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

Patrick Holzer, Thomas Wunderer(✉), and Johannes A. Buchmann

TU Darmstadt, Darmstadt, Germany
patrick.holzer@stud.tu-darmstadt.de,
{twunderer,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, find a shortest generator of the principal ideal. The folklore approach to this problem is to first, recover some arbitrary generator of the ideal, which is known as the *principal ideal problem (PIP)* and second, solve a bounded distance decoding (BDD) problem in the *log-unit lattice* to transform this arbitrary generator into a shortest one. The PIP can be solved in polynomial time on *quantum* computers for arbitrary number fields under the *generalized Riemann hypothesis* due to Biasse and Song. Cramer et al. showed, based on the work of Campbell et al., that the second problem can be solved in polynomial time on *classical* computers for *cyclotomic fields of prime-power conductor.*

In this work, we extend the work of Cramer et al. to cyclotomic 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 BDD problem in the log-unit lattice 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.

Keywords: Lattice-based cryptography · Principal ideal lattices
SG-PIP · Cryptanalysis

1 Introduction

Over the past decade, lattice-based cryptography [23] has emerged as one of the most promising candidates for post-quantum cryptography [18]. The security of lattice-based schemes relies on the hardness of lattice problems such as

T. Wunderer—This research was supported by the DFG as part of project P1 within the CRC 1119 CROSSING.

A. Patra and N. P. Smart (Eds.): INDOCRYPT 2017, LNCS 10698, pp. 346–368, 2017.
https://doi.org/10.1007/978-3-319-71667-1_18

finding a shortest non-zero vector of a lattice. In order to boost the efficiency or achieve additional functionality, more structured lattices have been taken into consideration, for example lattices induced by (principal) fractional ideals in algebraic number fields, called *ideal lattices* [16,17]. Some recent cryptographic constructions – including a public key encryption scheme [6], a fully homomorphic encryption scheme [26], and a candidate multilinear map construction [11] – rely on the hardness of the *short generator principal ideal problem* (*SG-PIP*) [8]: 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, find a shortest generator of $\mathfrak{a}$.

The folklore approach to solve this problem, as sketched by Bernstein [2] and Campbell et al. [6] 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 $\operatorname{Log}(g') \in \operatorname{Log}(g) + \operatorname{Log}(\mathcal{O}_K^\times)$, where Log denotes the logarithmic embedding. Since $\operatorname{Log}(g)$ is short, we can therefore find $\operatorname{Log}(g)$ (and hence g) by solving a closest vector problem in the *Dirichlet log-unit lattice* $\operatorname{Log}(\mathcal{O}_K^\times)$.

The PIP can be solved in polynomial time on quantum computers for cyclotomic fields $K = \mathbb{Q}(\xi_m)$ of prime-power conductor $m = p^\alpha$ [4,6,10] and, under the *generalized Riemann hypothesis*, also for arbitrary number fields [5]. Following the sketch of Campbell et al. [6], Cramer et al. [8] 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 $K^+ = \mathbb{Q}(\xi_m + \xi_m^{-1})$. Their algorithm 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 $\operatorname{Log}\left(\frac{\xi_m^j - 1}{\xi_m - 1}\right)^*$ for all $j \in {}^{\mathbb{Z}_m}/\{\pm 1\}$ is small enough if m is a prime-power.

The proofs given in [8] heavily use that the underlying cyclotomic number fields have prime-power conductor.

In this work, we extend the work of Cramer et al. to cyclotomic number fields $K = \mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$, where p, q are distinct odd primes. We show that in this case, under some conditions, the BDD problem in the log-unit lattice can efficiently be solved 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 [5] 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 $p^\alpha q^\beta$.

In consequence, we extend the quantum polynomial time key-recover attacks [6,8] on the cryptographic schemes of [6,11,26] 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).

Outline. This work is structured as follows. In Sect. 2, we provide the necessary mathematical background for this work. In Sect. 3, we sketch the algorithmic approach and sufficient success conditions presented in [2,6,8] to find a shortest generator of some principal fractional ideal, given an arbitrary generator. In Sect. 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 $m = p^\alpha q^\beta$.

2 Preliminaries

We denote $\mathbb{N} := \{1, 2, 3, \ldots\}$ and $\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$. 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 basis $\mathbf{B} \subseteq \mathbb{R}^n$ is defined as the $\mathbb{R}$-basis of $\mathrm{span}_{\mathbb{R}}(\mathbf{B})$ with $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = \delta_{i,j}$ for all $i, j \in \{1, \ldots, k\}$, i.e., $\mathbf{B}^T \cdot \mathbf{B}^* = (\mathbf{B}^*)^T \cdot \mathbf{B} = \mathbf{I}_k$. 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 denote the index of K in L by $[L : K] := \dim_K L$. An **algebraic number field** K is an extension field of $\mathbb{Q}$ of finite index. 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 $\alpha \in \mathcal{O}_K$. Without loss of generality 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 [22, 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** $\mathrm{Cl}_K = {}^{\mathcal{I}_K}/_{\mathcal{P}_K}$ of K is the quotient of the abelian multiplicative group of fractional ideal $\mathcal{I}_K$ and the subgroup of principal fractional ideals $\mathcal{P}_K$. The **class number** h_K of an algebraic number field K is $h_K := |\mathrm{Cl}_K| < \infty$, see [22, Sect. 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 $\delta_1, \ldots, \delta_r : K \to \mathbb{R}$ of K and s the number of non real embeddings (up to complex conjugation) $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$. 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

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

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., $r = 0$ and therefore $n = 2s$, it is sufficient to use the **reduced logarithmic embedding** of $K^\times$:

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

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* [22, Theorem (7.3)].

Theorem 2.1 (Dirichlet's Unit Theorem)**.** *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 $\mathbf{1} := (1, \ldots, 1) \in \mathbb{R}^{r+2s}$. We call Γ the **log-unit lattice**.*

Lemma 2.2 ([22, (7.1) Proposition])**.** *For an algebraic number field K it holds that $ker\left(Log|_{\mathcal{O}_K^\times}\right) = \mu(K)$.*

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 $\mu(K) \times \mathbb{Z}^{r+s-1}$, i.e., 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 $\mathcal{O}_K$. We now define a "short generator" of a principal fractional ideal.

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.

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 $K_m/\mathbb{Q}$ is Galois with index $[K_m : \mathbb{Q}] = \varphi(m)$, where $\varphi(\cdot)$ is the Euler totient function. The automorphisms $\sigma_i(\cdot)$ of K_m are characterized by $\sigma_i(\xi_m) := \xi_m^i$ for $i \in \mathbb{Z}_m^\times$. Therefore, the Galois group $\mathrm{Gal}(K_m/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_m^\times$. 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 $m = 2 \cdot k$ for some odd $k \in \mathbb{N}$, we have $\xi_m = -\xi_k$ and therefore $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_k)$. Hence, without loss of generality it is sufficient to assume $m \not\equiv 2 \mod 4$. The ring of integers is given by $\mathcal{O}_m = \mathbb{Z}[\xi_m]$ (e.g. [22, Proposition (10.2)]).

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

A proof of the previous lemma can be found in the extended version of this paper [13]. 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 $\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^\times} (X - \xi_m^i)$. 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 [12, Corollary 4].

2.5 Circulant Matrices and Characters

We follow along [8, Sect. 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* [27, 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 $\chi_h(b) := \xi_n^{h\cdot\log_g(b)}$ for $0 \le h \le n-1$, 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. □

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 $\pi : \mathbb{Z}_m \to \mathbb{Z}_n$ 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 $\Psi \in \widehat{\mathbb{Z}_{f_\chi}^\times}$. 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 $\mathrm{Im}(\chi) \in \{\pm 1\}$ is called **quadratic**. 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 $\chi'(z) := \chi_{f_\chi}(z)$ if $\gcd(z, f_\chi) = 1$ and zero else, 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 an arbitrary finite abelian group G with the complex vector $(\chi(g))_{g\in G} \in \mathbb{C}^G$. This allows for geometrical calculations on characters and provides coherence between circular matrices and characters. For a proof of the following lemma see [8, Sect. 2.2] and use the fact, that $G \cong \widehat{G}$ holds for all finite abelian groups G.

Lemma 2.10. *Let G be a finite abelian group. Then the following holds.*

(1) For all $\chi \in \widehat{G}$ we have $\sum_{g\in G} \chi(g) = |G|$ if $\chi \equiv 1$ and 0 else.
(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 $\sum_{\chi\in\widehat{G}} \chi(g) = |G|$ if g is the identity element of G and 0 else.

Definition 2.11. *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 2.10 that $\boldsymbol{P}_G$ is unitary, i.e., $\boldsymbol{P}_G^{-1} = \overline{\boldsymbol{P}_G}^T$.

Lemma 2.12 ([8, 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 matrix $\boldsymbol{A}$ 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 2.13. *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

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

2.6 Dirichlet L-Series

Definition 2.14. *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 $\mathbb{H}_t := \{s \in \mathbb{C} | \ \Re(s) > t\}$ with $t > 1$. 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 [21, Theorem 10.7. ff]. Therefore, $L(1, \chi)$ is well defined in this case.

Theorem 2.15. *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 $f_\chi > 1$

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

In particular, $L(1, \chi) \neq 0$ if χ is a non-trivial Dirichlet character.

The first inequality was proven by Landau, see [15, p. 29]. For the second inequality, see [25] or [14] 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 [2,6,8] 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 $\min_{\boldsymbol{v} \in \mathcal{L}} ||\boldsymbol{v} - \boldsymbol{t}||_2 \leq r$ for some $r < \frac{1}{2}\lambda_1(\mathcal{L})$, where $\lambda_1(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}} ||\mathbf{v}||_2$, find the unique vector $\boldsymbol{v} \in \mathcal{L}$ with $||\boldsymbol{v} - \boldsymbol{t}||_2 \leq r$.*

We will use the following **Round-off Algorithm** [1] 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, [8, 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 $\boldsymbol{v} = \boldsymbol{B} \cdot \boldsymbol{a}$ on 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
    $\varGamma = \mathrm{Log}(\mathcal{O}_K^\times)$.
**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, [8, 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 (without loss of generality 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 [8, Sect. 5] for arbitrary cyclotomic fields $\mathbb{Q}(\xi_m)$ a natural distribution satisfying Condition 3.5 with a not too small parameter $\omega > 0$ for the basis discussed in Sect. 4.2 is the continuous Gaussian distribution. This is a consequence of the following theorem (for more details see [8, 5 Tail Bounds]).

Lemma 3.7 ([8, 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 with this approach. 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, given a number field K, such basis is not known. 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 [3] or quantum [10] 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, if $K = \mathbb{Q}(\xi_m)$ is a cyclotomic field, we obtain $|d_K| \in O(n\log(m))$ as a direct consequence of [27, 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 extended version of this paper [13].

In this work, we show that for cyclotomic number fields $\mathbb{Q}(\xi_m)$ the index of the basis presented in Sect. 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.

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 $j \in \mathbb{Z}_m^\times$ in the case where $m = p^\alpha q^\beta$ has only two distinct odd prime factors. We show that 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)**.*

The definition of generator prime pairs is useless for testing given prime pairs on this property, since infinitely many pairs of α and β have to be checked. To obtain a better criterion, we use the following result.

Theorem 4.2 ([7, 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 $p \in \mathbb{P}$, which implies the following corollaries. The proofs can be found in the extended version of this paper [13].

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 $\chi_h(b) := \xi_{\varphi(p^l)}^{h \cdot a(b)}$ for $0 \leq h \leq \varphi(p^l) - 1$ and h 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 $g^{a(b)} = b \in \mathbb{Z}_{p^l}^\times$.*

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.

With Corollary 4.4 we can easily check prime pairs if they are generator prime pairs by testing if they are a $(2, 2)$-GPP.

In the extended version of this paper [13] we provide some examples and numerical data of generator prime pairs. By computation, more than 35% of all odd prime pairs up to 32600 are generator prime pairs, see Fig. 1. An interesting fact is that a similar notion of prime pairs was used in the proof of Catalan's conjecture by Mihailescu [19], 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 [24, Chap. 1]. More information about their relation can be found in the extended version of this paper [13].

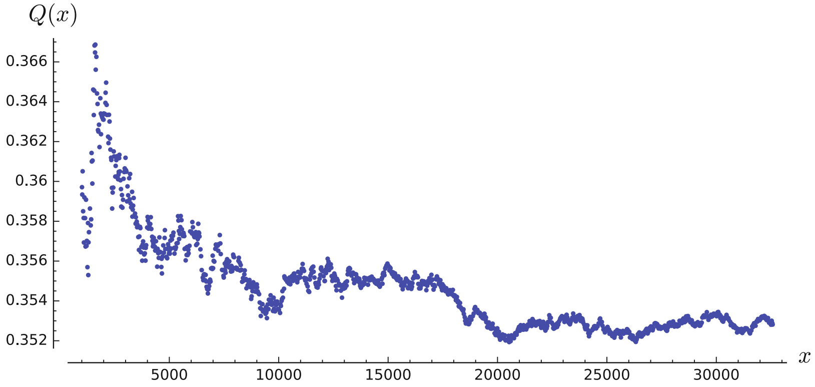

Fig. 1. Values of the quotient $Q(x) = \frac{\text{Number of GPP } (p,q) \text{ with } 2<p<q\leq x}{\text{Number of prime pairs } (p,q) \text{ with } 2<p<q\leq x}$

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

$$b_j := \frac{\xi_m^j - 1}{\xi_m - 1} \in \mathcal{O}_m^\times \quad \text{and} \quad \mathbf{b}_j := \operatorname{Log}_r(b_j) \in \mathbb{R}^{n/2}, \tag{1}$$

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 $\{l \in \mathbb{N}|\ 1 \leq l < \frac{m}{2} \text{ with } \gcd(l, m) = 1\}$) and let $\mathcal{S}_m$ denote the group generated by $\{b_j|\ j \in G_m\backslash\{1\}\}$ and $\pm\xi_m$, i.e., 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 identify 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 [27, Corollary 8.8].

Lemma 4.5. *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*

$$[\mathcal{O}_m^\times : \mathcal{S}_m] = 2h_m^+ \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p | m \\ p \in \mathbb{P}}} (1 - \chi(p))$$

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

For $m \in \mathbb{N}$ we define

$$\beta_m := \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p | m \\ p \in \mathbb{P}}} (1 - \chi(p)) .$$

Theorem 4.6. *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

$$\beta_m = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t | m \\ t \in \mathbb{P}}} (1 - \chi(p)) = \left(\prod_{\substack{\chi \in \widehat{G_{p^\alpha}} \\ \chi \neq 1}} (1 - \chi(q)) \right) \cdot \left(\prod_{\substack{\chi \in \widehat{G_{q^\beta}} \\ \chi \neq 1}} (1 - \chi(p)) \right),$$

because $\chi(p) = \chi(q) = 0$ and therefore $(1-\chi(p))(1-\chi(q)) = 1$ if $pq|f_\chi$. 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 $\gcd\left(a, \frac{\varphi(q^\beta)}{2}\right) = 1$ 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

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

where we used in equality *(1)* that multiplying with a is a permutation of $\mathbb{Z}_{\frac{\varphi(q^\beta)}{2}}$ with $0 \cdot a \equiv 0 \mod \frac{\varphi(q^\beta)}{2}$, since $\gcd\left(a, \frac{\varphi(q^\beta)}{2}\right) = 1$, 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., without loss of generality 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 $g^a \equiv p \mod q^l$. We conclude that $\gcd\left(a, \frac{\varphi(q^\beta)}{2}\right) > 1$ holds. Hence, there exists a prime number $t \in \mathbb{P}$ such that $t | \gcd\left(a, \frac{\varphi(q^\beta)}{2}\right)$ holds. Then $h := \frac{\varphi\left(q^\beta\right)}{t} \in \mathbb{N}$ is even and $1 \le h \le \varphi\left(q^\beta\right) - 1$. By Corollary 4.3, there is a non-trivial, even Dirichlet character χ_h of $\mathbb{Z}_{q^\beta}^\times$ with

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

which implies $\beta_m = 0$ 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 4.7 ([20, Theorem 1.1]). *Let m be a composite integer, $m \not\equiv 2 \bmod 4$, and let $\mathbb{Q}(\xi_m)^+$ denote the maximal real subfield of the m-th cyclotomic field $\mathbb{Q}(\xi_m)$. 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 4.8. *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 4.7 one could conjecture that the class number h_m^+ is bounded by some polynomial. In [9] 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 [8, Chap. 3].

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

$$z_j := \xi_m^j - 1 \in \mathcal{O}_m \quad \text{and} \quad \mathbf{z}_j := \mathrm{Log}_r(z_j) \in \mathbb{R}^{n/2}$$

for all $j \in \mathbb{Z}_m^\times$ (again, $n = \varphi(m)$). Note that $\mathbf{z}_j$ is well defined since $\xi_m^{-j} - 1$ is the complex conjugate of $\xi_m^j - 1$. 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 4.9. *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 $\mathbf{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is $\lambda_\chi = 0$.*

Proof. By Theorem 2.13, the eigenvalue of the G_m-circulant matrix $\mathbf{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is given by

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

where (1) follows from Lemma 2.6. □

Lemma 4.10. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Furthermore, let $\chi \in \widehat{G_m}$ 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*

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

This can be proven similar to the prime power case in [8, Corollary 3.4], a proof can be found in the extended version of this paper [13].

Lemma 4.11. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Furthermore, let $\chi \in \widehat{G}_m$ be an even 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 $1 \le e \le \alpha$. 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 $\pi^{-1}(a) = \Psi^{-1}\left(\left\{a' + k\cdot f \in \mathbb{Z}_{p^\alpha}^\times \middle| \, 0 \le k < \frac{p^\alpha}{f}\right\} \times \mathbb{Z}_{q^\beta}^\times\right) \subseteq \mathbb{Z}_m^\times$ by Chinese remainder theorem, where $\Psi : \mathbb{Z}_m \to \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{q^\beta}, a \mapsto (a \mod p^\alpha, a \mod q^\beta)$. There exists $r_1, r_2 \in \mathbb{Z}$ such that $r_1 q^\beta \equiv 1 \mod p^\alpha$ and $r_2 p^\alpha \equiv 1 \mod q^\beta$, which yields

$$\pi^{-1}(a) = \left\{(a' + k\cdot f)\cdot r_1 q^\beta + y\cdot r_2 p^\alpha \in \mathbb{Z}_m^\times \middle| \, 0 \le k < \frac{p^\alpha}{f},\ y \in \mathbb{Z}_{q^\beta}^\times\right\} \subseteq \mathbb{Z}_m^\times \tag{3}$$

for a fixed integer representative $a' \in \mathbb{Z}$ of $a \in \mathbb{Z}_f^\times$. We obtain

$$\prod_{\substack{j\in\mathbb{Z}_m^\times \\ \pi(b)=a}} (1-\xi_m^j) = \prod_{y\in\mathbb{Z}_{q^\beta}^\times}\ \prod_{0\le k<\frac{p^\alpha}{f}} \left(1-\xi_{\frac{p^\alpha}{f}}^{kr_1}\cdot\xi_{q^\beta}^{yr_2}\cdot\xi_{p^\alpha}^{a'r_1}\right) \underset{(1)}{=} \prod_{y\in\mathbb{Z}_{q^\beta}^\times}\left(1-\xi_{q^\beta}^{yr_2\frac{p^\alpha}{f}}\cdot\xi_{p^\alpha}^{a'r_1\frac{p^\alpha}{f}}\right)$$

$$\underset{(2)}{=} \prod_{y\in\mathbb{Z}_{q^\beta}^\times}\left(1-\xi_{q^\beta}^{y\frac{p^\alpha}{f}}\cdot\xi_f^{ar_1}\right) \underset{(3)}{=} \frac{1-\xi_f^{ar_1q^\beta}}{1-\xi_f^{ar_1q^{\beta-1}}} \underset{(4)}{=} \frac{1-\xi_f^a}{1-\xi_f^{ar_1q^{\beta-1}}}.$$

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 $Y := \xi_{q^\beta}^{yr_2} \cdot \xi_{p^\alpha}^{ar_1}$, 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 $Y = \xi_f^{ar_1}$. 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 can calculate the eigenvalue λ_χ.

$$\begin{aligned}
\lambda_\chi = \langle \mathbf{z}_1, \chi \rangle &= \frac{1}{2} \sum_{j \in \mathbb{Z}_m^\times} \overline{\chi}(j) \cdot \log\left(\left|1 - \xi_m^j\right|\right) = \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \sum_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(j) = a}} \log\left(\left|1 - \xi_m^j\right|\right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| \prod_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(j) = a}} (1 - \xi_m^j) \right|\right) = \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left| \frac{1 - \xi_f^a}{1 - \xi_f^{ar_1 q^{\beta-1}}} \right|\right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left|1 - \xi_f^a\right|\right) - \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left|1 - \xi_f^{ar_1 q^{\beta-1}}\right|\right) \\
&\underset{(5)}{=} \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left|1 - \xi_f^a\right|\right) - \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a \cdot q) \log\left(\left|1 - \xi_f^a\right|\right) \\
&= \frac{1}{2}(1 - \overline{\chi}(q)) \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left|1 - \xi_f^a\right|\right),
\end{aligned}$$

where we used in (5) the substitution a for $ar_1 q^{\beta-1}$ 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 4.12 ([27, 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*

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

We collect the previous results in the following theorem. A proof can be found in the extended version of this paper [13].

Theorem 4.13. *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Further, let $\chi \in \widehat{G_m}$ 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 $\chi \in \widehat{G_m}$ are non-zero iff (p, q) is an (α, β)-generator prime pair.

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 [8, Lemma 3.2].

Lemma 4.14. *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*

$$||\boldsymbol{b}_j^*||_2^2 = |G_m|^{-1} \cdot \sum_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} |\lambda_\chi|^{-2},$$

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. 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., $\widehat{G_m} = \{\chi_1, \dots, \chi_n\}$ 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 $\lambda_1, \dots, \lambda_k$ of $\mathbf{Z}$, where $\lambda_1 = 0$ by Lemma 4.9 and $\lambda_j \neq 0$ for $2 \leq j \leq n$ by Theorem 4.13. Since $\mathbf{Z}$ is a G_m-circulant matrix, Lemma 2.12 implies

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

We define

$$\mathbf{D}^T := \mathbf{P}_{G_m} \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & \frac{1}{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{1}{\lambda_n} \end{pmatrix} \mathbf{P}_{G_m}^{-1} \quad \text{and} \quad \mathbf{Z}_1^M := \mathbf{Z} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} = (\mathbf{z}_1, \dots, \mathbf{z}_1) \in \mathbb{R}^{G_m \times G_m},$$

where the first row of the matrix, which only has ones in the first row and zeroes elsewhere, corresponds to $1 \in G_m$.

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 $\operatorname{span}(\mathbf{B}) \subseteq \mathbb{R}^{G_m} \cong \mathbb{R}^n$ 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 2.12. 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 $i, j \in G_m \backslash \{1\}$. Since $\mathbf{b}_j = \mathbf{z}_j - \mathbf{z}_1$ for all $j \in G_m \backslash \{1\}$, 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 $\mathbf{M}$ is given by $\mathbf{M}_{i,j} = \frac{1}{|G_m|} \sum_{\substack{\chi \in \widehat{G_m} \\ \chi \not\equiv 1}} \chi\left(i \cdot j^{-1}\right)$. Together with Lemma 2.10 *(4)* we obtain

$$\mathbf{M}_{i,j} - \mathbf{M}_{i,1} = \frac{1}{|G_m|}\left(\sum_{\substack{\chi \in \widehat{G_m} \\ \chi \not\equiv 1}} \chi\left(ij^{-1}\right) - \sum_{\substack{\chi \in \widehat{G_m} \\ \chi \not\equiv 1}} \chi\left(i\right) \right) = \frac{1}{|G_m|}\left(\underbrace{\sum_{\chi \in \widehat{G_m}} \chi\left(ij^{-1}\right)}_{\substack{=|G_m|, \text{ if } i=j \\ =0, \text{ else}}} - \underbrace{\sum_{\chi \in \widehat{G_m}} \chi\left(i\right)}_{\substack{=0 \\ \text{since } i \neq 1}} \right) = \delta_{i,j}.$$

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 2.13 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 $0, \frac{1}{\lambda_2}, \dots, \frac{1}{\lambda_n}$ and, again, the components of $\mathbf{d}_j$ are just a permutation of the components of $\mathbf{d}_1$. □

The following theorem summarizes the presented results and provides an upper bound for $||\mathbf{b}_j^*||_2$. It can be proven similar to the prime power case in [8, Sect. 3], we only need to bound the new occurring factor $|(1 - \overline{\chi}(p))(1 - \overline{\chi}(q))|$. Therefore we just sketch the proof of the following theorem, for a detailed version see the extended version of this paper [13].

Theorem 4.15. *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. Without loss of generality we just consider the inequality without the GRH. Like in the prime power case, we 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 $\mathbb{Z}_{p^\alpha}^\times \cong \widehat{\mathbb{Z}_{p^\alpha}^\times}$ with conductor p. Therefore $\widehat{\mathbb{Z}_m^\times} \cong \widehat{\mathbb{Z}_{p^\alpha}^\times} \times \widehat{\mathbb{Z}_{q^\beta}^\times}$ has only three non-trivial quadratic characters of $\mathbb{Z}_m^\times$ of conductor p, q and pq. Hence, 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 Theorems 2.15 and 4.13. This implies

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

with $l(m) := C \log(m) \geq C \log(f_\chi)$ for some constant $C > 0$ by Theorem 2.15. Hence, we have to bound the occurring sum. 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 $\left| (1 - \overline{\chi}(p)) (1 - \overline{\chi}(q)) \right| = 1$, therefore

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

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

For the case $q \nmid f_\chi = p^e$ we use the inequality $\sum_{k=1}^{n-1} \frac{1}{|1 - \xi_n^k|^2} \leq 1 + \frac{n}{4} + \frac{1}{9} n^2$, which can be proven by basic analysis, see the extended version of this paper [13]. This and Corollary 4.3 implies

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

Analogously follows the same bound for the case $p \nmid f_\chi$. Altogether we have

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

where $l(m) = C\log(m)$ for some constant $C > 0$. We have used that $\frac{\alpha}{p} + \frac{\beta}{q} \leq \frac{\alpha}{3} + \frac{\beta}{5} \leq \frac{\alpha+\beta}{3}$. □

The upper theorem implies $||\mathbf{b}_j^*||_2^2 \in O\left(l^3 \cdot \frac{p^l + q^{l+c}}{p^l q^{l+c}}\right)$, where $\alpha = l$ and $\beta = l + c$ for some constant $c \in \mathbb{N}_0$. The following corollary is a direct consequence of this fact and shows, 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 bounded. A proof can be found in the extended version of this paper [13].

Corollary 4.16. *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 $||\boldsymbol{b}_j^*||_2 \to 0$ for $l \to \infty$ and 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.

References

1. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1–13 (1986)
2. Bernstein, D.: A subfield-logarithm attack against ideal lattices, February 2014. http://blog.cr.yp.to/20140213-ideal.html
3. Biasse, J.-F., Fieker, C.: Subexponential class group and unit group computation in large degree number fields. LMS J. Comput. Math. **17**(A), 385–403 (2014)
4. Biasse, J.-F., Song, F.: 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)
5. Biasse, J.-F., Song, F.: 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, pp. 893–902. Society for Industrial and Applied Mathematics (2016)
6. Campbell, P., Groves, M., Shepherd, D.: Soliloquy: a cautionary tale. In: ETSI 2nd Quantum-Safe Crypto Workshop, pp. 1–9 (2014)
7. Cohen, H.: A Course in Computational Algebraic Number Theory, vol. 4. Springer, Heidelberg (2000)

8. Cramer, R., Ducas, L., Peikert, C., Regev, O.: Recovering short generators of principal ideals in cyclotomic rings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 559–585. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_20
9. Cramer, R., Ducas, L., Wesolowski, B.: Short Stickelberger class relations and application to Ideal-SVP. Technical report, Cryptology ePrint Archive, Report 2016/885 (2016). http://eprint.iacr.org/2016/885
10. Eisenträger, K., Hallgren, S., Kitaev, A., Song, F.: 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 2014, New York, NY, USA, pp. 293–302. ACM (2014)
11. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_1
12. Ge, Y.: Elementary properties of cyclotomic polynomials. Math. Reflect. **2**, 1–8 (2008)
13. Holzer, P., Wunderer, T., Buchmann, J.: Recovering short generators of principal fractional ideals in cyclotomic fields of conductor p$^\alpha$ q$^\beta$. IACR Cryptology ePrint Archive 2017/513 (2017)
14. Ji, C.-G., Lu, H.-W.: Lower bound of real primitive L-function at s = 1. Acta Arith. **111**, 405–409 (2004)
15. Landau, E.: Über Dirichletsche Reihen mit komplexen Charakteren. J. für die reine und angewandte Mathematik **157**, 26–32 (1927)
16. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1
17. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 35–54. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_3
18. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-Quantum Cryptography, pp. 147–191. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-540-88702-7_5
19. Mihailescu, P.: Primary cyclotomic units and a proof of Catalan's conjecture. J. für die reine und angewandte Mathematik (Crelles Journal) **572**, 167–195 (2004)
20. Miller, J.C.: Class numbers of real cyclotomic fields of composite conductor. LMS J. Comput. Math. **17**(A), 404–417 (2014)
21. Montgomery, H.L., Vaughan, R.C.: Multiplicative Number Theory I: Classical Theory, vol. 97. Cambridge University Press, Cambridge (2006)
22. Neukirch, J., Schappacher, N.: Algebraic Number Theory. Grundlehren der mathematischen Wissenschaften. Springer, Heidelberg (1999)
23. Peikert, C., et al.: A decade of lattice cryptography. Found. Trends® Theor. Comput. Sci. **10**(4), 283–424 (2016)
24. Schoof, R.: Catalan's Conjecture. Springer Science & Business Media, Heidelberg (2010)
25. Siegel, C.: Über die Classenzahl quadratischer Zahlkörper. Acta Arith. **1**(1), 83–86 (1935)
26. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 420–443. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_25
27. Washington, L.C.: Introduction to Cyclotomic Fields, 2nd edn. Springer, Heidelberg (1996)