-23042x^2+11809025$	$(7,7)$
$(41,337,16)$	2	$y^8-1512y^6+574224y^4-58626560y^2+1806336$ $x^4-27634x^2+45886257$	$(3,3)$

References

[1] Hester Graves. $\mathbb{Q}(\sqrt{2},\sqrt{35})$ has a non-principal Euclidean ideal. *International Journal of Number Theory*, 7(08):2269–2271, 2011.

[2] Hester Graves. Growth results and Euclidean ideals. *Journal of Number Theory*, 133(8):2756–2769, 2013.

[3] Hester Graves and M Murty. A family of number fields with unit rank at least 4 that has Euclidean ideals. *Proceedings of the American Mathematical Society*, 141(9):2979–2990, 2013.

[4] The PARI Group. Pari/gp version `2.7.0`, jun 2014.

[5] M. Harper. $\mathbb{Z}[\sqrt{14}]$ is Euclidean. *Canad. J. Math.*, 56:55–70, 2004.

[6] Malcolm Harper and M Ram Murty. Euclidean rings of algebraic integers. *Canadian Journal of Mathematics*, 56(1):71–76, 2004.

[7] D.R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37:27–38, 1986.

[8] H.K. Lenstra. Euclidean ideal classes. *Astérisque*, 61:121–131, 1979.

[9] Pierre Lezowski. Examples of norm-Euclidean ideal classes. *International Journal of Number Theory*, 8(05):1315–1333, 2012.

[10] Th Motzkin. The Euclidean algorithm. *Bulletin of the American Mathematical Society*, 55(12):1142–1146, 1949.

[11] Wladyslaw Narkiewicz. Units in residue classes. *Archiv der Mathematik*, 51(3):238–241, 1988.

[12] Xavier-Francois Roblot. Table of Hilbert class field of totally real fields of degree 2,3,4, 2013.

[13] Blair K Spearman and Kenneth S Williams. The conductor of a cyclic quartic field using Gauss sums. *Czechoslovak Mathematical Journal*, 47(3):453–462, 1997.