Recovering Short Generators of Principal Fractional Ideals in Cyclotomic Fields of Conductor $p^\alpha q^\beta$

Patrick Holzer[1], Thomas Wunderer[1], and Johannes A. Buchmann[1⋆]

TU Darmstadt
patrick.holzer@stud.tu-darmstadt.de, twunderer@cdc.informatik.tu-darmstadt.de,
buchmann@cdc.informatik.tu-darmstadt.de

Abstract. Several recent cryptographic constructions – including a public key encryption scheme, a fully homomorphic encryption scheme, and a candidate multilinear map construction – rely on the hardness of the *short generator principal ideal problem* (SG-PIP): given a $\mathbb{Z}$-basis of some principal (fractional) ideal in an algebraic number field that is guaranteed to have an exceptionally short generator with respect to the logarithmic embedding, find a shortest generator of the principal ideal. The folklore approach to solve this problem is to split it into two subproblems. First, recover some arbitrary generator of the ideal, which is known as the *principal ideal problem (PIP)*. Second, solve a bounded distance decoding (BDD) problem in the *log-unit lattice* to transform this arbitrary generator into a shortest generator of the ideal. The first problem, i.e., solving the PIP, is known to be solvable in polynomial time on *quantum* computers for arbitrary number fields under the *generalized Riemann hypothesis* due to Biasse and Song. Cramer, Ducas, Peikert, and Regev showed, based on the work of Campbell, Groves, and Shepherd, that the second problem can be solved in polynomial time on *classical* computers for *cyclotomic number fields of prime-power conductor*.
In this work, we extend the work of Cramer, Ducas, Peikert, and Regev to cyclotomic number fields $K = \mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$, where p, q are distinct odd primes.
In more detail, we show that the second problem can be solved in classical polynomial time (with quantum polynomial time precomputation) under some sufficient conditions, if (p, q) is an (α, β)-*generator prime pair*, a new notion introduced in this work. We further provide experimental evidence that suggests that roughly 35% of all prime pairs are (α, β)-generator prime pairs for all α and β. Combined with the work of Biasse and Song our results show that under sufficient conditions the SG-PIP can be solved in quantum polynomial time in cyclotomic number fields of composite conductor of the form $p^\alpha q^\beta$.

Keywords: Lattice-based cryptography, principal ideal lattices, SG-PIP, SVP, key recovery, cryptanalysis.

1 Introduction

Modern cryptographic schemes such as RSA and the Diffie-Hellmann protocol rely on the conjectured hardness of integer factorization and the difficulty of finding discrete logarithms in certain groups. However, in 1999, Shor [33] presented a quantum algorithm that can solve these problems in polynomial time, rendering these systems insecure in the face of the possible future existence of large scale quantum computers. This threat has lead to a new field of research called post-quantum cryptography [23] which is resistant against quantum adversaries. Many of today's promising post-quantum schemes are lattice-based (see, e.g., [30,20,1,15,11,31,29,16]), i.e., their security relies on

[⋆] This research was supported by the DFG as part of project P1 within the CRC 1119 CROSSING.

the hardness of lattice problems such as finding a shortest non-zero vector of a lattice, for which no efficient quantum algorithm is known. In order to boost the efficiency or achieve additional functionality, more structured lattices have been taken into consideration, for example lattices induced by ideals or even principal ideals in certain rings, called *ideal lattices* [21,22]. Some recent cryptographic constructions – including a public key encryption scheme [7], a fully homomorphic encryption scheme [35], and a candidate multilinear map construction [13] – rely on the hardness of the *short generator principal ideal problem* (*SG-PIP*) [9]: Given a $\mathbb{Z}$-basis of a principal fractional ideal $\mathfrak{a}$ in some algebraic number field K that is guaranteed to have an exceptionally short generator with respect to the logarithmic embedding, find a shortest generator of the principal ideal $\mathfrak{a}$.

The folklore approach to solve this problem, as sketched by Bernstein [3] and Campbell, Groves, and Shepherd [7] is to split it into the following two problems.

1. Recover some arbitrary generator $g' \in K$ of the ideal $\mathfrak{a}$, which is known as the *principal ideal problem (PIP)*.
2. Transform this generator into some shortest generator. In more detail, let $g = ug'$ for some unit $u \in \mathcal{O}_K^\times$ be a shortest generator of $\mathfrak{a}$ with respect to the logarithmic embedding. In this case it holds that $\mathrm{Log}(g') \in \mathrm{Log}(g) + \mathrm{Log}(\mathcal{O}_K^\times)$, where Log denotes the logarithmic embedding. Since $\mathrm{Log}(g)$ is short, we can therefore find $\mathrm{Log}(g)$ (and hence g) by solving a closest vector problem in the *Dirichlet log-unit lattice* $\mathrm{Log}(\mathcal{O}_K^\times)$.

The best known classical algorithm for solving the principal ideal problem is the algorithm of Biasse and Fieker [4], whose running time is subexponential in $n = [K : \mathbb{Q}]$. In [7,5,12], a quantum algorithm with polynomial running time in n was described for cyclotomic fields $K = \mathbb{Q}(\xi_m)$ of prime-power conductor $m = p^\alpha$. If we assume that the *generalized Riemann hypothesis* is true, there is an efficient quantum algorithm for solving the principal ideal problem in arbitrary algebraic number fields, see [6].

Following the sketch of Campbell, Groves, and Shepherd [7], Cramer, Ducas, Peikert, and Regev [9] proved that the second problem can be solved in classical polynomial time for cyclotomic fields $K = \mathbb{Q}(\xi_m)$ of prime-power conductor $m = p^\alpha$, under some conjecture concerning the class number h_m^+ of $K^+ = \mathbb{Q}(\xi_m + \xi_m^{-1})$. The crucial part of their strategy to solve the problem relies on the fact that the units $\frac{\xi_m^j - 1}{\xi_m - 1} \in \mathbb{Z}[\xi_m]^\times$ for $j \in {}^{\mathbb{Z}_m}\!/\!_{\{\pm 1\}}$ form a well suited basis of the so called *cyclotomic units*, a subgroup of finite index in the unit group $\mathcal{O}_K^\times = \mathbb{Z}[\xi_m]^\times$ in the prime-power case $m = p^\alpha$. The success of their algorithm relies on the following two facts.

1. The index of the group of cyclotomic units in $\mathbb{Z}[\xi_m]^\times$ is sufficiently small, i.e., bounded by some constant (or at least by some polynomial in $n = \varphi(m)$) if m is a prime-power.
2. The norm of the dual vectors $\mathrm{Log}\left(\frac{\xi_m^j - 1}{\xi_m - 1}\right)^*$ for all $j \in {}^{\mathbb{Z}_m}\!/\!_{\{\pm 1\}}$ is small enough if m is a prime-power.

The proofs given in [9] heavily use that the underlying cyclotomic number fields have prime-power conductor. For instance, it is known that if the conductor has at least four distinct prime factors, the group generated by the units $\frac{\xi_m^j - 1}{\xi_m - 1} \in \mathbb{Z}[\xi_m]^\times$ for $j \in {}^{\mathbb{Z}_m}\!/\!_{\{\pm 1\}}$ has infinite index in the full unit group, hence in this case the first necessary condition is not satisfied.

In this work, we extend the work of Cramer, Ducas, Peikert, and Regev to cyclotomic number fields $K = \mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$, where p, q are distinct odd primes. As in the prime-power case, we investigate if the units $\frac{\xi_m^j - 1}{\xi_m - 1} \in \mathcal{O}_K^\times = \mathbb{Z}[\xi_m]^\times$ for $j \in {}^{\mathbb{Z}_m}\!/\!_{\{\pm 1\}}$ are well suited to solve the BDD problem in the log-unit lattice and hence recover some shortest generator. In particular, we examine if the group generated by these units has small enough finite index in $\mathcal{O}_K^\times$ and if the norm of the dual vectors of these units in the logarithmic embedding is sufficiently small. We show that (under some conditions) for cyclotomic number fields of conductor $m = p^\alpha q^\beta$, both of these properties are satisfied for these units if (p, q) is an (α, β)-*generator prime pair*, a new notion introduced in this work. We further provide experimental evidence that suggests that roughly 35% of prime pairs are (α, β)-generator prime pairs for all α and β. Combined with the results of Biasse and Song [6] our results show that under sufficient conditions, the SG-PIP can be solved in classical polynomial time in cyclotomic number fields of composite conductor of the form $p^\alpha q^\beta$ with quantum polynomial time precomputation.

Cryptographic Implications. In consequence, we extend the quantum polynomial time key-recover attacks [7,9] on the cryptographic schemes of [35,13,7] to the case of cyclotomic number fields $\mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$ for (α, β)-generator prime pairs (p, q). Hence, SG-PIP based schemes are broken by quantum computers in this case (assuming the generalized Riemann hypothesis).

Outline. This work is structured as follows. In Section 2, we provide the necessary mathematical background for this work. In Section 3, we sketch the algorithmic approach and sufficient success conditions presented in [9,7,3] to find a shortest generator of some principal fractional ideal, given an arbitrary generator. In Section 4, we derive sufficient conditions, under which the algorithmic approach described in the previous section is successful in the case of cyclotomic fields of conductor $m = p^\alpha q^\beta$. We conclude this work by stating some interesting questions that remain open for future work in Section 5.

2 Preliminaries

We denote the natural numbers without zero by $\mathbb{N} := \{1, 2, 3, \ldots\}$ and the natural numbers including zero by $\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$. The set of primes is denoted by $\mathbb{P}$. We denote the real and imaginary part of a complex number $z \in \mathbb{C}$ by $\Re(z)$ and $\Im(z)$, respectively. We use the common notation "**iff**" for "if and only if".

We denote vectors by lower-case bold letters, e.g., $\mathbf{x} \in \mathbb{R}^n$, and matrices by upper-case bold letters, e.g., $\mathbf{X} \in \mathbb{R}^{n \times m}$. For $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{R}^n$ we write $(\mathbf{x}_1, \ldots, \mathbf{x}_k) =: \mathbf{X} \in \mathbb{R}^{n \times k}$ for the $n \times k$ matrix $\mathbf{X}$ whose columns are the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_k$. The canonical inner product and the Euclidean norm over $\mathbb{R}^n$ are denoted by $\langle \cdot, \cdot \rangle$ and $|| \cdot ||_2$.

The common rounding function is denoted by $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor \in \mathbb{Z}$. For a vector $\mathbf{v} = (v_1, \ldots, v_n)^T \in \mathbb{R}^n$ we define $\lfloor v \rceil := (\lfloor v_1 \rceil, \ldots, \lfloor v_n \rceil)^T \in \mathbb{Z}^n$ component wise.

2.1 Lattices

A **lattice** $\mathcal{L}$ is an additive subgroup of an n-dimensional $\mathbb{R}$-vectorspace V such that there exists $\mathbb{R}$-linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$ with $\mathcal{L} = \mathbb{Z}\mathbf{v}_1 + \ldots + \mathbb{Z}\mathbf{v}_k$. The vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$ are called **basis** of the lattice $\mathcal{L}$. If $V = \mathbb{R}^n$, we write $\mathcal{L}(\mathbf{B}) := \mathbb{Z}\mathbf{b}_1 + \ldots + \mathbb{Z}\mathbf{b}_k$ for the lattice whose basis is given by the columns of a matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$. The **dimension** of a lattice is defined as $\dim \mathcal{L} := k$. A **full rank** lattice is a lattice with $n = k = \dim \mathcal{L}$. A **sublattice** $\mathcal{L}'$ of $\mathcal{L}$ is a lattice with $\mathcal{L}' \subseteq \mathcal{L}$.

The **dual basis** $\mathbf{B}^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_k^*) \in \mathbb{R}^{n \times k}$ of a lattice $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{R}^n$ is defined as the $\mathbb{R}$-basis of $\text{span}(\mathbf{B}) = \mathbf{B} \cdot \mathbb{R}^k$ with $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = \delta_{i,j}$ for all $i, j \in \{1, \ldots, k\}$. In other words, $\mathbf{B}^* \in \mathbb{R}^{n \times k}$ is the unique matrix with the properties

$$\mathbf{B}^T \cdot \mathbf{B}^* = (\mathbf{B}^*)^T \cdot \mathbf{B} = \mathbf{I}_k \text{ and } \text{span}(\mathbf{B}) = \text{span}(\mathbf{B}^*),$$

where $\mathbf{I}_k$ denotes the $k \times k$ identity matrix.

It is easy to see that the unique dual basis $\mathbf{B}^*$ is given by

$$\mathbf{B}^* = \mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}.$$

2.2 Algebraic Number Fields

Let L be a field and $K \subseteq L$ a subfield of L. We write L/K for this field extension and denote the index of K in L by $[L : K] := \dim_K L$ (i.e., the dimension of L as a K-vectorspace).

An **algebraic number field** K is an extension field of $\mathbb{Q}$ of finite index, i.e., $[K : \mathbb{Q}] < \infty$. For an algebraic number field K we define the (finite) group of roots of unity as $\mu(K) := \{x \in K |\ x^n = 1 \text{ for some } n \in \mathbb{N}\}$ and its **ring of integers** $\mathcal{O}_K$ as

$$\mathcal{O}_K := \{\alpha \in K |\ \exists p \in \mathbb{Z}[X] \backslash \{0\} : \ p \text{ is monic and } p(\alpha) = 0\}.$$

We say $\alpha \in K$ is **integral** iff $\alpha \in \mathcal{O}_K$.

W.l.o.g. it is sufficient to consider $K \subseteq \mathbb{C}$ for an algebraic number field K, since there is only one algebraic closure of $\mathbb{Q}$ up to isomorphisms, so we assume $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Note that $\mathcal{O}_K$ is a subring of K, see for example [28, p. 7].

A **principal fractional ideal** in K is a subring of K of the form $g\mathcal{O}_K$ for some $g \in K^\times$.

The **class group** $\text{Cl}_K = {}^{\mathcal{I}_K}/_{\mathcal{P}_K}$ of K is the quotient of the abelian multiplicative group of fractional ideal $\mathcal{I}_K$ and the subgroup of principle fractional ideals $\mathcal{P}_K$. The **class number** h_K of an algebraic number field K is defined as the cardinality of its class group, i.e., $h_K := |\text{Cl}_K| < \infty$, see [28, §3. Ideals].

2.3 Logarithmic Embedding

Let K be an algebraic number field of degree $n = [K : \mathbb{Q}]$. Moreover, let r be the number of real embeddings of K, i.e., homomorphisms of the form $\delta_1, \ldots, \delta_r : K \to \mathbb{R}$, and s the number of non real homomorphisms (up to complex conjugation) $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} \to \mathbb{C}$. Note that $n = r + 2s$ holds. In this case, we call (r, s) the *signature* of the number field K. We define the **logarithmic embedding** as

$$\begin{aligned} \text{Log} : \ & K^\times \to \mathbb{R}^{r+2s} \\ & x \mapsto \big(\log(|\delta_1(x)|), \ldots, \log(|\delta_r(x)|), \log(|\sigma_1(x)|), \ldots, \log(|\overline{\sigma_s}(x)|)\big), \end{aligned}$$

This mapping defines a group homomorphism from the multiplicative group $K^\times$ to the additive group $\mathbb{R}^{r+2s} = \mathbb{R}^n$.

If the number field K has no real embedding, i.e., $n = 2s$, it is sufficient to use the **reduced logarithmic embedding** of $K^\times$:

$$Log_r(x) := \Big(\log\left(|\sigma_1(x)|\right), \ldots, \log\left(|\sigma_s(x)|\right)\Big) \in \mathbb{R}^{n/2}$$

for all $\alpha \in K^\times$, where $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$ are the different embeddings of K into $\mathbb{C}$.

The following is known as *Dirichlet's unit theorem* [28, Theorem (7.3)].

Theorem 2.1. *Let K be an algebraic number field of degree $n = [K : \mathbb{Q}]$ with signature (r, s). The group $\Gamma := Log(\mathcal{O}_K^\times)$ is a lattice of dimension $k := r + s - 1$, orthogonal to the vector $\mathbf{1} := (1, \dots, 1) \in \mathbb{R}^{r+2s}$. We call Γ the **log-unit lattice**.*

Lemma 2.2 ([28, (7.1) Proposition])**.** *For an algebraic number field K the following holds.*

$$ker\left(Log|_{\mathcal{O}_K^\times}\right) = \mu(K).$$

Theorem 2.1 and Lemma 2.2 imply the following corollary.

Corollary 2.3. *Let K be an algebraic number field of degree $n = [K : \mathbb{Q}]$ with signature (r, s). The group of units $\mathcal{O}_K^\times$ is isomorphic to $\mu(K) \times \mathbb{Z}^{r+s-1}$, which means there are units $\eta_1, \dots, \eta_k \in \mathcal{O}_K^\times$ (where $k := r + s - 1$), such that each $\alpha \in \mathcal{O}_K^\times$ can be written as $\alpha = \zeta \eta_1^{e_1} \cdots \eta_k^{e_k}$ with unique $e_1, \dots, e_k \in \mathbb{Z}$ and $\zeta \in \mu(K)$.*

Such sets $\{\eta_1, \dots \eta_k\} \subseteq \mathcal{O}_K^\times$ of multiplicative independent units which generates $\mathcal{O}_K^\times$ up to roots of unity like in Corollary 2.3 are called **fundamental systems of units** of $\mathcal{O}_K$.

Now we are prepared to define what we mean by "short generator" of a principal fractional ideal in an algebraic number field.

Definition 2.4. *Let K be an algebraic number field and $g \in K^\times$. Then $g' \in K^\times$ is called a **shortest generator** of the principal fractional ideal $g\mathcal{O}_K$ if $g'\mathcal{O}_K = g\mathcal{O}_K$ and*

$$||Log(g')||_2 = \min_{u \in \mathcal{O}_K^\times} ||Log(g \cdot u)||_2 = \min_{u \in \mathcal{O}_K^\times} ||Log(g) + Log(u)||_2.$$

This means g' is a generator of $g\mathcal{O}_K$ with minimal norm in the logarithmic embedding.

Note that the minimum in Definition 2.4 exists since $\mathrm{Log}(g) + \mathrm{Log}(\mathcal{O}_K^\times) \subseteq \mathbb{R}^n$ is a discrete subset of $\mathbb{R}^n$, where $n = [K : \mathbb{Q}]$.

2.4 Cyclotomic Fields

A **cyclotomic field** K_m is an algebraic number field of the form $K_m = \mathbb{Q}(\xi_m)$ for some **primitive** m-th root of unity $\xi_m \in \mathbb{C}$, i.e., $\mathrm{ord}(\xi_m) = m$. If $m \not\equiv 2 \mod 4$, the number m is called the **conductor** of K_m.

The field extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$ is Galois with index $[\mathbb{Q}(\xi_m) : \mathbb{Q}] = \varphi(m)$, where $\varphi(\cdot)$ is the Euler totient function (and $\xi_m \in \mathbb{C}$ a primitive m-th root of unity). The automorphisms $\sigma_i(\cdot)$ of $\mathbb{Q}(\xi_m)$ are characterized by $\sigma_i(\xi_m) := \xi_m^i$ for $i \in \mathbb{Z}_m^\times$. From now on we fix $\xi_m := e^{2\pi i/m}$ and $K_m := \mathbb{Q}(\xi_m)$ and define $\mathcal{O}_m := \mathcal{O}_{K_m}$.

If $m \equiv 2 \mod 4$, i.e., $m = 2 \cdot k$ for some odd $k \in \mathbb{N}$, we have $\xi_m = -\xi_k$ and therefore $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_k)$. Hence, w.l.o.g. it is sufficient to assume $m \not\equiv 2 \mod 4$.

We can specify the ring of integers $\mathcal{O}_m$, namely $\mathcal{O}_m = \mathbb{Z}[\xi_m]$ (e.g. [28, Prop. (10.2)]).

The Galois group $\mathrm{Gal}(K_m/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_m^\times$, and for $m \geq 3$ the automorphisms $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ with $i \in \mathbb{Z}_m^\times$ are complex and come in conjugated pairs, i.e., $\sigma_{-i} = \overline{\sigma_i}$.

Lemma 2.5. *For a cyclotomic field K_m we have $\mu(K_m) = \langle \pm\xi_m \rangle = \left\{\pm\xi_m^i \middle|\, i \in \mathbb{Z}\right\}$.*

Proof. Since $(\pm\xi_m)^{2m} = 1$, the inclusion $\mu(K_m) \supseteq \langle \pm\xi_m \rangle$ is clear. To proof the reverse inclusion, we need the fact that finite subgroups of the multiplicative group of a field are cyclic. Hence, let $\eta \in \mu(K_m)$ be a generator of $\mu(K_m)$, i.e., $\mu(K_m) = \langle \eta \rangle$. We have $\eta \in \mu(K_m) \subseteq \mathbb{Q}(\xi_m)$, which yields $\mathbb{Q}(\eta) = \mathbb{Q}(\xi_m)$. This implies $\varphi(t) = \varphi(m)$ and $m|t$ or $2m|t$ for $t := \operatorname{ord}(\eta) = |\mu(K_m)|$, which yields $t = m$ if m is even and $t = 2m$, if m is odd. This yields the claim. □

The m-th cyclotomic polynomial $\Phi_m(X) \in \mathbb{Z}[X]$ is defined as the minimal polynomial of the m-th root of unity $\xi_m \in \mathbb{C}$ over $\mathbb{Q}$. It is given by $\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^\times} \left(X - \xi_m^i\right)$. We need the value of the cyclotomic polynomials in $X = 1$.

Lemma 2.6. *Let $m \in \mathbb{N}$ with $m \geq 2$. Then the following holds.*

$$\Phi_m(1) = \begin{cases} p \ , & \text{if } m = p^l \text{ for some prime } p \text{ and } l \in \mathbb{N} \\ 1 \ , & \text{else.} \end{cases}$$

This lemma is a direct consequence of [14, Corollary 4].

2.5 Circulant Matrices and Characters

We follow along [9, Section 2.2] and present some facts about circulant matrices and characters of finite abelian groups.

Definition 2.7 (Circulant matrices)**.** *Let G be a finite abelian group and $\boldsymbol{a} = (a_g)_{g \in G} \in \mathbb{C}^G$ a complex vector indexed by G. The G-**circulant matrix** associated with $\boldsymbol{a}$ is the $G \times G$ matrix*

$$\boldsymbol{A} := \left(a_{i \cdot j^{-1}}\right)_{(i,j) \in G \times G} \in \mathbb{C}^{G \times G}.$$

Notice that the transposed matrix of a G-circulant matrix $\mathbf{A}$ associated to $\mathbf{a} = (a_g)_{g \in G}$ is again a G-circulant matrix associated to $\mathbf{a}' = (a_{g^{-1}})_{g \in G}$.

Definition 2.8 (Characters)**.** *Let G be a finite abelian group. A **character** of G is a group homomorphism*

$$\chi : G \to \mathbb{S}^1 := \{z \in \mathbb{C} |\ |z| = 1\},$$

*i.e., $\chi(g \cdot h) = \chi(g) \cdot \chi(h)$ for all $g, h \in G$. The set of all characters of G is denoted by $\widehat{G}$ and forms a group with the usual multiplication of functions, i.e., $(\chi \cdot \Psi)(g) := \chi(g) \cdot \Psi(g)$ for all $\chi, \Psi \in \widehat{G}$ and $g \in G$. The inverse of a character $\chi \in \widehat{G}$ as a group element is given by $\overline{\chi}$, the composition of the complex conjugation and χ. The constant character $\chi \equiv 1$ is the identity element of $\widehat{G}$ and is called **trivial character**. Each finite abelian group G is isomorphic to $\widehat{G}$. In particular, $|G| = |\widehat{G}|$, see [37, Lemma 3.1].*

Theorem 2.9. *Let G be a cyclic group of order n with generator $g \in G$. Then all characters of G are given by*

$$\chi_h(b) := \xi_n^{h \cdot \log_g(b)} \quad \textit{for } 0 \leq h \leq n-1,$$

where $\xi_n \in \mathbb{C}$ is a primitive root of unity of order n and $\log_g(b) \in \mathbb{Z}$ with $g^{\log_g(b)} = b \in G$.

Proof. Let $\chi \in \widehat{G}$ be a character, then $1 = \chi(1) = \chi(g^n) = \chi(g)^n$ holds. Therefore $\chi(g)$ has to be an n-th root of unity. It is easy to see that the functions χ_h are well defined and n different characters. Since there are only $|\widehat{G}| = |G| = n$ different characters, that are all characters of G. □

Definition 2.10 (Dirichlet Characters)**.** *A **Dirichlet character** $\chi \mod n$ is a character of the group $G = \mathbb{Z}_n^\times$, for some $n \in \mathbb{N}$. If $n|m$, the character χ of $\mathbb{Z}_n^\times$ induces a character of $\mathbb{Z}_m^\times$ via concatenation of the natural projection $\pi : \mathbb{Z}_n \to \mathbb{Z}_m$ and χ, i.e., $\chi \circ \pi$. The **conductor** of a character $\chi \in \widehat{Z_n^\times}$ is defined as the smallest number $f_\chi \in \mathbb{N}$ with $f_\chi|n$, such that χ is induced by some character $\Psi \in \widehat{\mathbb{Z}_{f_\chi}^\times}$, i.e., $\chi = \Psi \circ \pi$, where $\pi : \mathbb{Z}_n \to \mathbb{Z}_{f_\chi}$ is the natural projection. If $n = f_\chi$ for some character $\chi \mod n$, then χ is called **primitive character**.*

*A character $\chi \in \widehat{\mathbb{Z}_n^\times}$ is said to be **even** if $\chi(-1) = 1$, else we say χ is **odd**. A non-trivial character χ with values in $\mathbb{R}$, i.e., $Im(\chi) \in \{\pm 1\}$, is called **quadratic** (since $\chi^2 \equiv 1$ holds in this case).*

We extend a Dirichlet character $\chi : \mathbb{Z}_n^\times \to \mathbb{S}^1$ of conductor f_χ to a multiplicative function $\chi' : \mathbb{Z} \to \mathbb{S}^1 \cup \{0\}$ by

$$\chi'(z) := \begin{cases} \chi_{f_\chi}(z) \ , & \textit{if } \gcd(z, f_\chi) = 1 \\ 0 \ , & \textit{else,} \end{cases}$$

where $\chi_{f_\chi} : \mathbb{Z}_{f_\chi}^\times \to \mathbb{S}^1$ is a primitive character which induces χ. We just write χ instead of χ', when needed.

We identify characters χ of a finite abelian group G with the complex vector $(\chi(g))_{g\in G} \in \mathbb{C}^G$. This lets us do some geometrical calculations on characters and provides a coherence between circular matrices and characters.

We collect some properties concerning characters. For a proof see [9, Section 2.2] and use the fact, that $G \cong \widehat{G}$ holds for all finite abelian groups G.

Lemma 2.11. *Let G be a finite abelian group. Then the following holds.*

1.) For all $\chi \in \widehat{G}$ we have

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| \ , & \textit{if } \chi \equiv 1 \\ 0 \ , & \textit{else.} \end{cases}$$

2.) All characters $\chi \in \widehat{G}$ have Euclidean norm $||\chi||_2 = \sqrt{\langle \chi, \chi \rangle} = \sqrt{|G|}$.

3.) Different characters $\chi, \Psi \in \widehat{G}$ are pairwise orthogonal, i.e. $\langle \chi, \Psi \rangle = 0$.

4.) For all $g \in G$ we have

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} |G| \ , & \textit{if } g \textit{ is the identity element of } G \\ 0 \ , & \textit{else.} \end{cases}$$

Definition 2.12. *The **circulant matrix** of a finite abelian group G is defined as*

$$\boldsymbol{P}_G := |G|^{-1/2} \cdot (\chi(g))_{(g,\chi)\in G\times\widehat{G}} \in \mathbb{C}^{G\times\widehat{G}}.$$

It follows directly from Lemma 2.11 that $\boldsymbol{P}_G$ is unitary, i.e., $\boldsymbol{P}_G^{-1} = \overline{\boldsymbol{P}_G}^T$.

Lemma 2.13 ([9, Lemma 2.4])**.** *Let G be a finite abelian group and $\boldsymbol{A} \in \mathbb{C}^{G\times G}$ be a complex $G \times G$ matrix. The $\boldsymbol{A}$ is G-circulant if and only if the $\widehat{G} \times \widehat{G}$ matrix $\boldsymbol{P}_G^{-1} \cdot \boldsymbol{A} \cdot \boldsymbol{P}_G$ is diagonal; equivalently the columns of $\boldsymbol{P}_G$ are the eigenvectors of $\boldsymbol{A}$. If $\boldsymbol{A}$ is the G-circulant matrix associated with $\boldsymbol{a} = (a_g)_{g\in G}$, its eigenvalues corresponding to $\chi \in \widehat{G}$ is $\lambda_\chi = \langle \boldsymbol{a}, \chi \rangle = \sum_{g\in G} a_g \cdot \overline{\chi(g)}$.*

The following statement is a direct consequence of the previous lemma.

Theorem 2.14. *Let G be a finite abelian group, $\boldsymbol{a} = (a_g)_{g\in G} \in \mathbb{C}^G$ be a complex vector with associated G-circulant matrix $\boldsymbol{A}$. The norm of the vector $\boldsymbol{a}$ is given by*

$$||\boldsymbol{a}||_2^2 = |G|^{-1} \cdot \sum_{\chi\in\widehat{G}} |\lambda_\chi|^2,$$

where $\lambda_\chi = \langle \boldsymbol{a}, \chi\rangle = \sum_{g\in G} a_g \cdot \overline{\chi}(g)$ is the eigenvalue of $\boldsymbol{A}$ corresponding to the eigenvector χ.

Proof. Since $\mathbf{P}_G$ and therefore $\overline{\mathbf{P}}_G^T$ is unitary, which means that it is norm preserving, we have

$$\begin{aligned} ||\mathbf{a}||_2^2 = \big|\big|\overline{\mathbf{P}}_G^T \cdot \mathbf{a}\big|\big|_2^2 &= \sum_{\chi\in\widehat{G}} \big| \sum_{g\in G} a_g \cdot |G|^{-1/2}\overline{\chi}(g)\big|^2 \\ &= |G|^{-1} \sum_{\chi\in\widehat{G}} |\lambda_\chi|^2. \end{aligned}$$

□

2.6 Dirichlet L-Series

Definition 2.15. *Let χ be any Dirichlet character, then the Dirichlet L-function $L(\cdot,\chi)$ is defined as*

$$L(\cdot,\chi) : \mathbb{H} \to \mathbb{C}, \quad s \mapsto L(s,\chi) := \sum_{n\in\mathbb{N}} \frac{\chi(n)}{n^s},$$

where $\mathbb{H} := \{s \in \mathbb{C} |\ \Re(s) > 1\}$.

Since the sum in the definition is absolutely convergent for every $s \in \mathbb{H}$, the sum converges uniformly on every $\mathbb{H}_t := \{s \in \mathbb{C} |\ \Re(s) > t\}$ for every $t > 1$. Hence, $L(\cdot,\chi)$ is an analytic function on $\mathbb{H}$. If χ is the trivial character mod 1, i.e., $\chi(n) = 1$ for all $n \in \mathbb{Z}$, the Dirichlet L-function $L(\cdot,\chi)$ is given by the Riemann zeta function $\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s}$. If χ is a non-trivial character mod $m \in \mathbb{N}$, the Dirichlet L-function $L(\cdot,\chi)$ can be extended uniquely to the whole complex plane, see for example [27, Theorem 10.7. ff]. Therefore, $L(1,\chi)$ is well defined in this case.

Theorem 2.16 ([27, Theorem 4.9.]). *If χ is a non-trivial character mod $m \in \mathbb{N}$, then*

$$L(1,\chi) \neq 0.$$

Theorem 2.17. *There exists a constant $C > 0$, such that for every non quadratic Dirichlet character χ mod $m \in \mathbb{N}$ of conductor $f_\chi > 1$*

$$|L(1,\chi)| \geq \frac{1}{C\log(f_\chi)},$$

and for every quadratic character χ mod $m \in \mathbb{N}$ of conductor $f_\chi > 1$

$$|L(1,\chi)| \geq \frac{1}{C\sqrt{f_\chi}}.$$

Proof. The first inequality was proven by Landau, see [19, p. 29]. For the second inequality, see [34] or [17] for concrete results on the constant $C > 0$. □

3 General Algorithmic Approach

In this section we sketch the algorithmic approach and sufficient success conditions presented in [9,7,3] to find a shortest generator of some principal fractional ideal, given an arbitrary generator.

A standard approach for recovering a short generator of a principal fractional ideal is shifting this problem to a closest vector problem with requirements to the distance of the target point to the lattice, called **bounded-distance decoding** (**BDD**).

Problem 3.1 (BDD)**.** *Given a lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$ and a target point $\boldsymbol{t} \in span(\boldsymbol{B})$ with the property $\min_{v\in\mathcal{L}} ||\boldsymbol{v} - \boldsymbol{t}||_2 \le r$ for some $r < \frac{1}{2}\lambda_1(\mathcal{L})$, where $\lambda_1(\mathcal{L}) := \min_{v\in\mathcal{L}\setminus\{\boldsymbol{0}\}} ||\boldsymbol{v}||_2$, find the unique vector $\boldsymbol{v} \in \mathcal{L}$ with $||\boldsymbol{v} - \boldsymbol{t}||_2 \le r$.*

We will use the following **Round-off Algorithm** [2] for solving this problem in our setting.

```
Algorithm 1: Round-off Algorithm
Input: $\mathbf{B}, \mathbf{t}$.
Output: A lattice vector $\mathbf{v} \in \mathcal{L}$.
$\mathbf{a} \leftarrow \lfloor (\mathbf{B}^*)^T \cdot \mathbf{t} \rceil$
$\mathbf{v} \leftarrow \mathbf{B} \cdot \mathbf{a}$
return $(\mathbf{v}, \mathbf{a})$
```

Lemma 3.2 (Correctness Round-off Algorithm, [9, Claim 2.1])**.** *Let $\mathcal{L}(\boldsymbol{B}) \subseteq \mathbb{R}^n$ be a lattice and $\boldsymbol{t} := \boldsymbol{v} + \boldsymbol{e} \in \mathbb{R}^n$ for some $\boldsymbol{v} \in \mathcal{L}(\boldsymbol{B})$ and $\boldsymbol{e} \in \mathbb{R}^n$. If $\langle \boldsymbol{e}, \boldsymbol{b}_j^* \rangle \in [-\frac{1}{2}, \frac{1}{2})$ holds for all $j \in \{1, \ldots, k\}$, the Round-off Algorithm 1 outputs $\boldsymbol{v} = \boldsymbol{B} \cdot \boldsymbol{a}$ by input $\boldsymbol{B}, \boldsymbol{t}$.*

Note that in general the condition $\langle \mathbf{b}_j^*, \mathbf{e} \rangle \in \left[-\frac{1}{2}, \frac{1}{2}\right)$ for all $j \in \{1, \ldots, k\}$ does not guarantee that the vector $\mathbf{v}$ is in fact the closest vector in $\mathcal{L}(\mathbf{B})$ to $\mathbf{t} = \mathbf{v} + \mathbf{e}$. Therefore, one needs a "sufficiently good" basis $\boldsymbol{B}$ of the lattice.

Provided that the input basis is sufficiently well suited, Algorithm 2 recovers a shortest generator of a principal fractional ideal in some algebraic number field K.

```
Algorithm 2: Recovering a short generator with given basis of $\mathcal{O}_K^\times$
Input: A generator $g' \in K^\times$ of some principal fractional ideal $\mathfrak{a}$ and $b_1, \ldots, b_k \in \mathcal{O}_K^\times$
  such that $\mathbf{B} := \{\mathrm{Log}(b_1), \ldots, \mathrm{Log}(b_k)\}$ is a basis of $\Gamma = \mathrm{Log}(\mathcal{O}_K^\times)$.
Output: A generator $g_e \in K$ of $\mathfrak{a}$.
$(a_1, \ldots, a_k)^T \leftarrow \lfloor (\mathbf{B}^*)^T \cdot \mathrm{Log}(g') \rceil$ (Round-off-Step)
$u' \leftarrow \prod_{i=1}^{k} b_i^{a_i}$
$g_e \leftarrow {}^{g'}/_{u'}$
return $g_e$
```

Lemma 3.3 (Correctness of Algorithm 2, [9, Theorem 4.1])**.** *Let $\mathfrak{a}$ be a principal fractional ideal in some algebraic number field K of degree $n = [K : \mathbb{Q}]$ with signature (r, s) and $k := r + s - 1$ and let $b_1, \ldots, b_k \in \mathcal{O}_K^\times$ be a fundamental system of units of $\mathcal{O}_K^\times$. Assume that there exists some generator*

$g \in K^\times$ of $\mathfrak{a}$ satisfying

$$\left|\langle Log(g), Log(b_i)^* \rangle\right| < \frac{1}{2} \qquad \text{for all } i \in \{1, \ldots, k\}.$$

Then for any input generator $g' \in K^\times$ of $\mathfrak{a}$ Algorithm 2 outputs a generator g_e of $\mathfrak{a}$ with same norm as g, i.e., $||Log(g)||_2 = ||Log(g_e)||_2$.

Theorem 3.4. *Algorithm 2 has (classical) polynomial running time in $n = [K : \mathbb{Q}]$.*

Proof. Since $k = r + s - 1 \leq n$, the algorithm only computes the $n \times k$ matrix $\mathbf{B}$, the dual basis $\mathbf{B}^*$, which includes computing the inverse of a $k \times k$ matrix, and some matrix and vector multiplications of matrices and vectors of size k, which is all polynomial in n. □

One natural question arises: If we draw a generator $g \in K^\times$ from a distribution D over K (w.l.o.g. we ignore the case $g = 0$), does the condition $\left|\langle \mathrm{Log}(g), \mathrm{Log}(b_i)^* \rangle\right| < \frac{1}{2}$ hold for all $i \in \{1, \ldots, k\}$ with non-negligible probability $\omega > 0$ for a fixed basis $b_1, ..., b_k$? Lemma 3.3 gives rise to the following definition.

Condition 3.5. *Let D be a probability distribution over some algebraic number field K and $M > 0$. If the probability that for all vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in \mathbb{R}^n$ of Euclidean norm 1 orthogonal to the all-one vector $\boldsymbol{1} \in \mathbb{R}^n$ the inequalities*

$$\left|\langle Log(g), \boldsymbol{v}_i \rangle\right| < \frac{1}{2M} \qquad \text{for all } i \in \{1, \ldots, k\}$$

*are satisfied is at least $\omega \in (0, 1)$, where $g \in K$ is drawn from D, we say D **satisfies Condition 3.5 with parameters** M and ω.*

Condition 3.5 can be seen as a sufficient success condition on Algorithm 2, as shown in the following theorem.

Theorem 3.6. *If D is a distribution over an algebraic number field K satisfying Condition 3.5 with parameters $M = \max\{||Log(b_1)^*||_2, \ldots, ||Log(b_k)^*||_2\}$ and $\omega \in (0, 1)$ for the input basis $b_1, ..., b_k \in \mathcal{O}_K^\times$ and $g \in K$ is chosen from D, then for any input generator g' of $\mathfrak{a} = g\mathcal{O}_K$, Algorithm 2 outputs a generator $g_e \in K$ of $\mathfrak{a}$ with Euclidean norm at most the norm of g with probability at least $\omega > 0$.*

Proof. We set $v_i := {}^{\mathrm{Log}(b_i)^*}/_{||\mathrm{Log}(b_i)^*||_2}$, which have norm 1 and are orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^n$, where $n = [K : \mathbb{Q}]$. Since the distribution D satisfies Condition 3.5 with parameters M and $\omega > 0$ for $b_1, ..., b_k \in \mathcal{O}_K^\times$, we conclude that

$$\left|\langle \mathrm{Log}(g), \mathrm{Log}(b_i)^* \rangle\right| = ||\mathrm{Log}(b_i)^*||_2 \cdot \left|\langle \mathrm{Log}(g), \mathbf{v}_i \rangle\right| < M\frac{1}{2M} = \frac{1}{2}$$

holds with probability ω. □

As shown in [9, Section 5] for arbitrary cyclotomic fields $\mathbb{Q}(\xi_m)$ two natural distributions satisfy Condition 3.5 with a not too small parameter $\omega > 0$ for the basis discussed in Section 4.2: The continuous Gaussian and other natural distributions. The former is a consequence of the following theorem about the Gaussian distribution, for more details see [9, 5 Tail Bounds].

Lemma 3.7 ([9, Lemma 5.4.]). *Let $n \in \mathbb{N}$, $X_1, \ldots, X_n, X'_1, \ldots, X'_n$ be i.i.d. $N(0, \sigma^2)$ variables for some $\sigma > 0$, and let $\widehat{X}_i = \left(X_i^2 + (X'_i)^2\right)^{1/2}$ for $i \in \{1, \ldots, n\}$. Then for any set of $l \in \mathbb{N}$ vectors $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(l)} \in \mathbb{R}^n$ of Euclidean norm 1 that are orthogonal to the all-one vector $\boldsymbol{1} \in \mathbb{R}^n$ and every $t \geq C_\sigma$ for some universal constant C_σ (that only depends on σ) it holds that*

$$Pr\left[\exists j : \left|\left\langle \left(\log(\widehat{X}_1), ..., \log(\widehat{X}_n)\right)^T, \boldsymbol{a}^{(j)} \right\rangle\right| \geq t\right] \leq 2l \exp\left(-\frac{t}{4}\right).$$

Applied to our setting of cyclotomic number fields, we obtain that Condition 3.5 is satisfied for Gaussian distributions if the norms of the basis elements in the logarithmic embedding are sufficiently short.

Corollary 3.8. *Let $m \in \mathbb{N}$, $m \geq 3$, $n = \varphi(m)$, and $k = {}^{n}\!/_{2} - 1$. If $M := \max\{||Log(b_j)^*||_2, \ldots, ||Log(b_k)^*||_2\}$ is small enough, i.e., ${}^{1}\!/_{2M} \geq C_\sigma$, Condition 3.5 is satisfied for Gaussian distributions (with standard deviation σ) with parameters M and $\omega(m) = 1 - 2k \exp\left(-\frac{1}{8M}\right)$, if $\omega(m) > 0$.*

There is one issue we did not mentioned yet. Algorithm 2 uses a basis $b_1, \ldots, b_k$ of $\mathcal{O}_K^\times$ (up to roots of unity), i.e., a fundamental set of units, with sufficiently short dual vectors. However, in general such a basis is not known for some algebraic number field K. Instead, for special instances of cyclotomic number fields $K = \mathbb{Q}(\xi_m)$, namely if m is a prime-power or a product of two prime powers (as analyzed in the next section), only a well suited basis $b_1, \ldots, b_k \in \mathcal{O}_m^\times$ of a subgroup F with finite index in $\mathcal{O}_m^\times$ is known. This can be compensated for by computing a fundamental system of units of $\mathcal{O}_K^\times$ and afterwards a set of representatives $u_1, \ldots, u_f \in \mathcal{O}_K^\times$ of ${}^{\mathcal{O}_K^\times}\!/_{\mu(K)F}$, using classical [4] or quantum [12] algorithms. The quantum algorithm has running time polynomial in $n = [K : \mathbb{Q}]$ and $\log(|d_K|)$, where d_K denotes the discriminant of K. Notice, in the case that $K = \mathbb{Q}(\xi_m)$ is a cyclotomic field, we obtain $|d_K| \in O(n \log(m))$ as a direct consequence of [37, Proposition 2.7.]. Hence, the quantum algorithm runs in polynomial time in m. Note that the calculation of the set of representatives $u_1, \ldots, u_f \in \mathcal{O}_K^\times$ of ${}^{\mathcal{O}_K^\times}\!/_{\mu(K)F}$ has to be done only once for each cyclotomic field $K = \mathbb{Q}(\xi_m)$ and can therefore be seen as precomputation cost. If one has computed such a set of representatives $u_1, \ldots, u_f \in \mathcal{O}_K^\times$, we can enumerate over all of them and apply Algorithm 2 for each ${}^{g'}\!/_{u_i}$, increasing the running time only by the factor $f := |{}^{\mathcal{O}_K^\times}\!/_{\mu(K)F}|$. The detailed algorithm if one has precomputed such a set of representatives can be found in the appendix, see Algorithm 3.

In this work, we show that for cyclotomic number fields $\mathbb{Q}(\xi_m)$ the index of the basis presented in Section 4.2 is polynomial in m, if $m = p^\alpha q^\beta$ for some suitable odd primes p and q. This yields a polynomial running time in m of Algorithm 2 in this case.

4 Finding Shortest Generators in Cyclotomic Fields of Conductor $m = p^\alpha q^\beta$

In this section we study the SG-PIP in cyclotomic fields of composite conductor $m = p^\alpha q^\beta$ for distinct odd primes p, q. We first introduce a new notion that is crucial to our analysis, see Subection 4.1. In Subection 4.2, we fix the subgroup of the units and a corresponding basis we are using in our approach for Algorithm 3. In Subection 4.3, we derive sufficient conditions under which the index of this subgroup is sufficiently small for Algorithm 3 to work. In Subection 4.4, we show that under sufficient conditions, our basis of this subgroup is sufficiently well suited for Algorithm 3 to recover a shortest generator, as required by Theorem 3.6. This section is concluded in Subsection 4.5, which puts all the results derived in the previous subsections together, showing that, under sufficient conditions, the SG-PIP can be solved efficiently in cyclotomic fields of conductor $m = p^\alpha q^\beta$.

4.1 Generator Prime Pairs

In the next section we investigate the group generated by the elements $\frac{\xi_m^u - 1}{\xi_m - 1} \in \mathcal{O}_m^\times$ with $j \in \mathbb{Z}_m^\times$ for the case, that $m = p^\alpha q^\beta$ only has two distinct odd prime factors. We show the index of this group in the full group of units is finite iff p is a generator of $\mathbb{Z}_{q^\beta}^\times$ or a square of a generator and q is a generator of $\mathbb{Z}_{p^\alpha}^\times$ or a square of a generator. Therefore, we introduce the following notion and derive several results surrounding it.

Definition 4.1. *Let $\alpha, \beta \in \mathbb{N}$ and $p, q \in \mathbb{P}$ be two distinct odd primes with the following properties:*

i)
- *If $q - 1 \equiv 0 \mod 4$: p is a generator of $\mathbb{Z}_{q^\beta}^\times$.*
- *If $q - 1 \not\equiv 0 \mod 4$: p is a generator of $\mathbb{Z}_{q^\beta}^\times$ or has order $\frac{\varphi(q^\beta)}{2} = q^{\beta-1} \cdot \frac{q-1}{2}$ in $\mathbb{Z}_{q^\beta}^\times$.*

And

ii)
- *If $p - 1 \equiv 0 \mod 4$: q is a generator of $\mathbb{Z}_{p^\alpha}^\times$.*
- *If $p - 1 \not\equiv 0 \mod 4$: q is a generator of $\mathbb{Z}_{p^\alpha}^\times$ or has order $\frac{\varphi(p^\alpha)}{2} = p^{\alpha-1} \cdot \frac{p-1}{2}$ in $\mathbb{Z}_{p^\alpha}^\times$.*

*We call such a pair (p, q) an (α, β)-**generator prime pair** ((α, β)-**GPP**). If (p, q) is an (α, β)-generator prime pair for every $\alpha, \beta \in \mathbb{N}$, we just say that (p, q) is a **generator prime pair (GPP)**.*

Theorem 4.2 ([8, Lemma 1.4.5.])**.** *Let p be an odd prime, and let $g \in \mathbb{Z}$ be a primitive root modulo p. Then either g or $g + p$ is a primitive root modulo every power of p.*

In particular, if $g \in \mathbb{Z}$ is a generator of $\mathbb{Z}_{p^2}^\times$ and therefore also for $\mathbb{Z}_p^\times$, then g is a generator for all $\mathbb{Z}_{p^l}^\times$ with $l \in \mathbb{N}$.

A direct consequence of Theorem 4.2 is that $\mathbb{Z}_{p^l}^\times$ is cyclic for every $l \in \mathbb{N}$ and odd prime number $p \in \mathbb{P}$.

Corollary 4.3. *Let p be an odd prime, $l \in \mathbb{N}$ and $g \in \mathbb{Z}_{p^l}^\times$ be a generator. Then the even Dirichlet characters of $\mathbb{Z}_{p^l}^\times$ are given by*

$$\chi_h(b) := \xi_{\varphi(p^l)}^{h \cdot a(b)} \quad \textit{for } 0 \leq h \leq \varphi(p^l) - 1 \textit{ and } h \textit{ is even},$$

where $\xi_{\varphi(p^l)} \in \mathbb{C}$ is a primitive root of unity of order $\varphi\left(p^l\right)$ and $a(b) \in \mathbb{Z}$ with $g^{a(b)} = b \in \mathbb{Z}_{p^l}^\times$.

Proof. Since $\mathbb{Z}_{p^l}^\times$ is cyclic, there exists a generator $g \in \mathbb{Z}_{p^l}^\times$. Hence, all characters of $\mathbb{Z}_{p^l}^\times$ are given by $\chi_1, \ldots, \chi_{\varphi(p^l)-1}$, where χ_h for $0 \leq h \leq \varphi\left(p^l\right) - 1$ denotes the corresponding character from Theorem 2.9. We only have to prove that χ_h is even iff h is even. Since $g^a \equiv -1 \mod p^l$ for $a = \frac{\varphi(p^l)}{2}$ (because g has order $\varphi\left(p^l\right)$), we have $\chi_h(-1) = \xi_{\varphi(p^l)}^{ah} = (-1)^h = 1$ iff h is even. □

Corollary 4.4. *Let (p, q) be an (α, β)-GPP for some $\alpha, \beta \in \mathbb{N}$ and $\beta \geq 2$. Then (p, q) is an (α, l)-GPP for every $l \in \mathbb{N}$. Analogously, the same results follows if we swap p and q.*

In particular, (p, q) is a GPP iff it is a $(2, 2)$-GPP.

Proof. If p is a generator of $\mathbb{Z}_{q^\beta}^\times$ and therefore also for $\mathbb{Z}_{q^2}^\times$ and $\mathbb{Z}_q^\times$ (here we used $\beta \geq 2$), then p is a generator of $\mathbb{Z}_{q^l}^\times$ for all $l \in \mathbb{N}$ by Theorem 4.2.

Else, the order of p in $\mathbb{Z}_{q^\beta}^\times$ is $\frac{\varphi(q^\beta)}{2}$. Let $g \in \mathbb{Z}$ be a generator of $\mathbb{Z}_{q^\beta}^\times$ with $g^2 \equiv p \mod q^\beta$. Again, g is a generator for all $\mathbb{Z}_{q^l}^\times$ with $l \in \mathbb{N}$. Now, let $a \in \mathbb{Z}$ with $g^a \equiv p \mod q^l$ for some $l \geq \beta \geq 2$. We conclude $g^a \equiv p \equiv g^2 \mod p^\beta$, hence $a \equiv 2 \mod \varphi\left(q^\beta\right)$, which implies $a \equiv 2 \mod \varphi\left(q^2\right) = q \cdot \frac{q-1}{2}$. Since

$$2 = \gcd\left(a, \varphi\left(q^2\right)\right) = \gcd\left(a, \varphi\left(q^l\right)\right)$$

the order of g^a in $\mathbb{Z}_{q^l}^\times$ is $\frac{\varphi\left(q^l\right)}{2}$.

The only case left is $l < \beta$, but since $g^2 \equiv p \mod q^\beta$ implies $g^2 \equiv p \mod q^l$ and g is also a generator of $\mathbb{Z}_{q^l}^\times$, p has order $\frac{\varphi\left(q^l\right)}{2}$ in $\mathbb{Z}_{q^l}^\times$. $\square$

Notation 4.5. *Let $p, q \in \mathbb{P}$ be two distinct odd primes and $\alpha, \beta \in \{0, 1, 2\}$ be maximally chosen, such that (p, q) is an (α, β)-GPP. We denote this by saying that (p, q) is an $(\alpha, \beta)_M$-**generator prime pair**. The M indicates, that α and β are chosen maximally.*

Figure 1 lists an example for each tuple $(\alpha, \beta) \in \{0, 1, 2\}^2$, such that (p, q) is an $(\alpha, \beta)_M$-generator prime pair with $p < q$. As we show in this work, the index of the group generated by the elements $\frac{\xi_m^j - 1}{\xi_m - 1}$ in the full group of units for the case $m = p^\alpha q^\beta$ is finite iff (p, q) is an (α, β)-generator prime pair, if we only consider odd prime factors. Hence, if (p, q) is a generator prime pair, the finiteness of this index only depends on the prime pair (p, q) and not on the exponents $\alpha, \beta \in \mathbb{N}$.

	0	1	2
0	5, 29	53, 59	5, 11
1	3, 37	3, 1006003	3, 17
2	3, 13	3, 11	3, 5

Fig. 1. $(\alpha, \beta)_M$-generator prime pairs

Figure 2 lists the four smallest primes $q > p$ for $p = 3, 5, 7, 11, 13, 17$ such that (p, q) is a generator prime pair.

p	q	p	q	p	q	p	q	p	q	p	q	p	q
3	5	5	17	7	11	11	13	13	37	17	23	19	23
3	7	5	23	7	17	11	17	13	41	17	31	19	29
3	23	5	37	7	23	11	29	13	59	17	37	19	41
3	29	5	47	7	47	11	31	13	67	17	41	19	47

Fig. 2. Generator prime pairs

Figure 3 shows the value of

$$Q(x) := \frac{\text{Number of GPP } (p, q) \text{ with } 2 < p < q \leq x}{\text{Number of Primepairs } (p, q) \text{ with } 2 < p < q \leq x}$$

for $x \in \mathbb{N}$ with $x \geq 5$. It seems reasonable, that being a generator prime pair for two distinct odd primes p, q is a relatively common case, i.e., approximately 35% of all odd prime pairs up to 32600 are generator prime pairs, as Figure 3 shows.

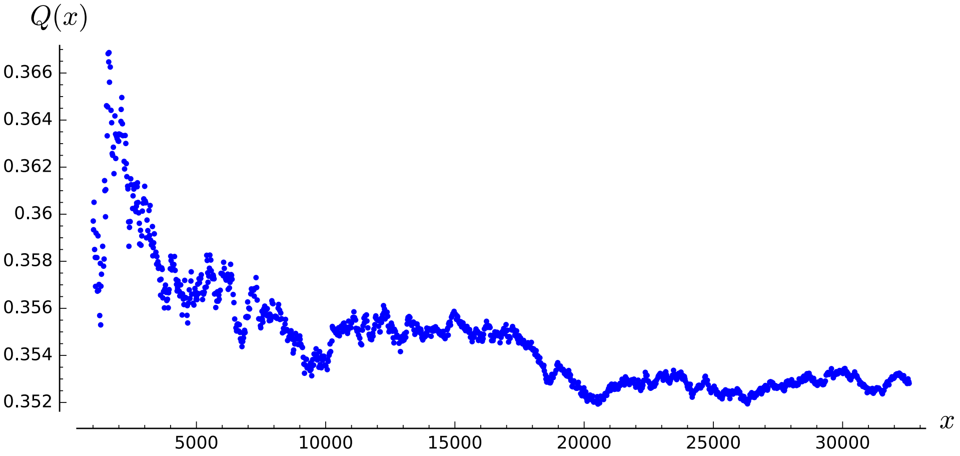

Fig. 3. Values of the quotient $Q(x) = \frac{\text{Number of GPP } (p,q) \text{ with } 2<p<q\leq x}{\text{Number of prime pairs } (p,q) \text{ with } 2<p<q\leq x}$

An interesting fact is that a similar notion of prime pairs was used in the proof of Catalan's conjecture by Preda Mihăilescu [24], namely **double Wieferich prime pairs** (p, q), which satisfy

$$p^{q-1} \equiv 1 \mod q^2 \quad \text{and} \quad q^{p-1} \equiv 1 \mod p^2,$$

see [32, Chapter 1]. They are related to generator prime pairs as follows.

Lemma 4.6. *Let (p, q) be a $(1, 1)_M$-generator prime pair. Then (p, q) is a double Wieferich prime pair.*

Proof. Since (p, q) is a $(1, 1)_M$-generator prime pair, the order of $p \in \mathbb{Z}_{q^2}^\times$ is given by $\frac{q-1}{2}$ or $q - 1$. This implies $p^{q-1} \equiv 1 \mod q^2$. The equation $q^{p-1} \equiv 1 \mod p^2$ follows analogously. □

There are only six known double Wieferich prime pairs, namely $(p, q) = (2, 1093)$, $(3, 1006003)$, $(5, 1645333507)$, $(83, 4871)$, $(911, 318917)$ and $(2903, 18787)$, see [36]. Only two of them are $(1, 1)_M$-generator prime pairs, $(p, q) = (3, 1006003)$ and $(5, 1645333507)$.

4.2 Suitable Units in the Case $m = p^\alpha q^\beta$

Let $m \in \mathbb{N}$ with $m \geq 3$. For the rest of this section, for $j \in \mathbb{Z}_m^\times$ let

$$b_j := \frac{\xi_m^j - 1}{\xi_m - 1} \in \mathcal{O}_m^\times \tag{1}$$

and

$$\mathbf{b}_j := \mathrm{Log}_r(b_j) \in \mathbb{R}^{n/2},$$

where $n = \varphi(m)$. Further, let $G_m := \mathbb{Z}_m^\times/\{\pm 1\}$ (one can identify the group G_m with the set of representatives $\{l \in \mathbb{N} |\ 1 \leq l < \frac{m}{2}$ with $\gcd(l, m) = 1\}$) and let $\mathcal{S}_m$ denote the group generated by $\{b_j |\ j \in G_m \backslash \{1\}\}$ and $\pm\xi_m$, i.e.,

$$\mathcal{S}_m := \big\langle \pm \xi_m,\ b_j |\ j \in G_m \backslash \{1\} \big\rangle = \Big\langle \pm \xi_m,\ b_j |\ 1 < j < \frac{m}{2},\ \gcd(j, m) = 1 \Big\rangle \subseteq \mathcal{O}_m^\times.$$

We collect the vectors $\mathbf{b}_j$ for $j \in G_m\backslash\{1\}$ in the matrix

$$\mathbf{B} := \left(\log\left(\left|\frac{\xi_m^{ij}-1}{\xi_m^i-1}\right|\right)\right)_{\substack{i\in G_m\\ j\in G_m\backslash\{1\}}}. \tag{2}$$

Notice that $b_{-j} = \xi_m^a \cdot b_j$ for some $a \in \mathbb{Z}_m$, hence it is sufficient to consider a set of representatives of $\{b_j|\ j \in G_m\backslash\{1\}\}$ as generators of $\mathcal{S}_m$. The characters of $G_m = \mathbb{Z}_m^\times/\{\pm 1\}$ correspond to the even characters of $\mathbb{Z}_m^\times$ via concatenation with the canonical projection $\mathbb{Z}_m^\times \to \mathbb{Z}_m^\times/\{\pm 1\}$. We indentify the characters of G_m with the even characters of $\mathbb{Z}_m^\times$.

If $[\mathcal{O}_m^\times : \mathcal{S}_m]$ is finite, the elements b_j for $j \in G_m\backslash\{1\}$ have to be a basis of the group $\mathcal{S}_m$, by comparing the $\mathbb{Z}$-rank of $\mathcal{S}_m$ and $\mathcal{O}_m^\times$, which is $\frac{\varphi(m)}{2} - 1 = |G_m\backslash\{1\}|$.

4.3 Index of the Subgroup in the Full Unit Group

We determine the index of $\mathcal{S}_m$ in the full group of units $\mathcal{O}_m^\times$ in the case $m = p^\alpha q^\beta$ with $\alpha, \beta \in \mathbb{N}$ and distinct odd primes p, q. As we show in this work, the index is finite iff (p, q) is an (α, β)-generator prime pair. Moreover, in this case the index is bounded by the product of the class number h_m^+ and a factor, which is linear in m.

The next lemma provides an explicit expression for the index of $\mathcal{S}_m$ in the full group of units $\mathcal{O}_m^\times$, which is a direct consequence of [37, Corollary 8.8.].

Lemma 4.7. *Let $m \in \mathbb{N}$ with $m \geq 3$ and $m \not\equiv 2 \mod 4$. If m is not a prime-power, i.e., has at least two distinct prime factors, the index of $\mathcal{S}_m$ in $\mathcal{O}_m^\times$ is given by*

$$[\mathcal{O}_m^\times : \mathcal{S}_m] = 2h_m^+ \prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}} \prod_{\substack{p|m\\ p\in\mathbb{P}}} (1-\chi(p))$$

if the right hand side is not equal 0, else the index is infinite. The factor h_m^+ is the class number of $\mathbb{Q}(\xi_m)^+ := \mathbb{Q}(\xi_m + \xi_m^{-1})$.

We define

$$\beta_m := \prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}} \prod_{\substack{p|m\\ p\in\mathbb{P}}} (1-\chi(p))$$

for $m \in \mathbb{N}$.

Theorem 4.8. *Let p, q be two distinct odd primes and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$. Then*

$$\beta_m = \frac{\varphi(m)}{4} = \frac{(p-1)(q-1)}{4pq} m$$

iff (p, q) is an (α, β)-GPP, and $\beta_m = 0$ otherwise.

In particular, the index is finite and bounded by $[\mathcal{O}_m^\times : \mathcal{S}_m] = h_m^+ \frac{(p-1)(q-1)}{2pq} m \leq h_m^+ \cdot \frac{m}{2}$, iff (p, q) is an (α, β)-GPP.

Proof. Assume that (p,q) is an (α,β)-generator prime pair. Since m is only divisible by the primes p,q, we obtain

$$\beta_m = \prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}} \prod_{\substack{t|m\\ t\in\mathbb{P}}} (1-\chi(p)) = \prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}} (1-\chi(p))\,(1-\chi(q))\,.$$

If $\chi\in\widehat{\mathbb{Z}_m^\times}$ is an even character of conductor $f_\chi>1$ with $pq|f_\chi$, then $\chi(p)=\chi(q)=0$ and therefore $(1-\chi(p))\,(1-\chi(q))=1$. Hence, we split the product into two products over non-trivial, even Dirichlet characters of $\mathbb{Z}_{p^\alpha}^\times$ and $\mathbb{Z}_{q^\beta}^\times$.

$$\prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}} (1-\chi(p))\,(1-\chi(q)) = \left(\prod_{\substack{\chi\in\widehat{G_{p^\alpha}}\\ \chi\not\equiv 1}} (1-\chi(q))\right)\cdot\left(\prod_{\substack{\chi\in\widehat{G_{q^\beta}}\\ \chi\not\equiv 1}} (1-\chi(p))\right).$$

Hence it is sufficient to prove

$$\prod_{\substack{\chi\in\widehat{G_{q^\beta}}\\ \chi\not\equiv 1}} (1-\chi(p)) = \frac{\varphi\left(q^\beta\right)}{2}.$$

Let g be a generator of $\mathbb{Z}_{q^\beta}^\times$, and $a\in\mathbb{Z}$ with $g^a\equiv p \mod q^\beta$. Since (p,q) is an (α,β)-generator prime pair, we conclude $\gcd\left(a,\frac{\varphi\left(q^\beta\right)}{2}\right)=1$ by comparing the order of p in $\mathbb{Z}_{q^\beta}^\times$, independent whether $q-1\equiv 0 \mod 4$ or $q-1\not\equiv 0 \mod 4$. The even characters of $\mathbb{Z}_{q^\beta}^\times$ are given by Corollary 4.3, which implies

$$\begin{aligned}
\prod_{\substack{\chi\in\widehat{G_{q^\beta}}\\ \chi\not\equiv 1}} (1-\chi(p)) &= \prod_{\substack{1\le h\le\varphi\left(q^\beta\right)-1\\ h \text{ even}}} \left(1-\xi_{\varphi\left(q^\beta\right)}^{ha}\right)\\
&= \prod_{1\le k\le\frac{\varphi\left(q^\beta\right)}{2}-1} \left(1-\xi_{\frac{\varphi\left(q^\beta\right)}{2}}^{ka}\right)\\
&\underset{(1)}{=} \prod_{1\le k\le\frac{\varphi\left(q^\beta\right)}{2}-1} \left(1-\xi_{\frac{\varphi\left(q^\beta\right)}{2}}^{k}\right)\\
&\underset{(2)}{=} \frac{X^{\frac{\varphi\left(q^\beta\right)}{2}}-1}{X-1}\Big|_{X=1}\\
&= \left(X^{\frac{\varphi\left(q^\beta\right)}{2}-1}+X^{\frac{\varphi\left(q^\beta\right)}{2}-2}+\ldots+1\right)\Big|_{X=1} = \frac{\varphi\left(q^\beta\right)}{2},
\end{aligned}$$

where we used in equality *(1)* that multiplying with a is a permutation of $\mathbb{Z}_{\frac{\varphi\left(q^\beta\right)}{2}}$ with $0\cdot a\equiv 0 \mod \frac{\varphi\left(q^\beta\right)}{2}$, since $\gcd\left(a,\frac{\varphi\left(q^\beta\right)}{2}\right)=1$, and in *(2)* we used $X^l-1=\prod_{0\le k\le l-1}\left(X-\xi_l^k\right)$ for all $l\in\mathbb{N}$.

Conversely, assume that (p, q) is not an (α, β)-generator prime pair, i.e., w.l.o.g. p is not a generator of $\mathbb{Z}_{q^\beta}^\times$ and has not order $\frac{\varphi\left(q^\beta\right)}{2}$ in $\mathbb{Z}_{q^\beta}^\times$ if $q - 1 \not\equiv 0 \mod 4$. Again, let g be a generator of $\mathbb{Z}_{q^\beta}^\times$, and $a \in \mathbb{Z}$ with $g^a \equiv p \mod q^l$.

– If $\varphi\left(q^\beta\right) \equiv q - 1 \equiv 0 \mod 4$, we have $\gcd\left(a, \varphi\left(q^\beta\right)\right) > 1$, else p would generate $\mathbb{Z}_{q^\beta}^\times$. Let $t \in \mathbb{P}$ with $t | \gcd\left(a, \varphi\left(q^\beta\right)\right)$. Then $h := \frac{\varphi\left(q^\beta\right)}{t} \in \mathbb{N}$ is even and $1 \leq h \leq \varphi\left(q^\beta\right) - 1$. Notice, this also holds for $t = 2$, since $4 | \varphi\left(q^\beta\right)$. By Corollary 4.3, there is a non-trivial, even Dirichlet character χ_h of $\mathbb{Z}_{q^\beta}^\times$ with

$$\chi_h(p) = \xi_{\varphi(q^\beta)}^{ah} = \xi_{\varphi(q^\beta)}^{\frac{a}{t}\varphi\left(q^\beta\right)} = 1.$$

– If $q - 1 \not\equiv 0 \mod 4$ and therefore $\varphi\left(q^\beta\right) \not\equiv 0 \mod 4$, we have $\gcd\left(a, \varphi\left(q^\beta\right)\right) > 2$, else p would have order $\varphi\left(q^\beta\right)$ or $\frac{\varphi\left(q^\beta\right)}{2}$ in $\mathbb{Z}_{q^\beta}^\times$. Since $4 \nmid \varphi\left(q^\beta\right)$, there is some $t \in \mathbb{P}$ with $t \neq 2$ and $t | \gcd\left(a, \varphi\left(q^\beta\right)\right)$. Then $h := \frac{\varphi\left(q^\beta\right)}{t} \in \mathbb{N}$ is even and $1 \leq h \leq \varphi\left(q^\beta\right) - 1$. Again, by Corollary 4.3, there is a non-trivial, even Dirichlet character χ_h of $\mathbb{Z}_{q^\beta}^\times$ with

$$\chi_h(p) = \xi_{\varphi(q^\beta)}^{ah} = \xi_{\varphi(q^\beta)}^{\frac{a}{t}\varphi\left(q^\beta\right)} = 1.$$

We conclude $\beta_m = 0$ in this case. □

We have proven that the factor β_m is sufficiently small, if $m = p^\alpha q^\beta$ for some (α, β)-generator prime pair (p, q). The second factor of the index $[\mathcal{O}_m^\times : \mathcal{S}_m]$ is given by the class number h_m^+, which has to be sufficiently small, too.

Theorem 4.9 ([25, Theorem 1.1.]). *Let m be a composite integer, $m \not\equiv 2 \mod 4$, and let $\mathbb{Q}(\xi_m)^+ = \mathbb{Q}(\xi_m + \xi_m^{-1})$. Then the class number h_m^+ of $\mathbb{Q}(\xi_m)^+$ is*

$$h_m^+ = \begin{cases} 1 \text{ if } \varphi(m) \leq 116 \text{ and } m \neq 136, 145, 212, \\ 2 \text{ if } m = 136, \\ 2 \text{ if } m = 145, \\ 1 \text{ if } m = 256, \end{cases}$$

where $\varphi(\cdot)$ is the Euler phi function. Furthermore, under the generalized Riemann hypothesis (GRH), $h_{212}^+ = 5$ and $h_{512}^+ = 1$.

Remark 4.10. *In our case, $m = p^\alpha q^\beta$ for some (α, β)-generator prime pair (p, q). Since we want a polynomial running time in m of Algorithm 2 for cyclotomic fields $K_m = \mathbb{Q}(\xi_m)$, we need a polynomial bound of the index $[\mathcal{O}_m^\times : \mathcal{S}_m] = 2h_m^+\beta_m$. The factor $\beta_m \in \mathbb{N}$ is bounded by $\frac{m}{4}$, hence it is sufficient if h_m^+ is bounded by some polynomial in m, if $m = p^\alpha q^\beta$, at least for a fixed generator prime pair (p, q). We do not know if such a bound holds. However, by Theorem 4.9 one could conjecture that the class number h_m^+ is bounded by some polynomial. In [10] this is presented as a reasonable conjecture.*

4.4 Norms of the Basis Elements

We determine the norm of the dual vectors $\mathbf{b}_j^*$ for $j \in G_m \backslash \{1\}$ in the case, that $m = p^\alpha q^\beta$, for some $\alpha, \beta \in \mathbb{N}$ and (p, q) is an (α, β)-generator prime pair. Again, we follow along [9, Chapter 3], but there are some issues with the used methods there, since they only work in the prime-power case. For example, some eigenvalues of the matrix $\mathbf{Z}$ (see below) are equal zero, hence we can not evaluate the norm of the vector associated to the G_m-circulant inverse. Further, the calculation of the eigenvalues in the non-prime-power case is more complicated. As we show in this work, the eigenvalues of $\mathbf{Z}$ corresponding to the non-trivial characters are all non-zero iff (p, q) is an (α, β)-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$.

Let $m \in \mathbb{N}$ with $m \geq 2$. We define

$$z_j := \xi_m^j - 1 \in \mathcal{O}_m$$

for all $j \in \mathbb{Z}_m^\times$, and

$$\mathbf{z}_j := \operatorname{Log}_r(z_j) \in \mathbb{R}^{n/2}$$

for all $j \in G_m$ (again, $n = \varphi(m)$). Notice that $\mathbf{z}_j$ is well defined since $\xi_d^{-j} - 1$ is the complex conjugate of $\xi_d^j - 1$, hence $|\xi_m^{-j} - 1| = |\xi_m^j - 1|$ and therefore $\operatorname{Log}_r(z_j) = \operatorname{Log}_r(z_{-j})$. We collect all the vectors $\mathbf{z}_{j^{-1}}$ for $j \in G_m$ in the matrix $\mathbf{Z} \in \mathbb{R}^{n/2 \times n/2}$, i.e.,

$$\mathbf{Z} := \left(\log\left(\left|\xi_m^{i \cdot j^{-1}} - 1\right|\right)\right)_{i,j \in G_m}.$$

Since the entry with index $(i, j) \in G_m \times G_m$ only depends on $i \cdot j^{-1}$, the matrix $\mathbf{Z}$ is G_m-circulant and associated with $\mathbf{z}_1$. Notice that the vectors $\mathbf{z}_j$ and the matrix $\mathbf{Z}$ only depend on m.

Our first goal is to prove that only the eigenvalue of $\mathbf{Z}$ corresponding to the trivial character of $\mathbb{Z}_m^\times$ is zero, in the case that $m = p^\alpha q^\beta$, for some $\alpha, \beta \in \mathbb{N}$ and distinct primes p and q.

Lemma 4.11. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Then the eigenvalue λ_χ of $\boldsymbol{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is $\lambda_\chi = 0$.*

Proof. By Theorem 2.14, the eigenvalue of the G_m-circulant matrix $\mathbf{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is given by

$$\lambda_\chi = \langle \mathbf{z}_1, 1 \rangle = \frac{1}{2} \sum_{j \in \mathbb{Z}_m^\times} \log\left(\left|\xi_m^j - 1\right|\right) = \frac{1}{2} \log\left(\left| \prod_{j \in \mathbb{Z}_m^\times} \left(\xi_m^j - 1\right) \right|\right) = \frac{1}{2} \log\left(\left|\Phi_m(1)\right|\right) \underset{(1)}{=} 0,$$

where (1) follows from Corollary 2.6. □

Lemma 4.12. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Furthermore, let $\chi \in G_m$ be an even character of conductor $f_\chi > 1$ with $pq | f_\chi$. Then the eigenvalue λ_χ of $\boldsymbol{Z}$ corresponding to χ is given by*

$$\lambda_\chi = \frac{1}{2} \sum_{a \in \mathbb{Z}_{f_\chi}^\times} \overline{\chi}(a) \cdot \log(|1 - \xi_{f_\chi}^a|).$$

Proof. Let $\pi : \mathbb{Z}_m^\times \to \mathbb{Z}_f^\times$ be the canonical projection and $f := f_\chi > 1$ be the conductor of χ. For $a \in \mathbb{Z}_f^\times$ and a fixed integer representative $a' \in \mathbb{Z}$ of $a \in \mathbb{Z}_f^\times$ we have

$$\pi^{-1}(a) = \left\{ a' + k \cdot f \in \mathbb{Z}_m^\times \middle| \ 0 \leq k < \frac{m}{f} \right\}, \tag{3}$$

since $pq|f$ implies $\gcd(a' + k \cdot f, m) = 1$, and the kernel of π has size $\frac{m}{f}$. One can easy see that the $\frac{m}{f}$ different numbers $a' + k \cdot f$ for $0 \leq k < \frac{m}{f}$ are indeed different $\mod m$. Now, by Theorem 2.14, the eigenvalue of the G_m-circulant matrix $\boldsymbol{Z}$ corresponding to χ is given by

$$\begin{aligned}
\lambda_\chi = \langle \mathbf{z}_1, \chi \rangle &= \sum_{j \in G_m} \overline{\chi}(j) \cdot \log\left(\left|\xi_m^j - 1\right|\right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \sum_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(j) = a}} \log\left(\left|1 - \xi_m^j\right|\right) \\
&\underset{(3)}{=} \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\prod_{0 \leq k < \frac{m}{f}} \left|1 - \xi_m^{a' + k \cdot f}\right| \right) \\
&\underset{(\star)}{=} \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left|1 - \xi_f^a\right|\right),
\end{aligned}$$

where we used in $(\star)$ the identity $X^n - Y^n = \prod_{0 \leq k < n} \left(X - \xi_n^k Y\right)$ for $n := \frac{m}{f}$, $X := 1$ and $Y := \xi_m^{a'}$, together with the fact that $\xi_m^{k \cdot f} = \xi_n^k$ and $\xi_f^{a'} = \xi^a$. □

Lemma 4.13. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Furthermore, let $\chi \in G_m$ (i.e., χ is an even character of $\mathbb{Z}_m^\times$) be a character of conductor $f_\chi > 1$ with $q \nmid f_\chi$. Then the eigenvalue λ_χ of $\boldsymbol{Z}$ corresponding to χ is given by*

$$\lambda_\chi = \frac{1}{2}\left(1 - \overline{\chi}(q)\right) \sum_{a \in \mathbb{Z}_{f_\chi}^\times} \overline{\chi}(a) \cdot \log(|1 - \xi_{f_\chi}^a|).$$

Analogously, the same results hold if we swap p and q.

Proof. Let $f := f_\chi > 1$ be the conductor of χ, i.e., $f = p^e$ for some $1 \leq e \leq \alpha$. Further, let $\pi : \mathbb{Z}_m^\times \to \mathbb{Z}_f^\times$ be the canonical projection. For $a \in \mathbb{Z}_f^\times$ and a fixed integer representative $a' \in \mathbb{Z}$ of $a \in \mathbb{Z}_f^\times$ we have

$$\pi^{-1}(a) = \varPsi^{-1}\left(\left\{ a' + k \cdot f \in \mathbb{Z}_{p^\alpha}^\times \middle| \ 0 \leq k < \frac{p^\alpha}{f} \right\} \times \mathbb{Z}_{q^\beta}^\times \right) \subseteq \mathbb{Z}_m^\times \tag{4}$$

by Chinese remainder theorem, where

$$\begin{aligned}
\varPsi : \mathbb{Z}_m &\to \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{q^\beta} \\
a &\mapsto (a \mod p^\alpha, a \mod q^\beta).
\end{aligned}$$

Therefore, the Chinese remainder theorem implies that there are $r_1, r_2 \in \mathbb{Z}$ such that $r_1 q^\beta \equiv 1 \mod p^\alpha$ and $r_2 p^\alpha \equiv 1 \mod q^\beta$, which yields

$$\pi^{-1}(a) = \left\{ (a' + k \cdot f) \cdot r_1 q^\beta + y \cdot r_2 p^\alpha \in \mathbb{Z}_m^\times \middle| \, 0 \leq k < \frac{p^\alpha}{f}, \; y \in \mathbb{Z}_{q^\beta}^\times \right\} \subseteq \mathbb{Z}_m^\times \tag{5}$$

for a fixed integer representative $a' \in \mathbb{Z}$ of $a \in \mathbb{Z}_f^\times$. For $a \in \mathbb{Z}_f^\times$ we have

$$\begin{aligned}
\prod_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(b)=a}} \left(1 - \xi_m^j\right) &= \prod_{y \in \mathbb{Z}_{q^\beta}^\times} \prod_{0 \leq k < \frac{p^\alpha}{f}} \left(1 - \xi_{\frac{p^\alpha}{f}}^{k r_1} \cdot \xi_{q^\beta}^{y r_2} \cdot \xi_{p^\alpha}^{a' r_1}\right) \\
&\underset{(1)}{=} \prod_{y \in \mathbb{Z}_{q^\beta}^\times} \left(1 - \xi_{q^\beta}^{y r_2 \frac{p^\alpha}{f}} \cdot \xi_{p^\alpha}^{a' r_1 \frac{p^\alpha}{f}}\right) \\
&\underset{(2)}{=} \prod_{y \in \mathbb{Z}_{q^\beta}^\times} \left(1 - \xi_{q^\beta}^{y \frac{p^\alpha}{f}} \cdot \xi_f^{a r_1}\right) \\
&\underset{(3)}{=} \frac{1 - \xi_f^{a r_1 q^\beta}}{1 - \xi_f^{a r_1 q^{\beta-1}}} \\
&\underset{(4)}{=} \frac{1 - \xi_f^{a}}{1 - \xi_f^{a r_1 q^{\beta-1}}}.
\end{aligned}$$

In equation (1) we have used again the identity $X^n - Y^n = \prod_{0 \leq k < n} \left(X - \xi_n^k Y\right)$ for $n := \frac{p^\alpha}{f}$, $X := 1$ and $Y := \xi_{q^\beta}^{y r_2} \cdot \xi_{p^\alpha}^{a r_1}$, where $r_1 \in \mathbb{Z}_{\frac{p^\alpha}{f}}^\times$ and therefore multiplication with r_1 is a permutation of $\mathbb{Z}_{\frac{p^\alpha}{f}}$. The same permutation argument implies equation (2), since $r_2 \in \mathbb{Z}_{q^\beta}^\times$. In (3) we have used the identity

$$\prod_{a \in \mathbb{Z}_{q^\beta}^\times} \left(X - \xi_{q^\beta}^a Y\right) = \frac{X^{q^\beta} - Y^{q^\beta}}{X^{q^{\beta-1}} - Y^{q^{\beta-1}}}$$

for $X = 1$ and $Y = \xi_f^{a r_1}$. The hypothesis $r_1 q^\beta \equiv 1 \mod p^\alpha$ implies $r_1 q^\beta \equiv 1 \mod f$ and therefore equation (4). Finally, we calculate the eigenvalue λ_χ.

$$\begin{aligned}
\lambda_\chi = \langle \mathbf{z}_1, \chi \rangle &= \frac{1}{2} \sum_{j \in \mathbb{Z}_m^\times} \overline{\chi}(j) \cdot \log\left(\left| 1 - \xi_m^j \right| \right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \sum_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(j)=a}} \log\left(\left| 1 - \xi_m^j \right| \right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| \prod_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(j)=a}} \left(1 - \xi_m^j\right) \right| \right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| \frac{1 - \xi_f^a}{1 - \xi_f^{a r_1 q^{\beta-1}}} \right| \right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| 1 - \xi_f^a \right| \right) - \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| 1 - \xi_f^{a r_1 q^{\beta-1}} \right| \right) \\
&\underset{(5)}{=} \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| 1 - \xi_f^a \right| \right) - \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a \cdot q) \log\left(\left| 1 - \xi_f^a \right| \right) \\
&= \frac{1}{2}(1 - \overline{\chi}(q)) \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| 1 - \xi_f^a \right| \right),
\end{aligned}$$

where we used in (5) the substitution a for $ar_1q^{\beta-1}$ and the fact, that $r_1 q^\beta \equiv 1 \mod p^\alpha$ implies $r_1 q^{\beta-1} \cdot q \equiv r_1 q^\beta \equiv 1 \mod f$, i.e., q is the multiplicative inverse of $r_1 q^{\beta-1} \mod f$. □

The next theorem provides a connection between the occurring sum in the eigenvalues λ_χ and the Dirichlet L-function.

Theorem 4.14 ([37, Lemma 4.8. and Theorem 4.9.])**.** *Let χ be an even Dirichlet character* mod *$m \in \mathbb{N}$ of conductor $f_\chi > 1$. Then*

$$\Big| \sum_{a \in \mathbb{Z}_{f_\chi}^\times} \overline{\chi}(a) \cdot \log\left(\left| 1 - \xi_{f_\chi}^a \right| \right) \Big| = \sqrt{f_\chi} \cdot |L(1, \chi)|.$$

Theorem 4.15. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Further, let $\chi \in G_m$ be an even Dirichlet character* mod *m of conductor $f_\chi > 1$. Then the eigenvalue $\lambda_\chi = \langle \boldsymbol{z}_1, \chi \rangle$ of $\boldsymbol{Z}$ corresponding to χ is given by*

$$|\lambda_\chi| = \frac{1}{2} \big| \left(1 - \overline{\chi}(p)\right) \left(1 - \overline{\chi}(q)\right) \big| \cdot \sqrt{f_\chi} \cdot |L(1, \chi)|.$$

In particular, if p, q are odd primes, all eigenvalues λ_χ corresponding to some non-trivial even character $\chi \in G_m$ are non-zero iff (p, q) is an (α, β)-generator prime pair.

Proof. If $pq | f_\chi$, then $\chi(p) = \chi(q) = 0$, i.e., $\left(1 - \overline{\chi}(p)\right)\left(1 - \overline{\chi}(q)\right) = 1$. Else, if $f_\chi = p^e$ for some $1 \le e \le \alpha$, then $\chi(p) = 0$, what implies $\left(1 - \overline{\chi}(p)\right)\left(1 - \overline{\chi}(q)\right) = \left(1 - \overline{\chi}(q)\right)$. Analogously follows

$(1-\overline{\chi}(p))\,(1-\overline{\chi}(q)) = (1-\overline{\chi}(p))$, if $f_\chi = q^e$ for some $1 \leq e \leq \beta$. Therefore, Lemma 4.12, Lemma 4.13 and Theorem 4.14 imply

$$|\lambda_\chi| = \frac{1}{2}\big|\,(1-\overline{\chi}(p))\,(1-\overline{\chi}(q))\,\big|\cdot\Big|\sum_{a\in\mathbb{Z}_{f_\chi}^\times}\overline{\chi}(a)\cdot\log\left(\left|1-\xi_{f_\chi}^a\right|\right)\Big| = \frac{1}{2}\big|\,(1-\overline{\chi}(p))\,(1-\overline{\chi}(q))\,\big|\cdot\sqrt{f_\chi}\cdot|L(1,\chi)|.$$

By Theorem 2.16, $L(1,\chi)\neq 0$ holds for all non-trivial characters. Hence, we conclude that $\lambda_\chi = 0$ holds for some non-trivial, even character χ mod m iff

$$0 = \prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}}(1-\overline{\chi}(p))\,(1-\overline{\chi}(q)) = \prod_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}}\prod_{\substack{t|m\\ t\in\mathbb{P}}}(1-\chi(t)) = \beta_m,$$

where we used the fact that concatenation with the complex conjugation is a permutation of $\widehat{G_m}$. By Theorem 4.8, $\beta_m \neq 0$ holds iff (p,q) is an (α,β)-generator prime pair (where $m = p^\alpha q^\beta$). This yields the second claim. □

We are now prepared to express the norm of the dual vectors $\mathbf{b}_j^*$ in terms of the eigenvalues λ_χ. Notice that this is the same result as in the prime-power case, but is more complicated to prove since $\mathbf{Z}$ is not invertible, see [9, Lemma 3.2.].

Lemma 4.16. *Let (p,q) be an (α,β)-generator prime pair, and $m := p^\alpha q^\beta$. Then the norm of $\boldsymbol{b}_j^*$ for all $j\in G_m\backslash\{1\}$ is given by*

$$||\boldsymbol{b}_j^*||_2^2 = |G_m|^{-1}\cdot\sum_{\substack{\chi\in\widehat{G_m}\\ \chi\not\equiv 1}}|\lambda_\chi|^{-2},$$

where $\lambda_\chi = \langle\boldsymbol{z}_1,\chi\rangle$ denotes the eigenvalue of $\boldsymbol{Z}$ corresponding to χ.

In particular, all dual vectors $\boldsymbol{b}_j^*$ have the same norm.

Proof. First, we note that the sum on the right hand side is well defined by Theorem 4.15. Our goal is to prove the claim by defining a "pseudo inverse" $\mathbf{D}$ of $\mathbf{Z}^T$ and show that $\mathbf{b}_j^*$ is the j-th column of $\mathbf{D}$.

For simplification, we fix an order of $\widehat{G_m}$, i.e., $\widehat{G_m} = \{\chi_1,\ldots,\chi_n\}$ with $n = \frac{\varphi(m)}{2}$ and $\chi_1 \equiv 1$ is the trivial character mod m. This allows us to represent $\widehat{G_m}\times\widehat{G_m}$ matrices by $n\times n$ matrices. Notice that the characters χ_j are different from the characters of Theorem 2.9, we only used a similar notation. The order of $\widehat{G_m}$ yields an order of the eigenvalues $\lambda_1,\ldots,\lambda_k$ of $\mathbf{Z}$, where $\lambda_1 = 0$ by Lemma 4.11 and $\lambda_j \neq 0$ for $2\leq j\leq n$ by Theorem 4.15. Since $\mathbf{Z}$ is a G_m-circulant matrix, Lemma 2.13 implies

$$\mathbf{Z} = \mathbf{P}_{G_m}\begin{pmatrix}0 & 0 & \ldots & 0\\ 0 & \lambda_2 & \ldots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \ldots & \lambda_n\end{pmatrix}\mathbf{P}_{G_m}^{-1}.$$

We define

$$\mathbf{D}^T := \mathbf{P}_{G_m} \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & \frac{1}{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{1}{\lambda_n} \end{pmatrix} \mathbf{P}_{G_m}^{-1}.$$

Let $\mathbf{d}_j$ be the j-th column of $\mathbf{D}$ for $j \in G_m$. We claim that $\mathbf{d}_j = \mathbf{b}_j^*$ for all $j \in G_m \backslash \{1\}$. Since span $(\mathbf{B}) \subseteq \mathbb{R}^{G_m} \cong \mathbb{R}^n$ is the subspace orthogonal to the all-one vector $\mathbf{1}$, we have to prove $\langle \mathbf{d}_j, \mathbf{1} \rangle = 0$ or all $j \in G_m \backslash \{1\}$, first. The components of the vector $\mathbf{d}_j$ just differ by the order of the entries of $\mathbf{d}_1$, since $\mathbf{D}$ is a G_m-circulant matrix associated to $\mathbf{d}_1$ by Lemma 2.13. Hence,

$$\langle \mathbf{d}_j, \mathbf{1} \rangle = \langle \mathbf{d}_1, \mathbf{1} \rangle = 0,$$

since $\langle \mathbf{d}_1, \mathbf{1} \rangle$ is the eigenvalue of $\mathbf{D}$ corresponding to the trivial character $1 \equiv \chi \in \widehat{G_m}$.

Now, we only have to prove $\langle \mathbf{d}_i, \mathbf{b}_j \rangle = \delta_{i,j}$ for all $i, j \in G_m \backslash \{1\}$. We define

$$\mathbf{Z}_1^M := \mathbf{Z} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} = (\mathbf{z}_1, \dots, \mathbf{z}_1) \in \mathbb{R}^{G_m \times G_m},$$

where the first row of the matrix, which only has ones in the first row and zeroes elsewhere, corresponds to $1 \in G_m$. Since $\mathbf{b}_j = \mathbf{z}_j - \mathbf{z}_1$ for all $j \in G_m \backslash \{1\}$ (see definition), we have

$$\begin{aligned} \langle \mathbf{d}_i, \mathbf{b}_j \rangle &= \left(\mathbf{D}^T \mathbf{B} \right)_{i,j} = \left(\mathbf{D}^T \mathbf{Z} - \mathbf{D}^T \mathbf{Z}_1^M \right)_{i,j} \\ &= \left(\underbrace{\mathbf{P}_{G_m} \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \mathbf{P}_{G_m}^{-1}}_{=:\mathbf{M}} - \underbrace{\mathbf{P}_{G_m} \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \mathbf{P}_{G_m}^{-1}}_{=\mathbf{M}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \right)_{i,j} \\ &= \mathbf{M}_{i,j} - \mathbf{M}_{i,1} \end{aligned}$$

for all $i, j \in G_m \backslash \{1\}$. The entry $\mathbf{M}_{i,j}$ of $\mathbf{M}$ can easily be calculated , we obtain

$$\mathbf{M}_{i,j} = \frac{1}{|G_m|} \sum_{\substack{\chi \in \widehat{G_m} \\ \chi \not\equiv 1}} \chi \left(i \cdot j^{-1} \right).$$

Lemma 2.11 *4.)* implies for all $i, j \in G_m \backslash \{1\}$

$$\begin{aligned}
\mathbf{M}_{i,j} - \mathbf{M}_{i,1} &= \frac{1}{|G_m|} \left(\sum_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \chi\left(i \cdot j^{-1}\right) - \sum_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \chi\left(i\right) \right) \\
&= \frac{1}{|G_m|} \left(\underbrace{\sum_{\chi \in \widehat{G_m}} \chi\left(i \cdot j^{-1}\right)}_{\substack{=|G_m|, \text{ if } i=j \\ =0, \text{ else}}} - \underbrace{\sum_{\chi \in \widehat{G_m}} \chi\left(i\right)}_{\substack{=0 \\ \text{since } i \neq 1}} \right) \\
&= \delta_{i,j}.
\end{aligned}$$

By the uniqueness of the dual basis, this implies $\mathbf{b}_j^* = \mathbf{d}_j$ for all $j \in G_m \backslash \{1\}$. Therefore, Theorem 2.14 implies

$$||\mathbf{b}_j^*||_2^2 = ||\mathbf{d}_j||_2^2 = ||\mathbf{d}_1||_2^2 = |G_m|^{-1} \cdot \sum_{\chi \in \widehat{G_m} \backslash \{1\}} |\lambda_\chi|^{-2}$$

for all $j \in G_m \backslash \{1\}$, since the eigenvalues of $\mathbf{D}$ are given by $\frac{1}{\lambda_2}, \ldots, \frac{1}{\lambda_n}$ and, again, the components of $\mathbf{d}_j$ are just a permutation of the components of $\mathbf{d}_1$. □

To obtain an upper bound for $||\mathbf{b}_j^*||_2$, we need a lower bound for the eigenvalues λ_χ. We need the following lemma.

Lemma 4.17. *Let $n \in \mathbb{N}$. Then*

$$\sum_{k=1}^{n-1} \frac{1}{|1 - \xi_n^k|^2} = \frac{1}{2} \sum_{k=1}^{n-1} \frac{1}{1 - \cos\left(\frac{2\pi}{n} k\right)} \leq 1 + \frac{n}{4} + \frac{1}{9} n^2.$$

A proof can be found in the appendix. The following theorem summarizes the presented results and provides an upper bound for $||\mathbf{b}_j^*||_2$.

Theorem 4.18. *Let (p, q) be an (α, β)-generator prime pair, and $m := p^\alpha q^\beta$. Then the norm of all $\boldsymbol{b}_j^*$ for $j \in G_m \backslash \{1\}$ is equal and bounded by*

$$||\boldsymbol{b}_j^*||_2^2 \leq \frac{15C'}{m} + C^2 \log^2(m) \cdot \left(\frac{15\alpha\beta}{2m} + \frac{55(\alpha + \beta)}{8m} + \frac{5\beta}{12p^\alpha} + \frac{5\alpha}{12q^\beta} \right)$$

without the GRH, and

$$||\boldsymbol{b}_j^*||_2^2 \leq C^2 (\log \circ \log)^2(m) \cdot \left(\frac{15\alpha\beta}{2m} + \frac{55(\alpha + \beta)}{8m} + \frac{5\beta}{12p^\alpha} + \frac{5\alpha}{12q^\beta} \right),$$

if the GRH holds, for some constants $C, C' > 0$, where C' depends on p, q and C is independent of m. Note that $\log(m) = \alpha \log(p) + \beta \log(q)$ holds for $m = p^\alpha q^\beta$.

Proof. Under the *GRH*, we have

$$\begin{aligned}||\mathbf{b}_j^*||_2^2 = |G_m|^{-1} \cdot \sum_{\substack{\chi\in\widehat{G_m}\\ \chi\neq 1}} |\lambda_\chi|^{-2} &= \frac{8pq}{(p-1)(q-1)} \cdot \frac{1}{m} \sum_{\substack{\chi\in\widehat{G_m}\\ \chi\neq 1}} \frac{1}{\big|\left(1-\overline{\chi}(p)\right)\left(1-\overline{\chi}(q)\right)\big|^2 \cdot f_\chi \cdot |L(1,\chi)|^2} \\ &\leq \frac{15}{m} \cdot l^2(m) \sum_{\substack{\chi\in\widehat{G_m}\\ \chi\neq 1}} \frac{1}{\big|\left(1-\overline{\chi}(p)\right)\left(1-\overline{\chi}(q)\right)\big|^2 \cdot f_\chi}\end{aligned}$$

with $l(m) := C\log(\log(m)) \geq C\log(\log(f_\chi))$ for some constant $C>0$ by Theorem 2.17 (we take the sum over all non-trivial characters, therefore $3 \leq f_\chi | m$ holds for each of these characters χ), Lemma 4.16 and Theorem 4.15. We have used that $\frac{pq}{(p-1)(q-1)}$ is maximal for $p=3$ and $q=5$.

Without the *GRH*, we have to distinguish between the quadratic and non quadratic characters. Since $\mathbb{Z}_{p^\alpha}^\times$ is cyclic, there is exactly one non-trivial quadratic character of $\mathbb{Z}_{p^\alpha}^\times \cong \widehat{\mathbb{Z}_{p^\alpha}^\times}$. We claim that the conductor of this quadratic character is p. Let Ψ be the non-trivial quadric character of $\mathbb{Z}_p^\times$, then Ψ induces a non-trivial quadratic character of $\mathbb{Z}_{p^\alpha}^\times$ via concatenation with the natural projection from $\mathbb{Z}_{p^\alpha}^\times$ to $\mathbb{Z}_p^\times$. However, there is only one non-trivial character of $\mathbb{Z}_{p^\alpha}^\times$, hence it has conductor p. Analogously follows, that there is exactly one non-trivial quadratic character of $\mathbb{Z}_{q^\beta}^\times$, which has conductor q. Since $\widehat{\mathbb{Z}_m^\times} \cong \widehat{\mathbb{Z}_{p^\alpha}^\times} \times \widehat{\mathbb{Z}_{q^\beta}^\times}$, there are only three non-trivial quadratic characters of $\mathbb{Z}_m^\times$, which have conductor p, q and pq. Therefore, there exists a constant $C'>0$, such that

$$\sum_{\substack{\chi\in\widehat{G_{p^{l_1}q^{l_2}}}\setminus\{1\}\\ \chi \text{ is quadratic}}} |\lambda_\chi|^{-2} \leq C'$$

for all $l_1, l_2 \in \mathbb{N}$, since the bound of the eigenvalues λ_χ only depends on the conductor f_χ by Theorem 4.15 and Theorem 2.17. This implies

$$\begin{aligned}||\mathbf{b}_j^*||_2^2 &= |G_m|^{-1} \cdot \left(\sum_{\substack{\chi\in\widehat{G_m}\setminus\{1\}\\ \chi \text{ is quadr.}}} |\lambda_\chi|^{-2} + \sum_{\substack{\chi\in\widehat{G_m}\setminus\{1\}\\ \chi \text{ is not quadr.}}} |\lambda_\chi|^{-2} \right) \\ &\leq \frac{15C_1}{m} + \frac{15}{m} \cdot \sum_{\substack{\chi\in\widehat{G_m}\setminus\{1\}\\ \chi \text{ is not quadr.}}} \frac{1}{\big|\left(1-\overline{\chi}(p)\right)\left(1-\overline{\chi}(q)\right)\big|^2 \cdot f_\chi \cdot |L(1,\chi)|^2} \\ &\leq \frac{15C_1}{m} + \frac{15}{m} \cdot l^2(m) \sum_{\substack{\chi\in\widehat{G_m}\\ \chi\neq 1}} \frac{1}{\big|\left(1-\overline{\chi}(p)\right)\left(1-\overline{\chi}(q)\right)\big|^2 \cdot f_\chi}\end{aligned}$$

with $l(m) := C\log(m) \geq C\log(f_\chi)$ for some constant $C>0$ by Theorem 2.17. Hence, in both cases (with and without the *GRH*) we have to bound the occurring sum. Again, we split the sum into three sums over the characters with $pq|f_\chi$, $q \nmid f_\chi$ and $p \nmid f_\chi$. If $pq|f_\chi$, then $\big|\left(1-\overline{\chi}(p)\right)\left(1-\overline{\chi}(q)\right)\big| = 1$, therefore

$$\begin{aligned}
\sum_{\substack{\chi\in\widehat{G_m}\\ pq|f_\chi}} \frac{1}{\left|\,(1-\overline{\chi}(p))\,(1-\overline{\chi}(q))\,\right|^2\cdot f_\chi} &= \sum_{\substack{\chi\in\widehat{G_m}\\ pq|f_\chi}} \frac{1}{f_\chi} = \sum_{pq|t|m} \frac{1}{t} \sum_{\substack{\chi\in\widehat{G_m}\\ f_\chi=t}} 1 \\
&\le \sum_{pq|t|m} \frac{1}{t}\cdot\frac{t}{2} = \frac{1}{2}\alpha\cdot\beta,
\end{aligned}$$

where we used that there at most $|\widehat{G_t}| = \frac{\varphi(t)}{2} \le \frac{t}{2}$ characters of conductor t in $\widehat{G_m}$.

If $q\nmid f_\chi = p^e$ for some $1\le e\le\alpha$, then $\left|\,(1-\overline{\chi}(p))\,(1-\overline{\chi}(q))\,\right| = \left|\,(1-\overline{\chi}(q))\,\right|$. Let $g\in\mathbb{Z}$ be a generator of $\mathbb{Z}_{p^\alpha}^\times$ and $a\in\mathbb{Z}$ with $g^a\equiv q \mod p^\alpha$. Since (p,q) is an (α,β)-generator prime pair, it follows $\gcd\left(a, \frac{\varphi(p^e)}{2}\right)=1$ for every $1\le e\le\alpha$. Therefore, by Corollary 4.3 it holds

$$\begin{aligned}
\sum_{\substack{\chi\in\widehat{G_m}\\ 1<f_\chi|p^\alpha}} \frac{1}{\left|\,(1-\overline{\chi}(p))\,(1-\overline{\chi}(q))\,\right|^2\cdot f_\chi} &= \sum_{\substack{\chi\in\widehat{G_m}\\ 1<f_\chi|p^\alpha}} \frac{1}{\left|1-\overline{\chi}(q)\right|^2\cdot f_\chi} \\
&\le \sum_{e=1}^{\alpha} \frac{1}{p^e} \sum_{\substack{\chi\in\widehat{G_{p^e}}\\ \chi\not\equiv 1}} \frac{1}{\left|1-\overline{\chi}(q)\right|^2} \\
&= \sum_{e=1}^{\alpha} \frac{1}{p^e} \sum_{k=1}^{\frac{\varphi(p^e)}{2}-1} \frac{1}{\left|1-\xi^k_{\frac{\varphi(p^e)}{2}}\right|^2} \\
&\underset{(1)}{\le} \sum_{e=1}^{\alpha} \frac{1}{p^e}\cdot\left(1+\frac{\varphi(p^e)}{8}+\frac{\varphi(p^e)^2}{36}\right) \\
&= \sum_{e=1}^{\alpha} \frac{1}{p^e} + \frac{p-1}{8p} + \frac{(p-1)^2p^{e-2}}{36} \\
&\le \frac{\alpha}{p} + \frac{\alpha}{8} + \alpha p^{\alpha-2}\frac{(p-1)^2}{36},
\end{aligned}$$

where (1) follows from Lemma 4.17. Analogously follows

$$\sum_{\substack{\chi\in\widehat{G_m}\\ 1<f_\chi|q^\beta}} \frac{1}{\left|\,(1-\overline{\chi}(p))\,(1-\overline{\chi}(q))\,\right|^2\cdot f_\chi} \le \frac{\beta}{q} + \frac{\beta}{8} + \beta q^{\beta-2}\frac{(q-1)^2}{36}.$$

Altogether we have

$$\begin{aligned}
||\mathbf{b}_j^*||_2^2 &\le \frac{15C_1}{m} + \frac{15}{m}\cdot l^2(m)\left(\frac{\alpha}{p}+\frac{\beta}{q}+\frac{1}{2}\alpha\cdot\beta+\frac{\alpha+\beta}{8}+\beta q^{\beta-2}\frac{(q-1)^2}{36}+\alpha p^{\alpha-2}\frac{(p-1)^2}{36}\right) \\
&\le \frac{15C_1}{m} + l^2(m)\left(\frac{15\alpha\beta}{2m}+\frac{55(\alpha+\beta)}{8m}+\frac{5\beta}{12p^\alpha}+\frac{5\alpha}{12q^\beta}\right),
\end{aligned}$$

where $l(m)$ is either $l(m) = C \log(\log(m))$ under the *GRH* or $l(m) = C \log(m)$ without the *GRH* for some constant $C > 0$. We have used that $\frac{\alpha}{p} + \frac{\beta}{q} \leq \frac{\alpha}{3} + \frac{\beta}{5} \leq \frac{\alpha+\beta}{3}$. Notice that the term $\frac{15C'}{m}$ can be omitted under the *GRH*, since it does not occur in the bound of $||\mathbf{b}_j^*||_2^2$. □

The following corollary states, that the basis $\mathbf{b}_1, \ldots, \mathbf{b}_k$ for $m = p^\alpha q^\beta$ is well suited for BDD, if (p, q) is a generator prime pair and the distance between α and β is not too big.

Corollary 4.19. *Let (p, q) be a generator prime pair and $c \in \mathbb{N}_0$. Further, let $\alpha_l := l$, $\beta_l := l + c$ and $m_l := p^{\alpha_l} q^{\beta_l}$ for all $l \in \mathbb{N}$. Then*

$$||\boldsymbol{b}_j^*||_2 \to 0 \text{ for } l \to \infty$$

for all $j \in G_m \backslash \{1\}$ and

$$m_l \cdot \exp\left(-\frac{1}{8||\boldsymbol{b}_j^*||_2}\right) \to 0 \text{ for } l \to \infty.$$

In particular, for every $\omega \in (0, 1)$ Condition 3.5 holds with parameters $M = ||Log(b_j)^*||_2$ for all $j \in G_m \backslash \{1\}$ and ω for large enough m_l, if the generator $g \in K_{m_l}$ is drawn from a continuous Gaussian.

Proof. It is sufficient to prove the statement by using the bound without the *GRH*.

Since $\log(m_l) = \alpha_l \log(p) + \beta_l \log(q) \leq C \cdot l$ for some constant $C > 0$, Theorem 4.18 implies

$$||\mathbf{b}_j^*||_2^2 \in O\left(l^3 \cdot \frac{p^l + q^{l+c}}{p^l q^{l+c}}\right).$$

This implies $||\mathbf{b}_j^*||_2^2 \to 0$ for $l \to \infty$. Further, if we assume $p < q$, we obtain

$$\begin{aligned}
m_l \cdot \exp\left(-\frac{1}{8||\mathbf{b}_j^*||_2}\right) &= \exp\left(\log(m_l) - \frac{1}{8||\mathbf{b}_j^*||_2}\right) \\
&\leq \exp\left(Cl - C' \frac{p^{l/2} q^{(l+c)/2}}{8 l^{3/2} \sqrt{p^l + q^{l+c}}}\right) \\
&= \exp\left(Cl - C' \frac{p^{l/2}}{8 l^{3/2} \sqrt{\frac{p^l}{q^{l+c}} + 1}}\right) \\
&\leq \exp\left(Cl - C' \frac{p^{l/2}}{16 l^{3/2}}\right) \to 0 \text{ for } l \to \infty
\end{aligned}$$

for some constant $C' > 0$.

Hence, Condition 3.5 holds with parameter $\omega > 0$ and $M = ||\mathbf{b}_j^*||_2$ for $j \in G_m \backslash \{1\}$ and large enough l by Theorem 3.8. □

4.5 Conclusion

We have extended the results of [9] to cyclotomic number fields of conductor $m = p^\alpha q^\beta$ for some distinct odd primes p and q. We have investigated the group $\mathcal{S}_m$ generated by the roots of unity and the elements

$$\frac{\xi_m^j - 1}{\xi_m - 1} \in \mathcal{O}_m^\times$$

for $j \in \mathbb{Z}_m^\times$, if m is the product of two odd prime-powers, and presented a criterion to determine when $[\mathcal{O}_m^\times : \mathcal{S}_m] = 2h_m^+\beta_m \neq 0$ holds if $m = p^\alpha q^\beta$. We showed that this is the case if and only if (p, q) is an (α, β)-generator prime pair. Moreover, we have proven that the factor β_m is bounded by $\frac{m}{4}$ in this case. As mentioned in Remark 4.10, if the class number h_m^+ is bounded by some polynomial in m, at least for fixed (p, q), Algorithm 2 can be executed in polynomial running time in m by Theorem 3.4.

To guarantee that Algorithm 2 outputs a short generator with non negligible probability $\omega \in (0, 1)$, we need Condition 3.5 to be satisfied for Gaussian distributions with parameters $M = \max\{||\mathbf{b}_j^*||_2 \big| \ j \in G_m \backslash \{1\}\}$ and ω. We have proven that this condition is satisfied for all $\omega \in (0, 1)$ for large enough $m = p^\alpha q^\beta$, if $|\alpha - \beta|$ is bounded by some constant, see Corollary 4.19.

Therefore, we can efficiently recover shortest generators of principle fractional ideals in K_m with overwhelming probability in the case that $m = p^\alpha q^\beta$ is sufficiently large, the distance of α and β is not too big, and (p, q) is a GPP and the shortest generators are chosen from some continuous Gaussian (and if h_m^+ is small enough).

5 Future Work

We extended the results of [9] to cyclotomic fields, whose conductor is the product of two odd prime powers, by studying the group generated by the units $\frac{\xi_m^j - 1}{\xi_m - 1}$ for $j \in G_m \backslash \{1\}$.

However, there are some interesting questions that remain open. First, can our results be extended to the case $p = 2$, i.e., $m = 2^\alpha q^\beta$ for some odd prime q? The issue with the prime 2 is that $\mathbb{Z}_{2^\alpha}^\times$ is cyclic if and only if $\alpha = 1$ or $\alpha = 2$. However, the structure of of $\mathbb{Z}_{2^\alpha}^\times$ for $\alpha \geq 3$ is given by

$$\mathbb{Z}_{2^\alpha}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}},$$

see [8, Theorem 1.4.1]. It seems reasonable that this fact can be used to extend our results to the case $p = 2$. Further, by computation we conjecture

$$\beta_{2^\alpha q^\beta} = \frac{\varphi\left(2^\alpha q^\beta\right)}{4}$$

in the case that $\beta_{2^\alpha q^\beta} \neq 0$.

A second open question is the case, that m is the product of more than two prime-powers. In fact, if m has at least four distinct prime factors, the index of our considered units in the full group of units is always infinite, see Lemma 5.1 in the appendix. Therefore, our techniques can not be applied in thes case in a straight-forward manner. We leave the question whether our techniques can be extended to the case that the conductor is the product of exactly three prime-powers to future work. In this case, we note that, since more eigenvalues of the introduced matrix $\mathbf{Z}$ are zero, Lemma 4.16 is no longer valid and thus needs to be extended. For arbitrary m, a basis of some finite index subgroup of $\mathcal{O}_m^\times$ is known, namely

$$b_j := \prod_{d \in D_m} \frac{\xi_d^j - 1}{\xi_d - 1} \in \mathcal{O}_m^\times$$

for $j \in G_m \backslash \{1\}$, where $D_m := \{d \in \mathbb{N} |\ d|m,\ d > 1 \text{ and } \gcd(d, \frac{m}{d}) = 1\}$. However, the index of these units in the full group of units is given by

$$[(\mathcal{O}_m^+)^\times : \mathcal{G}_m^+] = h_m^+ \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p|m \\ p \nmid f_\chi \\ p \in \mathbb{P}}} (\varphi(p^{e_p}) + 1 - \chi(p)) \neq 0,$$

where $m = \prod_{p|m} p^{e_p}$ denotes the prime factorization of m and h_m^+ is the class number of $K_m^+ = \mathbb{Q}(\xi_m)^+$, see [37, Theorem 8.3.]. This index however is growing too fast with m for our purpose.

References

1. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In T. Holz and S. Savage, editors, *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343. USENIX Association, 2016.
2. L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
3. D. Bernstein. A subfield-logarithm attack against ideal lattices. `http://blog.cr.yp.to/20140213-ideal.html`, Febuary 2014.
4. J.-F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A):385–403, 2014.
5. J.-F. Biasse and F. Song. On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in $\mathbb{Q}(\zeta_{p^n})$. Technical report, Tech Report CACR 2015-12, 2015.
6. J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 893–902. Society for Industrial and Applied Mathematics, 2016.
7. P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale. In *ETSI 2nd Quantum-Safe Crypto Workshop*, pages 1–9, 2014.
8. H. Cohen. *A course in computational algebraic number theory*, volume 4. Springer, 2000.
9. R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 559–585. Springer, 2016.
10. R. Cramer, L. Ducas, and B. Wesolowski. Short Stickelberger class relations and application to Ideal-SVP. Technical report, Cryptology ePrint Archive, Report 2016/885, 2016. http://eprint. iacr. org/2016/885, 2016.
11. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2013.
12. K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 293–302, New York, NY, USA, 2014. ACM.
13. S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–17. Springer, 2013.
14. Y. Ge. Elementary properties of cyclotomic polynomials. *Mathematical Reflections*, 2, 2008.
15. C. Gentry. Fully homomorphic encryption using ideal lattices. In Mitzenmacher [26], pages 169–178.

16. J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In J. Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.
17. C.-G. Ji and H.-W. Lu. Lower bound of real primitive L-function at s= 1. *Acta Arithmetica*, 111:405–409, 2004.
18. K. Königsberger. Analysis 1., Sechste Auflage, 2004.
19. E. Landau. Über Dirichletsche Reihen mit komplexen Charakteren. *Journal für die reine und angewandte Mathematik*, 157:26–32, 1927.
20. R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In A. Kiayias, editor, *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer, 2011.
21. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer Berlin Heidelberg, 2010.
22. V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-LWE cryptography. In T. Johansson and P. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2013.
23. D. Micciancio and O. Regev. Lattice-based cryptography. In D. J. Bernstein, J. Buchmann, and E. Dahmen, editors, *Post-Quantum Cryptography*, pages 147–191. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
24. P. Mihailescu. Primary cyclotomic units and a proof of catalan's conjecture. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 572:167–195, 2004.
25. J. C. Miller. Class numbers of real cyclotomic fields of composite conductor. *LMS Journal of Computation and Mathematics*, 17(A):404–417, 2014.
26. M. Mitzenmacher, editor. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009.* ACM, 2009.
27. H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory I: Classical theory*, volume 97. Cambridge University Press, 2006.
28. J. Neukirch and N. Schappacher. *Algebraic number theory.* Grundlehren der mathematischen Wissenschaften. Springer, Berlin, New York, Barcelona, 1999.
29. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Mitzenmacher [26], pages 333–342.
30. C. Peikert. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016.
31. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.
32. R. Schoof. *Catalan's conjecture.* Springer Science & Business Media, 2010.
33. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
34. C. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arithmetica*, 1(1):83–86, 1935.
35. N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In *International Workshop on Public Key Cryptography*, pages 420–443. Springer, 2010.
36. R. Steiner. Class number bounds and catalan's equation. *Mathematics of Computation of the American Mathematical Society*, 67(223):1317–1322, 1998.
37. L. C. Washington. *Introduction to Cyclotomic Fields.* Springer, Berlin, New York, Barcelona, second edition edition, 1996.

Appendix

The case that m has at least four distinct prime factors

We give a proof of Exercise 8.8 in [37].

Lemma 5.1. *Let $m \in \mathbb{N}$ with $m \not\equiv 2 \mod 4$ have at least four distinct prime factors, say $p < q < r < s$. Then the index $[\mathcal{O}_m : \mathcal{S}_m]$ is infinite.*

Proof. Let χ_q, χ_r and χ_s are the non trivial quadratic characters of $\mathbb{Z}_q^\times, \mathbb{Z}_r^\times$ and $\mathbb{Z}_s^\times$, respectively. If $\chi_l(p) = 1$ and $\chi_l(-1) = 1$ for some $l \in \{q, r, s\}$, then the index is infinite by Lemma 4.7. Else, if there are two characters, say χ_q and χ_r, such that $\chi_q(p) = \chi_q(p)$ and $\chi_q(-1) = \chi_r(-1)$, then $\chi_{qr} := \chi_q \cdot \chi_r$ is a non trivial quadratic character of $\mathbb{Z}_{qr}^\times \cong \mathbb{Z}_q^\times \times \mathbb{Z}_r^\times$, where $\chi_{qr}(a) := \chi_q(a) \cdot \chi_r(a)$ for all $a \in \mathbb{Z}_{qr}^\times$. Since $\chi_{qr}(p) = \chi_q(p) \cdot \chi_r(p) = 1$ and analogously $\chi_{qr}(-1) = 1$, this implies the finiteness of the index in this case again by Lemma 4.7. The only case left is $\{(\chi_q(p), \chi_q(-1)), (\chi_r(p), \chi_r(-1)), (\chi_s(p), \chi_s(-1))\} = \{(-1, 1), (1, -1), (-1, -1)\}$. In this case, $\chi_{qrs} := \chi_q \cdot \chi_r \cdot \chi_s$ is a non trivial quadratic Dirichlet character of $\mathbb{Z}_{qrs}^\times$ with $\chi_{qrs}(p) = 1$ and $\chi_{qrs}(-1) = 1$, hence the index is infinite by Lemma 4.7. □

Proof of Lemma 4.17

Proof of Lemma 4.17. We prove this by splitting the sum into the sum over the points ξ_n^k with $\Re\left(\xi_n^k\right) \le 0$, which yields $|1 - \xi_n^k| \ge 1$, and the sum over the points ξ_n^k with $\Re\left(\xi_n^k\right) > 0$. The following holds.

$$
\begin{aligned}
\sum_{k=1}^{n-1} \frac{1}{|1-\xi_n^k|^2} &= \sum_{k=1}^{n-1} \frac{1}{\left|1-\left(\cos\left(\frac{2\pi}{n}k\right)+i\sin\left(\frac{2\pi}{n}k\right)\right)\right|^2} \\
&= \frac{1}{2}\sum_{k=1}^{n-1} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)} \\
&= \frac{1}{2}\left(\sum_{k=1}^{\lfloor\frac{n-1}{4}\rfloor} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)} + \sum_{k=\lfloor\frac{n-1}{4}\rfloor+1}^{n-1-\lfloor\frac{n-1}{4}\rfloor} \underbrace{\frac{1}{1-\underbrace{\cos\left(\frac{2\pi}{n}k\right)}_{\le 0}}}_{\le 1} + \sum_{k=n-\lfloor\frac{n-1}{4}\rfloor}^{n-1} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)}\right) \\
&\le \frac{1}{2}\left(2\sum_{k=1}^{\lfloor\frac{n-1}{4}\rfloor} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)} + \left(\left(n-1-\left\lfloor\frac{n-1}{4}\right\rfloor\right) - \left(\left\lfloor\frac{n-1}{4}\right\rfloor+1\right)+1\right)\right) \\
&= \frac{1}{2}\left(2\sum_{k=1}^{\lfloor\frac{n-1}{4}\rfloor} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)} + 2\left(\frac{n-1}{4}+\frac{n-1}{4}-\left\lfloor\frac{n-1}{4}\right\rfloor\right)\right) \\
&\le \frac{1}{2}\left(2\sum_{k=1}^{\lfloor\frac{n-1}{4}\rfloor} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)} + 2\left(1+\frac{n-1}{4}\right)\right) \le 1+\frac{n}{4}+\sum_{k=1}^{\lfloor\frac{n-1}{4}\rfloor} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)}.
\end{aligned}
$$

For all $x \in (0,2]$ the inequality $\cos(x) < 1 - \frac{x^2}{2} + \frac{x^4}{24}$ holds, see for example [18, Section 8.7, Einschließungslemma]. Since $\frac{2\pi}{n}k \in (0,2)$ for $k = 1, ..., \left\lfloor \frac{n-1}{4} \right\rfloor$ (if $n \leq 4$, the following sum is empty, hence equals zero), we have

$$\begin{aligned}
\sum_{k=1}^{\lfloor \frac{n-1}{4} \rfloor} \frac{1}{1-\cos\left(\frac{2\pi}{n}k\right)} &\leq \sum_{k=1}^{\lfloor \frac{n-1}{4} \rfloor} \frac{1}{1-1+\frac{\left(\frac{2\pi}{n}k\right)^2}{2} - \frac{\left(\frac{2\pi}{n}k\right)^4}{24}} = \frac{2}{4\pi^2} \sum_{k=1}^{\lfloor \frac{n-1}{4} \rfloor} \frac{n^2}{k^2\left(1-\frac{4\pi^2k^2}{12n^2}\right)} \\
&\leq \frac{1}{2\pi^2} \sum_{k=1}^{\lfloor \frac{n-1}{4} \rfloor} \frac{n^2}{k^2\left(1-\frac{\pi^2\left(\lfloor \frac{n-1}{4} \rfloor\right)^2}{3n^2}\right)} \\
&\leq \frac{n^2}{2\pi^2} \sum_{k=1}^{\lfloor \frac{n-1}{4} \rfloor} \frac{1}{k^2\left(1-\frac{\pi^2}{48}\right)} \leq \frac{n^2}{2\pi^2} \sum_{k=1}^{\lfloor \frac{n-1}{4} \rfloor} \frac{4}{3k^2} \\
&\leq \frac{2n^2}{3\pi^2} \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{2n^2}{3\pi^2} \cdot \frac{\pi^2}{6} = \frac{n^2}{9},
\end{aligned}$$

where we used in the last line the equality $\zeta(2) = \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$ for the Riemann zeta function ζ, see for example [18, Section 15.4]. □

Recovering a short generator with a basis of a finite subgroup of $\mathcal{O}_K^\times$

Algorithm 3: Recovering a short generator with a basis of a finite subgroup of $\mathcal{O}_K^\times$

```
Input: A generator $g' \in K^\times$ of $g\mathcal{O}_K$ and $b_1, ..., b_k \in \mathcal{O}_K^\times$ such that
  $\mathbf{B} := \{\mathrm{Log}(b_1), ..., \mathrm{Log}(b_k)\}$ is a basis of a subgroup of $\Gamma = \mathrm{Log}(\mathcal{O}_K^\times)$ with finite index $f$.
  Set $F := \langle b_1, ..., b_k \rangle \subseteq \mathcal{O}_K^\times$.
Output: A generator $g_h \in K^\times$ of $g\mathcal{O}_K$ with norm less or equal to the norm of the (short)
  generator $g$.
Calculate a set of representatives $u_1, ..., u_f$ of $\mathcal{O}_K^\times / \mu(K)F$ (This can be preprocessed)
$N \leftarrow \infty$
for $i = 1, ..., f$ do
    $g_e(i) \leftarrow$ output $g_e$ of Algorithm 2 with input $g'/u_i$ and $b_1, ..., b_k$
    if $||Log(g_e(i))||_2 < N$ then
        $g_h \leftarrow g_e(i)$
        $N \leftarrow ||\mathrm{Log}(g_e(i))||_2$
return $g_h$
```