J. Ramanujan Math. Soc. **33,** No.2 (2018) 135–147

Admissible primes and Euclidean quadratic fields

M. Ram Murty[1], Kotyada Srinivas[2] and Muthukrishnan Subramani[3]

[1] *Department of Mthematics and Statistics, Jeffery Hall, Queen's University, Kingston, Ontario, K7L 3N6, Canada*
e-mail: murty@mast.queensu.ca

[2] *Institute of Mathematical Sciences, HBNI, CIT Campus, Taramani,*
Chennai 600 113, India
e-mail: srini@imsc.res.in

[3] *Chennai Mathematical Institute, SIPCOT IT Park, Siruseri, Chennai 603 103, India*
e-mail: subramani@cmi.ac.in

Communicated by: Dr. Anupam Saikia

Received: January 31, 2017

Abstract. Let K be a real quadratic field with ring of integers $\mathcal{O}_K$. We exhibit an infinite family of real quadratic fields K, such that $\mathcal{O}_K$ contains an *admissible* set of primes with *two* elements. We then study the implications of this construction to the determination of Euclidean real quadratic fields and related questions.

2010 *Mathematics Subject Classification:* Primary 11A05; Secondary 11R04.

1. Introduction

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. The number ring $\mathcal{O}_K$ is called Euclidean with respect to a given function $\phi : \mathcal{O}_K \to \mathbb{N} \cup \{0\}$ if ϕ has the following properties

(1) $\phi(\alpha) = 0$ if and only if $\alpha = 0$, and
(2) for all $\alpha, \beta \neq 0 \in \mathcal{O}_K$ there exists a $\gamma \in \mathcal{O}_K$ such that $\phi(\alpha - \beta\gamma) < \phi(\beta)$.

In particular, if ϕ is the absolute value norm, then $\mathcal{O}_K$ is called norm-Euclidean.

It is easy to show that if $\mathcal{O}_K$ is Euclidean then $\mathcal{O}_K$ is a principal ideal domain so that its class number is one. The converse, however, is not true.

Indeed, in 1949, Motzkin [11] derived a useful criterion for any ring to be Euclidean and using it, he showed that the ring of integers of $\mathbb{Q}(\sqrt{-d})$ with $d = 19, 43, 67$ and 163 are not Euclidean, though they all have class number one. As there are only nine imaginary quadratic fields with class number one, Motzkin's paper shows that only five of these are Euclidean (and in fact, they are all norm-Euclidean). Are there any other examples of rings $\mathcal{O}_K$ with class number one which are **not** Euclidean? In 1973, Weinberger [17] showed that if we assume the generalized Riemann hypothesis (GRH), there are no more counterexamples. In other words, apart from the five imaginary quadratic fields found by Motzkin, there are no further examples of $\mathcal{O}_K$ having class number one and not being Euclidean, if we believe in the GRH! This surprising result makes one wonder how an analytic hypothesis can lead to such an algebraic result and if the use of the GRH in such questions is necessary. Such a program of research was initiated by M. Ram Murty and his school. We will describe their results below.

Determining all norm-Euclidean quadratic number fields is a classical problem that has received a lot of attention. The situation for imaginary quadratic fields has been described above. It is known that $\mathbb{Q}(\sqrt{d})$, $d > 0$ is norm-Euclidean if and only if $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Thus, we have a complete list of quadratic number fields which are Euclidean with respect to the absolute value norm. We refer the reader to [9] for a survey of these classical results.

Thus, it is an interesting question to ask whether or not a given real quadratic field is Euclidean with respect to a function different from the absolute value norm. As indicated earlier, in 1949, Motzkin [11] proved a fundamental result which gives a criterion for an integral domain to be Euclidean. His result is the following:

Let R be an integral domain. Define the sets E_k, $k \geq 0$, as follows:

Let $E_0 := \{0\}$, $E_k := \{0\} \cup \{\alpha \in R$: *each residue class mod* α *contains* $\beta \in E_{k-1}\}$, *for* $k \geq 1$. *Then,* R *is Euclidean if and only if* $\cup_{k\geq 0} E_k = R$.

As an application of Motzkin's construction, one obtains that if $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, then $\mathcal{O}_K$ is Euclidean if and only if $d = -1, -2, -3, -7, -11$, which is the classical result mentioned in the beginning. But, it seems difficult to use Motzkin's construction directly for real quadratic fields due to the presence of infinitely many units! However, with the additional assumption of the generalized Riemann hypothesis (GRH), Weinberger proved that $\mathcal{O}_K$ is Euclidean if and only if it has class number one [17] by adapting an argument of Hooley [8] used in his solution of the Artin primitive root conjecture. On the other hand, for a certain class of integers $\mathcal{O}_S$, called S-integers (defined below) Gupta, Murty and Murty [5] established that the ring of S-integers is Euclidean if and only if $\mathcal{O}_S$ is a PID without the use of the GRH. Here is a precise statement of their result.

Let S be a finite set of places of K containing the infinite places S_∞. An element x of K is called an S-integer if $ord_{\mathfrak{p}}(x) \geq 0$ for all primes $\mathfrak{p}$ of K not in S. Let $\mathcal{O}_S$ denote the ring of S-integers. Let $g := gcd \ \{N_{K/\mathbb{Q}}(\mathfrak{p}) - 1 : \mathfrak{p} \in S - S_\infty\}$. Then

Theorem 1.1 (Gupta, Murty, Murty [5]). *Let K be Galois over $\mathbb{Q}$ such that*

(1) $|S| \geq \max\{5, 2[K : \mathbb{Q}] - 3\}$*;*
(2) *K has a real embedding or $\zeta_g \in K$.*

If $\mathcal{O}_S$ is a PID, then it is Euclidean.

Though their work initiated a method of removing GRH from these questions, it could not be applied to study the rings $\mathcal{O}_K$.

In 1995, Murty and Clark [2] developed a new criteria for the existence of a Euclidean algorithm to hold in a general number ring. In order to state their result (see Theorem 1.2), we need the concept of an *admissible* set of primes in $\mathcal{O}_K$ which we define in what follows.

Assume that $\mathcal{O}_K$ has class number one. Let $\pi_1, \ldots, \pi_s \in \mathcal{O}_K$ be distinct non-associate primes. A set of primes $\{\pi_1, \ldots, \pi_s\}$ is called an *admissible* set of primes if, for all $\beta = \pi_1^{a_1} \ldots \pi_s^{a_s}$ with a_i non-negative integers, every co-prime residue class $\pmod{\beta}$ can be represented by a unit $\varepsilon \in \mathcal{O}_K^\times$. In other words, the set $\{\pi_1, \ldots, \pi_s\}$ is *admissible* if the canonical map $\mathcal{O}_K^\times \to \left(\mathcal{O}_K/(\pi_1^{a_1} \ldots \pi_s^{a_s})\right)^\times$ is surjective.

In [2], the authors showed that it is enough to take $a_1 = a_2 = \cdots = a_s = 2$ in the above definition, (i.e,. the set $\{\pi_1, \ldots, \pi_s\}$ is *admissible* if the canonical map $\mathcal{O}_K^\times \to \left(\mathcal{O}_K/(\pi_1^2 \ldots \pi_s^2)\right)^\times$ is surjective).

Using this concept, Clark and Murty proved:

Theorem 1.2 (Murty, Clark [2]). *Let K be a totally real Galois extension with degree n_K such that $\mathcal{O}_K$ has class number one. If $\mathcal{O}_K$ has a set S of admissible primes with $m = |n_K - 4| + 1$ elements, then $\mathcal{O}_K$ is Euclidean.*

When $K/\mathbb{Q}$ is abelian, Murty and Harper obtained a more precise and useful criteria which we state below.

Theorem 1.3 (Murty, Harper [7]). *Let $K/\mathbb{Q}$ be abelian of degree n with $\mathcal{O}_K$ having class number one, that contains a set of admissible primes with s elements. Let r be the rank of the unit group. If $r + s \geq 3$, then $\mathcal{O}_K$ is Euclidean.*

There are other notable results in [7]. Specifically, Harper and Murty show that if $K/\mathbb{Q}$ is a finite Galois extension with unit rank > 3, then $\mathcal{O}_K$ is Euclidean if and only if $\mathcal{O}_K$ is a PID. This still leaves open the discussion for fields of small degree, in particular, real quadratic fields. This will be the focus of this paper.

For real quadratic fields, $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, it is therefore enough to exhibit the existence of an *admissible* set having two elements, as in this case the rank of the unit group is one. Harper [6] proved that $\mathbb{Z}[\sqrt{14}]$ is Euclidean, by exhibiting the set $\{5 - \sqrt{14}, 3 - 2\sqrt{14}\}$ as an *admissible* set of primes. Additionally, in his thesis Harper also established that all the real quadratic fields with discriminant ≤ 500 and having class number one are Euclidean. Thus, the explicit construction of admissible primes is of independent interest in its own right and it is the purpose of this paper to construct a set of admissible primes for an infinite family of real quadratic fields. It is possible that this family contains infinitely many fields with class number one and we give some reasons at the end of the paper for this belief.

In this context, two famous conjectures have some bearing on our goals. The first one concerns the Hardy-Littlewood conjecture which we state below.

Conjecture 1.4 (Hardy-Littlewood conjecture). Fix a natural number r and b coprime to r. Hardy and Littlewood conjectured that the number of primes $p \leq x$ with $p \equiv b \pmod{r}$ such that $2p + 1$ is also prime is

$$\gg \frac{x}{\log^2 x}.$$

The second conjecture we need is an estimate for the number of Wieferich primes. We call this the Wieferich primes conjecture. Though this is generally believed, we have not found a precise formulation of it in the literature so we give one here.

Conjecture 1.5 (Wieferich primes conjecture). Let ε be an element of $\mathcal{O}_K^{\times}$ of infinite order. The number of primes $p \leq x$ such that

$$\varepsilon^{p-1} \equiv 1 \quad (\text{mod} p^2)$$

is $o(x/\log^2 x)$.

Both of these conjectures are unproven though sieve theory has made some progress towards the Hardy-Littlewood conjecture. They will be relevant to our discussion below.

2. Statement of the theorems

The following result is inspired from the works in [6], [7], which we state as

Theorem 2.1. *Let L be a number field, $\mathcal{O}_L$ be its ring of integers and let $\varepsilon \in \mathcal{O}_L$ be a unit of infinite order. If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are distinct, unramified prime ideals with odd prime norms q_1 and q_2 and if*

(1) *ε has order $q_1(q_1 - 1)/2$ modulo $\mathfrak{q}_1^2$;*
(2) $q_1 \equiv 3 \pmod 4$;
(3) $gcd\big(q_1(q_1 - 1)/2,\ q_2(q_2 - 1)\big) = 1$; *and*
(4) *ε has order $q_2(q_2 - 1)$ modulo $\mathfrak{q}_2^2$;*

then $\mathcal{O}_L^\times$ maps onto $\big(\mathcal{O}_L/\mathfrak{q}_1^2\mathfrak{q}_2^2\big)^\times$.

Proof. We shall use the notation $G = \langle g\rangle$ to mean that g generates the group G.

Let

$$\beta := \varepsilon^{q_1(q_1-1)/2}.$$

By (3) and (4), it follows that

$$\langle\beta\rangle = (\mathcal{O}_L/\mathfrak{q}_2^2)^\times.$$

On the other hand by (1), we have

$$\beta \equiv 1 \pmod{\mathfrak{q}_1^2}.$$

Since β generates the group $(\mathcal{O}_L/\mathfrak{q}_2^2)^\times$ and the image of ε lies in $(\mathcal{O}_L/\mathfrak{q}_2^2)^\times$, there exists a positive integer k such that

$$(\beta^k)(-\varepsilon) \equiv 1 \pmod{\mathfrak{q}_2^2}.$$

i.e., β^k is the inverse of $-\varepsilon$ modulo $\mathfrak{q}_2^2$.

Now, let

$$\alpha := -\beta^k\varepsilon.$$

Then by the above congruence, we have

$$\alpha \equiv 1 \pmod{\mathfrak{q}_2^2}.$$

Also,

$$\alpha \equiv -\varepsilon \pmod{\mathfrak{q}_1^2}.$$

Thus by (1), α generates the group $(\mathcal{O}_L/\mathfrak{q}_1^2)$. By the Chinese remainder theorem

$$\big(\mathcal{O}_L/\mathfrak{q}_1^2\mathfrak{q}_2^2\big)^\times \simeq \big(\mathcal{O}_L/\mathfrak{q}_1^2\big)^\times \times \big(\mathcal{O}_L/\mathfrak{q}_2^2\big)^\times.$$

Let $(x, y) \in \big(\mathcal{O}_L/\mathfrak{q}_1^2\big)^\times \times \big(\mathcal{O}_L/\mathfrak{q}_2^2\big)^\times$. Then there exist positive integers e, f such that

$$\alpha^e \equiv x \pmod{\mathfrak{q}_1^2} \text{ and } \beta^f \equiv y \pmod{\mathfrak{q}_2^2}.$$

Now the element $z := \alpha^e\beta^f$ maps onto the element (x, y). Since (x, y) was arbitrary, the canonical map takes $\mathcal{O}_L^\times$ onto $\big(\mathcal{O}_L/\mathfrak{q}_1^2\mathfrak{q}_2^2\big)^\times$. □

In particular, we can use the previous theorem to produce admissible primes for any real quadratic field.

Theorem 2.2. *Assume the Hardy-Littlewood and the Wieferich primes conjectures. If K is a real quadratic field such that $\mathcal{O}_K$ has class number one, then $\mathcal{O}_K$ is Euclidean.*

Proof. The strategy is as follows. We want to select two primes q_1, q_2 satisfying the conditions of our previous theorem and then apply Theorem 1.3. The Hardy-Littlewood conjecture predicts that there are

$$\gg \frac{x}{\log^2 x}$$

primes such that $2q_1 + 1$ is also a prime p (say). Let ε be a fundamental unit of $\mathcal{O}_K{}^{\times}$. If we want ε to be a square mod p, we want

$$\varepsilon^{(p-1)/2} \equiv 1 \pmod{p}. \tag{2.3}$$

But this means that p splits in the quadratic field $K(\sqrt{\varepsilon})$ which is an abelian extension of $\mathbb{Q}$. By the Kronecker-Weber theorem, it is contained in a cyclotomic extension $\mathbb{Q}(\zeta_r)$ for some primitive r-th root of unity ζ_r. The condition 2.3 above is equivalent to saying that p lies in a certain arithmetic progression (mod r). By the Hardy-Littlewood conjecture, the number of primes $p \leq x$ such that $2p + 1$ is prime and p splits in $K(\sqrt{\varepsilon})$ is

$$\gg \frac{x}{\log^2 x}.$$

Let us call this set T_x and let us denote by the set S_x those primes $p \leq x$ such that $2p + 1$ is prime and ε is not a quadratic residue (mod p). This means that the primes in S_x lie in a certain arithmetic progression (mod r). Now, Hardy-Littlewood conjecture implies that S_x has $\gg \frac{x}{\log^2 x}$ primes.

By the Wieferich primes conjecture, the number of primes $p \leq x$ such that

$$\varepsilon^{p-1} \equiv 1 \pmod{p^2},$$

is $o(x/\log^2 x)$ and so, after removing these primes from T_x and S_x (if necessary), we deduce that the number of primes in each of these sets is $\gg x/\log^2 x$. These are also disjoint sets on account of the splitting and non-splitting conditions. Let $p_1 \in T_x$ and $p_2 \in S_x$ and write $q_1 = 2p_1 + 1$, $q_2 = 2p_2 + 1$. Then, clearly, $\gcd(q_1(q_1 - 1)/2, q_2(q_2 - 1)) = \gcd(q_1 p_1, q_2 p_2) = 1$ and it is easily checked that all the conditions of the theorem are satisfied. Finally, we need only apply the theorem of Harper and Murty to deduce the final conclusion. □

3. Explicit constructions

Now we give an explicit construction of admissible primes for a certain infinite family of real quadratic fields.

Fix two primes $p_1 := 11$ and $p_2 := 13$. Let

$$d := (a+1)^2b^2n^2 + 2(a+1)^2n + 23 \tag{3.1}$$

where a, b, n are integers such that

$$a \equiv 24 \pmod{p_1^3p_2^3},\ b \equiv 5 \pmod{p_1^3p_2^3}, \tag{3.2}$$

and

$$n \equiv 0 \pmod{p_1p_2}.$$

We define

$$K := \mathbb{Q}(\sqrt{d}) = \mathbb{Q}\left(\sqrt{\left((a+1)^2b^2n^2 + 2(a+1)^2n + 23\right)}\right). \tag{3.3}$$

With the above notations, we state the main theorem as follows.

Theorem 3.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be as defined above. Then there exists a set $\{\mathfrak{p}_1, \mathfrak{p}_2\}$ of two unramified prime ideals with odd prime norms p_1 and p_2 respectively such that the canonical map $\mathcal{O}_K^\times \to \left(\mathcal{O}_K/{\mathfrak{p}_1}^2{\mathfrak{p}_2}^2\right)^\times$ is surjective.*

As a consequence of Theorem (3.4) , we deduce:

Theorem 3.5. *There exists a family $C := \left\{\mathbb{Q}(\sqrt{d})\ :\ d\ is\ prime\right\}$ of real quadratic fields such that $\mathcal{O}_K$ is Euclidean if and only if it has class number one.*

Remark 1. The family C contains infinitely many elements under Buniakovsky conjecture (stated in Section 4).

Remark 2. The reason for the above choice of d is governed by the fact that in $\mathbb{Q}(\sqrt{d})$, units can be found by solving the Brahmagupta-Pell equation

$$u^2 - dv^2 = 1$$

with

$$u := u(n) = b^4(a+1)n^2 + 2b^2(a+1)n + a$$

and

$$v := v(n) = b^3n + b.$$

where a, b have to satisfy the Brahmagupta-Pell equation $x^2 - 23y^2 = 1$.

The family is motivated by a construction of Zapponi [18].

4. Proof of the theorems

Proof of Theorem 3.4. In our case, $K = \mathbb{Q}(\sqrt{d})$ with d as defined in the equation (3.1), we only need to find a unit ε and primes such that all hypotheses of Theorem 2.1 are satisfied for K. As $p_1 = 11$ and $p_2 = 13$, we see that (2) and (3) are satisfied. It is enough to check conditions (1) and (4) of Lemma 2.1.

Therefore, it remains to find a unit $\varepsilon \in \mathcal{O}_K^\times$ and show that p_1, p_2 are unramified primes in $\mathcal{O}_K$, (i.e., the primes p_1, p_2 split in $\mathcal{O}_K$). Then Lemma 4.1 (below) allows us to find an *admissible* set of primes $\{\mathfrak{p}_1, \mathfrak{p}_2\}$.

Let us set $\varepsilon := u+v\sqrt{d}$ where u and v are as defined before (see Remark 1). Since u and v satisfies the Brahmagupta-Pell equation

$$u^2 - dv^2 = 1,$$

we explicitly get a unit $\varepsilon \in \mathcal{O}_K^\times$.

We now show that the two rational primes p_1 and p_2 split in $\mathcal{O}_K$. By construction of integers d, we see that $d \equiv 23 \pmod{p_1}$. The discriminant, d_K, of the field K is congruent to 1 *or* 4 $\pmod{p_1}$. In either case d_K is a square modulo p_1. Therefore, by a standard result about splitting of primes in quadratic fields (see Theorem 25, [10]), the rational prime p_1 splits in $\mathcal{O}_K$. Similarly, d_K is congruent to 10 or 40 $\pmod{p_2}$. Thus, p_2 also splits in $\mathcal{O}_K$.

For a given unit $\rho \in \mathcal{O}_K^\times$ and an unramified prime ideal $\mathfrak{q}$, the following lemma tells us when the set $\{\mathfrak{q}\}$ is an *admissible* set.

Lemma 4.1. *Let $\rho \in \mathcal{O}_K^\times$ be a unit and $\mathfrak{q}$ be an unramified prime ideal with odd prime norm q. If ρ is a primitive root modulo $\mathfrak{q}$, and $\mathfrak{q}$ is a non-Wieferich prime to the base ρ, i.e., $\rho^{q-1} \not\equiv 1 \pmod{\mathfrak{q}^2}$, then ρ generates the group $(\mathcal{O}_K/\mathfrak{q}^2)^\times$.*

Proof. We only need to show that ρ has order $q(q-1)$ modulo $\mathfrak{q}^2$. We proceed by contradiction: suppose $\rho^l \equiv 1 \pmod{\mathfrak{q}^2}$ for some divisor l of $q-1$, then $\rho^{q-1} \equiv 1 \pmod{\mathfrak{q}^2}$, this contradicts our assumption that $\rho^{q-1} \not\equiv 1 \pmod{\mathfrak{q}^2}$.

Now, if $\rho^{ql} \equiv 1 \pmod{\mathfrak{q}^2}$ for some $l | q-1$. Then $\rho^{ql} \equiv 1 \pmod{\mathfrak{q}}$. Since ρ is a primitive root modulo $\mathfrak{q}$, we have $q-1 | ql$. This forces $l = q-1$. Hence ρ generates $(\mathcal{O}_K/\mathfrak{q}^2)^\times$. □

In order to use Lemma 4.1 in our case, we need to show that (i) ε is a primitive root modulo $\mathfrak{p}_1$, a prime ideal lying above p_1 in $\mathcal{O}_K$, and (ii) $\mathfrak{p}_1$ is a non-Wieferich prime to the base ε.

Note that

$$N(\varepsilon^2 - 1) = \varepsilon^2\bar{\varepsilon}^2 - (\varepsilon^2 + \bar{\varepsilon}^2) + 1 \equiv 2 - 2(a^2 + 23b^2) \equiv 10 \pmod{p_1}, \tag{4.2}$$

and

$$\begin{aligned} N(\varepsilon^5 - 1) &= \varepsilon^5\bar{\varepsilon}^5 - (\varepsilon^5 + \bar{\varepsilon}^5) + 1 = 2 - 2(u^5 + 10u^3v^2d + 5uv^4d^2) \\ &\equiv 2 - 2(-1) \equiv 4 \pmod{p_1}. \end{aligned} \tag{4.3}$$

The equation (4.2) and (4.3) shows that ε does not have order 2 and 5 modulo any prime ideal in $\mathcal{O}_K$ lying above p_1. Since $p_1 - 1 = 2 \times 5$, the unit ε is a primitive root modulo any prime ideal lying above p_1.

Next, to establish (ii), note that

$$N(\varepsilon^5 - 1) = (\varepsilon^5 - 1)(\bar{\varepsilon}^5 - 1) = 2 - (\varepsilon^5 + \bar{\varepsilon}^5) \equiv 367 \pmod{p_1^3},$$

and

$$\begin{aligned} N(\varepsilon^5 + 1) &= (\varepsilon^5 + 1)(\bar{\varepsilon}^5 + 1) \\ &= 2 + (\varepsilon^5 + \bar{\varepsilon}^5) = 4 - N(\varepsilon^5 - 1) \equiv 968 \pmod{p_1^3}. \end{aligned}$$

Thus,

$$N(\varepsilon^{10} - 1) = N(\varepsilon^5 + 1)N(\varepsilon^5 - 1) \equiv 1210 \not\equiv 0 \pmod{p_1^3}. \tag{4.4}$$

From (4.4), we conclude that there exists a prime ideal in $\mathcal{O}_K$ lying above p_1, say $\mathfrak{p}_1$, such that

$$\varepsilon^{10} \not\equiv 1 \pmod{\mathfrak{p}_1^2}.$$

As $p_1 - 1 = 10$, the prime ideal $\mathfrak{p}_1$ is a non-Wieferich prime with respect to the base ε. Therefore, by applying Lemma 4.1, ε has order $p_1(p_1 - 1)$ modulo $\mathfrak{p}_1^2$.

Now we shall show that ε has order $p_2(p_2 - 1)$ modulo $\mathfrak{p}_2^2$, where $\mathfrak{p}_2$ is a prime ideal lying above p_2 in $\mathcal{O}_K$. Observe that

$$N(\varepsilon^4 - 1) \equiv 2 - 2(a^4 + 138a^2b^2 + 23^2b^4) \equiv 3 \not\equiv 0 \pmod{p_2},$$

and

$$N(\varepsilon^3 - 1) \equiv 2 - 2(a^3 + 69ab^2) \equiv 2 - 2(0) \equiv 2 \not\equiv 0 \pmod{p_2}.$$

From this, we obtain

$$N(\varepsilon^3 + 1) = 4 - N(\varepsilon^3 - 1) \equiv 4 - 2 \equiv 2 \pmod{p_2}.$$

Therefore,

$$N(\varepsilon^6 - 1) = N(\varepsilon^3 - 1)N(\varepsilon^3 + 1) \equiv 4 \not\equiv 0 \pmod{p_2}.$$

This shows that ε does not have order 4 and 6 modulo any prime ideal in $\mathcal{O}_K$ lying above p_2, which means ε is a primitive root modulo any prime lying above p_2.

Again, by routine computation, we see that

$$N(\varepsilon^6 - 1) \equiv 511 \pmod{p_2^3},$$

and

$$N(\varepsilon^6 + 1) = 4 - N(\varepsilon^6 - 1) \equiv 4 - 511 \equiv 1690 \pmod{p_2^3}.$$

This gives,

$$N(\varepsilon^{12} - 1) = N(\varepsilon^6 - 1)N(\varepsilon^6 + 1) \equiv 169 \pmod{p_2^3},$$

we conclude that there exists a prime ideal, say $\mathfrak{p}_2$, lying above p_2 in $\mathcal{O}_K$ which is a non-Wieferich prime with respect to the base ε. Thus, ε has order $p_2(p_2 - 1)$ modulo $\mathfrak{p}_2^2$.
Now, we set

$$\tau := -\varepsilon,$$

and observe that

$$\tau^{\frac{p_1(p_1-1)}{2}} \equiv -1 \times \varepsilon^{\frac{p_1(p_1-1)}{2}} \equiv -1 \times -1 \equiv 1 \pmod{\mathfrak{p}_1^2}, \tag{4.5}$$

which shows that τ has order $\frac{p_1(p_1-1)}{2}$ modulo $\mathfrak{p}_1^2$.

Since $p_2 \equiv 1 \pmod 4$, the units ε and $-\varepsilon$ have the same order modulo $\mathfrak{p}_2^2$. Hence τ has order $p_2(p_2 - 1)$ modulo $\mathfrak{p}_2^2$. Therefore, conditions (1) and (4) are satisfied for the unit τ and primes $\mathfrak{p}_1, \mathfrak{p}_2$. This leads us to conclude that $\mathcal{O}_K$ contains a set of two *admissible* primes $\{\mathfrak{p}_1, \mathfrak{p}_2\}$. Thus, if $\mathcal{O}_K$ has class number one, then by Lemma 2.1, $\mathcal{O}_K$ is Euclidean.

In order to prove Theorem 3.5, we need the following propositions.

Proposition 4.6. *Let (a, b) be a solution for the Brahmagupta-Pell equation*

$$x^2 - 23y^2 = 1 \tag{4.7}$$

satisfying

$$a \equiv 24 \pmod{p_1^3 p_2^3} \quad \text{and} \quad b \equiv 5 \pmod{p_1^3 p_2^3}. \tag{4.8}$$

Then there are infinitely many square free integers d of the form

$$d = (a + 1)^2 b^2 n^2 + 2(a + 1)^2 n + 23,$$

where $n \equiv 0 \pmod{p_1 p_2}$. Further, there are infinitely many pair of solutions (a, b) of (4.7) *satisfying* (4.8).

Proof. Our main ingredient is the classical result of Ricci [15] who showed that if $f(x) \in \mathbb{Z}[X]$ is a separable quadratic polynomial with $gcd\{f(n) : n \in \mathbb{Z}\}$ a square-free integer, then there are infinitely many square-free values taken by $f(n)$ (in fact, he had shown that a positive proportion of the values are square-free). Now consider the quadratic polynomial $f(n) := (a+1)^2b^2n^2+2(a+1)^2n+23$, $n \in \mathbb{Z}$. The discriminant of this polynomial is $8(a+1)^3$, which is not zero. Therefore, $f(n)$ is a separable polynomial and the $gcd\{f(m) : m \in \mathbb{Z}\}$ is square-free. Thus, the result of Ricci implies that there are infinitely many square-free values taken by $f(n)$.

We shall now prove that there are infinitely many solutions a, b to the Brahmagupta-Pell equation (4.7) satisfying the conditions (4.8).

Note that $24 + 5\sqrt{23}$ is the fundamental unit in the ring of integers for the field $\mathbb{Q}(\sqrt{23})$, therefore $a = 24, b = 5$ is a pair satisfying (4.7) and (4.8).

Let us set

$$\mu := 24 + 5\sqrt{23},$$

and define

$$\mu^k := a_k + b_k\sqrt{23}, \quad a_k, b_k \in \mathbb{N}.$$

Observe that each pair (a_k, b_k) is a solution for the equation (4.7). A simple computation carried out in Python gives us the following:

$$a_{1210r+1} \equiv 24 \pmod{p_1^3} \text{ and } b_{1210r+1} \equiv 5 \pmod{p_1^3} \text{ for all } r \in \mathbb{N},$$

and

$$a_{2028s+1} \equiv 24 \pmod{p_2^3} \text{ and } b_{2028s+1} \equiv 5 \pmod{p_2^3} \text{ for all } s \in \mathbb{N}.$$

Thus, $a_{k+1} \equiv 24 \pmod{p_1^3p_2^3}$ and $b_{k+1} \equiv 5 \pmod{p_1^3p_2^3}$, for $k = 1210r = 2028s$, for all $r, s \in \mathbb{Z}$. This shows that there are infinitely many integer pairs (a, b) satisfying (4.7) and (4.8). □

The second proposition uses a famous conjecture of Buniakovsky [1] which we state below.

Conjecture 4.9 (Buniakovsky conjecture). If $g(x) \in \mathbb{Z}[x]$ is irreducible and $N := \gcd\{g(m) : m \in \mathbb{N}\}$ then there are infinitely many $m \in \mathbb{N}$ such that $(1/N)|g(m)|$ is prime.

Proposition 4.10. *With the same notations as in Proposition* (4.6)*, the polynomial*

$$f(n) = (a+1)^2b^2n^2 + 2(a+1)^2n + 23, n \in \mathbb{Z}$$

assumes infinitely many prime values under Buniakovsky conjecture.

Proof. Take $a = 24$ and $b = 5$, for example, then $N = 1$. Thus by Buniakovsky's conjecture, our polynomial $f(n)$ assumes infinitely many prime values. □

Proof of Theorem 3.5. From Proposition 4.6 there are infinitely many square free values taken by the polynomial $f(n)$. However, if the square-free values taken by $f(n)$ has t distinct prime factors, then 2^{t-1} divides the class number of $\mathbb{Q}(\sqrt{d})$ (see Problem 8.3.11, [4]). Thus, we need only consider the prime values of $f(n)$ if we want that the class number of $\mathbb{Q}(\sqrt{d})$ is one. Proposition 4.10, guarantees that our polynomial $f(n)$ assumes infinitely many prime values. Thus, as we vary a, b and n, we get an infinite family of real quadratic fields of the form $\mathbb{Q}(\sqrt{d})$, d prime. The proof now follows from Theorem (1.3) and Theorem (3.4). □

5. Concluding remarks

The set of quadratic fields with class number one in the family C is non-empty since $\mathbb{Q}(\sqrt{23}) \in C$. We expect there are more examples and this may be useful to investigate further numerically. For ease of exposition, we fixed the primes $p_1 = 11$ and $p_2 = 13$. In fact, the main theorem holds true for any real quadratic field K provided there exists two unramified rational primes $p_1 \equiv 3 \pmod 4$ and $p_2 \equiv 1 \pmod 4$ satisfying the following conditions:

(1) $N(\varepsilon^{p_1(p_1-1)}) \not\equiv 0 \pmod{p_1}$;
(2) $N(\varepsilon^{p_2(p_2-1)}) \not\equiv 0 \pmod{p_2}$; and
(3) $gcd\big(p_1(p_1-1)/2,\ p_2(p_2-1)\big) = 1$;

for any fixed unit $\varepsilon \in \mathcal{O}_K^\times$.

It should be possible to go further. For example, the results of this paper can be easily extended to study cubic fields which are Euclidean. In these cases, the unit rank is either 1 or 2 and so a similar dichotomy emerges. Also, the results of [7] were confined to the case that K is Galois over the rationals. This was due to a similar restriction in the work of Murty and Murty [12]. But this restriction was recently removed in a work of Murty and Peterson [13] and consequently, there is a wide scope for further progress. We relegate this research to a future paper.

The two hypotheses we assumed, namely the Hardy-Littlewood conjecture and the Wieferich primes hypothesis are both reasonable from a heuristic perspective. Indeed, the former is encouraging given the recent progress on the twin prime problem. As for the second, it is unclear at the moment. Heuristic reasoning suggests that the number of such primes less than x should not be more than $O(\log\log x)$. Our hypothesis is much weaker from this viewpoint in that we postulate the number is $o(x/\log^2 x)$. Certainly these hypotheses are far less imposing than the elusive and fugitive generalized Riemann hypothesis.

Acknowledgements

The first author was partially supported from an NSERC Discovery grant. The third author would like to express his sincere gratitude to Prof. T. R. Ramadas for encouragement and also acknowledges with thanks for financial support extended by DST through the J. C. Bose Fellowship. We thank Prof. Stéphane Louboutin for some useful conversations and Paramjit Singh for some computational advice. Finally, our sincere thanks to the referee for suggesting some useful corrections. This work constitutes a part of the PhD thesis of the third author.

References

[1] V. Buniakovsky, Sur les diviseurs numeriques invariables des fonctions rationnelles entieres, *Mem Acad. Sci. St Petersburg*, **6** (1857) 305–329.

[2] David A. Clark and M. Ram Murty, The Euclidean algorithm for Galois extensions, *Journal für die reine und angewandte Mathematik*, **459** (1995) 151–162.

[3] David S. Dummit and Richard M. Foote, Abstract Algebra, John Wiley & Sons (2004).

[4] Jody Esmonde and M. Ram Murty, Problems in Algebraic Number Theory, Graduate texts in Mathematics, Springer Science and Business Media (2005).

[5] Rajiv Gupta, M. Ram Murty and V. Kumar Murty, The Euclidean algorithm for S-integers In: Number Theory (Montreal, June 1985), *CMS Conf. Proc. 7, Amer. Math. Soc.* (1987) 189–201.

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

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

[8] C. Hooley, On Artin's conjecture, *J. Reine Agew. Math.*, **225** (1967) 209–220.

[9] Franz Lemmermeyer, The euclidean algorithm in algebraic number fields, *Exposition. Math.*, **13** (1995) no. 5, 385–416

[10] Daniel A. Marcus, Number Fields, Graduate texts in mathematics, Springer-Verlag (1977).

[11] T. Motzkin, The Euclidean algorithm, *Bull. Am. Math. Soc.*, **55** (1949) no. 12, 1142–1146.

[12] M. Ram Murty and V. Kumar Murty, A variant of the Bombieri-Vinogradov theorem, in Number Theory, *Proceedings of the 1985 Montreal Conference*, **7** (1987) 243–272.

[13] M. Ram Murty and Kathleen Petersen, A Bombieri-Vinogradov theorem for all number fields, *Transactions of the American Math. Society*, **365** (2013) no. 9, 4987–5032.

[14] T. Nagell, Zur Arithmetik der Polynome, *Abhandl. Math. Sem. Hamburg*, **1** (1922) 179–194.

[15] G. Ricci, Ricerche aritmetiche sui polinomi, *Rend. Circ. Mat. Palermo*, **57** (1933) 433–475.

[16] Pierre Samuel, About Euclidean rings, *Journal of Algebra*, Vol. 19 Issue 2 (1971) 282–301.

[17] P. J. Weinberger, On Euclidean rings of algebraic integers, *Proc. Symp. Pure Math.*, Analytic number theory, AMS, **24** (1973) 321–332 6.

[18] Leonardo Zapponi, Parametric solutions of Pell equations arXiv:1503.00637v1.