On a Generalization of Artin's Conjecture for Primitive Roots in Gaussian Integers

Dimitar Chakarov

under the direction of
Yichi Zhang
Department of Mathematics, Massachusetts Institute of Technology

January 15, 2020

Abstract

We propose a generalization of Artin's conjecture on primitive roots to the ring $\mathbb{Z}[i]$ of Gaussian integers. We conjecture that for a fixed $q \in \mathbb{Z}^{+}$, every $a \in \mathbb{Z}[i] \setminus \{\pm i, 0, \pm 1\}$ generates a cyclic subgroup of the multiplicative group $(\mathbb{Z}[i]/\mathfrak{p})^{\times}$ of index $[(\mathbb{Z}[i]/\mathfrak{p})^{\times} : \langle a \rangle/\mathfrak{p}] = q$ for infinitely many prime ideals $\mathfrak{p}$. We prove the conjecture when $a \in \mathbb{Z}$, and in several special cases reduce it either to the classical Artin's conjecture, or to its extension for near-primitive roots, the Golomb's conjecture. We conclude by showing that for every integer a, we have $\sum_{q=1}^{\infty} \delta_{a,q} = 1$, where $\delta_{a,q}$ is density of the prime ideals $\mathfrak{p}$ yielding subgroups of index precisely q.

Summary

Artin's conjecture on primitive roots tells us that every integer number is a primitive root for infinitely many primes. In Golomb's conjecture for near-primitive roots one of the conditions of Artin's problem is relaxed. We consider both conjectures in the ring of the Gaussian integers $\mathbb{Z}[i]$. We prove a special case of our conjecture where we pose the restriction that one of the variables must be an integer instead of a Gaussian integer. We explore several explicit constructions and reduce them to cases of Artin's and Golomb's conjectures. Finally, we show that the sum over all densities of a fixed near-primitive root as the index changes equals one.

1 Introduction

In 1927 the German mathematician Emil Artin [1] conjectured that for every square-free integer $a > 1$, there exist infinitely many primes p such that $a^{p-1} \equiv 1 \pmod{p}$, and $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for every $q \in \mathbb{Z}^+$ such that $p \equiv 1 \pmod{q}$ and $q \neq 1$. Since it was proposed, Artin's conjecture has been widely researched. No significant progress was made, however, until 1967 when Hooley [2] proved the conjecture under the assumptions of the Generalized Riemann Hypothesis. Later Murty [3] extended the result to a family of number fields. Murty and Gupta [4] unconditionally proved that Artin's conjecture holds for infinitely many integers a. Heath-Brown [5] proved that there at most two prime values of a for which the conjecture does not hold. A generalization of Artin's conjecture was formulated by Golomb, which reads essentially as follows: for every integer $a > 1$ that is not a perfect square and every $q \in \mathbb{Z}^+$, there exist infinitely many primes $p \equiv 1 \pmod{q}$ such that $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, and $a^{\frac{p-1}{r}} \not\equiv 1 \pmod{p}$ for every integer $r > q$, such that $p \equiv 1 \pmod{r}$. Franc and Murty [6] partially showed and then Moree [7] completely showed an analogous result to Hooley's result for Golomb's conjecture.

We consider an extension of Golomb's conjecture to the ring of the Gaussian integers $\mathbb{Z}[i]$.

Conjecture 1. *Let $a \in \mathbb{Z}[i] \setminus \{\pm i, 0, \pm 1\}$ and $q \in \mathbb{Z}^+$. For every pair (a, q) with possibly certain restrictions, there exist infinitely many prime ideals $\mathfrak{p} = p\mathbb{Z}[i]$, such that a generates a cyclic subgroup of $(\mathbb{Z}[i]/\mathfrak{p})^\times$ of order $\dfrac{|(\mathbb{Z}[i]/\mathfrak{p})^\times|}{q}$.*

In the context of the versions of Artin's conjecture, the Gaussian integers are of specific interest, since they are both a quadratic field extension and a cyclotomic field. Thus, they allow us to observe properties of both algebraic objects. We examine several explicit constructions in the setting of the conjecture and show how they can be reduced to Golomb's conjecture. We prove a case of Conjecture 1 when $a \in \mathbb{Z}$. We also record several partial results. Finally, we study the density of the set of primes satisfying our conjecture. All results are under the assumptions of the Generalized Riemann Hypothesis (GRH).

Section 2 presents the necessary definitions for our problem and the notation used throughout the paper. In Section 3 we formally outline the established theoretical results, and in Section 4 we show how they directly relate to the generalized problem in $\mathbb{Z}[i]$. Section 5 describes our Density Theorem, which shows how to express the density of the Gaussian primes in terms of Wagstaff's sum functions. In Section 6 we provide a result regarding the sum of the densities over a fixed a for all (a, q).

2 Preliminaries

In this section we review classical notions and results from the algebraic number theory of number fields, particularly focusing on imaginary quadratic fields and cyclotomic extensions. We also reinterpret the definitions of primitive and near-primitive roots in those terms.

Throughout the paper we assume familiarity with fundamental algebraic objects — group, ring, field, ideal — and their standard notation. However, for a quick reference we provide a broad overview in Appendix A. For a detailed introduction to algebraic number theory, we refer the reader to Lidl and Niederreiter's *Introduction to Finite Fields* [8] and Rotman's *Galois Theory* [9].

2.1 Primitive Roots

A nonzero integer a is a *primitive root modulo prime* p if $a^{p-1} \equiv 1 \pmod{p}$ and $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$, for every $q \in \mathbb{Z}^+$ such that $p \equiv 1 \pmod{q}$ and $q \neq 1$. A nonzero integer a is a *near-primitive root modulo prime p of index q* if $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ and $a^{\frac{p-1}{r}} \not\equiv 1 \pmod{p}$, for every integer $r > q$ such that $p \equiv 1 \pmod{r}$. In other words, a is a primitive root modulo p if and only if a is a generator of the multiplicative group of the field of integers modulo p, i.e. the finite group $(\mathbb{Z}/p\mathbb{Z})^\times$; and a is a near-primitive root of index q if and only if it generates a multiplicative subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $\dfrac{p-1}{q}$.

2.2 Gaussian Integers

We denote by $\mathbb{Z}[i]$ the ring of the Gaussian integers. The Gaussian integers consist of all complex numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$. It is straightforward to see that they form a ring and $\mathbb{Z}[i] \subset \mathbb{C}$. For $z \in \mathbb{C}$ let the norm of $z = a + bi$ be $\mathrm{Nm}(z) = z\bar{z} = (a+bi)(a-bi) = a^2 + b^2$. A Gaussian prime p we define as a Gaussian integer such that if $p|ab$ for $a, b \in \mathbb{Z}[i]$, then $p|a$ or $p|b$. The following proposition is a well-known property of the Gaussian primes.

Proposition 1. *A Gaussian integer p is a Gaussian prime if and only if either*

- *$p \in \mathbb{Z}$ and p is a prime of the form $4k + 3$, or*
- *$p \notin \mathbb{Z}$ and $\mathrm{Nm}(p)$ is 2 or a prime number of the form $4k + 1$.*

By $\mathbb{Z}[i]/\mathfrak{p}$ we denote the finite quotient field modulo the Gaussian prime p, where $\mathfrak{p} = p\mathbb{Z}[i]$, with $(\mathbb{Z}[i]/\mathfrak{p})^\times$ being its multiplicative group. Further on, we use the fact that $|(\mathbb{Z}[i]/\mathfrak{p})^\times| = \mathrm{Nm}(p) - 1$.

2.3 Number Fields

The expression F/K denotes a *field extension* F of a field K, i.e. K is a subfield of F. The symbol $[F : K]$ denotes the *degree* of the extension F/K with respect to K. It equals the dimension of F as a vector space over K. In the case of a finite degree extension, the degree equals the smallest integer n such that there are elements $f_1, f_2, \ldots, f_n \in F$ with the property that every $f \in F$ can be expressed in the form $f = \sum_{i=1}^{n} k_i f_i$ for $k_1, k_2, \ldots, k_n \in K$. A finite degree extension of the field of rational numbers $K = \mathbb{Q}$ is called a *number field.* The degrees of a sequence of extensions satisfies the tower law.

Proposition 2. *If $K \subset F \subset E$ are fields with $[E : F]$ and $[F : K]$ finite, then E/K is finite and*

$$[E : K] = [E : F]\,[F : K]\,.$$

We introduce the notion of splitting. Recall that $K[x]$ is the set of polynomials with coefficient in K. We say a polynomial $f(x) \in K[x]$ *splits* over F if it is a product of linear factors in $F[x]$. Moreover, the *splitting field* of $f(x) \in K[x]$ is a field extension F/K in which $f(x)$ splits, while $f(x)$ does not split in any proper subfield F' of F.

The *ring of integers* of an algebraic number field K, denoted $\mathcal{O}_K$, is the set of elements $k \in K$ such that k is a root of a monic polynomial $m_k(x) \in \mathbb{Z}[x]$. A well-known result states that every number field F is of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in F$, and so $F \cong \mathbb{Q}[x]/\langle m_\alpha(x)\rangle$, where $m_\alpha(x)$ is the monic polynomial with integer coefficients of smallest degree having α as a root. Hence, pursuing analogy with the case of splitting for polynomials, one can define the splitting of ideals.

Definition 1. Let p be a prime in the ring of integers $\mathcal{O}_K$ of a number field K and let F/K be a field extension of degree n. The prime p *splits* in F if

$$\mathfrak{p} = p\mathcal{O}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_i,\ i = 1, \ldots, g$ are distinct maximal ideals of $\mathcal{O}_F$ and $g > 1$. Furthermore, $\mathfrak{p}$ is said to *split completely* if $e_i = 1$ for every $i = 1, \ldots, n$ and $g = n$.

2.4 Special Notation

By (a, q) we denote such a and q as in Conjecture 1. By N and $N(x)$ we denote the set of primes that satisfy a set of given conditions over all primes and the primes up to x respectively (in our case these conditions are given by the variations of Artin's conjecture). Their corresponding natural densities (see Appendix B) we denote by δ and $\delta(x)$. By $\mathbb{L}_k/K$ we denote the field extension $K(\zeta_k, \sqrt[k]{a})$, where ζ_k is a k-th root of unity and a belongs to some (a, q). In particular, when $K = \mathbb{Q}[i]$, we just write $\mathbb{L}_k$. With $\mu(n)$ and $\varphi(n)$ we denote the Möbius function and Euler's totient function respectively. We use n_t to denote the biggest power of t dividing n. Note that $n_t = t^{\nu_t(n)}$, where $\nu_t(n)$ denotes the largest e such that $t^e | n$ and $t^{e+1} \nmid n$. In equations, we denote the greatest common divisor and the least common multiple of a and b by $\gcd(a, b)$ and $[a, b]$ respectively.

3 Previous Results

In this section, we outline previously established results that are fundamental to our question. The theorems in this section are all proved under the assumptions of the Generalized Riemann Hypothesis.

3.1 Early Findings

Theorem 1 states Artin's conjecture in the corrected form that Hooley [2] proved. Theorem 2 shows the corrected version of Golomb's conjecture proved by Franc and Murty [6].

Theorem 1. *For every non-square integer $a > 1$, there exist infinitely many primes p, so that it is a primitive root modulo p. Let $a = bc^2$ where b is square-free. Then the natural density (see Appendix B) of the set of satisfactory primes $N_a(x)$ is*

$$\delta_a(x) \sim \beta(b)A\frac{x}{\log x},$$

where A is the Artin constant, defined as

$$A = \prod_q \left(1 - \frac{1}{q(q-1)}\right),$$

for q prime and

$$\beta(b) = \begin{cases} 1 & \textit{for } b \not\equiv 1 \pmod{p}, \\ 1 - \mu(b)\displaystyle\prod_{q|b} \frac{1}{q(q-1)-1} & \textit{for } b \equiv 1 \pmod{p}. \end{cases}$$

Theorem 2. *Let $a = \pm a_0^h$ be a nonzero integer. Let $N_{a,q}(x)$ be the set of primes $p < x$, such that a is a near-primitive root of index q modulo p. Then $\delta_{a,q} = 0$, in the following disjoint cases*

- $2 \nmid q$, $d(a) \mid q$;
- $a > 0$, $2h_2 \mid q_2$, $3 \nmid q$, $3 \mid h$, $d(-3a_0) \mid q$;
- $a < 0$, $h_2 = 1$, $q_2 = 2$, $3 \nmid q$, $3 \mid h$, $d(3a_0) \mid q$;
- $a < 0$, $h_2 = 2$, $q_2 = 2$, $d(2a_0) \mid 2q$;
- $a < 0$, $h_2 = 2$, $q_2 = 4$, $3 \nmid q$, $3 \mid h$, $d(-6a_0) \mid q$;
- $a < 0$, $4h_2 \mid q_2$, $3 \nmid q$, $3 \mid h$, $d(-3a_0) \mid q$,

where $d(n) = n$ if $n \equiv 1 \pmod{4}$, and $d(n) = 4n$ otherwise. In all other cases $\delta_{a,q}$ is positive and

$$\delta_{a,q}(x) \sim \beta(a,q)A\frac{x}{\log x},$$

where A is the Artin constant and $\beta(a,q)$ is a constant depending on a and q.

3.2 Lenstra's Theorem

A general version of Artin's conjecture in terms of a generator of a subgroup of a fixed index modulo a prime ideal was studied by Lenstra in [10]. He proved the following theorem (see Appendix C for theoretical background).

Theorem 3. *Let there be given a field extension K of $\mathbb{Q}$, a finite Galois extension F of K, a subset $C \subset \operatorname{Gal}(F/K)$ which is a union of conjugacy classes, a finitely generated* *subgroup $W \subset K^\times$, and an integer $k > 0$ which is coprime to the characteristic of K. Let $M(K, F, C, W, k)$ be the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which satisfy*

- *the Artin symbol $(F/K, \mathfrak{p}) \subset C$ (see [11] for detailed description of the Artin symbol),*
- $\mathrm{ord}_{\mathfrak{p}}(w) = 0$ *for all $w \in W$,*
- *if $\psi : W \to (K/\mathfrak{p})^\times$ is reduction of W over $\mathfrak{p}$, then the index of $\psi(W)$ in $(K/\mathfrak{p})^\times$ divides k.*

Let $c(n) = |C \cap \mathrm{Gal}(F/F \cap L_n)|$. Then, M has natural density δ_M, given by

$$\delta_M = \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{\left[F \cdot \mathbb{L}_{f(n)}/K : K\right]},$$

where for a prime n, set $f(n)$ equal to the smallest power of n not dividing k, whereas, for a composite n, set $f(n) = \prod_{l|n} f(l)$.

3.3 Wagstaff's Sum Functions

In his research on Artin's conjecture, Wagstaff [12] introduced special sum functions as an efficient intermediary step in the examination of the density $\delta_{a,q}$ of some (a, q) as in Conjecture 1. We describe them briefly. The sum function $S(h, q, m)$ is defined as follows:

$$S(h, q, m) = \sum_{\substack{n=1 \\ m|nq}}^{\infty} \frac{\mu(n) \gcd(nq, h)}{\varphi(nq)nq}.$$

We present several lemmas regarding the behaviour of these sum functions. Lemma 1 is due to Wagstaff [12] and Lemma 2 and 3 are due to Moree [7].

Lemma 1. *Let $M = \dfrac{m}{\gcd(m, q)}$, $H = \dfrac{h}{\gcd(Mq, h)}$ and p be a prime, then,*

$$S(h, q, m) = A\mu(M) \gcd(Mq, h) \prod_{p|\gcd(M,q)} \frac{1}{p^2 - 1} \prod_{\substack{p|M \\ p\nmid q}} \frac{1}{p^2 - p - 1} \prod_{\substack{p|\gcd(H,q) \\ p\nmid M}} \frac{p}{p+1} \prod_{\substack{p|H \\ p\nmid Mq}} \frac{p(p-2)}{p^2 - p - 1},$$

where A is the Artin constant.

Lemma 2. *We have*

$$S(h, q, 1) = \frac{\gcd(q, h)}{t^2} \prod_{\substack{p|q \\ h_p|q_p}} \left(1 + \frac{1}{p}\right) \prod_{p\nmid q} \left(1 - \frac{\gcd(p, h)}{p(p-1)}\right).$$

In particular, $S(h, q, 1) = 0$ if and only if $2|h$ and $2 \nmid q$.

Lemma 3. *Let m be an integer, having square-free odd part. Let h and q be positive integers, with the requirement that q is even if h is even. Then,*

$$S(h, q, m) = S(h, q, 1)E(m_2) \prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{\gcd(p,h)} - 1},$$

where p is prime and

$$E(m_2) = \begin{cases} 1 & \textit{if } m_2 | q_2, \\ -\dfrac{1}{3} & \textit{if } m_2 = q_2 \textit{ and } [2, h_2] \,| q_2, \\ -1 & \textit{if } m_2 = q_2 \textit{ and } [2, h_2] \nmid q_2, \\ 0 & m_2 \nmid q_2. \end{cases}$$

4 Explicit Constructions in $\mathbb{Z}[i]$

This section demonstrates our results in Lemmas 4 through 6 in the cases when a of some (a, q) as in Conjecture 1 is either purely imaginary or an integer. The following result due to Murty [3] is fundamental for our findings:

Theorem 4. *Every Gaussian integer $a \in \mathbb{Z}[i] \setminus \{\pm i, 0, \pm 1\}$ is a generator of $(\mathbb{Z}[i]/\mathfrak{p})^\times$ for infinitely many Gaussian primes p.*

Lemmas 4 and 5 summarize our results for an integer a when the Gaussian prime is either an integer or not.

Lemma 4. *Let the nonzero integer $a \neq \pm 1$ satisfy the conditions of Theorems 1 and 2. Let p be a Gaussian prime with $\mathrm{Im}(p) = 0$, such that the integer a is a near-primitive root of index q modulo p. Then it generates a cyclic subgroup of $(\mathbb{Z}[i]/\mathfrak{p})^\times$ of index $(p+1)q$.*

Lemma 5. *Let the nonzero integer $a \neq \pm 1$ satisfy the conditions of Theorems 1 and 2. Let p be a Gaussian prime with $\mathrm{Im}(p) > 0$. If the integer a is a near-primitive root of index q modulo $\mathrm{Nm}(p)$, then a generates a cyclic subgroup $(\mathbb{Z}[i]/\mathfrak{p})^\times$ of index q.*

Lemma 6 presents a similar result for a purely imaginary ai for $a \in \mathbb{Z}$.

Lemma 6. *Let the nonzero integer $a \neq \pm 1$ be a near-primitive root of index q modulo $p = 4k + 3$ $(k \in \mathbb{Z})$ for a prime p. Let us have a purely imaginary ai. If q is odd, then ai generates a cyclic subgroup of $(\mathbb{Z}[i]/\mathfrak{p})^\times$ of index $\dfrac{q(p+1)}{2}$. If q is even, then ai generates a cyclic subgroup of $(\mathbb{Z}[i]/\mathfrak{p})^\times$ of index $\dfrac{q(p+1)}{4}$.*

5 Main Density Theorem

This section presents our main result concerning Conjecture 1 when a is an integer, i.e. when $\mathrm{Im}(a) = 0$. For the sake of clarity let us define $d(a_0) = a_0$ if $a_0 \equiv 1 \pmod 4$ and $d(a_0) = 4a_0$ otherwise. We set $m = [2h_2, d(a_0)]$ if $a > 0$, and $m = [4h_2, d(a_0)]$ if $a < 0$.

Theorem 5 (Density Theorem)**.** *Let us consider (a, q) as in Conjecture 1, where $a \neq \pm 1$ is a nonzero integer such that $a = \pm a_0^h$ and $a_0 \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Then if $a > 0$,*

$$\delta_{a,q} = S(h, q, 1) + S(h, q, 4) + S(h, q, m) + S(h, q, [4, m]),$$

and if $a < 0$

$$\delta_{a,q} = S(h,q,1) + S(h,q,[4,2h_2]) + S(h,q,m) + S(h,q,[4,m]),$$

where the S-functions are Wagstaff's sum functions.

5.1 Proof

We begin by connecting the general construction in Conjecture 1 with Lenstra's result. Then we consider the case in Theorem 5. It is imperative to note that we work in $\mathbb{Q}[i]$ because $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}[i]}$. Recall that $\mathbb{L}_t = \mathbb{Q}[i](\zeta_t, \sqrt[t]{a})$ for $t \in \mathbb{N}$ and $t > 2$.

Lemma 7. *Let the set $M(K,F,C,W,k)$ be defined as in Theorem 3. For an integer a the set of primes satisfying Conjecture 1 is exactly $M(K,F,C,W,k) = M(\mathbb{Q}[i], \mathbb{L}_q, \mathrm{id}_{\mathbb{L}_q}, \langle a \rangle, q)$. Moreover, it has density*

$$\delta_{a,q} = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{L}_{nq} : \mathbb{Q}[i]]}.$$

Proof. Let N_a be the set of primes satisfying our conjecture. It is straightforward to see that $N_a \subset M(\mathbb{Q}[i], \mathbb{Q}[i], \mathrm{id}_{\mathbb{Q}[i]}, \langle a \rangle, q)$, since this implies that M is the set of prime ideals $\mathfrak{p} \in \mathbb{Q}[i]$, such that the index of a modulo $\mathfrak{p}$ is divisible by q. Let us denote the index of a by k. To enforce equality we need to strengthen the condition on the field extension. We want $q|k$, hence, we want $\mathfrak{p}$ to split completely over $\mathbb{L}_q$. We have

$$a^{\frac{\mathrm{Nm}(\mathfrak{p})-1}{q}} \equiv 1 \pmod{\mathfrak{p}} \iff a \equiv x^q \pmod{\mathfrak{p}},$$

for some $x \in \mathbb{Q}[i]/\mathfrak{p}$. By a principle of Dedekind for prime ideals ([13], Chapter 1, §8, Proposition 25), this is equivalent to $\mathfrak{p}$ splitting completely over $\mathbb{Q}[i](\zeta_q, \sqrt[q]{a}) = \mathbb{L}_q$, since it is the splitting field of the polynomial $g(x) = x^q - a$ with $g \in \mathbb{Q}[i][x]$ and g does not split in any proper subfield of $\mathbb{Q}[i](\zeta_q, \sqrt[q]{a})$. Hence, $N_a = M(\mathbb{Q}[i], \mathbb{L}_q, \mathrm{id}_{\mathbb{L}_q}, \langle a \rangle, q))$. □

Now, we can apply the summation formula from Theorem 3 to the density $\delta_{a,q}$ of the primes satisfying Conjecture 1 for (a,q) as in Conjecture 1. Hence,

$$\delta_{a,q} = \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[\mathbb{L}_{nq} : \mathbb{Q}[i]]}$$

Because $C = \{\mathrm{id}_{L_q}\}$, we get that the constant $c(n) = 1$. After decomposing the index we get

$$\delta_{a,q} = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{L}_{nq} : \mathbb{Q}[i]]} = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}[i](\zeta_{nq}, \sqrt[nq]{a}) : \mathbb{Q}[i](\zeta_{nq})] \cdot [\mathbb{Q}[i](\zeta_{nq}) : \mathbb{Q}[i]]}.$$

Lemma 8 and 9 address the two indices in the denominator separately.

Lemma 8. *If $4|k$, then $[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}[i]] = \dfrac{\varphi(k)}{2}$, and $[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}[i]] = \varphi(k)$ otherwise.*

Proof. If $4|k$, then i is a k-th root of unity. We have $[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}[i]] = \dfrac{[\mathbb{Q}(\zeta_k) : \mathbb{Q}]}{[\mathbb{Q}[i] : \mathbb{Q}]}$. Hence, $[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}[i]] = \dfrac{\varphi(k)}{2}$. Now, if $4 \nmid k$, then i is not a k-th root of unity. Similarly,

$$[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}[i]] = \frac{[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}]}{[\mathbb{Q}[i] : \mathbb{Q}]} = \frac{[\mathbb{Q}(\zeta_{[4,k]}) : \mathbb{Q}]}{[\mathbb{Q}[i] : \mathbb{Q}]}.$$

Hence, $[\mathbb{Q}[i](\zeta_k) : \mathbb{Q}[i]] = \dfrac{\varphi([4,k])}{2} = \varphi(k)$. □

Lemma 9. *Let $a = \pm a_0^h$ and $a, a_0 \in \mathbb{Z}$. Then $[\mathbb{Q}[i](\zeta_k, \sqrt[k]{a}) : \mathbb{Q}[i](\zeta_k)] = \dfrac{k}{\gcd(k,h)\varepsilon(k)}$. If $a > 0$,*

$$\varepsilon(k) = \begin{cases} 2 & 2h_2|k \text{ and } d(a_0)|k \iff m|k \\ 1 & \text{otherwise,} \end{cases}$$

and if $a < 0$,

$$\varepsilon(k) = \begin{cases} 2 & 2h_2|k \text{ and } d(a_0)|k \iff m|k \\ \frac{1}{2} & 4|k \text{ and } 2h_2 \nmid k \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let us first note that the introduction of the constant $\varepsilon(k)$ is due to the fact that $\mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(\zeta_t)$ for some t, which is a direct consequence of the Kronecker-Weber theorem ([13], Chapter X, §3, Corollary 3). Moreover, we know that $\mathbb{Q}(\sqrt[l]{a}) \not\subset \mathbb{Q}(\zeta_t)$ for all $l > 2$ (ibid). Hence, $\varepsilon(k) \leq 2$.

We have $\varepsilon(k) = 2$ if and only if $\mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(\zeta_k)$, therefore, again from Kronecker, we get $d(a)|k$. Furthermore, we want the index to be an integer; hence, $2|\frac{k}{\gcd(k,h)} \iff 2h_2|k$. The only special case occurs when $a < 0$. Since $\sqrt[k]{-1} \notin \mathbb{Q}(\zeta_k)$, when $4|k$ and $k_2 \leq h_2$, we need to have $\varepsilon(k) = \dfrac{1}{2}$ in order to compensate for it. □

Proof of Theorem 5. Combining the summation formula with the two previous lemmas we get the following expression for the density

$$\delta_{a,q} = \sum_{n=1}^{\infty} \frac{\mu(n) \gcd(nq, h)\varepsilon'(nq)}{\varphi(nq)nq}.$$

where $\varepsilon'(nq)$ is a constant term, determined by the values of $\varepsilon(nq)$ in Lemma 9 and the $\dfrac{1}{2}$ coefficient from Lemma 8. Taking into account the divisibility requirements we can express the summation formula in terms of Wagstaff's sum functions as done in the theorem statement. □

5.2 Corollaries

A few corollaries follow from the density formulas in Theorem 5.

Corollary 1. *If $2|h$ and $2 \nmid q$, then $\delta_{a,q} = 0$.*

Proof. Let us note that from Lemma 2, we have $S(h, q, 1) = 0$ if and only if $2|h$ and $2 \nmid q$. Since q is odd, we have

$$S(h,q,4) = \sum_{\substack{n=1 \\ 4|nq}}^{\infty} \frac{\mu(n)\gcd(nq,h)}{\varphi(nq)nq} = \sum_{\substack{n=1 \\ 4|n}}^{\infty} \frac{\mu(n)\gcd(nq,h)}{\varphi(nq)nq} = 0.$$

Since $2|h$, we also get $4|m$, $4|\,[4, 2h_2]$ and $4|\,[4, m]$. Let us consider $S(h, q, m)$. Because $4|m$ and q is odd, we get $S(h, q, m) = 0$ due to $\mu(n) = 0$ for $4|m|n$. We similarly examine $S(h, q, [4, 2h_2]) = 0$ and $S(h, q, [4, m]) = 0$. Hence, for $a > 0$,

$$\delta_{a,q} = S(h,q,1) + S(h,q,4) + S(h,q,m) + S(h,q,[4,m]) = 0,$$

and for $a < 0$,

$$\delta_{a,q} = S(h,q,1) + S(h,q,[4,2h_2]) + S(h,q,m) + S(h,q,[4,m]) = 0.$$

□

Corollary 2. *If h is odd or q is even, then $\delta_{a,q} = S(h, q, 1)\beta(m)$, where if $a > 0$,*

$$\beta(m) = 1 + E(4) + E(m_2)\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{\gcd(p,h)} - 1} + E([4,m]_2)\prod_{\substack{p|[4,m] \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{\gcd(p,h)} - 1},$$

and if $a < 0$,

$$\beta(m) = 1 + E([4,2h_2]_2) + E(m_2)\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{\gcd(p,h)} - 1} + E([4,m]_2)\prod_{\substack{p|[4,m] \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{\gcd(p,h)} - 1}.$$

Proof. We apply Lemma 3 directly. □

Now, building on Corollary 2 we formulate the following theorem describing the zeros of the density $\delta_{a,q}$ (for proof of the different cases see Appendix E).

Theorem 6 (Vanishing of the Density)**.** *Let $d'(a_0) = \dfrac{d(a_0)}{d(a_0)_2}$. The set $N_{a,q}$ has density $\delta_{a,q} = 0$ in the following mutually disjoint cases*

- $2 \nmid q$, $2|h$,
- $q_2 = 2$, $h_2 = 1$, $3 \nmid q$, $3|h$, $d(3a_0)|q$,
- $q_2 = 4$, $h_2 = 2$, $d'(a_0)|q$,
- $a < 0$, $q_2 = 2h_2$, $h_2 > 2$, $3|h$, $d'(a_0)|q$,
- $4h_2|q_2$, $h_2 > 2$, $3 \nmid q$, $3|h$, $d(3a_0)|q$.

6 Sum of Densities

In this section we describe a property of the densities $\delta_{a,q}$ over all positive integers q for a fixed a, which follows from the summation formula, derived from Lemma 7.

Theorem 7. *Let us fix an integer a. Then* $\delta_a := \sum_{q=1}^{\infty} \delta_{a,q} = 1$, *where* $\delta_{a,q}$ *are as in Theorem 5.*

Proof. Let $f(k) = [\mathbb{Q}[i](\zeta_k, \sqrt[k]{a}) : \mathbb{Q}[i]]^{-1}$ and $\tau(t)$ be the number of divisors of t. We have $f(k) \leq \dfrac{4h}{k\varphi(k)}$ due to Lemma 8 and 9. Hence, $f(k) = O(k^{-2+\varepsilon})$ for some $\varepsilon > 0$. Moreover, for $\varepsilon > 0$, we have $\tau(t) = O(t^{\varepsilon})$ when $t \to \infty$. Therefore, the sum $\sum_{k=1}^{\infty} f(k)\tau(k)$ converges. Now, we find that

$$\delta_a = \sum_{q=1}^{\infty} \delta_{a,q} = \sum_{q=1}^{\infty}\sum_{n=1}^{\infty} f(nq)\mu(n)$$

is an absolutely convergent double sum, since

$$\delta_a \leq \sum_{q=1}^{\infty}\sum_{n=1}^{\infty} f(nq)|\mu(n)| \leq \sum_{t=1}^{\infty} f(t)\tau(t).$$

Therefore, $\delta_a = \sum_{t=1}^{\infty} f(t) \sum_{d|t}^{\infty} \mu(d) = f(1) = 1.$ □

7 Conclusion

We have examined a generalization of Artin's conjecture on primitive roots into the field of the Gaussian integers $\mathbb{Z}[i]$. We have shown a connection between several special constructions and already known instances of an Artin-type problem, namely Golomb's conjecture on near-primitive roots. For an integer a we have reduced the problem to finding the non-zero values of a certain arithmetic function. Finally, we have proved a fact about the overall structure of the primes satisfying Conjecture 1.

The next step in this research project would be to study Conjecture 1 when a has a non-zero imaginary part. Another idea would be to generalize our results to an arbitrary quadratic extension $\mathbb{Q}(\sqrt{d})$ or an arbitrary cyclotomic field $\mathbb{Q}(\zeta_k)$ as they are abelian extensions of $\mathbb{Q}$, i.e. their Galois group is abelian, and allow us to utilize the full force of class field theory.

8 Acknowledgements

I would like to sincerely acknowledge my mentor Yichi Zhang for the useful resources and insightful discussions. My deepest gratitude goes to Professor David Vogan for suggesting the topic and meeting with me to discuss our progress and giving invaluable insight. I would also like to express my gratitude to my tutor, Jessica Shi, for thoroughly checking the contents of this paper and revising it. I thank Gary Lee for his helpful comments on the early drafts of the paper. I would like to thank Miles Dillon Edwards, Stanislav Atanasov, Dr. Tanya Khovanova, Rayna Gadzheva, and Sean Elliott for the constructive criticism and the useful advice regarding my writing. I would like to acknowledge Professor David Jerison and Professor Ankur Moitra for providing advice on the topic. I thank the Center for Excellence in Education and the Massachusetts Institute of Technology for hosting the 2019 Research Science Institute, as well as Dr. Amy Sillman, the director of RSI, and Joann P. DiGennaro, the president of CEE, for making it possible for me to conduct this research. I would like to acknowledge my main sponsor—the America for Bulgaria Foundation—and the supporting organizations—the Sts. Cyril and Methodius International Foundation, the American Foundation for Bulgaria, the Eureka Foundation and the Union of Bulgarian Mathematicians—for sponsoring my participation in RSI.

References

[1] E. Artin and S. Lang. *Collected papers.* Springer, 1965.

[2] C. Hooley. On Artin's Conjecture. *Journal für die reine und angewandte Mathematik*, 225:209–220, 1967.

[3] M. Murty. On Artin's Conjecture. *Journal of Number Theory*, 16(2):147–168, 1983.

[4] R. Gupta and M. R. Murty. A Remark on Artin's Conjecture. *Inventiones Mathematicae*, 78(1):127–130, 1984.

[5] D. Heath-Brown. Artin's Conjecture for Primitive Roots. *The Quarterly Journal of Mathematics*, 37(1):27–38, 1986.

[6] M. R. Franc, C.; Murty. On a Generalization of Artin's Conjecture. 4(4):1–12, 2008.

[7] P. Moree. On Golomb's Near-primitive Root Conjecture. 1:1–5, 2009.

[8] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications.* Cambridge University Press, 2nd edition, 1996.

[9] J. Rotman. *Galois Theory.* Universitext. Springer New York, New York, NY, 1998.

[10] H. W. Lenstra. On Artin's Conjecture and Euclid's Algorithm in Global Fields. *Inventiones Mathematicae*, 42(1):201–224, 1977.

[11] F. Lemmermeyer. *Reciprocity Laws.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[12] S. Wagstaff. Pseudoprimes and a Generalization of Artin's Conjecture. *Acta Arithmetica*, 41(2):141–150, 1982.

[13] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics.* Springer New York, New York, NY, 1994.

A General Algebraic Objects

A *group* is a set G closed under an associative binary operation $\circ : G \times G \to G$, such that there is an *identity element* e satisfying $a \circ e = e \circ a = a$, and for every $a \in G$ there is an *inverse element* a' satisfying $a \circ a' = a' \circ a = e$. A group with a commutative binary operation is called an *abelian* group. By $|G|$ we denote the number of elements in the group, also called the *order* of the group. A *generator* of a group G is an element g such that for every $a \in G$ there is some integer j for which $a = g^j$. Moreover, a *generator of index* q of a group G is an element g such that for every element a of a subgroup $G' \subseteq G$ with order $|G'| = \dfrac{|G|}{q}$ there is some integer j such that $a = g^j$.

A *ring* is a set R closed under addition $(+)$ and multiplication $(\times)$, such that R is an abelian group under addition, multiplication is associative, for every non-zero $a \in R$ there is a *multiplicative identity* e satisfying $a \times e = e \times a = a$ and the *distributive law* holds — for every $a, b, c \in R$ we have $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$. An *ideal*, denoted I, is a subset of a ring R, such that I is a subgroup of R under addition and for every $r \in R$ and $i \in I$, it follows that $ir \in I$. An ideal is *prime* if $ab \in I$ implies $a \in I$ or $b \in I$. Finally, a *field* is a set F, such that F is a ring with a *multiplicative inverse* a^{-1} satisfying $a^{-1} \times a = a \times a^{-1} = e$, where e is the multiplicative identity of F. With $\langle a_1, a_2, \ldots, a_n \rangle$ we denote an algebraic object — group, ring, field, ideal — generated by a_1 through a_n.

B Natural Density

Definition 2. Let $A \subseteq \mathbb{Z}$ be a subset of the integers. Let $N(x)$ denote the elements $a \in A$ such that $a \leq x$, then the *natural density* δ of A is defined to be

$$\frac{|N(x)|}{x} \sim \delta,$$

as $x \to \infty$ provided that the limit exists.

In other words, the natural density is a way of measuring how large a subset of the integers is. It is clear from the definition that for the natural density δ satisfies $0 \leq \delta \leq 1$.

Notice that positive natural density implies the infinite order of the subset, however, a zero density does not directly lead to a finite order. For example, the set of prime integers has natural density δ equal to zero. This is a direct consequence of the Prime Number Theorem, which tells us that the number of primes up to a fixed x, denoted $\pi(x)$, is $\pi(x) \sim \dfrac{x}{\log(x)}$. Hence, $\delta = \lim_{x\to\infty} \dfrac{1}{\log(x)} = 0$.

C Theoretical Background of Theorem 3

Here we outline the necessary theoretical background needed to fully grasp Theorem 3. We refer the reader to Rotman's *Galois Theory* [9] and Lang's *Algebraic Number Theory* [13] for a more in-depth overview of the presented theory.

Definition 3. An extension F/K is *normal* if every polynomial $f(x) \in K[x]$ either has no roots in L or splits into linear factors over L.

Definition 4. An extension F/K is *separable* if for every $f \in F$ the minimal polynomial of f in K — the polynomial of least degree for which f is root — has no two equal roots over K.

Separability is automatic for all fields of characteristic zero; in particular, all extensions of number fields are separable.

Definition 5. A field extension F/K is a *Galois extension* if and only if it is both normal and separable.

Definition 6. For a Galois extension F/K, the *Galois group*, denoted $\mathrm{Gal}(F/K)$, is the group of automorphisms $\sigma : F \to F$, such that $\sigma(k) = k$ for every $k \in K$.

Definition 7. Let G be a group. Two elements $a, b \in G$ are conjugates if there exists an element $g \in G$ such that $gag^{-1} = b$. The equivalence class that contains the element $a \in G$ is defined as

$$Cl(a) = \{b \in G \mid \exists g \in G \text{ s.t.} b = gag^{-1}\}.$$

Moreover, $Cl(a)$ is called the *conjugacy class* of a.

Definition 8. Let F/K be a finite extension of number fields and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_F$. We say that $\mathfrak{p}$ is *unramified* in K if in the prime ideal decomposition

$$\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_g^{e_g}$$

all e_i equal to 1.

It is a classical result that in a finite extension of number fields all but finitely many primes are unramified. The ramified primes are precisely these dividing the discriminant of the extension.

Definition 9 ([11])**.** Given a number field K, a Galois extension field F, and prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and $\mathfrak{P}$ of $\mathcal{O}_F$ unramified over $\mathfrak{p}$, there exists a unique element $\sigma = (F/K, \mathfrak{P})$, denoted the *Artin symbol*, of the Galois group $\mathrm{Gal}(F/K)$ such that for every element $f \in F$, we have

$$\sigma(f) = f^{\mathrm{Nm}(\mathfrak{p})} \pmod{\mathfrak{P}},$$

where $\mathrm{Nm}(\mathfrak{p})$ is the norm of the prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.

The Artin symbols $(F/K, \mathfrak{P})$ and $(F/K, \mathfrak{P}')$ for two distinct primes $\mathfrak{P}$ and $\mathfrak{P}'$ lying over $\mathfrak{p}$ are conjugate inside $\mathrm{Gal}(F/K)$. Particularly, if F/K is an abelian extension of K — namely, its Galois group is abelian — then $(F/K, \mathfrak{P})$ depends only on the prime ideal $\mathfrak{p}$ (and not on the choice of a prime $\mathfrak{P}$ above), so we may denote it by $(F/K, \mathfrak{p})$.

D Proofs of Lemma 4, 5 and 6

Proof of Lemma 4. Since $\mathrm{Im}(a) = 0$, a is an integer. Hence, a is a generator of index q for infinitely many integer primes with $\langle a \rangle \subset \mathbb{Z}/p\mathbb{Z}$ and $|\langle a \rangle| = \dfrac{|\mathbb{Z}/p\mathbb{Z}|}{q}$. The desired result follows from $\langle a \rangle$ also being a subgroup of $(\mathbb{Z}[i]/\mathfrak{p})^\times$ with order

$$\frac{q\,|(\mathbb{Z}[i]/\mathfrak{p})^\times|}{|\mathbb{Z}/p\mathbb{Z}|} = \frac{q(p^2-1)}{p-1} = q(p+1).$$

□

Proof of Lemma 5. First, because $p = x + yi$ is a prime with positive imaginary part, it follows that $\mathrm{Nm}(p) = x^2 + y^2 = 4k + 1 = l$, where $k \in \mathbb{Z}$ and l is an integer prime. Now, we seek to show

$$a^{\frac{l-1}{q}} \equiv 1 \pmod{p}.$$

This is equivalent to showing that $a^{\frac{l-1}{q}} = pz + 1$ for some appropriate $z \in \mathbb{Z}[i]$. After multiplying with the conjugate of p and taking into account that l is a prime number, we get that

$$(x - yi)\left(a^{\frac{l-1}{q}} - 1\right) \equiv 0 \pmod{l}.$$

Since l is an integer and both the real and the imaginary parts need to be divisible by l. Hence, the desired result is, in fact, equivalent to $a^{\frac{l-1}{q}} \equiv 1 \pmod{l}$. The latter is true by the assumption that a is a near-primitive root of index q modulo l. □

Proof of Lemma 6. Since a is an integer, the powers of ai alternate between the imaginary and the real axis. Hence, ai is a generator of a subgroup of the union of the groups $(\mathbb{Z}/p\mathbb{Z})^\times$ and $i(\mathbb{Z}/p\mathbb{Z})^\times$, whose order is $2(p-1)$. Recall that $|(\mathbb{Z}[i]/\mathfrak{p})^\times| = p^2 - 1 = (p-1)(p+1)$. From $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, we get that q is either odd or even with $4 \nmid q$. If q is odd, then $(ai)^{\frac{2(p-1)}{q}} \equiv 1 \pmod{p}$ with $\dfrac{2(p-1)}{q}$ being the smallest power satisfying the equivalence. Hence, ai is a near-primitive root of index $\dfrac{q(p+1)}{2}$. If q is even, for the imaginary term to vanish, we need 4 to divide the power. Similarly, we get $(ai)^{\frac{4(p-1)}{q}} \equiv 1 \pmod{p}$ with $\dfrac{2(p-1)}{q}$ being the smallest power satisfying the equivalence. Hence, ai is a near-primitive root of index $\dfrac{q(p+1)}{4}$. □

E Proof of Theorem 6

We use the result from Corollary 2. We note that

$$\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{(p,h)}-1} = \begin{cases} 1, & \text{if } d'(a_0)|q, \\ -1, & \text{if } d(3a_0)|q,\ 3\nmid q,\ 3|h, \\ (-1,1), & \text{otherwise.} \end{cases}$$

The case $(2\nmid q,\ 2|h)$**.** This is just the statement in Lemma 1. Hence, $\delta_{a,q}=0$.
The case $(q_2=2,\ h_2=1,\ 3\nmid q,\ 3|h,\ d(3a_0)|q)$**.** Since $E(4)=E([4,2h_2])=0$ for $h_2=1$ and $q_2=2$, we can examine the cases $a>0$ and $a<0$ simultaneously. By the assumptions in the case, we get

$$\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{(p,h)}-1} = -1.$$

Moreover, $E(m_2)=1$ and $E([4,m_2])=0$ because $q_2=2$ and $h_2=1$. Hence, $\delta_{a,q}=0$.
The case $(q_2=4,\ h_2=2,\ d'(a_0)|q)$**.** Due to $d'(a_0)|q$, we have

$$\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{(p,h)}-1} = 1.$$

Moreover, $E(4)=E([4,2h_2])=E(m_2)=E([4,m_2])=-\frac{1}{3}$ because $q_2=4$ and $2h_2=4$. Hence, after plugging these values, we get $\delta_{a,q}=0$.
The case $(a<0,\ q_2=2h_2,\ h_2>2,\ d'(a_0)|q)$**.** Due to $d'(a_0)|q$, we have

$$\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{(p,h)}-1} = 1.$$

Moreover, $E([4,2h_2])=E(m_2)=E([4,m_2])=-\frac{1}{3}$ because $q_2=2h_2$ and $h_2\geq 4$. Thus, the density $\delta_{a,q}=0$.
The case $(4h_2|q_2,\ h_2>2,\ 3\nmid q,\ 3|h,\ d(3a_0)|q)$**.** Due to $3\nmid q$, $3|h$, $d(3a_0)|q$, we have

$$\prod_{\substack{p|m \\ p\nmid q}} \frac{-1}{\frac{p(p-1)}{(p,h)}-1} = -1.$$

We have $E(4)=E([4,2h_2])=1$ and $E([4,m_2])=E([4,m_2])=1$ because $4h_2|q_2$ and $h_2\geq 4$. Thus, the density $\delta_{a,q}=0$.