A Multiquadratic Field Generalization of Artin’s Conjecture

M. E. Stadnik

Abstract

We prove (under the assumption of the generalized Riemann hypothesis) that a totally real multiquadratic number field $K$ has a positive density of primes $p$ in $\mathbb{Z}$ for which the image of $\mathcal{O}_K^\times$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ has minimal index $(p - 1)/2$ if and only if $K$ contains a unit of norm $-1$. An explicit formula for this density is provided. We also discuss an application to ray class fields of conductor $p\mathcal{O}_K$.

Keywords: Artin’s conjecture, Frobenius elements, multiquadratic fields

Contents

1 Introduction 2

2 Reformulation of the problem 5

2.1 Restrictions on the field $K$ ...................................... 6

2.2 Translation to $G$–representations ................................ 6

2.3 Translation to Frobenius elements ................................. 7

3 Multiquadratic fields 10

3.1 Determination of the map $\psi$ at $\ell = 2$ ...................... 10

3.2 Frobenius elements for $\ell \neq 2$ .................................. 12

4 Application of analytic number theory 13

4.1 Classical argument ................................................. 13

4.2 Bounding $N(x)$ .................................................. 15

4.3 Establishing the density formula ............................... 17

4.4 Nonvanishing of density ......................................... 20

5 Units in multiquadratic fields 22

6 Application to ray class fields 24
1. Introduction

In 1927, Emil Artin [1] conjectured that for any integer \( a \) not equal to \( \pm 1 \) or a square, there is a positive density of primes \( p \) for which \( a \) is a primitive root in \( \mathbb{F}_p^\times \). In 1967, Hooley [5] proved that this density exists and is positive if a set of generalized Riemann hypotheses (GRH) is true for particular number fields. Many authors have since adapted the analytic methods of Hooley to different settings and proved that the GRH implies a variety of interesting results. Weinberger [21] showed that if the ring of integers is a principal ideal domain, then it is a Euclidean domain for certain number fields. Cooke and Weinberger [3] proved that all \( 2 \times 2 \) matrices in the special linear group of certain rings can be expressed as a product of nine elementary matrices. Matthews [12] generalized Hooley’s argument to count the number of primes for which each element of a set of integers is a primitive root mod \( p \). Necessary and sufficient conditions for the conjectural density to be nonzero in a more general global field setting were found by Lenstra [10]. He also provided an application of his results to the existence of a Euclidean algorithm in certain arithmetic rings. In the 1980s, Murty [15] generalized Hooley’s methods to count prime ideals in any family of normal finite extension fields of a number field \( K \) and included an application to elliptic curves. His methods were generalized by Roskam [16, 17] to prove analogs of Artin’s conjecture in quadratic fields in the early 2000s. More recently, Lenstra, Stevenhagen, and Moree [11] interpreted the correction factors that arise in the density computations as character sums describing how the particular number fields are entangled and provided an application to Serre curves.

In [2], Cangelmi and Pappalardi generalized Artin’s conjecture from an integer \( a \) to a finitely generated multiplicative subgroup of \( \mathbb{Q}^\times \) and proved there is a positive density of primes \( p \) for which reducing the elements of the subgroup mod \( p \) yields the full multiplicative group of coprime residue classes mod \( p \). Roskam [16] generalized the conjecture from \( \mathbb{F}_p^\times \) to \( (\mathcal{O}_K/p\mathcal{O}_K)^\times \) for a real quadratic field \( K \) and proved there is a positive density of primes \( p \) for which the image of a fundamental unit \( \epsilon \) in \( (\mathcal{O}_K/p\mathcal{O}_K)^\times \) is maximal (or equivalently, has index as small as possible). We further generalize these results and investigate when the image of the full unit group \( \mathcal{O}_K^\times \) in \( (\mathcal{O}_K/p\mathcal{O}_K)^\times \) has index as small as possible for a positive density of primes \( p \) and prove a result for multiquadratic fields. When \( K \) is a totally real multiquadratic field that is not quadratic, \( \mathcal{O}_K^\times \) has rank greater than 1 and so there is not a single natural element to consider such as a fundamental unit. Thus we decided to formulate a generalization using the entire ring \( \mathcal{O}_K^\times \) instead of an individual element. This has the added advantage of removing the ambiguity in the density formulas based on the choice of fundamental unit \( \epsilon \) in [16].
This article deals with the following generalization of Artin’s conjecture:

**Main question:** For which number fields $K/Q$ is the index of the unit group $O_K^\times$ in $(O_K/pO_K)^\times$ precisely $(p - 1)/2$ for infinitely many primes $p$?

For any prime $p$ completely split in $K/Q$, let $\psi_p$ denote the map $O_K^\times \to (O_K/pO_K)^\times$. The image of $O_K^\times$ lies in the kernel of the norm map $N : (O_K/pO_K)^\times \to \mathbb{F}_p^\times / \{\pm 1\}$, and the smallest possible index of $\psi_p(O_K^\times)$ in $(O_K/pO_K)^\times$ is $(p - 1)/2$. We say that $K$ has **minimal index mod $p$** if this index is exactly $(p - 1)/2$. If every unit of $K$ has norm $-1$, then $\psi_p(O_K^\times)$ is contained in the kernel of the map $N : (O_K/pO_K)^\times \to \mathbb{F}_p^\times$ and the index of $\psi_p(O_K^\times)$ in $(O_K/pO_K)^\times$ is at least $p - 1$. Immediately we deduce that $K$ must contain a unit of norm $-1$ if this generalization of Artin’s conjecture is to be true. Additionally, by counting embeddings, we can deduce that $K$ must be totally real (Proposition 2.1).

To derive this generalization of Artin’s conjecture, we describe the original motivation behind the conjectural density. An integer $a \neq \pm 1$ or a square is a primitive root in $\mathbb{F}_p^\times$ if and only if for all $\ell \mid p - 1$, $a^{(p-1)/\ell} \not\equiv 1 \mod p$, or equivalently, if and only if $p$ is not split in the field extension $\mathbb{Q}(\zeta_\ell, \sqrt{a})/\mathbb{Q}$ for all $\ell \mid p - 1$, where $\zeta_\ell$ denotes a primitive $\ell$th root of unity. Thus, at first glance one expects the density $A(a)$ of primes $p$ for which $a$ is a primitive root in $\mathbb{F}_p^\times$ to be

$$A(a) = \prod_{\ell \text{ prime}} \left(1 - \frac{1}{[\mathbb{Q}(\zeta_\ell, \sqrt{a}) : \mathbb{Q}]}ight),$$

except that this formula must be modified to account for the fact that some events are not independent.

To adjust this to our setting, let $K \neq \mathbb{Q}$ denote a multiquadratic field containing a unit of norm $-1$. Let $K_\ell = K(\zeta_\ell, \sqrt{1/O_K^\times})$ if $\ell \neq 2$ is prime and let $K_2 = K(\sqrt{-1})$. In Theorem 3.5, we prove that for a prime $p \in \mathbb{Z}$ completely split in $K$, $K$ has minimal index mod $p$ if and only if for every prime $\ell \mid p - 1$, the Frobenius element $\sigma_p$ of any prime $\mathfrak{P}$ of $K(\zeta_\ell)$ lying above $p$ generates $G_\ell = \text{Gal}(K_\ell/K(\zeta_\ell))$ as a $G$–module. Since $G_\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^{n-1}$ as groups, we expect the probability that $\sigma_p$ will generate $G_\ell$ as a $G$–module is $(\ell - 1)^{n-1}$. Thus naively we expect that the density of primes $p$ completely split in $K/Q$ for which $K$ has minimal index mod $p$ is

$$\frac{1}{[K : \mathbb{Q}]} \prod_{\ell \text{ prime}} \left(1 - \frac{1}{[K(\zeta_\ell) : K]} \left(1 - \frac{(\ell - 1)^{n-1}}{\ell^{n-1}}\right)\right),$$

with some modification to account for the fact that certain events are not independent. In this article, we adapt the techniques of Hooley to prove the following theorem.
Theorem 1.1. Let $K$ be a totally real multiquadratic field with unit group $\mathcal{O}_K^\times$. The generalized Riemann hypothesis implies that there is a positive density $c$ of primes split in $K/\mathbb{Q}$ for which the image of $\mathcal{O}_K^\times$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ has index $(p-1)/2$ if and only if $K$ contains a unit of norm $-1$. Moreover, when $K$ contains a unit of norm $-1$, the density $c$ is given by

$$c = \frac{1}{2[K: \mathbb{Q}]} \left( \sum_{k \mid d_K} \frac{\mu(k)|C_k|}{|K_k : K|} \prod_{\ell \mid 2d_K} \left( 1 - \frac{1}{(\ell - 1)} \left( 1 - \frac{(\ell - 1)^n - 1}{\ell^n - 1} \right) \right) \right).$$

Here $d_K = |\text{disc}(K/\mathbb{Q})|$, $\mu$ denotes the Möbius function, $K_k = \prod_{\ell \mid k} K_\ell$, and $C_k$ is the union of conjugacy classes of $\sigma \in \text{Gal}(K_k/\mathbb{Q})$,

$$C_k = \bigcup \{ \sigma : \sigma|_K = (id), \sigma|_{\mathbb{Q}(\zeta_\ell)} = (id) \text{ and } \sigma|_{K_\ell} \text{ does not generate } G_\ell \text{ as a } G - \text{module for all } \ell \mid k \}.$$

As an example, consider the field $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$, which satisfies the hypotheses of the theorem. Using PARI, we computed the density of primes $p$ split in $K/\mathbb{Q}$ for which $K$ has minimal index mod $p$ among the first two hundred thousand primes to be 0.05176.

In this paper, we prove that the generalized Riemann hypothesis implies the density of such primes $p$ should be

$$\frac{1}{8} \prod_{\ell \neq 2} \left( 1 - \frac{1}{[K(\zeta_\ell) : K]} \left( 1 - \frac{(\ell - 1)^3}{\ell^3} \right) \right) = 0.05142184\ldots,$$

which is very close to our calculations.

We also consider the related problem of determining which multiquadratic fields contain a unit of norm $-1$.

Theorem 5.6 If $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_m})$ is a multiquadratic field of degree $n = 2^m$, $m \geq 3$ and the class number of $K$ is odd, then every unit in $K$ has norm 1.

As a main application of Theorem 1.1, we prove that the ray class field of conductor $p\mathcal{O}_K$ has the explicit construction as the smallest extension of the Hilbert class field $H$, $H(\zeta_p + \zeta_p^{-1})$ for a positive density of primes $p$ split in $K/\mathbb{Q}$ if and only if $K$ contains a unit of norm $-1$. This application is interesting because class field theory provides a non-constructive proof and an explicit description is typically unknown.

Relationship to Artin-type problems. Other Artin-type problems, such as Weinberger’s results for PIDs [21], become easier as the field degree increases. This is partly the case in our setting, because
as the field degree \( n = [K : \mathbb{Q}] \) increases, so does the rank of the unit group \( \mathcal{O}_K^\times \) since \( K \) is totally real. However, unlike some other Artin-type problems, as the field degree \( n \) increases, the condition we impose requires that the image of the unit group \( \mathcal{O}_K^\times \) generates modules with increasing cardinality. More precisely, for odd primes \( \ell | p - 1 \), we require that the image of the unit group (which has rank \( n - 1 \)) generates a vector space in \( \prod_n \left( \mathbb{F}_p^\times / (\mathbb{F}_p^\times)_{\ell} \right) \) of rank \( n - 1 \). The freedom obtained by increasing the rank is offset by the increasing constraint.

**Restriction to multiquadratic fields.** Roskam [17, pg. 309] observed that it is difficult to generalize part of his argument to non-quadratic fields. We overcome this difficulty by using representation theory to establish the required analytic bounds by using the quadratic subfields of \( K \). For such a technique to work, it is easiest to assume that \( K \) is generated by its quadratic subfields. For our representation theory arguments, we assume that the left regular action of \( G = \text{Gal}(K/\mathbb{Q}) \) on \( \mathbb{F}_\ell[G] \) (modulo the trivial representation) is diagonalizable. To meet these assumptions, \( K \) must be an abelian extension generated by its quadratic subfields, that is, \( K \) is multiquadratic.

**Generalizations.** In this article we choose only to investigate primes \( p \in \mathbb{Z} \) that are split completely in \( K/\mathbb{Q} \). This is done to simplify many calculations and concretize the structure of \( (\mathcal{O}_K/p\mathcal{O}_K)^\times \). It is expected that our arguments can be generalized to count densities of primes \( p \) not split in \( K/\mathbb{Q} \) in a manner similar to Roskam [16, 17], where split primes and inert primes were treated separately. Primes not split in \( K/\mathbb{Q} \) must be treated on a case by case basis for each Galois group. In [17], Roskam expanded his result from [16] to prove that for an arbitrary element \( \alpha \in K^\times \) for a quadratic field \( K \), Artin’s conjecture holds. It would be interesting to consider generalizations of our results from \( \mathcal{O}_K^\times \) to other subsets of \( K^\times \).

**Organization.** This article is organized as follows. Section 2 reformulates the problem in terms of Frobenius elements in field extensions \( K_\ell/K \) as \( \ell \) ranges over all prime numbers. Section 3 further refines these results in the case that \( K \) is multiquadratic. The techniques of Hooley are adapted in Section 4 to prove the main theorem (1.1). Section 5 contains results on when multiquadratic fields contain units of norm \(-1\). Finally, Section 6 includes the application to ray class fields of conductor \( p\mathcal{O}_K \).

### 2. Reformulation of the problem

Let \( K \neq \mathbb{Q} \) be a Galois number field containing a unit of norm \(-1\). Let \( G = \text{Gal}(K/\mathbb{Q}) \) and \( n = |G| = [K : \mathbb{Q}] \). Let \( \mathcal{O}_K \) denote the ring of algebraic integers of \( K \), and let \( \mathcal{O}_K^\times \) denote the group of units of \( \mathcal{O}_K \), which we will refer to as units of \( K \).
2.1. Restrictions on the field \( K \)

Not every Galois number field \( K \) containing a unit of norm \(-1\) will have have minimal index mod \( p \) for a positive density of split primes \( p \). We quickly deduce a necessary condition for this to be the case.

**Proposition 2.1.** If \( K \) is a number field that has minimal index mod \( p \) for infinitely many primes \( p \) split in \( K \), then \( K \) is a totally real number field.

**Proof.** Suppose \( K \) has signature \((r, s)\) and that \( K \) has minimal index mod \( p \) for infinitely many primes \( p \) split in \( K/\Q \). Let \( t = r + s - 1 \) be the rank of \( \mathcal{O}_K^\times \), so that \( \mathcal{O}_K^\times \cong \mathbb{Z}^t \oplus (\mathcal{O}_{K_{tor}}^\times) \), and let \( m = |(\mathcal{O}_K^\times)_{tor}| < \infty \). \( \mathcal{O}_K^\times \) has rank \( t = r + s - 1 \). Consider a prime \( p > m + 1 \) completely split in \( K \) for which \( K \) has minimal index mod \( p \); then \( |\psi_p(\mathcal{O}_K^\times)| = 2(p - 1)^{n-1} \). The maximal size of the image of \( \psi_p \) is \( m(p - 1)^t \), so \( m(p - 1)^t = 2(p - 1)^{n-1} \). Since \( m < p - 1 \), this implies \( t = n - 1 \).

From now on we add the assumption that \( K \) is totally real.

2.2. Translation to \( G \)-representations

Throughout this section, fix a prime \( p \in \mathbb{Z} \) which splits completely in \( K/\Q \). We will suppress the subscript \( p \) from the map \( \psi_p \). \( G \) acts transitively and faithfully on the set \( \{p = p_1, p_2, \ldots, p_n\} \) of prime ideals of \( K \) lying over \( p \). Enumerate elements \( g_i \in G \) so that \( g_i(p) = p_i \). Let \( a \) be a choice of a generator of \( \mathbb{F}_p^\times \). Define a \( G \)-module map \( \phi \) as the composition

\[
\mathcal{O}_K^\times \xrightarrow{\psi_p} (\mathcal{O}_K/p\mathcal{O}_K)^\times \xrightarrow{\sim} \prod_{i=1}^n(\mathcal{O}_K/p_i)^\times \xrightarrow{\sim} \prod_{i=1}^n\mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{Z}/(p - 1)\mathbb{Z}[G],
\]

\[
u \mapsto (a^{t_1}, \ldots, a^{t_n}) \mapsto \sum_{i=1}^n t_i[g_i] =: \phi(\nu).
\]

The image of \( \psi \) lies in the kernel of the composition \( (\mathcal{O}_K/p\mathcal{O}_K)^\times \xrightarrow{N} \mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{F}_p^\times /\{\pm 1\} \). This image is isomorphic as a \( G \)-module to the \( G \)-submodule \( I = \ker(\mathbb{Z}/(p - 1)\mathbb{Z}[G] \to \mathbb{Z}/((p - 1)/2)\mathbb{Z}) \) of \( \mathbb{Z}/(p - 1)\mathbb{Z}[G] \). Notice \( |I| = 2(p - 1)^{n-1} \) and \( |\text{Im}(\nu)| = |\text{Im}(\phi)| \).

**Lemma 2.2.** If \( K \) has minimal index mod \( p \), then for every prime \( \ell \) there is an isomorphism of \( \mathbb{F}_\ell[G] \)-modules \( \mathcal{O}_K^\times /((\mathcal{O}_K^\times)^\ell) \xrightarrow{\sim} I/\ell I \).

**Proof.** Suppose that \( K \) has minimal index mod \( p \), so that \( |\text{Im}(\psi)| = 2(p - 1)^{n-1} \). Since \( 2(p - 1)^{n-1} = |I| \), \( \phi : \mathcal{O}_K^\times \to I \) is an epimorphism. Tensoring this map with \( \mathbb{Z}/\ell\mathbb{Z} \) gives an epimorphism of \( \mathbb{F}_\ell[G] \)-modules \( \mathcal{O}_K^\times /((\mathcal{O}_K^\times)^\ell) \to I/\ell I \). Both \( \mathcal{O}_K^\times /((\mathcal{O}_K^\times)^\ell) \) and \( I/\ell I \) are \( \mathbb{F}_\ell \)-vector spaces of rank \( n - 1 \) if \( \ell \neq 2 \) or \( \mathbb{F}_2 \)-vector spaces of rank \( n \) if \( \ell = 2 \), so this map must be an isomorphism. If \( \ell \mid p - 1 \), then both \( \mathcal{O}_K^\times /((\mathcal{O}_K^\times)^\ell) \) and \( I/\ell I \) are 0 and the map is an isomorphism.

The additive module \( I \) fits into the exact sequence of \( \mathbb{Z} \)-modules

\[
0 \to I \to \mathbb{Z}/(p - 1)\mathbb{Z}[G] \xrightarrow{\text{Tr}} \mathbb{Z}/((p - 1)/2)\mathbb{Z} \to 0,
\]

where \( \text{Tr} \) denotes the trace map that sends an element \( \sum_{g \in G} a_g[g] \) to \( \sum_{g \in G} a_g \in \mathbb{Z}/((p - 1)/2)\mathbb{Z} \).

Let \( B_\ell = \{x = \sum x_i[g_i] \in \mathbb{F}_\ell[G] : \sum x_i = 0\} \subseteq \mathbb{F}_\ell[G] \). Applying the long exact sequence of Tor, we deduce that \( I/\ell I \cong B_\ell \) if \( \ell \neq 2 \). For \( \ell = 2 \) the situation is more complicated.
Lemma 2.3.  
(a) If $p \equiv 3 \mod 4$, then $I/2I \cong F_2[G]$.
(b) If $p \equiv 1 \mod 4$ and $|G|$ is odd, then $I/2I \cong F_2[G]$.
(c) If $p \equiv 1 \mod 4$ and $|G|$ is even, then $I/2I$ is not isomorphic to $F_2[G]$.

Proof. (a) : Apply the long exact sequence of Tor.

(b), (c) : Suppose $p \equiv 1 \mod 4$. As an abelian group, $I \cong (\mathbb{Z}/(p-1)\mathbb{Z})^{n-1} \oplus \mathbb{Z}/2\mathbb{Z}$, and so $I/2I$ is a rank $n$ vector space over $F_2$. Let $d$ be such that $2^d|p-1$; note $d \geq 2$. Define $T = \ker(\mathbb{Z}/2^d\mathbb{Z}[G] \to \mathbb{Z}/(2^d-1)\mathbb{Z})$ that is induced by the trace map, and define a $G$–module homomorphism $\delta : I \to T$ by reducing coefficients of elements of $I$ mod $2^d$. This map is an epimorphism by the generalized Chinese remainder theorem. Tensoring with $\mathbb{Z}/2\mathbb{Z}$ we obtain a $G$–module epimorphism $I/2I \to T/2T$ between $G$–modules over $F_2$ of the same rank, thus it is an isomorphism. Define $\alpha = (2^d-1-|G|)[g_1] + \sum_{i=1}^n [g_i] \in T$.

First suppose that $|G|$ is odd. Every element in $T$ can be written as $2^{d-1} + \sum_{i=1}^n a_i [g_i]$, where $\sum_{i=1}^n a_i \equiv 0 \mod 2^d$. Then for any $g_j \in G$, $g_j \alpha = \alpha + (2^{d-1}-|G|)([g_j] - [g_1])$. Since $2^{d-1}-|G|$ is odd, the set $\{g_j \alpha - \alpha\}_{j=1}^n$ generates all elements $\sum_{i=1}^n a_i [g_i]$ in $T$ with $\sum_{i=1}^n a_i \equiv 0 \mod 2^d$ as a module over $\mathbb{Z}/2\mathbb{Z}$. Hence $\alpha$ generates all of $T/2T$ as a $G$-module, and so $T/2T$ is a cyclic $G$–module of rank $n$. We deduce $I/2I \cong T/2T \cong F_2[G]$.

Now suppose that $|G|$ is even. The element $\alpha$ lies in the $G$ invariants of $T/2T$ since for any $g_j \in G$, $g_j \alpha - \alpha = (2^{d-1}-|G|)([g_j] - [g_1]) \in 2T$. Since also $2^{d-1}[g_1]$ lies in the $G$ invariants of $T/2T$, the $G$ invariants of $T/2T$ is at least $2$–dimensional over $F_2$. Since the $G$ invariants of $F_2[G]$ is $1$–dimensional, $T/2T$ is not isomorphic to $F_2[G]$ as $G$–modules, and so $I/2I$ is not isomorphic to $F_2[G]$ as $G$–modules. \(\blacksquare\)

Definition 2.4. For any $\ell$ (except $\ell = 2$ when $|G|$ is even), let $\phi_\ell$ denote the composition of $\phi$ with the map to $F_\ell[G]$ obtained from the previous lemmas.

Explicitly, the map $\phi_\ell$ is simply reduction mod $\ell$ of the coefficients $t_i$ of elements of $\mathbb{Z}/(p-1)\mathbb{Z}[G]$.

Using the previous three lemmas, we deduce the following theorem.

Theorem 2.5. If $p \equiv 3 \mod 4$ or if $p \equiv 1 \mod 4$ and $|G|$ is odd, then $K$ has minimal index mod $p$ if and only if the image of $\phi_\ell$ equals $B_\ell$ for every odd $\ell|p-1$ and the image of $\phi_\ell$ is all of $F_2[G]$. If $p \equiv 1 \mod 4$ and $|G|$ is even, then $K$ has minimal index mod $p$ if and only if the image of $\phi_\ell$ equals $B_\ell$ for every odd $\ell|p-1$ and $O_K^\times / (O_K^\times)^2 \cong I/2I$.

Using the simpler conditions away from $\ell = 2$, we also deduce the following weaker theorem that will be useful later.

Theorem 2.6. The index of $\psi(O_K^\times)$ in $(O_K/pO_K)^\times$ is a power of 2 times $(p-1)/2$ if and only if the image of $\phi_\ell$ equals $B_\ell$ for every odd $\ell|p-1$.

2.3. Translation to Frobenius elements

Given a prime $\ell|p-1$, let $K_\ell = K \left(\zeta_\ell, \sqrt[n]{O_K^\times} \right)$ where $\zeta_\ell$ denotes a primitive $\ell^{th}$ root of unity. $K_\ell$ is a Galois extension of $K(\zeta_\ell)$. Let $G_\ell = \text{Gal}(K_\ell/K(\zeta_\ell))$ denote its Galois group. $O_K^\times$ is a $Z$–module of rank $n-1$ with $(O_K^\times)_{\text{tors}} = \{\pm 1\}$, so for $\ell \neq 2$, we have that $|G_\ell| = \ell^{n-1}$ and $G_\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^{n-1}$ as groups. In contrast, for $\ell = 2$, $\sqrt{-1}$ is in $K_2$, but not in $K(\zeta_2) = K$; thus $G_2 = \text{Gal}(K_2/K(\zeta_2)) \cong (\mathbb{Z}/2\mathbb{Z})^n$ and $|G_2| = 2^n$. 

7
The next few lemmas will lead us to deduce that the fields $K_\ell$ can be generated as a $G$–module over $K(\zeta_\ell)$ by a single unit.

**Lemma 2.7.** [20, Lemma 5.27] There is a unit $\epsilon$ of $K$ such that the set of units \( \{g_i(\epsilon)\}_{i=1}^{n-1} \) is multiplicatively independent, hence is such that \( [O_K^\times : \mathbb{Z}_G \cdot \epsilon] = N < \infty \).

**Lemma 2.8.** For $\ell \nmid n = |G|$ (in particular, for the finitely many $\ell|N$ that are coprime to $n$), there is a unit $\epsilon_\ell$ so that $\text{gcd}(\{O_K^\times : \mathbb{Z}_G \cdot \epsilon_\ell\}, \ell) = 1$.

**Proof.** See [18].

**Remark 2.9.** It remains to consider those primes $\ell|n$. The following condition must be satisfied by the field $K$:

\[ (G1) \text{ If } \ell|n, \text{ then there is a unit } \epsilon_\ell \in O_K^\times \text{ such that } \text{gcd}(\{O_K^\times : \mathbb{Z}_G \cdot \epsilon_\ell\}, \ell) = 1. \]

We prove in Theorem 3.4 that this condition is satisfied in a multiquadratic field by any unit that has norm $-1$.

For a unit $\eta \in O_K^\times$, let $U_\eta = \mathbb{Z}_G \cdot \eta$ be the multiplicative subgroup of $O_K^\times$ generated by $\eta$ as a $G$–module.

**Lemma 2.10.** If $\eta$ is a unit satisfying $\text{gcd}(\{O_K^\times : U_\eta\}, \ell) = 1$ then $O_K^\times \cdot \sqrt[\ell]{U_\eta} = \sqrt[\ell]{O_K^\times}$.

**Proof.** See [18].

For a unit $\eta$, set $\eta_i := g_i^{-1}(\eta)$ for $1 \leq i \leq n$. By Lemmas 2.7, 2.8, and 2.10, and when $K$ satisfies condition $(G1)$, we deduce that for every prime $\ell$ there is a unit $\epsilon$ such that $K_\ell = K(\zeta_\ell, \sqrt[\ell]{\eta_1}, \ldots, \sqrt[\ell]{\eta_n})$. Also, note that as a consequence of Lemma 2.7, there are only finitely many distinct $\epsilon$ for all $\ell$ prime.

Given a prime $\mathfrak{P}$ of $K(\zeta_\ell)$ lying above $\mathfrak{p} \subseteq O_K$, let $\sigma_\mathfrak{P} = (\mathfrak{P}, K_\ell/K(\zeta_\ell)) \in G_\ell$ be the Frobenius element attached to a prime $\mathfrak{P}$. This is a well defined element of $G_\ell$ (independent of choice of prime ideal $\mathfrak{B}|\mathfrak{P}$ in $K_\ell$) since the extension $K_\ell/K(\zeta_\ell)$ is abelian.

**Theorem 2.11.** Let $p \in \mathbb{Z}$ be a completely split prime in $K$. Assume that $K$ satisfies condition $(G1)$.

(a) If $p \equiv 3 \mod 4$, $K$ has minimal index mod $p$ if and only if for every $\ell|p-1$, the Frobenius element $\sigma_\mathfrak{P}$ of any prime $\mathfrak{P}$ of $K(\zeta_\ell)$ lying above $\mathfrak{p}$ generates $G_\ell = \text{Gal}(K_\ell/K(\zeta_\ell))$ as a $\mathbb{G}$–module.

(b) If $p \equiv 1 \mod 4$ and $|G|$ is even, then $K$ has minimal index mod $p$ if and only if $O_K^\times/(O_K^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$ and for every $\ell|p-1$, $\ell \neq 2$, the Frobenius element $\sigma_\mathfrak{P}$ of any prime $\mathfrak{P}$ of $K(\zeta_\ell)$ lying above $\mathfrak{p}$ generates $G_\ell$ as a $\mathbb{G}$–module.

(c) If $p \equiv 1 \mod 4$ and $|G|$ is odd, then $K$ does not have minimal index mod $p$.

**Proof.** For any $\ell|p-1$, let $G'_\ell := \text{Gal}(K_\ell/K)$. From Kummer theory, there is a short exact sequence

\[ 1 \to \mu_\ell \to K^\times \to K^\times \to 1 \]

given by sending an element of $K^\times$ to its $\ell$th power, where $\mu_\ell$ denotes the set of $\ell$th roots of unity. Taking invariants under the absolute Galois group $\text{Gal}(K(\zeta_\ell)/K(\zeta_\ell))$ of $K(\zeta_\ell)$ and noticing that $H^1(K(\zeta_\ell), K^\times) = 0$ by Hilbert’s theorem 90, we obtain the Kummer isomorphism $H^1(K(\zeta_\ell), \mu_\ell) \cong K(\zeta_\ell)^{x/\ell}$. Since
\( \mu_\ell \) is trivial over \( K(\zeta_\ell) \). \( H^1(K(\zeta_\ell), \mu_\ell) \) records the homomorphisms from the absolute Galois group of \( K(\zeta_\ell) \) to \( \mu_\ell \). This is dual to the Galois group \( \Gamma_{K(\zeta_\ell)} \) of the maximal abelian extension of \( K(\zeta_\ell) \), and so we have

\[
\Gamma_{K(\zeta_\ell)} \cong \text{Hom}(K(\zeta_\ell)^\times / K(\zeta_\ell)^{\times \ell}, \mu_\ell) = \text{Hom}(K(\zeta_\ell)^\times, \mu_\ell)
\]
given by sending \( \sigma \) to \( (\alpha \mapsto \frac{\sigma(\sqrt[\ell]{\alpha})}{\sqrt[\ell]{\alpha}}) \). For any place \( v \) in \( K(\zeta_\ell) \) above \( p \), we have the commutative diagram

\[
\begin{array}{ccc}
\Gamma_{K(\zeta_\ell)_v} & \longrightarrow & \text{Hom}(K(\zeta_\ell)_v^\times, \mu_\ell) \\
\downarrow & & \downarrow \\
\Gamma_{K(\zeta_\ell)} & \longrightarrow & \text{Hom}(K(\zeta_\ell)^\times, \mu_\ell)
\end{array}
\]

where the vertical maps are isomorphisms. Let \( k \) be the residue field of \( K(\zeta_\ell) \) at \( v \); \( p \) is completely split so this is also the residue field of \( K \) at \( p \). Then there is a map

\[
\Gamma_{K(\zeta_\ell)_v} = \text{Hom}(K(\zeta_\ell)_v^\times, \mu_\ell) \rightarrow \text{Hom}(O_{\ell,v}^\times, \mu_\ell) \rightarrow \text{Hom}(k^\times, \mu_\ell)
\]

that corresponds to the maximal unramified quotient of \( \Gamma_{K(\zeta_\ell)_v} \). The image of a lift of the Frobenius element is computed on \( \alpha \in O'_{\ell,v} \) by reducing modulo \( p \) in \( K \) and considering the corresponding action on \( k^\times = (O_K/p)^\times \). In particular, for the extension \( K_\ell \), there is a commutative diagram

\[
\begin{array}{ccc}
\prod_v G'_{\ell,v} & \longrightarrow & \prod_p \text{Hom}((O_K/p)^\times, \mu_\ell) \\
\downarrow & & \downarrow \\
G'_{\ell} & \cong & \text{Hom}(O_K^\times, \mu_\ell)
\end{array}
\]

where the vertical arrow denotes reduction modulo \( p \), and the image is exactly the Frobenius element at \( p \). Since \( G \) permutes the Frobenius elements transitively, we deduce that the \( G \)–module generated by any Frobenius element is precisely the image of the map

\[
\text{Hom}((O_K/pO_K)^\times, \mu_\ell) \rightarrow \text{Hom}(O_K^\times, \mu_\ell)
\]

induced by \( O_K^\times \twoheadrightarrow (O_K/pO_K)^\times \). If \( \ell \neq 2 \), then \( \text{Hom}(O_K^\times, \mu_\ell) \) has order \( \ell^{n-1} \), and the above map is surjective if and only if the image of \( O_K^\times \) in \( (O_K/pO_K)^\times / (O_K/pO_K)^{\times \ell} \) has order \( \ell^{n-1} \), or equivalently if and only if \( O_K^\times \) surjects onto the trace zero part of \( \mathbb{F}_\ell[G] \) under the map \( \phi_\ell \). If \( \ell = 2 \), then \( \text{Hom}(O_K^\times, \mu_\ell) \) has order \( 2^n \), and the reduction map \( O_K^\times \twoheadrightarrow (O_K/pO_K)^\times / (O_K/pO_K)^{\times 2} \) must be an isomorphism. Now apply Theorem 2.5.

A priori there are \( [K(\zeta_\ell) : \mathbb{Q}] \) primes \( \mathfrak{P} \) of \( K(\zeta_\ell) \) lying above \( p \) since \( p \) is split in \( K/\mathbb{Q} \) and \( \ell | p - 1 \). However, for two primes \( \mathfrak{P} \) and \( \mathfrak{P}' \) lying above \( p \), \( \sigma_{\mathfrak{P}} \) and \( \sigma_{\mathfrak{P}'} \) generate subgroups in \( G_\ell \) of the same size which are conjugate in \( \text{Gal}(K_\ell/\mathbb{Q}) \), and so \( \sigma_{\mathfrak{P}} \) generates \( G_\ell \) as a \( G \)–module if and only if \( \sigma_{\mathfrak{P}'} \) does. Hence the choice of Frobenius element \( \sigma_{\mathfrak{P}} \in G_\ell \) is independent of \( \mathfrak{P} | p \) (and so also independent of choice of \( p | p \)), and we may choose the Frobenius element of any \( \mathfrak{P} \) lying over \( p \).

\[ \square \]

Using Theorem 2.6 we also deduce the following.

**Theorem 2.12.** Assume that \( K \) satisfies condition (G1). Let \( p \in \mathbb{Z} \) be a completely split prime in \( K \). The index of \( \psi_p(O_K^\times) \) in \( (O_K/pO_K)^\times \) is a power of 2 times \( (p-1)/2 \) if and only if for every odd \( \ell | p - 1 \), the Frobenius element \( \sigma_{\mathfrak{P}} \) of any prime \( \mathfrak{P} \) of \( K(\zeta_\ell) \) lying above \( p \) generates \( G_\ell \) as a \( G \)–module.
3. Multiquadratic fields

We will now add the assumption that $K$ is a multiquadratic field. Throughout this section and the next, $K$ will denote a totally real multiquadratic field containing a unit of norm $-1$ of degree $n = 2^m$ over $\mathbb{Q}$ and $G = \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^m$, $m \geq 1$. In this section we will reinterpret the equivalent conditions for $K$ to have minimal index mod $p$ given in Theorem 2.11 for multiquadratic fields and prove that when $p \equiv 3 \mod 4$, the condition always holds. We also prove that $K$ satisfies condition (G1).

3.1. Determination of the map $\psi$ at $\ell = 2$

In this section we prove that if $K$ has minimal index mod $p$, then $p \equiv 3 \mod 4$ and the map $\phi_2$ is an epimorphism.

Lemma 3.1. An element $x = \sum_{i=1}^{n} x_i [g_i] \in \mathbb{F}_2[G]$ generates $\mathbb{F}_2[G]$ as a $G$–module if and only if

$$\sum_{i=1}^{n} x_i \equiv 1 \mod 2.$$

Proof. Let $x = \sum_{i=1}^{n} x_i [g_i]$. First suppose $\sum_{i=1}^{n} x_i \equiv 1 \mod 2$. Then there are an odd number of nonzero coefficients of $x$. Let $g_{i_1}, \ldots, g_{i_{2k+1}}$ be the $2k + 1$ elements of $G$ with nonzero $x_i$ coefficients. Then

$$x \cdot x = \sum_{j=1}^{2k+1} [g_{i_j}] \cdot \sum_{t=1}^{2k+1} [g_{i_t}] = \sum_{j=1}^{2k+1} \sum_{t=1}^{2k+1} [g_{i_j} \cdot g_{i_t}]$$

$$= (2k + 1) [g_1] + 2 \sum_{j \neq t} [g_{i_j} \cdot g_{i_t}] = (2k + 1) [g_1] + 0 = [g_1],$$

since we are working in characteristic 2 and every element of $G$ has order 2. Thus $x^2 = [g_1]$. The action of $G$ gives us all elements of $\mathbb{F}_2[G]$ with exactly one nonzero coefficient, and adding these together will give us all elements of $\mathbb{F}_2[G]$ with exactly 2, 3, …, and $n$ nonzero coefficients. Hence $x$ will generate $\mathbb{F}_2[G]$ as a $G$–module. Conversely, if $\sum_{i=1}^{n} x_i \equiv 0 \mod 2$, then $x$ is in the kernel of the trace map $\mathbb{F}_2[G] \rightarrow \mathbb{F}_2$.

By Lemma 2.2, if $K$ has minimal index mod $p$, then there is an isomorphism of $\mathbb{F}_2[G]$–modules $O_K^\times/(O_K^\times)^{2} \rightarrow I/2I$. Also, by Lemma 2.3, $I/2I$ is not isomorphic to $\mathbb{F}_2[G]$ as $G$–modules.

Lemma 3.2. $O_K^\times/(O_K^\times)^{2} \cong \mathbb{F}_2[G]$ as $G$–modules.

Proof. Consider the composition

$$O_K^\times \rightarrow \prod_{v|\infty} \mathbb{R}^\times / (\mathbb{R}^\times)^{2} \xrightarrow{\cong} \mathbb{F}_2[G] \xrightarrow{\text{Tr}} \mathbb{F}_2,$$

$$u \mapsto (\sigma_v(u))_{v|\infty} = ((-1)^{t_v})_{v|\infty} \rightarrow \sum_{v|\infty} t_v[\sigma_v] \rightarrow \sum_{v|\infty} t_v,$$

where we naturally identify the $n$ real infinite places $v$ with elements $\sigma_v$ of $G = \text{Gal}(K/\mathbb{Q})$ and $\text{Tr}$ is the trace map. This map factors through $O_K^\times/(O_K^\times)^{2}$, giving a homomorphism of $G$–modules $O_K^\times/(O_K^\times)^{2} \rightarrow \mathbb{F}_2[G]$. By assumption there is a unit $\epsilon$ of $K$ of norm $-1$, and so the image under the above map of $\epsilon$ is $1 \in \mathbb{F}_2$. By Lemma 3.1, the image of $\epsilon$ in $\mathbb{F}_2[G]$ generates $\mathbb{F}_2[G]$. This gives an epimorphism $O_K^\times/(O_K^\times)^{2} \rightarrow \mathbb{F}_2[G]$ onto a free module, which is an isomorphism since both $O_K^\times/(O_K^\times)^{2}$ and $\mathbb{F}_2[G]$ have the same size. 

\end{document}
Thus if \( p \equiv 1 \mod 4 \), since \( I/2I \) is not isomorphic to \( F_2[G] \), the map \( \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \rightarrow I/2I \) cannot be an isomorphism of \( G \)-modules. By Lemma 2.2, \( K \) does not have minimal index mod \( p \). Next we turn to the case \( p \equiv 3 \mod 4 \).

**Lemma 3.3.** If \( p \equiv 3 \mod 4 \), then the map \( \phi_2 \) from Definition 2.4 is an epimorphism.

**Proof.** Using the notation from section 2.2, the image under \( \psi \) of \( \epsilon' \) in \( \prod_{i=1}^n (\mathcal{O}_K/p_i)^\times \) can be written

\[
(\epsilon' \mod p_1, \ldots, \epsilon' \mod p_n) = ((g_1(a))^{t_1}, \ldots, (g_n(a))^{t_n}),
\]

where \( a \) is a generator for \( (\mathcal{O}_K/p)^\times \), and so \( \prod_{i=1}^n g_i^{-1}(\epsilon') = N_{\mathbb{Q}/p}(\epsilon') = -1 \equiv \prod_{i=1}^n a^{t_i} = a^{\sum t_i} \mod p \).

Since \( a \) is a generator for \( (\mathcal{O}_K/p)^\times \), \(-1 \equiv a^{(p-1)/2} \mod p \) and so \( a^{(p-1)/2} = a^{\sum t_i} \mod p \). Then \((p-1)/2 \equiv \sum_{i=1}^n t_i \mod p-1 \), implying \( \sum_{i=1}^n t_i \equiv 1 \mod 2 \) since \( p \equiv 3 \mod 4 \).

Thus

\[
\phi_2(\epsilon') = \sum_{i=1}^n t_i [g_i] \in \{ x = \sum x_ig_i \in F_2[G] | \sum x_i = 1 \}.
\]

By Lemma 3.1, we see that \( \phi_2(\epsilon') \) will generate \( F_2[G] \) as a \( G \)-module, and so \( \phi_2 \) is an epimorphism. \( \square \)

We deduce that if \( p \equiv 3 \mod 4 \) it is always the case that the Frobenius element \( \sigma_P \) of any prime \( P \) of \( K(\zeta_2) \) lying above \( p \) generates \( G_2 = \text{Gal}(K_2/K(\zeta_2)) \) as a \( G \)-module. For any prime ideal above \( p \) generating \( \text{Gal}(K(\sqrt{-1})/K(\zeta_2)) = \text{Gal}(K(\sqrt{-1}/K)) \) as a \( G \)-module.

Finally we prove that the condition \((\text{G1})\) is satisfied for every multiquadratic field \( K \) containing a unit of norm \(-1\).

**Theorem 3.4.** If \( \epsilon' \) is a unit of norm \(-1\), then \( \gcd\left([\mathcal{O}_K^\times : \mathbb{Z}[G] \cdot \epsilon'], 2\right) = 1 \).

**Proof.** Let \( M = \mathbb{Z}[G] \cdot \epsilon' \) and \( N = \mathcal{O}_K^\times \); then the sequence

\[
0 \rightarrow M \xrightarrow{i} N \rightarrow N/M \rightarrow 0
\]

is exact. Using Lemma 3.2 we deduce that the map \( i \) is an isomorphism mod 2. By Nakayama’s lemma, this implies that \( (N/M)_{(2)} = 0 \). Thus \( N/M \) is torsion as a \( \mathbb{Z} \)-module and has order coprime to 2. \( \square \)

Combining this with the previous results of this section, we can now restate Theorem 2.11 for multiquadratic fields.

**Theorem 3.5.** Let \( K_\ell = K \left( \zeta_\ell, \sqrt{\mathcal{O}_K^\times} \right) \) if \( \ell \neq 2 \) is prime and let \( K_2 = K(\sqrt{-1}) \). For a prime \( p \in \mathbb{Z} \) completely split in \( K \), \( K \) has minimal index mod \( p \) if and only if for every prime \( \ell \mid p-1 \), the Frobenius element \( \sigma_P \) of any prime \( P \) of \( K(\zeta_\ell) \) lying above \( p \) generates \( G_\ell = \text{Gal}(K_\ell/K(\zeta_\ell)) \) as a \( G \)-module.
3.2. Frobenius elements for \( \ell \neq 2 \)

In this section we will further reformulate the condition on the Frobenius elements \( \sigma_\wp \) given in Theorem 2.11 for \( \ell \neq 2 \) into a set of conditions on the Frobenius elements in the \( n - 1 \) quadratic subfields of \( K \). In essence, we will prove that the Frobenius element \( \sigma_\wp \) generates \( G_\ell \) as a \( G \)-module if and only if a set of Frobenius elements in the simpler \( n - 1 \) quadratic subfields are non-trivial. This simplification will allow us to adapt analytic techniques for quadratic fields used by Roskam [16, 17] in the next section.

Fix a prime \( \ell \neq 2 \). For \( 1 \leq i \leq n - 1 \), let \( Q_i \) denote the \( n - 1 \) quadratic subfields of \( K \) and define \( H_i = \text{Gal}(K/Q_i) \) as the corresponding index two subgroup of \( G \). Since \( \ell \mid |G| = 2^m \), \( G_\ell \cong \bigoplus_{i=1}^{n-1} V_i \) as \( G \)-modules, where each \( V_i \) is a one dimensional \( G \)-module. Explicitly, the action of an element \( \sigma \in G_\ell \) on \( K_\ell = K(\zeta, \sqrt{\ell}, \ldots, \sqrt{\ell^n}) \) is given by \( \sigma(\sqrt{\ell^k}) = \zeta^{\ell^k} \sqrt{\ell^k} \), and for each \( i \), \( V_i = \mathbb{F}_\ell \left[ \sum_{h \in H_i} \sqrt{\ell^h} - \sum_{g \in H_i \setminus g} g \right] \).

For \( 1 \leq i \leq n - 1 \), define \( M_i := \bigoplus_{j \neq i} V_j \) and let \( u_i := \prod_{h \in H_i} h(\epsilon) \in Q_i \subseteq K \) where \( \epsilon \) is the unit for which \( K_\ell = K(\zeta, \sqrt{\ell}, \ldots, \sqrt{\ell^n}) \) given in subsection 2.3.

**Lemma 3.6.** For every \( 1 \leq i \leq n - 1 \), \( K_\ell^{M_i} = K(\zeta, \sqrt{u_i}) \).

**Proof.** \([K_\ell^{M_i} : K(\zeta)] = \ell\) so it is enough to show that \( \sqrt{u_i} \in K_\ell^{M_i} \). Consider for any \( i \neq j \) the containment \( H_i \leq H_i H_j \leq G \). The first containment is proper because \( i \neq j \). Since \([G : H_i] = 2\), \( H_i H_j = G \). Then \(|H_i \cap H_j| = \frac{|H_i||H_j|}{|H_i H_j|} = 2^{m-2}\), and so for every \( i \neq j \), \([H_j : H_i \cap H_j] = 2\). Thus for any \( j \neq i \) and for any \( \sigma \in V_j = \mathbb{F}_\ell \left[ \sum_{h \in H_j} h - \sum_{g \in H_j \setminus g} g \right] \), say \( \sigma = a(\sum_{h \in H_j} h - \sum_{g \in H_j \setminus g} g) \), we have

\[
\sigma(\sqrt{u_i}) = \sigma \left( \prod_{h \in H_i} \sqrt{h(\epsilon)} \right) = \prod_{h \in H_i \cap H_j} \zeta^{\sigma} \sqrt{h(\epsilon)} \cdot \prod_{h \in H_i \setminus H_j} \zeta^{-\sigma} \sqrt{h(\epsilon)} = \sqrt{u_i}.
\]

For each \( 1 \leq i \leq n - 1 \), let \( \Omega_i := \wp \cap \mathcal{O}_{Q_i}(\zeta) \); then \( \Omega_i \) is a completely split prime of \( Q_i(\zeta) \) that \( \wp \) lies above.

**Lemma 3.7.** \( \sigma_\wp \) generates \( G_\ell \) as a \( G \)-module if and only if for all \( 1 \leq i \leq n - 1 \), the Frobenius element \((\Omega_i, Q_i(\zeta, \sqrt{u_i})/Q_i(\zeta)) \neq (\text{id})\).

**Proof.** Since \( G_\ell \cong \bigoplus_{i=1}^{n-1} V_i \) as \( G \)-modules with \( V_i \) irreducible \( G \)-modules, \( \sigma_\wp \) generates \( G_\ell \) as a \( G \)-module if and only if \( \sigma_\wp|_{K_\ell^{M_i}} \neq (\text{id}) \) for all \( 1 \leq i \leq n - 1 \). Now,

\[
\sigma_\wp|_{K_\ell^{M_i}} = (\wp, K_\ell/K(\zeta))|_{K_\ell^{M_i}} = (\wp, K_\ell^{M_i}/K(\zeta)) = (\wp, K(\zeta, \sqrt{u_i})/K(\zeta)).
\]

Thus \( \sigma_\wp \) generates \( G_\ell \) as a \( G \)-module if and only if for every \( 1 \leq i \leq n - 1 \), \( (\wp, K(\zeta, \sqrt{u_i})/K(\zeta)) \neq (\text{id}) \). The element \( u_i = \prod_{h \in H_i} h(\epsilon) \in Q_i = K^{H_i} \) since \( u_i \) is fixed by every element of \( H_i \). Then \( (\wp, K(\zeta, \sqrt{u_i})/K(\zeta)) \neq (\text{id}) \) if and only if the Frobenius element \((\Omega_i, Q_i(\zeta, \sqrt{u_i})/Q_i(\zeta)) \neq (\text{id})\), since both elements have order a power of \( \ell \) and their order differs by at most \( 2^{m-1} = |K : Q_i| \).
4. Application of analytic number theory

4.1. Classical argument

In this section we will adapt analytic techniques originally given by Hooley [5] in his proof of Artin’s conjecture on primitive roots. Given an integer \( a \) not \( \pm 1 \) or a square, Hooley proved that the density of primes \( p \) for which \( a \) is a primitive root mod \( p \) exists and is equal to a nonzero number \( A(a) \) using the following method. To count the number of primes \( p \) less than \( x \) for which \( a \) is a primitive root mod \( p \), he divided the number line between 0 and \( x \) into four pieces and counted the number of desired primes in each range. Using analytic techniques, he proved primes in the higher three ranges were each \( O \left( \frac{x \log \log x}{\log^2 x} \right) \) and primes in the first range were equal to \( A(a) \frac{x \log x}{\log x} + O \left( \frac{x \log \log x}{\log^2 x} \right) \). The generalized Riemann hypothesis (GRH) was assumed to hold for fields of the form \( \mathbb{Q}(\zeta_k, \sqrt[a]{a}) \) to prove the statements for the lower two ranges. Dividing by \( x/\log x \) and applying the prime number theorem, he deduced that the desired density was \( A(a) \).

We will adapt these techniques to our setting. Recall that \( K \) is a totally real multiquadratic field containing a unit of norm \(-1\). Lemma 3.7 allows us to convert conditions pertaining to the multiquadratic field \( K \) into conditions pertaining to its quadratic subfields. Several of the proofs, including those of Lemmas 4.2 and 4.6, are then modifications of Roskam’s results for quadratic fields (see [17]) and are omitted from this article. Full details can be found in [18]. These two lemmas will not directly generalize to other number fields \( K \). We fix notation which we will use throughout the rest of this section.

**Notation 4.1.** Let \( \ell \) denote a prime number. Let \( k \) denote a positive squarefree integer. For any number field \( F \), let \( d_F := |\text{disc}(F/\mathbb{Q})| \).

In what follows we disregard the prime \( p = 2 \) since we are only interested in the asymptotic behavior of \( p \). Recall \( K_\ell = K \left( \zeta_\ell, \sqrt[\ell]{\mathcal{O}_K} \right) \) for \( \ell \neq 2 \), \( K_2 = K(\sqrt{-1}) \), and \( G_\ell = \text{Gal}(K_\ell/K(\zeta_\ell)) \). For \( p \in \mathbb{Z} \) a prime that splits completely in \( K \), let

\[
R(p, \ell) := \begin{cases} 
1 & \text{if } \ell | p - 1 \text{ and } F_\ell[G] \sigma \mathfrak{P} \subseteq G_\ell \text{ for any } \mathfrak{P} | p \text{ of } K(\zeta_\ell) \\
0 & \text{otherwise.}
\end{cases}
\]

Define the following for \( x, \delta, \delta_1, \delta_2 \in \mathbb{R} \).

\[
N(x, \delta) := |\{p \text{ split in } K/\mathbb{Q} : p \leq x, R(p, \ell) = 0 \ \forall \ \ell \leq \delta\}|
\]

\[
N(x) := N(x, x - 1) = |\{p \text{ split in } K/\mathbb{Q} : p \leq x, R(p, \ell) = 0 \ \forall \ \ell \leq x - 1\}|
\]
\[ P(x, k) := |\{ p \text{ split in } K/Q : p \leq x, R(p, \ell) = 1 \forall \ell|k\}| \]

\[ M(x, \delta_1, \delta_2) := |\{ p \text{ split in } K/Q : p \leq x, R(p, \ell) = 1 \exists \ell \in (\delta_1, \delta_2)\}| \]

\[ S := \{ \text{primes } p \text{ completely split in } K/Q : \forall \ell|p-1, \sigma_p \text{ generates } G_\ell \text{ as a } G-\text{module for any } \mathfrak{p}|p \text{ of } K(\zeta_\ell) \} \]

By Theorem 3.5, \( K \) has minimal index mod \( p \) if and only if \( p \) is an element of \( S \), and so we wish to show that the set \( S \) has a positive density

\[ \delta(S) = \lim_{x \to \infty} \frac{|\{ p \in S : p \leq x\}|}{\pi(x)} = \lim_{x \to \infty} \frac{N(x)}{\pi(x)} \]

in the set of all primes, where \( \pi(x) \) denotes the number of prime numbers \( p \) less than or equal to \( x \). We will do so by investigating the limit as \( x \to \infty \) of the ratio \( \frac{N(x)}{x/\log x} \).

Define \( b := 2n + 3 \), where \( n = [K : \mathbb{Q}] \); note that \( b \) only depends on the degree of the multiquadratic field \( K \). Let

\[ \xi_1(x) = \frac{1}{2b} \log(x), \ \xi_2(x) = \frac{\sqrt{x}}{\log^2 x}, \ \text{and} \ \xi_3(x) = \sqrt{x} \log x. \]

In addition, define \( M_1(x) := M(x, \xi_1(x), \xi_2(x)) \), \( M_2(x) := M(x, \xi_2(x), \xi_3(x)) \), and \( M_3(x) := M(x, \xi_3(x), x-1) \). As in the argument of Hooley, we deduce

\[ N(x) = N(x, \xi_1(x)) + O(M(x, \xi_1(x), x-1)). \]

Also, we trivially have

\[ M(x, \xi_1(x), x-1) \leq M(x, \xi_1(x), \xi_2(x)) + M(x, \xi_2(x), \xi_3(x)) + M(x, \xi_3(x), x-1) = M_1(x) + M_2(x) + M_3(x). \]

**Lemma 4.2.** \( M_3(x) = O\left(\frac{x}{\log^2 x}\right) \).

**Proof.** Sketch. This is the part of Hooley’s argument that Roskam [17] generalizes to quadratic fields and says will not directly generalize to higher degree fields. Using Lemma 3.7, we adapt the techniques of Roskam [17] by bounding \( 2^{M_3(x)} \) by the product over all numbers less than \( \frac{\sqrt{x}}{\log(x)} \) of a finite product of norms of elements in the \( n-1 \) quadratic subfields. Standard analytic techniques are used to finish the proof. For full details, see [18].
Lemma 4.3. $M_2(x) = O\left(\frac{x \log \log x}{\log^2 x}\right)$.

Proof. This proof is a straightforward adaptation of a method dating back to Hooley. The Brun-Titchmarsh Theorem and a theorem of Mertens are used. For full details, see [18].

Because $\frac{x}{\log^2 x} = O\left(\frac{x \log \log x}{\log^2 x}\right)$, we arrive at the following conclusion.

\[
N(x) = N(x, \xi_1(x)) + O(M(x, \xi_1(x), x - 1)) = N(x, \xi_1(x)) + O(M_1(x)) + O\left(\frac{x \log \log x}{\log^2 x}\right). \tag{1}
\]

4.2. Bounding $N(x)$

From (1) we see that to estimate $N(x)$ it remains to estimate both $M_1(x)$ and $N(x, \xi_1(x))$. If $p$ is counted in $M_1(x)$, then there is a prime $\ell_0 \in (\xi_1(x), \xi_2(x))$ such that $R(p, \ell_0) = 1$, and so $p$ will be counted in $P(x, \ell_0)$. Thus

\[
M_1(x) \leq \sum_{\ell \in (\xi_1(x), \xi_2(x))} P(x, \ell).
\]

Also, by the inclusion/exclusion principle we have

\[
N(x, \xi_1(x)) = \sum_{k \in U(x)} \mu(k)P(x, k),
\]

where $\mu(x)$ denotes the Möbius function and $U(x) = \{k : \ell|k \text{ then } \ell \leq \xi_1(x)\}$. For $k$ a squarefree integer, define

\[
K_k = \prod_{\ell|k} K_\ell = \begin{cases} K(\zeta_k, \sqrt[d_1]{K}) & \text{if } 2 \nmid k \\
K(\sqrt{-1}, \zeta_j, \sqrt[d_1]{K}) & \text{if } k = 2^j.
\end{cases}
\]

$K_k$ is a Galois extension of $\mathbb{Q}$ and for all $k$, $k^{n-1}\phi(k)/2 \leq [K_k : \mathbb{Q}] \leq 2n\phi(k)k^{n-1}$, where $n = [K : \mathbb{Q}]$ and $\phi(k)$ denotes the Euler phi function. The following technical lemma is due to Roskam [17].

Lemma 4.4. [17, Prop.13] There is a constant $\kappa_1$, depending on $\epsilon$, such that for all $x \geq 2$ and all subfields $F \subseteq K_k$ we have $\log d_F^{1/[F:Q]} \leq \kappa_1 \log k$.

To estimate the sum $P(x, k)$ we will use the following conditional result originally due to Lagarias-Odlyzko [9] and found in [17].

Theorem 4.5. Let $F/\mathbb{Q}$ be a Galois extension with Galois group $G$ and $C$ a union of conjugacy classes of $G$. Define

\[
\pi_C(x) = |\{p \leq x \text{ unramified in } F/\mathbb{Q} : (p, F/\mathbb{Q}) \subseteq C\}|.
\]

The generalized Riemann hypothesis implies that there is an absolute constant $\kappa_2$ such that for all $x \geq 2$ the following inequality holds:

\[
|\pi_C(x) - \frac{|C|}{|G|} Li(x)| \leq \kappa_2|C|\sqrt{x}(\log d_F^{1/[F:Q]} + \log x),
\]
with $Li(x) = \int_{2}^{x} \frac{dt}{\log t}$ the logarithmic integral.

This theorem is applied to two different sets of fields to finish the proof.

**Lemma 4.6.** $M_1(x) = O\left(\frac{x}{\log^2 x}\right)$.

**Proof. Sketch.** Using Lemma 3.7, we deduce that

$$M_1(x) \leq \sum_{\ell \in (\xi_1(x), \xi_2(x))} P(x, \ell) \leq \sum_{\ell \in (\xi_1(x), \xi_2(x))} \sum_{i=1}^{n-1} |\{p \leq x : p \text{ splits in } K(\zeta_\ell, \sqrt{u_1})/\mathbb{Q}\}|.$$

We apply Theorem 4.5 to the fields $K(\zeta_\ell, \sqrt{u_1})$ and $C$ the completely split conjugacy class. Adapting the techniques of Roskam [17], we use Lemma 4.4 and analytic techniques to obtain the desired bound. For full details, see [18].

Next we apply Theorem 4.5 to the fields $F = K_k$ to estimate the sum $P(x, k)$. Let $C_k$ denote the union of conjugacy classes in $\text{Gal}(K_k/\mathbb{Q})$,

$$C_k = \bigcup \{\sigma \in \text{Gal}(K_k/\mathbb{Q}) : \sigma|_K = (id), \sigma|_{Q(\xi)} = (id) \text{ and}$$

$$\sigma|_{K_\ell} \text{ does not generate } G_\ell \text{ as a } G - \text{module for all } \ell|k\}.$$

Then by definition $\pi_{C_k}(x) = P(x, k)$. By Theorem 4.5 the GRH implies that

$$|P(x, k) - \frac{|C_k|}{[K_k : \mathbb{Q}]} Li(x)| \leq \kappa_2 |C_k| \sqrt{x} (\log d_k^{1/|F: \mathbb{Q}|} + \log x).$$

This, combined with Lemma 4.4, shows

$$|P(x, k) - \frac{|C_k|}{[K_k : \mathbb{Q}]} Li(x)| \leq \kappa_2 |C_k| \sqrt{x} (\kappa_1 \log k + \log x)$$

$$= O\left(|C_k| \sqrt{x} \log(kx)\right).$$

Hence $P(x, k) = \frac{|C_k|}{[K_k : \mathbb{Q}]} Li(x) + O\left(|C_k| \sqrt{x} \log(kx)\right)$. \hspace{1cm} (2)

**Lemma 4.7.** $N(x, \xi_1(x)) = \sum_{k \in U(x)} \mu(k) |C_k| \frac{x}{[K_k : \mathbb{Q}] \log x} + O \left(\frac{x}{\log^2 x}\right)$.

**Proof.** We have that $N(x, \xi_1(x)) = \sum_{k \in U(x)} \mu(k) P(x, k)$, where $U(x) = \{k : \text{if } \ell|k \text{ then } \ell \leq \xi_1(x)\}$. Using equation (2) for $P(x, k)$ we deduce

$$N(x, \xi_1(x)) = \sum_{k \in U(x)} \mu(k) \left[\frac{|C_k|}{[K_k : \mathbb{Q}]} Li(x) + O\left(|C_k| \sqrt{x} \log x\right)\right]$$

$$= \sum_{k \in U(x)} \mu(k) |C_k| \frac{Li(x)}{[K_k : \mathbb{Q}]} + \sum_{k \in U(x)} O\left(|C_k| \sqrt{x} \log x\right).$$
Since $K \neq \mathbb{Q}$ and $\tau \neq j$

**Proof.** Let

$$N(x, \xi_1(x)) = \sum_{k \in U(x)} \frac{\mu(k)C_k}{[K_k : \mathbb{Q}]} \cdot Li(x) = \sum_{k \in U(x)} O\left( |C_k| \sqrt{x \log x} \right) \leq \sum_{k \leq x^{1/2}} O\left( k^n \sqrt{x \log x} \right) = O\left( x^{1/b}x^{n/b} \sqrt{x \log(x^{1+1/b})} \right) = O\left( x^{n+1 \over 4m+6} \log(x) \right) = O\left( \frac{x}{\log^2 x} \right).$$

\[\Box\]

Combining Lemmas 4.6 and 4.7 with the equation (1), we arrive at

$$N(x) = \sum_{k \in U(x)} \frac{\mu(k)C_k}{[K_k : \mathbb{Q}]} \cdot Li(x) + O\left( \frac{x \log \log x}{\log^2 x} \right). \quad (3)$$

4.3. Establishing the density formula

From the results of the previous subsection and equation (3),

$$\delta(S) = \lim_{x \to \infty} \frac{N(x)}{\pi(x)} = \lim_{x \to \infty} \frac{\sum_{k \in U(x)} \frac{\mu(k)C_k}{[K_k : \mathbb{Q}]} \cdot Li(x) + O\left( \frac{x \log \log x}{\log^2 x} \right)}{x / \log(x)}.$$

To show this limit exists, we will show that the sum \( \sum_{k \in U(x)} \frac{\mu(k)C_k}{[K_k : \mathbb{Q}]}) \) approaches a limit as \( x \to \infty \). To do so, we will need several lemmas.

**Lemma 4.8.** For \( r \) odd, the largest abelian extension of \( \mathbb{Q} \) contained in \( K_r \) is \( K(\zeta_r) \).

**Proof.** Let \( G_r = \text{Gal}(K_r/\mathbb{Q}) \); we show the commutator \([G_r,G_r]\) of \( G_r \) is \( H = \text{Gal}(K_r/(K(\zeta_r))) \). Since \( G_r/H \cong \text{Gal}(K(\zeta_r)/\mathbb{Q}) \) is abelian, \([G_r,G_r] \subseteq H \). To show \( H \subseteq [G_r,G_r] \), it is enough to show that the generators \( \sigma_i \in H \) all lie in \([G_r,G_r]\), where \( \sigma_i \) is defined by \( \sigma_i(\sqrt[r]{\zeta_j}) = \zeta_j^r \sqrt[r]{\zeta_j} \), and \( \sigma_i \) fixes \( \zeta_r \) and all \( \sqrt[r]{\zeta_j} \) for \( j \neq i \). For \( \sigma_i \), define \( \rho_i, \tau_i \in G_r \) by \( \rho_i(\zeta_j) = \zeta_j^r, \rho_i(\sqrt[r]{\zeta_j}) = \sqrt[r]{\zeta_j} \) for all \( j \), \( \tau_i(\zeta_r) = \zeta_r, \tau_i(\sqrt[r]{\zeta_j}) = \zeta_j^r \sqrt[r]{\zeta_j}, \) and \( \tau_i(\sqrt[r]{\zeta_j}) = \sqrt[r]{\zeta_j} \) for \( j \neq i \). Then \( \tau_i \rho_i \tau_i^{-1} \rho_i^{-1}(\sqrt[r]{\zeta_j}) = \zeta_j^r \sqrt[r]{\zeta_j} \) and for \( j \neq i \), \( \tau_i \rho_i \tau_i^{-1} \rho_i^{-1}(\sqrt[r]{\zeta_j}) = \sqrt[r]{\zeta_j}, \) so \( \tau_i \rho_i \tau_i^{-1} \rho_i^{-1} = \sigma_i \) and thus \( \sigma_i \in [G_r,G_r] \).

\[\Box\]

**Lemma 4.9.** \( K_\ell \cap K_2 = K \) for all \( \ell \neq 2 \).

**Proof.** Suppose to the contrary that \( \ell \) is a prime such that \( K_2 \cap K_\ell = K(\sqrt{-1}) \). Since \( K(\sqrt{-1}) \) is abelian over \( \mathbb{Q} \) and contained in \( K_\ell \), by Lemma 4.8, \( K(\sqrt{-1}) \subseteq K(\zeta_\ell) \). Since \( K(\sqrt{-1}) \) is the unique degree two extension of \( K \) in \( K(\zeta_\ell) \), we deduce \( K(\sqrt{-1}) \subseteq K(\sqrt{-1}) \). Two cases arise.

**Case 1:** If \( \ell \equiv 3 \) mod 4, then \( K(\sqrt{-\ell}) \subseteq K(\sqrt{-1}) \). \( K(\sqrt{-\ell}) \) is ramified over \( \mathbb{Q} \) at the prime \( \ell \). Since \( K \) contains a unit of norm \( -1 \), no prime \( \ell \equiv 3 \) mod 4 can ramify in \( K/\mathbb{Q} \), and so \( \ell \) is unramified in \( K(\sqrt{-1})/\mathbb{Q} \), a contradiction.
Case 2: If \( \ell \equiv 1 \pmod{4} \), then \( K \left( \sqrt{\ell} \right) \subset K \left( \sqrt{-1} \right) \), and the containment must be proper since \( K \left( \sqrt{\ell} \right) \subseteq \mathbb{R} \). This forces \( \sqrt{\ell} \in K \), and so \( 2 \mid \left[ K \cap \mathbb{Q} \left( \sqrt{\ell} \right) : \mathbb{Q} \right] \). By Galois theory the isomorphism \( \text{Gal} \left( K \left( \sqrt{\ell} \right) / K \right) \cong \text{Gal} \left( \mathbb{Q} \left( \sqrt{\ell} \right) / \mathbb{Q} \right) \) gives \( \left[ K \left( \sqrt{-1} \right) \cap \mathbb{Q} \left( \sqrt{\ell} \right) : K \cap \mathbb{Q} \left( \sqrt{\ell} \right) \right] = 2 \). This implies that \( \left( K \left( \sqrt{-1} \right) \cap \mathbb{Q} \left( \sqrt{\ell} \right) : \mathbb{Q} \right) \), a contradiction since \( \text{Gal} \left( K \left( \sqrt{-1} \right) \cap \mathbb{Q} \left( \sqrt{\ell} \right) / \mathbb{Q} \right) \) is a quotient of both the cyclic group \( \text{Gal} \left( \mathbb{Q} \left( \sqrt{\ell} \right) / \mathbb{Q} \right) \) and the elementary abelian group \( \text{Gal} \left( K \left( \sqrt{\ell} \right) / \mathbb{Q} \right) \). \( \square \)

Let \( E \) denote the genus field of \( K \), the largest Abelian extension of \( \mathbb{Q} \) contained in the Hilbert class field of \( K \). Define \( E_k \) as the compositum \( E_k = E \cdot K_k \) for \( k \) odd and squarefree. The fields \( K_k \) are not linearly disjoint (see Lemma 4.10), but if we pass to the genus field \( E \) of \( K \), the corresponding fields \( E_k \) become linearly disjoint and we can use this fact to complete the theorem.

**Lemma 4.10.** Let \( r \) and \( s \) denote squarefree odd integers with \( \gcd(r, s) = 1 \).

(a) \( E_r \cap E_s = E \).

(b) If \( \gcd(r, d_K) = 1 \), then \( K_r \cap K_s = K \).

**Proof.** (a): The field extensions \( K_r/K \) and \( E_r/E \) are ramified only at primes lying above primes \( \ell | k \). Therefore since \( \gcd(r, s) = 1 \), the extension \( E_r \cap E_s/E \) is unramified. Since the extension \( E/K \) is unramified, also \( E_r \cap E_s/K \) is unramified. We show \( E_r \cap E_s/Q \) is abelian; this implies \( E_r \cap E_s \) is contained in the genus field of \( K \), which is \( E \), and so \( E_r \cap E_s = E \). Notice \( E_r \cap E_s \) is a subfield of both \( E_r(\zeta_{r,s}) \) and \( E_s(\zeta_{r,s}) \), and so \( E_r \cap E_s \subseteq E_r(\zeta_{r,s}) \cap E_s(\zeta_{r,s}) \). The extension \( E_r(\zeta_{r,s}) \) of \( E(\zeta_s) \) is obtained by adjoining \( r \)th roots, and so its degree is power of \( r \); likewise \( \left| E_s(\zeta_{r,s}) : E(\zeta_r) \right| \) is a power of \( s \). Since \( \gcd(r, s) = 1 \), \( E_r(\zeta_{r,s}) \cap E_s(\zeta_{r,s}) = E(\zeta_s) \). Thus \( E_r \cap E_s \subseteq E(\zeta_s) \), and so \( E_r \cap E_s \) is abelian over \( Q \).

(b): Now suppose \( \gcd(r, d_K) = 1 \). For a prime \( \ell | r \), \( K \) is unramified at \( \ell \) and \( \mathbb{Q}(\zeta_r) \) is totally ramified at \( \ell \), and so \( K(\zeta_r) = K \cdot \mathbb{Q}(\zeta_r) \) is totally ramified over \( K \). The extension \( K(\zeta_r) \cap E \) is both totally ramified and unramified over \( K \), and so \( K(\zeta_r) \cap E \) is a subfield of \( E(\zeta_r) \cap K \), and so \( K_r \cap K_s = K(\zeta_r) \). Hence \( K_r \cap K_s = E \) and \( K(\zeta_r) = K \), so \( K_r \cap K_s = K \).

**Lemma 4.11.** \(|C_{r,s}| = |C_r||C_s| \) if \( \gcd(r, s) = 1 \).

**Proof.** It is enough to prove this for \( r, s \) prime numbers not equal to 2. We show the map \( C_{r,s} \rightarrow C_r \times C_s \), \( \sigma \mapsto (\sigma|_{K_r}, \sigma|_{K_s}) \) is a bijection of sets. It is clearly an injection since \( K_{r,s} = K_r K_s \). To see the map is a surjection, suppose \( \rho, \sigma \in C_r \times C_s \). \( K_r \cap K_s \subseteq E_r \cap E_s \), so by Lemmas 4.8 and 4.10, \( K_r \cap K_s \) is abelian over \( Q \), and contained in \( K(\zeta_r) \cap K(\zeta_s) \). By assumption \( \rho = (id) \) on \( K(\zeta_r) \) and \( \sigma = (id) \) on \( K(\zeta_s) \), and so \( \rho \) and \( \sigma \) agree and are the identity on \( K_r \cap K_s \). Hence we can make a map \( \tau : K_r \rightarrow K_s \) by defining \( \tau(x) = \rho(x) \) for all \( x \in K_r \) and \( \tau(x) = \sigma(x) \) for all \( x \in K_s \). By the conditions on \( \rho \) and \( \sigma \), we deduce that \( \tau \in C_{r,s} \) and \( \tau \) maps to \( (\rho, \sigma) \).

**Lemma 4.12.** \(|C_{d}| \leq 2^{(n-1)\ell^{n-2}} \) for every \( \ell \neq 2 \).

**Proof.** If \( \ell \neq 2 \), then \( \ell \mid |G| \), and so \( G_{\ell} \cong \bigoplus_{i=1}^{n-1} V_i \), where \( V_i \) are distinct one-dimensional \( G \)-modules. Thus the number of elements that generate \( G_{\ell} \) as a \( G \)-module is \( (\ell - 1)^{n-1} \), and so \( |C_{d}| = \ell^{n-1} - (\ell - 1)^{n-1} \).

For any \( \ell, (\ell - 1)^{n-1} \geq \ell^{n-1} - \sum_{i=0}^{n-2} \binom{n-1}{i} \ell^i \), and so

\[
|C_{\ell}| \leq \sum_{i=0}^{n-2} \binom{n-1}{i} \ell^i \leq \sum_{i=0}^{n-2} \binom{n-1}{i} \ell^{n-2} \leq 2^{n-1} \ell^{n-2}.
\]

\( \square \)
Lemma 4.13. 1. \[ \lim_{x \to \infty} \sum_{k \in \mathcal{U}(x)} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} < \infty. \]

2. \[ \lim_{x \to \infty} \sum_{k \in \mathcal{U}(x)} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} = \sum_{k=1}^{\infty} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \]

Proof. If \( k \notin \mathcal{U}(x) \), then \( k > \xi_1(x) \). Thus

\[ \left| \sum_{k=1}^{\infty} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} - \sum_{k \in \mathcal{U}(x)} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \right| \leq \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \leq \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \]

and so we can prove both statements in the same step. Let \( 1 > \delta > 0 \). Recall that for squarefree \( k \), \( [K_k : \mathbb{Q}] \geq \frac{\phi(k)k^{n-1}}{2^n} \). Thus

\[ \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \leq \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|2^{n-1}}{\phi(k)k^{n-1}}. \]

By Lemmas 4.11 and 4.12, \( |C_k| = \prod_{\ell | k} |C_{\ell^k}| \leq \prod_{\ell | k} 2^{(n-1)\ell^{n-2}} \). Thus

\[ \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|2^{n-1}}{\phi(k)k^{n-1}} \leq \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|2^{n-1}\ell^{n-2}}{\phi(k)k^{n-1}} = \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|2^{n-2}}{\phi(k)k} \]

We show that there is a \( \kappa(\delta) \) such that for all \( k \) squarefree,

\[ \prod_{\ell | k} 2^{2n-2} \leq \frac{\kappa(\delta)}{k^{2-\delta}}, \quad \text{or equivalently} \quad \frac{\prod_{\ell | k} 2^{2n-2}}{\phi(k)} \leq \frac{\kappa(\delta)}{k^{1-\delta}}. \]

Define \( w = (2^{2n-1})^{1/\delta} \) and \( \kappa(\delta) = 2^{(2n-2)w} \prod_{\ell \leq w} \ell^{1-\delta} \). In this case, \( 1/\ell^{1-\delta} > 2^{2n-2}/(\ell - 1) \) for all \( \ell > w \).

We deduce that for \( k \) squarefree,

\[ \frac{\prod_{\ell | k} 2^{2n-2}}{\phi(k)} = \prod_{\ell | k} 2^{2n-2} - 1 \leq \prod_{\ell | k, \ell \leq w} 2^{2n-2} - 1 \cdot \frac{1}{\ell^{1-\delta}} \]

\[ \leq \prod_{\ell | k} \frac{1}{\ell^{1-\delta}} \cdot (2^{(2n-2)w}) \prod_{\ell \leq w} \ell^{1-\delta} \]

\[ = \prod_{\ell | k} \frac{1}{\ell^{1-\delta}} \cdot \kappa(\delta) = \frac{\kappa(\delta)}{k^{1-\delta}}. \]

Hence

\[ \sum_{k > \xi_1(x)} \frac{\mu(k)|C_k|2^{n-1}}{\phi(k)k^{n-1}} \leq \kappa(\delta) \sum_{k > \xi_1(x)} \frac{1}{k^{2-\delta}}, \]

which converges since \( 1 > \delta > 0 \) and \( \kappa(\delta) \) does not depend on \( x \). □

Taking a limit and applying Lemma 4.13 to equation (3), we conclude

\[ \delta(S) = \lim_{x \to \infty} \frac{N(x)}{x/\log x} = \sum_{k=1}^{\infty} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \]

19
4.4. Nonvanishing of density

Let
\[ c = \sum_{k=1}^{\infty} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]}. \]

It remains to show that \( c \neq 0 \) to conclude that the set \( S \) has positive density. By Lemma 4.9, \( K_2 \cap K_\ell = K \) for all \( \ell \neq 2 \), and so

\[ c = \left( 1 - \frac{|C_2|}{[K_2 : K]} \right) \frac{1}{2} \sum_{k \text{ odd}} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \]

Using Theorem 2.12 we conclude \( 2c = \sum_{k \text{ odd}} \frac{\mu(k)|C_k|}{[K_k : \mathbb{Q}]} \) is the density of primes \( p \in \mathbb{Z} \) completely split in \( K \) for which the index of \( \psi_p(\mathcal{O}_K^\times) \) in \( \mathcal{O}_K/p\mathcal{O}_K \times \) is a power of 2 times \((p - 1)/2\). Define \( d \) to be the density of primes \( p \in \mathbb{Z} \) completely split in \( E \) for which the index of \( \psi_p(\mathcal{O}_K^\times) \) in \( \mathcal{O}_K/p\mathcal{O}_K \times \) is a power of 2 times \((p - 1)/2\). Since every prime that splits in \( E \) is already split in \( K \), \( d \leq 2c \). We show \( d > 0 \) to conclude that \( c > 0 \).

Remark 4.14. In any multiquadratic field \( K' \), for any \( p \neq 2 \), the ramification index \( e_p(K'/\mathbb{Q}) \leq 2 \). Because \( K \) contains a unit of norm \(-1\), any prime that ramifies in \( K \) is either 2 or congruent to 1 mod 4. Thus for every prime \( p \), the ramification index \( e_p(K/\mathbb{Q}) \) is at most 2. The result is more general; see [4, III.3.6].

Lemma 4.15. The genus field \( E \) of \( K \) is a multiquadratic field.

Proof. Since the genus field \( E \) is abelian over \( \mathbb{Q} \), we prove \( E \) is multiquadratic field by showing that every cyclic quotient of \( \text{Gal}(E/\mathbb{Q}) \) of prime power order is of order 2. Let \( \text{Gal}(E/\mathbb{Q}) \to \mathbb{Z}/\ell^n\mathbb{Z} \) for some prime \( \ell \) and some \( n \geq 1 \). By Galois theory, there is a subfield \( R \) of \( E \) with \( \text{Gal}(R/\mathbb{Q}) \cong \mathbb{Z}/\ell^n\mathbb{Z} \). At least one prime must be totally ramified in \( R/\mathbb{Q} \): to see this, suppose not. Then the inertia group of every prime is proper in \( \text{Gal}(R/\mathbb{Q}) \) and so is a subgroup of \( H \), the unique subgroup of \( \text{Gal}(R/\mathbb{Q}) \) of order \( \ell^n - 1 \). The fixed field \( R^H \) of \( H \) is then a field extension of degree \( \ell \) over \( \mathbb{Q} \) that is unramified at every prime, a contradiction.

Let \( p \) be a prime that is totally ramified in \( R/\mathbb{Q} \). Then the ramification index \( e_p(R/\mathbb{Q}) \) equals \([R : \mathbb{Q}]\). Since ramification indices are multiplicative, \( e_p(K/\mathbb{Q}) \leq 2 \) by Remark 4.14, and the extension \( E/K \) is unramified at every prime, we conclude that \( e_p(R/\mathbb{Q}) \leq e_p(E/\mathbb{Q}) \leq 2 \). Hence it must be that \( e_p(R/\mathbb{Q}) = 2 = [R : \mathbb{Q}] \).

For any odd integer \( k \geq 1 \), let \( C'_k \) denote the union of conjugacy classes in \( \text{Gal}(E_k/\mathbb{Q}) \) given by
\[ C'_k = \bigcup \{ \sigma \in \text{Gal}(E_k/\mathbb{Q}) : \sigma|_E = (id), \sigma|_{\mathbb{Q}(\zeta)} = (id) \text{ and } \sigma|_{K_\ell} \text{ does not generate } G_\ell \text{ as a } G \text{-module for all } \ell|k \}. \]

Using Lemma 4.15, we deduce from a symmetric argument to the one provided that
\[ d = \sum_{k \text{ odd}} \frac{\mu(k)|C'_k|}{[E_k : \mathbb{Q}]}. \]

Lemma 4.16. If \( k \geq 1 \) is odd, \( |C_k| = |C'_k| \).
Proof. We have the following diagram.

\[
\begin{array}{c}
1 \longrightarrow \text{Gal}(K_k/K(\zeta_k)) \longrightarrow \text{Gal}(K_k/K) \longrightarrow \text{Gal}(K(\zeta_k)/K) \longrightarrow 1 \\
1 \longrightarrow \text{Gal}(E_k/E(\zeta_k)) \longrightarrow \text{Gal}(E_k/E) \longrightarrow \text{Gal}(E(\zeta_k)/E) \longrightarrow 1
\end{array}
\]

Since \(E/K\) is unramified, \(\text{Gal}(E(\zeta_k)/E) \cong \text{Gal}(K(\zeta_k)/K)\), and for any \(\ell\) such that \(\ell\mid k\), an element of \(\text{Gal}(K_k/K)\) that is the identity on \(E\) generates \(G_{\ell}\) as a \(G\)-module if and only if its image in \(\text{Gal}(E_k/E)\) also generates \(G_{\ell}\) as a \(G\)-module. The result follows. \(\square\)

By Lemmas 4.10 and 4.11 we deduce \(d\) is completely multiplicative. Combining this with Lemma 4.16, we have

\[
d = \sum_{k \text{ odd}} \frac{\mu(k)|C_k|}{[E_k : \mathbb{Q}]} = \frac{1}{[E : \mathbb{Q}]} \sum_{k \text{ odd}} \frac{\mu(k)|C_k|}{[E_k : E]}
\]

\[
= \frac{1}{[E : \mathbb{Q}]} \prod_{\ell \neq 2 \text{ prime}} \left(1 + \frac{\mu(\ell)|C_\ell|}{[E_\ell : E]}\right)
\]

\[
= \frac{1}{[E : \mathbb{Q}]} \prod_{\ell \neq 2 \text{ prime}} \left(1 - \frac{|C_\ell|}{[E_\ell : E]}\right)
\]

\[
= \frac{r_K}{[E : \mathbb{Q}]} \prod_{\ell \neq 2 \text{ prime}} \left(1 - \frac{|C_\ell|}{(\ell - 1)^{n-1}}\right),
\]

where \(r_K \neq 0\) is a correction factor for those primes ramifying in \(K/\mathbb{Q}\). We show this product is nonzero by proving the corresponding series

\[
\log \left( \prod_{\ell \text{ prime}} \left(1 - \frac{|C_\ell|}{(\ell - 1)^{n-1}}\right) \right) = \sum_{\ell \text{ prime}} \log \left(1 - \frac{|C_\ell|}{(\ell - 1)^{n-1}}\right)
\]

is absolutely convergent. By elementary comparisons we deduce

\[
\sum_{\ell \text{ prime}} \log \left(1 - \frac{|C_\ell|}{(\ell - 1)^{n-1}}\right) \leq \sum_{\ell \text{ prime}} \frac{|C_\ell|}{(\ell - 1)^{n-1}}.
\]

Applying Lemma 4.12,

\[
\sum_{\ell \text{ prime}} \frac{|C_\ell|}{(\ell - 1)^{n-1}} \leq \sum_{\ell \text{ prime}} \frac{2^{n-1} \ell^{n-2}}{(\ell - 1)^{n-1}} = \sum_{\ell \text{ prime}} \frac{2^{n-1}}{(\ell - 1)^{n-1}} \leq 2^{n-1} \sum_r \frac{1}{(r-1)r} < \infty
\]

We conclude \(d > 0\), so \(S\) has a positive density in the set of all primes. Since also \([K(\zeta_\ell) : K] = \ell - 1\) for all \(\ell \nmid d_K\), we have shown that the density of \(S\) equals

\[
c = \frac{1}{2[K : \mathbb{Q}]} \left( \sum_{k \mid d_K} \frac{\mu(k)|C_k|}{[K_k : K]} \right) \prod_{\ell \nmid 2d_K} \left(1 - \frac{1}{(\ell - 1)^{n-1}} \left(1 - \frac{(\ell - 1)^{n-1}}{(\ell - 1)^{n-1}}\right)\right).
\]

Thus we have proven Theorem 1.1.
5. Units in multiquadratic fields

For a totally real multiquadratic field $K$ of degree $n = 2^m$ over $\mathbb{Q}$, we call a set of $n - 1$ generators for the non-torsion summand of the unit group a system of fundamental units of $K$. The question of which multiquadratic fields contain a unit of norm $-1$ has been extensively studied in the literature. Kuroda’s class number formula for multiquadratic fields relates units of $K$ with units and class numbers of subfields (see [8] or [19]).

**Theorem 5.1. (Kuroda’s class number formula)** Let $K$ denote a totally real multiquadratic field with $|\text{Gal}(K/\mathbb{Q})| = n = 2^m$. Let $Q_i$, $i = 1, \ldots, n - 1$ denote the $n - 1$ distinct quadratic subfields of $K$. Let $h_i$ denote the class number of $Q_i$, and let $\mathcal{O}^\times_{Q_i}$ be the unit group of $Q_i$. Let $v = m(2^{m-1} - 1)$, and let $h$ denote the class number of $K$. Then

$$ h = \frac{1}{2^n} \left[ \mathcal{O}^\times_K : \prod_{i=1}^{n-1} \mathcal{O}^\times_{Q_i} \right] \cdot \prod_{i=1}^{n-1} h_i. $$

**Proposition 5.2.** If $K$ is a number field containing a unit of norm $-1$, then every subfield $F$ of $K$ also contains a unit of norm $-1$.

Thus we consider units in (multiquadratic) subfields. If a quadratic field $\mathbb{Q}(\sqrt{d})$ contains a unit of norm $-1$, then all prime divisors of $d$ are either 2 or equivalent to 1 mod 4. If $K$ is a totally real biquadratic field, choose positive integers $m$ and $n$ such that $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Call the fundamental units in the three quadratic subfields $Q_1 = \mathbb{Q}(\sqrt{m})$, $Q_2 = \mathbb{Q}(\sqrt{n})$, and $Q_3 = \mathbb{Q}(\sqrt{mn})$ $\epsilon_1$, $\epsilon_2$ and $\epsilon_3$, respectively. In [7] (see also [14], [22]), Kubota completely classified the structure of the unit group of $K$ into one of seven types.

Kubota’s work proves that if each quadratic subfield of $K$ has a unit $x_i \in Q_i$ of norm $N^Q_{x_i} x_i = -1$, then a system of fundamental units of $K$ must be of one of the two forms $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ or $\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1 \epsilon_2 \epsilon_3}\}$. The latter occurs if and only if the element $z = \sqrt{\epsilon_1 \epsilon_2 \epsilon_3}$ lies in $K$. In this case, $z$ will be a unit of $K$ of norm $-1$.

**Proposition 5.3.** If $K$ is a totally real biquadratic field containing a unit of norm $-1$, then a system of fundamental units of $K$ is $\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_1 \epsilon_2 \epsilon_3}\}$, where each $\epsilon_i$ is the fundamental unit of the quadratic subfield $Q_i$.

**Proof.** Let $u \in \mathcal{O}^\times_K$. If $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ is a system of fundamental units for $K$, $u = \pm \epsilon_1^{a_1} \epsilon_2^{a_2} \epsilon_3^{a_3}$ for some integers $a_i$. Hence

$$ N^K_Q(u) = N^K_Q(\pm \epsilon_1^{a_1} \epsilon_2^{a_2} \epsilon_3^{a_3}) = \prod_{i=1}^{3} (N^K_{Q_i} \epsilon_i)^{a_i} $$

$$ = \prod_{i=1}^{3} (N^Q_{Q_i}(N^K_{Q_i} \epsilon_i))^{a_i} = \prod_{i=1}^{3} (N^Q_{Q_i}(\epsilon_i)^2)^{a_i} = \prod_{i=1}^{3} ((\pm 1)^2)^{a_i} = 1 $$

22
because $\epsilon_i \in \mathbb{Q}_i$. \hfill \qed

It is known (see [6] Ch. 17, [7]) that for primes $p, q \equiv 1 \mod 4$ with Legendre symbol $\left( \frac{p}{q} \right) = -1$, the fields $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{pq})$, and $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ contain a unit of norm $-1$.

**Example 5.4.** Consider the field $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$, which contains a unit of norm $-1$ and has genus field $E = K$. Only the primes 5 and 13 ramify in $K/\mathbb{Q}$, and for these primes $[K(\zeta_\ell) : K] = (\ell - 1)/2$. Using Theorem 1.1, we compute the density $D$ of primes for which $K$ has minimal index mod $p$ to be

$$D = \frac{1}{4} \cdot \frac{1}{2} \prod_{\ell \not\equiv 2} \left( 1 - \frac{1}{[K(\zeta_\ell) : K]} \left( 1 - \frac{(\ell - 1)^3}{\ell^3} \right) \right) = \frac{1}{4} \cdot \frac{1}{2} \cdot 35 \cdot \frac{189}{54} \cdot \frac{1931}{250} \cdot \frac{2058}{2058} \cdots = 0.05142184 \ldots$$

The accuracy of this numerical approximation can be verified following the method given in [13], which gives error bounds on the log value of

$$\prod_{k=2}^{\infty} \zeta(k)^{-\epsilon_k}$$

and proves that this product is an equivalent form of the product given above. Using PARI, we computed the empirical density among the first two hundred thousand primes for which $K$ has minimal index mod $p$ to be

$$0.05176.$$  

**Lemma 5.5.** If $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_m})$ has odd class number, then in fact each $d_i = p_i$ is a prime number with $p_i \equiv 1 \mod 4$ for each $i$, except possibly $d_1 = 2$.

**Proof.** Let $p_1, \ldots, p_s$ denote all of the prime factors of the various $d_i$, with $p_1 = 2$ or an odd prime congruent to 1 mod 4, and all other $p_k \equiv 1 \mod 4$. Since by assumption $d_i \nmid d_j$ if $i \neq j$, we know $s \geq m$, with equality holding if and only if each $d_i = p_i$ is a prime number. Now, if $s > m$, then the field $F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_s})$ is a proper field extension of $K$ of degree $2^s$ contained in the genus field $E$ of $K$. Hence $F \subseteq H$, the Hilbert class field of $K$, and so $2 | [C_K]$. This is impossible by assumption, so it must be that $s = m$ and each $d_i = p_i$ is a prime number, as claimed. \hfill \qed

**Theorem 5.6.** If $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_m})$ is a totally real multiquadratic field of degree $n = 2^m$, $m \geq 3$ and the class number of $K$ is odd, then every unit in $K$ has norm 1.

**Proof.** Sketch. Induct on $m$. To prove the base case $m = 3$, assume to the contrary that $K$ contains a unit of norm $-1$. Then by Proposition 5.3, each of the seven elements $\alpha_i = (\sqrt{d_1} \cdots \sqrt{d_i})$ lies in $\mathcal{O}_K^\times$, and one can show that the $\alpha_i \in \mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2$ generate a rank 4 module over $\mathbb{Z}/2\mathbb{Z}$. This fact, combined with Kuroda’s class number formula for $K$ and the assumption that the class number of $K$ is odd, implies that $\mathcal{O}_K^\times = \prod_{i=1}^{7} \mathcal{O}_B^\times$ for $B_i$ the biquadratic subfields of $K$. Using properties of norms, one can deduce from this fact that every unit of $K$ has norm $+1$, a contradiction. The inductive step follows from Proposition 5.2, Lemma 5.5, and the more general fact that in a totally ramified extension $F \subseteq K$, the class number of $F$ divides the class number of $K$. For full details, see [18]. \hfill \qed

It should be noted that there are multiquadratic fields of degree at least eight that do contain units of norm $-1$; one such example is $\mathbb{Q}(\sqrt{5}, \sqrt{13}, \sqrt{37})$, which has class number 2.
6. Application to ray class fields

For a totally real Galois extension $K$ of $\mathbb{Q}$ of degree $n$, let $H$ denote the Hilbert class field of $K$ and let $C_K$ denote the class group of $K$, so that $C_K \cong \text{Gal}(H/K)$. For a prime $p \in \mathbb{Z}$ which splits completely in $K$, consider the ray class field $L_p$ of $K$ of conductor $(p) = pO_K$. The corresponding ray class group $RC(p) \cong \text{Gal}(L_p/K)$ of $L_p/K$ fits into the exact sequence

$$O_K^\times \xrightarrow{\psi_p} (O_K/pO_K)^\times \rightarrow RC(p) \rightarrow C_K \rightarrow 1.$$ 

By exactness, the size of the group $RC(p)$ is $|RC(p)| = |C_K| \left(\frac{(p-1)^n}{|\psi_p(O_K^\times)|}\right)$.

Let $\zeta_p$ denote a primitive $p^{th}$ root of unity and notice $\zeta_p + \zeta_p^{-1} \in \mathbb{R}$. Since $H(\zeta_p + \zeta_p^{-1})$ is an abelian extension of $K$ which is ramified only at primes dividing $pO_K$, $H(\zeta_p + \zeta_p^{-1}) \subseteq L_p$.

**Proposition 6.1.** For a prime $p$ completely split in $K$, $L_p = H(\zeta_p + \zeta_p^{-1})$ if and only if $K$ has minimal index mod $p$.

**Proof.** Since $p$ splits completely in $K/\mathbb{Q}$, $(O_K/pO_K)^\times \cong \prod_{i=1}^n \mathbb{F}_p^\times$. Thus $|RC(p)| = |C_K| \left(\frac{(p-1)^n}{|\psi_p(O_K^\times)|}\right)$, and $|\text{Im}(\psi_p)| = 2(p-1)^{n-1}$ if and only if $|RC(p)| = |C_K| \left(\frac{(p-1)^n}{|\psi_p(O_K^\times)|}\right) = |C_K|(p-1)/2$, or equivalently $[L_p : K] = [H(\zeta_p + \zeta_p^{-1}) : K]$. Since $H(\zeta_p + \zeta_p^{-1}) \subseteq L_p$, this happens if and only if $H(\zeta_p + \zeta_p^{-1}) = L_p$. \hfill $\square$

We can now use Theorem 1.1 to deduce the following.

**Theorem 6.2.** Let $K$ be a totally real multiquadratic field, let $H$ be the Hilbert class field of $K$ and let $\zeta_p$ be a primitive $p^{th}$ root of unity. Then the generalized Riemann hypothesis implies that there is a positive density of primes completely split in $K/\mathbb{Q}$ for which the ray class field $L_p$ of $K$ of conductor $(p) = pO_K$ equals $H(\zeta_p + \zeta_p^{-1})$ if and only if $K$ contains a unit of norm $-1$.

7. Acknowledgments

This article is a summary and generalization of my doctoral research at Northwestern University. I would like to thank Frank Calegari for his guidance, support, and patience throughout this process, as well as his partial support of this research with NSF grants DMS-0701048 and DMS-0846285. I would also like to thank Matt Emerton for helpful conversations and the referees for insightful comments and suggestions. Lastly, I would like to thank the administration and my colleagues at Birmingham-Southern College for support while I completed this project, including partial support from the Faculty Development Committee.

[1] E. Artin. *The collected papers of Emil Artin*. Edited by Serge Lang and John T. Tate. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 1965.

[2] L. Cangelmi and F. Pappalardi. On the $r$-rank Artin conjecture. II. *J. Number Theory*, 75(1):120–132, 1999.
[3] G. Cooke and P. J. Weinberger. On the construction of division chains in algebraic number rings, with applications to SL$_2$. Comm. Algebra, 3:481–524, 1975.

[4] A. Fröhlich and M. J. Taylor. Algebraic number theory. Cambridge studies in advanced mathematics. Cambridge University Press, 1991.

[5] C. Hooley. On Artin’s conjecture. J. Reine Angew. Math., 225:209–220, 1967.

[6] K. Ireland and M. Rosen. A classical introduction to modern number theory, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990.

[7] T. Kubota. Über den bizyklischen biquadratischen Zahlkörper. Nagoya Math. J., 10:65–85, 1956.

[8] S. Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. Nagoya Math. J., 1:1–10, 1950.

[9] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pages 409–464. Academic Press, London, 1977.

[10] H. W. Lenstra, Jr. On Artin’s conjecture and Euclid’s algorithm in global fields. Invent. Math., 42:201–224, 1977.

[11] H. W. Lenstra, Jr., P. Stevenhagen, and P. Moree. Character sums for primitive root densities. Math. Proc. Cambridge Philos. Soc., 157(3):489–511, 2014.

[12] K. R. Matthews. A generalisation of Artin’s conjecture for primitive roots. Acta Arith., 29(2):113–146, 1976.

[13] P. Moree. Approximation of singular series and automata. Manuscripta Math., 101(3):385–399, 2000. With an appendix by Gerhard Niklasch.

[14] A. Mouhib. On the parity of the class number of multiquadratic number fields. J. Number Theory, 129(6):1205–1211, 2009.

[15] M. R. Murty. On Artin’s conjecture. J. Number Theory, 16(2):147–168, 1983.

[16] H. Roskam. A quadratic analogue of Artin’s conjecture on primitive roots. J. Number Theory, 81(1):93–109, 2000.

[17] H. Roskam. Artin’s primitive root conjecture for quadratic fields. J. Théor. Nombres Bordeaux, 14(1):287–324, 2002.
[18] M. E. Stadnik. A multiquadratic field generalization of artin’s conjecture, unabridged. Ph.D. Thesis, Northwestern University, pages 1–110, 2012.

[19] H. Wada. On the class number and the unit group of certain algebraic number fields. J. Fac. Sci. Univ. Tokyo Sect. I, 13:201–209 (1966), 1966.

[20] L. C. Washington. Introduction to cyclotomic fields, volume 83 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997.

[21] P. 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.

[22] Q. Wu. Computing fundamental units in bicyclic biquadratic global fields. J. Ramanujan Math. Soc., 23(4):357–380, 2008.