Mildly Short Vectors in Ideals of Cyclotomic Fields Without Quantum Computers

Jean-François Biasse[1,*], Muhammed Rashad Erukulangara[1], Claus Fieker[2], Tommy Hofmann[3], William Youmans[1]

[1]Center for Cryptographic Research, University of South Florida
[2]Department of Mathematics, University of Kaiserslautern
[3]Department of Mathematics, University of Siegen

Received: 15th June 2022 | Accepted: 15th July 2022

Abstract *We present an algorithm for finding mildly short vectors in ideal lattices of cyclotomic fields, i.e. solutions to γ-SVP for $\gamma \in 2^{\tilde{O}(\sqrt{n})}$ where n is the degree of the field. Our algorithm is an adaptation of a method due to Cramer, Ducas and Wesolowski which is designed to use quantum computers. Our method, which only uses classical computers, leverages recursive methods using subfield computations based on norm relations introduced by Biasse, Fieker, Hofmann and Page. Our method applies to non-cyclic cyclotomic fields. In certain fields, the search for mildly short vectors efficiently reduces to subfield computations in fields of significantly smaller degree. In particular, we are able to identify infinite families of number fields where mildly short vectors can be found in time $2^{n^{o(1)}}$, which is a superpolynomial improvement over the BKZ algorithm.*

Keywords: Ideal lattices, Cyclotomic fields, Approximate short vector problem, Mildly short vectors, Ideal class group, S-unit group

2010 Mathematics Subject Classification: 11Y16, 20C05, 11R32, 11R29, 11R04, 11Y40, 11R18, 11R27

1 INTRODUCTION

Background Given a Euclidean lattice $\mathcal{L}$ and $\lambda \geq 1$, the problem of finding a non-zero $u \in \mathcal{L}$ such that $\|u\| \leq \gamma\lambda_1(\mathcal{L})$, where $\lambda_1(\mathcal{L})$ is the length of a shortest non-zero vector of $\mathcal{L}$ (i.e. its first minimum), is called the γ-Shortest Vector Problem (γ-SVP). The security of lattice-based cryptosystems such as LWE schemes [38] relies on the hardness of γ-SVP for γ polynomial in the dimension of the lattice. The LLL algorithm [26] solves γ-SVP for $\gamma \in 2^{O(n)}$ in polynomial time in n. Exponential algorithms such as sieve methods [2] can solve exact SVP (i.e. $\gamma = 1$) in time $2^{O(n)}$, while the BKZ algorithm [39] allows one to solve γ-SVP for $\gamma \in 2^{O(n/k)}$ in time $2^{O(k)}$. In particular, the time to solve γ-SVP for $\gamma \in 2^{\tilde{O}(\sqrt{n})}$ is in $2^{\tilde{O}(\sqrt{n})}$. In [17], solutions of γ-SVP for $\gamma \in 2^{\tilde{O}(\sqrt{n})}$ are referred to as *mildly short vectors*. We use this terminology throughout this paper. The study of the hardness of γ-SVP is crucial both from a fundamental standpoint and for its applications to cryptology. In particular, there are no efficient algorithms to solve γ-SVP for non-exponential γ. In the subexponential γ regime, any superpolynomial improvement over the state of the art (i.e. the BKZ algorithm) represents a significant step forward.

To gain efficiency, variants of lattice-based cryptosystems using lattices that are ideals in cyclotomic number fields were introduced. This is the case of cryptosystems based on the Ring Learning With Error (RLWE) problem [28]. It can be shown that γ-SVP in the cyclotomic field $\mathbb{Q}(\zeta_m)$ with a polynomial γ reduces to RLWE in this field. The most typical cyclotomic fields used in RLWE cryptosystems are those of the form $\mathbb{Q}(\zeta_{2^l})$ for some l (i.e. the fields with a power-of-two conductor). However, the use of general cyclotomic fields is possible [29]. One of the main security assumptions on which ideal lattice based cryptosystems rely is that γ-SVP in ideals of cyclotomic fields is not significantly easier than in general Euclidean lattices. Because of that, γ-SVP algorithms for ideals of $\mathbb{Q}(\zeta_m)$ that outperform the BKZ reduction method are of particular interest. Indeed, they document the gap between the hardness of this problem in the special case of ideals in cyclotomic fields and in the case of general lattices. However, such improvements do not necessarily imply an attack against RLWE schemes. Indeed, the proof of security of RLWE schemes relies on the hardness of γ-SVP for a polynomial γ. Hence, the hardness of the search for mildly short vectors does not directly impact it. In addition, even an efficient algorithm for the resolution of γ-SVP with a polynomial γ would not necessarily imply the cryptanalysis of RLWE schemes. It would however render the security proof moot.

Because of its close connection to the security proof of RLWE cryptosystems, the investigation of the hardness of γ-SVP in ideal lattices of cyclotomic fields (including the search for mildly short vectors) is a crucial stake

[*]Corresponding Author: biasse@usf.edu

in mathematical cryptology. It was heuristically observed by a scientific team from the British Government Communications Headquarter (GCHQ) that the search for short generators of principal ideals of $\mathbb{Q}(\zeta_{2^l})$ should be efficient with a quantum computer [15]. This observation relied on two conjectures: a) Quantum computers allow us to efficiently find generators of principal ideals in number fields, and b) The search for a short generators of a principal ideal in $\mathbb{Q}(\zeta_{2^l})$ efficiently reduces (on a classical computer) to the search for an arbitrary generator. Point a) was proven by Biasse and Song [11], while Point b) was proven by Cramer, Ducas, Peikert and Regev [18]. In particular, it is shown in [18] that a short generator of a principal ideal of $\mathbb{Q}(\zeta_{2^l})$ is a solution to γ-SVP for $\gamma \in 2^{\tilde{O}(\sqrt{n})}$ with $n = [\mathbb{Q}(\zeta_{2^l}) : \mathbb{Q}]$ (i.e. a mildly short vector). This is the first example of a superpolynomial gap between the hardness of γ-SVP in ideal lattices and in general lattices. This line of work was further expanded by Cramer, Ducas and Wesolowski [16] who showed that there was an efficient heuristic quantum reduction from the search for mildly short vectors in general ideal lattices of $\mathbb{Q}(\zeta_{2^l})$ (i.e. not necessarily principal) and the search for generators in principal ideals. This result was later extended to ideal lattices of $\mathbb{Q}(\zeta_m)$ for arbitrary m in [17]. In this paper, we refer to this heuristic reduction as CDW. To achieve an efficient quantum reduction, the CDW approach relies on two assumptions: a) The class group of the maximal real subfield $\mathbb{Q}(\zeta_m)^+$ of $\mathbb{Q}(\zeta_m)$ is small, and b) The minus part $\mathrm{Cl}^-(\mathcal{O}_K)$ of the ideal class group of $K = \mathbb{Q}(\zeta_m)$ is generated by few prime ideals. Limited numerical data in support of these conjectures is available, and most of it concerns the case $m = p$ a prime.

One of the key aspects of $\mathbb{Q}(\zeta_m)$ that enables the CDW approach is the knowledge of a set of units with good properties: the cyclotomic units. Indeed, units in number fields can be arbitrarily large, but in $\mathbb{Q}(\zeta_m)$, one can efficiently construct a set of small units that generate a subset of finite index of the group of units. This approach has been generalized by Pellet-Mary, Hanrot, and Stehlé who used S-units instead of units for a small enough set of primes S that generates the ideal class group of the field [36]. This method, known as PHS, allows one to solve γ-SVP for γ in $2^{O(n^a)}$ where $a < 1/2$ at the cost of an exponential precomputation on the S-units based on the work of Laarhoven [25]. The PHS approach was further improved [6], but the cost of the precomputation prevents it from solving γ-SVP more efficiently than the benchmark BKZ method. Recent preliminary work from Bernstein and Lange [8] conjectured that S-units of cyclotomic field have properties allowing one to adapt the PHS approach to outperform BKZ in the search for solutions to γ-SVP where $\gamma \in 2^{O(n^a)}$ with $a < 1/2$. To this date, there is no available strong evidence of this conjecture, even if it seems like the lattice of logarithmic embeddings of S-units of cyclotomic fields might not comply with so-called "Gaussian heuristics" which provide estimates for the first minima of random lattices. Independent work of Bernard, Lesavourey, Nguyen and Roux-Langlois [7] aimed to improve S-unit attacks by investigating sets of small S-units analogously to the case of cyclotomic units. They also attempted to remove the need for quantum computers in the CDW approach, but they were not able to improve the bottleneck of the method which consists in decompositions of ideals in the ideal class group.

Our contribution The main contribution of this paper is to propose a classical variant of the CDW algorithm for the computation of mildly short vectors in ideals of cyclotomic fields that reduces to computations in subfields. To achieve such reduction, our method uses the norm relations introduced by Biasse, Fieker, Hofmann, and Page [14]. Our method applies to the density 1 set of non-cyclic cyclotomic fields, but depending on the conductor m, the relative degree of the subfields of $\mathbb{Q}(\zeta_m)$ where computations are taking place varies. For certain conductors, we achieve an asymptotic speed-up over BKZ, and we were even able to exhibit a family of cyclotomic fields in which our methods enable the search for mildly short vectors in time $2^{n^{o(1)}}$. More specifically, here are the main technical contributions of this paper:

1. An algorithm using computations in subfields given by norm relations to decompose the ideal class of an ideal in a number field according to a set of generators of the ideal class group (Section 5).
2. An algorithm for computing the minus part of the ideal class group using computations in subfields given by norm relations (Section 7) .
3. The description of a classical analogue to the CDW method using subfield information (Algorithm 9).
4. The asymptotic analysis of our new subfield methods, as well as an infinite family of cyclotomic fields where the cost is in $2^{n^{o(1)}}$ (Section 8).
5. An implementation of the classical CDW technique, as well as numerical data in support of the heuristics made in [16] to support the asymptotic cost of CDW (Section 9).

Organization of the paper In Section 3, we begin with a high level description of the CDW technique from [16, 17]. Then, in Section 4, we recall the main facts about the norm relation techniques from [14] that will be used to describe a classical subfield variant of CDW. In Section 5, we show how to leverage norm relations to decompose the ideal class of an ideal according to a set of generators of $\mathrm{Cl}(\mathcal{O}_K)$. This building block is the cornerstone of our subfield CDW variant. Then in Section 6, we show how to solve the Principal Ideal Problem (PIP) using norm relations. Solving the PIP consists in deciding whether an ideal is principal, and if so, finding one of its generators. Then, in Section 7, we show how to compute the minus part of $\mathrm{Cl}(O_K)$ with norm relations, and how to find a small set of primes that generate this group. In Section 8, we analyze the asymptotic cost of our methods, and in Section 9, we present an implementation of our subfield CDW variant, as well as numerical data in support of the heuristics made to support the runtime of the CDW method. In Section 10, we conclude by mentioning potential future work to use norm relations in the context of PHS S-units attacks.

2 BACKGROUND IN NUMBER THEORY

Let K be an algebraic number field of degree n, that is, a finite extension of the rational numbers $\mathbb{Q}$ with $n = [K : \mathbb{Q}]$. For an element $\alpha \in K$ the minimal polynomial is the unique monic irreducible polynomial $f \in \mathbb{Q}[x]$ with $f(\alpha) = 0$ and we call α *integral* if the minimal polynomial is in $\mathbb{Z}[x]$. The set of all integral elements of K is a subring of K, which is called the *ring of integers* of K and which is denoted by O_K. The ring of integers O_K as well as all non-zero ideals of O_K are free $\mathbb{Z}$-modules of rank n. For a non-zero ideal $\mathfrak{a}$ of O_K, the quotient $O_K/\mathfrak{a}$ is a finite abelian group, whose order is called the *norm* of $\mathfrak{a}$ and which we denote by $\mathrm{N}(\mathfrak{a})$. By setting $\mathrm{N}(\{0\}) = 0$ for the zero ideal, the norm becomes a multiplicative map on the set of all ideals of O_K. Any $\mathbb{Z}$-basis of O_K is called an *integral basis*. Given such an integral basis $\omega_1, \ldots, \omega_n$, we denote by $\Delta_K = \det((\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j))_{1\leq i,j\leq n)}$ the *discriminant* of K, whose value is independent of the chosen integral basis.

A *fractional ideal* of K is a non-zero O_K-submodule of K, or equivalently, a set of the form $\frac{\mathfrak{a}}{d}$, where $\mathfrak{a}$ is a non-zero ideal of O_K and $d \in \mathbb{Z}$, $d \neq 0$. The set I_K of fractional ideals of K is a group with respect to multiplication with neutral element O_K. The inverse of a fractional ideal $\mathfrak{a}$ is given by $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq O_K\}$. The group of fractional ideals is free on the set of non-zero prime ideals of O_K and therefore the norm map extends uniquely to a group homomorphism $I_K \to \mathbb{Q}$, which we also denote by N. Of particular interest are *principal fractional ideals*, which are the fractional ideals of the form αO_K with $\alpha \in K^\times$. The set P_K of principal fractional ideals is a subgroup of the abelian group I_K. The quotient group I_K/P_K is the *(ideal) class group* of O_K or K, which we denote by $\mathrm{Cl}(O_K)$. A classical theorem of algebraic number theory asserts that $\mathrm{Cl}(O_K)$ is a finite group. We denote its order by h_K and call it the *class number* of O_K or K. When two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class, we denote this as $\mathfrak{a} \sim \mathfrak{b}$. We denote by h_m the class number of $K = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity (i.e. K is the *cyclotomic field* of conductor m). By h_m^+ we denote the class number of $K^+ := \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, and by $\mathrm{Cl}^-(O_K) \subseteq \mathrm{Cl}(O_K)$ the kernel of the map $[\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}]$, where $^-$ denotes complex conjugation. The cardinality of $\mathrm{Cl}^-(O_K)$ is denote by h_m^-, and we have $h_m = h_m^+ h_m^-$.

Since K is of degree n, there are n embeddings $\sigma \colon K \to \mathbb{C}$, which can be classified as follows: If the image of σ is contained in the real numbers $\mathbb{R}$, we call σ a *real embedding* of K. Otherwise σ is called a *complex embedding*. Because of complex conjugation, the complex embeddings of K always come in pairs. If $2s$ denotes the number of complex embeddings and r the number of real embeddings, then (r, s) is the *signature* of K. Denote by $\sigma_1, \ldots, \sigma_r$ the real embeddings and by $\sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+s}$ the complex embeddings. We call K *totally real* if all embeddings are real and *totally complex* if all embeddings are complex. Since for an embedding $K^\times \to \mathbb{R}, \alpha \mapsto \log|\sigma(\alpha)|$ is a group morphism, we obtain the *logarithmic embedding*

$$\mathrm{Log}\colon K^\times \longrightarrow \mathbb{R}^{r+s},\ \alpha \longmapsto (\log(|\sigma_1(\alpha)|), \ldots, \log(|\sigma_{r+s}(\alpha)|)).$$

The celebrated theorem of Dirichlet asserts that $\mathrm{Log}(O_K^\times)$ is a lattice of rank $r + s - 1$ and $\ker(\mathrm{Log})$ is equal to the torsion units of K. In particular $O_K^\times \cong \mathbb{Z}^{r+s-1} \times T$, where T are the torsion units of K. For S a set of k distinct prime ideals, the S-unit group $O_{K,S}^\times \subseteq K$ is the multiplicative group of all α that generate a principal ideal of the form $(\alpha)O_K = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{x_\mathfrak{p}}$. The S-unit group is isomorphic to $\mathbb{Z}^{r+s+k-1} \times T$.

Assume now that L/K is a finite extension of number fields of degree d with $\mathrm{Tr}_{L/K} \colon L \to K$ the corresponding trace map. Then we define the *(relative) discriminant* $\Delta_{L/K}$ of L/K to be the O_K-ideal $\langle \det((\mathrm{Tr}_{L/K}(\omega_i\omega_j))_{1\leq i,j\leq d}) \mid \omega_1, \ldots, \omega_d \in O_L\rangle$. Using this notion, (relative) discriminants behave well in extension of number fields. Indeed, we have $\Delta_L = \mathrm{N}_{L/K}(\Delta_{L/K})\Delta_K^{[L:K]}$.

3 THE CDW TECHNIQUE

3.1 SHORT GENERATORS OF PRINCIPAL IDEALS

Assume we obtained a (not necessarily short) generator in compact representation (see [10, 20]) of an input principal ideal I of the the cyclotomic field $K = \mathbb{Q}(\zeta_m)$ of degree $n = \varphi(m)$ for some $m > 0$. In this section, we recall the main results of [18, 17] regarding the techniques for the computation of a short generator of I. The techniques we are using in this section were originally stated in the case were $m = 2^k$ for some k, but they were recently extended to the case of an arbitrary conductor in [17]. It relies on the so-called cyclotomic units, which are the units generated by $\{\pm\zeta_m\} \cup \{1 - \zeta_m^i \mid i = 1, \dots, m-1\}$. We denote this subgroup of $O_K^\times$ by C. From [45, Th 4.12], we know that $[\mathrm{Log}(O_K^\times) : \mathrm{Log}(C)]$ has finite index. Let the p_i be the prime divisors of $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, and let $m_i := m/p_i^{\alpha_i}$. From [17, Th 3.4], we know that the elements $\mathrm{Log}(v_j)$ generate $\mathrm{Log}(C)$ and that $\left\|\mathrm{Log}(v_j)\right\| \in O(\sqrt{m})$, where

$$v_j = \begin{cases} 1 - \zeta_m^j & \text{if for all indices } i \text{, we have } m_i \nmid j; \\ \frac{1-\zeta_m^j}{1-\zeta_m^{m_i}} & \text{otherwise, for the unique } i \text{ such that } m_i \mid j, \end{cases}$$

for $j = 1, \dots, m$. Denote by G the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and by $\tau \in G$ the complex conjugation. The algorithm for finding a short generator given any generator is summarized in Algorithm 1.

Algorithm 1 Finding a short generator of gO_K

```
Require: A generator $g$ of $I = gO_K$ where $K = \mathbb{Q}(\zeta_m)$.
Ensure: A unit $u$ such that $ug$ is a short generator of $I$.
1: $\forall i, w_i \leftarrow \mathrm{Log}(v_i), W \leftarrow (w_1, \dots, w_{m-1})$.
2: $s(G) \leftarrow \sum_{\sigma \in G} \sigma \in \mathbb{R}[G]/(1-\tau)$.
3: $t' \leftarrow \mathrm{Log}(g), t'' \leftarrow \frac{1}{\varphi(m)} \cdot \log(\mathrm{N}(g)) \cdot s(G)$.
4: $t \leftarrow t' - t'' \in \mathrm{Log}(O_K^\times) \otimes \mathbb{R}, x \leftarrow (0, \dots, 0)$.
5: while $\|W \cdot x - t\|_\infty > \sqrt{2 \cdot \log(4\varphi(m))} \cdot \max_{w \in W} \|w\|$ do
6:     $x \leftarrow \mathrm{CV}_\infty(W, t)$.
7: end while
8: return $u := \prod_i v_i^{-x_i}$.
```

The procedure $\mathrm{CV}_\infty(W, t)$ in Step 6 is described in [17, Cor. 2.2] and finds a vector x in W that is close to t for the infinity norm, given the set of short generators w_i for W that we have as input. One of the technical challenges outlined in [17] is that we need to ensure that we can work with rational approximations of the w_i, and of $\mathrm{Log}(g)$ while ensuring numerical stability. Assume the input g is given as the (non-evaluated) product $g = \prod_{i \le k} \gamma_i^{k_i}$ for $\gamma_i \in O_K$, $k_i > 0$, and let $p = \left\lceil \log_2\left(\max(\|L \cdot k\|, \|k\|_\infty, 10\sqrt{n}\|W\|^{2n-3})\right) \right\rceil$. In [17, Sec. 3.4], fixed point approximations with $p + m^2$ bits of precision were used, that is, the approximation of $x \in \mathbb{R}$ is given by $\overline{x} \in \mathbb{Q}$ of the form $\frac{a_x}{2^{p+m^2}}$ where $a_x \in \mathbb{Z}$. Then, to use $\mathrm{CV}_\infty(W, t)$, we need an approximation $\overline{W}$ of W with $p + m^2$ bits of precision that lies in $\mathrm{Log}(O_K^\times) \otimes \mathbb{R}$. This is achieved by computing an approximation $\tilde{W}$ of W with $p + m^2 + 1$ bits of precision and setting

$$\overline{w}_i := \tilde{w}_i - \frac{2}{\varphi(m)} \sum_{j=1}^{\varphi(m)/2} \widetilde{w_{i,j}} s(G).$$

The matrix $\overline{W}$ satisfies $\|\overline{W} - \tilde{W}\|_\infty \le \frac{1}{2^{p+m^2+1}}$, and for all i we have $\overline{w}_i \in (s(G) \cdot \mathbb{R})^\perp = \log(O_K^\times) \otimes \mathbb{R}$. Then it can be shown that the element $\overline{x}$ such that

$$\|\overline{W} \cdot \overline{x} - \overline{t}\|_\infty \le \sqrt{2\log(4\varphi(m))} \max_{w \in W} \|\overline{w}\|$$

gives us a short generator $g \cdot \prod_i v_i^{-\overline{x}_i}$ of I.

Theorem 1 ([17, Th. 3.6])**.** *There is a randomized algorithm that for any $g \in O_K$ finds an element $h \in O_K$ such that $gO_K = hO_K$ and*

$$\|h\| = e^{O\left(\sqrt{m\log(m)}\right)} \cdot \mathrm{N}(g)^{1/\varphi(m)}.$$

3.2 THE CLOSE PRINCIPAL MULTIPLE PROBLEM

The input to the CDW algorithm for the search for a mildly short vector is not necessarily a principal ideal. To reduce the search for mildly short vectors to short-PIP, we first find an ideal $\mathfrak{b} \subseteq O_K$ such that $\mathfrak{ab}$ is principal, and $\mathrm{N}(\mathfrak{b}) \in 2^{\tilde{O}(n^{3/2})}$ where $n = [K : \mathbb{Q}]$. In [16], this task is referred to as the Close Principal Multiple Problem. Then, the techniques of Section 3.1 yield a short generator of $\mathfrak{ab}$, which is a solution to γ-SVP in $\mathfrak{a}$ for γ in $2^{\tilde{O}(\sqrt{n})}$. This involves three main steps:

1. Multiply $\mathfrak{a}$ by random ideals of small norm $\mathfrak{a}_0$ until the class of $\mathfrak{a}' := \mathfrak{a}_0\mathfrak{a}$ is in $\mathrm{Cl}^-(O_K) \subseteq \mathrm{Cl}(O_K)$, the "minus part" of $\mathrm{Cl}(O_K)$.
2. Decompose the class of $\mathfrak{a}'$ in $\mathrm{Cl}^-(O_K)$ according to a set $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ of prime ideals that generate $\mathrm{Cl}^-(O_K)$.

3. Find a close vector v in a lattice $\mathcal{L}$ (which is known to annihilate $\mathrm{Cl}^-(O_K)$) to $t \in \mathbb{Z}^k$ such that $\mathfrak{a}'^{-1} \sim \prod_i \mathfrak{p}_i^{t_i}$. Then the solution to the problem is $\mathfrak{b} := \mathfrak{a}_0 \prod_i \mathfrak{p}_i^{t_i - v_i} \sim \mathfrak{a}^{-1}$ (which has small norm if the vector v found in Step (3) is close enough to t). In [16, 17], Steps (1) and (2) require the quantum polynomial time algorithm of [11]. With classical computers, subexponential algorithms for ideal class group computations and the principal ideal problem (PIP) such as [13] can be used, but they do not provide a better complexity than the BKZ algorithm. Step (3) on the other hand, can be performed efficiently on a classical computer with the methods introduced in [16].

If $\mathfrak{a} \sim \prod_i \mathfrak{p}_i^{x_i}$, then $\mathfrak{b} = \prod_i \mathfrak{p}_i^{x'_i}$ with $x'_i = -x_i \bmod h$ and $h = |\mathrm{Cl}(O_K)|$ satisfies that $\mathfrak{ab}$ is principal. The issue is that the x'_i can be quite large, thus preventing $\mathfrak{b}$ from satisfying $\mathrm{N}(\mathfrak{b}) \leq 2^{\tilde{O}(n^{3/2})}$. However, the techniques of [16, 17] show how to derive $\mathfrak{b} \sim \prod_i \mathfrak{p}_i^{x'_i}$ with small exponents. We recall the general idea of this method, and we refer to [16, 17] for the details of the proofs. This task involves the search for close vectors in the so-called Stickelberger lattice, and to bound the runtime, we need to rely on a key conjecture:

Conjecture 1 ([17, Assumption 1]). *There are integers $l \leq \mathrm{Polylog}(m)$ and $B \leq \mathrm{Poly}(m)$ such that the following holds. Choose uniformly at random l prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ among the primes of norm less than B that lie in $\mathrm{Cl}^-(O_K)$. Then the set $S := \{\mathfrak{p}_i^\sigma \mid \sigma \in G\}$ generates $\mathrm{Cl}^-(O_K)$ with probability at least $1/2$.*

We first compute a short generating set of $\mathrm{Cl}^-(O_K)$. Then we perform a random walk in the Cayley graph of $\mathrm{Cl}(O_K)$ whose edges are defined by the primes in S from Conjecture 1. In other words, this means that we multiply $\mathfrak{a}$ by random elements of S until we get an ideal $\mathfrak{a}'$ whose class lies in $\mathrm{Cl}^-(O_K)$. This is described in [17, Alg. 5]. Its cost is in $O\left(h_K^+ \cdot \mathrm{Poly}(m, \log(\mathrm{N}(\mathfrak{a}))) \cdot \mathrm{Cost}(\mathrm{PIP})\right)$ according to [17, Lem. 5.2], where h_K^+ denotes the class number of the totally real subfield $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$. To bound this asymptotic cost, we need to assume that h_K^+ is small enough:

Conjecture 2 ([17, Assumption 2]). *For any integer m, it holds that $h^+(m) \leq \mathrm{Poly}(m)$.*

So we find small $x_i \leq 0$ such that the class of $\mathfrak{a}' := \mathfrak{a} \cdot \prod_i \mathfrak{p}_i^{x_i}$ is in $\mathrm{Cl}^-(O_K)$, and then we decompose the ideal class of $\mathfrak{a}'$ according to the set of primes S defined by Conjecture 1 to get a vector $\vec{y}$ such that $\mathfrak{a}' \sim \prod_i \mathfrak{p}_i^{y_i}$. Then [17, Sec. 4] constructs a lattice of vectors in $\mathbb{Z}[G]$ that act trivially on $\mathrm{Cl}^-(O_K)$ from the Stickelberger ideal. The Stickelberger ideal (see [17, Sec. 4.1]) is an ideal of $\mathbb{Z}[G]$ that annihilates $\mathrm{Cl}(O_K)$ but that does not have full rank as a $\mathbb{Z}[G]$-module. To get a full rank module, we project it to $R = \mathbb{Z}[G]/(1+\tau)$, where τ is the complex conjugation. The action of the resulting lattice L of R-rank $\varphi(m)/2$ annihilates $\mathrm{Cl}^-(O_K)$ because $\tau + 1$ annihilates $\mathrm{Cl}^-(O_K)$. The decomposition of $\mathfrak{a}'$ is then split according to each cycle under the action of R:

$$\mathfrak{a}' \sim \left(\prod_{\sigma \in G} (\mathfrak{p}_1^\sigma)^{y_{1,\sigma}}\right)\left(\prod_{\sigma \in G} (\mathfrak{p}_2^\sigma)^{y_{2,\sigma}}\right) \ldots \left(\prod_{\sigma \in G} (\mathfrak{p}_d^\sigma)^{y_{d,\sigma}}\right)$$

Then, we apply [17, Alg. 3] on each cycle $\vec{y}_i := (y_{i,\sigma})_{\sigma \in G}$. According to [17, Th. 4.7], this yields a vector $\vec{y}'_i$ such that $\prod_{\sigma \in G} \left(\mathfrak{p}_i^\sigma\right)^{y_{i,\sigma}} \sim \prod_{\sigma \in G} \left(\mathfrak{p}_i^\sigma\right)^{y'_{i,\sigma}}$ with $\|\vec{y}'_i\|_1 \leq \frac{1}{4}\varphi(m)^{3/2}$ in polynomial time in $\log \|\vec{y}_i\|$. Then, under Conjecture 1, $\mathfrak{b} := \prod_i \prod_\sigma (\mathfrak{p}_i^\sigma)^{y'_{i,\sigma}}$ satisfies $\mathrm{N}(\mathfrak{b}) \in 2^{O(n^{3/2})}$ and $\mathfrak{ab}$ is principal, thus solving the Close Principal Multiple Problem.

4 NORM RELATIONS

4.1 DEFINITION

In this section, we recall some facts about norm relations and their existence. We refer the reader to [14] for details. Let K be a Galois number field with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. For a subgroup $H \leq G$ we denote by $N_H = \sum_{h \in H} h \in \mathbb{Q}[G]$ the norm of H as an element of the group algebra $\mathbb{Q}[G]$. A *norm relation of G* is an equality of the form $1 = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i$ in $\mathbb{Q}[G]$ with $a_i, b_i \in \mathbb{Q}[G]$ and subgroups $1 \neq H_i \leq G$. By clearing denominators, a norm relation can always be written as

$$d = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i \tag{1}$$

with $d \in \mathbb{N}_{>0}$ minimal such that $a_i, b_i \in \mathbb{Z}[G]$. We call d the *denominator* of the norm relation.

The existence of such a norm relation for a number field implies relations between arithmetic objects of the field K and its subfields (see [14]). In the present paper, we will use the fact that Equation (1) implies that for all $x \in K^\times$ we have

$$x^d = \prod_{i=1}^{l} \mathrm{N}_{K/K^{H_i}}(x^{b_i})^{a_i}, \tag{2}$$

where $K^H = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ is the fixed field of H, and $x^a = \prod_{g\in G} g(x)^{a_g}$ for all $x \in K^\times$ and $a = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$. We will most often use an equality of the form (2) when referring to a norm relation. Let now $\mathfrak{a}$ be a fractional ideal of K. From [33, Chapter III, §1, Proposition 1.6] it follows that for a subgroup $H \leq G$ the following relation holds: $\mathrm{N}_{K/K^H}(\mathfrak{a})\mathcal{O}_K = \prod_{\sigma\in H}\sigma(\mathfrak{a}) = \mathfrak{a}^{N_H}$. In particular, from Equation (1), we also obtain

$$\mathfrak{a}^d = \prod_{i=1}^{l} \mathrm{N}_{K/K^H}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K. \tag{3}$$

Example 1. *Let $G = C_2 \times C_2 = \langle\sigma,\tau\rangle$. Then we have the norm relation $2 = N_{\langle\sigma\rangle} + N_{\langle\tau\rangle} - \sigma N_{\langle\sigma\tau\rangle}$. This is the norm relation used implicitly in both [5] and [12].*

Due to Funakura [21] we have the following simple criterion for the existence of norm relations for abelian groups G. Note that this implies that norm relations exist if and only if G is not cyclic. Thus, for cyclotomic fields $K = \mathbb{Q}(\zeta_m)$ this implies that a norm relation exists if and only if m is not 2, 4, p^k or $2p^k$, where p is an odd prime and $k \in \mathbb{N}$.

Theorem 2 ([14, Theorem 2.27])**.** *Let G be a finite abelian group, and write $G \cong C \times Q$ where C is the largest cyclic factor of G.*

1. *The group G admits a norm relation with denominator 1 if and only if $|Q|$ is divisible by at least two distinct primes. If the condition is satisfied, then G admits a norm relation with $a_i \in \mathbb{Z}$, denominator 1, and where all H_i satisfy that G/H_i is a p_i-group times a cyclic group, for some prime number p_i.*
2. *Assume that Q is a p-group. Then G admits a norm relation if and only if $Q \neq 1$. If the condition is satisfied, then G admits a norm relation with $a_i \in \mathbb{Z}$, denominator a power of p and where all H_i satisfy that G/H_i is a cyclic group.*

4.2 SATURATION TECHNIQUES

Equation (2) shows us that when a norm relation of denominator d involving the fields $K_1, \ldots, K_l$ exists, then we know that the d-th powers of all elements $x \in K$ can be expressed as products of elements in $K_1, \ldots, K_l$. Suppose we want to compute a generating set of a multiplicative group $U \subseteq K^\times$ (typically the group of units, of the S-unit group for a certain set S), we can use the following recursive strategy:

1. Compute a subgroup $V \subseteq U$ such that $V \cap (K^\times)^d = U^d$.
2. Compute generators $v_1, \ldots, v_k$ of $V \cap (K^\times)^d$.
3. Take the d-th roots of the v_i and deduce generators of U.

When U is the S-unit group for a set of prime ideals S that is stable under the action of the Galois group, we can take V to be the subgroup of U generated by all the S_i-unit groups of K_i, where S_i is the set of prime ideals of K_i lying under the primes of S. Then, since V contains all $\mathrm{N}_{K/K_i}(U)$, we know from equation (2) that it contains all d-th powers of U. Additionally, if $x^d \in V$, then x must be only divisible by elements of S, hence $x \in U$ and $V \cap (K^\times)^d = U^d$. Step (2) is known as a *saturation* technique. We define the *d-saturation* W of V as the smallest group $W \subseteq K^\times$ with $V \subseteq W$ and $K^\times/W$ being d-torsion free. The group V is d-saturated if it equals its d-saturation. The saturation technique takes the subgroup V of the group U that we desire to compute, with the guarantee that U equals the d-saturation of V, and computes generators for $(V \cap (K^\times)^d)/V^d$.

When dealing with an arbitrary denominator d, we first factor d as a product of prime powers, and we repeat Steps (2) and (3) for all prime powers dividing d. Thus from now on we will assume that d is a prime power. Saturation employs local computations to detect global powers. This a well known technique in computational algebraic number theory, used for example in the class and unit group computation of number fields ([37, Section 5.7]) or the number field sieve ([1]). Note that, in contrast to previous applications of this technique, in our case the number d is in general not a prime. As a consequence, we will rely on the Grunwald–Wang theorem (see [3, Chapter X] or [34, Chapter IX, §1]) and therefore have to consider the following dichotomy. For $k \in \mathbb{Z}_{\geq 1}$ denote by ζ_k a primitive k-th root of unity and set $\eta_k = \zeta_k + \zeta_k^{-1}$. Let $s \geq 2$ be an integer such that $\eta_s \in K$ but $\eta_{s+1} \notin K$. Moreover let S be a finite set of prime ideals of $\mathcal{O}_K$. Recall that d is a prime power. We say that we are in the *bad case* when the following conditions are simultaneously satisfied:

1. The number $d = 2^t$ is even and $t > s$.
2. The elements $-1, 2 + \eta_s$ and $-(2 + \eta_s)$ are non-squares in K.
3. We have
$$\{\mathfrak{p} \mid 2 \in \mathfrak{p} \text{ and } -1, 2+\eta_s \text{ and } -(2+\eta_s) \text{ are non-squares in } K_\mathfrak{p}\} \subseteq S.$$

If we are not in the bad case, we say that we are in the *good case*. The terminology is explained by the theorem of Grunwald–Wang, which gives the following connection between global and local d-th powers.

Theorem 3 (Grunwald–Wang)**.** *Consider the canonical map*

$$K^\times/(K^\times)^d \longrightarrow \prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d.$$

If we are in the good case, this map is injective. If we are in the bad case, the kernel of the map is $\langle \bar{\eta}_s \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

The good case Finding d-th powers in the good case can be done exclusively by detecting local d-th powers modulo a set of prime ideals. Recall that for a set S of prime ideals of $\mathcal{O}_K$ we denote by $\mathcal{O}_{K,S}$ the ring of S-integers, that is, the elements $x \in K$ with $v_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \notin S$, and $\mathcal{O}_{K,S}^\times$ the group of S-units, i.e., the elements $x \in K^\times$ such that $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \notin S$.

Proposition 1 ([14, Proposition 4.5])**.** *Assume that $\mathfrak{p}$ is a non-zero prime ideal with $d \notin \mathfrak{p}$ and let $\varpi \in K$ be a local uniformizer at $\mathfrak{p}$, that is, an element with $v_\mathfrak{p}(\varpi) = 1$. Then the map*

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d \longrightarrow \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d, \quad \bar{x} \longmapsto (\bar{v}, \overline{x\varpi^{-v}}) \text{ where } v = v_\mathfrak{p}(x),$$

is an isomorphism.

Proposition 2. *Assume that we are in the good case of Grunwald–Wang. For a multiplicative finitely generated subgroup $V \subseteq K^\times$ we have*

$$(V \cap (K^\times)^d)/V^d = \bigcap_{d\notin\mathfrak{p}} \ker(V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$

There exists $c_0 \in \mathbb{R}_{>0}$ (depending on K, V and d) such that

$$(V \cap (K^\times)^d)/V^d = \bigcap_{d\notin\mathfrak{p}, \mathrm{N}(\mathfrak{p})\leq c_0} \ker(V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$

Proof. The first part is [14, Proposition 4.6]. As V is finitely generated, V/V^d is a finitely generated $(\mathbb{Z}/d\mathbb{Z})$-module. Thus V/V^d is Artinian and the existence of c_0 follows from the first part. □

The general case In the general case, d is a power of 2, but the approach we sketch here applies to $d = p^t$ a power of an arbitrary prime p. In essence, it consists in inductively computing the p-saturation of V and replacing it with its p-saturation t times. At each step, p-th roots of generators of $(V \cap (K^\times)^p)/V^p$ need to be computed, which makes this process in practice more computationally expensive than in the so-called good case, but does not change the overall asymptotic complexity.

5 IDEAL DECOMPOSITION FROM NORM RELATIONS

Given an input ideal $\mathfrak{a}$ whose ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ is known to be a product of powers of the classes of $\mathfrak{g}_1, \dots, \mathfrak{g}_k$, the task of finding exponents such that $\mathfrak{a} \sim \prod_i \mathfrak{g}_i^{x_i}$ is central to the CDW framework. In [16], this requires a quantum computer. The best classical algorithms for ideal class decomposition have the same asymptotic cost as the computation of $\mathrm{Cl}(\mathcal{O}_K)$, which is subexponential. In this section, we show how to leverage norm relations to reduce the decomposition of the class of an input ideal $\mathfrak{a} \subseteq K$ to subfield computations. We assume that there are subfields $(K_i)_{i\leq l}$ such that ideals of K satisfy the norm equation (2). We first tackle the case of the decomposition of $\mathfrak{a}$ according to a set S of prime ideals invariant under the action of $\mathrm{Gal}(K/\mathbb{Q})$. Then, given a subgroup $H \subseteq \mathrm{Cl}(\mathcal{O}_K)$, and generators $\mathfrak{g}_1, \dots, \mathfrak{g}_k$ of order $d_1, \dots, d_k$ such that $H \simeq \langle \mathfrak{g}_1 \rangle \times \dots \times \langle \mathfrak{g}_k \rangle$, we show how to find the unique $(x_1, \dots, x_k) \in \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$ such that $\mathfrak{a} \sim \prod_i \mathfrak{g}_i^{x_i}$.

5.1 IDEAL DECOMPOSITION WITH RESPECT TO PRIMES

Let $S = \{\mathfrak{p}_i\}_{i\leq k}$ be a set of non-zero prime ideals of $\mathcal{O}_K$ that is stable under the action of $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\langle S \rangle \subseteq \mathrm{Cl}(\mathcal{O}_K)$ be the subgroup of $\mathrm{Cl}(\mathcal{O}_K)$ generated by the classes of the elements of S. Assume that an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ satisfies (3), i.e. $\mathfrak{a}^d = \prod_{i=1}^l \mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K$. Then, for each i, one can recursively find the decomposition of $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})$ in $\mathrm{Cl}(\mathcal{O}_{K_i})$ with respect to the $\mathfrak{p} \cap K_i$ for $\mathfrak{p} \in S$, and deduce the decomposition of $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K$ in $\mathrm{Cl}(\mathcal{O}_K)$ with respect to S (each $(\mathfrak{p} \cap K_i)\,\mathcal{O}_K$ is a product of elements of S since it is assumed to be stable under the action of G). At this point, we have $\vec{x}$ such that $\mathfrak{a}^d \sim \prod_i \mathfrak{p}_i^{x_i}$.

This information alone is not enough to decompose $\mathfrak{a}$ with respect to the $\mathfrak{p}_i$ in $\mathrm{Cl}(\mathcal{O}_K)$. In particular, we need to use a generator of the principal ideal $\mathfrak{a}^d \prod_i \mathfrak{p}_i^{-x_i}$. To get this information, in each subfield, we can make sure that we obtain an identity of the form

$$\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K = (\alpha_i)\prod_j \mathfrak{p}_j^{x_{i,j}}.$$

This can be done by working exclusively in the subfields (an ideal class decomposition in $\mathrm{Cl}(\mathcal{O}_{K_i})$ followed by solving a PIP in K_i). By recombining all subfield information, we obtain an identity of the form

$$\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}, \tag{4}$$

where $\vec{y} \in \mathbb{Z}^k$ and $\alpha \in K$ is given in product form. We summarize this procedure in Algorithm 2.

Algorithm 2 Decomposition of $\mathfrak{a}^d$ with norm relation

```
Require: Number field $K$ of unit rank $r$, norm relation $d = \sum_i a_i \mathrm{N}_{H_i} b_i$, ideal $\mathfrak{a}$ and set $S$ of $k$ prime ideals stable under the action of $G = \mathrm{Gal}(K/\mathbb{Q})$, and with $[\mathfrak{a}] \in \langle S \rangle$.
Ensure: $\vec{y}$ and $\alpha$ such that $\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}$.
Compute a basis $(\beta_i)_{i \le r+k}$ for the $S$-unit group (using recursive norm relation techniques), and let $M \in \mathbb{Z}^{(r+k)\times k}$ such that $(\beta_i) = \prod_j \mathfrak{p}_j^{M_{i,j}}$.
for $K_i$ in the norm relation do
    Compute $\alpha_i, \vec{x}_i$ such that $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K = (\alpha_i)\prod_j (\mathfrak{p}_j \cap K_i)^{x_{i,j}}$.
end for
Deduce $\alpha$ in product form and $\vec{y}$ such that $\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}$.
return $\alpha, \vec{y}$.
```

Computing d-th root in $\mathrm{Cl}(\mathcal{O}_K)$ Now we also know that since the class of $\mathfrak{a}$ is a product of the classes of S, there must exist $\vec{z} \in \mathbb{Z}^k$ and $\beta \in K$ such that $\mathfrak{a} = (\beta)\prod_i \mathfrak{p}_i^{z_i}$, which means that

$$\mathfrak{a}^d = (\beta^d)\prod_i \mathfrak{p}_i^{dz_i}.$$

Now we have the equality of ideals $(\beta^d)\prod_i \mathfrak{p}_i^{dz_i} = (\alpha)\prod_i \mathfrak{p}_i^{y_i}$, but since α is not necessarily β^d, we don't necessarily have $y_i = dz_i$. However, we know that $\prod_i \mathfrak{p}_i^{y_i} \sim \mathfrak{p}_i^{dz_i}$ so we must have $\vec{y} - d\vec{z} \in \mathcal{L}$ where $\mathcal{L} \subseteq \mathbb{Z}^k$ is the lattice of relations between the $\mathfrak{p}_i$, i.e. the lattice of vectors $\vec{u}$ such that $\prod_i \mathfrak{p}_i^{u_i}$ is a principal ideal. We want to re-write α as $\alpha = \beta'^d \cdot \delta$ where δ is an S-unit with $(\delta)\mathcal{O}_K = \prod_i \mathfrak{p}_i^{u_i}$ such that $\vec{u} + \vec{y} \in d\mathbb{Z}^k$. If this is the case, then $\mathfrak{a}^d = (\beta'^d)\prod_i \mathfrak{p}_i^{dz'_i}$ where $\vec{z'} := \vec{u} + \vec{y}$. Once an S-unit δ_0 such that $(\delta_0) = \prod_i \mathfrak{p}_i^{u_i^0}$ with $\vec{u}^{(0)} + \vec{y} \in d\mathbb{Z}^k$ is found, then any other solution δ is of the form $\delta = \delta_0\delta'$ where δ' is an S-unit satisfying $(\delta')\mathcal{O}_K = \prod_i \mathfrak{p}_i^{u'_i}$ with $\vec{u'} \in d\mathbb{Z}^k$. The set of such δ' is a subgroup of the S-unit group

Using saturation methods sketched in Section 4.2, we can compute generators $\alpha_1, \ldots, \alpha_{r+k+1}$ of the S-unit group from subfield computations (where r is the rank of the unit group), together with a matrix $M \in \mathbb{Z}^{(r+k+1)\times k}$ whose rows are the valuations of the α_i according to the primes in S. Thus, there is $\vec{x} \in \mathbb{Z}^{r+k+1}$ such that $\vec{y} = \vec{x}M + d\vec{z}$, i.e.

$$\vec{y} = \vec{x}M \bmod d.$$

This system does not have a unique solution. However, we can put M in row reduced echelon form modulo d and find

1. a solution $\vec{x}^{(0)}$ to $\vec{y} = \vec{x}M \bmod d$,
2. a basis $\vec{x}^{(1)}, \ldots, \vec{x}^{(m)}$ of the left kernel of $M \bmod d$.

So all the $\vec{x}$ such that $\vec{y} = \vec{x}M \bmod d$ are of the form $\vec{x} = \vec{x}^{(0)} + \sum_j a_j\vec{x}^{(j)}$, including the one that satisfies $\vec{y} = \vec{x}M + d\vec{z}$ for $\vec{z}$ defined above. We denote by $\vec{x}^{(j)}M_i$ the i-th coefficient of $\vec{x}^{(j)}M$, and by $\alpha_i \in K$ the element that satisfies $\prod_j \mathfrak{p}_j^{M_{i,j}} = (\alpha_i)\mathcal{O}_K$. With the notation previously used, $\delta_0 = \prod_i \alpha_i^{x_i^{(0)}}$, while the subgroup of δ''s is generated by $\delta_i := \prod_i \alpha_i^{x_i^{(j)}}$ for $i = 1, \ldots, m$. Therefore, we have

$$\begin{aligned}(\alpha)\prod_i \mathfrak{p}_i^{y_i} &= (\alpha)\prod_i \mathfrak{p}_i^{\vec{x}M_i}\cdot\prod_i \mathfrak{p}_i^{y_i-\vec{x}M_i}\\ &= (\alpha)\prod_i \mathfrak{p}_i^{\vec{x}^{(0)}M_i}\cdot\prod_{j\le m}\left[\prod_i \mathfrak{p}_i^{\vec{x}^{(j)}M_i}\right]^{a_j}\cdot\prod_i \mathfrak{p}_i^{y_i-\vec{x}M_i}\\ &= (\alpha)\left(\prod_i \alpha_i^{x_i^{(0)}}\right)\cdot\left(\prod_{j\le m}\left[\prod_i \alpha_i^{x_i^{(j)}}\right]^{a_j}\right)\cdot\prod_i \mathfrak{p}_i^{y_i-\vec{x}M_i}\\ &= (\alpha')\left(\prod_j \delta_j^{a_j}\right)\cdot\prod_i \mathfrak{p}_i^{dz'_i}\ \text{ for some } z'_i\in\mathbb{Z}\end{aligned}$$

where we have a product representation of $\alpha'\in K$ and the $\delta_j\in K$.

So we are looking for $(a_j)_{i\le m}$ such that $\alpha'\cdot\prod_j\delta_j^{a_j}=\beta'^d$ for some $\beta'\in K$. Once we find $(a_j)_{i\le m}$, we derive the corresponding $\vec{x}=\vec{x}^{(0)}+\sum_{j\le m}a_j\vec{x}^{(j)}$ and then $\vec{z'}=\frac{1}{d}(\vec{y}-\vec{x}M)$. This means that we have the identity

$$\mathfrak{a}^d=(\beta'^d)\prod_i\mathfrak{p}_i^{dz'_i}.$$

Such an identity exists at least for $\beta'=\beta$ and $z'_i=z_i$ (with the notation above), but other choices of $(a_i)_{i\le m}$ might lead to other solutions. Once a solution is found, we have $\mathfrak{a}=(\beta')\prod_i\mathfrak{p}_i^{z'_i}$ since an equality of fractional ideals of the form $I^d=J^d$ implies that $I=J$ by uniqueness of prime decomposition. Thus, we are able to conclude that $\mathfrak{a}\sim\prod_i\mathfrak{p}_i^{z'_i}$, which solves the ideal class decomposition problem.

Now the question is how to find the desired $(a_i)_{i\le m}$? Since there is a solution, we know that α' is a d-th power modulo U for $U=\langle\delta_1,\dots,\delta_m\rangle$. This means that there are $x\in K^\times$ and $u\in U$ such that $\alpha'=u\cdot x^d$. To find the a_i, we apply a variation of the saturation methods described in Section 4.2. We begin with the case of d a prime power in the good case of Grunwald–Wang.

The good case. We assume that we are in the good case of Grunwald–Wang. The aforementioned discussion shows that it is sufficient to determine whether an element $\alpha'\in K$ is a d-th power modulo $U=\langle\delta_1,\dots,\delta_m\rangle$.

Proposition 3. *Let $V=\langle U,\beta\rangle$ where $U=\langle\alpha_1,\dots,\alpha_l\rangle$, and assume $U\cap\langle\beta\rangle=\{1\}$, d is a prime power, and that we are in the good case of Grunwald–Wang. Furthermore let $c\in\mathbb{R}_{>0}$ be arbitrary. Assume that the intersection*

$$\bigcap_{d\notin\mathfrak{p},\mathrm{N}(\mathfrak{p})\le c}\ker(V/V^d\to\mathbb{Z}/d\mathbb{Z}\times k_{\mathfrak{p}}^\times/(k_{\mathfrak{p}}^\times)^d)\subseteq V/V^d$$

is generated by the classes of $\alpha_1\beta^{n_1},\dots,\alpha_l\beta^{n_l}\in V$ with $\alpha_i\in U$, $n_i\in\mathbb{Z}$.

1. *If $\gcd(d,n_1,\dots,n_l)\neq1$, then β is not a d-th power modulo U.*
2. *Assume β is not a d-th power modulo U. Then for c sufficiently large we have $\gcd(d,n_1,\dots,n_l)\neq1$.*
3. *Assume β is a d-th power modulo U. Then for c sufficiently large we have $\gcd(d,n_1,\dots,n_l)=1$ and that the element $\alpha_1^{k_1}\cdots\alpha_l^{k_l}\beta$ is a d-th power, where $k_i\in\mathbb{Z}$ are integers with $1=k_0d+\sum_{i=1}^l k_in_i$.*

Proof. Let us denote by W/V^d the intersection of the kernels.

(1): Assume that β is a d-th power modulo U, that is, $\alpha\beta\in V\cap(K^\times)^d$ for some $\alpha\in U$. As $(V\cap(K^\times)^d)/V^d\subseteq W/V^d$, there exist integers $0<k_i<d$ such that

$$\overline{\alpha\beta}=\overline{(\alpha_1\beta^{n_1})^{k_1}\cdots(\alpha_l\beta^{n_l})^{k_l}}$$

in $W/V^d\subseteq V/V^d$. As V is generated by U and β, the group V^d is generated by U^d and β^d. Hence there exists $\alpha_0\in U$ and $k_0\in\mathbb{Z}$ such that

$$\alpha\beta=(\alpha_1\beta^{n_1})^{k_1}\cdots(\alpha_l\beta^{n_l})^{k_l}\alpha_0^d(\beta^d)^{k_0}.$$

From $U\cap\langle\beta\rangle=\{1\}$ we get $1=k_0d+\sum_{i=1}^l k_in_i$ i.e. $\gcd(d,n_1,\dots,n_l)=1$.

(2): Let c_0 be the constant from Proposition 2 and assume $c\ge c_0$. In particular it holds $(V\cap(K^\times)^d)/V^d=W/V^d$. Assume $\gcd(d,n_1,\dots,n_l)=1$. Then there exist $k_i\in\mathbb{Z}$, $0\le i\le l$, such that $1=k_0d+\sum_{i=1}^l k_in_i$. Then the element $\alpha=\alpha_1^{k_1}\cdots\alpha_l^{k_l}$ satisfies

$$\alpha\beta=\alpha\beta^{n_1k_1}\cdots\beta^{n_lk_l}\beta^{dk_0}=(\alpha_1\beta^{n_1})^{k_1}\cdots(\alpha_l\beta^{n_l})^{k_l}\beta^{dk_0},$$

that is $\overline{\alpha\beta} \in W/V^d = (V \cap (K^\times)^d)/V^d$ and β is a d-th power modulo U.

(3): Let c_0 be as in Proposition 2 and assume $c \geq c_0$. Note that as β is a d-th power modulo U, it follows from (1) that $\gcd(d, n_1, \ldots, n_l) = 1$. The result follows, since

$$\alpha^{k_1} \cdots \alpha^{k_l}\beta = (\alpha_1\beta^{n_1})^{k_1} \cdots (\alpha_l\beta^{n_l})^{k_l}(\beta^{k_0})^d$$

and for all $1 \leq i \leq l$ we have $\alpha_i\beta^{n_i} \in (K^\times)^d$ (as $c \geq c_0$). □

As we know that α' is a d-th power modulo U, we should have $\gcd(d, n_1, \ldots, n_m) = 1$, where the n_i are the exponents defined in Proposition 3 which are obtained from the intersection of the kernels. Let k, and $(a_i)_{i\leq m}$ such that $1 = kd + \sum_{i=1}^m a_i n_i$. With this choice of a_i we have that $\alpha' \prod_i \delta_i^{a_i}$ is a d-th power and we can find the decomposition of $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O}_K)$. Note that taking the d-th root of $\alpha' \prod_i \delta_i^{a_i}$ can be done efficiently by keeping elements in so-called *compact representation*. We summarize this procedure in Algorithm 3.

Algorithm 3 Ideal decomposition from subfields in the good case where $d = p^t$

```
Require: Number field $K$ of unit rank $r$, norm relation $d = \sum_i a_i \mathrm{N}_{H_i} b_i$ where $d$ is a prime power in the good case
    of Grunwald–Wang, ideal $\mathfrak{a}$ and set $S$ of $k$ primes stable under the action of $G = \mathrm{Gal}(K/\mathbb{Q})$, together with $\alpha, \vec{y}$
    such that $\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}$.
Ensure: $\beta', \vec{z'}$ such that $\mathfrak{a} = (\beta')\prod_i \mathfrak{p}_i^{z'_i}$.
  Compute a basis $(\alpha_i)_{i\leq k+r+1}$ for the $S$-unit group (using recursive norm relation techniques), and let $M \in$
    $\mathbb{Z}^{(r+k+1)\times k}$ such that $(\alpha_i) = \prod_j \mathfrak{p}_j^{M_{i,j}}$.
  Put $M$ in row reduced echelon form mod$d$. Find $\vec{x}^{(0)}$ solution to $\vec{y} = \vec{x}M$ mod $d$.
  Compute $\vec{x}^{(1)}, \ldots, \vec{x}^{(m)}$ basis of the left kernel of $M$ mod $d$.
  $\alpha' \leftarrow (\alpha)\left(\prod_i \alpha_i^{x_i^{(0)}}\right)$. For $j \leq m$: $\delta_j \leftarrow \prod_i \alpha_i^{x_i^{(j)}}$.
  $U \leftarrow \langle\delta_1, \ldots, \delta_m\rangle$. Let $c \leq c_0$ large enough.
  Compute a $(\mathbb{Z}/d\mathbb{Z})$-generating set $\overline{\delta_1\alpha'^{n_1}}, \ldots, \overline{\delta_m\alpha'^{n_m}}$ of
      $$\bigcap_{p\notin\mathfrak{p},\mathrm{N}(\mathfrak{p})\leq c} \ker(\langle U, \alpha'\rangle/\langle U, \alpha'\rangle^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$
  Compute $k, a_i \in \mathbb{Z}$, $1 \leq i \leq m$, with $1 = kd + \sum_{i=1}^m a_i n_i$. Let $\vec{x} \leftarrow \vec{x}^{(0)} + \sum_{j\leq m} a_j \vec{x}^{(j)}$.
  return $\sqrt[d]{\alpha' \cdot \prod_j \delta_j^{a_j}}, \frac{1}{d}(\vec{y} - \vec{x}M)$.
```

General case The following cases need extra care:

1. The case where α is an S-unit (which leads to $U \cap \langle\alpha'\rangle \neq \{1\}$ for $U = \langle\delta_1, \ldots, \delta_m\rangle$).
2. The case of d not a prime power.
3. The bad case of Grunwald–Wang.

Case (1) can be easily avoided by replacing α by $\alpha \cdot x^d$ where x is outside of the S-unit group. The procedure will succeed, and lead to the computation of appropriate exponents $a_1, \ldots, a_m$. For Case (2), assume that d is not a prime power. We rely on the following lemma

Lemma 1. *Let a, b be coprime integers such that $d = ab$. Assume that with Algorithm 3 we can find $\beta_x, \vec{x}, \beta_y, \vec{y}$ such that*

$$\mathfrak{a}^d = (\beta_x^a)\prod_i \mathfrak{p}_i^{ax_i} = (\beta_y^b)\prod_i \mathfrak{p}_i^{by_i}.$$

Then $\mathfrak{a} = (\beta_x^s\beta_y^r)\prod_i \mathfrak{p}_i^{sx_i+ry_i}$.

Proof. Let r, s be such that $ra + sb = 1$. This means that

$$\begin{aligned}\mathfrak{a}^d &= \left(\mathfrak{a}^d\right)^{ra+sb} = \left(\mathfrak{a}^d\right)^{ra}\left(\mathfrak{a}^d\right)^{sb}\\ &= \left((\beta_y)\prod_i \mathfrak{p}_i^{y_i}\right)^{rab}\left((\beta_x)\prod_i \mathfrak{p}_i^{x_i}\right)^{sab}\\ &= \left((\beta_x^s\beta_y^r)\prod_i \mathfrak{p}_i^{sx_i+ry_i}\right)^d.\end{aligned}$$

Therefore, by equality of ideals, we have a $\beta, \vec{z}$ such that $\mathfrak{a} = (\beta) \prod_i \mathfrak{p}_i^{z_i}$. □

This process can be iterated for all prime powers that divide d, thus reducing the case of arbitrary d to that of d being a prime power.

Finally, Case (3) concerns the bad case of Grunwald–Wang. Because of the above consideration, we can assume that d is a prime power, and since the bad case only concerns powers of two, there is t such that $d = 2^t$. Algorithm 3 cannot be applied directly on input d, but we can use it with denominator 2. This leads to the creation of $\beta', \vec{z}'$ such that

$$\mathfrak{a}^{2^{t-1}} = (\beta') \prod_i \mathfrak{p}_i^{z_i'}.$$

This can be iterated t times, eventually leading to the decomposition of $\mathfrak{a}$.

5.2 DECOMPOSITION WITH RESPECT TO ELEMENTARY GENERATORS OF $H \subseteq \mathrm{Cl}(O_K)$

Let H be a subgroup of $\mathrm{Cl}(O_K)$. In this paper, the two cases of interest are $H = \mathrm{Cl}^-(O_K)$, the minus part of the class group, and $H = \mathrm{Cl}(O_K)$. In the previous section, we established how to decompose the class of an input ideal $\mathfrak{a}$ with respect to a given set of primes S (if this decomposition exists, which is always the case when we pick S a generating set of $\mathrm{Cl}(O_K)$). Now, we need to leverage this routine in order to decompose the class of $\mathfrak{a}$ according to a fixed set of generators $\mathfrak{g}_1, \ldots, \mathfrak{g}_k$ where

$$H \simeq \langle[\mathfrak{g}_1]\rangle \times \cdots \times \langle[\mathfrak{g}_k]\rangle \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}.$$

We assume that $S = \{\mathfrak{p}_i\}_{i\leq k}$ is a set of non-zero prime ideals stable under the action of $\mathrm{Gal}(K/\mathbb{Q})$ such that $\langle S\rangle = H$. By using the recursive S-unit group computation, we can find a matrix $M \in \mathbb{Z}^{k\times k}$ such that the rows of M generate the lattice of vectors $\vec{v} \in \mathbb{Z}^k$ such that $\prod_i \mathfrak{p}_i^{v_i} \sim (1)$. This can be done by working in the subfields involved in the norm relation. Then, we compute the Smith Normal Form (SNF) $\mathrm{diag}(d_1, \ldots, d_k)$ of M and unimodular matrices U, V such that $UMV = \mathrm{diag}(d_1, \ldots, d_k)$ (note that some d_i might equal 1).

Given a fractional ideal $\mathfrak{a}$ such that $[\mathfrak{a}] \in H$, we are interested in computing the unique exponents in $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ of the decomposition of $[\mathfrak{a}]$ according to the generators $(\mathfrak{g}_i)_{i\leq k}$. The previous section shows how to decompose $[\mathfrak{a}]$ according to the primes in S. We can convert this decomposition into one with respect to the $\mathfrak{g}_i$ via linear algebra involving V. Indeed, the conversion back-and-forth between a representation over the $\mathfrak{g}_i$ and one over the $\mathfrak{p}_j$ corresponds to a multiplication of V^{-1} (resp. V) with the vector of exponents:

$$\mathfrak{a} \sim \prod_j \mathfrak{p}_j^{x_j} = \prod_j \left(\prod_i \mathfrak{g}_i^{x_j\cdot V^{-1}_{i,j}}\right) = \prod_i \mathfrak{g}_i^{\sum_j x_j V^{-1}_{i,j}} = \prod_i \mathfrak{g}_i^{(V^{-1}\cdot\vec{x}^T)}.$$

Therefore $\mathfrak{a} \sim \prod_i \mathfrak{g}_i^{x_i'}$ for $\vec{x}' := V^{-1}\cdot\vec{x}$. By a similar argument, if $\mathfrak{a} \sim \prod_i \mathfrak{g}_i^{y_i'}$, then $\mathfrak{a} \sim \prod_i \mathfrak{p}_i^{y_i}$ where $\vec{y} = V\cdot\vec{y}'$.

Algorithm 4 Conversion of decomposition with respect to primes in S to generators

```
Require: Number field $K$, Set $S$ of non-zero primes $(\mathfrak{p}_i)_{i\leq s}$, vector $\vec{x}$ such that $\mathfrak{a} \sim \prod_i \mathfrak{p}_i^{x_i}$, $U, V$ unimodular such
    that $UMV = \mathrm{diag}(d_1, \ldots, d_k)$ where the rows of $M$ are a basis of the lattice of relations between primes in $S$.
Ensure: $\vec{x}'$ with $\mathfrak{a} \sim \prod_i \mathfrak{g}_i^{x_i'}$ where $\langle S\rangle = \langle[\mathfrak{g}_1] \times \ldots \times \langle[\mathfrak{g}_k]\rangle$.
  return $\vec{x}' := V^{-1}\cdot\vec{x}$.
```

6 THE PRINCIPAL IDEAL PROBLEM

Given an input fractional ideal $\mathfrak{c}$, the Principal Ideal Problem (PIP) is two fold: 1) Decide whether $\mathfrak{c}$ is principal, and 2) If $\mathfrak{c}$ is principal, compute a generators. Item (1), which is the decisional part of the PIP is repeatedly used in the CDW algorithm, more specifically in the resolution of the Close Principal Multiple problem. Step (1) of Section 3.2 consists in testing many elements of the form $\mathrm{N}_{K/K^+}(\mathfrak{a})$ for principality. Likewise, Step (2) of Section 3.2 requires the testing that $\mathrm{N}_{K/K^+}(\mathfrak{p})$ is principal for many prime ideals $\mathfrak{p}$ (in order to create a generating set of prime ideals in $\mathrm{Cl}^-(O_K)$. Item (2) on the other hand, has to be used only once a close principal multiple $\mathfrak{b}$ to the input $\mathfrak{a}$ is found, to find a generator of $\mathfrak{a}\mathfrak{b}$.

Decisional PIP Deciding whether $\mathfrak{c}$ is principal is the same as deciding whether the ideal class $[\mathfrak{c}] \in \mathrm{Cl}(O_K)$ is the trivial element of the class group. Following the notation of Section 5, with $H = \mathrm{Cl}(O_K)$, this means that $\mathfrak{c}$ is a principal ideal if and only if it is represented by the vector $(0, \ldots, 0) \in \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z}$. Therefore, to solve the decisional PIP, one needs to precompute a set of primes S stable under that action of $\mathrm{Gal}(K/\mathbb{Q})$ generating the class group, and then apply Algorithms 3 and 4.

Algorithm 5 Decisional PIP

```
Require: Number field $K$, fractional ideal $\mathfrak{a}$, set $S$ of non-zero primes $(\mathfrak{p}_i)_{i\leq s}$ that generate $\mathrm{Cl}(\mathcal{O}_K)$, vector $\vec{x}$ such that $\mathfrak{a} \sim \prod_i \mathfrak{p}_i^{x_i}$, $U, V$ unimodular such that $UMV = \mathrm{diag}(d_1, \ldots, d_k)$ where the rows of $M$ are a basis of the lattice of relations between primes in $S$.
Ensure: Whether $\mathfrak{a}$ is principal.
Compute vector $\vec{x}$ such that $\mathfrak{a} \sim \prod_i \mathfrak{p}_i^{x_i}$ with Algorithm 3.
Use $\vec{x}$ and $V$ to produce $\vec{y}$ such that $\mathfrak{a} \sim \prod_i \mathfrak{g}_i^{y_i}$ where $\mathrm{Cl}(\mathcal{O}_K) \simeq \langle \mathfrak{g}_1 \rangle \times \ldots \times \langle \mathfrak{g}_k \rangle$.
return $\mathfrak{a}$ is principal if $\vec{y} = \vec{0}$.
```

Search-PIP The computation of a generator of an input fractional ideal $\mathfrak{a}$ can also be done using S-units, but the main difference with the decisional variant of PIP is that the S-unit group that needs to be calculated depends on the instance $\mathfrak{a}$. Therefore, a new S-unit group needs to be calculated for each instance, which makes the repetition of multiple instances of Search-PIP more expensive in practice than multiple instances of the decisional PIP.

Given the input ideal $\mathfrak{a}$, we first enumerate $\alpha \in \mathfrak{a}$ that are small combinations of an LLL-reduced basis of $\mathfrak{a}$ until $(\alpha)/\mathfrak{a} = \mathfrak{p}$ a prime ideal. Then let $S = \{\mathfrak{p}^\sigma \text{ for } \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}$. Compute a generating set $\alpha_1, \ldots \alpha_{r+s}$ of the S-unit group modulo torsion using the recursive technique based on norm relations of [14], where r is the rank of $\mathcal{O}_K^\times$ and $s = |S|$, together with vectors $\vec{v}_1, \ldots, \vec{v}_{r+s} \in \mathbb{Z}^s$ describing the finite valuations of the α_i. Solve a linear system to find $\vec{x} \in \mathbb{Z}^{r+s}$ such that $\sum_i x_i \vec{v}_i$ is the vector with zeros everywhere except for a 1 in the entry corresponding to $\mathfrak{p}$. Then $\prod_i \alpha_i^{x_i}$ is a generator of $\mathfrak{p}$, and $g = \alpha \cdot \prod_i \alpha_i^{-x_i}$ is a generator of $\mathfrak{a}$.

Algorithm 6 PIP using S-units

```
Require: $\mathfrak{a} \subseteq \mathcal{O}_K$ principal.
Ensure: A generator $g \in \mathcal{O}_K$ of $\mathfrak{a}$
$B \leftarrow$ LLL-reduced basis of $\mathfrak{a}$, $\alpha \xleftarrow{\mathcal{R}} \mathrm{Span}(B)$.
while $(\alpha)/\mathfrak{a}$ is not prime do
    $\alpha \xleftarrow{\mathcal{R}} \mathrm{Span}(B)$.
end while
$S \leftarrow \{\mathfrak{p}^\sigma$ for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})\}$ with $\mathfrak{p}_1 = \mathfrak{p}$.
Find generators $(\alpha_i)_{s+r}$ of the $S$-unit group modulo torsion using [14, Alg. 4.16].
Let $M \in \mathbb{Z}^{(r+s)\times s}$ such that row $i$ is the valuations of $\alpha_i$.
Solve $\vec{x} \cdot M = \vec{y}$ for $\vec{y} = (1, 0, \ldots, 0)$.
return $\alpha \cdot \prod_i \alpha_i^{-x_i}$
```

7 COMPUTING THE MINUS PART OF $\mathrm{Cl}(\mathcal{O}_K)$

The computation of the minus part of the class group is an essential building block of Step (2) of Section 3.2. In essence, we need to compute the kernel of the map $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_{K^+})$ given by

$$[\mathfrak{a}] \mapsto \left[\mathrm{N}_{K/K^+}(\mathfrak{a})\right].$$

Let $\mathfrak{g}_1, \ldots, \mathfrak{g}_k$ be such that $\mathrm{Cl}(\mathcal{O}_K) = \langle[\mathfrak{g}_1]\rangle \times \cdots \times \langle[\mathfrak{g}_k]\rangle$, and $\mathfrak{g}'_1, \ldots, \mathfrak{g}'_l$ be such that $\mathrm{Cl}(\mathcal{O}_{K^+}) = \langle[\mathfrak{g}'_1]\rangle \times \cdots \times \langle[\mathfrak{g}'_l]\rangle$. We could compute our norm map by decomposing each $\mathrm{N}_{K/K^+}(\mathfrak{g}_i)$ with respect to the $\mathfrak{g}'_j$ in $\mathrm{Cl}(\mathcal{O}_{K^+})$, however, we only know the $\mathfrak{g}_i$ in a product representation from the primes in $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ that generate $\mathrm{Cl}(\mathcal{O}_K)$. Evaluating these products would be costly. Instead, it is easier to decompose each $\mathrm{N}_{K/K^+}(\mathfrak{p}_i)$ with respect to the $\mathfrak{g}'_j$ in $\mathrm{Cl}(\mathcal{O}_{K^+})$. Then, since we know how to express each $\mathfrak{g}_i$ with respect to the primes in S, this allows us to associate with each $\mathrm{N}_{K/K^+}(\mathfrak{g}_i)$ a vector $\vec{x} \in \mathbb{Z}/d'_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d'_l\mathbb{Z}$ that corresponds to the exponents of the decomposition of $\mathrm{N}_{K/K^+}(\mathfrak{g}_i)$. Therefore, we get a map

$$\varphi : \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \to \mathbb{Z}/d'_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d'_l\mathbb{Z}$$

whose kernel is isomorphic to $\mathrm{Cl}^-(\mathcal{O}_K)$. We summarize this procedure in Algorithm 7.

Under the Generalized Riemann Hypothesis, there is a polynomial size set S of prime ideals that generate the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$, namely $S := \{\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq 12\log^2 |\Delta_K|\}$, where Δ_K is the discriminant of K (see [4]). We refer to this bound on the norm of the prime ideals as Bach's bound. While this means that Steps (1) and (2) of Algorithm 7 are asymptotically efficient, one can hope to find generating sets of size at most $O(\log |\Delta_K|)$. However, the effort required might be commensurate with that of computing the ideal class group. A method for class group computations using norm relations is described in [14, Alg. 4.23]. A byproduct of this algorithm is a set of primes

S that generate the ideal class group. In a nutshell, it uses the fact that when K admits a norm relation of the form (3), the group $\mathrm{Cl}(\mathcal{O}_K) \otimes \mathbb{Z}[1/d]$ is isomorphic to a direct summand of $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(\mathcal{O}_{K_i}) \otimes \mathbb{Z}[1/d]$, and the group $\mathrm{Cl}(\mathcal{O}_K)/\mathrm{Cl}(\mathcal{O}_K)[d]$ is isomorphic to a subgroup of $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(\mathcal{O}_{K_i})$. This means that a subset of $\mathrm{Cl}(\mathcal{O}_K)$ (namely $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(\mathcal{O}_{K_i}) \otimes \mathbb{Z}[1/d]$) is generated by the prime ideals above the primes that generate the $\mathrm{Cl}(\mathcal{O}_{K_i})$. The rest of the generators are chosen at random (Step (9) of [14, Alg. 4.23]). This probabilistic method relies on subfield computations, and is likely to return a generating set significantly smaller than that obtained from Bach's bound (which is quadratic in $\log(|\Delta_K|)$. Therefore we recommend the use of [14, Alg. 4.23] to perform Steps (1) and (2) of Algorithm 7. Note that there is no direct analogue of [14, Alg. 4.23] to compute the minus part of the class group. Indeed, no formula linking $\mathrm{Cl}^-(\mathcal{O}_K)$ to the minus part of the class groups of the subfields involved in (3) exists, to the best of our knowledge. Therefore, we need to rely on the new ideal decomposition method introduced in Section 5 to perform this task.

Algorithm 7 Minus part of the ideal class group

```
Require: Number field $K$ that admits a norm relation of the form (3).
Ensure: $\mathrm{Cl}^-(\mathcal{O}_K)$.
 1: Compute a set of non-zero primes $S$ that generate $\mathrm{Cl}(\mathcal{O}_K)$ .
 2: Compute a set of non-zero primes $S_+$ that generate $\mathrm{Cl}(\mathcal{O}_{K^+})$ .
 3: Compute a matrix $M$ whose rows are a basis of the relations between $\mathfrak{p}_i$ in $S$.
 4: Compute a matrix $M_+$ whose rows are a basis of the relations between $\mathfrak{q}_j$ in $S_+$.
 5: Compute unimodular matrices $U, V$ such that $UMV = \mathrm{diag}(d_1, \dots, d_k)$.
 6: Compute unimodular matrices $U', V'$ such that $U'M_+V' = \mathrm{diag}(d'_1, \dots, d'_l)$.
 7: for all $\mathfrak{p}_i$ do
 8:     Find $\vec{x_i}$ such that $\mathrm{N}_{K/K^+}(\mathfrak{p}_i) \sim \prod_j \mathfrak{q}_j^{x_{i,j}}$ with Algorithm 3.
 9:     Find $\vec{x'_i}$ such that $\mathrm{N}_{K/K^+}(\mathfrak{p}_i) \sim \prod_j \mathfrak{g}'_j{}^{x'_{i,j}}$ with Algorithm 4.
10: end for
11: for all $\mathfrak{g}_i$ do
12:     Find $\vec{y_i}$ such that $\mathfrak{g}_i \sim \prod_j \mathfrak{p}_j^{y_{i,j}}$ with the inverse of Algorithm 4.
13:     $\vec{y'_i} \leftarrow \sum_j y_{i,j}\vec{x'_j}$ (hence $\mathrm{N}_{K/K^+}(\mathfrak{g}_i) \sim \prod_j \mathfrak{g}'_j{}^{y'_{i,j}}$)
14: end for
15: Let $\varphi$ defined by $(0, \dots, 0, \underbrace{1}_{i}, 0, \dots, 0) \in \prod_j \mathbb{Z}/d_j\mathbb{Z} \mapsto \vec{y'_i} \in \prod_j \mathbb{Z}/d'_j\mathbb{Z}$.
16: return $\ker(\varphi)$.
```

The computation of the minus part of the class group enables Step (2) of Section 3.2 which consists in calculating a generating set of primes for $\mathrm{Cl}^-(\mathcal{O}_K)$ under Conjecture 1. Given the parameters l, B, we construct the set of prime ideals of K whose classes are in the minus part with norm bounded by B, and we repeatedly draw d sets of conjugates until one such subset generates the minus part of the class group. This procedure is summarized in Algorithm 8.

Algorithm 8 Creation of a generating set for $\mathrm{Cl}^-(\mathcal{O}_K)$

```
Require: Integers $l, B > 0$, number field $K$, and a norm relation $d = \sum_i a_i \mathrm{N}_{H_i} b_i$.
Ensure: A set $S = \{\mathfrak{p}_i\}_{i \leq k}$ of prime ideals such that $\forall i$, $[\mathfrak{p}_i] \in \mathrm{Cl}^-(\mathcal{O}_K)$, and the classes of $\mathfrak{p}^\sigma$ for $\sigma \in G$ generate
    $\mathrm{Cl}^-(\mathcal{O}_K)$.
$S_0 \leftarrow \{\}$.
for primes ideal $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) \leq B$ do
    if $\mathrm{N}_{K/K^+}(\mathfrak{p})$ is principal (using Algorithm 5) then
        $S_0 \leftarrow S_0 \cup \{\mathfrak{p}\}$.
    end if
end for
Compute $\mathrm{Cl}^-(\mathcal{O}_K)$ with Algorithm 7.
while true do
    $S \leftarrow d$ elements of $S_0$ chosen uniformly at random. $S' \leftarrow \{\mathfrak{p}^\sigma \mid \sigma \in G, \mathfrak{p} \in S\}$.
    Compute the $S'$-unit group and from the finite valuations of a generating set, deduce $\langle S' \rangle \subseteq \mathrm{Cl}(\mathcal{O}_K)$.
    if $\langle S' \rangle = \mathrm{Cl}^-(\mathcal{O}_K)$, then return $S$.
end while
```

8 ASYMPTOTIC ANALYSIS

In this section, we analyze the asymptotic cost of our classical norm relation based variant of the CDW algorithm for the search of mildly short vectors in ideals of $K = \mathbb{Q}(\zeta_m)$ when K admits a norm relation of the form (3). We show that the cost is dominated (up to polynomial factors) by the cost of S-unit group computation and ideal class decomposition in the subfields involved in (3). Note that unless K is cyclic, which happens e.g. when $m = p^l$ is an odd prime power, there is always a norm relation that we can exploit to lower down the cost of ideal decompositions and computation of $\mathrm{Cl}(\mathcal{O}_K)$ and $\mathrm{Cl}^-(\mathcal{O}_K)$. This results in a practical gain for these tasks in almost all cyclotomic fields. Additionally, we also observe asymptotic gains over the BKZ algorithm when the degrees of the fields involved in the norm relation (3) are significantly smaller than $n = [K : \mathbb{Q}]$. In particular, we exhibit an infinite family of cyclotomic fields for which the search for mildly short vectors has asymptotic cost $2^{n^{o(1)}}$, which is a superpolynomial improvement over the cost of the BKZ reduction, which is in $2^{O(\sqrt{n})}$.

8.1 REDUCTION TO SUBFIELD COSTS

The building blocks presented in the previous sections are all that is needed to classically implement the CDW search for mildly short vectors. For the sake of clarity, we recall the entire procedure in Algorithm 9.

Algorithm 9 Classical CDW search for mildly short vectors from norm relations

```
Require: Number field $K = \mathbb{Q}(\zeta_m)$ that admits a norm relation of the form (3). Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$.
Ensure: A mildly short vector of $\mathfrak{a}$.
 1: Let $S = \{\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq 12\log^2|\Delta_K|\}$ (i.e. $S$ generates $\mathrm{Cl}(\mathcal{O}_K)$ under GRH).
 2: while true do
 3:     Draw a random short product $\prod_i \mathfrak{p}_i^{x_i}$ of elements in $S$.
 4:     if $\mathrm{N}_{K/K^+}\left(\mathfrak{a}\prod_i \mathfrak{p}_i^{x_i}\right)$ is principal (with Algorithm 5) then $\mathfrak{a}_0 \leftarrow \mathfrak{a}\prod_i \mathfrak{p}_i^{x_i}$. break
 5: end while
 6: Compute a generating set of primes $S' = \{\mathfrak{p}_i\}_{i\leq s}$ of $\mathrm{Cl}^-(\mathcal{O}_K)$ with Algorithm 8.
 7: Find $\vec{x}$ such that $\mathfrak{a}_0 \sim \prod_i \mathfrak{p}_i^{x_i}$ with Algorithm 3 (on input $S'$).
 8: Use $\vec{x}$ to derive $\mathfrak{b}$ with $\mathrm{N}(\mathfrak{b}) \in 2^{\tilde{O}(n^{3/2})}$ with [17, Alg. 4].
 9: Find a generator $\alpha$ of $\mathfrak{a}_0\mathfrak{b}$ with Algorithm 6.
10: Use Algorithm 1 to derive a short generator $\alpha'$ of $\mathfrak{a}_0\mathfrak{b}$.
11: return $\alpha'$.
```

Proposition 4. *Under Conjecture 1, Conjecture 2, and GRH, the cost of Algorithm 9 is in*

$$\mathrm{Poly}([K : \mathbb{Q}], \log \mathrm{N}(\mathfrak{a}), l, \max_i \log a_i)\ (\mathrm{Cost}_{S\text{-}unit}(subfields) + \mathrm{Cost}_{Ideal\ Dec}(subfields)),$$

where $\mathrm{Cost}_{S\text{-}unit}(subfields)$ *is the cost of computing S-units in the subfields involved in the norm relation* (3)*, and* $\mathrm{Cost}_{Ideal\ Dec}(subfields)$ *is the cost of Algorithm 2 in the subfields involved in the norm relation* (3)*.*

Proof. The random walk in Steps (2) to (5) of Algorithm 9 takes time in $O\left(h_K^+ \cdot \mathrm{Poly}(m, \log(\mathrm{N}(\mathfrak{a}))) \cdot \mathrm{Cost}(\mathrm{PIP})\right)$. Under Conjecture 2, h_K^+ is polynomial, and the cost of the decisional PIP is that of Algorithm 2 (up to polynomial factors). The cost of Algorithm 8 requires the computation of S-units (through Steps (3)-(4) of Algorithm 7, and Step (11) of Algorithm 8). It also requires ideal decompositions from Algorithm 2. Then Step (7) is another decomposition with Algorithm 2. Step (8) has an efficient solution from [17, Alg. 3], as well as Step (10) (with Algorithm 1). Finally, the resolution of Search-PIP with Algorithm 6 reduces to the computation of S-units (Steps (2)-(3) of Algorithm 6 find an α with $(\alpha)/\mathfrak{a}$ prime in polynomial time). Hence, up to polynomial factors, the cost of Algorithm 9 is that of

- the computation of S-units and,
- the decomposition of the ideal class of an ideal according to a set of primes.

The computation of the S-unit group of K from the S-unit groups of the subfields involved in the norm relation relation (3) is shown to take (up to polynomial factors) the same cost as that of computing the S-unit groups of subfields [14, Th. 4.8]. On the other hand, the decomposition of the ideal class of an ideal according to a set of primes itself requires an S-unit group computation. Additionally, we need decompositions of ideals in the subfields involved in the norm relation. Note that d-th roots can be efficiently calculated as long as we maintain a so-called *compact representation* of the input elements, that is, a representation of the form $\alpha = \prod_i \alpha_i^{d^i}$ where each α_i has polynomial size. These compact representations are efficiently computable as long as we know the prime decomposition of the input α, which is the case for all our subroutines, see [20]. Therefore, the cost of

Algorithm 9 (up to polynomial factors), is that of S-unit group calculations and ideal class decompositions in the subfields involved in the norm relation. □

The cost of S-unit group computation and ideal class decomposition in subfields derives from the heuristic subexponential methods of Biasse and Fieker [10]. More specifically, the subexponential methods of [9, 10] allow us to compute S-unit groups for S a generating set of the class group, compute ideal class decompositions, and to solve the PIP. Combined with Simon's work [43], this also allows the computation of S-unit groups for arbitrary sets S.

Lemma 2. *Let K be a cyclotomic field of degree n, $\mathfrak{a}$ be an ideal of K and S be a set of prime ideals of K. Then, under the heuristics of [10]:*

- *The computation of the S-unit group takes time in* $\mathrm{Poly}(\max_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p}), |S|)2^{\tilde{O}(n^{2/3})}$.
- *The resolution of the PIP on input $\mathfrak{a}$ takes time i n* $\mathrm{Poly}(\log \mathrm{N}(\mathfrak{a}))2^{\tilde{O}(n^{2/3})}$

So far, our cost analysis takes the norm relation (3) as input. Fortunately, we know an efficient method from [14] to derive norm relations.

Proposition 5. *Let K be an abelian number field of degree n and Galois group $G = C \times Q$ where C is the maximal cyclic subgroup of G and Q is non trivial. Then Algorithm 10 is correct, runs in polynomial time, and returns a norm relation $d = \sum_{i\leq l} a_i \mathrm{N}_{H_i}$ with $a_i \in \mathbb{Z}$ and that satisfies $d, l, |a_i| \leq n$, and* $\max_i [K^{H_i} : \mathbb{Q}] \leq |C|$.

Proof. The number of subgroups H_i is less than $|\hat{G}| = n$. The computation of the n_i/d_i requires the factorization of n which is polynomial in $\log |\Delta_K|$. For all subgroups H_i with cyclic quotient we have $|G/H_i| \mid |C|$, which proves the bound on the degrees of the K^{H_i}. Finally, the bound on (a_i) and d comes from $\mu(x) \in \{-1, 0, 1\}$ and [14, Prop. 2.26 (3)]. □

Algorithm 10 Norm relation with minimal subfields (abelian case)

```
Require: Non-cyclic abelian number field $K$ with Galois group $G$.
Ensure: Subgroups $(H_i)_{i\leq l}$ of $G$, integers $(a_i)_{i\leq l}$, $d > 0$, with $d = \sum_i a_i \mathrm{N}_{H_i}$.
$\hat{G} \leftarrow$ dual of $G$, $\mathcal{H} \leftarrow \{H \leq G$ with $G/H$ cyclic$\}$.
for $H_i \in \mathcal{H}$ do
    $C \subseteq \hat{G} \leftarrow \langle \chi \rangle$ where $H_i = \ker(\chi)$.
    $\frac{n_i}{d_i} \leftarrow \frac{1}{|\ker \chi|} \sum_{C \leq C' \leq \hat{G} \text{ cyclic}} \mu([C' : C])$ where $\mu$ is the Möbius function.
end for
Find minimal $(a_i), d$ such that $d = \sum_i a_i \mathrm{N}_{H_i} \Leftrightarrow 1 = \sum_i \frac{n_i}{d_i} \mathrm{N}_{H_i}$.
return $\mathcal{H}, (a_i), d$.
```

We will use the following lemma. For cyclotomic fields, the Carmichael function gives us the size of the largest cyclic factor of the Galois group, which in turns yields the degree of the largest subfield occurring in a norm relation found with Algorithm 10.

Lemma 3. *Let $m > 0$ and $K = \mathbb{Q}(\zeta_m)$, Algorithm 10 finds a norm relation $d = \sum_{i\leq l} a_i \mathrm{N}_{H_i}$ in polynomial time where $l, d, a_i \leq \varphi(m)$ and for all i we have $[K^{H_i} : \mathbb{Q}] \leq \lambda(m)$ where $\lambda(m)$ is the Carmichael function.*

Proof. We apply Proposition 5 and use the fact that $\lambda(m) = |C|$. □

Unfortunately, the Carmichael function oscillates a lot, so there is no simple function f yielding a useful bound $\lambda(m) \leq f(m)$. We can however make the following statement conditional on the size of $\lambda(m)$ relative to $\varphi(m)$.

Proposition 6. *Assume the heuristics of [10], as well as Conjecture1, and Conjecture 2. Let $a > 0$ and $(m_k)_{k\in\mathbb{Z}_{>0}}$ be a sequence of integers satisfying $\lambda(m_k) \leq \varphi(m_k)^a$ for all k. Then Algorithm 9 applied to the infinite family of fields $K_k := \mathbb{Q}(\zeta_{m_k})$ has asymptotic complexity*

$$\mathrm{Poly}(\log(\mathrm{N}(\mathfrak{a}))) \cdot 2^{\tilde{O}\left([K_k:\mathbb{Q}]^{2a/3}\right)}.$$

Proof. By Lemma 3 the largest degree of a subfield occurring in the norm relation is $\lambda(m_k) \leq \varphi(m_k)^a$. The main term of the complexity of the subfield operations is $2^{\tilde{O}((\log |\Delta_i|)^{2/3})}$, and by Lemma 4

$$(\log |\Delta_i|)^{2/3} \leq \left(\frac{n_i}{n} \log |\Delta|\right)^{2/3} \in \tilde{O}(n_i^{2/3}) = \tilde{O}(n^{2a/3}),$$

where Δ is the discriminant of K_k, n is its degree, and $n_i = \lambda(m_k)$ is the largest degree of a subfield occurring in the norm relation. This proves our complexity bound. □

Lemma 4. *Let $m \geq 2$, $K = \mathbb{Q}(\zeta_m)$ and $L \subset K$ a subfield. Let $n = [K : \mathbb{Q}]$ and $n' = [L : \mathbb{Q}]$. We have*

1. $|\Delta_L| \leq |\Delta_K|^{n'/n}$.
2. $\log(n) = \log(m) + O(\log\log(m))$ *and* $\log(m) = \log(n) + O(\log\log(n))$.
3. $\log|\Delta_K| = n\left(\log(n) + O(\log\log(n))^2\right)$.

Proof. The first inequality derives directly from the fact that the discriminants satisfy $\Delta_K = \mathrm{N}_{L/\mathbb{Q}}(\Delta_{K/L})\Delta_L^{[K:L]}$ where $\Delta_{K/L}$ is the relative discriminant between K and L. Since K is a cyclotomic field, we have

$$\Delta_K = (-1)^{\varphi(m)/2}\frac{m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}},$$

so $\log|\Delta_K| = \varphi(m)\left(\log(m) - \sum_{p|m}\frac{\log(p)}{p-1}\right)$. Let $d \leq \log_2(m)$ be the number of distinct prime divisors of m:

$$\begin{aligned}
&\sum_{p|m}\frac{\log(p)}{p-1} = \sum_{p|m}\frac{\log(p)}{p} + \sum_{p|m}\frac{\log(p)}{p^2-p}\\
&= \sum_{p|m}\frac{\log(p)}{p} + O(1)\\
&\leq \sum_{k=3}^{d+2}\frac{\log(k)}{k} + O(1) \text{ since } t \mapsto \frac{\log(t)}{t} \text{ is decreasing on } [3,\infty)\\
&\leq \int_1^{\log_2(m)}\frac{\log(t)}{t}dt + O(1)\\
&= O(\log\log(m))^2.
\end{aligned}$$

Moreover we have

$$\begin{aligned}
\log(n) &= \log(\varphi(m))\\
&= \log(m) + \sum_{p|m}\log\left(1 - \frac{1}{p}\right)\\
&= \log(m) - \sum_{p|m}\frac{1}{p} + O(1)\\
&= \log(m) + O(\log\log(m)) \text{ by the same argument as above,}
\end{aligned}$$

and therefore $\log(m) = \log(n) + O(\log\log(n))$. This gives

$$\log|\Delta_K| = \varphi(m)\left(\log(m) + O(\log\log(m))^2\right) = n\left(\log(n) + O(\log\log(n))^2\right),$$

as claimed. □

In families of fields for which $a < 3/4$, the above proposition shows how to find mildly short vectors with a superpolynomial improvement over the complexity of BKZ which is in $2^{\tilde{O}(\sqrt{n})}$ for $n = [K : \mathbb{Q}]$. Of course, not all infinite sequences of numbers m_k satisfy $\lambda(m_k) \leq \varphi(m_k)^a$ for an $a < 3/4$. In fact, according to [19, Th. 2], a density 1 subset of $\mathbb{Z}_{>0}$ satisfies $\lambda(n) \in \tilde{\Omega}(n)$, meaning that infinite families for which $a < 3/4$ must have negligible density. However, as we see in Table 1, in the practical range ($n < 100,000$), a significant fraction of n satisfies $\lambda(n) < \varphi(n)^a$ for $a < 3/4$.

$n < N$	$\frac{\log(\lambda(n))}{\log(\varphi(n))} < 3/8$	$\frac{\log(\lambda(n))}{\log(\varphi(n))} < 1/2$	$\frac{\log(\lambda(n))}{\log(\varphi(n))} < 5/8$	$\frac{\log(\lambda(n))}{\log(\varphi(n))} < 3/4$
1000	0.300%	2.000%	11.70%	30.20%
10000	0.180%	1.780%	10.42%	29.45%
100000	0.092%	1.580%	8.830%	26.32%

Table 1: Proportion of n with low $\lambda(n)$ in the practical range

8.2 AN EXAMPLE OF WEAK FAMILIES OF CYCLOTOMIC FIELDS

We construct an infinite family of conductors with small Carmichael numbers by using the following theorem of Erdös, Pomerance and Schmutz.

Theorem 4 (Erdös–Pomerance–Schmutz [19, Theorem 1 part 2])**.** *There exists an infinite sequence $m_1 < m_2 < \cdots$ of positive integers such that*

$$\lambda(m_k) = (\log(m_k))^{O(\log\log\log(m_k))}.$$

Remark 1. *Integers as in Theorem 4 are easy to construct in practice, as follows. Let L be a highly divisible number (for instance, take L to be a product of a few small primes). Then let Q be the set of all primes p such that $p - 1$ divides L, and let $m = \prod_{p \in Q} p$. This integer satisfies $\lambda(m) \mid L$, and the proof of Theorem 4 shows that for suitable choices of L, the integer m is much larger than L.*

Example 2. *We illustrate the construction by taking L to be the product of the first prime numbers.*

1. $L = 2 \cdot 3 = 6$, $m = 2 \cdot 3 \cdot 7 = 42$, $\varphi(m) = 12$, $\lambda(m) = 6$.
2. $L = 2 \cdot 3 \cdot 5 = 30$, $m = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 31 = 14322$, $\varphi(m) = 3600$, $\lambda(m) = 30$.
3. $L = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, $m = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 31 \cdot 43 \cdot 71 \cdot 211 = 9225988926$, $\varphi(m) = 2222640000$, $\lambda(m) = 210$.

Theorem 5 (under GRH, Conjecture 1 and 2)**.** *There exists an infinite sequence of integers $m_1 < m_2 < \cdots$ such that Algorithm 9 has complexity*

$$\mathrm{Poly}([K_k : \mathbb{Q}], \log(\mathrm{N}(\mathfrak{a}))) \cdot 2^{(\log(m_k))^{O(\log\log\log(m_k))}}.$$

Proof. Take (m_k) to be the sequence from Theorem 4. Let $m = m_k$ be a term in this sequence, and $K_k = \mathbb{Q}(\zeta_{m_k})$ be the corresponding field. Let D be the maximum absolute value of the discriminant of a subfield used by Algorithm 9 applied to K_k. Then by Lemma 4 we have $D \leq m^{\lambda(m)}$, so that

$$\log(D) \leq \lambda(m)\log(m) = (\log(m))^{O(\log\log\log(m))}$$

by Theorem 4. In particular, using the algorithm of Theorem 6 for the base case, the cost for the subfields is $2^{(\log(D))^{O(1)}} = 2^{(\log(m))^{O(\log\log\log(m))}}$. □

Remark 2. *Let Δ_k be the discriminant of K_k. Then we have $\log(m_k) = O(\log\log|\Delta_k|)$, so that the second term of the complexity is*

$$2^{(\log\log|\Delta_k|)^{O(\log\log\log\log|\Delta_k|)}}.$$

This complexity is not quite quasi-polynomial (which would correspond to $O(1)$ instead of $O(\log\log\log\log|\Delta_k|)$ in the second exponent), but it is strongly subexponential, as can be seen by rewriting it as

$$2^{(\log|\Delta_k|)^{O\left(\frac{\log\log\log\log|\Delta_k|\log\log\log|\Delta_k|}{\log\log|\Delta_k|}\right)}} = 2^{(\log|\Delta_k|)^{o(1)}}.$$

This complexity is in time $2^{n^{o(1)}}$.

9 NUMERICAL RESULTS

Our efforts to implement all algorithms presented in this paper are a significant part of our contribution. More specifically, we propose numerical data to achieve the following goals:

- Support for Conjecture 1 on the generators of the minus part of the class group.
- Support for Conjecture 2 on the size of the ideal class group h^+ of the maximal real subfield.
- Demonstration that Algorithm 9 is practical.

In [16], some justification in support of Conjecture 1 and Conjecture 2 is given. Below, we review existing data in the literature, and we discuss the novelty of the data provided via our techniques based on norm relations.

9.1 NUMERICAL DATA ON h^+ (CONJECTURE 2)

Previous efforts The computation of the “plus part” of the class number of a cyclotomic field has been described as "notoriously hard" [41]. Therefore, little data is available in the literature to support Conjecture 2. Masley [30] used lower discriminant bounds proved by Odlyzko [35] to compute real class numbers. These results, later extended by Van der Linden [27], yielded the unconditional computation of the class numbers of all real cyclotomic fields of composite conductor $m \leq 200$, $\phi(m) \leq 72$ and $m \neq 148, 152$.

However, for fields of larger degree, the root discriminant becomes too large for Masley's method to handle. To overcome the problem of large root discriminant, Miller [31] established a lower bound on sums over prime ideals of Hilbert class field, which in turn establishes an upper bound on the class number. According to [31, Th. 1.1], for a composite integer $m \not\equiv 2 \bmod(4)$, the class number of the maximal real subfield of the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$ is $h_m^+ = 1$ if $\phi(m) \leq 116$ and $m \neq 136, 145, 212$. Also, $h_m^+ = 2$ for $m = 136, 145$ and $h_{256}^+ = 1$. Under the GRH, Miller [31] was able to compute $h_{212}^+ = 5$ and $h_{512}^+ = 1$. The method was later extended to prime conductors in [32]. According to [32, Th. 3.1.1], for a prime number p one has $h_p^+ = 1$ if $p \leq 151$. Under GRH we have $h_p^+ = 1$ for $p \leq 263$ and $p \neq 163, 191, 229, 257$. Also $h_{163}^+ = 4$, $h_{191}^+ = 11$, $h_{229}^+ = 3$, and $h_{257}^+ = 3$.

Tables 4.1 and 4.2 of [32] provide the class numbers of the n-th layers of cyclotomic $\mathbb{Z}_p$-extensions over the rationals implying that $h_{169}^+ = h_{289}^+ = h_{361}^+ = 1$. Also, under GRH $h_{243}^+ = h_{529}^+ = h_{841}^+ = h_{961}^+ = 1$

Great advances in the direction of computing class numbers of real cyclotomic fields were made by Schoof [41] who presented a table of the orders of certain subgroups of the class groups of the real cyclotomic fields for prime conductors less than 10000. Based on the Cohen–Lenstra heuristics, the probability that the main table presented in [41] is actually a table of class numbers is at least 98%. The largest order in this table is 130473 for the prime conductor 8017. So, according to the Schoof's table, with high probability for prime conductor m the class number of the real cyclotomic field is less than $17m$.

Our results Concrete results on h_m^+ (even conditional to GRH) only exist for relatively small degrees, a few sporadic reasonable size degree ($m = 512, 529, 841, 961$), or probabilistically for certain large prime conductors. The methods based on the norm relations presented in this paper allowed us to compute h_m^+ (under the GRH) for many conductors for which this invariant was not known before. What is even more interesting about the numerical data we provide is that our methods perform better for highly composite conductors, which are the opposite of the prime conductors for which some probabilistic data is already available. All in all, we were able to compute 149 values of h_m^+ that were not previously known in the literature. We reached a maximum conductor of 2730. Our data supports Conjecture 2 which stipulates that h_m^+ has moderate size. Besides the support of the CDW heuristics, this data is interesting in its own rights. Given the large number of values of h_m^+ we calculated, we chose to disseminate the data on a dedicated webpage: `https://www.cyclodb.org/` which, to this day, contains 362 values, including the 149 that were not previously known. Note that each entry of the database contains $\mathrm{Cl}(O_K)$, h_m, the factorization of h_m, h_m^-, h_m^+, and the regulator of the field. We will continue populating it in the future as this data is of general interest.

9.2 NUMERICAL DATA ON $\mathrm{Cl}^-(O_K)$ (CONJECTURE 1)

Previous efforts Conjecture 1 is an ad-hoc assumption made for the first time in [16] that was not previously studied in the literature. In some sense, the numerical data we provide in this section is the first to ever put Conjecture 1 to the test strictly speaking. However, the authors of [16, 17] presented a rationale to justify Conjecture 1 based on existing numerical data. In [17, Prop. 6.1], it is proven that if a number s satisfies $s \geq r\left(\log\log_2(h^-) + \alpha\right)$ for a parameter $\alpha \geq 1$ and r the the number of $\mathbb{Z}[G]$-generators of $\mathrm{Cl}^-(O_K)$, then the probability that s elements of $\mathrm{Cl}^-(O_K)$ drawn uniformly at random generates $\mathrm{Cl}^-(O_K)$ is at least $1 - O(2^{-\alpha})$. This means that if we know that the number of (not necessarily prime) generators of $\mathrm{Cl}^-(O_K)$ is small, then on average few random elements are required to generate $\mathrm{Cl}^-(O_K)$. The purpose of [17, Prop. 6.1] is to relate Conjecture 1 with existing numerical data from the literature which concerns the number of generators of $\mathrm{Cl}^-(O_K)$ rather than the number of prime generators of $\mathrm{Cl}^-(O_K)$ (which is what is needed in Conjecture 1). However, to justify Conjecture 1 from [17, Prop. 6.1], one needs to make the extra unproven assumption that [17, Prop. 6.1] is still true even if we draw s short prime elements (as opposed to elements chosen uniformly at random). This extra heuristic seems reasonable, but it means that numerical results on the number of generators of $\mathrm{Cl}^-(O_K)$ do not, on its own, directly support Conjecture 1.

Below, we recall known results on $\mathrm{Cl}^-(O_K)$. Most of the existing literature concerns its cardinality h^-, but not the structure itself. Motivated by the results on divisibility properties of class numbers of cyclotomic fields, Kummer [24] was the first to carry out computations of relative class numbers of cyclotomic fields of prime conductor, for primes below 163. These calculations were extended by Lehmer and Masley [30] in 1978 to the primes $p \leq 509$. According to these results, h_p^- grows rapidly with p. For instance, h_{491}^- already has 138 decimal digits. Later, Fung, Granville and Williams [22] computed all h_p^- for $p \leq 3000$. Then, Shokrollahi [42] extended this result to all $p \leq 10000$.

Regarding the structure of the minus part, in [24], Kummer proved that $\mathrm{Cl}^-(O_{\mathbb{Q}(\zeta_p)})$ is cyclic for every prime $p \leq 100$ and $p \neq 29, 41$. Furthermore, $\mathrm{Cl}^-(O_{\mathbb{Q}(\zeta_{29})})$ and $\mathrm{Cl}^-(O_{\mathbb{Q}(\zeta_{41})})$ are abelian groups of type $(2, 2, 2)$ and $(11, 11)$ respectively. Subsequently, Kummer's methods were refined by Tateyama [44], Horie and Ogura [23] and many other authors. Tateyama was able to compute the structure of $\mathrm{Cl}^-(O_{\mathbb{Q}(\zeta_p)})$ for prime numbers p smaller than 227 except for seven cases. Horie and Ogura determined the structure of the minus part of any cyclotomic field with conductor less than 100. Later, Schoof [40] determined the structure of $\mathrm{Cl}^-(O_{\mathbb{Q}(\zeta_p)})$ for $l \leq 509$. As an example, Schoof showed that $\mathrm{Cl}^-(\mathcal{O}_{\mathbb{Q}(\zeta_{491})})$ is isomorphic to a product of 6 cyclic groups. Also, Theorem 3 of [40] roughly states that for prime divisors p of $\ell - 1$, the p-part of $\mathrm{Cl}^-(\mathcal{O}_{\mathbb{Q}(\zeta_\ell)})$ is cyclic whenever it is small.

Our results We present the first experiments that directly test the validity of Conjecture 1 without relying on extra assumptions. Additionally, similar to the case of the provision of numerical data on h^+, our methods work for non-cyclic cyclotomic fields, which makes them valuable since all previous data used to justify Conjecture 1 was restricted to prime conductors. The results of our experiments are presented in Table 2. For each conductor m for which we tested Conjecture 1, we found the minimum B and d for which we could generate $\mathrm{Cl}^-(\mathcal{O}_K)$. Then we repeated 100 time the following experiment: draw d prime ideals of norm less than B uniformly at random, and check whether their conjugates generate $\mathrm{Cl}^-(\mathcal{O}_K)$. We report the corresponding probability. We also report the runtime of the computation of $\mathrm{Cl}^-(\mathcal{O}_K)$ in CPU hours, which is of independent interest. Conjecture 1 is of asymptotic nature, and hence difficult to justify with a finite number of experiments, but the results of Table 2 are clearly consistent with the prediction of a moderate B and d with a high probability of generating $\mathrm{Cl}^-(\mathcal{O}_K)$.

9.3 TIMINGS OF THE SUBFIELD VARIANT OF CDW

In Table 9.3, we report timings of our implementation of Algorithm 9, i.e. our subfield variant of the CDW method for the computation of mildly short vectors. We selected fields with conductor m ranging between $m = 46$ and $m = 154$. For each field, we report "lb N", the bit size of the algebraic norm of the input ideal, "lb $\mathrm{N}_{\mathrm{svp}}$", the bit size of the algebraic norm of the short generator of the principal ideal found in Step (10) of Algorithm 9, "t_{gen}", the time to find a generating set for $\mathrm{Cl}^-(\mathcal{O}_K)$ (Step (6) of Algorithm 9), "t_{cpm}", the time to solve the Close Principal Multiple problem, and "t_{svp}", the time to find the short generator of Step (10). Timings are reported in CPU seconds unless otherwise stated.

10 CONCLUSION

We have presented a classical variant of the CDW algorithm that uses norm relations from [14] to reduce the computations to subfields of cyclotomic fields of conductor $m \neq 2, 4, p^k, 2p^k$ for $p \neq 2$ (i.e., a density 1 subset of the conductors). Of independent interest, we have provided an algorithm to compute the minus part of the ideal class group from subfield information in Galois number fields admitting a norm relation. We used our recursive methods to provide numerical evidence in support of the conjectures made in the original CDW paper [16].

Our asymptotic results show that our methods can outperform the BKZ reduction method in certain families of cyclotomic number fields. Our numerical experiments provided new insight on h^+ and on the structure of $\mathrm{Cl}^-(\mathcal{O}_K)$ that was not previously available. They also demonstrated the practicality of our CDW variant. We are however not able to reach higher dimensions than BKZ at the moment. This is due to the fact that certain subroutines need to be optimized to fully leverage the potential of norm relations. Indeed, S-unit group computations are particularly difficult to perform recursively in practice due to the presence of many root calculations which require compact representations of the input. While this step runs in polynomial time, its practical implementation is currently the bottleneck of our methods. This is in particular the reason why no S-units, or solutions to the PIP were calculated in [14] where the norm relation techniques were originally described. Instead, only certain class groups calculations that avoid d-th root calculations altogether were presented.

However, the new mathematical approach for computing mildly short vectors we presented in this paper clearly shows future promise. In addition, once the root computation is optimized, the norm relations methods will allow the computation of S-unit groups for large sets S in large degree number fields. Beyond the impact on the CDW methods presented in this paper, this will also allow the provision of numerical data on the performance of the PHS method [36, 6] and its conjectured improvements [8]. This will be a crucial tool to contribute to the debate on the potential of the so-called "S-unit attacks".

ACKNOWLEDGMENT

This work was supported by Project B2 of SFB-TRR 195 "Symbolic Tools in Mathematics and their Application" of the German Research Foundation (DFG), and project 1846166 "CAREER: Algebraic Methods for the Computation of Approximate Short Vectors in Ideal Lattices" of the National Science Foundation (NSF).

Table 2: Experiments on $\mathrm{Cl}^-(\mathcal{O}_K)$

m	n	$\mathrm{Cl}^-(\mathcal{O}_K)$	B	d	prob.	time
23	22	[3]	47	2	100.0	0.01
46	22	[3]	47	2	100.0	0.01
39	24	[2]	13	1	100.0	0.01
52	24	[3]	13	1	100.0	0.01
56	24	[2]	8	1	100.0	0.01
72	24	[3]	9	1	100.0	0.01
78	24	[2]	13	1	100.0	0.01
29	28	[2, 2, 2]	59	2	100.0	0.01
58	28	[2, 2, 2]	59	2	100.0	0.01
31	30	[9]	32	2	100.0	0.01
62	30	[9]	32	2	100.0	0.01
51	32	[5]	103	1	100.0	0.01
64	32	[17]	193	2	100.0	0.01
68	32	[8]	137	2	100.0	0.02
96	32	[3, 3]	97	2	100.0	0.01
102	32	[5]	103	1	100.0	0.01
37	36	[37]	149	2	100.0	0.01
57	36	[9]	229	2	100.0	0.01
63	36	[7]	64	1	100.0	0.01
74	36	[37]	149	2	100.0	0.01
76	36	[19]	229	1	100.0	0.01
108	36	[19]	109	2	100.0	0.01
114	36	[9]	229	2	100.0	0.01
126	36	[7]	64	1	100.0	0.01
41	40	[11, 11]	83	2	100.0	0.01
55	40	[10]	11	1	100.0	0.03
75	40	[11]	151	2	100.0	0.01
82	40	[11, 11]	83	2	100.0	0.01
88	40	[55]	89	1	100.0	0.02
100	40	[55]	101	2	100.0	0.02
110	40	[10]	11	1	100.0	0.03
132	40	[11]	397	2	100.0	0.01
150	40	[11]	151	2	100.0	0.01
43	42	[211]	173	2	100.0	0.04
49	42	[43]	197	2	100.0	0.02
86	42	[211]	173	2	100.0	0.04
98	42	[43]	197	2	100.0	0.03
69	44	[69]	139	1	100.0	0.02
92	44	[201]	277	1	100.0	0.02
138	44	[69]	139	1	100.0	0.02
47	46	[695]	283	2	100.0	0.13
94	46	[695]	283	2	100.0	0.17
65	48	[2, 2, 4, 4]	131	1	100.0	0.18
105	48	[13]	211	1	100.0	0.02
112	48	[3, 156]	113	3	100.0	0.22
130	48	[2, 2, 4, 4]	131	1	100.0	0.18
144	48	[13, 39]	433	4	100.0	0.05
53	52	[4889]	107	2	100.0	0.24
106	52	[4889]	107	2	100.0	0.24
81	54	[2593]	163	2	100.0	0.46
162	54	[2593]	163	2	100.0	0.34
87	56	[8, 8, 24]	523	2	100.0	0.4
116	56	[8, 8, 168]	233	2	100.0	0.33
174	56	[8, 8, 24]	523	2	100.0	0.38
59	58	[41241]	709	2	100.0	3.39
118	58	[41241]	709	2	100.0	2.65
61	60	[76301]	367	2	100.0	4.90
77	60	[4, 4, 4, 20]	463	1	100.0	0.29
93	60	[6795]	373	2	100.0	0.09
99	60	[31, 93]	199	1	100.0	0.12
122	60	[76301]	367	2	100.0	6.34
124	60	[2, 22878]	373	3	100.0	0.33
154	60	[4, 4, 4, 20]	463	1	100.0	0.31
186	60	[6795]	373	2	100.0	0.08
85	64	[6205]	1021	2	100.0	0.14
170	64	[6205]	1021	2	100.0	0.12
192	64	[3, 20451]	193	2	100.0	1.78
91	72	[4, 13468]	547	2	100.0	0.07
95	72	[107692]	571	2	98.0	2.74
135	72	[75961]	271	2	100.0	0.94
148	72	[4827501]	593	3	100.0	0.51
152	72	[19, 171, 513]	457	2	100.0	0.51
190	72	[107692]	571	2	96.0	2.54
123	80	[8, 8, 88, 1496]	739	1	100.0	5.16
164	80	[11, 7528840]	821	2	100.0	14.43
165	80	[92620]	331	2	100.0	7.16
176	80	[5, 5874275]	353	1	100.0	5.27
147	84	[5874617]	883	2	100.0	2.23
189	108	[105778197511]	379	1	100.0	2.60

Table 3: Computation of mildly short vectors with our subfield CDW variant.

m	n	lb N	lb N$_{\text{svp}}$	t_{cpm}	t_{pip}	t_{svp}	m	n	lb N	lb N$_{\text{svp}}$	t_{cpm}	t_{pip}	t_{svp}
23	22	51	68	3.05	0.01	0.98	43	42	52	82	4.18	0.15	1.09
46	22	55	72	3.06	0.01	1.04	49	42	58	73	1.01	0.14	1.35
39	24	46	49	1.44	0.01	0.89	86	42	57	105	3.74	0.17	1.03
52	24	52	56	1.17	0.01	0.96	98	42	55	88	3.22	0.1	0.99
56	24	53	56	1.14	0.01	0.92	69	44	54	78	6.08	0.1	0.77
72	24	58	68	3.23	0.01	0.68	92	44	52	94	479.72	0.12	0.71
78	24	52	56	1.22	0.01	0.72	138	44	54	78	5.62	15.1	1.28
29	28	54	77	2.96	0.03	1.22	47	46	55	100	3.26	0.29	1.14
58	28	53	75	2.81	0.02	1.01	94	46	50	104	6.21	0.19	1.12
31	30	56	66	1.04	0.03	1.00	65	48	53	152	1342.92	57.64	1.37
62	30	58	79	2.57	0.03	0.84	112	48	51	264	1894.87	45.02	1.14
51	32	55	62	1.48	0.03	0.92	144	48	53	175	1988.98	71.09	1.58
64	32	56	81	3.51	0.05	1.27	87	56	52	139	5.79	73.53	1.49
68	32	56	172	289.47	0.08	0.7	116	56	56	294	1644.03	81.35	2.07
96	32	53	79	4.14	0.03	0.73	174	56	59	153	7.13	66.76	1.81
102	32	60	73	3.82	0.03	0.69	77	60	56	243	1496.5	69.37	1.30
37	36	52	78	3.15	0.05	1.01	93	60	50	133	7.68	101.88	2.13
57	36	46	70	3.69	0.05	1.12	99	60	55	124	6.76	78.57	1.29
63	36	51	63	4.06	0.04	0.73	124	60	48	147	5.70	124.02	2.25
74	36	55	81	3.29	0.05	0.98	186	60	57	140	7.33	0.47	1.57
76	36	47	80	202.89	0.05	1.10	85	64	58	155	8.17	1023.02	9.26
108	36	59	83	3.90	0.07	0.76	192	64	51	131	6.75	1117.83	16.92
114	36	55	83	4.41	0.06	0.90	91	72	51	137	10.63	73.88	2.60
41	40	57	92	2.78	0.08	1.26	95	72	53	139	8.14	528.04	3.21
55	40	52	69	4.01	0.07	0.81	135	72	52	136	8.50	503.78	3.62
75	40	57	71	1.94	0.07	0.83	148	72	54	160	7.24	368.24	3.45
82	40	55	86	3.39	0.09	1.45	152	72	57	148	6.18	950.51	9.39
88	40	55	75	3.96	0.06	0.73	123	80	54	127	12.38	1834.57	11.32
100	40	58	97	416.62	0.11	0.69	164	80	58	153	11.35	1897.85	9.99
150	40	55	79	4.59	0.07	0.90	176	80	55	126	14.97	5500.97	39.56

REFERENCES

[1] L. M. Adleman. “Factoring Numbers Using Singular Integers”. In: *Proceedings of STOC ’91*. 1991, pp. 64–71.

[2] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. “A sieve algorithm for the shortest lattice vector problem”. In: *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*. Ed. by Jeffrey Scott Vitter, Paul G. Spirakis, and Mihalis Yannakakis. ACM, 2001, pp. 601–610. DOI: 10.1145/380752.380857. URL: https://doi.org/10.1145/380752.380857.

[3] E. Artin and J. Tate. *Class field theory*. Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009, pp. viii+194. ISBN: 978-0-8218-4426-7.

[4] E. Bach. “Explicit bounds for primality testing and related problems”. In: *Math. Comp.* 55.191 (1990), pp. 355–380.

[5] J. Bauch et al. “Short Generators Without Quantum Computers: The Case of Multiquadratics”. In: *Proceedings of EUROCRYPT 2017*. 2017, pp. 27–59. DOI: 10.1007/978-3-319-56620-7_2. URL: https://doi.org/10.1007/978-3-319-56620-7%5C_2.

[6] O. Bernard and A. Roux-Langlois. “Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices”. In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*. Ed. by S. Moriai and H. Wang. Vol. 12492. Lecture Notes in Computer Science. Springer, 2020, pp. 349–380. DOI: 10.1007/978-3-030-64834-3_12. URL: https://doi.org/10.1007/978-3-030-64834-3%5C_12.

[7] O. Bernard et al. “Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP”. In: *IACR Cryptol. ePrint Arch.* (2021), p. 1384. URL: https://eprint.iacr.org/2021/1384.

[8] D. Bernstein and T. Lange. “Non-randomness of S-unit lattices”. In: *IACR Cryptol. ePrint Arch.* (2021), p. 1428. URL: https://eprint.iacr.org/2021/1428.

[9] J.-F. Biasse. “Subexponential time relations in the class group of large degree number fields”. In: *Advances in Mathematics of Communications* 8.4 (2014), pp. 407–425. URL: http://aimsciences.org/journals/displayArticlesnew.jsp?paperID=10551.

[10] J.-F. Biasse and C. Fieker. “Subexponential class group and unit group computation in large degree number fields”. In: *LMS J. Comput. Math.* 17.suppl. A (2014), pp. 385–403. DOI: 10.1112/S1461157014000345. URL: https://doi.org/10.1112/S1461157014000345.

[11] J.-F. Biasse and F. Song. “Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields”. In: *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*. Ed. by R. Krauthgamer. SIAM, 2016, pp. 893–902. ISBN: 978-1-61197-433-1. DOI: 10.1137/1.9781611974331.ch64. URL: http://dx.doi.org/10.1137/1.9781611974331.ch64.

[12] J.-F. Biasse and C. van Vredendaal. “Fast multiquadratic S-unit computation and application to the calculation of class groups”. In: *Proceedings of ANTS XIII*. 2019, pp. 103–118.

[13] J.-F. Biasse et al. “Computing Generator in Cyclotomic Integer Rings”. In: *Proceedings of EUROCRYPT 2017*. 2017, pp. 60–88.

[14] J.-F. Biasse et al. “Norm relations and computational problems in number fields”. In: *Journal of the London Mathematical Society* 105.4 (2022), pp. 2373–2414. DOI: https://doi.org/10.1112/jlms.12563. eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms.12563. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms.12563.

[15] P. Campbell, M. Groves, and D. Shepherd. *SOLILOQUY: a cautionary tale*. online draft available at http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.

[16] R. Cramer, L. Ducas, and B. Wesolowski. “Short Stickelberger Class Relations and Application to Ideal-SVP”. In: *Proceedings of EUROCRYPT 2017*. 2017, pp. 324–348.

[17] R. Cramer, L. Ducas, and B. Wesolowski. “Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time”. In: *J. ACM* 68.2 (2021), 8:1–8:26. DOI: 10.1145/3431725. URL: https://doi.org/10.1145/3431725.

[18] R. Cramer et al. "Recovering Short Generators of Principal Ideals in Cyclotomic Rings". In: *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*. Ed. by M. Fischlin and J.-S. Coron. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 559–585. DOI: 10.1007/978-3-662-49896-5_20. URL: https://doi.org/10.1007/978-3-662-49896-5%5C_20.

[19] P. Erdős, C. Pomerance, and E. Schmutz. "Carmichael's lambda function". In: *Acta Arith.* 58.4 (1991), pp. 363–385. ISSN: 0065-1036. DOI: 10.4064/aa-58-4-363-385.

[20] C. Fieker, T. Hofmann, and C. Sircana. "On the construction of class fields". In: *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*. Vol. 2. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2019, pp. 239–255.

[21] T. Funakura. "On Artin theorem of induced characters". In: *Comment. Math. Univ. St. Paul.* 27.1 (1978/79), pp. 51–58. ISSN: 0010-258X.

[22] G. Fung, A. Granville, and H. Williams. "Computation of the first factor of the class number of cyclotomic fields". In: *Journal of Number Theory* 42.3 (1992), pp. 297–312. ISSN: 0022-314X. DOI: https://doi.org/10.1016/0022-314X(92)90095-7. URL: https://www.sciencedirect.com/science/article/pii/0022314X92900957.

[23] K. Horie and H. Ogura. "On the Ideal Class Groups of Imaginary Abelian Fields with Small Conductor". In: *Transactions of the American Mathematical Society* 347.7 (1995), pp. 2517–2532. ISSN: 00029947. URL: http://www.jstor.org/stable/2154835 (visited on 06/08/2022).

[24] E. Kummer. "Memoir on the theory of complex numbers composed of roots of unity and integers." fre. In: *Journal of Pure and Applied Mathematics* (1851), pp. 377–498. URL: http://eudml.org/doc/235621.

[25] T. Laarhoven. "Sieving for Closest Lattice Vectors (with Preprocessing)". In: *Selected Areas in Cryptography - SAC 2016 - 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers*. Ed. by R. Avanzi and H. Heys. Vol. 10532. Lecture Notes in Computer Science. Springer, 2016, pp. 523–542. DOI: 10.1007/978-3-319-69453-5_28. URL: https://doi.org/10.1007/978-3-319-69453-5%5C_28.

[26] A.K. Lenstra, H.W. Lenstra, and L. Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 261 (1982), pp. 515–534.

[27] F. J. van der Linden. "Class Number Computations of Real Abelian Number Fields". In: *Mathematics of Computation* 39.160 (1982), pp. 693–707. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/2007347 (visited on 06/01/2022).

[28] V. Lyubashevsky, C. Peikert, and O. Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*. Ed. by H. Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1. URL: https://doi.org/10.1007/978-3-642-13190-5%5C_1.

[29] V. Lyubashevsky, C.s Peikert, and O. Regev. "A Toolkit for Ring-LWE Cryptography". In: *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*. Ed. by T.s Johansson and P. Nguyen. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 35–54. DOI: 10.1007/978-3-642-38348-9_3. URL: https://doi.org/10.1007/978-3-642-38348-9%5C_3.

[30] J. Masley. "Class numbers of real cyclic number fields with small conductor". In: *Compositio Mathematica* 37 (1978), pp. 297–319.

[31] J. Miller. "Class numbers of real cyclotomic fields of composite conductor". In: *LMS Journal of Computation and Mathematics* 17 (2014), pp. 404–417.

[32] J. Miller. "Class numbers of totally real number fields". PhD thesis. Rutgers University, 2015.

[33] J. Neukirch. *Algebraic number theory*. Comprehensive Studies in Mathematics. ISBN 3-540-65399-6. Springer-Verlag, 1999.

[34] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008, pp. xvi+825. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1. URL: https://doi.org/10.1007/978-3-540-37889-1.

[35] A. Odlyzko. “Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results”. In: *Journal de Theorie des Nombres de Bordeaux* 2 (1990), pp. 119–141.

[36] A. Pellet-Mary, G. Hanrot, and D. Stehlé. “Approx-SVP in Ideal Lattices with Pre-processing”. In: *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II*. Ed. by Y. Ishai and V. Rijmen. Vol. 11477. Lecture Notes in Computer Science. Springer, 2019, pp. 685–716. DOI: `10.1007/978-3-030-17656-3\_24`. URL: `https://doi.org/10.1007/978-3-030-17656-3%5C_24`.

[37] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*. Vol. 30. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1989, pp. xiv+465. ISBN: 0-521-33060-2. DOI: `10.1017/CBO9780511661952`. URL: `https://doi.org/10.1017/CBO9780511661952`.

[38] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. Ed. by H. Gabow and R. Fagin. ACM, 2005, pp. 84–93. DOI: `10.1145/1060590.1060603`. URL: `https://doi.org/10.1145/1060590.1060603`.

[39] C. P. Schnorr and M. Euchner. “Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems”. In: *Math. Program.* 66.2 (Sept. 1994), pp. 181–199. ISSN: 0025-5610. DOI: `10.1007/BF01581144`. URL: `http://dx.doi.org/10.1007/BF01581144`.

[40] R. Schoof. “Minus class groups of the fields of the l-th roots of unity”. In: *Math. Comput.* 67 (1998), pp. 1225–1245.

[41] R. Schoof. “Class numbers of real cyclotomic fields of prime conductor”. In: *Math. Comput.* 72 (2003), pp. 913–937.

[42] A. Shokrollahi. “Relative class number of imaginary Abelian fields of prime conductor below 10000”. In: *Math. Comput.* 68 (1999), pp. 1717–1728.

[43] D. Simon. “Équations dans les corps de nombres et discriminants minimaux”. PhD thesis. Université Bordeaux I, 1998.

[44] K. Tateyama. “On the ideal class groups of some cyclotomic fields”. In: *Proceedings of the Japan Academy, Series A, Mathematical Sciences* 58.7 (1982), pp. 333–335. DOI: `10.3792/pjaa.58.333`. URL: `https://doi.org/10.3792/pjaa.58.333`.

[45] L. Washington. *Introduction to cyclotomic fields*. Second Edition. Springer, 1997.