PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 9, September 2013, Pages 2979–2990
S 0002-9939(2013)11602-3
Article electronically published on May 10, 2013

A FAMILY OF NUMBER FIELDS WITH UNIT RANK AT LEAST 4 THAT HAS EUCLIDEAN IDEALS

HESTER GRAVES AND M. RAM MURTY

(Communicated by Matthew A. Papanikolas)

Abstract. We will prove that if the unit rank of a number field with cyclic class group is large enough and if the Galois group of its Hilbert class field over $\mathbb{Q}$ is abelian, then every generator of its class group is a Euclidean ideal class. We use this to prove the existence of a non-principal Euclidean ideal class that is not norm-Euclidean by showing that $\mathbb{Q}(\sqrt{5}, \sqrt{21}, \sqrt{22})$ has such an ideal class.

1. Introduction

Euclidean ideals, introduced by Lenstra, generalize Euclidean algorithms in that the existence of a Euclidean algorithm for a domain R implies that R has trivial class group, while the existence of a Euclidean ideal in a domain R implies that R has cyclic class group. If an ideal is Euclidean, then so is every other ideal in its ideal class, and therefore we say the ideal class is Euclidean. If a domain R has a Euclidean ideal class $[C]$, then $[C]$ generates the class group of R.

Lenstra showed ([9]), assuming the generalized Riemann hypothesis (henceforth abbreviated GRH), that if K is a number field with ring of integers $\mathcal{O}_K$ and class group Cl_K, and if $|\mathcal{O}_K^\times| = \infty$, then

$$\mathrm{Cl}_K = \langle [C] \rangle \text{ if and only if } [C] \text{ is a Euclidean ideal class.}$$

Using techniques used by Harper and Murty ([7], [8]), we will prove the following weaker result without assuming the GRH.

Theorem 1. *Let K be a number field, Galois over $\mathbb{Q}$, with ring of integers $\mathcal{O}_K$ and cyclic class group Cl_K. If its Hilbert class field, $H(K)$, has an abelian Galois group over $\mathbb{Q}$ and if rank$(\mathcal{O}_K^\times) \geq 4$, then*

$$\mathrm{Cl}_K = \langle [C] \rangle \textit{ if and only if } [C] \textit{ is a Euclidean ideal class.}$$

2. Euclidean ideal classes

The following is equivalent to Lenstra's definition [9] but is stated differently [4].

Definition 1. Suppose R is a Dedekind domain and that $\mathbb{I}$ is the set of its non-zero integral ideals. If C is an ideal of R, then it is called *Euclidean* if there exists a function $\psi : \mathbb{I} \longrightarrow W$, W a well-ordered set, such that for all integral ideals I and all $x \in I^{-1}C \setminus C$, there exists some $y \in C$ such that

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

Received by the editors May 27, 2011 and, in revised form, October 5, 2011 and November 16, 2011.

2010 *Mathematics Subject Classification.* Primary 11-XX, 13F07.

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

Generalizing the work of Malcolm Harper ([7]), the first author showed the following growth result ([3]).

Theorem 2. *Let K be a number field with ring of integers $\mathcal{O}_K^\times$ and cyclic class group Cl_K. Fix an ideal class $[C]$ in Cl_K. If $|\mathcal{O}_K^\times| = \infty$ and if*

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

then $[C]$ is a Euclidean ideal class.

3. Primes and Hilbert class fields

Suppose that K is a number field Galois over $\mathbb{Q}$ and that its Hilbert class field $H(K)$ has abelian Galois group over $\mathbb{Q}$. Let $f(K)$ be the conductor of K, which is also the conductor of $H(K)$, so that both fields are contained in $\mathbb{Q}(\zeta_{f(K)})$, where $\zeta_{f(K)}$ is a primitive $f(K)$-th root of unity. Note that $H(K)$ lies in $\mathbb{Q}(\zeta_{f(K)})$ because $\mathrm{Gal}(H(K)/\mathbb{Q})$ is abelian. We define d to be the smallest even number such that every root of unity in K is a d-th root of unity.

Given a prime p in $\mathbb{Q}$, we choose a prime $\mathfrak{p}$ in K that lies above p, a prime $\mathfrak{P}$ in $H(K)$ that lies above $\mathfrak{p}$, and a prime P in $\mathbb{Q}(\zeta_{f(K)})$ that lies above $\mathfrak{P}$:

$$\begin{array}{cc}
\mathbb{Q}(\zeta_{f(K)}) & P \\
| & | \\
H(K) & \mathfrak{P} \\
| & | \\
K & \mathfrak{p} \\
| & | \\
\mathbb{Q}(\zeta_d) & | \\
| & | \\
\mathbb{Q} & p
\end{array}$$

If $[C]$ generates the class group of K, then the Artin map maps all primes $\mathfrak{q}$ such that $[\mathfrak{q}] = [C]$ to a particular element σ of $\mathrm{Gal}(H(K)/K)$ because $\mathrm{Cl}_K \cong \mathrm{Gal}(H(K)/K)$. The Galois group $\mathrm{Gal}(H(K)/K)$ is isomorphic to

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{f(K)})/K)/\mathrm{Gal}(\mathbb{Q}(\zeta_{f(K)})/H(K)).$$

We can therefore identify $\mathrm{Gal}(H(K)/K)$ (and thus Cl_K) with a set of elements in $\mathrm{Gal}(\mathbb{Q}(\zeta_{f(K)})/\mathbb{Q})$, as $\mathrm{Gal}(\mathbb{Q}(\zeta_{f(K)})/K)$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{f(K)})/\mathbb{Q})$. By the isomorphism

$$\tau : \mathrm{Gal}(\mathbb{Q}(\zeta_{f(K)})/\mathbb{Q}) \to (\mathbb{Z}/f(K)\mathbb{Z})^\times,$$

we can see that there exists some $0 < a < f(K), (a, f(K)) = 1$, such that if $p \equiv a \pmod{f(K)}$, then $\mathfrak{p}$ is of first degree and $[\mathfrak{p}] = [C]$.

This, along with Theorem 2, implies that in order to prove Theorem 1, it suffices to show that

$$\left|\{\text{primes } p \le x : p \equiv a \pmod{f(K)}, \mathcal{O}_K^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p})^\times\}\right| \gg \frac{x}{\log^2 x}, \tag{1}$$

where the implied constant depends only on K. Using the linear sieve, we will show this when $\mathrm{rank}(\mathcal{O}_K^\times) \ge 4$.

4. The linear sieve

The following notation is taken from Halberstam and Richert [6]. Suppose that $\mathfrak{A}$ is a finite set of integers, that P is a collection of primes, and let $z \in \mathbb{R}, z \geq 2$. We define $S(\mathfrak{A}; P, z)$ to be the number of elements of $\mathfrak{A}$ that are not divisible by any prime p in P such that $p \leq z$. It is a generalization of $\pi(y; q, a)$, the number of primes less than or equal to y which are congruent to $a \pmod q$. In order to bound $S(\mathfrak{A}; P, z)$, we need to have a decent estimate for the size of $\mathfrak{A}$, which we denote by X.

For q square-free, we define $\mathfrak{A}_q := \{a \in \mathfrak{A} : a \equiv 0 \pmod q\}$ and we choose a function ω_0; we will be using $\frac{\omega_0(p)}{p}X$ to estimate $|\mathfrak{A}_p|$ for p prime. The definition of ω_0 is extended to all square-free q by defining $\omega_0(1) = 1$ and $\omega_0(q) = \prod_{p|q} \omega_0(p)$. In sieve theory we begin with this data, where we use approximations of the sizes of sets $\mathfrak{A}_q$ and keep track of the error terms that emanate from this calculation.

We now relate these definitions to the set of primes P. For ease of notation, we define the set of all primes not in P to be $\overline{P}$, so that $P \cap \overline{P} = \emptyset$ and $P \cup \overline{P}$ is the set of all primes. For p a prime, we define

$$\omega(p) = \begin{cases} \omega_0(p) & \text{if } p \in P, \\ 0 & \text{if } p \in \overline{P}. \end{cases}$$

For q square-free, we define $\omega(1) = 1$, $\omega(q) = \prod_{p|q} \omega(p)$, and

$$R_q := |\mathfrak{A}_q| - \frac{\omega(q)}{q} X \text{ if } \mu(q) \neq 0,$$

where μ is the Möbius function. The linear sieve can only be applied if the sets $\mathfrak{A}$ and P satisfy certain conditions, enumerated below.

Condition 1. There exists a constant $A_1 \geq 1$ such that

$$0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1}.$$

Condition 2. There exist constants L and A_2, both at least one, independent of z and w, such that if $2 \leq w \leq z$, then

$$-L \leq \sum_{w \leq p \leq z} \frac{\omega(p) \log p}{p} - \log\left(\frac{z}{w}\right) \leq A_2.$$

In order to state Condition 3, we define $(q, \overline{P}) = 1$ if every prime dividing q is in P.

Condition 3. There exists an $\alpha, 0 < \alpha \leq 1$, such that

$$\sum_{\substack{q < \frac{X^\alpha}{(\log X)^{A_4}} \\ (q, \overline{P}) = 1}} \mu^2(q) 3^{\nu(q)} |R_q| \leq A_5 \frac{X}{\log^2 X} \qquad (X \geq 2)$$

for some constants $A_4, A_5 \geq 1$.

Theorem 3 (The linear sieve lower bound). *If $\mathfrak{A}$ and P satisfy Conditions* 1, 2, *and* 3, *and if $z \leq X$, then*

$$S(\mathfrak{A}; P, z) \geq X \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)\left\{f\left(\alpha\frac{\log X}{\log z}\right) - B\frac{L}{(\log X)^{\frac{1}{14}}}\right\},$$

where B is an absolute constant and f is a classical function defined in [6]. *When $2 \leq u \leq 4$, $f(u) := \frac{2e^{\gamma}\log(u-1)}{u}$, where γ is the Euler-Mascheroni constant.*

5. Applying the linear sieve

In order to prove that (1) holds in any number field K satisfying the conditions in Theorem 1, we will show that for any given $x \in \mathbb{R}^{>0}$, $\mathfrak{A}$, P, and z satisfy Conditions 1, 2, and 3, where

$$\mathfrak{A} = \left\{\frac{p-1}{d} : p \leq x, p \equiv a \pmod{f(K)}, \left(\frac{p-1}{d}, 2f(K)\right) = 1\right\}$$

and P is the set of primes $\leq z$. The a in the definition of $\mathfrak{A}$ is chosen so that if $p \equiv a \pmod{f(K)}$, then $[\mathfrak{p}] = [C]$ and $\mathfrak{p}$ is of degree one. Note that $p \equiv 1 \pmod{d}$. Since

$$\left|\left\{\frac{p-1}{d} : p \leq x, p \equiv a \pmod{f(K)}\right\}\right| \sim \frac{\mathrm{li}(x)}{\phi(f(K))},$$

$|\mathfrak{A}| \sim \frac{C\mathrm{li}(x)}{\phi(f(K))}$ by the Eratosthenes sieve for some constant $0 < C < 1$ that depends only on $f(K)$.

If p' is a prime, $p' \leq x$, and $p' \nmid 2f(K)$, then $|\mathfrak{A}_{p'}| \sim \frac{C\mathrm{li}(x)}{\phi(f(K))\phi(p')}$, so

$$\frac{\omega_0(p')}{p'} = \frac{1}{\phi(p')}.$$

If p' is a prime, $p' \leq x$, and $p'|2f(K)$, then $|\mathfrak{A}_{p'}| = 0$, so $\frac{\omega_0(p')}{p'} = 0$. From this, we see that for all square-free q,

$$\omega(q) = \begin{cases} \frac{q}{\phi(q)} & \text{if } (q, \overline{P}) = 1, (q, 2f(K)) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1. *The sets $\mathfrak{A}$ and P satisfy Condition* 1.

Proof. Note that for $p > 2$, $\frac{\omega(p)}{p} = \frac{1}{\phi(p)}$ or 0 and

$$0 \leq \frac{1}{\phi(p)} \leq \frac{1}{2} = 1 - \frac{1}{2}.$$

As $2|2f(K)$, we can see that $0 \leq \frac{\omega(2)}{2} = 0 < 1 - \frac{1}{2}$. □

Lemma 2. *The set $\mathfrak{A}$, the set P, and the quantity z satisfy Condition* 2.

Proof. Suppose that $2 \leq w \leq z$. Then

$$\sum_{w \leq p \leq z} \frac{\omega(p)\log p}{p} = \sum_{w \leq p \leq z} \frac{\frac{p}{p-1}\log p}{p} - \sum_{w \leq p \leq z, p|2f(K)} \frac{\frac{p}{p-1}\log p}{p},$$

and as

$$\sum_{w\le p\le z, p|2f(K)} \frac{\frac{p}{p-1}\log p}{p} \le \sum_{p|2f(K)} \frac{\frac{p}{p-1}\log p}{p} = \mathcal{O}(1),$$

we know that

$$(2)\quad \sum_{w\le p\le z} \frac{\omega(p)\log p}{p} - \log\left(\frac{z}{w}\right) = \sum_{w\le p\le z} \frac{\log p}{p} + \sum_{w\le p\le z} \frac{\log p}{p(p-1)} - \log\left(\frac{z}{w}\right) - \mathcal{O}(1).$$

The sequence $\sum_{p\le x} \frac{\log p}{p(p-1)} = \mathcal{O}(1)$. By Chebyshev's Theorem (see [1], p. 6),

$$\sum_{p\le x} \frac{\log p}{p} = \log x + \mathcal{O}(1),$$

so (2) becomes

$$\log z - \log w - \log\left(\frac{z}{w}\right) + \mathcal{O}(1) = \mathcal{O}(1).$$

□

To prove that Condition 3 holds, we must first prove the following lemma.

Lemma 3. *If $c \in \mathbb{N}$, then*

$$\sum_{\substack{(q,\overline{P})=1 \\ q\le z \\ q \text{ square-free}}} \frac{c^{\nu(q)}}{q} \ll \log^c z,$$

where $\nu(q)$ is the number of distinct prime factors of q.

Proof. Note that

$$\sum_{\substack{(q,\overline{P})=1 \\ q\le z \\ q \text{ square-free}}} \frac{c^{\nu(q)}}{q} \le \prod_{p\le z}\left(1+\frac{c}{p}\right) \le \prod_{p\le z}\left(1+\frac{1}{p}\right)^c.$$

Now

$$\prod_{p\le z}\left(1+\frac{1}{p}\right) \le \prod_{p\le z}\left(\sum_{j=0}^{\infty}\frac{1}{p^j}\right) = \prod_{p\le z}\left(1-\frac{1}{p}\right)^{-1}.$$

Mertens' Theorem (see [10], p. 128) states that

$$\prod_{p\le z}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log z}\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right),$$

where γ is the Euler constant. Thus

$$\prod_{p\le z}\left(1-\frac{1}{p}\right)^{-1} = e^{\gamma}\log z\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right)^{-1}.$$

Noting that

$$\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right)^{-1} = 1+\mathcal{O}\left(\frac{1}{\log z}\right),$$

we see

$$\prod_{p\le z}\left(1-\frac{1}{p}\right)^{-1} = e^{\gamma}\log z + \mathcal{O}(1).$$

Thus

$$\prod_{p\leq z}\left(1+\frac{1}{p}\right)^{c}=\mathcal{O}(\log^{c}(z)). \qquad \square$$

Lemma 4. *The sets $\mathfrak{A}$ and P satisfy Condition* 3.

Proof. According to the Bombieri-Vinogradov inequality (see [1], p. 39), there exists some $B>1$ such that

$$\sum_{q\leq \frac{x^{\frac{1}{2}}}{\log^{B-1} x}} \max_{y\leq x}\max_{(\alpha,q)=1}\left|\pi(y;q,\alpha)-\frac{\mathrm{li}(y)}{\phi(q)}\right| \ll \frac{x}{\log^{13} x}.$$

By applying Cauchy-Schwarz (see [1], p. 27), we see that

$$\begin{aligned}\sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1}} \mu^2(q)3^{\nu(q)}|R_q| &\leq \sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1}} 3^{\nu(q)}|R_q|\\ &\leq \sqrt{\sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1}} 9^{\nu(q)}|R_q|}\ \sqrt{\sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1}} |R_q|}.\end{aligned}$$

Let us examine the first term in the product. We can see that for q square-free,

$$|R_q|\sim\left(|\mathfrak{A}_q|-\frac{C\mathrm{li}(x)}{\phi(qf(K))}\right)\ \text{if}\ (q,\overline{P})=(q,2f(K))=1$$

and

$$|R_q|=0\ \text{otherwise},$$

so

$$|R_q|\leq|\mathfrak{A}_q|+\left|\frac{C\mathrm{li}(x)}{\phi(qf(K))}\right|\leq\frac{2x}{q}.$$

Therefore

$$\sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1}} 9^{\nu(q)}|R_q|\leq 2x\sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1\\ q\ \text{square-free}}}\frac{9^{\nu(q)}}{q}\leq 2x\sum_{\substack{q\,\leq\,\frac{x^{\frac{1}{2}}}{\log^{B} x}\\ (q,\overline{P})\,=\,1\\ q\ \text{square-free}}}\frac{9^{\nu(q)}}{q}\ll 2x\log^{9} x$$

by Lemma 3.

We shall now examine the second term in the product. By definition, if $(q, 2f(K)) \neq 1$, then $|R_q| = 0$. If $(q, 2f(K)) = 1 = (q, \overline{P})$, then

$$|R_q| = \left| |\mathfrak{A}_q| - \frac{1}{\phi(q)} |\mathfrak{A}| \right|$$

$$= \left| \sum_{\substack{p \leq x \\ p \equiv a \bmod (f(K)) \\ p \equiv 1 \bmod (q) \\ \left(\frac{p-1}{d}, 2f(K)\right) = 1}} 1 - \frac{1}{\phi(q)} \sum_{\substack{p \leq x \\ p \equiv a \bmod (f(K)) \\ \left(\frac{p-1}{d}, 2f(K)\right) = 1}} 1 \right|$$

$$= \left| \sum_{\substack{p \leq x \\ p \equiv a \bmod (f(K)) \\ p \equiv 1 \bmod (q)}} \sum_{l | \left(\frac{p-1}{d}, 2f(K)\right)} \mu(l) - \frac{1}{\phi(q)} \sum_{\substack{p \leq x \\ p \equiv a \bmod (f(K))}} \sum_{l | \left(\frac{p-1}{d}, 2f(K)\right)} \mu(l) \right|$$

$$= \left| \sum_{l | 2f(K)} \mu(l) \left(\sum_{\substack{p \leq x \\ p \equiv a \bmod (f(K)) \\ p \equiv 1 \bmod (q) \\ p \equiv 1 \bmod (dl)}} 1 - \frac{1}{\phi(q)} \sum_{\substack{p \leq x \\ p \equiv a \bmod (f(K)) \\ p \equiv 1 \bmod (dl)}} 1 \right) \right|$$

$$\leq \sum_{l | 2f(K)} \left| \pi(x, q[f(K), dl], a') - \frac{1}{\phi(q)} \pi(x, [f(K), dl], a^*) \right|,$$

where a' is the smallest positive solution to $a' \equiv a \pmod{f(K)}$, $a' \equiv 1 \pmod{q}$, $a' \equiv 1 \pmod{dl}$; where a^* is the smallest positive solution to $a^* \equiv a \pmod{f(K)}$, $a^* \equiv 1 \pmod{dl}$; and where $[c_1, \cdots, c_k] = \mathrm{lcm}(c_1, \cdots, c_k)$. This means that

$$\sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q, \overline{P}) = 1}} |R_q| \leq \sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q, \overline{P}) = 1}} \left| \pi(x, q[f(K), dl], a') - \frac{\mathrm{li}(x)}{\phi(q[f(K), dl])} \right|$$
$$+ \sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q, \overline{P}) = 1}} \left| \frac{\mathrm{li}(x)}{\phi(q[f(K), dl])} - \frac{1}{\phi(q)} \pi(x, [f(K), dl], a^*) \right|.$$

Note that

$$\sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q, \overline{P}) = 1}} \left| \pi(x, q[f(K), dl], a') - \frac{\mathrm{li}(x)}{\phi(q[f(K), dl])} \right|$$

$$\leq \sum_{q \leq \frac{[f(K), dl] x^{\frac{1}{2}}}{\log^B x}} \left| \pi(x, q, a') - \frac{\mathrm{li}(x)}{\phi(q)} \right| \leq \sum_{q \leq \frac{[f(K), dl] x^{\frac{1}{2}}}{\log^B x}} \max_{(r,q)=1} \left| \pi(x, q, r) - \frac{\mathrm{li}(x)}{\phi(q)} \right|.$$

By definition, as $(q, [f(K), dl]) = 1$,

$$\frac{1}{\phi(q)}\pi(x, [f(K), dl], a^*) = \frac{1}{\phi(q)}\sum_{r=0}^{q-1}\pi(x, q[f(K), dl], a_r^*),$$

where a_r^* is the smallest positive solution to

$$t \equiv a^* \pmod{[f(K), dl]}, t \equiv r \pmod{q}.$$

The sum $\sum_{(r,q)\neq 1}\pi(x, [f(K), dl], a_r^*)$ counts all the primes less than or equal to x that are equivalent to $a^* \pmod{[f(K), dl]}$ and $r \pmod{q}$, where r is not relatively prime to q. If $p \equiv r \pmod{q}$ and $(r, q) \neq 1$, then p must divide q. Our sum, therefore, is bounded above by $\sum_{p|q} 1 = \nu(q) \leq \frac{\log q}{\log 2}$, so

$$\frac{1}{\phi(q)}\sum_{r=0}^{q-1}\pi(x, q[f(K), dl], a_r^*) = \frac{1}{\phi(q)}\nu(q) + \frac{1}{\phi(q)}\sum_{(r,q)=1}\pi(x, q[f(K), dl], a_r^*)$$

$$= \frac{1}{\phi(q)}\sum_{(r,q)=1}\pi(x, q[f(K), dl], r) + \frac{1}{\phi(q)}\nu(q).$$

This is used to rewrite

$$\sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q,P)=1}} \left|\frac{\mathrm{li}(x)}{\phi(q[f(K), dl])} - \frac{1}{\phi(q)}\pi(x, [f(K), dl], a^*)\right|$$

as

$$\sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q,P)=1}} \left|\frac{\nu(q)}{\phi(q)} + \frac{1}{\phi(q)}\sum_{(r,q)=1}\pi(x, q[f(K), dl], r) - \frac{\mathrm{li}(x)}{\phi(q[f(K), dl])}\right|,$$

which is bounded above by

$$\sum_{\substack{q \leq \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q,P)=1}} \frac{\nu(q)}{\phi(q)} + \left|\sum_{(r,q)=1}\frac{\pi(x, q[f(K), dl], r)}{\phi(q)} - \frac{\mathrm{li}(x)}{\phi(q)\phi(q[f(K), dl])}\right|$$

$$\leq \sum_{q \leq \frac{x^{\frac{1}{2}}}{\log^B x}} \frac{\log q}{\log 2} + \max_{(r,q)=1}\left|\pi(x, q[f(K), dl], r) - \frac{\mathrm{li}(x)}{\phi(q[f(K), dl])}\right|.$$

Putting the pieces together, we see that

$$\sum_{\substack{q \le \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q,P)=1}} |R_q| \le \sum_{l|2f(K)} \left(\sum_{q \le \frac{x^{\frac{1}{2}}[f(K),dl]}{\log^B x}} 2 \max_{(r,q)=1} \left| \pi(x,q,r) - \frac{\mathrm{li}(x)}{\phi(q)} \right| + \sum_{q \le \frac{x^{\frac{1}{2}}}{\log^B x}} \frac{\log q}{\log 2} \right)$$

$$\ll \frac{x^{\frac{1}{2}}}{\log^{B-1} x} + \sum_{q \le \frac{x^{\frac{1}{2}}[f(K),dl]}{\log^B x}} \max_{(r,q)=1} \left| \pi(x,q,r) - \frac{\mathrm{li}(x)}{\phi(q)} \right|$$

$$\ll \frac{x^{\frac{1}{2}}}{\log^{B-1} x} + \sum_{q \le \frac{x^{\frac{1}{2}}}{\log^{B-1} x}} \max_{(r,q)=1} \left| \pi(x,q,r) - \frac{\mathrm{li}(x)}{\phi(q)} \right|$$

$$\ll \frac{x^{\frac{1}{2}}}{\log^{B-1} x} + \frac{x}{\log^{13} x} \ll \frac{x}{\log^{13} x}.$$

In conclusion,

$$\sum_{\substack{q \le \frac{x^{\frac{1}{2}}}{\log^B x} \\ (q,P)=1}} \mu^2(q) 3^{\nu(q)} |R_q| \ll \sqrt{2x \log^9 x} \sqrt{\frac{x}{\log^{13} x}} \ll \frac{x}{\log^2 x}. \qquad \square$$

We may now apply the linear sieve to $\mathfrak{A}$.

Lemma 5. *For any small $\epsilon > 0$, there exists a positive constant k such that if x is large enough, then*

$$S(\mathfrak{A}, P, x^{\frac{1-\epsilon}{4}}) \ge k \frac{x}{\log^2 x}.$$

Proof. By Lemmas 1, 2, and 4 we may apply the linear sieve to $\mathfrak{A}$, implying that

$$S(\mathfrak{A}, P, x^{\frac{1-\epsilon}{4}})$$

$$\ge \frac{C\mathrm{li}(x)}{\phi(f(K))} \prod_{\substack{p < x^{\frac{1-\epsilon}{4}} \\ (p,2f(K))=1}} \left(1 - \frac{1}{\phi(p)}\right) \left\{ f\left(\frac{1}{2} \frac{\log\left(\frac{Cx}{\phi(f(K))\log x}\right)}{\log x^{\frac{1-\epsilon}{4}}} \right) - \frac{BL}{(\log x)^{\frac{1}{14}}} \right\}$$

$$\gg \frac{Cx}{\phi(f(K))\log x} \prod_{\substack{p < x^{\frac{1-\epsilon}{4}} \\ (p,2f(K))=1}} \left(1 - \frac{1}{\phi(p)}\right)$$

$$\times \left\{ f\left(\frac{1}{2} \frac{\log\left(\frac{Cx}{\phi(f(K))\log x}\right)}{\log x^{\frac{1-\epsilon}{4}}} \right) - \frac{BL}{(\log x)^{\frac{1}{14}}} \right\}.$$

For $0 < \epsilon' < \epsilon$ and for x large enough,

$$\frac{1}{2}\left(\frac{\log x - \log\log x + \log\left(\frac{C}{\phi(f(K))}\right)}{\left(\frac{1-\epsilon}{4}\right)\log x}\right) \leq \frac{1}{2}\left(\frac{\log x}{\left(\frac{1-\epsilon}{4}\right)\log x}\right) = \frac{2}{1-\epsilon} < 4 \text{ and}$$

$$\frac{1}{2}\left(\frac{\log x - \log\log x + \log\left(\frac{C}{\phi(f(K))}\right)}{\left(\frac{1-\epsilon}{4}\right)\log x}\right) \geq \frac{1}{2}\left(\frac{\log x(1-\epsilon')}{\left(\frac{1-\epsilon}{4}\right)\log x}\right) = \frac{2(1-\epsilon')}{1-\epsilon} > 2,$$

so that $f\left(\frac{1}{2}\frac{\log\left(\frac{Cx}{\phi(f(K))\log x}\right)}{\log x^{\frac{1-\epsilon}{4}}}\right)$ is bounded below by a positive constant.

Thus there exist constants $C_1, C_2 > 0$ such that for large enough x,

$$S(\mathfrak{A}, P, x^{\frac{1-\epsilon}{4}}) \geq \left(C_1\frac{x}{\log x} - C_2\frac{x}{(\log x)^{\frac{15}{14}}}\right)\prod_{p \leq x^{\frac{1-\epsilon}{4}}}\left(1-\frac{1}{p}\right)$$

$$\geq \left(C_1\frac{x}{\log x} - C_2\frac{x}{(\log x)^{\frac{15}{14}}}\right)\frac{e^{-\gamma}}{\log(x^{\frac{1-\epsilon}{4}})}\left(1 + \mathcal{O}\left(\frac{1}{\log(x^{\frac{1-\epsilon}{4}})}\right)\right)$$

by Mertens' Theorem (see [10], p. 128), and so there exists some $k > 0$ such that for large enough x,

$$S(\mathfrak{A}, P, x^{\frac{1-\epsilon}{4}}) \geq k\frac{x}{\log^2 x}. \qquad \square$$

6. Proof of Theorem 1

In order to prove Theorem 1, we first need to state the following definition and the Gupta-Murty bound [5].

Definition 2. If $\mathfrak{M}$ is a monoid in $\mathcal{O}_K$ such that its elements are relatively prime to an ideal I, then we define $f_{\mathfrak{M}}(I)$ to be the size of the image of $\mathfrak{M}$ in $(\mathcal{O}_K/\mathfrak{p})^\times$. We define $f(I)$ to be $f_{\mathcal{O}_K^\times}(I)$.

Proposition 1 (The Gupta-Murty bound [5])**.** *If $\mathfrak{M}$ is a monoid in $\mathcal{O}_K^\times$ containing t multiplicatively independent elements, then*

$$|\{\mathfrak{p} : f_{\mathfrak{M}}(\mathfrak{p}) \leq x\}| \ll x^{\frac{t+1}{t}}.$$

We can now prove Theorem 1.

Proof of Theorem 1. Recall that, by Lemma 5,

$$\left|\left\{p \leq x : \begin{array}{c} p \equiv a \pmod{f(K)} \\ \left(\frac{p-1}{d}, 2f(K)\right) = 1 \\ l|\frac{p-1}{d} \Rightarrow l = 1 \text{ or } l > x^{\frac{1-\epsilon}{4}} \end{array}\right\}\right| \geq k\frac{x}{\log^2 x} \text{ for some } k > 0.$$

For the following, suppose that p is one of the primes in the above set and that $\mathfrak{p}$ lies above it in K. Since $p \equiv a \pmod{f(K)}$, $\mathrm{Nm}(\mathfrak{p}) = p$ and $f(\mathfrak{p})|(p-1)$. Note that $\mathcal{O}_K^\times \twoheadrightarrow \left(\mathcal{O}_K^\times/\mathfrak{p}\right)^\times$ if and only if $f(\mathfrak{p}) = p-1$.

As $d \nmid f(\mathfrak{p})$ if and only if $p|\mathrm{Nm}(1-\zeta_d^{r-1})$ for some r such that $(r,d) = 1$, $d \nmid f(\mathfrak{p})$ implies that $p|d$. This is a contraction as $p \equiv a \equiv 1 \pmod{d}$, so $d|f(\mathfrak{p})$, and we can see that if $l|\frac{p-1}{f(\mathfrak{p})}$, then $l = 1$ or $l > x^{\frac{1-\epsilon}{4}}$. Thus either $\frac{p-1}{f(\mathfrak{p})} = 1$ or $\frac{p-1}{f(\mathfrak{p})} > x^{\frac{1-\epsilon}{4}}$.

If $\frac{p-1}{f(\mathfrak{p})} \neq 1$, we can see that $x^{\frac{3+\epsilon}{4}} > f(\mathfrak{p})$. The Gupta-Murty bound implies that $\left|\{\mathfrak{p} : f(\mathfrak{p}) \leq x^{\frac{3+\epsilon}{4}}\}\right| \ll x^{\frac{3+\epsilon}{4}\frac{5}{4}} = x^{\frac{15+5\epsilon}{16}}$ since we assumed that $\operatorname{rank}(\mathcal{O}_K^\times) \geq 4$.

This implies that

$$\left|\left\{p \leq x : \begin{array}{c} p \equiv a \pmod{f(K)} \\ \left(\frac{p-1}{d}, 2f(K)\right) = 1 \\ f(\mathfrak{p}) = p-1 \end{array}\right\}\right| \gg \frac{x}{\log^2 x},$$

so

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

and thus $[C]$ is a Euclidean ideal class by Theorem 2. □

7. Application

When Lenstra defined Euclidean ideals, he was initially inspired by rings for which the algebraic norm of its elements is a Euclidean algorithm, leading him to define norm-Euclidean ideals [9].

Definition 3. If K is a number field and C is a fractional ideal of $\mathcal{O}_K$, then C is norm-Euclidean if for all $x \in K$, there exists some $y \in C$ such that

$$\operatorname{Nm}(x-y) < \operatorname{Nm}(C).$$

One can check that this is equivalent to $\psi = \operatorname{Nm}$ in Definition 1. If C is norm-Euclidean, then we say that $[C]$ is a norm-Euclidean ideal class. A ring can have at most one norm-Euclidean ideal class [9].

In the same paper, Lenstra showed that K has a non-principal Euclidean ideal if $K = \mathbb{Q}(\sqrt{d})$, for $d = -20, -15, 40, 60$ and 85 [9]. In each of these situations, the class number is two and the generating ideal is norm-Euclidean. These examples were found without assuming GRH [9], [2]. The only other example in the literature that does not assume GRH is $\mathbb{Q}(\sqrt{2}, \sqrt{35})$, which has class number two [4]. It is unknown whether the generating ideal is norm-Euclidean.

Proposition 2. *The field $\mathbb{Q}(\sqrt{5}, \sqrt{21}, \sqrt{22})$ has a non-principal Euclidean ideal class that is not norm-Euclidean.*

Proof. If one enters the commands

```
sage: z=sqrt(5) + sqrt(22) + sqrt(21);
sage: f=z.minpoly();
sage: L.<a>=NumberField(f,'x');
sage: C=L.class_group();C
```

into SAGE [11], then the output is

```
Class group of order 4 with structure C4 of
Number Field in a with defining polynomial
x^8 - 192*x^6 + 8408*x^4 - 70272*x^2 + 163216
```

Thus the class group of $\mathbb{Q}(\sqrt{5}, \sqrt{21}, \sqrt{22})$ is cyclic and of size four. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ is an unramified, degree four extension of $\mathbb{Q}(\sqrt{5}, \sqrt{21}, \sqrt{22})$ and is therefore its Hilbert class field.

As
$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7},\sqrt{11})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^5$$
and $\mathrm{rank}(\mathcal{O}_{\mathbb{Q}(\sqrt{5},\sqrt{21},\sqrt{22})}) = 7 > 4$, both generators of the class group of $\mathbb{Q}(\sqrt{5},\sqrt{21},\sqrt{22})$ are Euclidean ideal classes by Theorem 1. At most one generator can be norm-Euclidean, so $\mathbb{Q}(\sqrt{5},\sqrt{21},\sqrt{22})$ has a non-principal Euclidean ideal class that is not norm-Euclidean. $\square$

References

[1] Alina Carmen Cojocaru and M. Ram Murty, *An Introduction to Sieve Methods and Their Applications*, London Mathematical Society Student Texts, 66. Cambridge University Press, Cambridge, 2006. MR2200366 (2006k:11184)

[2] Hester Graves and Nick Ramsey, *Euclidean Ideals in Quadratic Imaginary Fields*, Journal of the Ramanujan Math Society, 26, no. 1, March 2011. MR2789745

[3] Hester Graves, *Growth Results and Euclidean Ideals*, submitted, arXiv:1008.2479.

[4] Hester Graves, *$\mathbb{Q}(\sqrt{2},\sqrt{35})$ has a non-principal Euclidean ideal*, Int. J. Number Theory 7, no. 8, 2269–2271, 2011. MR2873154

[5] Rajiv Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. 78, 127-130, 1984. MR762358 (86d:11003)

[6] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, New York, 1974. MR0424730 (54:12689)

[7] M. Harper, *$\mathbb{Z}[\sqrt{14}]$ is Euclidean*, Canad. J. Math. 56, 55-70, 2004. MR2031122 (2005f:11236)

[8] M. Harper and M. Ram Murty, *Euclidean rings of algebraic integers*, Canad. J. Math. 56, 71-76, 2004. MR2031123 (2005h:11261)

[9] H.K. Lenstra, *Euclidean ideal classes*, Astérisque 61, 121-131, 1979. MR556669 (81b:12005)

[10] M. Ram Murty, *Problems in Analytic Number Theory*, GTM, 206, Springer, New York, 2001. MR1803093 (2001k:11002)

[11] William Stein, *SAGE Mathematics Software* (version 4.4.4), The SAGE Group, 2010, http://www.sagemath.org/.

Department of Mathematics, Queen's University, 99 University Avenue, Kingston, Ontario, K7L 3N6, Canada
E-mail address: gravesh@mast.queensu.ca

Department of Mathematics, Queen's University, 99 University Avenue, Kingston, Ontario, K7L 3N6, Canada