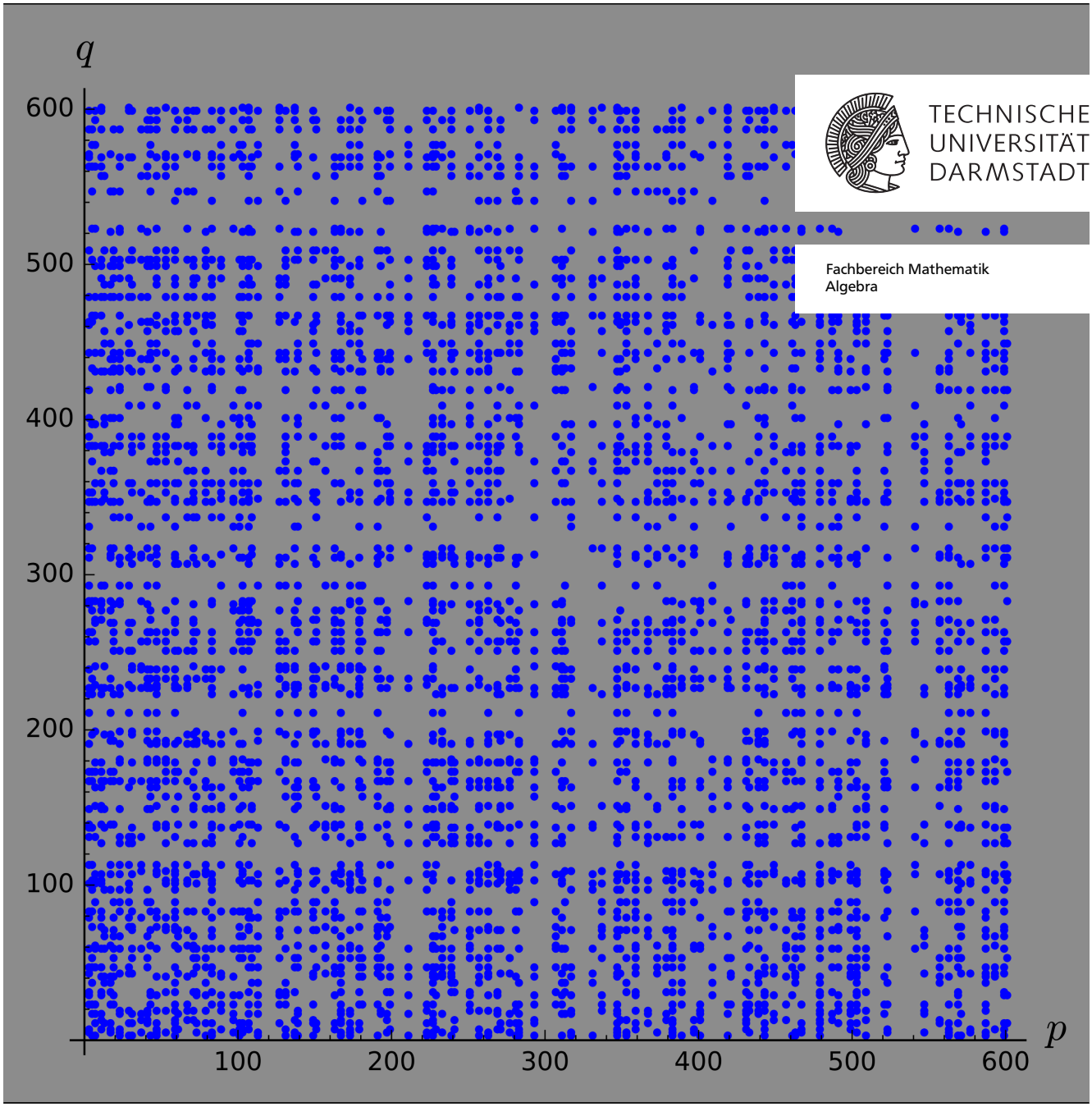
# Recovering Short Generators of Principal Fractional Ideals in Cyclotomic Fields of Conductor $p^\alpha q^\beta$

**Cryptography (Corrected Version, April 13, 2017)**

Master Thesis by Patrick Holzer

April 2017




TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Algebra

Recovering Short Generators of Principal Fractional Ideals in Cyclotomic Fields of Conductor $p^{\alpha}q^{\beta}$ Cryptography (Corrected Version, April 13, 2017)

Vorgelegte Master Thesis von Patrick Holzer

1. Gutachten: Prof. Dr. Dr. h.c. Johannes A. Buchmann
2. Gutachten: Dipl. Ing. Thomas Wunderer

Tag der Einreichung:

# Erklärung zur Master Thesis

Hiermit versichere ich, die vorliegende Master Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 13. April 2017

(Patrick Holzer)

# Danksagungen

An erster Stelle möchte ich meinem Betreuer Herrn Prof. Dr. Buchmann danken, der es mir ermöglichte, an diesem interessanten und aktuellen Thema zu arbeiten. Ebenso gilt mein außerordentlicher Dank Thomas Wunderer, der mir jederzeit für Fragen und Anregungen bereit stand.
Weiter möchte ich den fleißigen Korrekturlesern Ingmar, Sabrina, Florian, Oliver, Jan-Philipp und Katrin danken.
Nicht zuletzt danke ich meinen Eltern für die ganze Unterstützung während meiner Studienzeit.

# Corrected Version

In this version some minor mistakes of the original version were corrected. No contentual changes were made.

# Contents

# Abstract

Some recent cryptographic schemes rely on the hardness of finding a shortest generator of a principal (fractional) ideal in an algebraic number field $K$ in the logarithmic embedding with some guaranteed small generator, given some $\mathbb{Z}$-basis of the principal ideal. This problem can be split into two parts. First, recover some arbitrary generator of the ideal, which is known as the *principal ideal problem (PIP)*. Second, transform this generator into some shortest generator.
The first part is known to be solvable in polynomial time on quantum computers for cyclotomic fields of prime power conductor [CGS14, BS15] and for arbitrary number fields under the *generalized Riemann hypothesis*, see [BS16]. The second part is known to be solvable in polynomial time on classical computers for cyclotomic number fields of prime power conductor, see [CDPR16].
In this thesis, we entirely focus on the second task and extend the work of Cramer, Ducas, Peikert and Regev to cyclotomic fields $K = \mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$, where $p, q$ are distinct odd primes. Their algorithmic approach mainly relies on the fact that there is a well suited basis of the group of cyclotomic units which are a subgroup of $\mathcal{O}_K^\times = \mathbb{Z}[\xi_m]^\times$ with small enough finite index. We consider the group generated by these elements in the case that $m = p^\alpha q^\beta$ and introduce a new notion for odd prime pairs $(p, q)$, named *generator prime pairs*, which provides a criterion to check whether the index of this subgroup in $\mathcal{O}_K^\times$ is finite or not. We prove, that this basis is well suited to recover some shortest generator of a principal ideal in quantum polynomial time in the finite case, i.e., if $m = p^\alpha q^\beta$ for some generator prime pair $(p, q)$ with sufficiently large $\alpha, \beta \in \mathbb{N}$.
Further, we consider the approximate ideal shortest vector problem in cyclotomic fields $\mathbb{Q}(\xi_m)$, where the task is to find short elements in arbitrary ideals $\mathfrak{a}$ in $\mathcal{O}_K$ in the Minkowski embedding. In our second main contribution, we generalize the results of [CDPR16, CDW16] and argue, that one can efficiently solve the ideal shortest vector problem with an approximation factor $\exp(\tilde{O}(\sqrt{m}))$ in cyclotomic fields of conductor $m = p^\alpha q^\beta$ on quantum computers, if $(p, q)$ is an $(\alpha, \beta)$-generator prime pair.

# 1 Introduction

Modern cryptographic schemes like RSA and the Diffie-Hellmann protocol rely on the conjectured hardness of integer factorization and the difficulty of finding discrete logarithms in certain groups. Shor [Sho99] presented a quantum algorithm that solves these problems in polynomial time, which makes these systems insecure in the future if one would be able to build large enough quantum computers. This has lead to a search for alternative cryptographic schemes which are resistant against quantum adversaries. Many of today's promising schemes are lattice based, i.e., they rely on the hardness of lattice problems such as finding a shortest non-zero vector of a lattice, for which no efficient quantum algorithm is known. For efficiency reasons, more structured lattices are considered, for example lattices induced by some ideals or principal ideals in certain rings, called *ideal lattices*. In this work we consider the *Dirichlet log-unit lattice*, which is induced by the unit group $\mathcal{O}_K^\times$ via the logarithmic embedding of an algebraic number field $K$. This has applications to the fully homomorphic encryption scheme [SV10] and [GGH13], which works with the following keys.

- **Secret key:** A "short" generator $g \in K^\times$ of the principal (fractional) ideal $\mathfrak{a} = \langle g \rangle$ in the algebraic number field $K$.
- **Public key:** A "bad" $\mathbb{Z}$-basis of the ideal $\mathfrak{a}$ (and the algebraic number field $K$).

Hence, to break these schemes, it is sufficient if one can efficiently recover a short generator $g \in K^\times$ for each principal fractional ideal $\mathfrak{a} = \langle g \rangle$ with a guaranteed short generator. This so called *short generator of a principal ideal problem* (*SG-PIP*) can be split into the following two problems, as sketched by Campbell, Groves and Shepherd [CGS14].

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.

The best known classical algorithm for solving the principal ideal problem is the algorithm of Biasse and Fieker [BF14], whose running time is subexponential in $n = [K : \mathbb{Q}]$. In [CGS14, BS15], 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 [BS16].
Cramer, Ducas, Peikert and Regev [CDPR16] focused on the second problem and proved, that it 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 $\mathbb{Q}(\xi_m + \xi_m^{-1})$. The main part of their strategy 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 $\mathbb{Z}[\xi_m]^\times$ 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 if $m$ is a prime power (or is at least bounded by some polynomial in $n = \varphi(m)$).
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.

In this thesis, we follow their algorithmic approach and examine, in which case the group generated by the units $\frac{\xi_m^j-1}{\xi_m-1}$ for $j \in \mathbb{Z}_m/\{\pm 1\}$ is well suited to recover some shortest generator, if $m = p^\alpha q^\beta$ for some distinct primes $p, q$. This leads to a new notion called **generator prime pairs**, from which we obtain a simple criterion, whether the index of this generated group in $\mathbb{Z}[\xi_m]^\times$ is finite or not. Moreover, we prove in the finite case that the index is sufficiently small, as long as the class number $h_m^+$ is bounded by some polynomial in $m$, and the norm of the dual vectors is small enough.
Since we frequently use the field $\mathbb{Q}(\xi_m + \xi_m^{-1})$, which is the maximal real subfield of the cyclotomic field $\mathbb{Q}(\xi_m)$, we collect some basic results for the general case of CM-fields $K$ and prove that if one can recover shortest generators in $K$ with this algorithmic approach, i.e., one has a well suited basis for the unit group $\mathcal{O}_K$, then one can also recover shortest generators in their maximal real subfields $K^+$ and vice versa.
The last chapter is dedicated to the *ideal shortest vector problem* (*ideal-SVP*), where the task is to find some short elements in arbitrary ideals in the Minkowski embedding. As shown in [CDPR16, CDW16], one can efficiently find a solution of the ideal shortest vector problem up to the approximation factor $\exp\left(\tilde{O}(\sqrt{n})\right)$ in cyclotomic fields of prime power conductor with quantum computers. By solving the *close principal multiple problem* (*CPM*), this problem can be reduced to a principal ideal shortest vector problem. Again, we generalize their results to cyclotomic fields of conductor $m = p^\alpha q^\beta$ for some $(\alpha, \beta)$-generator prime pair $(p, q)$.

## 1.1 Cryptographic Implications

Since we only extend the results of [CDPR16, CDW16] to cyclotomic fields of conductor $m = p^\alpha q^\beta$ for $(\alpha, \beta)$-generator prime pairs $(p, q)$, we obtain the same cryptographic implications, which are:

- There is a quantum polynomial time algorithm for SG-PIP, implying a key-recover attack for the mentioned cryptographic schemes of [SV10, GGH13] in cyclotomic fields $\mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$ for $(\alpha, \beta)$-generator prime pairs $(p, q)$. Hence, SG-PIP based schemes are broken by quantum computers in this case.
- There is a quantum polynomial time algorithm for solving the $\exp\left(\tilde{O}(\sqrt{n})\right)$-approximate ideal SVP in cyclotomic fields $\mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$ for $(\alpha, \beta)$-generator prime pairs $(p, q)$, where $n = \varphi(m)$.

See [CDPR16, Implications and discussion].
However, most of today's promising schemes are not SG-PIP based and rely on the hardness of the *short integer solution problem* (*SIS*) and *learning with error* (*LWE*), both of them in the average case. To obtain better or more efficient results, one can consider these problems in the more structured version over lattices induced by ideals in certain rings, called *ring short integer solution problem* (*RSIS*) and *ring learning with error* (*RLWE*). These two problems, RSIS and RLWE, are related to the approximate ideal SVP. Ajtai and Regev have shown that solving the short integer solution problem and learning with error in the average cases is less or equal hard as solving the approximate ideal SVP in the worst case for good enough approximation factors, see [Ajt99, Reg09]. However, the approximation factor $\exp\left(\tilde{O}(\sqrt{n})\right)$ considered in this work is too large to affect cryptographic schemes relying on RSIS and RLWE. Nevertheless, in the recent past many improvements and generalizations were presented to obtain better approximation factors and faster algorithms for structured ideals, at least for certain number fields or rings.

# 2 Preliminaries

## 2.1 Overview

In this chapter we give an introduction and overview of the used mathematical objects and definitions in this thesis. We assume that the reader has basic algebraic knowledge and is familiar with some fundamental ideas of analytic and algebraic number theory. Like several parts of this thesis, our preliminaries are partly similar to the ones in [CDPR16], since we extend the results given in that paper.

## 2.2 Notation

### 2.2.1 General

We denote the natural numbers without zero by $\mathbb{N} := \{1, 2, 3, ...\}$ and the natural numbers including zero by $\mathbb{N}_0 := \{0, 1, 2, 3, ...\}$. 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". For non-empty sets $A$ and $B$ we define $B^A := \{f : A \to B |\ f \text{ is a function}\}$ as the set of all functions that map from $A$ to $B$ and denote its elements by $(b_i)_{i \in A} \in B^A$. We interpret $B^A$ as the set of all vectors with entries in $B$, whose components are indexed over $A$. In the case that $B = \mathbb{R}$ or $B = \mathbb{C}$ and $A$ is finite, this is equivalent to the set $\mathbb{R}^n$ or $\mathbb{C}^n$, respectively. 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 $\mathbf{x}_1, ..., \mathbf{x}_k \in \mathbb{R}^n$ we write $(\mathbf{x}_1, ..., \mathbf{x}_k) =: \mathbf{X} \in \mathbb{R}^{n \times k}$ for the $n \times k$ matrix $\mathbf{X}$ whose columns are the vectors $\mathbf{x}_1, ..., \mathbf{x}_k$. The canonical scalar product and the euclidean norm over $\mathbb{R}^n$ are denoted by $\langle \cdot, \cdot \rangle$ and $|| \cdot ||_2$. The scalar product $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^n$ is antilinear in the second argument.
Let $G$ be a group, $H \subseteq G$ be a subgroup and $S \subseteq G$ an arbitrary set. We denote the index of $H$ in $G$ by $[G : H] := \left|{}^{G}/_{H}\right|$. Furthermore we define $\langle S \rangle$ to be the smallest subgroup of $G$ containing $S$. If $a_1, ..., a_n \in G$, we simplify $\langle a_1, ..., a_n \rangle := \langle a_i |\ i = 1, ..., n \rangle := \langle \{a_1, ..., a_n\} \rangle$. The order of an element $a \in G$ is defined by $\text{ord}(a) := |\langle a \rangle|$.
Further we define $\mathbb{Z}_m := {}^{\mathbb{Z}}/_{m\mathbb{Z}}$ for $m \in \mathbb{N}$. We will switch implicitly and fluently between the cosets of $\mathbb{Z}_m$ and arbitrary representatives in $\mathbb{Z}$. The common rounding function is denoted by $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor \in \mathbb{Z}$. For a vector $\mathbf{v} = (v_1, ..., v_n)^T \in \mathbb{R}^n$ we define $\lfloor v \rceil := (\lfloor v_1 \rceil, ..., \lfloor v_n \rceil)^T \in \mathbb{Z}^n$ component wise.

### 2.2.2 Rings

In this work all rings are commutative rings with 1. Let $R$ be a ring. We denote the set of units in $R$ by $R^\times$. For example, if $K$ is a field, we have $K^\times = K \backslash \{0\}$. For two subsets $A, B \subseteq R$ we define $A + B := \{a + b \in R |\ a \in A, b \in B\}$, $A \cdot B := \{a \cdot b \in R |\ a \in A, b \in B\}$ and for simplification $a + A := \{a\} + A$ and $a \cdot A := \{a\} \cdot A$ for $a \in R$. Note that the multiplication of the two sets $A$ and $B$ differs slightly from the multiplication of two ideals in $R$, namely we do not take finite sums over the products of their elements. Like for groups, for any subset $S \subseteq R$ of the ring $R$ we define the subring $\langle S \rangle$ as the smallest subring of $R$ containing $S$. Again, we simplify the notation by $\langle a_1, ..., a_n \rangle := \langle a_i |\ i = 1, ..., n \rangle := \langle \{a_1, ..., a_n\} \rangle$ for $a_1, ...a_n \in R$.

### 2.2.3 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).
For a Galois extension $L/K$ we denote the corresponding Galois group by

$$\mathrm{Gal}(L/K) := \{\sigma : L \to L |\ \sigma \text{ is a homomorphism with } \sigma|_K = \mathrm{id}_K\}.$$

Furthermore the algebraic closure of $K$ is denoted by $\overline{K}$.
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 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 $\alpha \in \mathcal{O}_K$. Note that $\mathbb{Z}$ is **integrally closed**, which means $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
W.l.o.g. it is sufficient to consider $K \subseteq \mathbb{C}$ for an algebraic number field $K$, because there is only one algebraic closure of $\mathbb{Q}$ up to isomorphisms, so we reduce to the case $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Note that $\mathcal{O}_K$ is a subring of $K$, see for example [NS99, p. 7].
A **fractional ideal** $I$ in an algebraic number field $K$ is a finitely generated $\mathcal{O}_K$-module with $I \neq \{0\}$. **Integral ideals** are ideals in $K$ not equal $\{0\}$. 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 product of two fractional ideals $\mathfrak{a}, \mathfrak{b}$ in $K$ is defined as

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i \cdot b_i \in K \,\middle|\, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N}_0 \right\}.$$

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 principle fractional ideals $\mathcal{P}_K$. By $[\mathfrak{a}]$ we denote the equivalence class of $\mathfrak{a} \in \mathcal{I}_K$ in $\mathrm{Cl}_K$. The **class number** $h_K$ of an algebraic number field $K$ is defined as the cardinality of its class group, i.e., $h_K := |\mathrm{Cl}_K| < \infty$, see [NS99, §3. Ideals].
Let $L/K$ be a finite field extension and $x \in L$. We define the $K$-linear mapping

$$\begin{aligned} \varphi_x : L &\to L \\ \alpha &\mapsto x \cdot \alpha \end{aligned}$$

and the **norm** of $x$ by $N_{L/K}(x) := \det(\varphi_x)$. It is easy to see that the norm is multiplicative, i.e., $N_{L/K}(x \cdot y) = N_{L/K}(x) \cdot N_{L/K}(y)$ for all $x, y \in L$. We will need the following basic facts from algebraic number theory.

**Lemma 2.2.1.** *Let $K$ be an algebraic number field. Then the following holds.*

1.) *For all $z \in \mathcal{O}_K$ we have $N_{K/\mathbb{Q}}(z) \in \mathbb{Z}$.*

2.) *Let $n = [K:\mathbb{Q}]$ and $\sigma_1, ..., \sigma_n$ the $n$ different homomorphisms $K \to \mathbb{C}$. Then for all $x \in K$*

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$$

*holds.*

3.) *For $\alpha \in K$ and its minimal polynomial $m_{\alpha,\mathbb{Q}} = \sum_{i=0}^{n} c_i X^i \in \mathbb{Q}[X]$ over $\mathbb{Q}$ we have*

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = (-1)^n c_0.$$

*4.) Let $\alpha \in K$ and $k := [K : \mathbb{Q}(\alpha)]$. Then it holds*

$$N_{K/\mathbb{Q}}(\alpha) = \left(N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\right)^k.$$

A proof can be found in the standard literature about algebraic number theory, e.g., [NS99].
The **norm** of an ideal $\mathfrak{a} \neq 0$ in an algebraic number field $K$ is defined as

$$N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}] \in \mathbb{N}.$$

If $\mathfrak{a}$ is principal, i.e., $\mathfrak{a} = g\mathcal{O}_K$ for some $g \in \mathcal{O}_K \backslash \{0\}$, then it holds

$$N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(g)|.$$

The norm can be uniquely extended to a homomorphism

$$N : J_K \to \mathbb{R}_{>0}$$

over all fractional ideals in $K$.

**Lemma 2.2.2.** *Let $K$ be an algebraic number field. Then for $\alpha \in K$ the following are equivalent.*

*1.) $\alpha$ is integral, i.e., $\alpha \in \mathcal{O}_K$.*

*2.) The minimal polynomial $m_{\alpha,\mathbb{Q}}$ of $\alpha$ over $\mathbb{Q}$ lies in $\mathbb{Z}[X]$.*

*(The minimal polynomial is always monic).*

*Proof.* We have to prove two directions.

- "*(2) ⇒ (1)*": The minimal polynomial $m_{\alpha,\mathbb{Q}}$ is monic, hence *(1)* follows directly from the definition of $\mathcal{O}_K$.
- "*(1) ⇒ (2)*": Let $f \in \mathbb{Z}[X]$ be a monic polynomial with $f(\alpha) = 0$. Furthermore let $L \subseteq \mathbb{C}$ be a splitting field of $m_{\alpha,\mathbb{Q}}$. Note that $L$ is an algebraic number field. We know $m_{\alpha,\mathbb{Q}} | f$ in $\mathbb{Q}[X]$, so for each root $a_i \in L$ of $m_{\alpha,\mathbb{Q}}$ we have $f(a_i) = 0$, i.e., $a_i \in \mathcal{O}_L$ for $i = 1, ..., d := \deg(m_{\alpha,\mathbb{Q}})$. We conclude from the factorization $m_{\alpha,\mathbb{Q}} = \prod_{i=1}^{d} (X - a_i)$ over $L$, that the coefficients of $m_{\alpha,\mathbb{Q}}$ lies in $\mathbb{Q}$ by definition and are integral in $L$, since $\mathcal{O}_L$ is a ring. However, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, hence $m_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X]$.

□

Note that the proof of Lemma 2.2.2 would also work for non finite algebraic field extensions $K/\mathbb{Q}$.

**Lemma 2.2.3.** *Let $K$ be an algebraic number field, then the following holds.*

$$\mathcal{O}_K^\times = \left\{\alpha \in \mathcal{O}_K \,\middle|\, |N_{K/\mathbb{Q}}(\alpha)| = 1\right\}.$$

*Proof.* For $\alpha \in \mathcal{O}_K^\times$ there exists an element $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$ by definition. The multiplicativity of the norm and Lemma 2.2.1, property 1.) implies the equation

$$1 = \mathbb{N}_{K/\mathbb{Q}}(1) = \mathbb{N}_{K/\mathbb{Q}}(\alpha\beta) = \underbrace{\mathbb{N}_{K/\mathbb{Q}}(\alpha)}_{\in\mathbb{Z}} \underbrace{\mathbb{N}_{K/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}},$$

from which we conclude $\mathbb{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$. So it remains to be proven that elements in $\mathcal{O}_K$ with norm $\pm 1$ are units. Let $m_{\alpha,\mathbb{Q}} = \sum_{i=0}^{d} c_i X^i \in \mathbb{Z}[X]$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$, where we have used Lemma 2.2.2, and $k := [K : \mathbb{Q}(a)]$. Lemma 2.2.1, property 3.) and 4.) yield

$$\pm 1 = N_{K/\mathbb{Q}}(\alpha) = \left(N_{\mathbb{Q}(a)/\mathbb{Q}}(\alpha)\right)^k = (-1)^{kd} c_0^k,$$

which implies $c_0 = \pm 1$, since $c_0 \in \mathbb{Z}$. Hence $\alpha^{-1} \in K^\times$ is a root of the monic (up to sign) polynomial $\sum_{i=0}^{d} c_i X^{d-i} \in \mathbb{Z}[X]$ as we see by multiplying the following equation with $(\alpha^{-1})^d$

$$\begin{aligned} 0 &= \alpha^d + c_{d-1}\alpha^{d-1} + \ldots + c_1\alpha \pm 1 \\ \Rightarrow\ 0 &= 1 + c_{d-1}\alpha^{-1} + \ldots + c_1(\alpha^{-1})^{d-1} \pm (\alpha^{-1})^d, \end{aligned}$$

i.e., $\alpha^{-1} \in \mathcal{O}_K$ and therefore $\alpha \in \mathcal{O}_K^\times$. □

**Lemma 2.2.4.** *Let $K$ be an algebraic number field, then the group of roots of unity $\mu(K)$ is finite.*

*Proof.* Obviously $\mu(K)$ is a group. Let $\xi \in \mu(K)$ have order $m \in \mathbb{N}$. We conclude from the inequality

$$\infty > [K : \mathbb{Q}] \geq [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m) = \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \left(p^{e_p - 1}(p-1)\right) \geq \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \max\{p^{e_p-1}, p-1\},$$

where $\prod_{p \mid m} p^{e_p} = m$ is the prime factorization of $m$ with $e_p \in \mathbb{N}$, that there are only finitely many possible primes which can occur with only finitely many possible exponents in the factorization of $m$. Therefore there are only finitely many possible candidates for $m$. The fact that there exists exactly $\varphi(m)$-many roots of unity of order $m$ yields the stated claim. □

## 2.3 Lattices

**Definition 2.3.1** (Lattice)**.** *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 $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ with $\mathcal{L} = \mathbb{Z}\boldsymbol{v}_1 + \ldots + \mathbb{Z}\boldsymbol{v}_k$. The vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ are called **basis** of the lattice $\mathcal{L}$. If $V = \mathbb{R}^n$, we write $\mathcal{L}(\boldsymbol{B}) := \mathbb{Z}\boldsymbol{b}_1 + \ldots + \mathbb{Z}\boldsymbol{b}_k$ for the lattice whose basis is given by the columns of a matrix $\boldsymbol{B} \in \mathbb{R}^{n \times k}$. 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 $\mathcal{L}' \subseteq \mathcal{L}$.*

**Remark 2.3.2.** *In general, the basis of a lattice is not unique, for example*

$$\mathbb{Z}^2 = \mathcal{L}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \mathcal{L}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right).$$

The following is a non trivial criterion whether a subgroup of $\mathbb{R}^n$ is a lattice.

**Theorem 2.3.3** ([NS99, Proposition (4.2)])**.** *An (additive) subgroup $\mathcal{L} \subseteq \mathbb{R}^n$ is a lattice iff it is discrete.*

**Definition 2.3.4** (Dual basis)**.** *The **dual basis** $\boldsymbol{B}^* = (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_k^*) \in \mathbb{R}^{n \times k}$ to a lattice $\mathcal{L}(\boldsymbol{B}) \subseteq \mathbb{R}^n$ is defined as the $\mathbb{R}$-basis of $span(\boldsymbol{B}) = \boldsymbol{B} \cdot \mathbb{R}^k$ with the following property:*

$$\langle \boldsymbol{b}_i^*, \boldsymbol{b}_j \rangle = \delta_{i,j} \quad \text{for all } i, j \in \{1, \ldots, k\}.$$

*In other words, $\boldsymbol{B}^* \in \mathbb{R}^{n \times k}$ is the unique matrix with the properties*

$$\boldsymbol{B}^T \cdot \boldsymbol{B}^* = (\boldsymbol{B}^*)^T \cdot \boldsymbol{B} = \boldsymbol{I}_k$$

*and*

$$span(\boldsymbol{B}) = span(\boldsymbol{B}^*),$$

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

We first prove that the dual basis is unique.

**Lemma 2.3.5.** *Let $\boldsymbol{B} \in \mathbb{R}^{n\times k}$ be a basis of the lattice $\mathscr{L}(\boldsymbol{B}) \subseteq \mathbb{R}^n$. Then, if existent, the dual basis $\boldsymbol{B}^*$ is unique.*

*Proof.* Let $\mathbf{D}, \mathbf{D}' \in \mathbb{R}^{n\times k}$ be some dual basis to $\mathbf{B}$. Then

$$\operatorname{span}(\mathbf{D}) = \operatorname{span}(\mathbf{B}) = \operatorname{span}(\mathbf{D}'),$$

hence we can write each column $\mathbf{D}_1, ..., \mathbf{D}_k$ of $\mathbf{D}$ as a linear combination of the columns $\mathbf{D}'_1, ..., \mathbf{D}'_k$, i.e., $\mathbf{D}_i = \sum_{l=1}^{k} \lambda_{i,l}\mathbf{D}'_l$. Therefore, we conclude

$$\delta_{i,j} = \langle \mathbf{D}_i, \mathbf{B}_j \rangle = \sum_{l=1}^{k} \lambda_{i,l} \underbrace{\langle \mathbf{D}'_l, \mathbf{B}_j \rangle}_{=\delta_{l,j}} = \lambda_{i,j},$$

which yields $\mathbf{D} = \mathbf{D}'$. □

The next theorem proves the existence of the dual basis by providing an explicit formula for its computation.

**Theorem 2.3.6.** *Let $\boldsymbol{B} \in \mathbb{R}^{n\times k}$ be a basis of the lattice $\mathscr{L}(\boldsymbol{B}) \subseteq \mathbb{R}^n$. The dual basis is given by*

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

*Proof.* We first prove that $(\mathbf{B}^T\mathbf{B})^{-1}$ is well defined. Let $\mathbf{y} \in \mathbb{R}^k$ with $0 = \mathbf{B}^T\mathbf{B}\mathbf{y}$, then $0 = \mathbf{y}^T\mathbf{B}^T\mathbf{B}\mathbf{y}$ and therefore $0 = \mathbf{B}\mathbf{y}$, but $\mathbf{B}$ has rank $k$, hence $\mathbf{y} = 0$, which implies that the $k \times k$ matrix $\mathbf{B}^T\mathbf{B}$ is injective and therefore invertible.
From this follows

$$\mathbf{B}^T\left(\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}\right) = (\mathbf{B}^T\mathbf{B})(\mathbf{B}^T\mathbf{B})^{-1} = \mathbf{I}_k$$
$$\left(\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}\right)^T\mathbf{B} = (\mathbf{B}^T\mathbf{B})^{-1}(\mathbf{B}^T\mathbf{B}) = \mathbf{I}_k.$$

For all $\mathbf{x} \in \operatorname{span}(\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1})$ there is a $\mathbf{y} \in \mathbb{R}^k$ such that $\mathbf{x} = \mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}\mathbf{y}$ and therefore $\mathbf{x} = \mathbf{B}\left((\mathbf{B}^T\mathbf{B})^{-1}\mathbf{y}\right) \in \operatorname{span}(\mathbf{B})$, which implies $\operatorname{span}(\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}) \subseteq \operatorname{span}(\mathbf{B})$. Analogously follows $\operatorname{span}(\mathbf{B}) \subseteq \operatorname{span}(\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1})$, which yields $\mathbf{B}^* = \mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}$ by the uniqueness of the dual basis. □

If we have a full rank sublattice $\mathscr{L} = \mathscr{L}(\mathbf{B})$ of $\mathbb{Z}^n$, i.e., $\mathbf{B} \in \mathbb{Z}^{n\times n}$ and $\mathbf{B}$ has rank $n$, we are interested in finding a set of representatives for the cosets of the finite group $\mathbb{Z}^n/\mathscr{L}$ (the finiteness follows by the structure theorem for finitely generated modules over principal ideal domains). Therefore the matrix $\mathbf{B}$ can be (efficiently) transformed into the *Hermite normal form*, from which we obtain such a set of representatives.

**Definition 2.3.7.** *A matrix $\boldsymbol{H} \in \mathbb{Z}^{m\times n}$ with $n \geq m$ and rank $m$ is in **Hermite normal form** (**HNF**), if there is a lower triangular matrix $\boldsymbol{L} \in \mathbb{Z}^{m\times m}$ with $0 \leq l_{i,j} < l_{i,i}$ and $l_{i,j} = 0$ if $i < j$ for all $i = 1, ..., m$ and all $j = 1, ..., m$, such that*

$$\boldsymbol{H} = (\boldsymbol{L}, \boldsymbol{0}),$$

*where $\boldsymbol{0} \in \{0\}^{m\times(n-m)}$. The elements $l_i := l_{i,i} \in \mathbb{N}$ for $i = 1, ..., m$ are called **pivot elements** of $\boldsymbol{H}$.*

If we have a basis $\mathbf{B} = (\mathbf{b}_1, ..., \mathbf{b}_n) \in \mathbb{Z}^{n\times n}$ of a full rank sublattice $\mathscr{L}$ of $\mathbb{Z}^n$, we can do the following operations on $\mathbf{B}$, such that the resulting matrix remains a basis of the lattice $\mathscr{L}$.

- Switch two columns $\mathbf{b}_i$, $\mathbf{b}_j$ of $\mathbf{B}$, where $i \neq j$.
- Multiply a column $\mathbf{b}_i$ with $-1$.
- Add an integer multiplicative $a \cdot \mathbf{b}_j$ to a column $\mathbf{b}_i$, where $a \in \mathbb{Z}$ and $i \neq j$.

It is easy to see, that the resulting matrix remains a basis of the lattice $\mathscr{L}(\mathbf{B})$. With these operations, each basis $\mathbf{B}$ can be transformed efficiently into the *HNF*, which is the following theorem.

**Theorem 2.3.8** ([KB79])**.** *Let $\boldsymbol{B} \in \mathbb{Z}^{n \times n}$ with rank n, then there is an efficient algorithm which transforms the matrix $\boldsymbol{B}$ into the* HNF*, which only use the upper operations. The running time of this algorithm is polynomial in n and the required space is bounded by some polynomial in the binary encoding size of the entries of $\boldsymbol{B}$.*

If we have a full rank sublattice $\mathscr{L}(\mathbf{B})$ of $\mathbb{Z}^n$, whose basis $\mathbf{B}$ is given in *HNF*, the following theorem provides a set of representatives of $\mathbb{Z}^n/\mathscr{L}(\mathbf{B})$.

**Theorem 2.3.9.** *Let $\boldsymbol{B} = (\boldsymbol{b}_1, ..., \boldsymbol{b}_n) \in \mathbb{Z}^{n \times n}$ with rank n in Hermite normal form, and let $l_i = \boldsymbol{B}_{i,i} \in \mathbb{N}$ be the pivot elements of $\boldsymbol{B}$. Then the vectors*

$$(a_1, ..., a_n)^T \in \mathbb{Z}^n \text{ with } 0 \leq a_i < l_i \text{ for all } i = 1, ..., n$$

*form a set of representatives of $\mathbb{Z}^n/\mathscr{L}(\boldsymbol{B})$, i.e.,*

$$\mathbb{Z}^n/\mathscr{L}(\boldsymbol{B}) = \left\{(a_1, ..., a_n)^T + \mathscr{L}(\boldsymbol{B}) |\ 0 \leq a_i < l_i \text{ for all } i = 1, ..., n\right\}.$$

*Proof.* By assumption, $\mathbf{B}$ is in *HNF*, i.e., $\mathbf{B}$ is a lower triangular matrix with non zero, positive diagonal elements $l_i \in \mathbb{Z}$. Hence, if $(z_1, ..., z_n)^T \in \mathbb{Z}^n$, we reduce the first entry $z_1$ modulo $l_1$ by subtracting $a_1 \cdot \mathbf{b}_1$ from $(z_1, ..., z_n)^T$, where $a_1 := \left\lfloor \frac{z_1}{l_1} \right\rfloor$. The so resulting vector $(z_1', ..., z_n')^T = (z_1, ..., z_n)^T - a_1 \cdot \mathbf{b}_1$ satisfies $(z_1, ..., z_n)^T + \mathscr{L}(\mathbf{B}) = (z_1', ..., z_n')^T + \mathscr{L}(\mathbf{B})$ and $0 \leq z_1' < l_1$. By induction, we obtain a representative $(a_1, ..., a_n)^T \in \mathbb{Z}^n$ of $(z_1, ..., z_n)^T + \mathscr{L}(\mathbf{B})$ with $0 \leq a_i < l_i$ for all $i = 1, ..., n$. It is easy to see that these representatives correspond to different cosets. □

# 3 Algorithmic Approach

## 3.1 Overview

In this chapter we present the algorithm considered in [CDPR16] to recover a "short" generator $g$ of a principle fractional ideal in an algebraic number field $K$. The main idea is the following. Embed the unit group $\mathcal{O}_K^\times$ into $\mathbb{R}^n$ with $n = [K : \mathbb{Q}]$. It turns out, that the image of $\mathcal{O}_K^\times$ under this embedding is a lattice in $\mathbb{R}^n$. To make computations with this lattice, we need some basis of a subgroup of $\mathcal{O}_K^\times$ and therefore some basis of a sublattice of the embedding of $\mathcal{O}_K^\times$ with small index. We present an algorithm which reduces the logarithmic embedding of an arbitrary generator $g'$ of the fractional ideal $g\mathcal{O}_K^\times$ modulo this lattice by solving the closest vector problem and recovers $g$ from this arbitrary generator. The last section in this chapter discusses the probability aspects, that this algorithm recovers some shortest generator with non negligible probability, if the generator $g$ is drawn from some sufficient distribution over $K$.
We generalize the setting of [CDPR16] to the more general case of arbitrary algebraic number fields $K$, but consider the case of cyclotomic fields in some parts.

## 3.2 Logarithmic Embedding

**Definition 3.2.1** (Logarithmic embedding)**.** *Let $K$ be an algebraic number field with $[K : \mathbb{Q}] = n$. Moreover, let $r$ be the number of real embeddings of $K$, i.e., homomorphisms of the form $\delta_1, ..., \delta_r : K \to \mathbb{R}$, and $s$ the number of non real homomorphisms (up to complex conjugation) $\sigma_1, \overline{\sigma_1}, ..., \sigma_s, \overline{\sigma_s} \to \mathbb{C}$. Note that $n = r + 2s$ holds. We define the* ***logarithmic embedding*** *as*

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

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

From now on, the numbers $n, r, s \in \mathbb{N}_0$ for an algebraic number field $K$ are defined as in Definition 3.2.1. The following is a slightly different version of [NS99, Theorem (7.3)].

**Theorem 3.2.2** (Dirichlet's unit theorem)**.** *Let $K$ be an algebraic number field and $n = r + 2s$ as mentioned. The group $\Gamma := Log(\mathcal{O}_K^\times)$ is a lattice of dimension $k := r+s-1$, orthogonal to the vector $\boldsymbol{1} := (1, ..., 1) \in \mathbb{R}^{r+2s}$. We call $\Gamma$ the* ***log-unit lattice****.*

**Lemma 3.2.3.** *For an algebraic number field $K$ the following holds.*

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

*Proof.* The inclusion $\mu(K) \subseteq \ker\Big(\mathrm{Log}|_{\mathcal{O}_K^\times}\Big)$ is clear since roots of unity are mapped to roots of unity under the automorphisms $\sigma$. To prove the reverse inclusion, let $\alpha \in \ker\Big(\mathrm{Log}|_{\mathcal{O}_K^\times}\Big) \subseteq \mathcal{O}_K^\times$. Then Lemma 2.2.2 states that $m_{\alpha,\mathbb{Q}}(X) = \sum_{i=0}^{t} a_i X^i \in \mathbb{Z}[X]$, i.e., $a_t = 1$ and $a_i \in \mathbb{Z}$ for all $i = 0, ..., t$. Furthermore, by Galois theory we can write $m_{\alpha,\mathbb{Q}}(X) = \prod_{i=1}^{t}(X - \sigma_i(\alpha))$ for sufficient $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$. The assumption

$\alpha \in \ker\left(\mathrm{Log}|_{\mathcal{O}_K^\times}\right)$ implies $|\sigma_i(\alpha)| = 1$ for all $i = 1, ..., t$, hence we can bound the coefficients $a_i \in \mathbb{Z}$ of $m_{\alpha,\mathbb{Q}}$ by

$$|a_i| \leq \binom{t}{i} \leq \binom{t}{\lceil \frac{t}{2} \rceil} \text{ for all } i = 0, ..., t.$$

For each power $\alpha^l$ of $\alpha$ with $l \in \mathbb{N}$ we get the same bounds for the integer coefficients of the minimal polynomial $m_{\alpha^l,\mathbb{Q}} \in \mathbb{Z}[X]$, since $[\mathbb{Q}(\alpha^l) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = t$. We conclude that there are only finitely many monic polynomials in $\mathbb{Z}[X]$, which can have a power of $\alpha$ as a root. This implies that $\alpha$ is of finite order, i.e., $\alpha \in \mu(K)$. □

**Corollary 3.2.4.** *The group of units $\mathcal{O}_K^\times$ is isomorphic to $\mu(K) \times \mathbb{Z}^{r+s-1}$, which means there are units $\eta_1, ..., \eta_k \in \mathcal{O}_K^\times$ (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 $e_1, ..., e_k \in \mathbb{Z}$ and $\zeta \in \mu(K)$.*

*Proof.* This follows immediately from Dirichlet's unit Theorem 3.2.2 and Lemma 3.2.3. □

Such sets $\{\eta_1, ...\eta_k\} \subseteq \mathcal{O}_K^\times$ of multiplicative independent units which generates $\mathcal{O}_K^\times$ up to roots of unity like in Corollary 3.2.4 are called **fundamental systems of units** of $\mathcal{O}_K$.
We are now prepared to define what we mean by "short generator" of a principal fractional ideal in an algebraic number field.

**Definition 3.2.5.** *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 its logarithmic embedding.*

Note that the minimum in Definition 3.2.5 exists because $\mathrm{Log}(\mathcal{O}_K^\times) \subseteq \mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$ by Dirichlet's unit Theorem 3.2.2 and Theorem 2.3.3. Therefore, $\mathrm{Log}(g) + \mathrm{Log}(\mathcal{O}_K^\times) \subseteq \mathbb{R}^n$ is a discrete subset of $\mathbb{R}^n$, where $n = [K : \mathbb{Q}]$.
One could soften the definition of a shortest generator by saying $g'$ is a $C$-**approximate shortest generator** of $g\mathcal{O}_K$ if it is guaranteed to be relatively small, i.e., $||\mathrm{Log}(g')||_2 \leq C \cdot \min_{u \in \mathcal{O}_K^\times} ||\mathrm{Log}(g \cdot u)||_2$ holds for some fixed $C \geq 1$. W.l.o.g., we reduce to the case of recovering shortest generators, but all algorithmic results also works for $C$-approximate shortest generators.
If the number field $K$ has no real embedding, i.e., $n = 2s$, it is sufficient to use the **reduced logarithmic embedding** of $K^\times$:

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

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

## 3.3 Cyclotomic Fields

**Definition 3.3.1** (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., $ord(\xi_m) = m$. If $m \not\equiv 2 \mod 4$, the number $m$ is called the **conductor** of $K_m$.*

**Remark 3.3.2.** *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. [NS99, 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., $\sigma_{-i} = \overline{\sigma_i}$, which yields the following statement.

**Corollary 3.3.3** (Dirichlet's unit theorem for cyclotomic fields)**.** *The image $\Gamma_m := Log_r(\mathcal{O}_m^\times)$ is a $\varphi(m)/2 - 1$ dimensional lattice in $\mathbb{R}^{n/2}$ orthogonal to the vector $\mathbf{1} \in \mathbb{R}^{n/2}$ for $m \geq 3$ and $n = \varphi(m)$.*

*Proof.* This is the statement of Dirichlet's unit Theorem 3.2.2 for arbitrary algebraic number fields, together with the fact that there are no real embeddings of $\mathbb{Q}(\xi_m)$ for $m \geq 3$. □

**Lemma 3.3.4.** *For a cyclotomic field $K_m$ it holds:*

$$\mu(K_m) = \langle \pm\xi_m \rangle = \left\{ \pm\xi_m^i \mid i \in \mathbb{Z} \right\}$$

*Proof.* Since $(\pm\xi_m)^{2m} = 1$, we get the inclusion $\mu(K_m) \supseteq \langle \pm\xi_m \rangle$. 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 $\eta \in \mu(K_m) \subseteq \mathbb{Q}(\xi_m)$, hence we get $\mathbb{Q}(\eta) = \mathbb{Q}(\xi_m)$, which implies $\varphi(t) = \varphi(m)$ for $t := \mathrm{ord}(\eta) = |\mu(K_m)|$. We distinguish two cases to prove $\eta \in \langle \pm\xi_m \rangle$:

1. $m$ is even: The order of $\xi_m \in \mu(K_m)$ is $m$, so we obtain with basic group theory that $m|t$. Let $k = \prod_{\substack{p|t \\ p\in\mathbb{P}}} p^{e_p}$ be the prime factorization of $t \geq 2$ with $e_p \in \mathbb{N}$. We obtain $m = \prod_{\substack{p|t \\ p\in\mathbb{P}}} p^{e'_p}$ for suitable $e'_p \in \mathbb{N}_0$ and $e'_p \leq e_p$, since $m|t$. By the multiplicativity of the $\varphi$-function for coprime numbers we obtain

$$\prod_{\substack{p|t \\ p\in\mathbb{P}}} \varphi\left(p^{e'_p}\right) = \varphi(m) = \varphi(t) = \prod_{\substack{p|t \\ p\in\mathbb{P}}} \varphi\left(p^{e_p}\right).$$

   For each $p \in \mathbb{P}$ and $e_p, e'_p \in \mathbb{N}_0$ it holds $e'_p < e_p \Rightarrow \varphi(p^{e'_p}) < \varphi(p^{e_p})$, except the case $p = 2$, $e'_2 = 0$ and $e_2 = 1$. So for $m$ even (i.e., $e'_2 \geq 1$) we obtain $e'_p = e_p$ for all $p \in \mathbb{P}$ and therefore $m = 7$. This shows $t = \mathrm{ord}(\eta) = \mathrm{ord}(\xi_m)$.

2. $m$ is odd: The order of $-\xi_m \in \mu(K_m)$ is $2m$, so it follows analogously to the even case that $2m = t$, since $\varphi(2m) = \varphi(2) \cdot \varphi(m) = \varphi(m) = \varphi(t)$.

□

## 3.4 General Algorithmic Approach

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 3.4.1** (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 $\lambda_1(\mathcal{L}) := \min_{\boldsymbol{v}\in\mathcal{L}\setminus\{\boldsymbol{0}\}} ||\boldsymbol{v}||_2$, find the unique vector $\boldsymbol{v} \in \mathcal{L}$ with $||\boldsymbol{v}-\boldsymbol{t}||_2 \leq r$.*

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

**Algorithm 3.1:** Round-off Algorithm

**Input:** $\mathbf{B}, \mathbf{t}$.
**Output:** Closest vector $\mathbf{v} \in \mathcal{L}$ to $t$.
$\mathbf{a} \leftarrow \lfloor (\mathbf{B}^*)^T \cdot \mathbf{t} \rceil$
$\mathbf{v} \leftarrow \mathbf{B} \cdot \mathbf{a}$
**return** $(\mathbf{v}, \mathbf{a})$

**Lemma 3.4.2** (Correctness Round-off Algorithm). *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 $\langle \boldsymbol{b}_j^*, \boldsymbol{e}\rangle \in [-\frac{1}{2}, \frac{1}{2})$ holds for all $j = 1, ..., k$, the Round-off Algorithm 3.1 outputs $\boldsymbol{v} = \boldsymbol{B} \cdot \boldsymbol{a}$ by input $\boldsymbol{B}, \boldsymbol{t}$.*

*Proof.* Let $\mathbf{z} \in \mathbb{Z}^k$ with $\mathbf{v} = \mathbf{Bz}$, we obtain $(\mathbf{B}^*)^T \cdot \mathbf{t} = \mathbf{z} + (\mathbf{B}^*)^T \cdot \mathbf{e}$, which implies $\mathbf{a} = \lfloor (\mathbf{B}^*)^T \cdot \mathbf{t} \rceil = \mathbf{z}$ by the assumption $\langle \mathbf{b}_j^*, \mathbf{e}\rangle \in [-\frac{1}{2}, \frac{1}{2})$ for all $j = 1, ..., k$. The round-off algorithm outputs $\mathbf{B} \cdot \mathbf{a} = \mathbf{Bz} = \mathbf{v}$, which proofs the claim. □

We give a short explanation of the Round-off Algorithm: The algorithm takes the input $\mathbf{t} := \mathbf{v} + \mathbf{e} \in \mathbb{R}^n$ and calculates the coefficient vector $(\mathbf{B}^*)^T \cdot \mathbf{t}$ of $\mathbf{t}$ with respect to basis $\mathbf{B}$. In the next step it rounds the coefficient vector to the next integer vector and outputs the lattice point corresponding to this integer vector, see Figure 3.1.

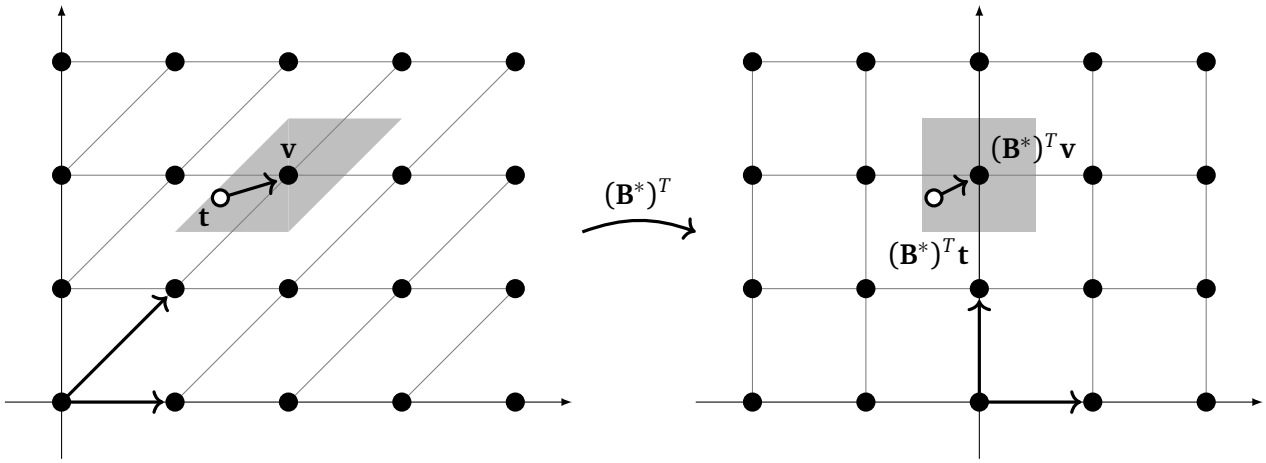



**Figure 3.1:** Round-off Algorithm

Note that in general the condition $\langle \mathbf{b}_j^*, \mathbf{e}\rangle \in \left[-\frac{1}{2}, \frac{1}{2}\right)$ for all $j = 1, ..., k$ does not guaranty that the vector $\mathbf{v}$ is the closest vector in $\mathcal{L}(\mathbf{B})$ to $\mathbf{t} = \mathbf{v} + \mathbf{e}$. Further the output depends on the the basis $\mathbf{B}$ of the lattice. In Figure 3.1 the grey area is the set of all vectors whose coefficient vectors only differ by maximally $\frac{1}{2}$ in

each component from the coefficient vector of $\mathbf{v}$ with respect to some basis $\mathbf{B}$, i.e., the grey area is the set of all vectors on which the Round-off Algorithm outputs $\mathbf{v}$. For a "nearly orthogonal" basis $\mathbf{B}$ the grey area is approximately the set of all vectors whose closest vector is $\mathbf{v}$, i.e., the Round-off Algorithm outputs really the closest vector in $\mathcal{L}(\mathbf{B})$ except for some small set. For results about the quality of the output of the Round-off Algorithm (under some assumptions to the basis) see [Bab86].
If one would be interested in solving BDD exactly in all possible inputs, this would be much harder, for some results about the approximate version see [LLM06].
Now we are prepared to introduce an algorithm which recovers a shortest generator of $g\mathcal{O}_K$ given an arbitrary generator $g' \in K^\times$ of $g\mathcal{O}_K$. This algorithm is presented in Algorithm 3.2 and illustrated in Figure 3.2.

**Algorithm 3.2:** Recovering a short generator with given basis of $\mathcal{O}_K^\times$

1 **Input:** A generator $g' = g \cdot u \in K^\times$ of $g\mathcal{O}_K$ with $u \in \mathcal{O}_K^\times$ 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 $\Gamma = \mathrm{Log}(\mathcal{O}_K^\times)$.
2 **Output:** A generator $g_e \in \mathcal{O}_K$ of $g\mathcal{O}_K$ with same norm as the short generator $g$.
3 $(a_1, ..., a_k)^T \leftarrow \lfloor (\mathbf{B}^*)^T \cdot \mathrm{Log}(g') \rceil$ (Round-off-Step)
4 $u' \leftarrow \prod_{i=1}^k b_i^{a_i}$
5 $g_e \leftarrow {}^{g'}\!/_{u'}$
6 **return** $g_e$

**Lemma 3.4.3** (Correctness of Algorithm 3.2)**.** *Let $K$ be an algebraic number field with $n = r+2s := [K : \mathbb{Q}]$ and $k := r+s-1$, $b_1, ..., b_k \in \mathcal{O}_K^\times$ a fundamental system of units of $\mathcal{O}_K^\times$ and $g \in K^\times$ a short generator of $g\mathcal{O}_K$ satisfying*

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

*Then for any generator $g' \in K^\times$ of $g\mathcal{O}_K$ Algorithm 3.2 outputs a short generator $g_e$ of $g\mathcal{O}_K$, i.e., $g\mathcal{O}_K = g_e\mathcal{O}_K$ and $||Log(g)||_2 = ||Log(g_e)||_2$.*

*Proof.* As $g'$ and $g$ are generators of the same fractional ideal, there exists a $u \in \mathcal{O}_K^\times$ such that $g' = g \cdot u$ and therefore $\mathrm{Log}(g') = \mathrm{Log}(g) + \mathrm{Log}(u)$. The round-off step of Algorithm 3.2 in line 3 outputs the coefficient vector of $\mathrm{Log}(u)$ with respect to the basis $\mathbf{B} := \{\mathrm{Log}(b_1), ..., \mathrm{Log}(b_k)\}$ by assumption on $\mathrm{Log}(g)$ and Lemma 3.4.2, i.e.

$$\mathrm{Log}(u) = \mathbf{B} \cdot (a_1, ..., a_k)^T = \mathrm{Log}\left(\prod_{i=1}^k b_i^{a_i}\right).$$

Lemma 3.2.3 states that there exist a $\eta \in \mu(K)$ such that $u = \eta \prod_{i=1}^k b_i^{a_i} = \eta u'$ where $u' := \prod_{i=1}^k b_i^{a_i}$, hence we conclude

$$g_e = \frac{g'}{u'} = \frac{\eta g u}{u} = \eta g.$$

This implies $g_e\mathcal{O}_K = g\mathcal{O}_K$ and $||\mathrm{Log}(g_e)||_2 = ||\mathrm{Log}(g)||_2$. □

**Theorem 3.4.4.** *Algorithm 3.2 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 by Theorem 2.3.6, and some matrix and vector multiplications of matrices and vectors of size $k$. This yields the claim. □

Again we give a short explanation of Algorithm 3.2. The main idea of this algorithm is to find the closest vector $\mathrm{Log}(u') \in \mathrm{Log}(\mathcal{O}_K^\times)$ to $\mathrm{Log}(g')$ in the lattice $\mathrm{Log}(\mathcal{O}_K^\times)$, which is a BDD-problem. Then $\mathrm{Log}(g') - \mathrm{Log}(u')$ is the shortest vector of $\mathrm{Log}(g') + \mathrm{Log}(\mathcal{O}_K^\times)$. The Round-off Algorithm provides the coefficient vector of $\mathrm{Log}(u')$ relative to the basis $\mathbf{B} = \{\mathrm{Log}(b_1), ..., \mathrm{Log}(b_k)\}$, from which we can recover $u' \in \mathcal{O}_K^\times$ (up to multiplication by some $\eta \in \mu(K)$) and therefore $g_e = {}^{g'}/_{u'}$, see Figure 3.2. As we are unable to solve the BDD-problem in the general case, we need the additional condition that $\left|\langle \mathrm{Log}(g), \mathrm{Log}(b_i)^* \rangle\right| < \frac{1}{2}$ holds for all $i = 1, ..., k$, to recover $g_e$ with the used Round-off Algorithm.

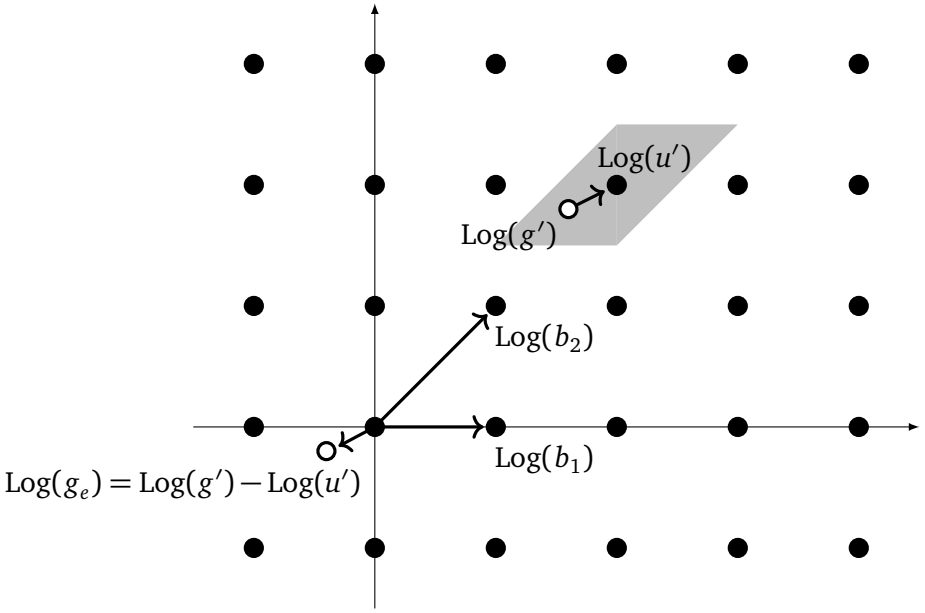



**Figure 3.2:** Algorithm 3.2

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 $\left|\langle \mathrm{Log}(g), \mathrm{Log}(b_i)^* \rangle\right| < \frac{1}{2}$ for all $i = 1, ..., k$ holds with a non negligible probability $\omega > 0$? The positive answer to this question can be split into two conditions:

1.) The dual basis is short enough, i.e. $||\mathrm{Log}(b_i)^*||_2$ is sufficiently small for all $i = 1, ..., k$.

2.) The vector $\mathrm{Log}(g)$ is small enough with non negligible probability $\omega > 0$. This is a condition on the distribution $D$ over $K$.

We specify and collect these two conditions in the following condition on the distribution $D$.

**Condition 3.4.5.** *Let $D$ be a probability distribution over $K$. If for all vectors $\mathbf{v}_1, ..., \mathbf{v}_k \in \mathbb{R}^n$ of Euclidean norm 1 which are orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^n$, and $M := \max\{||Log(b_1)^*||_2, ..., ||Log(b_k)^*||_2\}$ the inequalities*

$$\left|\langle Log(g), \mathbf{v}_i \rangle\right| < \frac{1}{2M} \quad \text{for all } i = 1, ..., k$$

*are satisfied with probability at least $\omega \in (0, 1)$, we say $D$ **satisfies this condition with parameter** $\omega$.*

**Theorem 3.4.6.** *If $D$ is a distribution over an algebraic number field $K$ satisfying Condition 3.4.5 with parameter $\omega \in (0, 1)$ and $g \in K$ is chosen from $D$, then Algorithm 3.2 outputs a generator $g_e \in K$ of $g\mathcal{O}_K$ with same Euclidean norm as $g$ with probability $\omega > 0$.*

*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 3.4.5 with parameter $\omega > 0$, 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 $\omega$. □

As shown in [CDPR16, Section 5] for algebraic number fields $K$ with no real embedding, i.e. $r = 0$, two natural distributions satisfy Condition 3.4.5 with a not to small parameter $\omega > 0$ if the $||\text{Log}(b_i)^*||_2$ are sufficiently small: The continuous Gaussian and a wide enough discrete Gaussian. In the next section we generalize this result for arbitrary algebraic number fields and a continuous Gaussian and other distributions. Therefore, in this case we can recover some shortest generator with non negligible probability $\omega > 0$.
There are two issues with Algorithm 3.2 which we did not mention yet. The first issue is that in reality all occurring instances, e.g. $g', b_1, ..., b_k \in K \subseteq \mathbb{C}$ and the vectors $\text{Log}(b_1), ..., \text{Log}(b_n)$, are given only with finite precision. The PIP algorithms presented in [BF14, Bia14, BS15] outputs for example a floating-point representation of $g'$ (or a similar format). By handling with sufficiently good multiplicative approximations of these occurring instances in Algorithm 3.2, the output $g_e$ can be made as good as the input $g'$. Therefore we ignore this issue from now on and consider all instances to be given exactly.
The second issue is that we implicitly assume in Algorithm 3.2 that we have a basis $b_1, ...b_k$ of $\mathcal{O}_K^\times$ (up to roots of unity), i.e., a fundamental set of units, with sufficiently short dual vectors. As we will see for example in the case of cyclotomic number fields $K = \mathbb{Q}(\xi_m)$, we only have a well suited basis of a subgroup of $\mathcal{O}_K^\times$ with (small) finite Index. We fix this with Algorithm 3.3 by enumerating over a set of a coset representatives of this subgroup in $\mathcal{O}_K^\times$.

**Algorithm 3.3:** 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 $\mathbf{B} := \{\text{Log}(b_1), ..., \text{Log}(b_k)\}$ is a basis of a subgroup of $\Gamma = \text{Log}(\mathcal{O}_K^\times)$ 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 $\mathcal{O}_K^\times/\mu(K)F$ (Algorithm 3.4)
$N \leftarrow \infty$
**for** $i = 1, ..., f$ **do**
    $g_e(i) \leftarrow$ output $g_e$ of Algorithm 3.2 with input $g'/u_i$ and $b_1, ..., b_k$
    **if** $||Log(g_e(i))||_2 < N$ **then**
        $g_h \leftarrow g_e(i)$
        $N \leftarrow ||\text{Log}(g_e(i))||_2$
**return** $g_h$

**Lemma 3.4.7** (Correctness of Algorithm 3.3)**.** *Let $K$ be an algebraic number field with $n = r + 2s = [K : \mathbb{Q}]$ and $k = r + s - 1$ as in Definition 3.2.1, $b_1, ..., b_k \in \mathcal{O}_K^\times$ a basis of a subgroup $F$ of $\mathcal{O}_K^\times$ with finite index $f := |\mathcal{O}_K^\times/\mu(K)F|$, and $g \in K^\times$ satisfying*

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

*Then for any generator $g' \in K^\times$ of $g\mathcal{O}_K$ Algorithm 3.2 outputs a generator $g_h$ of $g\mathcal{O}_K$, i.e. $g\mathcal{O}_K = g_h\mathcal{O}_K$ and $||Log(g_h)||_2 \leq ||Log(g)||_2$.*

*Proof.* The elements $g'$ and $g$ are generators of the same fractional ideal, hence they only differ by some unit $u \in \mathcal{O}_K^\times$. Therefore there exists $l \in \{1, ..., f\}$, $\eta \in \mu(K)$ and $b \in F$ such that $g' = g\eta u_l b$, where $u_1, ..., u_f$ denote the calculated set of representatives of $\mathcal{O}_K^\times/\mu(K)F$. Obviously $g'/u_l$ is also a generator of $g\mathcal{O}_K$ with $\text{Log}\left(g'/u_l\right) = \text{Log}(g) + \text{Log}(b)$. Analogue to the proof of Lemma 3.4.3 follows that the output $g_e(l)$ of Algorithm 3.2 with input $g'/u_l$ and $b_1, ..., b_k$ is $g_e(l) = g \cdot \xi$ for some $\xi \in \mu(K)$. Moreover, all outputs

$g_e(i)$ of Algorithm 3.2 are generators of $g\mathcal{O}_K$ because they only differ by some unit from $g$. Therefore Algorithm 3.3 outputs a generator $g_h$ of $g\mathcal{O}_K$ with

$$||\mathrm{Log}(g_h)||_2 = \min_{i=1,\dots,f} ||\mathrm{Log}(g_e(i))||_2 \leq ||\mathrm{Log}(g_e(l))||_2 = ||\mathrm{Log}(g)||_2.$$

□

In the case of cyclotomic number fields $K = \mathbb{Q}(\xi_m)$ for some special $m \in \mathbb{N}$ (especially if $m$ is a prime power) we can find such a well suited basis $b_1, \dots, b_k \in \mathcal{O}_K^\times$ of a subgroup with finite index depending only on $m$. Hence, the calculation of the set of representatives $u_1, \dots, u_f \in \mathcal{O}_K^\times$ of $\mathcal{O}_K^\times/\mu(K)F$ has to be done only once for each $m$, i.e., only once for each cyclotomic field $K = \mathbb{Q}(\xi_m)$, which is part of the public key. To obtain such a list of representatives, one could calculate fundamental system of units $\eta_1, \dots, \eta_k$ of $\mathcal{O}_K^\times$, using classical [BF14] or quantum [EHKS14] 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 [Was96, Proposition 2.7.]. Hence, the quantum algorithm runs in polynomial time in $m$. Furthermore, if we fix the maximal number of different primes which can occur in $m$, the quantum running time is even polynomial in $n = \varphi(m)$, since $n = \varphi(m) = m \cdot \frac{(p_1-1)}{p_1} \cdot \dots \cdot \frac{p_t-1}{p_t} \geq m\left(\frac{1}{2}\right)^t$ and therefore $n \in \Theta(m)$, if $p_1, \dots, p_t$ are the different primes occurring in $m$. After computing such a fundamental system of units, the basis $b_1, \dots, b_k$ of the subgroup $F$ can be written in terms of $\eta_1, \dots \eta_k$ with integer coefficients. If we write these coefficients in a matrix $\mathbf{M}$ and transform it into the *HNF*, we obtain a set of representatives for the coefficients by Theorem 2.3.9. From this we can compute the set of representatives $u_1, \dots, u_f \in \mathcal{O}_K^\times$. The exact algorithm is described in Algorithm 3.4.

**Algorithm 3.4:** Computing a set of representatives $u_1, \dots, u_f$ of $\mathcal{O}_K^\times/\mu(K)F$

**Input:** A fundamental system of units $\eta_1, \dots, \eta_k \in \mathcal{O}_K^\times$, a basis $b_1, \dots, b_k \in \mathcal{O}_K^\times$ of a subgroup $F$ of $\mathcal{O}_K^\times$ with finite index $f := [\mathcal{O}_K^\times : \mu(K)F]$.
**Output:** A set of representatives $u_1, \dots, u_f$ of $\mathcal{O}_K^\times/\mu(K)F$.
$\mathbf{E} := (\mathbf{e}_1, \dots, \mathbf{e}_k) \leftarrow (\mathrm{Log}(\eta_1), \dots, \mathrm{Log}(\eta_k))$
$\mathbf{B} := (\mathbf{b}_1, \dots, \mathbf{b}_k) \leftarrow (\mathrm{Log}(b_1), \dots, \mathrm{Log}(b_k))$
$\mathbf{M} \leftarrow (\mathbf{E}^*)^T \cdot \mathbf{B}$
$\mathbf{H} \leftarrow$ bring $\mathbf{M}$ in the *HNF*
$(l_1, \dots, l_k) \leftarrow (\mathbf{H}_{1,1}, \dots, \mathbf{H}_{k,k})$
Enumerate the set $\{0, \dots, l_1 - 1\} \times \dots \times \{0, \dots, l_k - 1\} = \left\{\left(a_1^i, \dots, a_k^i\right)^T \in \mathbb{Z}^n \mid i = 1, \dots, f\right\}$, where $f = l_1 \cdot \dots \cdot l_k$
**for** $i = 1, \dots, f$ **do**
    $u_i \leftarrow \eta_1^{a_1^i} \cdot \dots \cdot \eta_k^{a_k^i}$
**return** $u_1, \dots, u_f$

**Lemma 3.4.8** (Correctness Algorithm 3.4 and running time)**.** *Let $\eta_1, \dots, \eta_k \in \mathcal{O}_K^\times$ be a fundamental system of units, and $b_1, \dots, b_k \in \mathcal{O}_K^\times$ be a basis of a subgroup $F \subseteq \mathcal{O}_K^\times$ with finite index $f = [\mathcal{O}_K^\times : \mu(K)F]$. Then Algorithm 3.4 outputs a set of representatives $u_1, \dots, u_f \in \mathcal{O}_K^\times$ of $\mathcal{O}_K^\times/\mu(K)F$. Furthermore, the running time of Algorithm 3.4 is polynomial in $n = [K : \mathbb{Q}]$ and $f$.*

*Proof.* One can easily prove that

$$\mathbb{Z}^k/\mathcal{L}(\mathbf{M}) \to \mathcal{L}(\mathbf{E})/\mathcal{L}(\mathbf{B}) \to \mathcal{O}_K^\times/\mu(K)F$$
$$(a_1, \dots, a_k)^T + \mathcal{L}(\mathbf{M}) \mapsto \mathbf{E} \cdot (a_1, \dots, a_k)^T + \mathcal{L}(\mathbf{B}) \mapsto \eta_1^{a_1} \cdot \dots \cdot \eta_k^{a_k} \cdot \mu(K)F$$

are group isomorphisms. Hence we have to find a set of representatives of $\mathbb{Z}^k/\mathscr{L}(\mathbf{M})$, which is given by Theorem 2.3.9, if we transform the basis $\mathbf{M}$ into the basis $\mathbf{H}$ in *HNF* of $\mathscr{L}(\mathbf{M})$. This yields the correctness of the algorithm. The transformation into the *HNF* is polynomial in $k$ and therefore in $n \geq k$ by Theorem 2.3.8, and the loop in *line 9* has polynomial running time in $f$ and $n$. □

**Theorem 3.4.9.** *If one has precalculated a fundamental system of units $\eta_1, ..., \eta_k \in \mathcal{O}_K^\times$, the (classical) running time of Algorithm 3.3 is polynomial in $n = [K : \mathbb{Q}]$ and $f$.*
*In particular, if $K = \mathbb{Q}(\xi_m)$ is a cyclotomic field, there is a quantum algorithm which computes a fundamental system of units $\eta_1, ..., \eta_k \in \mathcal{O}_K^\times$ in polynomial time in m, hence the quantum running time of Algorithm 3.3 for cyclotomic fields is polynomial in m and $f$.*

*Proof.* The calculation of the set of representatives in *line 3* is polynomial in $n$ and $f$ by Lemma 3.4.8. The loop in *line 5-8* has polynomial running time in $n$ and $f$ by Theorem 3.4.4. This yields the claim. The quantum running time follows from [EHKS14] and $|d_K| \in O(n\log(n))$ ([Was96, Proposition 2.7.]) as mentioned before. □

We will argue later that it is reasonable that the index $f$ of some given subgroup of $\mathcal{O}_K^\times$, in the case that $K = \mathbb{Q}(\xi_m)$ is a cyclotomic field, is bounded by some polynomial in $m$, if $m$ is a prime power or contains only two different prime numbers with some properties. This yields a quantum polynomial running time in $m$ of Algorithm 3.3 in this case.
We close this section with the observation that the index of a subgroup $C$ in $\mathcal{O}_K^\times$ up to roots of unity is equal to the index of the generated sublattice $\mathrm{Log}(C)$ in $\Gamma$.

**Lemma 3.4.10.** *Let $K$ be an algebraic number field, $\Gamma = Log(\mathcal{O}_K^\times)$ and $C$ be a subgroup of $\mathcal{O}_K^\times$. Then*

$$[\Gamma : Log(C)] = \left[\mathcal{O}_K^\times : \mu(K)C\right].$$

*Proof.* The homomorphism

$$\begin{aligned}\Psi : \mathcal{O}_K^\times &\to {}^{\Gamma}/_{\mathrm{Log}(C)} \\ \alpha &\mapsto \mathrm{Log}(\alpha) + \mathrm{Log}(C)\end{aligned}$$

is surjective with kernel $\ker(\Psi) = \mu(K)C$ by Lemma 3.2.3. This implies that ${}^{\mathcal{O}_K^\times}/_{\mu(K)C}$ and ${}^{\Gamma}/_{\mathrm{Log}(C)}$ are isomorphic, which yields the claim. □

## 3.5 Condition on the Distribution

We follow the proof given in [CDPR16, 5], to generalize the given results for the distribution $D$ over an arbitrary algebraic number field $K$ with $n = [K : \mathbb{Q}]$, $\delta_1, ..., \delta_r, \sigma_1, \overline{\sigma_1}..., \sigma_s, \overline{\sigma_s}$ and $k = r + s - 1$ as before. We identify elements in $K$ with vectors in $\mathbb{R}^n$ by the following injective $\mathbb{Q}$-linear mapping:

$$\begin{aligned}F : K &\to \mathbb{R}^n \\ a &\mapsto (\delta_1(a), ..., \delta_r(a), \mathrm{Re}(\sigma_1(a)), \mathrm{Im}(\sigma_1(a)), \mathrm{Re}(\sigma_2(a)), \mathrm{Im}(\sigma_2(a)), ...\mathrm{Re}(\sigma_s(a)), \mathrm{Im}(\sigma_s(a))).\end{aligned}$$

**Definition 3.5.1.** *For $\alpha, \beta > 0$, a real-valued random variable $X$ is $(\alpha, \beta)$-**subexponential** if*

$$\mathbb{E}[cosh(\alpha X)] \leq \beta.$$

**Lemma 3.5.2** (Tail bound, [CDPR16, Lemma 5.2])**.** *Let $X_1, ..., X_n$ be independent centered (i.e. expectation zero) $(\alpha, \beta)$-subexponential real-valued random variables. Then, for any $\mathbf{a} = (a_1, ..., a_n)^T \in \mathbb{R}^n$ and every $t \geq 0$,*

$$Pr\left[\left|\sum_{i=1}^{n} a_i X_i\right| \geq t\right] \leq 2\exp\left(-\min\left(\frac{\alpha^2 t^2}{8\beta||\mathbf{a}||_2^2}, \frac{\alpha t}{2||\mathbf{a}||_\infty}\right)\right).$$

**Lemma 3.5.3.** *If $X$ is a non-negative random variable such that both $\mathbb{E}[X^\alpha]$ and $\mathbb{E}[X^{-\alpha}]$ are finite for $\alpha > 0$, then $\log X$ is an $(\alpha, \beta)$-subexponential random variable for some $\beta > 0$.*

*Proof.* We have

$$\mathbb{E}[\cosh(\alpha \log X)] = \frac{1}{2}\mathbb{E}\left[e^{\alpha \log X} + e^{-\alpha \log X}\right] = \frac{1}{2}\mathbb{E}\left[X^\alpha + X^{-\alpha}\right] = \frac{1}{2}\mathbb{E}[X^\alpha] + \frac{1}{2}\mathbb{E}\left[X^{-\alpha}\right] < \infty,$$

i.e., there exists a $\beta > 0$ with $\mathbb{E}[\cosh(\alpha \log X)] \leq \beta$. □

Now we are prepared to show that Condition 3.4.5 holds for continuous Gaussian distributions of any radius $\sigma$ for sufficiently small dual basis of the lattice.

**Theorem 3.5.4.** *Let $X_1, ..., X_r, Y_1, Y_1', ..., Y_s, Y_s'$ be i.i.d. $N(0, \sigma^2)$ variables for some $\sigma > 0$, and let $Z_i := |X_i|$ for $i = 1, ..., r$ and $Z_{r+2j} := Z_{r+2j-1} := \left(Y_j^2 + (Y_j')^2\right)^{1/2}$ for $j = 1, ..., s$. Then there exist constants $C, c > 0$, such that for all vectors $\boldsymbol{a}^{(1)}, ..., \boldsymbol{a}^{(l)} \in \mathbb{R}^n$ of Euclidean norm 1 that are orthogonal to the all-one vector $\boldsymbol{1} \in \mathbb{R}^n$ and all $t \geq C$*

$$Pr\left[\exists j : \left|\sum_{i=1}^{n} \boldsymbol{a}_i^{(l)} \log(Z_i)\right| \geq t\right] \leq 2l \exp\left(-\frac{t - Rc}{4}\right)$$

*holds, where $R := \max\left\{\left|\sum_{i=1}^{r} \boldsymbol{a}_i^{(j)}\right| \middle| j = 1, ..., l\right\}$.*

*Proof.* First we prove that $Z_1, ..., Z_r$ are $(1/2, \beta)$-subexponential random variables by using Lemma 3.5.3 and the formula $\mathbb{E}[g(Z)] = \int_{\mathbb{R}} g(x) f(x) \mathrm{d}x$ for a continuous function $g : \mathbb{R} \to \mathbb{R}$ and the density function $f$ of $Z$:

1. $i = 1, ..., r$: It's easy to see that

$$\mathbb{E}\left[Z_i^{1/2}\right] = \mathbb{E}\left[\sqrt{|X_i|}\right] = \int_{\mathbb{R}} \sqrt{|x|} \frac{1}{\sigma\sqrt{2\pi}} e^{-x^2/2\sigma^2} \mathrm{d}x < \infty$$

   and

$$\mathbb{E}\left[Z_i^{-1/2}\right] = \mathbb{E}\left[\sqrt{|X_i|^{-1}}\right] = \int_{\mathbb{R}} \frac{1}{\sqrt{|x|}} \frac{1}{\sigma\sqrt{2\pi}} e^{-x^2/2\sigma^2} \mathrm{d}x < \infty$$

   are both finite, i.e., the random variables $\log Z_i$ are $(1/2, \beta)$-subexponential for some $\beta > 0$.

2. $i = r+1, ..., n$: The random variables $Z_i$ are known as Rayleigh distributions with density functions $f(x) := \frac{x}{\sigma^2} e^{-x^2/2\sigma^2}$ for $x \geq 0$ and $f(x) = 0$ for $x < 0$. Thus we have

$$\mathbb{E}\left[Z_i^{1/2}\right] = \int_{[0,\infty)} \frac{x^{3/2}}{\sigma^2} e^{-x^2/2\sigma^2} \mathrm{d}x < \infty$$

   and

$$\mathbb{E}\left[Z_i^{-1/2}\right] = \int_{[0,\infty)} \frac{\sqrt{x}}{\sigma^2} e^{-x^2/2\sigma^2} \mathrm{d}x < \infty,$$

   which again implies, that the random variables $\log Z_i$ are $(1/2, \beta)$-subexponential for some $\beta > 0$.

Analogously follows $\mathbb{E}[\log Z_i] < \infty$ for $i = 1, ..., n$, hence the random variables $Z_i' := \log Z_i - \mathbb{E}[\log Z_i]$ are $(1/2, \beta')$-subexponential for some $\beta' > 0$ and centered. We set

$$e_r(\sigma) = \mathbb{E}[\log Z_1] = ... = \mathbb{E}[\log Z_r]$$

if $r > 0$ and $e_r(\sigma) = 0$ else, and

$$e_s(\sigma) = \mathbb{E}[\log Z_{r+1}] = ... = \mathbb{E}[\log Z_n]$$

if $s > 0$ and $e_s(\sigma) = 0$ else. Note that both $e_r(\sigma)$ and $e_s(\sigma)$ depend on $\sigma$, but for simplification we write $e_r$ and $e_s$ from now on. We set $c := e_s - e_r$ and $R_j := \sum_{i=1}^{r} \mathbf{a}_i^{(j)}$ to simplify the following equation.

$$\begin{aligned}\sum_{i=1}^{n} \mathbf{a}_i^{(j)} Z_i' &= \sum_{i=1}^{n} \mathbf{a}_i^{(j)} (\log Z_i - \mathbb{E}[\log Z_i]) = \sum_{i=1}^{n} \mathbf{a}_i^{(j)} (\log Z_i - \mathbb{E}[\log Z_i]) \\ &= \sum_{i=1}^{n} \mathbf{a}_i^{(j)} \log Z_i - \underbrace{\sum_{i=1}^{n} \mathbf{a}_i^{(j)}}_{=0} e_s + \underbrace{\sum_{i=1}^{r} \mathbf{a}_i^{(j)}}_{=R_j} \underbrace{(e_s - e_r)}_{=c} \\ &= \sum_{i=1}^{n} \mathbf{a}_i^{(j)} \log Z_i - R_j c.\end{aligned}$$

We are now prepared to apply Lemma 3.5.2 to the random variables $Z_i'$:

$$\begin{aligned}\Pr\left[\left|\sum_{i=1}^{n} \mathbf{a}_i^{(j)} \log Z_i\right| \geq t + R|c|\right] &\leq \Pr\left[\left|\sum_{i=1}^{n} \mathbf{a}_i^{(j)} \log Z_i\right| \geq t + |R_j c|\right] \leq \Pr\left[\left|\sum_{i=1}^{n} \mathbf{a}_i^{(j)} \log Z_i + R_j c\right| \geq t\right] \\ &= \Pr\left[\left|\sum_{i=1}^{n} \mathbf{a}_i^{(j)} Z_i'\right| \geq t\right] \underset{3.5.2}{\leq} 2\exp\left(-\min\left(\frac{t^2}{32\beta' ||\mathbf{a}^{(j)}||_2^2}, \frac{t}{4||\mathbf{a}^{(j)}||_\infty}\right)\right) \\ &\leq 2\exp\left(-\frac{t}{4}\right),\end{aligned}$$

for some $C > 0$ and all $t \geq C$, where we used the bound $||\mathbf{a}^{(j)}||_\infty \leq ||\mathbf{a}^{(j)}||_2 = 1$. By substituting we obtain

$$\Pr\left[\left|\sum_{i=1}^{n} \mathbf{a}_i^{(j)} \log Z_i\right| \geq t\right] \leq 2\exp\left(-\frac{t - Rc}{4}\right)$$

for some $C' > 0$ and all $t \geq C'$, which implies the stated inequality by union bound. □

Note that we only used the Gaussian distribution to show that the $Z_i's$ are subexponential random variables, so one could easily extend this result to other distributions, such that the $Z_i's$ are $(\alpha, \beta)$-subexponential for some $\alpha, \beta > 0$. The following corollary will be used in the case that $g \in K$ is chosen under the condition that all of its embeddings are real.

**Corollary 3.5.5.** *Let $X_1, ..., X_r, Y_1, ..., Y_s$ be i.i.d. $N(0, \sigma^2)$ variables for some $\sigma > 0$ and $Y_1', ..., Y_s' = 0$, as well as $Z_i := |X_i|$ for $i = 1, ..., r$ and $Z_{r+2j} := Z_{r+2j-1} := \left(Y_j^2 + (Y_j')^2\right)^{1/2} = |Y_j|$ for $j = 1, ..., s$. Then there exists a constant $C > 0$, such that for all vectors $\mathbf{a}^{(1)}, ..., \mathbf{a}^{(l)} \in \mathbb{R}^n$ of Euclidean norm 1 that are orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^n$ and all $t \geq C$ holds:*

$$Pr\left[\exists j : \left|\sum_{i=1}^{n} \mathbf{a}_i^{(l)} \log(Z_i)\right| \geq t\right] \leq 2l\exp\left(-\frac{t}{4}\right).$$

*Proof.* This follows analogously to the proof of Theorem 3.5.4 together with the fact that $e_r = e_s$ in the case $r, s > 0$. □

**Remark 3.5.6.** *Let $K$ be an algebraic number field and all notations as in Definition 3.2.1, furthermore set $M := \max\{||Log(b_1)^*||_2, ..., ||Log(b_k)^*||_2\}$ and let $\omega \in (0,1)$. If the generator $g$ is drawn from a continuous Gaussian and $\frac{1}{M} \geq C$, where $C$ is the corresponding constant from Theorem 3.5.4, and $2k \exp\left(-\frac{1/M - Rc}{4}\right) < 1 - \omega$, then Condition 3.4.5 holds with parameter $\omega > 0$.*

The number $R$ in Theorem 3.5.4 depends on the vectors $\mathbf{a}^{(1)}, ..., \mathbf{a}^{(k)} \in \mathbb{R}^n$. In our case these vectors are ${}^{\mathrm{Log}(b_1)^*}/_{||\mathrm{Log}(b_1)^*||_2}, ..., {}^{\mathrm{Log}(b_k)^*}/_{||\mathrm{Log}(b_k)^*||_2}$, i.e., $R$ depends on the chosen number field $K$ (and obviously on the chosen basis $b_1, ..., b_k \in \mathcal{O}_K^\times$). To satisfy the inequality given in Remark 3.5.6, we need the number $R$ to be sufficiently small.

**Remark 3.5.7.** *For $r = 0$ or $s = 0$ we have $R = 0$ by definition of $R$ and the vectors $\boldsymbol{a}^{(1)}, ..., \boldsymbol{a}^{(k)} \in \mathbb{R}^n$.*

As we will see for example in the case of cyclotomic number fields $K = \mathbb{Q}(\xi_{p^\alpha})$ with prime power conductor $m = p^\alpha$ (where $r = 0$ holds) we have $\frac{1}{M} \to \infty$ and $2k \exp\left(-\frac{1/2M}{4}\right) \to 0$ for $\alpha \to \infty$, which means that Condition 3.4.5 will hold with overwhelming probability for large enough $\alpha$, if $D$ is the continuous Gaussian.

# 4 Cyclotomic Units for $m = p^\alpha$

## 4.1 Overview

In this chapter we give a well suited basis of a subgroup of $\mathcal{O}_K^\times$ with small index, called *cyclotomic units*, if $m$ is a prime power. Since e.g. [Was96], [CDPR16] and other authors switch between the cyclomotic fields $\mathbb{Q}(\xi_m)$ and their maximal real subfields $\mathbb{Q}\left(\xi_m + \xi_m^{-1}\right)$, we introduce the general setting of CM-fields and show that recovering short generators in a CM-field $K$ is as hard as recovering short generators in its maximal real subfields $K^+$ with the used techniques. In the last section of this chapter we compute an example of the algorithm from the previous chapter for cyclotomic fields.

## 4.2 Maximal Real Subfields

**Definition 4.2.1** (CM-fields)**.** *Let $K$ be an algebraic number field and $n = r + 2s$ as always.*

1. *$K$ is called **totally real** if $s = 0$, i.e., $r = n$.*
2. *$K$ is called **totally imaginary** if $r = 0$, i.e., $2s = n$.*
3. *$K$ is called a **CM-field** (also known as **J-field**), if $K$ is totally imaginary and there is a subfield $K^+$ of $K$ with $[K : K^+] = 2$ and $K^+$ is totally real. Such a subfield $K^+$ is called the **maximal real subfield** of $K$. We set $\mathcal{O}_K^+ := \mathcal{O}_{K^+}$.*

The name *CM* in CM-fields is an abbreviation for *complex multiplication*, a theory of elliptic curves and abelian varieties.

**Lemma 4.2.2.** *Let $K$ be a CM-field and $K^+$ a maximal real subfield of $K$. Then $K^+$ is given by*

$$K^+ = K \cap \mathbb{R}.$$

*In particular, the maximal real subfield $K^+$ is unique. Moreover, $\mathcal{O}_K^+ = \mathcal{O}_K \cap \mathbb{R}$ holds.*

*Proof.* We have $K^+ \subseteq K$ by definition and $K^+ \subseteq \mathbb{R}$ because $\mathrm{id}|_{K^+} : K^+ \to \mathbb{C}$ is an embedding of $K^+$ into $\mathbb{C}$ and therefore real (here comes into play that we assumed $K \subseteq \mathbb{C}$ for algebraic number fields). This implies $K^+ \subseteq K \cap \mathbb{R}$. Since the index of $K^+$ in $K$ is equal 2, there are only two cases: $K^+ = K \cap \mathbb{R}$ or $K \cap \mathbb{R} = K$, which is equivalent to $K \subseteq \mathbb{R}$. The last case leads to a contradiction because this would mean that $\mathrm{id}|_K : K \to \mathbb{C}$ is a real embedding of $K$ into $\mathbb{C}$. Therefore $K^+ = K \cap \mathbb{R}$ holds, which implies $\mathcal{O}_K^+ \subseteq \mathcal{O}_K \cap \mathbb{R}$. Conversely, if $\rho \in \mathcal{O}_K \cap \mathbb{R}$, i.e., $\rho$ is integral and real, then $\rho \in K^+$ and therefore $\rho \in \mathcal{O}_K^+$. □

Notice that if $K$ is a CM-field and $K^+$ the maximal real subfield, the number $k = {}^{[K:\mathbb{Q}]}/_2 - 1 = [K^+ : \mathbb{Q}] - 1$ from Dirichlet's unit Theorem 3.2.2 is independent whether we consider $K$ or $K^+$ as underlying number field.
The embeddings of $K^+$ into $\mathbb{R}$ are given by $\sigma_1|_{K^+}, ..., \sigma_s|_{K^+} : K^+ \to \mathbb{R}$, where $\sigma_1, \overline{\sigma_1}, ..., \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$ are the embeddings of $K$ into $\mathbb{C}$.

**Example 4.2.3.** *For $m \geq 3$ the cyclotomic field $K_m = \mathbb{Q}(\xi_m)$ is a CM-field with maximal real subfield $K_m^+ = \mathbb{Q}(\xi_m + \xi_m^{-1})$.*

*Proof.* As mentioned before, $K_m$ has no real embeddings and is therefore totally imaginary. The embeddings of $\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)$ into $\mathbb{C}$ are of the form $\sigma|_{\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)}:\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)\to\mathbb{C}$, where $\sigma:K_m\to\mathbb{C}$ is an embedding of $K_m$ into $\mathbb{C}$. We obtain

$$\sigma\left(\xi_m+\xi_m^{-1}\right)=\sigma\left(\xi_m\right)+\overline{\sigma}\left(\xi_m\right)\in\mathbb{R},$$

which implies that $\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)$ is a totally real subfield of $K_m$ and therefore $\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)\subsetneq K_m$. Since $\xi_m$ is a root of the polynomial $X^2-\left(\xi_m+\xi_m^{-1}\right)X+1\in\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)[X]$, we conclude $\left[K_m:\mathbb{Q}(\xi_m+\xi_m^{-1})\right]=2$. Therefore $\mathbb{Q}\left(\xi_m+\xi_m^{-1}\right)$ is the maximal real subfield of $K_m$. □

**Remark 4.2.4.** *$K_m^+$ itself is an algebraic number field with ring of integers $\mathcal{O}_m^+:=\mathcal{O}_{K_m^+}=\mathbb{Z}\left[\xi_m+\xi_m^{-1}\right]$, see e.g. [Was96, Prop. 2.16].*

**Proposition 4.2.5.** *Let $K$ be a CM-field. Then the complex conjugation is an automorphism of $K$, i.e., $\overline{\alpha}\in K$ for all $\alpha\in K$. Moreover, we have $\overline{\alpha}\in\mathcal{O}_K$ for all $\alpha\in\mathcal{O}_K$ and $\overline{\beta}\in\mathcal{O}_K^\times$ for all $\beta\in\mathcal{O}_K^\times$.*

*Proof.* By definition we have $K=K^+\left(\sqrt{d}\right)$ for some $d\in K^+\subseteq\mathbb{R}$ with $d<0$, because $d\geq 0$ would imply that $id|_K:K\to\mathbb{R}$ is a real embedding of $K$. Therefore we conclude

$$\{\overline{x}\in\mathbb{C}|\ x\in K\}=K^+\left(\overline{i\sqrt{|d|}}\right)=K^+\left(-i\sqrt{|d|}\right)=K,$$

whereat we used again $K^+\subseteq\mathbb{R}$.
For all $\alpha\in\mathcal{O}_K$ there is a monic polynomial $f\in\mathbb{Z}[X]\backslash\{0\}$ with $f(\alpha)=0$, thus we have $0=\overline{0}=\overline{f(\alpha)}=f(\overline{\alpha})$ and therefore $\overline{\alpha}\in\mathcal{O}_K$. If $\beta\gamma=1$ for some $\beta,\gamma\in\mathcal{O}_K$, then $\overline{\beta}\overline{\gamma}=1$ and $\overline{\beta},\overline{\gamma}\in\mathcal{O}_K$, which yields $\overline{\beta}\in\mathcal{O}_K^\times$. □

The following theorem can be found in [Was96, Theorem 4.12].

**Theorem 4.2.6.** *Let $K$ be a CM-field. Then*

$$\left[\mathcal{O}_K^\times:\mu(K)\left(\mathcal{O}_K^+\right)^\times\right]\in\{1,2\}.$$

*Proof.* Define the homomorphism

$$\begin{aligned}\Phi:\mathcal{O}_K^\times&\to\mu(K)\\ \alpha&\mapsto{}^{\alpha}/_{\overline{\alpha}},\end{aligned}$$

whereby we have to prove that this mapping is well defined. Proposition 4.2.5 states that $\overline{\alpha}\in\mathcal{O}_K^\times$ and therefore ${}^{\alpha}/_{\overline{\alpha}}\in\mathcal{O}_K^\times$. We have

$$\mathrm{Log}\left(\Phi(\alpha)\right)=\mathrm{Log}(\alpha)-\mathrm{Log}(\overline{\alpha})=0$$

because of $\sigma(\overline{\alpha})=\overline{\sigma(\alpha)}$ for all embeddings $\sigma:K\to\mathbb{C}$. Thus $\Phi(\alpha)\in\ker\left(\mathrm{Log}|_{\mathcal{O}_K^\times}\right)=\mu(K)$ by Lemma 3.2.3 for all $\alpha\in\mathcal{O}_K^\times$ and the homomorphism $\Phi$ is well defined. Set $\mu:=\mu(K)$, then $\Phi$ induces a canonical homomorphism

$$\Psi:\mathcal{O}_K^\times\to{}^{\mu}/_{\mu^2}.$$

We prove $\mu\cdot(\mathcal{O}_K^+)^\times=\ker(\Psi)$. Let $\alpha=\xi\rho$ with $\xi\in\mu$ and $\rho\in(\mathcal{O}_K^+)^\times$, then $\Phi(\alpha)=\xi^2\in\mu^2$ and hence $\alpha\in\ker(\Psi)$. Conversely, if $\alpha\in\ker(\Psi)$, then there exists some $\xi\in\mu$ with ${}^{\alpha}/_{\overline{\alpha}}=\Phi(\alpha)=\xi^2$. This implies $\alpha\xi^{-1}=\overline{\alpha}\xi=\overline{\alpha\xi^{-1}}$ and therefore $\alpha\xi^{-1}\in\mathbb{R}\cap\mathcal{O}_K^\times=(\mathbb{R}\cap\mathcal{O}_K)^\times=(\mathcal{O}_K^+)^\times$. Thus we have $\alpha\in\mu\cdot(\mathcal{O}_K^+)^\times$, which yields $\mu\cdot(\mathcal{O}_K^+)^\times=\ker(\Psi)$. Therefore, ${}^{\mathcal{O}_K^\times}/_{\mu(K)(\mathcal{O}_K^+)^\times}$ is isomorphic to $\mathrm{Im}(\Psi)\subseteq{}^{\mu}/_{\mu^2}$.

Now we obtain $\left[\mathcal{O}_K^\times : \mu(K)\left(\mathcal{O}_K^+\right)^\times\right] \in \{1,2\}$ from $\left|\mu/\mu^2\right| = 2$, which may be verified by considering the group homomorphism

$$\begin{aligned}\mu &\to \mu^2\\ \xi &\mapsto \xi^2\end{aligned}$$

and the fact that $\xi^2 = \eta^2$ is equivalent to $\xi = \pm\eta$ for all $\xi, \eta \in \mu$ and $|\mu| < \infty$. □

**Corollary 4.2.7.** *Let $K$ be a CM-field, $C_+$ a subgroup of $(\mathcal{O}_K^+)^\times$ and $h^+ := \left[(\mathcal{O}_K^+)^\times : \{\pm 1\} \cdot C_+\right]$ (note that $\mu(K^+) = \{\pm 1\}$). Then $C_+$ is a subgroup of $\mathcal{O}_K^\times$ with*

$$\left[\mathcal{O}_K^\times : \mu(K)C_+\right] = \left[\mathcal{O}_K^\times : \mu(K)\left(\mathcal{O}_K^+\right)^\times\right]h^+ = h^+ \text{ or } 2h^+.$$

*Proof.* We define the group homomorphism

$$\begin{aligned}\Psi : (\mathcal{O}_K^+)^\times &\to {}^{\mu(K)(\mathcal{O}_K^+)^\times}/_{\mu(K)C_+}\\ \rho &\mapsto \rho \cdot \mu(K)C_+,\end{aligned}$$

which obviously is surjective. The kernel is given by

$$\begin{aligned}\ker(\Psi) &= (\mathcal{O}_K^+)^\times \cap (\mu(K)C_+)\\ &= \mathbb{R} \cap \mathcal{O}_K^\times \cap (\mu(K)C_+)\\ &= \mathbb{R} \cap \big(\mu(K)\underbrace{C_+}_{\subseteq \mathbb{R}}\big)\\ &= \{\pm 1\}C_+,\end{aligned}$$

which yields that ${}^{(\mathcal{O}_K^+)^\times}/_{\{\pm 1\}C_+}$ and ${}^{\mu(K)(\mathcal{O}_K^+)^\times}/_{\mu(K)C_+}$ are isomorphic. Therefore

$$\left[(\mathcal{O}_K^+)^\times : \{\pm 1\}C_+\right] = \left[\mu(K)(\mathcal{O}_K^+)^\times : \mu(K)C_+\right]$$

holds, which implies

$$\begin{aligned}\left[\mathcal{O}_K^\times : \mu(K)C_+\right] &= \left[\mathcal{O}_K^\times : \mu(K)\left(\mathcal{O}_K^+\right)^\times\right]\left[\mu(K)\left(\mathcal{O}_K^+\right)^\times : \mu(K)C_+\right]\\ &= \underbrace{\left[\mathcal{O}_K^\times : \mu(K)\left(\mathcal{O}_K^+\right)^\times\right]}_{=1 \text{ or } 2}\underbrace{\left[\left(\mathcal{O}_K^+\right)^\times : \{\pm 1\}C_+\right]}_{=h^+}\\ &= h^+ \text{ or } 2h^+.\end{aligned}$$

□

**Example 4.2.8.** *In the case of cyclotomic fields $K_m = \mathbb{Q}(\xi_m)$ we obtain*

$$\left[\mathcal{O}_m^\times : \mu(K_m)\left(\mathcal{O}_m^+\right)^\times\right] = 1 \text{ iff } m \text{ is a prime power},$$

*see [Was96, Corollary 4.13] (here we used $m \not\equiv 2 \mod 4$).*

**Lemma 4.2.9.** *Let $K$ be a CM-field, $n = [K : \mathbb{Q}]$ and $Log : K^\times \to \mathbb{R}^n$ and $Log_r|_{(K^+)^\times} = Log^+ : (K^+)^\times \to \mathbb{R}^{n/2}$ be the logarithmic embeddings of $K^\times$ and $(K^+)^\times$, respectively. Then for all $\alpha \in (K^+)^\times$*

$$||Log(\alpha)||_2 = \sqrt{2}||Log^+(\alpha)||_2$$

*and*

$$||Log(\alpha)^*||_2 = \frac{1}{\sqrt{2}}||Log^+(\alpha)^*||_2.$$

*Proof.* By definition

$$\begin{aligned}||\mathrm{Log}(\alpha)||_2 &= \left|\left|\left(\log(|\sigma_1(\alpha)|), \log(|\overline{\sigma_1}|\alpha)|), ..., \log(|\sigma_s(\alpha)|), \log(|\overline{\sigma_s}(\alpha)|)\right)^T\right|\right|_2 \\ &= \sqrt{2} \cdot \left|\left|\left(\log(|\sigma_1(\alpha)|), , ..., \log(|\sigma_s(\alpha)|)\right)^T\right|\right|_2 \\ &= \sqrt{2} \cdot ||\mathrm{Log}^+(\alpha)||_2,\end{aligned}$$

where we used the fact that the embeddings of $K^+$ into $\mathbb{C}$ are given by $\sigma_1|_{K^+}, ..., \sigma_s|_{K^+}$. From this $||\mathrm{Log}(\alpha)^*||_2 = \frac{1}{\sqrt{2}}||\mathrm{Log}^+(\alpha)^*||_2$ follows analogously from the definition of the dual basis. □

**Algorithmic Implications 4.2.10.** Let $K$ be a CM-field.

**" Attack for $K^+ \Rightarrow$ Attack for $K$".**

1. If one has a basis $b_1, ..., b_k \in (\mathcal{O}_K^+)^\times$ of a subgroup $C_+ \subseteq (\mathcal{O}_K^+)^\times$ which is well suited to apply Algorithm 3.3 to recover a shortest generator $g \in (K^+)^\times$ which is chosen from continuous Gaussian with parameter $\sigma$ (or an other well suited distribution), i.e., the basis has sufficiently short dual vectors $\mathrm{Log}^+(b_1)^*, ..., \mathrm{Log}^+(b_k)^*$ and is of small index $h^+ = \left[(\mathcal{O}_K^+)^\times : \{\pm 1\}C_+\right]$, then $b_1, ..., b_k$ is a well suited basis of the subgroup $C_+ \subseteq \mathcal{O}_K^\times$ to recover short generators $g \in K^\times$, which are chosen from a continuous Gaussian with the same parameter $\sigma$. The norm of the vectors $\mathrm{Log}(b_1)^*, ..., \mathrm{Log}(b_k)^*$ is smaller than the norm of their related dual vectors $\mathrm{Log}^+(b_1)^*, ..., \mathrm{Log}^+(b_k)^*$ by Lemma 4.2.9 and the index of $C_+$ in $\mathcal{O}_K^\times$ is at most $2h^+$, see Corollary 4.2.7.

**" Attack for $K \Rightarrow$ Attack for $K^+$".**

2. Conversely, if one has a basis $b_1, ..., b_k \in \mathcal{O}_K^\times$ of a subgroup $C \subseteq \mathcal{O}_K^\times$ which is well suited to apply Algorithm 3.3, one can use this algorithm with this basis to recover $g \in K^+$ which is chosen by some distribution $D^+$ over $K^+$, see Corollary 3.5.5.

   In the case $\left[\mathcal{O}_K^\times : \mu(K)\left(\mathcal{O}_K^+\right)^\times\right] = 1$ one can alternatively calculate a basis $b_1^+, ..., b_k^+ \in (\mathcal{O}_K^+)^\times$ of a subgroup $C_+ := \langle b_1^+, ..., b_k^+\rangle \subseteq (\mathcal{O}_K^+)^\times$ from $b_1, ..., b_k$ as follows: For all $i = 1, ..., k$ there are $\xi_i \in \mu(K)$ and $b_i^+ \in (\mathcal{O}_K^+)^\times$ such that $b_i = \xi_i b_i^+$. With Theorem 4.2.6 we obtain

$$\left[\mathcal{O}_K^\times : \mu(K)C\right] = \left[\mathcal{O}_K^\times : \mu(K)C_+\right] = \left[\left(\mathcal{O}_K^+\right)^\times : \{\pm 1\}C_+\right]$$

   and $||\mathrm{Log}^+(b_i^+)^*||_2 = \sqrt{2}||\mathrm{Log}(b_i^+)^*||_2 = \sqrt{2}||\mathrm{Log}(b_i)^*||_2$ from Lemma 4.2.9. Hence the index of $C_+$ in $(\mathcal{O}_K^+)^\times$ is equal to the index of $C$ in $\mathcal{O}_K^+$ and the norms of the dual vectors differ only by a factor of $\sqrt{2}$. Notice that the $b_i^+$ can be calculated numerically by $b_i^+ = \pm\sqrt{b_i\overline{b_i}}$.

As we have seen, if one have a well suited basis of $\mathcal{O}_K^\times$ for a CM-field $K$ to recover shortest generators in $K$, then one can also recover shortest generators in its maximal real subfield $K^+$ and vice versa.

## 4.3 Cyclotomic Units for Prime Powers

In general it is hard to find a (well suited) fundamental system of units of $\mathcal{O}_m^\times$ for arbitrary $m \in \mathbb{N}$. Our next step is to define the group of cyclotomic units, as introduced in [Was96, Chapter 8]. They have (small) finite index in $\mathcal{O}_m^\times$ and have a basis which has small enough dual vectors of the logarithmic embeddings for prime powers $m = p^\alpha$.

**Definition 4.3.1** (Cyclotomic units)**.** *Let $m \in \mathbb{N}$. We define the multiplicative group*

$$V_m := \langle \pm\xi_m, 1-\xi_m^l \mid 1 \le l \le m-1 \rangle \subseteq K_m^\times.$$

*Note that in general not all elements of $V_m$ are units of $\mathcal{O}_m$. The* ***group of cyclotomic units*** *$\mathcal{C}_m$ is defined by*

$$\mathcal{C}_m := V_m \cap \mathcal{O}_m^\times.$$

**Lemma 4.3.2.** *For $m, u, v \in \mathbb{N}$ with $m \ge 2$ and $\gcd(m, uv) = 1$ the element*

$$\frac{\xi_m^u - 1}{\xi_m^v - 1}$$

*is a unit of $\mathcal{O}_m = \mathbb{Z}[\xi_m]$.*

*Proof.* We conclude $\gcd(m, v) = 1$ from $\gcd(m, uv) = 1$. Set $t :\equiv v^{-1}u \mod m$, from which we obtain

$$\frac{\xi_m^u - 1}{\xi_m^v - 1} = \frac{\xi_m^{vt} - 1}{\xi_m^v - 1} = (\xi_m^v)^{t-1} + \ldots + \xi_m^v + 1 \in \mathbb{Z}[\xi_m].$$

Analogously $\frac{\xi_m^v - 1}{\xi_m^u - 1} \in \mathbb{Z}[\xi_m]$ follows, which proves the claim. □

**Lemma 4.3.3** (Generators of $\mathcal{C}_{p^\alpha}$)**.** *Let $p \in \mathbb{P}$ and $l \in \mathbb{N}$, we define*

$$b_j := \frac{\xi_{p^\alpha}^j - 1}{\xi_{p^\alpha} - 1}$$

*for $j \in \mathbb{Z}_{p^\alpha}^\times \backslash \{\pm 1\}$. The group $\mathcal{C}_{p^\alpha}$ is generated by $\pm\xi_{p^\alpha}$ and $b_j$ for $j \in \mathbb{Z}_{p^\alpha}^\times \backslash \{\pm 1\}$. Note that the equation*

$$b_j = \frac{\xi_{p^\alpha}^j - 1}{\xi_{p^\alpha} - 1} = -\xi_{p^\alpha}^j \frac{\xi_{p^\alpha}^{-j} - 1}{\xi_{p^\alpha} - 1} = -\xi_{p^\alpha}^j b_{-j}$$

*implies, that it is sufficient to reduce to a set of representatives of $\left(\mathbb{Z}_{p^\alpha}^\times / \{\pm 1\}\right) \backslash \{\pm 1\}$ for $j$, i.e.,*

$$\mathcal{C}_{p^\alpha} = \left\langle \pm\xi_{p^\alpha}, b_j \,\middle|\, 1 < j \le \frac{p^\alpha}{2}, \gcd(j, p^\alpha) = 1 \right\rangle.$$

For a proof see for example [Was96, Lemma 8.1]. Since we are interested in finding subgroups of $\mathcal{O}_m^\times$ of small index, we have to determine the index of the cyclotomic units in $\mathcal{O}_m$ first.

**Theorem 4.3.4.** *Let $p$ be a prime and $\alpha \ge 1$ with $(p, \alpha) \ne (2, 1)$. Further, let $h_{p^\alpha}^+$ be the class number of $K_{p^\alpha}^+ = \mathbb{Q}(\xi_{p^\alpha} + \xi_{p^\alpha}^{-1})$. Then*

$$h_{p^\alpha}^+ = \left[ \mathcal{O}_{p^\alpha}^\times : \mathcal{C}_{p^\alpha} \right].$$

*Proof.* Corollary 4.2.7 and Example 4.2.8 yield

$$\left[ \mathcal{O}_{p^\alpha}^\times : \mathcal{C}_{p^\alpha} \right] = \left[ \mathcal{O}_{p^\alpha}^\times : \mu(K_{p^\alpha}) \mathcal{C}_{p^\alpha} \right] = \left[ \left( \mathcal{O}_{p^\alpha}^+ \right)^\times : \mathcal{C}_{p^\alpha}^+ \right],$$

where $\mathcal{C}_{p^\alpha}^+$ is the group generated by $-1$ and $b_j^+ := \xi_{2p^\alpha}^{(1-j)} b_j \in \left( \mathcal{O}_{p^\alpha}^+ \right)^\times$, which we obtain as mentioned in the second point of 4.2.10 and by the simple calculation

$$b_j^+ = \pm\sqrt{b_j \overline{b_j}} = \pm\sqrt{\frac{\xi_{p^\alpha}^j - 1}{\xi_{p^\alpha} - 1} \cdot \frac{\xi_{p^\alpha}^{-j} - 1}{\xi_{p^\alpha}^{-1} - 1}} = \pm\sqrt{\xi_{p^\alpha}^{1-j} \frac{\xi_{p^\alpha}^j - 1}{\xi_{p^\alpha} - 1} \cdot \frac{\xi_{p^\alpha}^j - 1}{\xi_{p^\alpha} - 1}} = \pm\xi_{2p^\alpha}^{(1-j)} b_j.$$

The statement

$$h_{p^\alpha}^+ = \left[ \left( \mathcal{O}_{p^\alpha}^+ \right)^\times : \mathcal{C}_{p^\alpha}^+ \right]$$

is Theorem 8.2 of [Was96]. □

We collect some facts and conjectures concerning $h_m^+$.

**Remark 4.3.5.**

1. *For $m = 2^\alpha$ with $1 \leq \alpha \leq 8$ it has been proven that $h_m^+ = 1$, and under the generalized Riemann hypothesis that $h_{512}^+ = 1$, see [Mil14b, VdL82]. The conjecture $h_{2^\alpha}^+ = 1$ for all $\alpha \in \mathbb{N}$ is known as* ***Weber's class number problem****.*
2. *Miller [Mil15] also have proven that $h_{163}^+ = 4$, $h_{191}^+ = 11$, $h_{229}^+ = 3$ and $h_p^+ = 1$ for all other primes $p \leq 241$. It is conjectured that except of only finitely many pairs $(p, \alpha) \in \mathbb{P} \times \mathbb{N}$ the equation $h_{p^{\alpha+1}}^+ = h_{p^\alpha}^+$ holds, see [BPR04]. Hence, for fixed prime $p$ the class number $h_{p^\alpha}^+$ is bound for all $\alpha \in \mathbb{N}$.*

Finally we need the dual vectors of the basis of the cyclotomic units to be sufficiently small, which is the following theorem.

**Theorem 4.3.6** ([CDPR16, Theorem 3.1])**.** *Let $p$ be a prime and $m = p^\alpha$ for some $\alpha \in \mathbb{N}$ with $(p, \alpha) \neq (2, 1)$. Then all $||Log(b_j)^*||_2$ are equal for $1 < j \leq {}^{p^\alpha}/_2$ with $\gcd(j, p^\alpha) = 1$ and*

$$||Log(b_j)^*||_2^2 \in O\left(\frac{\log^3 m}{m}\right).$$

*$O$ denotes the Landau symbol.*

Notice that the logarithmic embedding in [CDPR16] is defined as the reduced logarithmic embedding, which is no issue since the norm of these embeddings only differ by the factor $\sqrt{2}$.

**Corollary 4.3.7.** *Let $p$ be a prime, $m = p^\alpha$ for some $\alpha \in \mathbb{N}$ with $(p, \alpha) \neq (2, 1)$ and $M(\alpha) := ||Log(b_j)^*||_2$ for any $j$ with $1 < j \leq {}^{p^\alpha}/_2$, $k(\alpha) := \frac{\varphi(p^\alpha)}{2} - 1$ and $\gcd(j, p^\alpha) = 1$. Then*

$$\frac{1}{2M(\alpha)} \to \infty \quad \text{for } \alpha \to \infty$$

*and*

$$2k(\alpha)\exp\left(-\frac{1}{8M(\alpha)}\right) \leq C \cdot m \exp\left(-\frac{\sqrt{m}}{8\log^{3/2}(m)}\right) \to 0 \quad \text{for } m \to \infty$$

*holds for some constant $C > 0$.*
*In particular, for all $\omega \in (0, 1)$ Condition 3.4.5*

$$\left|\langle Log(g), \mathbf{v}_i\rangle\right| < \frac{1}{2M(\alpha)} \quad \text{for all } i = 1, ..., k$$

*holds with parameter $\omega$, if the generator $g \in K_m$ is chosen by continuous Gaussian for all $\mathbf{v}_1, ..., \mathbf{v}_k \in \mathbb{R}^n$ of euclidean norm 1 and orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^n$ and large enough $m$.*

*Proof.* It follows immediately from Theorem 4.3.6 that $\frac{1}{2M(\alpha)} \to \infty$ holds for $\alpha \to \infty$. The convergence of $m\exp\left(-\frac{\sqrt{m}}{8\log^{3/2}(m)}\right)$ with limit 0 for $m \to \infty$ can be proven by basic analysis. Hence, the condition holds with parameter $\omega$ for large enough $m$, since the probability of

$$\left|\langle \mathrm{Log}(g), \mathbf{v}_i\rangle\right| \geq \frac{1}{2M(\alpha)} \quad \text{for some } i = 1, ..., k$$

for all $\mathbf{v}_1, ..., \mathbf{v}_k \in \mathbb{R}^{\varphi(m)}$ which have euclidean norm 1 and are orthogonal to the all one verctor $1 \in \mathbb{R}^{\varphi(m)}$ is bounded by $m\exp\left(-\frac{\sqrt{m}}{8\log^{3/2}(m)}\right)$ for large enough $m$ by Theorem 3.5.4. □

In Figure 4.1 we have listed some rounded values of $p^\alpha \exp\left(-\frac{\sqrt{p^\alpha}}{8\log^{3/2}(p^\alpha)}\right)$ for concrete pairs $(p, \alpha)$.

| $\alpha$ | 12 | 14 | 16 | 18 | 20 | 24 | 28 |
|---|---|---|---|---|---|---|---|
| $2^\alpha$ | $2.9 \cdot 10^3$ | $9.7 \cdot 10^3$ | $2.8 \cdot 10^4$ | $6.1 \cdot 10^4$ | $8.8 \cdot 10^4$ | $8.9 \cdot 10^3$ | $10^{-2}$ |
| $3^\alpha$ | $7.9 \cdot 10^4$ | $5.1 \cdot 10^4$ | $6.3 \cdot 10^2$ | $2.7 \cdot 10^{-4}$ | $2.6 \cdot 10^{-22}$ | $2.7 \cdot 10^{-202}$ | $7.2 \cdot 10^{-1511}$ |
| $5^\alpha$ | $2.5 \cdot 10^{-2}$ | $1.4 \cdot 10^{-30}$ | $9.4 \cdot 10^{-152}$ | $4.1 \cdot 10^{-669}$ | $2.6 \cdot 10^{-2891}$ | $1.6 \cdot 10^{-55184}$ | $< 10^{-1095764}$ |

**Figure 4.1:** Values for $p^\alpha \exp\left(-\frac{\sqrt{p^\alpha}}{8\log^{3/2}(p^\alpha)}\right)$

Figure 4.2 shows the upper bound of $1-\omega$ depending on $l$, such that Condition 3.4.5 with parameter $\omega > 0$ does *not* hold in the case of cyclotomic number fields $K_{p^\alpha}$, where the generator $g \in K_{p^\alpha}$ is chosen from a continuous Gaussian.

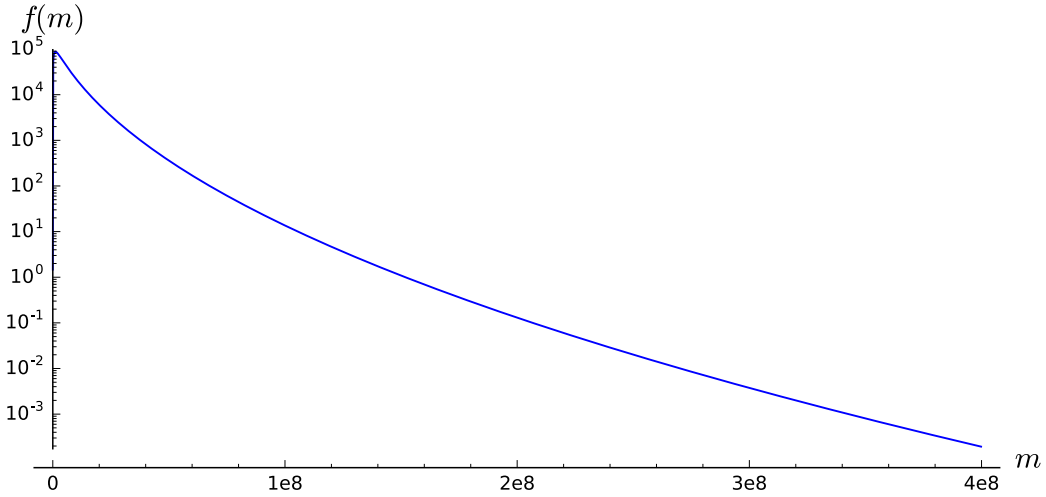



**Figure 4.2:** $m \mapsto m \exp\left(-\frac{\sqrt{m}}{8\log^{3/2}(m)}\right) =: f(m)$

## 4.4 Example of the Algorithm for Cyclotomic Fields of Prime Power

We collect all the presented results and illustrate with an example, how one can recover a short generator $g \in \mathbb{Q}(\xi_7)$ with the presented methods. We have $n = \varphi(7) = 6$ and $k = 6/2 - 1 = 2$, i.e., $\mathrm{Log}(\mathcal{O}_7^\times)$ is a 2-dimensional lattice in $\mathbb{R}^6$ whose vectors are all orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^6$. For simplicity, we identify the vectors $\mathrm{Log}(\alpha) \in \mathbb{R}^6$ for $\alpha \in \mathcal{O}_7^\times$ with the corresponding reduced vectors $\mathrm{Log}_r(\alpha) \in \mathbb{R}^3$.

**Lemma 4.4.1.** *For all $\alpha \in \mathcal{O}_m^\times$, the vector $\mathrm{Log}_r(\alpha)$ ist orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^{\varphi(m)/2}$.*

*Proof.* If we denote the all-one vectors by $\mathbf{1}_r \in \mathbb{R}^{\varphi(m)/2}$ and $\mathbf{1}_n \in \mathbb{R}^{\varphi(m)}$, this follows immediately from the corresponding fact for $\mathrm{Log}(\cdot)$ and

$$\mathbf{1}_r^T \cdot \mathrm{Log}_r(\alpha) = \frac{1}{2}\mathbf{1}_n^T \cdot \mathrm{Log}(\alpha) = 0.$$

□

The cyclotomic units $\mathcal{C}_7$ of $\mathbb{Q}(\xi_7)$ have index 1 in $\mathcal{O}_7^\times$ by Remark 4.3.5 and are generated by $\pm\xi_7$ and

$$b_2 = \frac{\xi_7^2 - 1}{\xi_7 - 1} = \xi_7 + 1$$
$$b_3 = \frac{\xi_7^3 - 1}{\xi_7 - 1} = \xi_7^2 + \xi_7 + 1.$$

We calculate the logarithmic embeddings of $b_2$ and $b_3$:

$$\mathbf{b}_2 := \mathrm{Log}_r(b_2) \approx \begin{pmatrix} 0.588862605761680 \\ -0.809586916044712 \\ 0.220724310283033 \end{pmatrix},$$
$$\mathbf{b}_3 := \mathrm{Log}_r(b_3) \approx \begin{pmatrix} 0.809586916044713 \\ -0.220724310283032 \\ -0.588862605761679 \end{pmatrix}.$$

The dual Basis $\mathbf{b}_2^*, \mathbf{b}_3^* \in \mathbb{R}^3$ can be computed with Theorem 2.3.6 by calculating $\mathbf{B}^* = \mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}$, where $\mathbf{B} := (\mathbf{b}_2, \mathbf{b}_3)$.

$$\mathbf{b}_2^* = \begin{pmatrix} 0.233536343541276 \\ -0.887136144108794 \\ 0.653599800567518 \end{pmatrix},$$
$$\mathbf{b}_3^* = \begin{pmatrix} 0.653599800567519 \\ 0.233536343541276 \\ -0.887136144108793 \end{pmatrix}.$$

Assume we have given

$$g' = \frac{4}{3}\xi_7^5 + 2\xi_7^4 + \frac{5}{3}\xi_7^3 + \frac{1}{6}\xi_7^2 - \xi_7 - \frac{7}{6} \in \mathbb{Q}(\xi_7)$$

as a generator of the ideal $g'\mathcal{O}_7$ and we want to recover some shortest generator of this fractional ideal. The first step of Algorithm 3.2 applies the round-off algorithm with basis $\mathbf{B}$ to the vector

$$\mathbf{t} := \mathrm{Log}_r(g') \approx \begin{pmatrix} 1.75900453738717 \\ -1.55144770999045 \\ -1.56860765302375 \end{pmatrix},$$

thus we get

$$\begin{pmatrix} a_2 \\ a_3 \end{pmatrix} = \lfloor (\mathbf{B}^*)^T \cdot t \rceil = \left\lfloor \begin{pmatrix} 0.761895177976256 \\ 2.17893413436999 \end{pmatrix} \right\rceil = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

The output of Algorithm 3.2 is the generator

$$\begin{aligned} g_e &= g' \cdot b_2^{-1} \cdot b_3^{-2} = g'(-\xi_7^5 - \xi_7^3 - \xi_7)(2\xi_7^5 + \xi_7^2 + \xi_7) \\ &= \frac{1}{2}\xi_7^3 + \frac{1}{2}\xi_7 + \frac{1}{3} \end{aligned}$$

with

$$\mathrm{Log}_r(g_e) \approx \begin{pmatrix} -0.449031900463937 \\ -0.300412173379674 \\ -0.611606751783427 \end{pmatrix}.$$

Figure 4.3 shows the two dimensional subspace of $\mathbb{R}^3$ which is orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^3$ and the projection of all these calculated vectors to this plane with basis $v := \left(1/\sqrt{2}, -1/\sqrt{2}, 0\right)^T$ and $w := \left(1/\sqrt{6}, 1/\sqrt{6}, -2/\sqrt{6}\right)^T$.

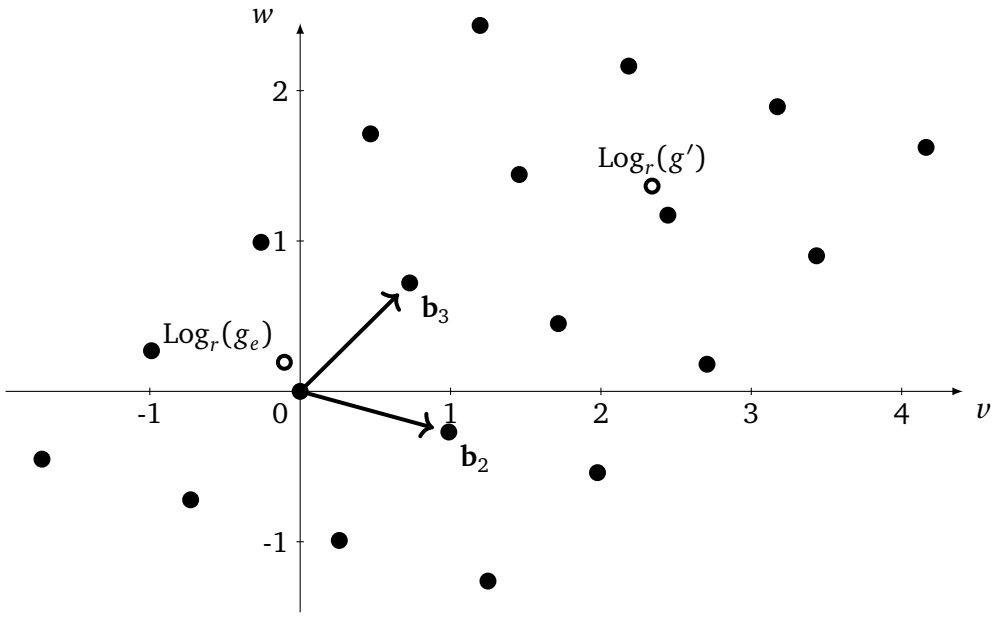



**Figure 4.3:** Projection onto the plane in $\mathbb{R}^3$ orthogonal to the vector $\mathbf{1} \in \mathbb{R}^3$.

Randomly producing non short generators will result in obtaining embedded elements with short projection on the orthogonal complement of the all-one vector $\mathbf{1}$. This outcome might appear contra intuitive, since the absolute value of the components of the logarithmic embedding increases if we choose smaller elements $g \in K^\times \subseteq \mathbb{C}^\times$. This relies on the fact, that we consider the projection to the subspace orthogonal to $\mathbf{1}$, hence the projection is small if the quotients of the components of the logarithmic embedding are nearly equal to one.

# 5 The Case $m = p^\alpha q^\beta$

## 5.1 Overview

In this chapter we investigate the group generated by the roots of unity and the units $\frac{\xi_m^j - 1}{\xi_m - 1}$ for $j \in \mathbb{Z}_m^\times$, if $m = p^\alpha q^\beta$ for some distinct, odd primes $p, q$. In particular, $m$ is not a prime power. We show, that under some conditions we can use these units to recover shortest generators in cyclotomic fields $K_m$ with similar techniques as for prime powers $m$ presented in [CDPR16].

## 5.2 Circulant Matrices and Characters

We follow along [CDPR16, Section 2.2] and present some facts about circulant matrices and characters of finite abelian groups.

**Definition 5.2.1** (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 5.2.2** (Characters)**.** *Let $G$ be a finite abelian group. A **character** of $G$ is a group homomorphism*

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

*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 $\chi$. The constant character $\chi \equiv 1$ is the identity element of $\widehat{G}$ and is called **trivial character**.*

**Lemma 5.2.3** ([Was96, Lemma 3.1])**.** *If $G$ is a finite abelian group, then $G$ is isomorphic to $\widehat{G}$. In particular, $|G| = |\widehat{G}|$.*

**Lemma 5.2.4.** *Let $G_1$ and $G_2$ be two finite abelian groups, then*

$$\begin{aligned} \Phi : \widehat{G_1} \times \widehat{G_2} &\to \widehat{G_1 \times G_2} \\ (\chi, \Psi) &\mapsto \chi \cdot \Psi \end{aligned}$$

*is a group isomorphism, where $(\chi \cdot \Psi)((g,h)) := \chi(g) \cdot \Psi(h)$.*

*Proof.* It is easy to see that $\Phi$ is indeed a group homomorphism, and since

$$|\widehat{G_1 \times G_2}| = |G_1 \times G_2| = |G_1| \cdot |G_2| = |\widehat{G_1}| \cdot |\widehat{G_2}| = |\widehat{G_1} \times \widehat{G_2}| < \infty$$

by Lemma 5.2.3, it is sufficient to show that $\Psi$ is injective. Therefore, let $(\chi, \Psi) \in \widehat{G_1} \times \widehat{G_2}$ with $\chi \cdot \Psi \equiv 1$, i.e., $(\chi \cdot \Psi)((g,h)) = 1$ for all $(g,h) \in G_1 \times G_2$. In particular, if we denote the identity elements by $e_1 \in G_1$ and $e_2 \in G_2$, respectively, we have $1 = (\chi \cdot \Psi)((g, e_2)) = \chi(g)$ for all $g \in G_1$ and $1 = (\chi \cdot \Psi)((e_1, h)) = \Psi(h)$ for all $h \in G_2$, hence $\chi \equiv 1$ and $\Psi \equiv 1$. Therefore, $\Phi$ is injective as requiered. □

**Theorem 5.2.5.** *Let $G$ be a cyclic group of order $n$ with generator $g \in G$. Then all characters of $G$ are given by*

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

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

*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 a $n$-th root of unity. It is easy to see that the functions $\chi_h$ are well defined and $n$ different characters. Since there are only $|\widehat{G}| = |G| = n$ different characters, that are all characters of $G$. □

**Corollary 5.2.6.** *Let $G$ be a finite abelian group and $g \in G$ be not the identity element. Then there exists a character $\chi \in \widehat{G}$ with $\chi(g) \neq 1$.*

*Proof.* By the structure theorem for finite abelian groups we have $G \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$ for some $n_1, ..., n_k \in \mathbb{N}\backslash\{1\}$. Hence, w.l.o.g. we assume $G = \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$. Since $g = (g_1, ..., g_k)$ is not the identity element of $G$, there is a component of $g$ with $g_i \neq 0$ for some $i \in \{1, ..., k\}$, w.l.o.g. $i = 1$. The group $\mathbb{Z}_{n_1}$ is cyclic with generator $1 \in \mathbb{Z}_{n_1}$, and of order $n_1$. Theorem 5.2.5 yields that there is a character $\chi_1$ of $\mathbb{Z}_{n_1}$ with $\chi_1(g_1) = \xi_{n_1}^{g_1} \neq 1$. This character induces a character $\chi$ of $\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$ with $\chi(g) = \chi_1(g_1) \neq 1$ via concatenation with the natural projection $\pi : \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k} \to \mathbb{Z}_{n_1}$. □

**Definition 5.2.7** (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 $\chi$ 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 $\chi$, 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 $\chi$ 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 $\chi$ 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 $\chi$ is **odd**. A non trivial character $\chi$ 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 $f_\chi$ to a multiplicative function $\chi' : \mathbb{Z} \to \mathbb{S}^1 \cup \{0\}$ by*

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

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

We identify characters $\chi$ 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.

**Lemma 5.2.8.** *Let $G$ be a finite abelian group. Then the following holds.*

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

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

*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*

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

*Proof.*

1.) If $\chi \equiv 1$, then $\sum_{g\in G} \chi(g) = \sum_{g\in G} 1 = |G|$. Else, there is some $h \in G$ with $\chi(h) \neq 1$. The multiplication with $h$ is a bijection from $G$ to $G$, hence

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(h\cdot g) = \sum_{g\in G} \chi(h)\cdot\chi(g) = \chi(h)\sum_{g\in G}\chi(g),$$

which yields $\sum_{g\in G}\chi(g) = 0$ because of $\chi(h) \neq 1$.

2.) This follows immediately by

$$||\chi||_2 = \sqrt{\langle \chi, \chi\rangle} = \sum_{g\in G} \chi(g)\cdot\overline{\chi}(g) = \sum_{g\in G} 1 = |G|.$$

3.) If $\chi$ and $\Psi$ are different characters of $G$, then $\chi\cdot\overline{\Psi} = \chi\cdot\Psi^{-1} \not\equiv 1$ is a non trivial character, therefore $\langle \chi, \Psi\rangle = \sum_{g\in G}(\chi\cdot\Psi^{-1})(g) = 0$ follows from *1.)*.

4.) If $g$ is the identity element, then $\sum_{\chi\in\widehat{G}}\chi(g) = \sum_{\chi\in\widehat{G}} 1 = |\widehat{G}| = |G|$ by Lemma 5.2.3. Else, there exists a $\Psi \in \widehat{G}$ with $\Psi(g) \neq 1$ by Corollary 5.2.6. Since multiplication with $\Psi$ is a permutation of $\widehat{G}$, we have

$$\underbrace{(1-\Psi(g))}_{\neq 0}\sum_{\chi\in\widehat{G}}\chi(g) = \sum_{\chi\in\widehat{G}}\chi(g) - \sum_{\chi\in\widehat{G}}\Psi(g)\chi(g) = \sum_{\chi\in\widehat{G}}\chi(g) - \sum_{\chi\in\widehat{G}}\chi(g) = 0,$$

which yields $\sum_{\chi\in\widehat{G}}\chi(g) = 0$.

□

**Definition 5.2.9.** *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 5.2.8 that $\boldsymbol{P}_G$ is unitary, i.e., $\boldsymbol{P}_G^{-1} = \overline{\boldsymbol{P}_G}^T$.*

**Lemma 5.2.10.** *Let $G$ be a finite abelian group and $\boldsymbol{A} \in \mathbb{C}^{G\times G}$ be a complex $G\times G$ matrix. Then the following are equivalent.*

*i) $\boldsymbol{A} = (a_{gh^{-1}})_{g,h\in G}$ is $G$-circulant associated to $\boldsymbol{a} = (a_g)_{g\in G}$.*

*ii) The $\widehat{G}\times\widehat{G}$ matrix $\boldsymbol{P}_G^{-1}\boldsymbol{A}\boldsymbol{P}_G$ is diagonal.*

*Proof.* We have to prove both directions.

- "$i) \Rightarrow ii)$": If $\mathbf{A}$ is $G$-circulant and $\chi \in \widehat{G}$, then

$$\mathbf{A}\chi = \left(\sum_{h\in G} a_{gh^{-1}}\chi(h)\right)_{g\in G} = \left(\sum_{k\in G} a_k \chi(gk^{-1})\right)_{g\in G} = \left(\chi(g)\sum_{k\in G} a_k\overline{\chi}(k)\right)_{g\in G} = \lambda_\chi \cdot \chi,$$

  where $\lambda_\chi := \sum_{k\in G} a_k\overline{\chi}(k) = \langle \mathbf{a}, \chi\rangle$ (therefore $\chi$ is a eigenvector of $\mathbf{A}$ and $\lambda_\chi$ is its corresponding eigenvalue). Hence, the columns of $\mathbf{P}_G$, which are the vectors $\chi$, are eigenvectors of $\mathbf{A}$, what implies that $\mathbf{P}_G^{-1}\mathbf{A}\mathbf{P}_G$ is diagonal.

- "$ii) \Rightarrow i)$": Let $\mathbf{P}_G^{-1}\mathbf{A}\mathbf{P}_G =: \mathbf{D} \in \mathbb{C}^{\widehat{G}\times\widehat{G}}$ be diagonal. We have to prove that $(\mathbf{A})_{g,h}$ only depends on $g \cdot h^{-1}$. We have

$$\begin{aligned}(\mathbf{A})_{g,h} = \left(\mathbf{P}_G\mathbf{D}\mathbf{P}_G^{-1}\right)_{g,h} &= \sum_{\chi\in\widehat{G}} (\mathbf{P}_G\mathbf{D})_{g,\chi}\cdot\left(\mathbf{P}_G^{-1}\right)_{\chi,h}\\ &= \sum_{\chi\in\widehat{G}}\sum_{\Psi\in\widehat{G}} (\mathbf{P}_G)_{g,\Psi}\cdot(\mathbf{D})_{\Psi,\chi}\cdot|G|^{-1/2}\overline{\chi}(h)\\ &= \sum_{\chi\in\widehat{G}} |G|^{-1}\chi(g)\cdot(\mathbf{D})_{\chi,\chi}\cdot\chi(h^{-1})\\ &= |G|^{-1}\sum_{\chi\in\widehat{G}}(\mathbf{D})_{\chi,\chi}\cdot\chi(gh^{-1}),\end{aligned}$$

  hence $(\mathbf{A})_{g,h}$ only depends on $g\cdot h^{-1}$ as required.

□

**Theorem 5.2.11.** *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 $\chi$.*
*If $\boldsymbol{A}$ is invertible, then $(\boldsymbol{A}^{-1})^T$ is $G$-circulant and the norm of the vector $\boldsymbol{a}^* \in \mathbb{C}^G$ associated to $(\boldsymbol{A}^{-1})^T$ is given by*

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

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

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

That $\lambda_\chi$ are the eigenvalues of $\mathbf{A}$ to the eigenvector $\chi$ we have already proven in Lemma 5.2.10. This Lemma also yields that, if existent, $(\mathbf{A}^{-1})^T$ is $G$-circulant. The eigenvalues of $(\mathbf{A}^{-1})^T$ are given by $\lambda_\chi^{-1}$, which yields $||\mathbf{a}^*||_2^2 = |G|^{-1}\cdot\sum_{\chi\in\widehat{G}}|\lambda_\chi|^{-2}$ for the vector $\mathbf{a}^*$ associated to $(\mathbf{A}^{-1})^T$. □

## 5.3 Dirichlet L-Series

Again, to generalize the results given in [CDPR16], we give a very similar introduction to the Dirichlet L-function and its applications, see [CDPR16, Section 2.3].

**Definition 5.3.1.** *Let $\chi$ be any Dirichlet character, then the Dirichlet L-function $L(\cdot, \chi)$ is defined as*

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

*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 $\chi$ 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 $\chi$ 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 [MV06, Theorem 10.7. ff]. Therefore, $L(1, \chi)$ is well defined in this case.

**Theorem 5.3.2** ([MV06, Theorem 4.9.])**.** *If $\chi$ is a non trivial character mod $m \in \mathbb{N}$, then*

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

**Theorem 5.3.3.** *There exists a constant $C > 0$, such that for every non quadratic Dirichlet character $\chi$ 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 $\chi$ 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 [Lan27, p. 29]. For the second inequality, see [Sie35] or [JL04] for concrete results on the constant $C > 0$. □

The following is a generalization of the famous Riemann hypothesis.

**Conjecture 5.3.4** (**Generalized Riemann Hypothesis (GRH)**)**.** *Let $\chi$ be a character mod $m \in \mathbb{N}$. If $L(s, \chi) = 0$ for some $s \in \mathbb{C}$ with $0 \leq \Re(s) \leq 1$, then $\Re(s) = \frac{1}{2}$.*
*In particular, if $\chi \equiv 1$ is the trivial character mod 1, this is the Riemann hypothesis.*

Under GRH, we have the following improved lower bound.

**Theorem 5.3.5** ([LLS15, Theorem 1.5.])**.** *Under GRH, there exists a constant $C > 0$, such that for every Dirichlet character $\chi$ mod $m \in \mathbb{N}$ of conductor $f_\chi \geq 3$*

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

## 5.4 Cyclotomic Polynomials

**Definition 5.4.1.** *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 $\mathbb{Q}$.*

Notice that $\xi_m \in \mathbb{C}$ is a root of the monic polynomial $X^m - 1 \in \mathbb{Z}[X]$, hence $\xi_m$ is integral, which implies that its minimal polynomial lies in $\mathbb{Z}[X]$ by Lemma 2.2.2.

**Lemma 5.4.2.** *The cyclotomic polynomial $\Phi_m$ for $m \in \mathbb{N}$ is given by*

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^\times} \left(X - \xi_m^i\right).$$

*Proof.* We know that $\mathbb{Q}(\xi_m)/\mathbb{Q}$ is Galois with Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}) \cong \mathbb{Z}_m^\times$, and the automorphisms $\sigma_i(\cdot) \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ are characterized by $\sigma_i(\xi_m) = \xi_m^i$ for $i \in \mathbb{Z}_m^\times$. Hence, from Galois theory we obtain

$$\Phi_m(X) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})} (X - \sigma(\xi_m)) = \prod_{i \in \mathbb{Z}_m^\times} \left(X - \xi_m^i\right).$$

□

Note that we have used $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}) \cong \mathbb{Z}_m^\times$ in the last proof, what is a non trivial fact, if one does not know the cyclotomic polynomial $\Phi_m$.

**Theorem 5.4.3.** *For $n, m \in \mathbb{N}$ we have the factorization in irreducible factors*

$$\Phi_n(X^m) = \prod_{\substack{d \mid m \\ \gcd(d,n)=1}} \Phi_{n \cdot \frac{m}{d}}(X).$$

*Proof.* In $\mathbb{C}$ we can factor

$$\Phi_n(X^m) = \prod_{k \in \mathbb{Z}_n^\times} \left(X^m - \xi_n^k\right),$$

hence it is sufficient to investigate the polynomials $X^m - \xi_n^k$. The roots of this polynomials are of course the $m$ different $m$-th roots of $\xi_n^k$, which are of the form

$$\xi_{mn}^{k+jn} = e^{2\pi i \frac{k}{nm} + 2\pi i \frac{j}{m}} \qquad \text{for } j = 0, \ldots, m-1.$$

From this the equation

$$\Phi_n(X^m) = \prod_{(k,j) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m} \left(X - \xi_{nm}^{k+jn}\right)$$

follows immediately, whereby we identify $\mathbb{Z}_n^\times = \{l \in \mathbb{N} |\ 1 \le l \le n,\ \gcd(l,n) = 1\}$ and $\mathbb{Z}_m = \{0, \ldots, m\}$. The next step is to prove the bijectivity of the mapping

$$\begin{aligned} \mathbb{Z}_n^\times \times \mathbb{Z}_m &\to \{z \in \mathbb{Z}_{nm} |\ d := \gcd(z, mn),\ d|m,\ \gcd(d,n) = 1\} =: M \\ (k, j) &\mapsto k + j \cdot n. \end{aligned}$$

- *Well defined:* Let $(k,j) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m$, $z := k + jn$ and $d := \gcd(z, mn)$. Obviously $z \in \mathbb{Z}_{mn} = \{0, ..., mn\}$ holds. We conclude from $\gcd(k,n) = 1$ the first condition
$$d = \gcd(k + jn, mn) = \gcd(k + jn, m) | m,$$
and analogously
$$\gcd(d,n) | \gcd(k + jn, n) = \gcd(k,n) = 1,$$
which yields $\gcd(d,n) = 1$.
- *Injective:* For $(k_1, j_1), (k_2, j_2) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m$ with $k_1 + j_1 n = k_2 + j_2 n$ we have $k_1 - k_2 = (j_2 - j_1)n$ and $|k_1 - k_2| < n$, which implies $j_2 - j_1 = 0$, i.e. $(k_1, j_1) = (k_2, j_2)$.
- *Surjective:* Let $z \in M$, we define $d := \gcd(z, mn)$. There is a unique $k \in \mathbb{Z}_n$ and $j \in \mathbb{Z}_m$ with $z = k + jn$, so we only have to prove $\gcd(k,n) = 1$. We observe
$$\gcd(k,n) = \gcd(k + jn, n) = \gcd(z,n) =: g.$$
By definition $g | \gcd(z, mn) = d$ and therefore $g | \gcd(d,n) = 1$ holds, from this, $g = 1$ follows immediately.

The order of $\xi_{mn}^z$ is $\frac{nm}{d}$ with $d := \gcd(z, mn)$, so together with the bijectivity of the mentioned mapping and the definition of the cyclotomic polynomials we conclude
$$\Phi_n(X^m) = \prod_{z \in M} \left(X - \xi_{nm}^z\right) = \prod_{\substack{d|m \\ \gcd(d,n)=1}} \Phi_{n \cdot \frac{m}{d}}(X).$$

□

**Corollary 5.4.4.** *Let $p$ be a prime and $n \in \mathbb{N}$. Then the following holds.*
$$\Phi_{p \cdot n}(X) = \begin{cases} \Phi_n(X^p), & \text{if } p | n \\ \frac{\Phi_n(X^p)}{\Phi_n(X)}, & \text{if } p \nmid n. \end{cases}$$

*Proof.* If $p|n$, Theorem 5.4.3 implies
$$\Phi_n(X^p) = \prod_{\substack{d|p \\ \gcd(d,n)=1}} \Phi_{n \cdot \frac{p}{d}}(X) = \Phi_{n \cdot p}(X).$$
Analogously, in the case $p \nmid n$ Theorem 5.4.3 yields
$$\Phi_n(X^p) = \prod_{\substack{d|p \\ \gcd(d,n)=1}} \Phi_{n \cdot \frac{p}{d}}(X) = \Phi_n(X) \cdot \Phi_{n \cdot p}(X),$$
which proves the claim. □

**Corollary 5.4.5.** *Let $m \in \mathbb{N}$ with $m \geq 2$. Then the following holds.*
$$\Phi_m(1) = \begin{cases} p, & \text{if } m = p^l \text{ for some prime } p \text{ and } l \in \mathbb{N} \\ 1, & \text{else.} \end{cases}$$

*Proof.* If $m = p^l$ for some prime $p$ and $l \in \mathbb{N}$, then by induction and Corollary 5.4.4
$$\Phi_m(1) = \Phi_{p^{l-1}}(1) = ... = \Phi_p(1) = p,$$
since $\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + ... + X^{p-1}$.
Else, there are distinct primes $p, q$ with $m = p^l \cdot q \cdot n$ and $p^{l+1} \nmid m$ for some $n \in \mathbb{N}$. Therefore $q \cdot n > 1$ and hence $\Phi_{q \cdot n}(1) \neq 0$, which implies by induction and Corollary 5.4.4
$$\Phi_m(1) = \Phi_{p^l \cdot q \cdot n}(1) = \Phi_{p^{l-1} \cdot q \cdot n}(1) = ... = \Phi_{p \cdot q \cdot n}(1) = \frac{\Phi_{q \cdot n}(1^p)}{\Phi_{q \cdot n}(1)} = 1.$$

□

## 5.5 Generator Prime Pairs

In the next section we investigate the group generated by the elements $\frac{\xi_m^u - 1}{\xi_m - 1}$ for the case, that $m = p^\alpha q^\beta$ only have two distinct odd prime factors. As it turns out, 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, in this section we work out some results for those prime pairs.

**Definition 5.5.1.** *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 $(\alpha, \beta)$-**generator prime pair**. If $(p, q)$ is an $(\alpha, \beta)$-generator prime pair for every $\alpha, \beta \in \mathbb{N}$, we just say that $(p, q)$ is a **generator prime pair (GPP)**.*

The following theorem states that if a number $g \in \mathbb{Z}$ generates $\mathbb{Z}_p^\times$ and $\mathbb{Z}_{p^2}^\times$ for an odd prime $p \in \mathbb{P}$, then $g$ is a generator of $\mathbb{Z}_{p^l}$ for every $l \in \mathbb{N}$.

**Theorem 5.5.2** ([Coh00, 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 $l \in \mathbb{N}$.*

**Corollary 5.5.3.** *Let $p$ be an odd prime. Then $\mathbb{Z}_{p^l}^\times$ is cyclic for every $l \in \mathbb{N}$.*

*Proof.* Since $\mathbb{Z}_p$ is a finite field for every prime $p$, the multiplicative group $\mathbb{Z}_p^\times$ is cyclic. Hence, the proposition follows immediately from Theorem 5.5.2. □

**Corollary 5.5.4.** *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 character of $\mathbb{Z}_{p^l}^\times$ are given by*

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

*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.* Corollary 5.5.3 states that $\mathbb{Z}_{p^l}^\times$ is cyclic, therefore there exists such a generator $g \in \mathbb{Z}_{p^l}^\times$. Hence, all characters of $\mathbb{Z}_{p^l}^\times$ are given by $\chi_1, ..., \chi_{\varphi(p^l)-1}$, where $\chi_h$ for $0 \le h \le \varphi\left(p^l\right) - 1$ denotes the corresponding character from Theorem 5.2.5. We only have to prove that $\chi_h$ 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 5.5.5.** *Let $(p, q)$ be an $(\alpha, \beta)$-generator prime pair for some $\alpha, \beta \in \mathbb{N}$ and $\beta \ge 2$. Then the following holds.*

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

*In other words, $(p, q)$ is an $(\alpha, l)$-generator prime pair for every $l \in \mathbb{N}$. Analogously, the same results follows if we swap $p$ and $q$.*

*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 5.5.2. 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 $g^2 \equiv p \mod q^\beta$, which exists by Corollary 5.5.3 and the fact, that the order of $p$ is $\frac{\varphi(q^l)}{2}$. Since $g \in \mathbb{Z}$ is a generator of $\mathbb{Z}_{q^\beta}^\times$ and therefore also for $\mathbb{Z}_{q^2}^\times$ and $\mathbb{Z}_q^\times$, since $\beta \geq 2$, Theorem 5.5.2 implies that $g$ 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 $a \equiv 2 \mod \varphi\left(q^2\right) = q \cdot \frac{q-1}{2}$. Therefore, there is some $k \in \mathbb{Z}$ with $a = 2 + k \cdot \varphi(q^2)$. Since

$$\gcd\left(1 + k \cdot q \cdot \frac{q-1}{2}, \frac{\varphi\left(q^l\right)}{2}\right) = \gcd\left(1 + k \cdot q \cdot \frac{q-1}{2}, q^{l-1} \cdot \frac{q-1}{2}\right) = 1,$$

the order of $g^a \equiv g^{2+kq(q-1)} \equiv g^{2\cdot\left(1+kq\frac{q-1}{2}\right)} \mod q^l$ is $\frac{\varphi\left(q^l\right)}{2}$ in $\mathbb{Z}_{q^l}^\times$, because $g$ is a generator of $\mathbb{Z}_{q^l}^\times$.
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 $\mathbb{Z}_{q^l}^\times$. □

**Theorem 5.5.6.** *Corollary 5.5.5 states, that we only have four cases for an $(\alpha, \beta)$-generator prime pair $(p, q)$, if we choose $\alpha, \beta \leq 2$ maximally, namely*

1. $(p, q)$ ***is a*** $(2, 2)$***-generator prime pair.***

   *In this case $(p, q)$ is an $(\alpha, \beta)$-generator prime pair for every $\alpha, \beta \in \mathbb{N}$, i.e., $(p, q)$ is a generator prime pair.*

2. $(p, q)$ ***is a*** $(1, 2)$***-generator prime pair or a*** $(2, 1)$***-generator prime pair.***

   *In this case $(p, q)$ is a $(1, \beta)$-generator prime pair for every $\beta \in \mathbb{N}$ or an $(\alpha, 1)$-generator prime pair for every $\alpha \in \mathbb{N}$, respectively.*

3. $(p, q)$ ***is a*** $(1, 1)$***-generator prime pair.***

4. $(p, q)$ ***is not a*** $(1, 1)$***-generator prime pair.***

As we will see, 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 $(\alpha, \beta)$-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 $\alpha, \beta \in \mathbb{N}$. By Theorem 5.5.6, to test whether $(p, q)$ is a generator prime pair or not, one only has to determine whether $(p, q)$ is a $(2, 2)$-generator prime pair or not.
Figure 5.1 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 |

**Figure 5.1:** Generator prime pairs

**Example 5.5.7.** *We give some examples for $(\alpha,\beta)$-generator prime pairs, if we choose $\alpha,\beta \leq 2$ as large as possible.*

1. $(3,5)$ *is a* $(2,2)$*-generator prime pair and therefore a generator prime pair.*
2. $(3,11)$ *is a* $(2,1)$*-generator prime pair, since* $3^5 \equiv 1 \mod 11^2$ *and* $\frac{\varphi(11^2)}{2} = 55$.
3. *There are no* $(1,1)$*-generator prime pairs for* $p,q \leq 37813$*, i.e., if* $(p,q)$ *is a* $(1,1)$*-generator prime pair, it is a* $(2,2)$*,* $(2,1)$ *or* $(1,2)$*-generator prime pair in this case. This result was computed with SageMathCloud, see Listing 6.2 in the appendix. We do not know whether there are such prime pairs.*
4. $(5,11)$ *is not a* $(1,1)$*-generator prime pair, since* $11 \equiv 1 \mod 5$ *and* $\varphi(5) = 4$.

In Figure 5.2 we have plotted all generator prime pairs $(p,q)$ with $p,q \leq 600$. Figure 5.3 and 5.4 show 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 5.4 shows. For the computation of $Q(x)$, see Listing 6.5 in the appendix.


**Figure 5.2:** Generator prime pairs

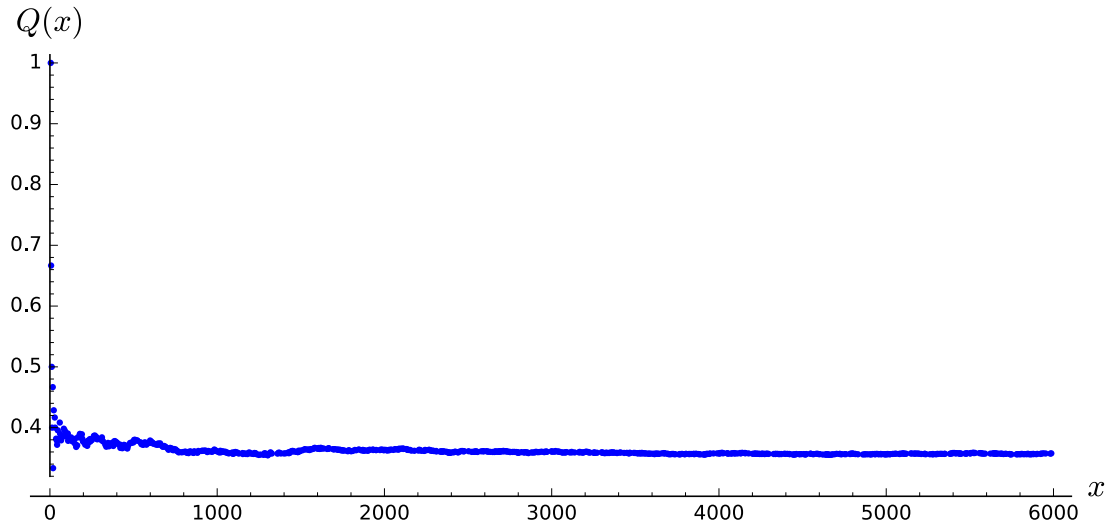



**Figure 5.3:** Values of the quotient $Q(x) = \frac{\text{Number of GPP } (p,q) \text{ with } 2 < p < q \leq x}{\text{Number of Primepairs } (p,q) \text{ with } 2 < p < q \leq x}$

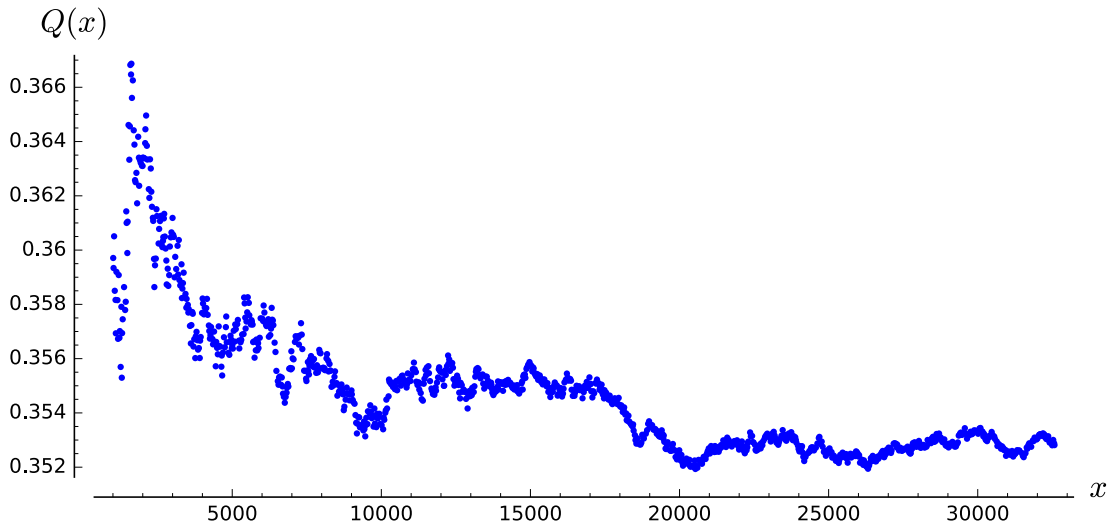



**Figure 5.4:** Values of the quotient $Q(x) = \frac{\text{Number of GPP } (p,q) \text{ with } 2 < p < q \leq x}{\text{Number of Primepairs } (p,q) \text{ with } 2 < p < q \leq x}$ for large $x$

An interesting fact is that a similar notion of prime pairs was used in the proof of Catalan's conjecture by Preda Mihăilescu in 2002, namely **double Wieferich prime pairs** $(p,q)$, which satisfies

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

see [Sch10, Chapter 1]. In particular, double Wieferich prime pairs can not be $(2,2)$, $(2,1)$ and $(1,2)$-generator prime pairs.

## 5.6 Units for $m = p^\alpha q^\beta$

Now we are prepared to investigate the group generated by the elements $\frac{\xi_m^j - 1}{\xi_m - 1}$ for the case, that $m = p^\alpha q^\beta$ only contains two distinct odd prime factors.

**Definition 5.6.1.** *Let $m \in \mathbb{N}$ with $m \geq 3$. For $j \in \mathbb{Z}_m^\times$ we define*

$$b_j := \frac{\xi_m^j - 1}{\xi_m - 1} \in \mathcal{O}_m^\times \tag{5.1}$$

*and*

$$\boldsymbol{b}_j := Log_r(b_j) \in \mathbb{R}^{n/2},$$

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

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

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

$$\boldsymbol{B} := \left( \log\left( \left| \frac{\xi_m^{ij} - 1}{\xi_m^i - 1} \right| \right) \right)_{\substack{i \in G_m \\ j \in G_m \backslash \{1\}}}. \tag{5.2}$$

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 $\frac{\varphi(m)}{2} - 1 = |G_m\backslash\{1\}|$.

### 5.6.1 Index

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 will see, the index is finite iff $(p,q)$ is an $(\alpha,\beta)$-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 statement [Was96, Corollary 8.8.] for the real case.

**Lemma 5.6.2.** *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*

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

*if the right hand side is not equal 0, else the index is infinite. Remember, the factor $h_m^+$ denotes the class number of $K_m^+ = \mathbb{Q}(\xi_m)^+$.*

*Proof.* By [Was96, Corollary 8.8.], the index of the group $\mathscr{S}_m^+$ generated by $-1$ and $b_j^+ = \xi_{2m}^{1-j} \cdot b_j \in (\mathscr{O}_m^+)^\times$ for $j \in G_m$ in $(\mathscr{O}_m^+)^\times$ is

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

Now, Corollary 4.2.7 and Example 4.2.8 implies

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

□

**Definition 5.6.3.** *We define the factor* $\prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} (1 - \chi(p))$ *for* $m \in \mathbb{N}$ *as*

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

**Theorem 5.6.4.** *Let* $p, q$ *be two distinct odd primes and* $m = p^\alpha q^\beta$ *for some* $\alpha, \beta \in \mathbb{N}$*. Then*

$$\beta_m = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t \mid m \\ t \in \mathbb{P}}} (1 - \chi(t)) \neq 0 \text{ iff } (p, q) \text{ is an } (\alpha, \beta)\text{-generator prime pair.}$$

*Proof.* The factor $\beta_m$ is zero iff there exists an even character $\chi \in \widehat{\mathbb{Z}_m^\times}$ with $\chi \not\equiv 1$ and $\chi(p) = 1$ or $\chi(q) = 1$, since $t$ can only be $t = p$ or $t = q$.
First, we assume that $(p, q)$ is an $(\alpha, \beta)$-generator prime pair, but the factor $z$ is zero. Therefore, w.l.o.g. we assume $\chi(p) = 1$ for some non trivial, even character $\chi \in \widehat{\mathbb{Z}_m^\times}$. If $p | f_\chi$, then $\chi(p) = 0$, hence $f_\chi = q^l$ for some $1 \leq l \leq \beta$. We may assume that $\chi$ is defined mod $q^l$, i.e., is a non trivial, primitive, even character of $\mathbb{Z}_{q^l}^\times$. By Corollary 5.5.5, $(p, q)$ is an $(\alpha, l)$-generator prime pair, hence we only have to distinguish the following two cases.

- If $p$ is a generator of $\mathbb{Z}_{q^l}^\times$, there exists an even $h \in \{1, ..., \varphi\left(q^l\right) - 1\}$ with $\chi(p) = \xi_{\varphi(q^l)}^h \neq 1$ by Corollary 5.5.4 (we have chosen $g := p$, therefore $p^1 \equiv p \mod q^l$), which contradicts $\chi(p) = 1$.

- Hence, the only case left is $q - 1 \not\equiv 0 \mod 4$ and $p$ has order $\frac{\varphi(q^l)}{2}$ in $\mathbb{Z}_{q^l}^\times$. It follows $\varphi\left(q^l\right) \equiv q^{l-1}(q-1) \not\equiv 0 \mod 4$, since $q$ is an odd prime. Let $g$ be a generator of $\mathbb{Z}_{q^l}^\times$, which exists by Corollary 5.5.3, and $a \in \mathbb{Z}$ with $g^a \equiv p \mod q^l$. If we compare the order, it follows $\gcd\left(a, \varphi\left(q^l\right)\right) = 2$. Again, there is some even $h \in \{1, ..., \varphi\left(q^l\right) - 1\}$ with $1 = \chi(p) = \xi_{\varphi(q^l)}^{ah}$ by Corollary 5.5.4. We conclude $4 | ah | \varphi\left(q^l\right)$, which contradicts $\varphi\left(q^l\right) \not\equiv 0 \mod 4$. Therefore, the factor $\beta_m$ cannot be zero.

Now, assume that $(p, q)$ is not an $(\alpha, \beta)$-generator prime pair, i.e., w.l.o.g. $p$ is not a generator of $\mathbb{Z}_{q^\beta}^\times$ and has not order $\frac{\varphi(q^\beta)}{2}$ 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 $t \mid \gcd\left(a, \varphi\left(q^\beta\right)\right)$. 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 $4 \mid \varphi\left(q^\beta\right)$. By Corollary 5.5.4, there is a non trivial, even Dirichlet character $\chi_h$ of $\mathbb{Z}_{q^\beta}^\times$ with

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

- 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 $t \mid \gcd\left(a, \varphi\left(q^\beta\right)\right)$. 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 5.5.4, there is a non trivial, even Dirichlet character $\chi_h$ of $\mathbb{Z}_{q^\beta}^\times$ with

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

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

**Theorem 5.6.5.** *If $(p,q)$ is an $(\alpha,\beta)$-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$, then*

$$\beta_m = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t \mid m \\ t \in \mathbb{P}}} (1 - \chi(t)) = \frac{\varphi(m)}{4} = \frac{(p-1)(q-1)}{4pq} m.$$

*Proof.* Since $m$ only has two prime factors $p, q$, we have

$$\prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t \mid m \\ t \in \mathbb{P}}} (1 - \chi(p)) = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} (1 - \chi(p))(1 - \chi(q)).$$

If $\chi \in \widehat{\mathbb{Z}_m^\times}$ is an even character of conductor $f_\chi > 1$ with $pq \mid f_\chi$, then $\chi(p) = \chi(q) = 0$ and therefore $(1-\chi(p))(1-\chi(q)) = 1$. Hence, we split the product into two products over even Dirichlet characters with prime power conductors $p^l$ and $q^l$ for some $l \in \mathbb{N}$. Since all these characters can be extended to even Dirichlet characters of $\mathbb{Z}_{p^\alpha}^\times$ or $\mathbb{Z}_{q^\beta}^\times$, we split the product into two products over non trivial, even Dirichlet characters of $\mathbb{Z}_{p^\alpha}^\times$ and $\mathbb{Z}_{q^\beta}^\times$. Alternatively, it is easy to see that the non trivial, even Dirichlet characters of $\mathbb{Z}_{p^\alpha}^\times$ correspond to the set of all non trivial, even Dirichlet characters of $\mathbb{Z}_m^\times$ whose conductor is not divisible by $q$, via concatenation with the natural projection $\pi : \mathbb{Z}_m^\times \to \mathbb{Z}_{p^\alpha}^\times$.

$$\begin{aligned}
\prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} (1 - \chi(p))(1 - \chi(q)) &= \left( \prod_{\substack{\chi \in \widehat{\mathbb{Z}_{p^\alpha}^\times} \\ \chi \neq 1 \\ \chi \text{ even}}} (1 - \chi(p))(1 - \chi(q)) \right) \cdot \left( \prod_{\substack{\chi \in \widehat{\mathbb{Z}_{q^\beta}^\times} \\ \chi \neq 1 \\ \chi \text{ even}}} (1 - \chi(p))(1 - \chi(q)) \right) \\
&= \left( \prod_{\substack{\chi \in \widehat{\mathbb{Z}_{p^\alpha}^\times} \\ \chi \neq 1 \\ \chi \text{ even}}} (1 - \chi(q)) \right) \cdot \left( \prod_{\substack{\chi \in \widehat{\mathbb{Z}_{q^\beta}^\times} \\ \chi \neq 1 \\ \chi \text{ even}}} (1 - \chi(p)) \right).
\end{aligned}$$

Hence it is sufficient to prove

$$\prod_{\substack{\chi \in \widehat{G_{q^\beta}} \\ \chi \neq 1}} (1-\chi(p)) = \frac{\varphi\left(q^\beta\right)}{2}.$$

Let $g$ be a generator of $\mathbb{Z}_{q^\beta}^\times$, and $a \in \mathbb{Z}$ with $g^a \equiv p \mod q^\beta$, which exists by Corollary 5.5.3. Since $(p,q)$ is an $(\alpha,\beta)$-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 5.5.4, which implies

$$\begin{aligned}
\prod_{\substack{\chi \in \widehat{G_{q^\beta}} \\ \chi \neq 1}} (1-\chi(p)) &= \prod_{\substack{1 \le h \le \varphi\left(q^\beta\right)-1 \\ h \text{ even}}} \left(1-\xi_{\varphi\left(q^\beta\right)}^{ha}\right) \\
&= \prod_{1 \le k \le \frac{\varphi\left(q^\beta\right)}{2}-1} \left(1-\xi_{\frac{\varphi\left(q^\beta\right)}{2}}^{ka}\right) \\
&\underset{(1)}{=} \prod_{1 \le k \le \frac{\varphi\left(q^\beta\right)}{2}-1} \left(1-\xi_{\frac{\varphi\left(q^\beta\right)}{2}}^{k}\right) \\
&\underset{(2)}{=} \frac{X^{\frac{\varphi\left(q^\beta\right)}{2}}-1}{X-1}\Big|_{X=1} \\
&= \left(X^{\frac{\varphi\left(q^\beta\right)}{2}-1} + X^{\frac{\varphi\left(q^\beta\right)}{2}-2} + \ldots + 1\right)\Big|_{X=1} = \frac{\varphi\left(q^\beta\right)}{2},
\end{aligned}$$

where we used in equality *(1)* that multiplying with $a$ is a permutation of $\mathbb{Z}_{\frac{\varphi(q^\beta)}{2}}$ 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 $l \in \mathbb{N}$. □

**Corollary 5.6.6.** *Let $(p,q)$ be a generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$, then*

$$[\mathcal{O}_m^\times : \mathcal{S}_m] = h_m^+ \frac{(p-1)(q-1)}{2pq} m \le h_m^+ \cdot \frac{m}{2}.$$

*Proof.* This is a direct consequence of Lemma 5.6.2, Theorem 5.6.4 and Theorem 5.6.5. □

In Figure 5.5 we have plotted the factor $\beta_m$ for $m = p^\alpha q^\beta \le 600$, where $\alpha, \beta \in \mathbb{N}$ and $p, q$ are two odd primes. Figure 5.6 shows the factor $\beta_m$ for the same case but allowing one prime factor to be 2.
By computation, we conjecture that

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

for all odd primes $q$ and $\alpha, \beta \in \mathbb{N}$ with $\alpha \ge 2$, whenever $\beta_{2^\alpha q^\beta} \neq 0$. Our techniques do not work in this case, since we used that $\mathbb{Z}_{q^l}^\times$ is cyclic for an odd prime $q$ and $l \in \mathbb{N}$. Unluckily, $\mathbb{Z}_{2^l}^\times$ is cyclic iff $l = 1$ or $l = 2$. However, the structure of $\mathbb{Z}_{2^l}^\times$ for $l \ge 3$ is given by

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

see [Coh00, Theorem 1.4.1.]. It seems very likely that this can be used to extend our results to the case, that one prime factor of $m$ is $p = 2$.

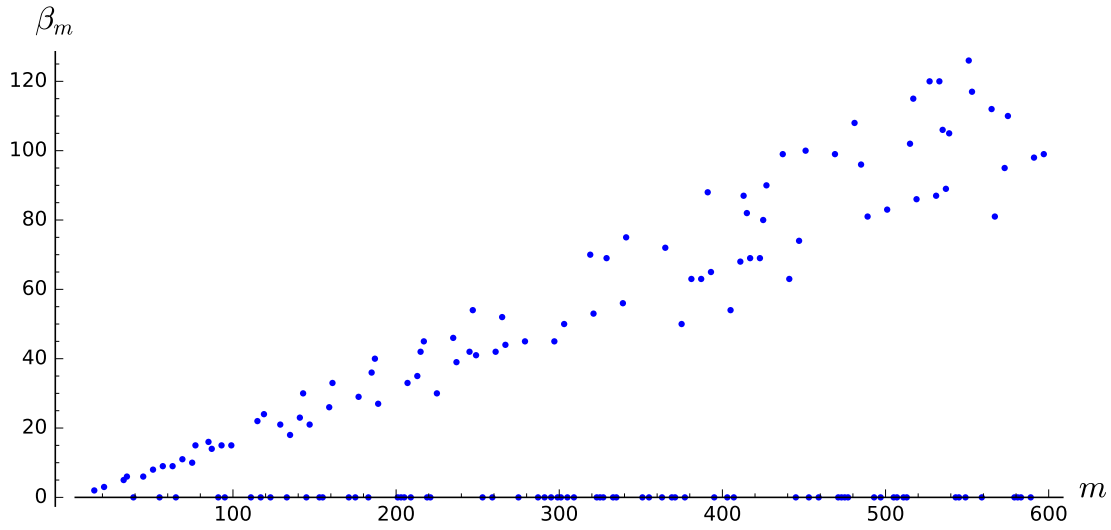



**Figure 5.5:** The factor $\beta_m$ for $m = p^\alpha q^\beta$ with two **odd** primes $p, q$

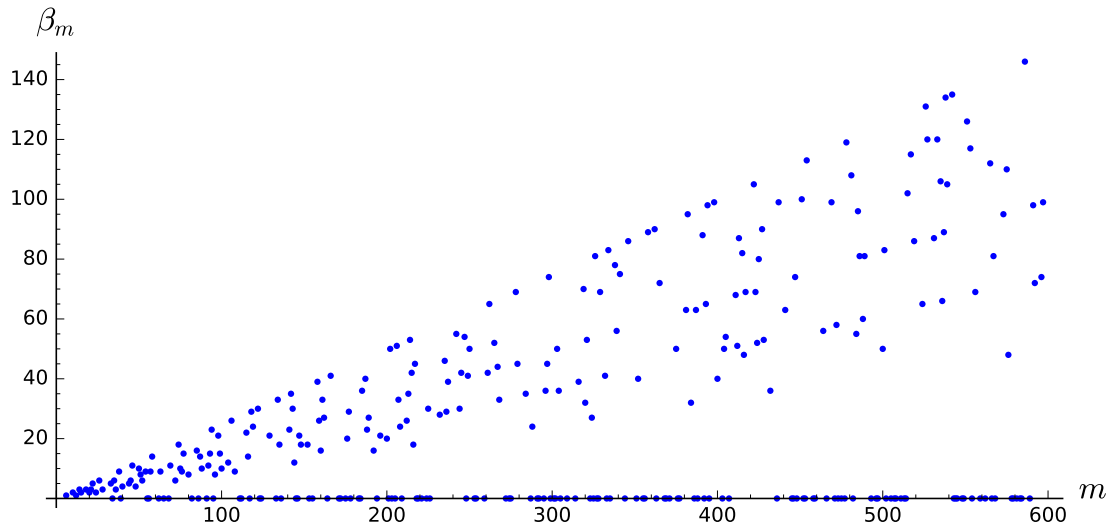



**Figure 5.6:** The factor $\beta_m$ for $m = p^\alpha q^\beta$ with two **arbitrary** primes $p, q$

We have proven that the factor $\beta_m$ is sufficiently small, if $m = p^\alpha q^\beta$ for some $(\alpha, \beta)$-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 5.6.7** ([Mil14a, Theorem 1.1.]). *Let $m$ be a composite integer, $m \not\equiv 2 \mod 4$, 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 5.6.8.** *In our case, $m = p^\alpha q^\beta$ for some $(\alpha,\beta)$-generator prime pair $(p,q)$. Since we want a polynomial running time in $m$ of Algorithm 3.3 for cyclotomic fields $K_m = \mathbb{Q}(\xi_m)$, we need an polynomial bound of the index $[\mathscr{O}_m^\times : \mathscr{S}_m] = 2h_m^+\beta_m$. 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 5.6.7 one could guess that there are similar results as in Remark 4.3.5 for the case that $m = p^\alpha q^\beta$ and the class number is $h_m^+$ is sufficiently small. In [CDW16] this is presented as a reasonable conjecture.*

### 5.6.2 Norm

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 $(\alpha,\beta)$-generator prime pair. Again, we follow along [CDPR16, 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 $\mathbf{Z}$ (which we will define soon) are equal 0, 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 it turns out, the eigenvalues of $\mathbf{Z}$ corresponding to the non trivial characters are all non zero iff $(p,q)$ is an $(\alpha,\beta)$-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

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

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

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

for all $j \in G_m$ (again, $n = \varphi(m)$ as in Definition 3.2.1). 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 $\mathrm{Log}_r(z_j) = \mathrm{Log}_r(z_{-j})$. 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 0, in the case that $m = p^\alpha q^\beta$, for some $\alpha,\beta \in \mathbb{N}$ and $(p,q)$ is an $(\alpha,\beta)$-generator prime pair.

**Lemma 5.6.9.** *Let $m = p^\alpha q^\beta$ for some distinct primes $p,q \in \mathbb{P}$ and $\alpha,\beta \in \mathbb{N}$. Then the eigenvalue $\lambda_\chi$ of $\mathbf{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is $\lambda_\chi = 0$.*

*Proof.* By Theorem 5.2.11, the eigenvalue of the $G_m$-circulant matrix $\mathbf{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is given by

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

where (1) follows from Lemma 5.4.2 and *(2)* is the statement of Corollary 5.4.5. □

**Remark 5.6.10.** *In the prime power case, i.e., if $m = p^\alpha$ for some prime $p$ and $\alpha \in \mathbb{N}$, the eigenvalue of the $G_m$-circulant matrix $\boldsymbol{Z}$ corresponding to the trivial character $1 \equiv \chi \in G_m$ is given by $\lambda_\chi = \frac{1}{2}\log(p) > 0$, since $\Phi_m(1) = p$ in this case. In particular, the eigenvalue is non zero. This argument was used but not proven in [CDPR16, Chapter 3].*

**Lemma 5.6.11.** *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Furthermore, let $\chi \in G_m$ (i.e., $\chi$ is an even character of $\mathbb{Z}_m^\times$) be a character of conductor $f_\chi > 1$ with $pq | f_\chi$. Then the eigenvalue $\lambda_\chi$ of $\boldsymbol{Z}$ corresponding to $\chi$ 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 $\chi$. 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

$$\pi^{-1}(a) = \left\{ a' + k \cdot f \in \mathbb{Z}_m^\times \middle| \ 0 \le k < \frac{m}{f} \right\}, \tag{5.3}$$

since $pq | f$ implies $\gcd(a' + k \cdot f, m) = 1$, and the kernel of $\pi$ has size $\frac{m}{f}$. One can easy see that the $\frac{m}{f}$ different numbers $a' + k \cdot f$ for $0 \le k < \frac{m}{f}$ are indeed different $\bmod m$. Now, by Theorem 5.2.11, the eigenvalue of the $G_m$-circulant matrix $\mathbf{Z}$ corresponding to $\chi$ is given by

$$\begin{aligned}
\lambda_\chi = \langle \mathbf{z}_1, \chi \rangle &= \sum_{j \in G_m} \overline{\chi}(j) \cdot \log\left(\left|\xi_m^j - 1\right|\right) \\
&= \frac{1}{2} \sum_{j \in \mathbb{Z}_m^\times} \overline{\chi}(j) \cdot \log\left(\left|1 - \xi_m^j\right|\right) \\
&= \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \sum_{\substack{j \in \mathbb{Z}_m^\times \\ \pi(j) = a}} \log\left(\left|1 - \xi_m^j\right|\right) \\
&\underset{(5.3)}{=} \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left( \prod_{0 \le k < \frac{m}{f}} \left|1 - \xi_m^{a' + k \cdot f}\right| \right) \\
&\underset{(\star)}{=} \frac{1}{2} \sum_{a \in \mathbb{Z}_f^\times} \overline{\chi}(a) \log\left(\left|1 - \xi_f^a\right|\right),
\end{aligned}$$

where we used in $(\star)$ the identity $X^n - Y^n = \prod_{0 \le k < n} \left(X - \xi_n^k Y\right)$ 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 5.6.12.** *Let $m = p^\alpha q^\beta$ for some distinct primes $p, q \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{N}$. Furthermore, let $\chi \in G_m$ (i.e., $\chi$ 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 $\lambda_\chi$ of $\boldsymbol{Z}$ corresponding to $\chi$ is given by*

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

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

*Proof.* Let $f := f_\chi > 1$ be the conductor of $\chi$, 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

$$\pi^{-1}(a) = \Psi^{-1}\left(\left\{a' + k \cdot f \in \mathbb{Z}_{p^\alpha}^\times \,\middle|\, 0 \le k < \frac{p^\alpha}{f}\right\} \times \mathbb{Z}_{q^\beta}^\times\right) \subseteq \mathbb{Z}_m^\times \tag{5.4}$$

by Chinese remainder theorem, where

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

and the commutativity of the following diagram, where $p_1 : \mathbb{Z}_{p^\alpha}^\times \times \mathbb{Z}_{q^\beta}^\times \to \mathbb{Z}_{p^\alpha}^\times$ denotes the projection to the first component, and $\pi' : \mathbb{Z}_{p^\alpha}^\times \to \mathbb{Z}_f^\times$ the canonical projection of $\mathbb{Z}_{p^\alpha}^\times$ to $\mathbb{Z}_f^\times$.

$$\begin{array}{ccc} \mathbb{Z}_m^\times & \xrightarrow{\pi} & \mathbb{Z}_f^\times \\ \downarrow{\scriptstyle \Psi} & & {\scriptstyle \pi'}\uparrow \\ \mathbb{Z}_{p^\alpha}^\times \times \mathbb{Z}_{q^\beta}^\times & \xrightarrow{p_1} & \mathbb{Z}_{p^\alpha}^\times \end{array}$$

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

$$\pi^{-1}(a) = \left\{(a' + k \cdot f) \cdot r_1 q^\beta + y \cdot r_2 p^\alpha \in \mathbb{Z}_m^\times \,\middle|\, 0 \le k < \frac{p^\alpha}{f},\ y \in \mathbb{Z}_{q^\beta}^\times\right\} \subseteq \mathbb{Z}_m^\times \tag{5.5}$$

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

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

In equation (1) we have used again the identity $X^n - Y^n = \prod_{0 \le k < n} \left(X - \xi_n^k Y\right)$ 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 $Y = \xi_f^{ar_1}$. 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 calculate the eigenvalue $\lambda_\chi$.

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

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 $\lambda_\chi$ and the Dirichlet L-function.

**Theorem 5.6.13** ([Was96, Lemma 4.8. and Theorem 4.9.])**.** *Let $\chi$ be an even Dirichlet character* mod *$m \in \mathbb{N}$ of conductor $f_\chi > 1$. Then*

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

**Theorem 5.6.14.** *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 $\lambda_\chi = \langle \mathbf{z}_1, \chi \rangle$ of $\boldsymbol{Z}$ corresponding to $\chi$ is given by*

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

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

*Proof.* If $pq|f_\chi$, then $\chi(p) = \chi(q) = 0$, i.e., $(1-\overline{\chi}(p))(1-\overline{\chi}(q)) = 1$. Else, if $f_\chi = p^e$ for some $1 \leq e \leq \alpha$, then $\chi(p) = 0$, what implies $(1-\overline{\chi}(p))(1-\overline{\chi}(q)) = (1-\overline{\chi}(q))$. 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 5.6.11, Lemma 5.6.12 and Theorem 5.6.13 imply

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

By Theorem 5.3.2, $L(1,\chi) \neq 0$ holds for all non trivial characters. Hence, we conclude that $\lambda_\chi = 0$ holds for some non trivial, even character $\chi \bmod m$ iff

$$0 = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} (1-\overline{\chi}(p))(1-\overline{\chi}(q)) = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t|m \\ t \in \mathbb{P}}} (1-\chi(t)) = \beta_m,$$

where we used the fact that concatenation with the complex conjugation is a permutation of $\widehat{G_m}$. By Theorem 5.6.4, $\beta_m \neq 0$ holds iff $(p,q)$ is an $(\alpha,\beta)$-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 $\lambda_\chi$. 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 [CDPR16, Lemma 3.2.].

**Lemma 5.6.15.** *Let $(p,q)$ be an $(\alpha,\beta)$-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 $\chi$.*
*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 5.6.14. 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., $\widehat{G_m} = \{\chi_1, ..., \chi_n\}$ 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 $\chi_j$ are different from the characters of Theorem 5.2.5, we only used a similar notation. The order of $\widehat{G_m}$ yields an order of the eigenvalues $\lambda_1, ..., \lambda_k$ of $\mathbf{Z}$, where $\lambda_1 = 0$ by Lemma 5.6.9 and $\lambda_j \neq 0$ for $2 \leq j \leq n$ by Theorem 5.6.14. Since $\mathbf{Z}$ is a $G_m$-circulant matrix, Lemma 5.2.10 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

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

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 5.2.10. 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

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

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

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

for all $i, j \in G_m \backslash \{1\}$. The entry $\mathbf{M}_{i,j}$ of $\mathbf{M}$ can be calculated as in the proof of Lemma 5.2.10, therefore we have

$$\mathbf{M}_{i,j} = \frac{1}{|G_m|} \sum_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \chi\left(i \cdot j^{-1}\right).$$

Lemma 5.2.8 *4.)* implies for all $i, j \in G_m \backslash \{1\}$

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

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

**Remark 5.6.16.** *If $(p,q)$ is not an $(\alpha,\beta)$-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$, then more eigenvalues $\lambda_\chi$ are equal to zero, i.e., the matrix $\boldsymbol{D}$ in the proof of Lemma 5.6.15 would not be well defined in this case. Furthermore, the norm of the vectors $\boldsymbol{b}_j^*$ don't necessarily coincide in this case, e.g., $m = 5 \cdot 11$, then $||\boldsymbol{b}_2^*||_2 \approx 0.64$ and $||\boldsymbol{b}_3^*||_2 \approx 0.45$ (Note, indeed $(5,11)$ is not a $(1,1)$-generator prime pair).*

To obtain an upper bound for $||\mathbf{b}_j^*||_2$, we need a lower bound for the eigenvalues $\lambda_\chi$. Unfortunately, the factor $\left|(1-\overline{\chi}(p))(1-\overline{\chi}(q))\right|$, which does not occur in the prime power case, can get very small if the character is of conductor $p^\alpha$ or $q^\beta$. We know, that $\chi(p)$ is a $\varphi\left(q^l\right)$-th root of unity for some $1 \leq l \leq \beta$. Analog holds for $\chi(q)$. Hence, to give an upper bound for $||\mathbf{b}_j^*||_2$, we have to bound the sum over the squares of the inverse of the distances between these roots of unity and 1, see Figure 5.7.

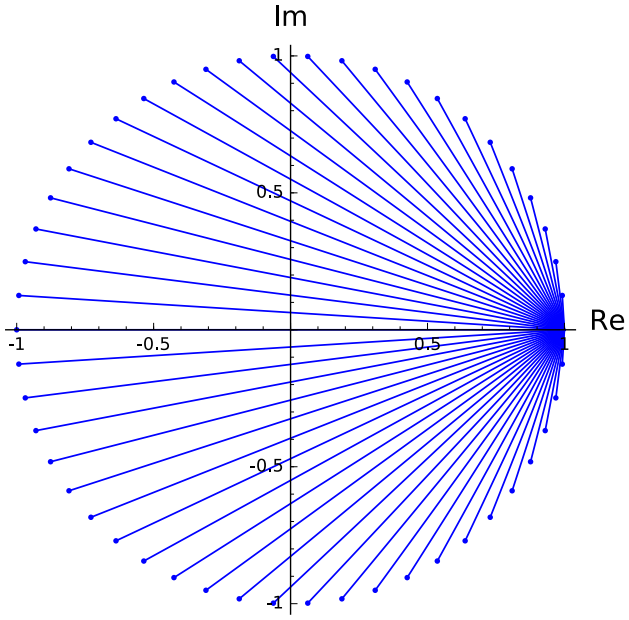



**Figure 5.7:** The distances between the 50-th roots of unity and 1

**Lemma 5.6.17.** *Let $n \in \mathbb{N}$. Then*

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

*Proof.* We will prove this by splitting the sum into the sum over the points $\xi_n^k$ with $\Re\left(\xi_n^k\right) \leq 0$, which yields $|1-\xi_n^k| \geq 1$, and the sum over the points $\xi_n^k$ with $\Re\left(\xi_n^k\right) > 0$, see Figure 5.7. The following holds.

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

For all $x \in (0,2]$ the inequality $\cos(x) < 1-\frac{x^2}{2}+\frac{x^4}{24}$ holds, see for example [Kön04, Section 8.7, Einschließungslemma]. Since $\frac{2\pi}{n}k \in (0,2)$ for $k = 1,\ldots,\left\lfloor\frac{n-1}{4}\right\rfloor$ (if $n \leq 4$, the following sum is empty, hence equals zero), we have

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

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 $\zeta$, see for example [Kön04, Section 15.4]. □

The following theorem summarizes the presented results and provides an upper bound for $||\mathbf{b}_j^*||_2$.

**Theorem 5.6.18.** *Let $(p,q)$ be an $(\alpha,\beta)$-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 universal constant $C > 0$ (i.e., $C$ 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

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

with $l(m) := C \log(\log(m)) \geq C \log(\log(f_\chi))$ for some constant $C > 0$ by Theorem 5.3.5 (we take the sum over all non trivial characters, therefore $3 \leq f_\chi | m$ holds for each of these characters $\chi$), Lemma 5.6.15 and Theorem 5.6.14. 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 are exactly two elements $h$ in $\mathbb{Z}_{p^\alpha}^\times$ with $h^2 = 1$, namely 1 and $g^{\frac{\varphi(p^\alpha)}{2}} \in \mathbb{Z}_{p^\alpha}^\times$, where $g$ is some generator of $\mathbb{Z}_{p^\alpha}^\times$. The isomorphism $\mathbb{Z}_{p^\alpha}^\times \cong \widehat{\mathbb{Z}_{p^\alpha}^\times}$ in Lemma 5.2.3 yields that there is exactly one non trivial quadratic character of $\mathbb{Z}_{p^\alpha}^\times$. We claim that the conductor of this quadratic character is $p$. Let $\Psi$ be the non trivial quadric character of $\mathbb{Z}_p^\times$, then $\Psi$ 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 $q$. By Lemma 5.2.4 we have $\widehat{\mathbb{Z}_m^\times} = \widehat{\mathbb{Z}_{p^\alpha}^\times} \times \widehat{\mathbb{Z}_{q^\beta}^\times}$, hence 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 $C_1 > 0$, such that

$$\sum_{\substack{\chi \in \widehat{G_{p^{l_1} q^{l_2}}} \backslash \{1\} \\ \chi \text{ is quadratic}}} |\lambda_\chi|^{-2} \leq C_1$$

for all $l_1, l_2 \in \mathbb{N}$, since the bound of the eigenvalues $\lambda_\chi$ only depends on the conductor $f_\chi$ by Theorem 5.6.14 and Theorem 5.3.3. This implies

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

with $l(m) := C_2 \log(m) \geq C_2 \log(f_\chi)$ for some constant $C_2 > 0$ by Theorem 5.3.3. 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 $\left|(1-\overline{\chi}(p))(1-\overline{\chi}(q))\right| = 1$, therefore

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

where we used that there at most $|\widehat{G_t}| = \frac{\varphi(t)}{2} \leq \frac{t}{2}$ characters of conductor $t$ in $\widehat{G_m}$.
If $q \nmid f_\chi = p^e$ for some $1 \leq e \leq \alpha$, 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 $(\alpha,\beta)$-generator prime pair, it follows $\gcd\left(a, \frac{\varphi(p^e)}{2}\right) = 1$ for every $1 \leq e \leq \alpha$. Therefore, by Corollary 5.5.4 it holds

$$
\begin{aligned}
\sum_{\substack{\chi \in \widehat{G_m} \\ 1 < f_\chi | p^\alpha}} \frac{1}{\left|(1-\overline{\chi}(p))(1-\overline{\chi}(q))\right|^2 \cdot f_\chi} &= \sum_{\substack{\chi \in \widehat{G_m} \\ 1 < f_\chi | p^\alpha}} \frac{1}{\left|1-\overline{\chi}(q)\right|^2 \cdot f_\chi} \\
&\leq \sum_{e=1}^{\alpha} \frac{1}{p^e} \sum_{\substack{\chi \in \widehat{G_{p^e}} \\ \chi \neq 1}} \frac{1}{\left|1-\overline{\chi}(q)\right|^2} \\
&= \sum_{e=1}^{\alpha} \frac{1}{p^e} \sum_{k=1}^{\frac{\varphi(p^e)}{2}-1} \frac{1}{\left|1-\xi_{\frac{\varphi(p^e)}{2}}^k\right|^2} \\
&\underset{(1)}{\leq} \sum_{e=1}^{\alpha} \frac{1}{p^e} \cdot \left(1 + \frac{\varphi(p^e)}{8} + \frac{\varphi(p^e)^2}{36}\right) \\
&= \sum_{e=1}^{\alpha} \frac{1}{p^e} + \frac{p-1}{8p} + \frac{(p-1)^2 p^{e-2}}{36} \\
&\leq \frac{\alpha}{p} + \frac{\alpha}{8} + \alpha p^{\alpha-2} \frac{(p-1)^2}{36},
\end{aligned}
$$

where (1) follows from Lemma 5.6.17. Analogously follows

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

Altogether we have

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

where $l(m)$ is either $l(m)=C_3\log(\log(m))$ under the *GRH* or $l(m)=C_2\log(m)$ without the *GRH* for some constants $C_3,C_2>0$ (we choose $\max\{C_1,C_2,C_3\}$ for the constant $C$ in the theorem). 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 $\frac{15C_1}{m}$ 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, if $(p,q)$ is a generator prime pair and the distance between $\alpha$ and $\beta$ is not too big.

**Corollary 5.6.19.** *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*

$$||\boldsymbol{b}_j^*||_2^2\to 0 \text{ for } l\to\infty$$

*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 3.4.5 holds with parameter $\omega$ 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 5.6.18 implies

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

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

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

for some constant $C' > 0$.
Hence, Condition 3.4.5 holds with parameter $\omega > 0$ for large enough $l$, since the probability of

$$\left|\langle \mathrm{Log}(g), \mathbf{v}_i \rangle\right| \geq \frac{1}{2||\mathbf{b}_j^*||_2} \quad \text{for some } i = 1, ..., k$$

for all $\mathbf{v}_1, ..., \mathbf{v}_k \in \mathbb{R}^{\frac{\varphi(m_l)}{2}}$, which have euclidean norm 1 and are orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^{\frac{\varphi(m_l)}{2}}$, is bounded by $m_l \cdot \exp\left(-\frac{1}{8||\mathbf{b}_j^*||_2}\right)$ for large enough $m_l$ by Theorem 3.5.4. □

## 5.7 Algorithmic Implications

We summarize all presented results. Our goal was to extend the algorithm presented in [CDPR16], which recovers a shortest generator of some principle fractional ideal in quantum polynomial time in $m$ by Theorem 3.4.9 (under some hypothesis concerning $h_m^+$), in the case of cyclotomic fields $K_m = \mathbb{Q}(\xi_m)$ for some prime power $m$. For this, we have investigated the group $\mathscr{S}_m$ generated by the roots of unity and the elements

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

for $j \in \mathbb{Z}_m^\times$, if $m$ has two distinct, odd prime factors. In this case, we have presented a criterion to determine when $[\mathscr{O}_m^\times : \mathscr{S}_m] = 2h_m^+\beta_m \neq 0$ holds if $m = p^\alpha q^\beta$, which is the case iff $(p, q)$ is an $(\alpha, \beta)$-generator prime pair. Moreover, we have proven that the factor $\beta_m$ is bounded by $\frac{m}{4}$ in this case. As mentioned in Remark 5.6.8, if the class number $h_m^+$ is bounded by some polynomial in $m$, at least for fixed $(p, q)$, Algorithm 3.3 can be executed in quantum polynomial running time in $m$ by Theorem 3.4.9.
To guarantee that Algorithm 3.3 outputs a short generator with non negligible probability $\omega \in (0, 1)$, we need Condition 3.4.5 to be satisfied with parameter $\omega$. We have proven that this condition is satisfied for all $\omega \in (0, 1)$ for large enough $m = p^\alpha q^\beta$, if the distance of $\alpha$ and $\beta$ is not too big, see Corollary 5.6.19.

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

We want to remark that our techniques used in this chapter can not be extended for numbers $m \in \mathbb{N}$ with arbitrary many prime factors. In particular, [Was96, Exercise 8.8.] states that if $m \not\equiv 2 \mod 4$ has at least four distinct prime factors, then the index of the subgroup $\mathscr{S}_m$ is infinite, i.e., the factor $\beta_m$ is zero.

## 5.8 Generalized Cyclotomic Units

For arbitrary $m \in \mathbb{N}$, there is known some basis of a subgroup of $\mathscr{O}_m^\times$ with finite index. These are studied in [JdR16, Section 6.2] and [Was96, Theorem 8.3.]. Unfortunately, the index of this subgroup is growing too fast with $m$, which is sketched in this section.
Notice, again we exclude w.l.o.g. the case $m \equiv 2 \mod 4$ for the cyclotomic field $\mathbb{Q}(\xi_m)$, but indicate when needed.

**Lemma 5.8.1.** *Let $m \in \mathbb{N}$ with $m \geq 3$. Furthermore, let $d \in \mathbb{N}$ with $d|m$ and $1 < d$. Then*

$$\frac{\xi_d^j - 1}{\xi_d - 1}$$

*is a unit in $\mathscr{O}_m^\times$ for all $j \in \mathbb{Z}_m^\times$.*

*Proof.* This follows from Lemma 4.3.2 together with the fact that $\gcd(j,m)=1$ implies $\gcd(j,d)=1$ and $\mathcal{O}_d^\times \subseteq \mathcal{O}_m^\times$. □

Now we define the *generalized cyclotomic units* as products of these units based on different orders.

**Definition 5.8.2** (Basis of the generalized cyclotomic units)**.** *Let $m \in \mathbb{N}$ with $m \geq 3$. Further, let $D_m := \{d \in \mathbb{N} |\ d|m,\ d>1$ and $\gcd(d, \frac{m}{d})=1\}$. For $j \in \mathbb{Z}_m^\times$ we define*

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

*and*

$$\boldsymbol{b}_j := Log_r(b_j) \in \mathbb{R}^{n/2},$$

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

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

Notice that $b_{-j} = \xi_m^a \cdot b_j$ holds for some $a \in \mathbb{Z}_m$, hence it is sufficient to consider a set of representatives of $\{b_j |\ j \in G\backslash\{1\}\}$ as generators of $\mathcal{G}_m$. If $m$ is a prime power, the units $b_j \in \mathcal{O}_m^\times$ are the same as in Lemma 4.3.3, since $D_{p^l} = \{p^l\}$ for all $p \in \mathbb{P}$ and $l \in \mathbb{N}$.

**Theorem 5.8.3** ([JdR16, Theorem 6.2.2])**.** *Let $m \in \mathbb{N}$ with $m \not\equiv 2 \mod 4$ and $m \geq 3$. Then*

$$\left\{ b_j \middle|\ 1<j<\frac{m}{2},\ \gcd(j,m)=1 \right\}$$

*is a basis of a free abelian subgroup of finite index in $\mathcal{O}_m^\times$. In particular, $\mathcal{G}_m$ is of finite index in $\mathcal{O}_m^\times$.*

For simplification we write $\mathbf{B}$ for the matrix whose columns are the vectors $\mathbf{b}_j$ (remember $n=\varphi(m)$).

**Theorem 5.8.4** ([Was96, Theorem 8.3.])**.** *Let $m \in \mathbb{N}$ with $m \geq 3$ and $m \not\equiv 2 \mod 4$. Then the index of $\mathcal{G}_m^+$ in $(\mathcal{O}_m^+)^\times$ 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 $K_m^+ = \mathbb{Q}(\xi_m)^+$.*

**Corollary 5.8.5.** *Let $m \in \mathbb{N}$ with $m \geq 3$ and $m \not\equiv 2 \mod 4$. Then*

$$[\mathcal{O}_m^\times : \mathcal{G}_m] \geq h_m^+ \prod_{\substack{p|m \\ p \in \mathbb{P}}} \left( \varphi(p^{e_p})^{\frac{\varphi\left(\frac{m}{p^{e_p}}\right)}{2}-1} \right).$$

*Proof.* It holds

$$\begin{aligned}
[\mathcal{O}_m^\times : \mathcal{G}_m] &\geq [(\mathcal{O}_m^+)^\times : \mathcal{G}_m^+] \\
&= h_m^+ \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p \mid m \\ p \nmid f_\chi \\ p \in \mathbb{P}}} (\varphi(p^{e_p}) + 1 - \chi(p)) \\
&\geq h_m^+ \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p \mid m \\ p \nmid f_\chi \\ p \in \mathbb{P}}} \varphi(p^{e_p}) \\
&= h_m^+ \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \prod_{\substack{\chi \in \widehat{G_{\frac{m}{p^{e_p}}}} \\ \chi \neq 1}} \varphi(p^{e_p}) \\
&= h_m^+ \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \left( \varphi(p^{e_p})^{\frac{\varphi\left(\frac{m}{p^{e_p}}\right)}{2} - 1} \right),
\end{aligned}$$

where the first inequality follows from Corollary 4.2.7 and the last equality follows from $|\widehat{G_k}| = \frac{\varphi(k)}{2}$ for all $k \in \mathbb{N}$ with $k \geq 3$. □

Corollary 5.8.5 states that the index of the generalized cyclotomic units is growing too fast with $m$, if $m$ is not a prime power. Figure 5.8 shows the factor

$$\beta'_m := \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{p \mid m \\ p \nmid f_\chi \\ p \in \mathbb{P}}} (\varphi(p^{e_p}) + 1 - \chi(p))$$

for $m \leq 600$, whereby the factor is equal 1 iff $m$ is a prime power. Hence, these generalized cyclotomic units are useless for our purpose.

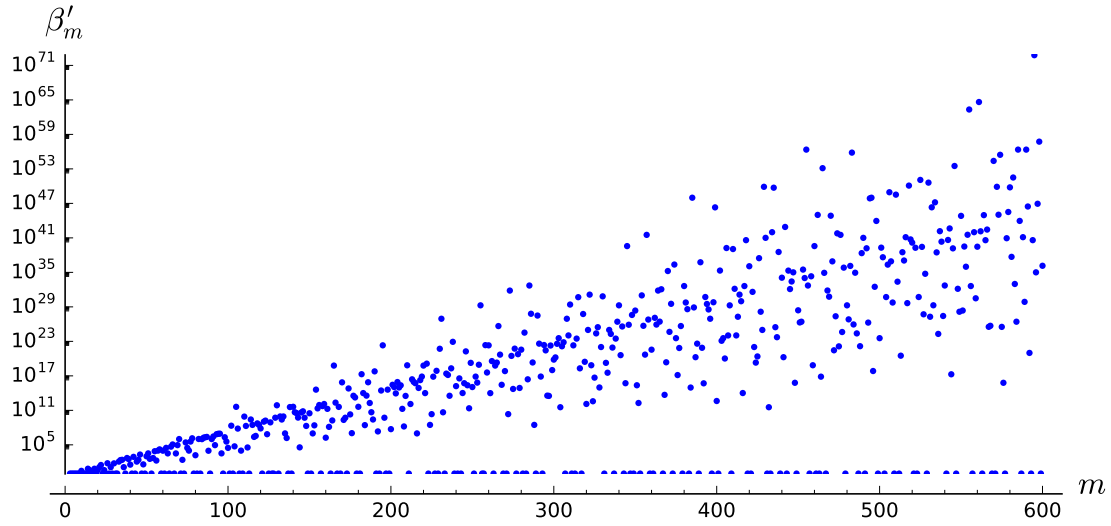



**Figure 5.8:** The factor $\beta'_m$

# 6 Ideal-SVP

## 6.1 Overview

In this chapter we argue that there exists a quantum algorithm which efficiently solves the approximate ideal shortest vector problem for cyclotomic fields $\mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$ for some $(\alpha, \beta)$-generator prime pair $(p, q)$ and approximation factor $\exp\left(\tilde{O}(\sqrt{n})\right)$. Our argumentation is based on the case of prime power conductors discussed in [CDPR16, Chapter 6] for principal ideals and [CDW16] for general ideals in $K_m$.

## 6.2 Foundations

Many cryptographic schemes rely on the hardness of finding short vectors in ideals of algebraic number fields $K$. As we have seen, given a generator $g \in K_m^\times$ of some principal fractional ideal $I = g\mathcal{O}_K$, we can compute a generator $g' \in K_m$ of $I$ with minimal norm in the logarithmic embedding with non negligible probability in quantum polynomial time, if $m$ is a prime power or is a product of two suitable prime powers. This was studied in the previous chapters.
Now we are interested in finding short vectors in arbitrary ideals, but with minimal norm in the Minkowsky embedding.

**Definition 6.2.1** (Minkowsky embedding)**.** *Let $K$ be an algebraic number field and $\sigma_1, ..., \sigma_n : K \to \mathbb{C}$ its embeddings into $\mathbb{C}$. The **Minkowsky embedding** is the injective group homomorphism*

$$\begin{aligned} j : K &\to \mathbb{C}^n \\ \alpha &\mapsto (\sigma_1(\alpha), ..., \sigma_n(\alpha)) . \end{aligned}$$

*This induces a norm on $K$, namely*

$$||\alpha||_K := ||j(\alpha)||_2$$

*for all $\alpha \in K$.*

**Proposition 6.2.2** ([NS99, (5.2) Proposition])**.** *Let $K$ be an algebraic number field and $n = [K : \mathbb{Q}]$. If $\mathfrak{a} \neq 0$ is an ideal in $\mathcal{O}_K$, then $\Gamma = j(\mathfrak{a})$ is an ideal in $\mathbb{C}^n$ of dimension $n$. In particular, $j(\mathfrak{a})$ is a discrete subset of $\mathbb{C}^n \cong \mathbb{R}^{2n}$ by Theorem 2.3.3.*
*Note that this statement remains true for fractional ideals in $K$, since for each fractional ideal $\mathfrak{a}$ in $K$ there exists some $c \in \mathcal{O}_K \backslash \{0\}$ such that $c \cdot \mathfrak{a}$ is an ideal in $K$, see [NS99, (3.7) Definition].*

We study the following problem.

**Problem 6.2.3** (Approximate-Ideal-SVP)**.** *Given an algebraic number field $K$, an integral ideal $\mathfrak{a}$ in $K$ and $C \geq 1$, find an element $g \in \mathfrak{a} \backslash \{0\}$ such that $||g||_K \leq C \cdot \min_{a \in \mathfrak{a} \backslash \{0\}} ||a||_K = C \cdot \lambda_1(j(\mathfrak{a}))$. Such an element $g$ is called a solution of the $C$-**approximate ideal shortest vector problem** ($C$-**approximate ideal SVP**).*

To keep the notation simple, we ignore logarithmic factors in the growth rates, since $\log(n) \in O(n^\varepsilon)$ for all $\varepsilon > 0$. Therefore, we use the following notation.

**Definition 6.2.4** (Bachmann-Landau Notation)**.** *Let $g : \mathbb{N} \to \mathbb{R}_{\geq 0}$ be a function. We define*

$$\tilde{O}(g) := \left\{ f : \mathbb{N} \to \mathbb{R}_{\geq 0} |\ f \in O\left(g(n) \cdot \log^k(n)\right) \text{ for some } k > 0 \right\} .$$

The approximate ideal SVP for the case that $K$ is a cyclotomic fields $\mathbb{Q}(\xi_m)$ with prime power conductor $m$ is studied in [CDW16]. They present an algorithm which runs in quantum polynomial time in $m$ for an approximation factor $C = \exp\left(\tilde{O}(\sqrt{n})\right)$, where $n = \varphi(m)$. We extend their results to cyclotomic fields with prime power conductors to the case that $m = p^\alpha q^\beta$ for some generator prime pair $(p, q)$.
To solve the $C$-approximate ideal SVP, we split it into the following two problems.

1. Solve the **close principal multiple problem** (**CPM**), i.e., find an integral ideal $\mathfrak{b}$, such that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ is a close *principal* multiple of $\mathfrak{a}$ with $N(\mathfrak{b}) \leq \exp\left(\tilde{O}(n^{1+c})\right)$ for some constant $c > 0$.

2. Given a principal ideal $\mathfrak{c}$, find a generator $g \in \mathcal{O}_K$ of $\mathfrak{c}$ with $||g||_K \leq (N(\mathfrak{c}))^{1/n} \cdot \exp\left(\tilde{O}(n^{1/2})\right)$.

If one can solve the upper two problems in quantum polynomial time in $m$ for cyclotomic fields of conductor $m$, one has efficiently found a solution $g \in \mathfrak{a}\backslash\{0\}$ of the $\exp\left(\tilde{O}\left(n^{\max\{1/2,c\}}\right)\right)$-approximate ideal SVP, since

$$\begin{aligned} ||g||_K &\leq (N(\mathfrak{c}))^{1/n} \cdot \exp\left(\tilde{O}(n^{1/2})\right) \\ &\leq (N(\mathfrak{a}))^{1/n} \cdot (N(\mathfrak{b}))^{1/n} \cdot \exp\left(\tilde{O}(n^{1/2})\right) \\ &\leq (N(\mathfrak{a}))^{1/n} \cdot \exp\left(\tilde{O}\left(n^{\max\{1/2,c\}}\right)\right) \\ &\leq \exp\left(\tilde{O}\left(n^{\max\{1/2,c\}}\right)\right) \cdot \lambda_1(j(\mathfrak{a})), \end{aligned}$$

where we have used in the last inequality that $N(\mathfrak{a})^{1/n} \leq p(n) \cdot \lambda_1(j(\mathfrak{a}))$ holds for some polynomial $p$, as mentioned in [CDW16, 2.1.1. Ideals as lattices]. They also state that it is plausible that the constant $c$ can be chosen as $c = \frac{1}{2}$ for a dense family of conductors $m$, in which case we have found a solution to the $\exp\left(\tilde{O}(\sqrt{n})\right)$ -approximation ideal SVP, see [CDW16, 2.2.5. Sufficient conditions].

## 6.3 The Principal Ideal Case

One may ask, if there is a connection between the problem of recovering short generators in the logarithmic embedding and the approximate ideal SVP in the Minkowsky embedding. Indeed, we can use the results from previous chapters to obtain a solution to the approximate ideal SVP. It is plausible that the approximation factor of a shortest generator as a solution of the approximate ideal SVP is exponential, since the computed generator of the principal ideal is short in the *logarithmic* embedding, but now we are searching for short vectors in $j(\mathfrak{c})$ in the *non logarithmic* Minkowsky embedding.
The approximate ideal SVP for principal ideals in cyclotomic fields $\mathbb{Q}(\xi_m)$ of prime conductor $m$ is studied in [CDPR16, Section 6.]. Again, our argumentation is nearly the same as in the prime power case to obtain the same results for $m = p^\alpha q^\beta$, where $(p, q)$ is some $(\alpha, \beta)$-generator prime pair, since the finiteness of the index $[\mathcal{O}_m^\times : \mathcal{S}_m]$ and Lemma 3.4.10 imply, that $[\mathrm{Log}_r(\mathcal{O}_m^\times) : \mathrm{Log}_r(\mathcal{S}_m)] = [\mathrm{Log}_r(\mathcal{O}_m^\times) : \mathcal{L}(\mathbf{B})]$ is finite and hence $\mathrm{span}(\mathrm{Log}_r(\mathcal{O}_m^\times)) = \mathrm{span}(\mathrm{Log}_r(\mathcal{S}_m)) \subseteq \mathbb{R}^{n/2}$ is the space orthogonal to the all-one vector $\mathbf{1} \in \mathbb{R}^{n/2}$.

**Definition 6.3.1** (Covering radius)**.** *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice. The **covering radius** of $\mathcal{L}$ is defined as*

$$\mu^{(\infty)}(\mathcal{L}) := \max_{\boldsymbol{x} \in span(\mathcal{L})} \min_{\boldsymbol{y} \in \mathcal{L}} ||\boldsymbol{x} - \boldsymbol{y}||_\infty = \max_{\boldsymbol{x} \in span(\mathcal{L})} \min_{\boldsymbol{v} \in \boldsymbol{x} + \mathcal{L}} ||\boldsymbol{v}||_\infty.$$

The covering radius of a lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is the maximal distance a point $\mathbf{x} \in \mathrm{span}(\mathcal{L})$ can have to $\mathcal{L}$.

**Definition 6.3.2.** *We denote the subspace of $\mathbb{R}^n$ orthogonal to the all-one vector $\boldsymbol{1} \in \mathbb{R}^n$ by $H_n \subseteq \mathbb{R}^n$. For some vector $\boldsymbol{g} \in \mathbb{R}^n$ we write $\boldsymbol{g} = s_{\boldsymbol{g}}\boldsymbol{1} + \boldsymbol{g}_H$ with $\boldsymbol{g}_H \in H_n$ and $s_{\boldsymbol{g}} \in \mathbb{R}$.*

**Lemma 6.3.3.** *Let $K_m = \mathbb{Q}(\xi_m)$ be a cyclotomic field of conductor $m \in \mathbb{N}$ with $m \geq 3$. Further, let $g \in \mathcal{O}_m\backslash\{0\}$, $\mathfrak{c} := g\mathcal{O}_m$ and $\boldsymbol{g} := Log_r(g) = s_{\boldsymbol{g}}\boldsymbol{1} + \boldsymbol{g}_H \in \mathbb{R}^{n/2}$ with $\boldsymbol{g}_H \in H_{n/2}$ and $s_{\boldsymbol{g}} \in \mathbb{R}$, where $n = \varphi(m)$. Then it holds*

$$s_{\boldsymbol{g}} = \frac{1}{\varphi(m)} \log(N(\mathfrak{c})) \geq 0.$$

*Proof.* It holds

$$\begin{aligned} N(\mathfrak{c}) = N_{K_m/\mathbb{Q}}(g) = \prod_{j\in\mathbb{Z}_m^\times} \sigma_j(g) &= \prod_{j\in G_m} \sigma_j(g)\cdot\overline{\sigma_j}(g) \\ &= \prod_{j\in G_m} |\sigma_j(g)|^2 \\ &= \prod_{j\in G_m} \exp\big(2\log\big(|\sigma_j(g)|\big)\big) \\ &= \exp\left(2\sum_{j\in G_m} \log\big(|\sigma_j(g)|\big)\right) \\ &= \exp\big(2\langle \mathbf{g}, \mathbf{1}\rangle\big) = \exp\big(s_{\mathbf{g}}\cdot\varphi(m)\big). \end{aligned}$$

This implies $s_{\mathbf{g}} = \frac{1}{\varphi(m)}\log(N(\mathfrak{c}))$. Since $N(\mathfrak{c})\in\mathbb{N}$, this yields $s_{\mathbf{g}}\geq 0$. □

The following Algorithm 6.1 based on [CDPR16, Lemma 6.1] is very similar to Algorithm 3.2 and outputs a generator $h\in\mathcal{O}_m$ of $\mathfrak{c} = g\mathcal{O}_m$ with small norm depending on the input $\mathbf{h}_H \in \mathbf{g}_H + \mathrm{Log}_r(\mathcal{S}_m)$.

**Algorithm 6.1:** Approximate ideal SVP with input $\mathbf{h}_H$

1 **Input:** $K_m = \mathbb{Q}(\xi_m)$, a generator $g\in\mathcal{O}_m\backslash\{0\}$ of $\mathfrak{c} = g\mathcal{O}_m$ and $\mathbf{h}_H\in\mathbf{g}_H + \mathrm{Log}_r(\mathcal{S}_m)$.
2 **Output:** A generator $h\in\mathcal{O}_m$ of $\mathfrak{c}$ with $||h||_{K_m} \leq \sqrt{\varphi(m)}\cdot\exp(||\mathbf{h}_H||_\infty)\cdot N(\mathfrak{c})^{1/\varphi(m)}$.
3 $\mathbf{g}\leftarrow \mathrm{Log}_r(g)$
4 $\mathbf{g}_H \leftarrow \mathbf{g} - \frac{2}{\varphi(m)}\langle\mathbf{g},\mathbf{1}\rangle\mathbf{1}$
5 $\mathbf{u}\leftarrow \mathbf{h}_H - \mathbf{g}_H$
6 $(a_1,\ldots,a_k)^T \leftarrow (\mathbf{B}^*)^T\cdot\mathbf{u}$ (The matrix $\mathbf{B}$ is defined in (5.2))
7 $h\leftarrow g\cdot\prod_{i=1}^k b_i^{a_i}$ (the $b_j\in\mathcal{O}_m$ are defined in (5.1))
8 **return** $h$

**Lemma 6.3.4** (Correctness of Algorithm 6.1 and running time)**.** *Let $(p,q)$ be an $(\alpha,\beta)$-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha,\beta\in\mathbb{N}$. Then Algorithm 6.1 has (classical) polynomial running time in $m$ and is correct, i.e., for each input $g\in\mathcal{O}_m\backslash\{0\}$ with $\mathfrak{c} = g\mathcal{O}_m$ and $\boldsymbol{h}_H\in\boldsymbol{g}_H + Log(\mathcal{S}_m)$ it outputs a generator $h\in\mathcal{O}_m$ of $\mathfrak{c}$ with $||h||_{K_m}\leq\sqrt{\varphi(m)}\cdot\exp(||\boldsymbol{h}_H||_\infty)\cdot N(\mathfrak{c})^{1/\varphi(m)}$.*

*Proof.* Since all occurring vectors and matrices are efficiently computable and are of size $m$ or $m\times m$, the polynomial running time is clear. It holds $\mathbf{g} = \mathrm{Log}_r(g) = s_{\mathbf{g}}\mathbf{1} + \mathbf{g}_H$ with $\mathbf{g}_H\in H_n$ and $s_{\mathbf{g}}\in\mathbb{R}$. The correctness follows from

$$\mathbf{h} := \mathrm{Log}_r(h) = \mathrm{Log}_r(g) + \mathbf{B}\cdot(a_1,\ldots,a_k)^T = s_{\mathbf{g}}\mathbf{1} + \mathbf{g}_H + \mathbf{u} = s_{\mathbf{g}}\mathbf{1} + \mathbf{h}_H,$$

which implies

$$\begin{aligned} ||h||_{K_m}^2 = \sum_{j\in\mathbb{Z}_m^\times} |\sigma_j(h)|^2 &\leq \varphi(m)\cdot\max_{j\in\mathbb{Z}_m^\times} \exp\big(\log\big(|\sigma_j(h)|\big)\big)^2 \\ &= \varphi(m)\cdot\exp\left(\max_{j\in\mathbb{Z}_m^\times}\log\big(|\sigma_j(h)|\big)\right)^2 \\ &= \varphi(m)\cdot\exp\big(||\mathbf{h}||_\infty\big)^2 \\ &\leq \varphi(m)\cdot\exp\Big(||\mathbf{h}_H||_\infty + \underbrace{|s_{\mathbf{g}}|}_{\geq 0}\Big)^2 \\ &= \varphi(m)\cdot\exp\big(||\mathbf{h}_H||_\infty\big)^2\cdot\exp\big(s_{\mathbf{g}}\big)^2 \\ &= \varphi(m)\cdot\exp\big(||\mathbf{h}_H||_\infty\big)^2\cdot N(\mathfrak{c})^{2/\varphi(m)}, \end{aligned}$$

where we have used Lemma 6.3.3.
We have used that the matrix $\mathbf{B}$ has rank $k$ in line 6 by using the dual matrix $\mathbf{B}^*$, which is the case if $m = p^\alpha q^\beta$ for some $(\alpha, \beta)$-generator prime pair $(p, q)$. □

**Corollary 6.3.5.** *Let $(p,q)$ be an $(\alpha,\beta)$-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$. For each principal ideal $\mathfrak{c} \neq \{0\}$ in $\mathcal{O}_m$ there exists a generator $h \in \mathcal{O}_m$ with*

$$||h||_K \leq \sqrt{\varphi(m)} \cdot \exp\left(\mu^{(\infty)}(Log(\mathcal{S}_m))\right) \cdot N(\mathfrak{c})^{1/\varphi(m)}.$$

*Proof.* Let $\mathbf{x} \in \text{span}(\text{Log}(\mathcal{S}_m))$ and $\mathbf{h}_H \in \mathbf{x} + \text{Log}(\mathcal{S}_m)$ such that $\mu^{(\infty)}(\text{Log}(\mathcal{S}_m)) = ||\mathbf{h}_H||_\infty$. Then Algorithm 6.1 outputs a generator $h \in \mathcal{O}_m$ of $\mathfrak{c}$ with

$$\begin{aligned} ||h||_K &\leq \sqrt{\varphi(m)} \cdot \exp\left(||\mathbf{h}_H||_\infty\right) \cdot N(\mathfrak{c})^{1/\varphi(m)} \\ &= \sqrt{\varphi(m)} \cdot \exp\left(\mu^{(\infty)}(\text{Log}(\mathcal{S}_m))\right) \cdot N(\mathfrak{c})^{1/\varphi(m)}. \end{aligned}$$

□

By Corollary 6.3.5, it is sufficient to find a vector $\mathbf{h}_H$ such that $||\mathbf{h}_K||_\infty$ is nearly $\mu^{(\infty)}(\text{Log}(\mathcal{S}_m))$. The following theorem can be proven word by word as in the prime power case for $m = p^\alpha q^\beta$, where $(p,q)$ is some $(\alpha,\beta)$-generator prime pair.

**Theorem 6.3.6** ([CDPR16, Theorem 6.3])**.** *Let $(p,q)$ be an $(\alpha,\beta)$-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$. There is an efficient randomized algorithm (i.e., the running time is polynomial in $m$) that given any vector $\boldsymbol{x} \in H_{n/2}$ outputs a vector $\boldsymbol{v} \in \boldsymbol{x} + Log(\mathcal{S}_m)$ such that $||\boldsymbol{v}||_\infty \in O(\sqrt{m \log(m)})$ with probability $\Omega(1/\sqrt{n})$, where $n = \varphi(m)$.*

The following randomized Algorithm 6.2 solves the $\exp\left(\tilde{O}(\sqrt{n})\right)$-approximation ideal SVP for principal ideals with high probability, namely $\Omega(1/\sqrt{n})$. The success probability can be increased by repeating the algorithm multiple times.

**Algorithm 6.2:** Approximate ideal SVP for principal ideals

1 **Input:** The conductor $m$ of $K_m = \mathbb{Q}(\xi_m)$ and a generator $g \in \mathcal{O}_m \backslash \{0\}$ of $\mathfrak{c} = g\mathcal{O}_m$.
2 **Output:** A generator $h \in \mathcal{O}_m$ of $\mathfrak{c}$ with $||h||_{K_m} \leq \exp(\tilde{O}(\sqrt{m})) \cdot N(\mathfrak{c})^{1/\varphi(m)}$.
3 $\mathbf{g} \leftarrow \text{Log}_r(g)$
4 $\mathbf{g}_H \leftarrow \mathbf{g} - \frac{2}{\varphi(m)} \langle \mathbf{g}, \mathbf{1} \rangle \mathbf{1}$
5 $\mathbf{h}_H \leftarrow$ The vector $\mathbf{v} \in \mathbf{g}_H + \text{Log}(\mathcal{S}_m)$ from Theorem 6.3.6
6 $h \leftarrow$ The output of Algorithm 6.1 with input $m$, $g$ and $\mathbf{h}_H$
7 **return** $h$

**Lemma 6.3.7.** *(Correctness of Algorithm 6.2 and running time) Let $(p,q)$ be an $(\alpha,\beta)$-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$. Then Algorithm 6.2 has (classical) polynomial running time in $m$ and is correct, i.e., for each input $g \in \mathcal{O}_m \backslash \{0\}$ with $\mathfrak{c} = g\mathcal{O}_m$ it outputs a generator $h \in \mathcal{O}_m$ of $\mathfrak{c}$ with $||h||_{K_m} \leq \sqrt{\varphi(m)} \cdot \exp(O(\sqrt{m \cdot \log(m)})) \cdot N(\mathfrak{c})^{1/\varphi(m)} = \exp(\tilde{O}(\sqrt{m})) \cdot N(\mathfrak{c})^{1/\varphi(m)}$ with high probability.*

*Proof.* Again, the polynomial running time in $m$ is clear, since all occurring instances have size $m$. By Theorem 6.3.6, the vector $\mathbf{h}_H$ satisfies $\mathbf{h}_H \in O(\sqrt{m \cdot \log(m)})$ with high probability. Now the correctness of Algorithm 6.1 implies the correctness of Algorithm 6.2, if $\mathbf{h}_H \in O(\sqrt{m \cdot \log(m)})$. □

## 6.4 Close Principal Multiple

We sketch the strategy to solve the close principal multiple problem presented in [CDW16].
Let $K$ be a CM-field such that $K/\mathbb{Q}$ is a Galois extension, $n = [K : \mathbb{Q}]$ and $G := \mathrm{Gal}(K/\mathbb{Q})$ through this section. The Galois group $G$ acts on the set of fractional ideals $\mathscr{I}_K$ in $K$ via

$$\mathfrak{a}^\sigma := \sigma(\mathfrak{a})$$

for all $\mathfrak{a} \in \mathscr{I}_K$ and $\sigma \in G$. This can be extended to a group action of the group ring $\mathbb{Z}[G]$ on $\mathscr{I}_K$, where $\mathbb{Z}[G]$ is the set of all formal sums over $\mathbb{Z}$ and $G$, i.e.,

$$\mathbb{Z}[G] := \left\{ \sum_{\sigma \in G} s_\sigma \sigma \,\middle|\, s_\sigma \in \mathbb{Z} \text{ for all } \sigma \in G \right\}$$

equipped with the common addition and multiplication. An element $s = \sum_{\sigma \in G} s_\sigma \sigma \in \mathbb{Z}[G]$ acts on $\mathfrak{a} \in \mathscr{I}_K$ via

$$\mathfrak{a}^s := \prod_{\sigma \in G} \sigma(\mathfrak{a})^{s_\sigma}.$$

The **relative class group** $\mathrm{Cl}_K^-$ of $K$ is defined as the kernel of the surjective **relative norm map**

$$\begin{aligned} N_{K/K^+} : \mathrm{Cl}_K &\to \mathrm{Cl}_{K^+} \\ [\mathfrak{a}] &\mapsto [\mathfrak{a}\mathfrak{a}^\tau], \end{aligned}$$

where $\tau \in G$ is the automorphism on $K$ induced by the complex conjugation. In particular we obtain

$$\mathrm{Cl}_{K^+} \cong {}^{\mathrm{Cl}_K}\!/_{\mathrm{Cl}_K^-}.$$

To sketch the algorithm for solving the close principal multiple problem, we start with some simplification. We assume for a moment that we have found a **prime factor base** of the form $\mathfrak{B} = \{\mathfrak{p}^\sigma | \sigma \in G\}$ whose ideal classes generates $\mathrm{Cl}_K$, where $\mathfrak{p} \in \mathscr{I}_K$ is some prime ideal, such that the norm $N(\mathfrak{p})$ is bounded by some polynomial $P(n)$ in $n$. In this case, the map

$$\begin{aligned} \Psi : \mathbb{Z}^{\mathfrak{B}} &\to \mathrm{Cl}_K \\ \left(e_\mathfrak{q}\right)_{\mathfrak{q} \in \mathfrak{B}} &\mapsto \prod_{\mathfrak{q} \in \mathfrak{B}} [\mathfrak{q}]^{e_\mathfrak{q}} \end{aligned}$$

is a surjective homomorphism, hence $\Lambda := \ker(\Psi) = \left\{ \left(e_\mathfrak{q}\right)_{\mathfrak{q} \in \mathfrak{B}} \,\middle|\, \left[\prod_{\mathfrak{q} \in \mathfrak{B}} \mathfrak{q}^{e_\mathfrak{q}}\right] = [\mathscr{O}_K] \right\}$ is a subgroup of $\mathbb{Z}^{\mathfrak{B}}$ and therefore a lattice with

$$\mathrm{Cl}_K \cong {}^{\mathbb{Z}^{\mathfrak{B}}}\!/_{\Lambda}.$$

Now we are able to rephrase the close principal multiple problem as a close vector problem. As proven in [CDW16, Proposition 3.1], there is a quantum algorithm that computes a vector $\mathbf{e} = \left(e_\mathfrak{q}\right)_{\mathfrak{q} \in \mathfrak{B}} \in \mathbb{Z}^{\mathfrak{B}}$ such that $\mathfrak{a} = \prod_{\mathfrak{q} \in \mathfrak{B}} \mathfrak{q}^{e_\mathfrak{q}}$ which has polynomial running time in $n$, $\max_{\mathfrak{q} \in \mathfrak{B}} \log(N(\mathfrak{q}))$, $\log(N(\mathfrak{a}))$ and $|\mathfrak{B}|$. If we can find a sufficiently close vector $\mathbf{v} = \left(v_\mathfrak{q}\right)_{\mathfrak{q} \in \mathfrak{B}} \in \Lambda$ to $\mathbf{e}$ in the $||\cdot||_1$-norm, we have found a sufficiently small fractional ideal

$$\mathfrak{b} := \prod_{\mathfrak{q} \in \mathfrak{B}} \mathfrak{q}^{v_\mathfrak{q} - e_\mathfrak{q}}$$

such that

$$[\mathfrak{a}\mathfrak{b}] = \left[\prod_{\mathfrak{q}\in\mathfrak{B}} \mathfrak{q}^{e_\mathfrak{q}}\right] \cdot \left[\prod_{\mathfrak{q}\in\mathfrak{B}} \mathfrak{q}^{v_\mathfrak{q}-e_\mathfrak{q}}\right] = \left[\prod_{\mathfrak{q}\in\mathfrak{B}} \mathfrak{q}^{v_\mathfrak{q}}\right] = [\mathcal{O}_K]$$

and

$$N(\mathfrak{b}) \leq P(n)^{||\mathbf{v}-\mathbf{e}||_1}.$$

As we have seen, we can shift the close principal multiple problem to a close vector problem. However, this is hard to solve in general, but in this case the structure of $\Lambda$ is well suited, i.e., we can find a good basis of $\Lambda$ (or more precisely, a basis of a full rank sublattice) to solve this close vector problem with a good enough approximation factor, if $K = \mathbb{Q}(\xi_m)$ is a cyclotomic field.
For the rest of this section, let $K = K_m$ be the cyclotomic field $\mathbb{Q}(\xi_m)$ of conductor $m \in \mathbb{N}$ with $m \geq 3$.

**Definition 6.4.1** ([CDW16, Definition 5.1.]). *The **Stickelberger** element $\theta \in \mathbb{Q}[G]$ is defined as*

$$\theta := \sum_{a\in\mathbb{Z}_m^\times} \left(\frac{a}{m} \mod 1\right)\sigma_a^{-1}.$$

*The **Stickelberger ideal** $S$ is defined as*

$$S := \mathbb{Z}[G] \cap \theta\mathbb{Z}[G].$$

**Theorem 6.4.2** ([Was96, Theorem 6.10.]). *The Stickelberger ideal $S$ annihilates the ideal class group $Cl_{K_m}$ of $K_m$, i.e., for any ideal $\mathfrak{a}$ in $\mathcal{O}_m$ and any $s \in S$,*

$$[\mathfrak{a}^s] = [\mathcal{O}_m].$$

We identify the Stickelberger ideal $S$ as a sublattice of $\mathbb{Z}^\mathfrak{B}$ via the $\mathbb{Z}$-module isomorphism

$$\begin{aligned}\Upsilon : \mathbb{Z}[G] &\to \mathbb{Z}^\mathfrak{B}\\ \sum_{\sigma\in G} e_\sigma\sigma &\mapsto (e_\sigma)_{\mathfrak{p}^\sigma\in\mathfrak{B}}.\end{aligned}$$

We set $\Lambda_S := \Upsilon(S) \subseteq \Lambda \subseteq \mathbb{Z}^\mathfrak{B}$. As shown in [CDW16], the lattice $\Lambda_S$ has many short elements which can explicitly be constructed, from which we obtain a solution of the close vector problem in $\mathbb{Z}^\mathfrak{B}$ with approximation factor $||\mathbf{v}-\mathbf{e}||_1 \leq n^{3/2}$. This provides a solution of the close principal multiple problem as desired.
We have made some assumptions, which are too restrictive.

1. We have assumed that there is some small enough prime ideal $\mathfrak{p}$ in $K$ such that the ideal classes of $\mathfrak{B} = \{\mathfrak{p}^\sigma | \sigma \in G\}$ generates $\mathrm{Cl}_K$. In fact, it is sufficient to have such a factor base for the relative class group $\mathrm{Cl}_K^-$, as long as the index of $\mathrm{Cl}_K^-$ in $\mathrm{Cl}_K$, which is $|\mathrm{Cl}_{K^+}| = h_K^+$, is bounded by some polynomial in $n = [K : \mathbb{Q}]$. Note that we have used this assumption right before in the last chapter in Remark 5.6.8 for cyclotomic fields $K_m$.

2. Our assumption, that the factor base consists of one prime ideal $\mathfrak{p}$ in $K$ and its conjugates, i.e., $\mathrm{Cl}_K^-$ is generated by one element as a $\mathbb{Z}[G]$-module, can be weakened by allowing that the factor base consists of a few prime ideals and their conjugates. We need the number of generators to be quite small (for example in $O(n^\epsilon)$ for some small $\epsilon > 0$). That such a factor basis can be found efficiently is discussed in [CDW16, Chapter 7.].

3. The lattice $\Lambda_S$ is not of full rank in $\mathbb{Z}^\mathfrak{B}$ in general. This can be fixed by working in the relative class group $\mathrm{Cl}_K^-$ with the so called augmented Stickelberger ideal $S'$.

## 6.5 Algorithmic Implications

As shown in [CDPR16], one can solve the $\exp\left(\tilde{O}(\sqrt{n})\right)$-approximate shortest vector problem in cyclotomic fields $K_m = \mathbb{Q}(\xi_m)$ of prime power conductor $m$ for principal ideals in quantum polynomial running time in $m$. This result was extended to arbitrary ideals in cyclotomic fields of prime power conductor in [CDW16] under some heuristics ans assumptions.
We have generalized these results to cyclotomic fields of conductor $m = p^\alpha q^\beta$, where $(p,q)$ is some $(\alpha,\beta)$-generator prime pair, since we only used the finiteness of the index of the subgroup $\mathscr{S}_m$ in $\mathscr{O}_m$. Hence, we can efficiently solve the $\exp\left(\tilde{O}(\sqrt{n})\right)$-approximate shortest vector problem in this case for arbitrary ideals in $K_m$, under some mild assumptions, e.g., the polynomial bound of the class number $h_m^+$.

# Bibliography


[Ajt99] Miklós Ajtai. Generating hard instances of the short basis problem. In *International Colloquium on Automata, Languages, and Programming*, pages 1–9. Springer, 1999.

[Bab86] László Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.

[BF14] Jean-François Biasse and Claus Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A):385–403, 2014.

[Bia14] Jean-François Biasse. Subexponential time relations in the class group of large degree number fields. *Adv. in Math. of Comm.*, 8(4):407–425, 2014.

[BPR04] Joe Buhler, Carl Pomerance, and Leanne Robertson. Heuristics for class numbers of prime-power real cyclotomic fields. *Fields Inst. Commun*, 41:149–157, 2004.

[BS15] Jean-François Biasse and Fang 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.

[BS16] Jean-François Biasse and Fang 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.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded 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.

[CDW16] Ronald Cramer, Léo Ducas, and Benjamin 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.

[CGS14] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: A cautionary tale. In *ETSI 2nd Quantum-Safe Crypto Workshop*, pages 1–9, 2014.

[Coh00] Henri Cohen. *A course in computational algebraic number theory*, volume 4. Springer, 2000.

[EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang 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.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–17. Springer, 2013.

[JdR16] Eric Jespers and Ángel del Río. *Orders and Generic Constructions of Units*. Walter de Gruyter GmbH & Co KG, 2016.

[JL04] Chun-Gang Ji and Hong-Wen Lu. Lower bound of real primitive L-function at s= 1. *Acta Arithmetica*, 111:405–409, 2004.

[KB79] Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *siam Journal on Computing*, 8(4):499–507, 1979.

[Kön04] Konrad Königsberger. Analysis 1., Sechste Auflage, 2004.

[Lan27] Edmund Landau. Über Dirichletsche Reihen mit komplexen Charakteren. *Journal für die reine und angewandte Mathematik*, 157:26–32, 1927.

[LLM06] Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio. On bounded distance decoding for general lattices. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 450–461. Springer, 2006.

[LLS15] Youness Lamzouri, Xiannan Li, and Kannan Soundararajan. Conditional bounds for the least quadratic non-residue and related problems. *Mathematics of Computation*, 84(295):2391–2412, 2015.

[Mil14a] John C Miller. Class numbers of real cyclotomic fields of composite conductor. *LMS Journal of Computation and Mathematics*, 17(A):404–417, 2014.

[Mil14b] John C. Miller. Class numbers of totally real fields and applications to the Weber class number problem. *Acta Arithmetica*, 164(4):381–397, 2014.

[Mil15] John Miller. Real cyclotomic fields of prime conductor and their class numbers. *Mathematics of Computation*, 84(295):2459–2469, 2015.

[MV06] Hugh L Montgomery and Robert C Vaughan. *Multiplicative number theory I: Classical theory*, volume 97. Cambridge University Press, 2006.

[NS99] Jürgen Neukirch and Norbert Schappacher. *Algebraic number theory*. Grundlehren der mathematischen Wissenschaften. Springer, Berlin, New York, Barcelona, 1999.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[Sch10] René Schoof. *Catalan's conjecture*. Springer Science & Business Media, 2010.

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[Sie35] Carl Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arithmetica*, 1(1):83–86, 1935.

[SV10] Nigel P Smart and Frederik Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In *International Workshop on Public Key Cryptography*, pages 420–443. Springer, 2010.

[VdL82] FJ Van der Linden. Class number computations of real abelian number fields. *Mathematics of Computation*, 39(160):693–707, 1982.

[Was96] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, Berlin, New York, Barcelona, second edition edition, 1996.

# Appendix

All Code were written for SageMathCloud.

```
m=100
#List of the first m primes
pf=primes_first_n(m)
#List of all odd prime pairs (p,q) with p<q and p,q in pf
primepairs=[[p,q] for p in pf if (p>2) for q in pf if(q>2 and p<q)]
#Compute a list of all generator prime pairs from the list primepairs
generatorprimepairs=[];
for r in primepairs:
#Fix the actual primes p,q
    p=r[0]
    q=r[1]
#h=q-1 mod 4
    h=euler_phi(q)%4
    v2=euler_phi(q^2)
#Compute the order of p mod q^2
    o2=Mod(p,q^2).multiplicative_order()
#If p is a generator or a square of a generator mod q^2,
#go on and test if q is a generator or a square of a generator mod p^2
    if((o2==v2) or (not h==0 and (( 2*o2==v2) or (o2==v2) or (2*o2==v2)))):
        p=r[1]
        q=r[0]
        h=euler_phi(q)%4
        v2=euler_phi(q^2)
        o2=Mod(p,q^2).multiplicative_order()
        if((o2==v2) or (not h==0 and ((2*o2==v2) or (o2==v2) or (2*o2==v2)))):
#If all conditions are satisfied, append the actual prime pair to the GPP list
            generatorprimepairs.append(r)
generatorprimepairs
```

**Listing 6.1:** Computes a list of GPPs

```
#Generator Prime Pairs
m=100
#List of the first m primes
pf=primes_first_n(m)
#Print the largest prime in pf
pf[m-1]
#List of all odd prime pairs (p,q) with p<q and p,q in pf
primepairs=[[p,q] for p in pf if (p>2) for q in pf if(q>2 and p<q)]
#Compute a list of all (1,1)-GPP in primepairs
oogeneratorprimepairs=[];
for r in primepairs:
    p=r[0]
    q=r[1]
    h=(q-1)%4
    v1=q-1
    o1=Mod(p,q).multiplicative_order()
    v2=q*(q-1)
    o2=Mod(p,q^2).multiplicative_order()
    if((h==0 and (o1==v1 and not o2==v2)) or (not h==0 and ((2*o1==v1 or o1==v1) and not
    (2*o2==v2 or o2==v2)))):
        p=r[1]
        q=r[0]
        h=(q-1)%4
        v1=q-1
        o1=Mod(p,q).multiplicative_order()
        v2=q*(q-1)
        o2=Mod(p,q^2).multiplicative_order()
        if((h==0 and (o1==v1 and not o2==v2)) or (not h==0 and ((2*o1==v1 or o1==v1) and
    not (2*o2==v2 or o2==v2)))):
            oogeneratorprimepairs.append(r)
oogeneratorprimepairs
```

**Listing 6.2:** Computes a list of all (1,1)- GPPs

```
#Input: Number m≥3
#Output: The factor β_m
def factorbetam(m):
    primdiv=[p[0] for p in list(factor(m))]
    G = DirichletGroup(m)
    nontrivialcharacter=[X for X in G  if(X.conductor() >1  and X(-1)==1)]
    z=prod(prod(1-X.restrict(X.conductor())(p) for p in primdiv)for  X in
    nontrivialcharacter)
    return z
```

**Listing 6.3:** The index $\beta_m$

```
#Input: Number m≥3
#Output: The factor β'_m
def factorbetams(m):
    G = DirichletGroup(m)
    nontrivialcharacter=[X for X in G if(X.conductor() >1 and X(-1)==1)]
    z=prod(prod((p[0]-1)*p[0]^(p[1]-1)+1-X.restrict(X.conductor())(p[0]) for p in [p for p
     in list(factor(m)) if(not p[0].divides(X.conductor()))])for  X in nontrivialcharacter
    )
    return z
```

**Listing 6.4:** The index $\beta'_m$

```
#First, compute the list of GPPs up to the m-th prime
m=200
pf=primes_first_n(m)
p=pf[m-1]
primepairs=[[p,q] for p in pf if (p>2) for q in pf if(q>2 and p>q)]
#compute a list of GPPs (p,q) with p>q sorted by the value of p (inreasing)
generatorprimepairs=[];
for r in primepairs:
    p=r[0]
    q=r[1]
    h=euler_phi(q)%4
    v2=euler_phi(q^2)
    o2=Mod(p,q^2).multiplicative_order()
    if((o2==v2) or (not h==0 and (( 2*o2==v2) or (o2==v2) or (2*o2==v2)))):
        p=r[1]
        q=r[0]
        h=euler_phi(q)%4
        v2=euler_phi(q^2)
        o2=Mod(p,q^2).multiplicative_order()
        if((o2==v2) or (not h==0 and ((2*o2==v2) or (o2==v2) or (2*o2==v2)))):
            generatorprimepairs.append(r)
#compute the list of values Q(x)
asymtoticlist=[]
#countlistpart counts the number of GPPs p<q<=g
countlistpart=0
#countlistall counts the number of all odd prime pairs p<q<=g
countlistall=0
#bound + 5 is the greatest value for x
bound=p-5
for g in range(bound):
    g=g+5
    stop=0
    #only computes the value of Q(g) if g is a prime
    if(is_prime(g)):
        #the loop counts the number of prime pairs and GPPs <=g
        while(stop==0):
            if(primepairs[countlistall][0]<=g):
                countlistall=countlistall+1
            if(generatorprimepairs[countlistpart][0]<=g):
                countlistpart=countlistpart+1
            if(primepairs[countlistall][0]>g and generatorprimepairs[countlistpart][0]>g):
                stop=1
        #append the values to the list
        asymtoticlist.append([g,countlistpart/(countlistall).n()])
#Plot the list
list_plot(asymtoticlist,axes_labels=['x','Q(x)'])
```

**Listing 6.5:** Compute the values of $Q(x)$