THE EUCLIDEAN ALGORITHM FOR NUMBER FIELDS AND PRIMITIVE ROOTS

M. R. MURTY AND K. L. PETERSEN

1. Introduction

In 1927 Artin formulated his famous conjecture about primitive roots.

Artin's Primitive Root Conjecture. *If a is not -1 or a square then there are infinitely many primes p such that a is a primitive root modulo p.*

In fact, for an explicit constant $A(a)$ Artin conjectured that the number of primes $p \leq x$ such that a is a primitive root modulo p is $\sim A(a)x/\log x$. Assuming the generalized Riemann hypothesis (GRH), Hooley proved this conjecture in 1967. In 1983 Gupta and M. R. Murty [3] proved without any hypothesis that there are infinitely many values of a which satisfy the conjecture. This was refined by Gupta, M.R. Murty and V.K. Murty [4] and later by Heath-Brown [7]. Heath-Brown's refinement implies that the conjecture fails for at most two prime values of a. Despite this, the conjecture is not known to hold for a single value of a. A connection between a number field version of this conjecture and the Euclidean algorithm was first touched on by Samuel [15] who applied a criterion of Motzkin to quadratic fields.

An integral domain R is Euclidean if there exists a map $\phi : R - \{0\} \to \mathbb{N}$ such that given any $a, b \in R$ there exist q and r so that $a = bq + r$ with either $r = 0$ or $\phi(r) < \phi(b)$. Any such R is a principal ideal domain (PID). It is a beautiful result of Weinberger's [16] that assuming the GRH this condition is sufficient when $\mathcal{O}_K$ is the ring of integers of any number field K other than an imaginary quadratic. That is, he proved the following conjecture conditionally.

Conjecture 1.1. *If K is a number field other than an imaginary quadratic, the ring of integers $\mathcal{O}_K$ is Euclidean if and only if it is a PID.*

For an integral domain R, define the set $A_0 = \{0\}$ and inductively define the sets A_n to be the set of all $r \in R$ such that every residue class modulo r has a representative in A_m for some $m < n$. Motzkin's criterion is that R is Euclidean if and only if

$$R = \bigcup_{n=0}^{\infty} A_n.$$

The set A_1 is the unit group, $R^\times$, of R and A_2 consists of those $r \in R$ such that the unit group surjects the non-zero residue classes modulo r.

There are only nine imaginary quadratic number fields whose integer rings are PIDs. These are the integer rings of $\mathbb{Q}(\sqrt{-d})$ for

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Motzkin used this criterion to prove that of these nine imaginary quadratic fields, only for the first five is the ring of integers Euclidean, and for these the absolute value of the norm map serves as the function ϕ. We call such fields norm Euclidean. Samuel's work made the prediction that real quadratic number fields whose ring of integers are PIDs are all Euclidean (but not necessarily norm Euclidean). Weinberger's work built upon these ideas and the work of Hooley.

Harper refined Motzkin's criterion. For a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, let $\varphi_\mathfrak{p}$ be the reduction modulo $\mathfrak{p}$ map. Harper showed the following [5].

1991 *Mathematics Subject Classification.* 11A07, 11N36.

Key words and phrases. Primitive Roots, Euclidean Algorithm, Large Sieve.

Harper's Criterion. *Let B be the set of all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times) = \varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times$ and let $B(x)$ be those $\mathfrak{p} \in B$ such that $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$. If $\mathcal{O}_K$ is a PID and*

$$|B(x)| \gg \frac{x}{(\log x)^2}$$

then $\mathcal{O}_K$ is Euclidean.

Harper [5] used a more robust version of this criterion to show that $\mathbb{Z}[\sqrt{14}]$ is Euclidean. The integer ring $\mathbb{Z}[\sqrt{14}]$ was known to be a PID and known not to be norm Euclidean. Weinberger's theorem, as echoed in Harper's theorem shows a direct connection between the Euclidean condition and primitive roots. The generalization of Artin's primitive root conjecture to number fields relevant to the Euclidean algorithm problem is the following.

Conjecture 1.2. *Let K be a number field other than $\mathbb{Q}$ or an imaginary quadratic. Then there are infinitely many prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times) = \varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times$.*

Harper and M.R. Murty [6] used Harper's criterion to show that Conjecture 1.2 holds for K Galois of unit rank at least four. M.R. Murty and Petersen [11] showed that Conjecture 1.2 holds for those K, even with the additional restriction that $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv a \pmod{b}$ for any $(a, b) = 1$ if $K \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}$. This generalization has applications to hyperbolic geometry (see [14]). The main goal of this paper is to remove the Galois condition. We prove the following.

Theorem 1.3. *Let K be a number field. If the unit rank of K is at least 4 and there is a subfield $M < K$ such that K/M is Galois with group G of order at least 4, then there are $\gg x/(\log x)^2$ prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ surjects $\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times$.*

The theorem below follows immediately using Harper's criterion.

Theorem 1.4. *For K as in Theorem 1.3, $\mathcal{O}_K$ is a PID if and only if $\mathcal{O}_K$ is Euclidean.*

We show in §5 that the following corollary can be deduced from the methods used in the proof of Theorem 1.3.

Corollary 1.5. *If K is a totally real number field of degree at least five and K has a proper subfield M such that K/M is Galois, then K satisfies Conjecture 1.1 and Conjecture 1.2.*

These results do not address small degree number fields, number fields K that are not Galois over any number fields M, and small degree extensions of these fields. In the spirit of Gupta and M.R. Murty's result, Narkiewicz [13] proved that at most two real quadratic number fields fail to satisfy Conjecture 1.1. Moreover, he proved that Conjecture 1.1 fails for at most two Galois cubic extensions. Narkiewicz's results follow from his work [12] proving that Conjecture 1.2 fails for at most two real abelian number fields. He proves that if such an exceptional field exists it is cubic and there is only one exception, or there are at most two quadratic exceptions.

The main tool in the proof of Theorem 1.3 is the lower bound sieve in the form given by Iwaniec [8]. We use the generalized Riemann hypothesis on the average proven by M.R. Murty and Petersen [10] to control the error term in the sieve. The sieve allows us to find many rational primes p lying under a split prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that $p - 1$ has only necessary small divisors (e.g. 2) and very large divisors. The image $\varphi_{\mathfrak{p}}(\mathcal{O}_K)$ has order $p - 1$, and we construct a conjugacy class in which the small divisors of such $p - 1$ do not divide the index $(p-1)/\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$. Therefore, if $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ does not surject $\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times$ the index is large, so that the order of $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ is small. The remainder of the proof is a counting argument. First, in §2 we review the lower bound sieve, and apply it to our situation in §3. After that, we prove Theorem 1.3 in §4. Finally, we make some concluding remarks in §5.

2. The lower bound sieve

Let L/M be a Galois extensions of number fields with group G, and let C be a conjugacy class in G. For an unramified prime ideal $\mathfrak{p}$ of M, let $\sigma_{L/M}(\mathfrak{p})$ denote the conjugacy class of the Frobenius element. The lower bound sieve estimates the number of prime ideals $\mathfrak{p}$ in M with $\sigma_{L/M}(\mathfrak{p}) = C$. Our reference for the lower bound sieve is [2].

Let $z \geq 2$ be a real parameter, and define $\mathcal{A}$ to be a finite sequence of integers (depending on the parameter z), and $\mathcal{P}$ a sequence of rational primes. With $P(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}}} p$, define

$$S(\mathcal{A}, \mathcal{P}, z) = \{a \in \mathcal{A} : (a, P(z)) = 1\},$$

the elements of $\mathcal{A}$ all of whose prime factors which belong to $\mathcal{P}$ are all greater than z. The lower bound sieve gives a lower bound for $|S(\mathcal{A}, \mathcal{P}, z)|$.

Let Z be a quantity which approximates $|\mathcal{A}|$. For a square-free integer d define $\mathcal{A}_d = \{a \in \mathcal{A} : d|a\}$. For each rational prime $p \in \mathcal{P}$, let $\omega(p)$ be a number such that $(\omega(p)/p)Z$ approximates $|\mathcal{A}_p|$. Set $\omega(1) = 1$ and $\omega(p) = 0$ for primes $p \notin \mathcal{P}$ and extend the definition of ω to square-free integers d multiplicatively. The error of the approximation is measured by

$$R_d = |\mathcal{A}_d| - \tfrac{\omega(d)}{d} Z.$$

We define

$$W(z) = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right)$$

and the functions $F(u)$ and $f(u)$ by setting

$$F(u) = 2e^{\gamma}u^{-1} \quad \text{and} \quad f(u) = 0$$

in the range $0 < u \leq 2$ where γ is Euler's constant. For $u > 2$, F and f are solutions to the differential-difference equations

$$(uF(u))' = f(u-1) \quad \text{and} \quad (uf(u))' = F(u-1)$$

so that f is defined by $f(u) = 2e^{\gamma}u^{-1}\log(u-1)$ for $2 \leq u \leq 4$.

We now state the lower bound ('linear') sieve in the form given by Iwaniec [8].

Theorem 2.1 (Iwaniec)**.** *Assume that $0 < \omega(p) < p$ and that there is a constant $A \geq 2$ such that for all $z > w \geq 2$,*

$$\prod_{w\leq p<z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log z}{\log w}\right)\left(1 + \frac{A}{\log w}\right).$$

Then for $\xi^2 \geq z$ there is a positive B such that the lower bound

$$|S(\mathcal{A}, \mathcal{P}, z)| \geq Z\, W(z) \left\{ f\left(\frac{\log \xi^2}{\log z}\right) - \frac{B}{(\log \xi)^{\frac{1}{3}}} \right\} - \sum_{\substack{d<\xi^2 \\ d|P(z)}} |R_d|$$

holds.

3. An application of the lower bound sieve

Let K be a number field Galois over M. Define $t_K = \max\{t : \mathbb{Q}(\zeta_t) \subset K\}$ where ζ_t is a primitive t^{th} root of unity. Let η be as in Theorem 3.4 and let $\epsilon > 0$ be specified. Define the set $T(x)$ as the set of all $p < x$ where p is a rational prime lying under a split prime ideal $\mathfrak{p}$ of K with the conditions that t_K divides $p-1$ and if a rational prime ℓ divides $(p-1)/\varphi_{\mathfrak{p}}(\mathcal{O}_K^{\times})$ then $\ell > x^{\frac{1}{2\eta}-\epsilon}$. For $\mathfrak{p}$ lying over such p, the index $[\varphi_{\mathfrak{p}}(\mathcal{O}_K)^{\times} : \varphi_{\mathfrak{p}}(\mathcal{O}_K^{\times})]$ is small. We will use a counting argument to show that there are 'few' $\mathfrak{p}$ associated to such small indices. The goal of this section is to prove the following estimate for $|T(x)|$.

Proposition 3.1. *There is a positive constant D so that*

$$|T(x)| = D\frac{x}{(\log x)^2} + O\Big(\frac{x}{(\log x)^3}\Big).$$

Before employing the sieve, we require a lemma that will enable us to handle the small divisors of $p-1$. We will do so by constructing a conjugacy class in a Galois extension of M containing K. For a rational prime ℓ define the number field K_ℓ by adjoining the ℓ^{th} roots of elements of a set of representatives of $\mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times})^{\ell}$ to K. The extension of number fields K_ℓ/K is Galois. Let L be the compositum of all K_ℓ as ℓ varies over the prime divisors of t_K. The intersection of all K_ℓ for ℓ dividing t_K is K and the extension

L/K is an abelian radical extension. Therefore L/M is Galois. Let $G = \mathrm{Gal}(L/M)$ and $G_\ell = \mathrm{Gal}(K_\ell/M)$. Let $H \cong \mathrm{Gal}(L/K)$, so that with $N = \mathrm{Gal}(K/M)$ we have $G/H = N$. For each ℓ, define $H_\ell \cong \mathrm{Gal}(L/K_\ell)$ and $N_\ell \cong K_\ell/K$ so that $H/H_\ell = N_\ell$.

Lemma 3.2. *There is a conjugacy class $C \subset G$ such that if $\mathfrak{p}$ is an unramified prime ideal in M then $\sigma_\mathfrak{p}(L/M) = C$ exactly for those $\mathfrak{p}$ which are split in K and not split in any K_ℓ. Furthermore, if $A < N$ is an abelian subgroup then A lifts to an abelian subgroup of G with the property that $G \cap C \neq \emptyset$.*

Proof. A prime ideal $\mathfrak{p} \subset K$ splits completely in K_ℓ if $\sigma_\mathfrak{p}(K_\ell/K) = 1 \in N_\ell$. Since $N_\ell = H/H_\ell$ this condition lifts to the subgroup $H_\ell < H$. That is, $\mathfrak{p} \subset K$ splits completely in K_ℓ if $\sigma_\mathfrak{p}(L/K) \in H_\ell$. Therefore, to ensure that $\mathfrak{p}$ does not split completely in K_ℓ for any ℓ it is enough to require that $\sigma_\mathfrak{p}(L/K)$ is in $H - \cup H_\ell$. Such conjugacy classes exist if $H \neq H_\ell$ since H is abelian. If $H = H_\ell$ the condition is satisfied by choosing a non-identity conjugacy class.

A prime ideal $\mathfrak{p} \subset M$ splits completely in K if $\sigma_\mathfrak{p}(K/M) = 1 \in N$. This condition lifts to $H < G$. That is, $\sigma_\mathfrak{p}(L/M) \in H$ corresponds to the condition that $\mathfrak{p}$ splits completely in K. To combine the requirements, it suffices to show that there is a conjugacy class in H that is not in $\cup H_\ell$. Such a conjugacy class exists unless $H = H_\ell$ for some (necessarily the only ℓ). As mentioned above, if $H = H_\ell$ we can choose any non-identity conjugacy class of H. This is the desired conjugacy class $C \subset G$.

The final statement follows because $G/H = N$ with H abelian. □

Now we employ the lower bound sieve. Let L, K, and M be as above. Let C be the conjugacy class prescribed in Lemma 3.2. Consider the sequence $\mathcal{P}$ consisting of the rational primes which do not divide t_K, and the set

$$\mathcal{A} = \{p^n - 1 \leq x : p^n = N_{M/\mathbb{Q}}(\mathfrak{p}), \sigma_{L/M}(\mathfrak{p}) = C\}$$

with $z = x^{\frac{1}{2\eta} - \epsilon}$. Note that $|S(\mathcal{A}, \mathcal{P}, z)|$ is the set consisting of the values $p^n - 1 = N_{M/\mathbb{Q}}(\mathfrak{p}) - 1$ where $\sigma_{L/M}(\mathfrak{p}) = C$ for an unramified prime ideal $\mathfrak{p}$ of M with the additional conditions that $p^n - 1$ is not divisible by any prime up to z other than those prime divisors of t_K.

Lemma 3.3. *There is a positive constant D such that* $|S(\mathcal{A}, \mathcal{P}, z)| \geq D\dfrac{x}{(\log x)^2} + O\left(\dfrac{x}{(\log x)^3}\right)$.

Proof. In the lower bound sieve, Z is a quantity which approximates $\mathcal{A}$ and $\frac{\omega(p)}{p}Z$ approximates $\mathcal{A}_p$. By the Čebotarev density theorem $\mathcal{A} \sim \frac{|C|}{|G|} li(x)$ and $\mathcal{A}_p \sim \frac{|C|}{|G|}\frac{li(x)}{\phi(p)}$. Therefore, we wish to choose $\omega(p)$ with $\frac{\omega(p)}{p}Z \sim \frac{|C|}{|G|}\frac{li(x)}{\phi(p)}$, so that $\frac{\omega(p)}{p} \sim \frac{1}{p-1}$. We choose $Z = li(x)$ and $\omega(p) = 1$ so that

$$(*) \qquad \prod_{w \leq p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} = \prod_{w \leq p < z} \left(1 - \frac{1}{p}\right)^{-1}.$$

By Mertens' theorem (see [9] Theorem 9.1.3),

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

Using this to estimate the product in $(*)$ for $w < p < z$ as a quotient of products from $1 < p < z$ and $1 < p < w$, one can easily deduce that

$$\prod_{w \leq p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log z}{\log w}\right)\left(1 + \frac{A}{\log w}\right)$$

is satisfied since $w < z$. Therefore, the conditions of the lower bound sieve hold.

Let $\pi(x, C, d, a)$ denote the number of prime ideals $\mathfrak{p}$ in M unramified in L such that $N_{M/\mathbb{Q}}(\mathfrak{p}) \leq x$, $N_{M/\mathbb{Q}}(\mathfrak{p}) \equiv a \pmod{d}$, and $\sigma_{L/M}(\mathfrak{p}) = C$. We first estimate the main terms in the sieve. Let $|R|$ denote the error term,

$$|R| = \sum_{\substack{d < \xi^2 \\ d | P(z)}} |R_d|.$$

First, we show that the term $f(\log \xi^2/\log z) - B(\log \xi)^{-\frac{1}{3}}$ from Theorem 2.1 is bounded. Choosing $z \geq \xi^{\frac{1}{2}}$ implies that $\log \xi^2/\log z \leq 4$. (We need to satisfy $\xi^{\frac{1}{2}} \leq z < \xi$.) In the range $2 \leq u \leq 4$, $f(u) = 2e^{\gamma}u^{-1}\log(u-1)$. We have

$$f\left(\frac{\log \xi^2}{\log z}\right) = \frac{2e^{\gamma}\log z}{\log \xi^2}\log\left(\frac{\log \xi^2}{\log z} - 1\right).$$

Since $\xi > z$, we conclude that $\log \xi^2/\log z > 2$. Taking $z = x^{\frac{1}{2\eta}-\epsilon}$, the term $f(\log \xi^2/\log z) - B(\log \xi)^{-\frac{1}{3}}$ is bounded and positive.

The sieve indicates that there is a positive constant C_1 so that

$$|S(\mathcal{A}, \mathcal{P}, z)| \geq W(z)\, li(x) C_1 - |R|.$$

The prime number theorem with the estimate that $li(x) \sim x/\log x$ shows that $\pi(x) \sim x/\log x$. Since $\omega(p) = 1$, the term

$$W(z) = \prod_{p \leq z}\Big(1 - \frac{1}{p}\Big) = \frac{e^{-\gamma}}{\log z}\Big(1 + O\Big(\frac{1}{\log z}\Big)\Big)$$

using Mertens' theorem. Therefore, there is a positive constant C_2 so that $W(z) \geq C_2/\log x$. Combining these estimates, there is a positive constant C_3 such that

$$|S(\mathcal{A}, \mathcal{P}, z)| \geq C_3 \frac{x}{(\log x)^2} + |R|.$$

By definition, $|S(\mathcal{A}, \mathcal{P}, z)|$ is the number of elements in $\mathcal{A}$ relatively prime to t_K, which are not divisible by any prime up to $z = x^{\frac{1}{2\eta}-\epsilon}$.

It suffices to show that the remainder term satisfies $|R| \ll x/(\log x)^3$. We have

$$|R_d| = \Big||\mathcal{A}_d| - \frac{\omega(d)}{d}Z\Big| \ll \Big|\pi(x, C, d, 1) - \frac{|C|}{|G|}\frac{li(x)}{\phi(d)}\Big| \ll \max_{(a,d)=1}\max_{y \leq x}\Big|\pi(y, C, d, a) - \frac{|C|}{|G|}\frac{li(y)}{\phi(d)}\Big|.$$

We make the standard change of function from the prime counting function π to Chebyshev's ψ function (see [10], for example) so that

$$|R_d| \ll \max_{(a,d)=1}\max_{y \leq x}\Big|\psi(y, C, d, a) - \frac{|C|}{|G|}\frac{y}{\phi(d)}\Big|.$$

We use the following variant of the Bombieri-Vinogradov theorem for number fields [10].

Theorem 3.4 (Murty-Petersen)**.** *Let L/M be a Galois extension of number fields, and C a conjugacy class in $G = Gal(L/M)$. Let A be an abelian subgroup of G so that $A \cap C \neq \emptyset$, and let E be the fixed field of A. For every $\epsilon > 0$ and $A > 0$*

$$\sum_{d \leq x^{\frac{1}{\eta}-\epsilon}}{}' \max_{(a,d)=1}\max_{y \leq x}\left|\psi(y, C, d, a) - \frac{|C|}{|G|}\frac{y}{\phi(d)}\right| \ll \frac{x}{(\log x)^A}$$

where $\eta = \max\{[E : \mathbb{Q}] - 2, 2\}$. The decoration $'$ on the summation indicates that the restriction to those d such that $L \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.

If Artin's holomorphy conjecture is true for L/M we can replace η by $\max_{\chi}\chi(1)$ where the maximum is over irreducible characters of G.

Choosing $\xi = x^{\frac{1}{2\eta}-\epsilon} \geq z$ and $A = 3$, Theorem 3.4 implies that

$$\sum_{\substack{d \leq \xi^2 \\ d|P(z)}} |R_d| \ll \frac{x}{(\log x)^3}.$$

The error term $|R|$ only counts the terms $|R_d|$ where d is coprime to t_K. By the construction of L, there are no prime factors of t_L that are not factors of t_K. Therefore there are no d counted in $|R|$ which are not counted in Theorem 3.4. That is, the $'$ on the summation eliminates only d which are not coprime to t_L (or equivalently, t_K). In our estimate of $|R|$ we require that $d|P(z)$, and as $\mathcal{P}$ avoids those primes dividing t_K these conditions are compatible. □

We now prove Proposition 3.1, which is a stronger form of Lemma 3.3.

Proof of Proposition 3.1. We wish to reduce to the split prime case. Let $S_I(x)$ be those elements $p^n - 1 \in S(\mathcal{A}, \mathcal{P}, z)$ such that $p^n = N_{M/\mathbb{Q}}(\mathfrak{p})$ for a prime ideal $\mathfrak{p}$ in M that is not split. That is, $N_{M/\mathbb{Q}}(\mathfrak{p}) = p^n$ and $n > 1$. The number of such x, $|S_I(x)|$, is bounded by the number of prime ideals $\mathfrak{p}$ in M lying over some p such that $N_{M/\mathbb{Q}}(\mathfrak{p}) = p^n \leq x$ with $n > 1$. This is, in turn, bounded by $[M : \mathbb{Q}]$ times the number of rational prime powers $p^n \leq x$ with $n > 1$. If $p^n \leq x$, upon taking logarithms, $n \log p \leq \log x$, so $n \leq \log x$. There are at most $x^{\frac{1}{2}}$ squares of primes less than x and for each higher order power $n > 2$ there are at most $x^{\frac{1}{n}}$ associated prime powers. Therefore

$$\sum_{\substack{p^n \leq x \\ n>1}} 1 \ll x^{\frac{1}{2}} + O(x^{\frac{1}{3}} \log x) \ll x^{\frac{1}{2}}.$$

This term is absorbed in the error, so we can assume that $\mathfrak{p}$ in M lying over p is split. By construction of the conjugacy class C, if $\mathfrak{p}$ in M is counted in $S(\mathcal{A}, \mathcal{P}, z)$ and $\mathfrak{q}$ in K lies over $\mathfrak{p}$, then $\mathfrak{q}$ splits completely over $\mathbb{Q}$. As a result, we may assume that p lies under a split prime in K.

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ and $G \cong \varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times$ be the cyclic group with presentation $G = \langle g : g^{p-1} = 1 \rangle$. Let ℓ be a rational prime dividing $p - 1$. The map $\psi_\ell : G \to G$ defined by $g \mapsto g^\ell$ has kernel consisting of the ℓ^{th} roots of the identity, of which all ℓ are in G since ℓ divides the order of G. Therefore the elements of G which are ℓ^{th} roots are a subgroup, H of G of index ℓ.

If ℓ divides t_K and also divides the index $\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times / \varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ then as G is cyclic, $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times) < H$. Therefore, every element of $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ has all ℓ^{th} roots in G. By definition K_ℓ is K adjoined with the ℓ^{th} roots of a set of representatives for $(\mathcal{O}_K^\times)/(\mathcal{O}_K^\times)^\ell$. If $\mathfrak{q} \subset K_\ell$ lies over $\mathfrak{p}$ then $(\mathcal{O}_{K_\ell}/\mathfrak{q})^\times$ is generated by the ℓ^{th} roots of some elements of $(\mathcal{O}_K^\times/\mathfrak{p})$. By the above, these are all in $H < G$. Therefore $\mathfrak{q}$ must split completely.

However, by construction all prime ideals $\mathfrak{q}$ in M lying over $\mathfrak{p}$ so that $\sigma_{L/M}(\mathfrak{q}) = C$ do not split completely in $\mathcal{O}_{K_\ell}$. Restricting to primes $\mathfrak{p}$ in K lying over p which are split with $\sigma_{L/M}(\mathfrak{q}) = C$ for $\mathfrak{q}$ in M lying over $\mathfrak{p}$, we can assume that if ℓ divides t_K, then ℓ does not divide the index $[\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times : \varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)]$. Therefore, for these primes p for any $\mathfrak{p}$ in $\mathcal{O}_K$ lying over p we may assume that $\mathfrak{p}$ splits completely and that if ℓ is a prime divisor of $(p-1)/\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$, then $\ell > x^{\frac{1}{2\eta} - \epsilon}$.

□

4. Proof of the main theorem

We will use the following estimate from Gupta and M.R. Murty [3].

Lemma 4.1 (Gupta-Murty)**.** *Let S be a multiplicative set in $\mathcal{O}_K$, $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$ coprime to the elements of S, and let r denote the rank of S. Then*

$$\#\{\mathfrak{p} \subset \mathcal{O}_K : |\varphi_{\mathfrak{p}}(S)| \leq Y\} \ll Y^{\frac{r+1}{r}}.$$

Proof of Theorem 1.3. Consider $p \in T(x)$ with the prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ lying over p. If the prime ℓ divides the index of $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ in $\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times$ then $\ell > x^{\frac{1}{2\eta} - \epsilon}$ by Proposition 3.1. For these primes, the index $[\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times : \varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)]$ is either 1 or is greater than $x^{\frac{1}{2\eta} - \epsilon}$. Consequently, if the index is not one, the order of $\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)$ is less than $x^{1 - \frac{1}{2\eta} + \epsilon}$. Choosing $Y = x^{1 - \frac{1}{2\eta} + \epsilon}$ in Lemma 4.1, we see that

$$\#\{\mathfrak{p} \subset \mathcal{O}_K : |\varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)| \leq x^{1 - \frac{1}{2\eta} + \epsilon}\} \ll (x^{1 - \frac{1}{2\eta} + \epsilon})^{\frac{r+1}{r}}.$$

There are $\gg x/(\log x)^2$ primes p in $T(x)$ where the index $[\varphi_{\mathfrak{p}}(\mathcal{O}_K)^\times : \varphi_{\mathfrak{p}}(\mathcal{O}_K^\times)]$ is one when

$$O(x^{(1 - \frac{1}{2\eta} + \epsilon)\frac{r+1}{r}}) = o\left(\frac{x}{(\log x)^2}\right).$$

This occurs when $2\eta < r + 1$.

We have $M \subset K \subset K_\ell \subset L$ and a conjugacy class C in $G = \mathrm{Gal}(L/M)$. We wish to rephrase this in terms of M and K alone. Let $N = \mathrm{Gal}(K/M)$ and $A < N$ an abelian subgroup. By Lemma 3.2, A lifts to an abelian subgroup of G satisfying $A \cap C \neq \emptyset$. Therefore, the fixed field of A is the same as the fixed field

of the lift. Let E be this field. We have $\eta = \max\{n_E - 2, 2\}$ where $n_E = [E : \mathbb{Q}]$. If this maximum is 2, then the inequality is satisfied when $r > 3$. It suffices to consider the case when $\eta = n_E - 2$. Let $I = [K : E]$ so that $n_E = n_K/I$. With r_1 and r_2 being the number of real and complex places of K, so that $n_K = r_1 + 2r_2$ and $r = r_1 + r_2 - 1$, the inequality is

$$r_1\big(1 - \tfrac{2}{I}\big) + r_2\big(1 - \tfrac{4}{I}\big) > -3.$$

This is certainly satisfied when $I \geq 4$. It suffices to consider the case when $I = [K : E] \leq 3$.

With $N = \mathrm{Gal}(K/M)$, if $|N|$ has a prime divisor which is at least 5, by Sylow theory, there is an abelian subgroup $A < N$ with $|A| > 4$, and we can use the above. As a result, we need only consider the case where $|N| = 2^a 3^b$. Likewise if $a, b \geq 2$ there is an abelian subgroup of order at least 4. Therefore, it remains to deal with the cases where $|N| = 1, 2, 3$ or $|N| = 6$ is not abelian.

A non-abelian group of order 6 is necessarily dihedral, and Artin's holomorphy conjecture is known to hold for these groups. By Theorem 3.4 the inequality is satisfied in this case as well.

□

Using Harper's Criterion, Theorem 1.4 immediately follows.

5. Concluding remarks

If K is a totally real field, we can be more specific. In this case, the inequality $2\eta < r + 1$ in the proof of Theorem 1.3 reduces to $r_1(1 - \frac{2}{I}) > -3$ and is satisfied when $I > 1$. As a result, the theorem holds for all real K if $r > 3$ and there is some $M \neq K$ such that K/M is Galois. If $r = r_1 - 1 \leq 3$ the index $[K : \mathbb{Q}]$ is at most four. This is the statement of Corollary 1.5.

The authors plan to address fields of small degree in future work.

References

[1] David A. Clark and M. Ram Murty. The Euclidean algorithm for Galois extensions of **Q**. *J. Reine Angew. Math.*, 459:151–162, 1995.

[2] Alina Carmen Cojocaru and M. Ram Murty. *An introduction to sieve methods and their applications*, volume 66 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2006.

[3] Rajiv Gupta and M. Ram Murty. A remark on Artin's conjecture. *Invent. Math.*, 78(1):127–130, 1984.

[4] Rajiv Gupta, M. Ram Murty, and V. Kumar Murty. The Euclidean algorithm for S-integers. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 189–201. Amer. Math. Soc., Providence, RI, 1987.

[5] Malcolm Harper. $\mathbb{Z}[\sqrt{14}]$ is Euclidean. *Canad. J. Math.*, 56(1):55–70, 2004.

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

[7] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986.

[8] Henryk Iwaniec. Rosser's sieve. *Acta Arith.*, 36(2):171–202, 1980.

[9] M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[10] M. Ram Murty and Kathleen L. Petersen. A Bombieri-Vinogradov theorem for all number fields. *submitted for publication.*

[11] M. Ram Murty and Kathleen L. Petersen. The generalized Artin conjecture and arithmetic orbifolds. In *Groups and symmetries*, volume 47 of *CRM Proc. Lecture Notes*, pages 259–265. Amer. Math. Soc., Providence, RI, 2009.

[12] W. Narkiewicz. Units in residue classes. *Arch. Math. (Basel)*, 51(3):238–241, 1988.

[13] Władysław Narkiewicz. Euclidean algorithm in small abelian fields. *Funct. Approx. Comment. Math.*, 37(, part 2):337–340, 2007.

[14] Kathleen L. Petersen. Counting cusps of subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$. *Proc. Amer. Math. Soc.*, 136(7):2387–2393, 2008.

[15] Pierre Samuel. About Euclidean rings. *J. Algebra*, 19:282–301, 1971.

[16] Peter J. Weinberger. On Euclidean rings of algebraic integers. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 321–332. Amer. Math. Soc., Providence, R. I., 1973.

M.Ram Murty
Department of Mathematics and Statistics
Queen's University
Kingston, ON K7L 3N6, Canada
email: murty@mast.queensu.ca

Kathleen L. Petersen
Department of Mathematics
Florida State University
Tallahassee, FL 32303, USA
email: petersen@math.fsu.edu