Subexponential time relations in the class group of large degree number fields

Jean-François Biasse
University of Calgary
2500 University Drive NW
Calgary, Alberta, Canada T2N 1N4

Abstract

Hafner and McCurley described a subexponential time algorithm to compute the ideal class group of a quadratic field, which was generalized to families of fixed degree number fields by Buchman. The main ingredient of this method is a subexponential time algorithm to derive relations between primes of norm bounded by a subexponential value. Besides ideal class group computation, this was successfully used to evaluate isogenies, compute endomorphism rings, solve the discrete logarithm problem in the class group and find a generator of a principal ideal. In this paper, we present a generalization of the relation search to classes of number fields with degree growing to infinity.

1 Introduction

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n and maximal order $\mathcal{O}_K$, $\mathfrak{a}$ be an ideal of an order $\mathcal{O} \subseteq \mathcal{O}_K$, and a bound $B > 0$. We consider the problem of finding a relation of the form

$$\mathfrak{a} = (\phi)\mathfrak{p}_1 \cdots \mathfrak{p}_k \tag{1}$$

where the $(\mathfrak{p}_i)_{i \leq k}$ are prime ideals of $\mathcal{O}$ with $\mathcal{N}(\mathfrak{p}_i) \leq B$ and $\phi \in \mathcal{O}$. This means that if $[\mathfrak{a}]$ is the class of a fractional ideal $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$, then $[\mathfrak{a}] = \prod_i [\mathfrak{p}_i]$. In the rest of the document we identify $\mathfrak{a}$ and $[\mathfrak{a}]$ when there is no ambiguity.

Relations in $\mathrm{Cl}(\mathbb{Z}[\theta])$ for a well chosen θ can be used to factor large numbers or solving the discrete logarithm problem via the number field sieve algorithm [23]. In the case of an arbitrary $\mathcal{O} \subseteq \mathcal{O}_K$, one can deduce the class group and the unit group of $\mathcal{O}$ from a generating set of all relations between prime ideals with $\mathcal{N}(\mathfrak{p}_i) \leq B$ for a large enough B. Relations of the form (1) can also be used to solve the discrete logarithm problem in $\mathrm{Cl}(\mathcal{O})$ (where $\mathfrak{a}$ is the challenge) or to test if an ideal $\mathfrak{a} \subseteq \mathcal{O}$ is principal. Very few cryptosystems rely on the hardness of the discrete logarithm problem in $\mathrm{Cl}(\mathcal{O})$, but it can be shown that this is at least as hard as factoring large integers. In addition, there is no known reduction between the discrete logarithm in the Jacobian of a curve and in $\mathrm{Cl}(\mathcal{O})$. Therefore, this is a viable alternative to the cryptosystems currently used. On the other hand, many homomorphic schemes rely on the hardness of finding a generator of a principal ideal. Finally, when K is a CM field, an isogeny between isomorphism classes of Abelian varieties with complex multiplication by $\mathcal{O}$ can be expressed as the composition of lower degree isogenies from relations of the form (1), thus enhancing its evaluation, which has a lot of cryptographic applications including point counting and transporting the discrete logarithm from the Jacobian of a curve to another group.

Buchmann [6] generalized a result of Hafner and McCurley [16] to prove that the ideal class group and the unit group of the maximal order of classes of number fields of fixed degree and discriminant Δ growing to infinity could be computed in time $L_\Delta(1/2, c)$ where $c > 0$ is a constant and $L_\Delta(a,b) := e^{b\log|\Delta|^a \log\log|\Delta|^{1-a}}$. His proof relies on the capacity to derive relations of the form (1) for $B = L_\Delta(1/2, c_1)$ in time $L_\Delta(1/2, c_2)$ for constants $c_1, c_2 > 0$. For classes of number fields of degree n growing to infinity, no such result was known until Biasse [2] showed that the class group and the unit group of the equation order $\mathbb{Z}[\theta]$ could be computed in time $L_\Delta(1/3, c)$ for some $c > 0$ in certain classes of number fields where the degree and the height of the defining polynomial of the field grow in certain proportions.

Our contribution is to extend the result of [2] to prove that one can derive relations of the form (1) for $B = L_\Delta(\alpha, c_1)$ in time $L_\Delta(\alpha, c_2)$ for constants $c_1, c_2 > 0$ and $0 < \alpha < 1$ in any order $\mathbb{Z}[\theta] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ in classes of number fields satisfying restrictions generalizing those described in [2]. We discuss the applications of our relation search algorithm to the computation of $\mathrm{Cl}(\mathcal{O})$, the resolution of the discrete logarithm problem in $\mathrm{Cl}(\mathcal{O})$, the computation of the generator of a principal ideal $\mathfrak{a} \subseteq \mathcal{O}$, and the relation search in the polarized class group $\mathfrak{C}(\mathcal{O})$.

Theorem (Main result)**.** *Let $\mathcal{O}$ be an order in a degree n number field $\mathbb{Q}(\theta)$, $\Delta = \mathrm{disc}(\mathcal{O})$, $B > 0$, and $\mathfrak{a} \subseteq \mathcal{O}$ an ideal. Then, under the Generalized Riemann Hypothesis (GRH) and Heuristic 1 there is an algorithm that returns a B-smooth decomposition in time*

$$\log\left(\mathcal{N}(\mathfrak{a})\right)^{1+o(1)} L_\Delta(\alpha, c_1) \text{ where } B = L_\Delta(\alpha, c_2) \text{ for some } c_1, c_2 > 0.$$

The value of α is

- *$\alpha = 2/3 + \varepsilon$ for ε arbitrarily small in the general case.*
- *$\alpha = 1/2$ when $n \leq \log(|\Delta|)^{3/4-\varepsilon}$ for ε arbitrarily small.*
- *$\alpha = 1/3$ when $n \sim \log(|\Delta|)^{1/3}$ (in this case $\Delta = \mathrm{disc}(\mathbb{Z}[\theta])$).*

2 Finding relations when $n \to \infty$

In this section, we present the general idea of our method for deriving relations in $\mathrm{Cl}(\mathcal{O})$ where $\mathcal{O}$ is an order in a degree n number field K. Given a smoothness bound $B > 0$ and $\mathfrak{a} \subseteq \mathcal{O}$, we want to find products of the form $\mathfrak{a} = (\phi)\mathfrak{p}_1 \cdots \mathfrak{p}_k$, where $\alpha \in \mathcal{O}$ and $(\mathfrak{p}_i)$ are prime ideals of $\mathcal{O}$ with $\mathcal{N}(\mathfrak{p}_i) \leq B$. We want our method to run in subexponential time $L_\Delta(\alpha, c_1)$ for some $c_1 > 0$ and $0 < \alpha < 1$ when B is a subexponential bound. Here Δ is the discriminant of the defining polynomial of K and the subexponential function is given by

$$L_\Delta(\alpha, c) := e^{c\log(|\Delta|)^\alpha \log\log(|\Delta|)^{1-\alpha}}.$$

One way of finding relations between ideals in $\mathrm{Cl}(\mathcal{O})$ is to enumerate random B-smooth ideals in $\mathcal{O}$ (which means that they are power products of prime ideals of norm bounded by B) until one is equivalent to another B-smooth ideal (this test usually involves reducing it first, as explained in Section 2.2). The other typical method to find relations is to enumerate elements $\phi \in \mathcal{O}$ until the principal ideal it generates is B-smooth. In one case, it is the probability of the smoothness of an ideal which rules the run time of an algorithm, and in the other case, it is the probability of smoothness of an element, which is much less understood, in particular due to the units of $\mathcal{O}$.

2.1 Smoothness of ideals

Our complexity analysis relies on a heuristic on the smoothness of ideals. To justify it, we rely on two separate observations. First, in [28], Scourfield established a result on the smoothness of ideals in a number field comparable to the ones known on integers. Let

$$\Psi(x,y) := \left|\{\mathfrak{a} \subseteq \mathcal{O}_K, \mathcal{N}(\mathfrak{a}) \leq x, \mathfrak{a}\ y-\mathrm{smooth}\}\right|,$$

and $\varepsilon > 0$, then $\Psi(x,y)/x \sim \lambda_K \rho(u)$, where $u = \log(x)/\log(y)$, ρ is the Dickman function, λ_K is the residue of the zeta function $\zeta_K(s)$ at $s = 1$ and

$$(\log\log(x))^{\frac{5}{3}+\varepsilon} \leq \log(y) \leq \log(x),\ x \geq x_0(\varepsilon)$$

for some $x_0(\varepsilon)$. Unfortunately, we do not know if this remains true when we restrict ourselves to principal ideals. This is one of the reasons why the complexity of the number field sieve [23] (NFS) in only heuristic. Scourfield's result is the motivation for the specific form of the probability function described in Heuristic 1. In addition to that, we require a stronger smoothness assumption to perform our $\mathfrak{q}$ descent that is sketched in Section 2.3 and fully described in Section 3. Indeed, we want the primes in our decomposition to be of inertia degree 1, that is of the form $p\mathcal{O} + (\theta - v_p)\mathcal{O}$, where v_p is a root of $T(X) \bmod p$. In general, prime ideals can have inertia degree $f \geq 2$ and thus be of the form $p\mathcal{O} + T_p(\theta)\mathcal{O}$ where $\deg(T_p) = f$. However, their proportion is low when $B = L_\Delta(\alpha, c)$ for some $0 < \alpha < 1$ and $c > 0$. For $2 \leq f \leq n$, we have

$$\#\left\{p \text{ prime} \mid p^f \leq B\right\} \sim \frac{fB^{1/f}}{\log B}.$$

The proportion of primes whose f-th power for $2 \leq f \leq n$ is below the smoothness bound B with respect to the primes bounded by B thus equals

$$\frac{1}{\pi(B)} \sum_{2\leq f\leq n} \frac{fB^{1/f}}{\log B} = \sum_{2\leq f\leq n} \frac{1}{L_\Delta(\alpha, c - c/f + o(1))} \leq \frac{1}{L_\Delta(\alpha, c/2 + o(1))},$$

since n is polynomial in $\log|\Delta|$. This justifies that the proportion of inertia degree 1 prime ideals is asymptotically dominant, and in Heuristic 1 we assume that the smoothness probability with respect to these ideals only is asymptotically the same as the smoothness with respect to all ideals.

Heuristic 1. We assume that under GRH, the probability $P(\iota, \mu)$ that a principal ideal of $\mathcal{O}$ of norm bounded by e^ι is is a power-product of inertia degree 1 primes ideals of norm bounded by e^μ satisfies

$$P(\iota, \mu) \geq e^{(-u \log u(1+o(1)))}, \tag{2}$$

for $u = \iota/\mu$.

Corollary 2.1. *Let*

$$\iota = \lfloor \log L_\Delta(\zeta, c) \rfloor = \left\lfloor c\,(\log|\Delta|)^\zeta\,(\log\log|\Delta|)^{1-\zeta} \right\rfloor$$
$$\mu = \lceil \log L_\Delta(\beta, d) \rceil = \left\lceil d\,(\log|\Delta|)^\beta\,(\log\log|\Delta|)^{1-\beta} \right\rceil,$$

then assuming Heuristic 1, we have

$$P(\iota, \mu) \geq L_\Delta\left(\zeta - \beta, \frac{-c}{d}(\zeta - \beta) + o(1)\right).$$

2.2 The BKZ-reduction

Given an ideal $\mathfrak{a} \subseteq \mathcal{O}$ and $B > 0$, the classic method derived from [6, 16] to produce a relation of the form $\mathfrak{a} = (\phi)\mathfrak{p}_1^{e_1}, \dots, \mathfrak{p}_N^{e_N}$ consists of choosing $\mathcal{B} = \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$ where $B \leq L_\Delta(1/2, O(1))$ and testing random ideals of the form $\mathfrak{a} \cdot \prod_i \mathfrak{p}_i^{e_i}$ where $\mathcal{N}(\mathfrak{p}_i) \leq 48(\log(|\Delta|))^2$ and and $e_i \leq |\Delta|$ for B-smoothness in $\mathrm{Cl}(\mathcal{O})$. Indeed, under the GRH, the classes of ideals of norm less than $48(\log(|\Delta|))^2$ generate the class group whose size is bounded by $|\Delta|$. A reduction precedes the test for smoothness of a power product of ideals $\mathfrak{a} \cdot \prod_i \mathfrak{p}_i^{e_i}$ to find an ideal $\mathfrak{b} \subseteq \mathcal{O}$ in the same equivalence class as $\mathfrak{a}' := \mathfrak{a} \cdot \prod_i \mathfrak{p}_i^{e_i}$ with a reasonably bounded norm. It is done by finding a short element $\phi \in \mathfrak{c}$ where $\mathfrak{a}'^{-1} = \frac{1}{l}\mathfrak{c}$ with $l \in \mathbb{Z}_{l>0}$ and $\mathfrak{c} \subseteq \mathcal{O}$. Such a short element satisfies

$$\|\phi\| \leq \lambda_{\mathcal{O}} |\Delta|^{\frac{1}{2n}} \mathcal{N}(\mathfrak{c})^{\frac{1}{n}},$$

where $\lambda_{\mathcal{O}}$ is an approximation factor depending on the reduction method that we use. With the LLL algorithm, we have $\lambda_{\mathcal{O}} = 2^{n/2}$ achieved in polynomial time in n. Then, the ideal $\mathfrak{b} := \frac{\phi}{l}\mathfrak{a}'$ satisfies $\mathcal{N}(\mathfrak{b}) \leq \lambda_{\mathcal{O}}^n \sqrt{|\Delta|}$ and is in the same class as $\mathfrak{a}'$ in $\mathrm{Cl}(\mathcal{O})$. We try to decompose $\mathfrak{b}$ over $\mathcal{B}$, that satisfies $\log(\mathcal{N}(\mathfrak{b})) \leq O\left(\log(|\Delta|)\right)$ in the case where n is fixed. This bound allows us to decompose $\mathfrak{b}$ over primes of norm bounded by $B \leq L_\Delta(1/2, O(1))$ in time bounded by $L_\Delta(1/2, O(1))$. Then, a decomposition of $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ naturally follows.

For classes of number fields for which $n \to \infty$, we have in general $n \leq \log(|\Delta|)$. To have a subexponential algorithm for computing $\mathrm{Cl}(\mathcal{O})$ (and solving related problems in $\mathrm{Cl}(\mathcal{O})$), we need to be able to find B-smooth relations in subexponential time for some subexponential bound B. In particular, if $B = L_\Delta(\alpha, c)$ for some $0 < \alpha < 1$ and $c > 0$, then according to Corollary 2.1, the expected time to find a B-smooth ideal arising from the LLL-reduction of some $\mathfrak{a} \subseteq \mathcal{O}$ is bounded by $L_\Delta(2 - \alpha, d)$ for some $d > 0$ since the norm of the LLL-reduced ideals is bounded by $2^{n^2/2}\sqrt{|\Delta|} \leq L_\Delta(2, e)$ for some $e > 0$. This leaves no chance to calculate $\mathrm{Cl}(\mathcal{O})$ in subexponential time.

However, the BKZ-reduction [27] offers the possibility of a trade-off between the time spent in the reduction and the approximation factor $\lambda_{\mathcal{O}}$. It depends on a parameter k and allows to find a approximate short vector with $\lambda_{\mathcal{O}} = k^{\frac{n}{2k}}$ in time $2^{O(k)} \times P(n)$ where P is a polynomial. This way, given an ideal $\mathfrak{a} \subseteq \mathcal{O}$, we can find $\mathfrak{b}$ in the same equivalence class as $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ that satisfies $\mathcal{N}(\mathfrak{b}) \leq k^{\frac{n^2}{2k}}\sqrt{|\Delta|}$ in time $2^{O(k)}$ and polynomial in n. In the general case, $n \leq \log(|\Delta|)$, and by choosing $k = \log(|\Delta|)^{2/3} \log\log(|\Delta|)^{1/3}$, the expected number of BKZ$_k$-reduced $\mathfrak{b}$ that we need to draw to find one that is $L_\Delta(2/3, O(1))$-smooth is in $L_\Delta(2/3{+}\varepsilon, O(1))$ for any arbitrary small $\varepsilon > 0$. This can lead to an $L_\Delta(2/3 + \varepsilon)$ algorithm to compute $\mathrm{Cl}(\mathcal{O})$. When $n \leq \log(|\Delta|)^{3/4-\varepsilon}$ for $\varepsilon > 0$, we even find ideals $\mathfrak{b}$ with $\mathcal{N}(\mathfrak{b}) \leq |\Delta|^{O(1)}$ in the same equivalence class as $\mathfrak{a}$ in time $2^{\log(|\Delta|)^{1/2}}$ thus allowing to find $L_\Delta(1/2, c_1)$-smooth relations in time $L_\Delta(1/2, c_2)$ for some constants $c_1, c_2 > 0$, which generalizes Buchmann's result [6] to some classes of large degree number fields.

Algorithm 1 BKZ reduction

```
Require: An ideal $\mathfrak{a} \subseteq \mathcal{O}$, and $k \geq 1$.
Ensure: $\mathfrak{b} \subseteq \mathcal{O}$ and $\phi \in K$ with $\mathcal{N}(\mathfrak{b}) \leq k^{\frac{n^2}{2k}}\sqrt{|\Delta|}$, where $\mathfrak{b} = (\phi)\mathfrak{a}$, $n = \dim(\mathcal{O})$ and $\Delta = \mathrm{disc}(\mathcal{O})$.
$\mathfrak{c} \leftarrow l\mathfrak{a}^{-1}$ where $l$ is the denominator of $\mathfrak{a}$.
Find a BKZ$_k$-reduced $\gamma \in \mathfrak{c}$.
$\mathfrak{b} \leftarrow \frac{\gamma}{l}\mathfrak{a}$.
return $\mathfrak{b}, \frac{\gamma}{l}$.
```

Proposition 2.2. *Let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal in an order of a degree n number field and $k \geq 1$, then the complexity of the BKZ reduction given by Algorithm 1 is in*

$$O\left(2^{O(k)}\,\mathrm{Poly}(n)\log\left(\mathcal{N}(\mathfrak{a})\right)^{1+o(1)}\right).$$

Proof. This is a direct application of the BKZ reduction with parameter k to the $\mathbb{Z}$-basis of $\mathfrak{c}$. Its complexity is in $O\left(2^{O(k)}\,\mathrm{Poly}(n) B^{1+o(1)}\right)$, where B is a bound on the bit size of the matrix of the vectors of the $\mathbb{Z}$-basis of $\mathfrak{c}$. We assume that the $\mathbb{Z}$-basis of an ideal is given in its Hermite Normal Form, which means that $B \leq \log(\mathcal{N}(\mathfrak{c}))$, As $l \leq \mathcal{N}(\mathfrak{a})$, we have

$$\log(\mathcal{N}(\mathfrak{c})) = \log\left(\mathcal{N}\left(l\mathfrak{a}^{-1}\right)\right) \leq \log\left(\mathcal{N}(\mathfrak{a}^{n-1})\right) \leq n\log(\mathcal{N}(\mathfrak{a})).$$

The statement follows directly. □

2.3 The $\mathfrak{q}$-descent

The generalization of Buchmann's method together with a BKZ-reduction can only yield an $L_\Delta(1/2)$ algorithm for computing $\mathrm{Cl}(\mathcal{O})$ and solving related problems. Indeed, no matter how small the approximation factor $\lambda_\mathcal{O}$ is, the norm of the reduced ideal cannot have a tighter bound than $|\Delta|^{O(1)}$. The idea of the $\mathfrak{q}$-descent derives from the algorithms based on the number field sieve [23] to solve the discrete logarithm problem in time $L_q(1/3)$ in $\mathbb{F}_q$ (see in particular [1, 15, 21]). Our method is directly inspired by the analogue for C_{ab} curves presented in [12].

According to Corollary 2.1, if one only wants to spend a time bounded by $L_\Delta(1/3, c_1)$ on the decomposition of an ideal (principal or not, given Heuristic 1) of norm bounded by $L_\Delta(\alpha, c_2)$ for some $0 < \alpha < 1$ and $c_1, c_2 > 0$, the final decomposition will be $L_\Delta(\alpha - 1/3, c_3)$-smooth for some $c_3 > 0$. To allow an $L_\Delta(1/3, d)$ algorithm to compute $\mathrm{Cl}(\mathcal{O})$, we need to compute $L_\Delta(1/3, c_3)$-smooth relations in time $L_\Delta(1/3, d)$ for some $c_3, d > 0$. However, when we draw reduced ideals $\mathfrak{b} \subseteq \mathcal{O}$, we usually do not have $\alpha = 2/3$.

For the $\mathfrak{q}$-descent algorithm, we restrict ourselves to the classes of orders satisfying $n \sim \log(|\Delta|)^{1/3}$. Given an ideal $\mathfrak{a} \subseteq \mathcal{O}$, we can easily find a $|\Delta|$-smooth ideal $\mathfrak{b} \subseteq \mathcal{O}$ equivalent to $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ (with a BKZ reduction for example). Then, we find short elements $\phi \in \mathfrak{q}$ for every $\mathfrak{q} \mid \mathfrak{b}$. This search is designed to take a subexponential time bounded by $L_\Delta(1/3, c_1)$ for some $c_1 > 0$. It can be shown that we can find enough short $\phi \in \mathfrak{q}$ to obtain one for which $(\phi)/\mathfrak{q}$ is $L_\Delta(1/3 + \tau/2, c_2)$-smooth for some $c_2 > 0$ and $\tau = 2/3$. The process is repeated with the new decomposition, going from a $L_\Delta(1/3 + \tau/2^i)$-smooth decomposition to a $L_\Delta(1/3 + \tau/2^{i+1})$-smooth decomposition until the last jump to a $L_\Delta(1/3)$-smooth decomposition can be done in time $L_\Delta(1/3)$.

3 Subexponential time decomposition algorithms

In this section, we describe algorithms for the decomposition in $\mathrm{Cl}(\mathcal{O})$ of a given ideal $\mathfrak{a} \subseteq \mathcal{O}$ over ideals of norm bounded by a given $B > 0$. We present an algorithm relying on BKZ-reductions with subexponential complexity on any infinite class of orders and a $\mathfrak{q}$-descent algorithm working on restricted classes. Given an ideal $\mathfrak{a}$, the latter allows us to compute an $L_\Delta(1/3, c_1)$-smooth decomposition of $\mathfrak{a}$ in heuristic expected time $L_\Delta(1/3, c_2)$ in some classes of orders $\mathcal{O}$ in number fields $K = \mathbb{Q}(\theta) = \mathbb{Q}[X]/T(X)$ for $\Delta = \mathrm{disc}(\mathcal{O})$ and some c_1, c_2. These classes are parametrized by constants $n_0, d_0 > 0$. Let $T(X) = t_n X^n + t_{n-1}X^{n-1} + \ldots + t_0 \in \mathbb{Z}[X]$, $n := [K : \mathbb{Q}]$ and d be a bound on the size of the coefficients of T, that is $d := \log H_T$, where $H_T := \max_i |t_i|$. We say that the order $\mathcal{O}$ in the number field K belongs to $\mathcal{C}_{n_0,d_0}$ if

$$n = n_0 \log\left(|\Delta|\right)^{1/3}(1 + o(1)) \tag{3}$$

$$d = d_0 \log\left(|\Delta|\right)^{2/3}(1 + o(1)). \tag{4}$$

In the rest of the paper, we will use $\kappa := n_0 d_0$ in the expression of the complexities. We refer to [2] for examples of such classes of number field.

3.1 BKZ reduction of random ideals

When we substitute the LLL reduction with the BKZ reduction in the classical subexponential algorithms of Buchmann and Hafner-McCurley [6, 16], we obtain a subexponential time decomposition algorithm in arbitrary classes of number fields of degree growing to infinity (unlike with the $\mathfrak{q}$-descent on which restrictions apply). The BKZ-reduction of an ideal is given by Algorithm 1. We describe how to use it to decompose ideals in Algorithm 2 which depends on a parameter $\varepsilon > 0$ to be adjusted according to the desired asymptotic complexity, which is discussed in Proposition 3.1. Before the $\mathfrak{q}$-descent, we use a modified version of Algorithm 2 to obtain a $|\Delta|$-smooth decomposition with certain properties. We present this in Algorithm 3.

Algorithm 2 Ideal decomposition with the BKZ-reduction

```
Require: Ideal $\mathfrak{a}$, $\varepsilon > 0$ and $B > 0$.
Ensure: Primes $\mathfrak{q}_i$ with $\mathcal{N}(\mathfrak{q}_i) \leq B$, $\phi \in K$ such that $\mathfrak{a} = (\phi) \cdot \prod_i \mathfrak{q}_i$.
k ← $\log(|\Delta|)^\varepsilon$.
$\mathfrak{a} \leftarrow (\phi_1)\mathfrak{a}$ where $\phi_1$ is the output of Algorithm 1 on $(\mathfrak{a}, k)$.
found ← false
while found = false do
    Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_N$ be random prime ideals with $\mathcal{N}(\mathfrak{q}_i) \leq 48\log(|\Delta|)^2$.
    $\mathfrak{a}' \leftarrow (\phi_i) \cdot \mathfrak{a} \prod_i \mathfrak{q}_i^{-1}$ where $\phi_2$ is the output of Algorithm 1 on $(\mathfrak{a} \cdot \prod_i \mathfrak{q}_i^{-1}, k)$.
    if $\mathfrak{a}'$ is $B$-smooth then
        found ← true
        Let $\beta$ and $(\mathfrak{p}_j)$ such that $\mathfrak{a}' = (\beta) \prod_j \mathfrak{p}_j$.
    end if
end while

return $\{(\mathfrak{q}_i)_{i \leq N}, (\mathfrak{p}_j)\}$, $\phi_1 \cdot \phi_2 \cdot \beta$
```

Proposition 3.1 (GRH-Heuristic 1). *Let $\mathcal{O}$ an order in a degree n number field, $\Delta = \operatorname{disc}(\mathcal{O})$, $B > 0$, and $\mathfrak{a} \subseteq \mathcal{O}$ an ideal. Then Algorithm 2 returns a B-smooth decomposition in time*

$$\log\left(\mathcal{N}(\mathfrak{a})\right)^{1+o(1)} L_\Delta(\alpha, c_1) \text{ where } B = L_\Delta(\alpha, c_2) \text{ for some } c_1, c_2 > 0.$$

The value of α is

- *$\alpha = 2/3 + \varepsilon$ for ε arbitrarily small in the general case.*
- *$\alpha = 1/2$ when $n \leq \log(|\Delta|)^{3/4-\varepsilon}$ for ε arbitrarily small.*

Proof. Following the discussion of Section 2.2, the reduced ideals $\mathfrak{b}$ that we test for smoothness satisfy $\mathcal{N}(\mathfrak{b}) \leq e^{\frac{n^2}{2k}\log(k)}\sqrt{|\Delta|}$, and each reduction step has a cost bounded by $O\left(2^{O(k)} \log\left(\mathcal{N}(\mathfrak{a})\right)^{1+o(1)} \operatorname{Poly}(n)\right)$. In the general case, we choose $k = \log|\Delta|^{2/3}$. In this case, the reduced ideals $\mathfrak{b}$ tested for smoothness satisfy

$$\begin{aligned}\log\left(\mathcal{N}(\mathfrak{b})\right) &\leq \frac{n^2}{2k}\log(k)(1+o(1)) \\ &\leq O(\log(|\Delta|)^{4/3}\log\log(|\Delta|)(1+o(1))) \\ &\ll O(\log(|\Delta|)^{4/3+\varepsilon}\log\log(|\Delta|)^{-2/3}(1+o(1)))\end{aligned}$$

for some arbitrarily small $\varepsilon > 0$. According to Corollary 2.1, the expected number of $\mathfrak{b}$ to test to find one that is $L_\Delta(2/3+\varepsilon, c_1)$-smooth for some $c_1 > 0$ is bounded by $L_\Delta(2/3, c_2)$ for some $c_2 > 0$.

When $n \leq \log(|\Delta|)^{3/4-\varepsilon}$ for some $\varepsilon > 0$, we choose $k = \log(|\Delta|)^{1/2-2\varepsilon}\log\log(|\Delta|)$. In this case, the reduction step has a cost bounded by $\log\left(\mathcal{N}(\mathfrak{a})\right)^{1+o(1)} L_\Delta(1/2, c_1)$ for some $c_1 > 0$, and the reduced ideals $\mathfrak{b}$ that we test for smoothness satisfy

$$\begin{aligned}\log\left(\mathcal{N}(\mathfrak{b})\right) &\leq \frac{n^2}{2k}\log(k)(1+o(1)) \\ &\leq O\left(\frac{\log(|\Delta|)^{3/2-2\varepsilon}}{\log(|\Delta|)^{1/2-2\varepsilon}\log\log(|\Delta|)}\log\log(|\Delta|)(1+o(1))\right) \\ &\leq O(\log(|\Delta|)(1+o(1)))\end{aligned}$$

Then according to Corollary 2.1, the expected number of $\mathfrak{b}$ to test to find one that is $L_\Delta(1/2, c_1)$-smooth for some $c_1 > 0$ is bounded by $L_\Delta(1/2, c_2)$ for some $c_2 > 0$. □

A modified version of Algorithm 2 needs to be called before starting the $\mathfrak{q}$-descent (which is described in Section 3.2) to decompose the ideal $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ as a power-product of inertia degree 1 prime ideals of norm bounded by $|\Delta|$. We describe this procedure in Algorithm 3 and analyze it in Lemma 3.2.

Lemma 3.2 (GRH-Heuristic 1)**.** *Let $\mathfrak{a}$ be an ideal in an order $\mathcal{O}$ of a number field K in $\mathcal{C}_{n_0,d_0}$ for some n_0, d_0, then we can decompose $[\mathfrak{a}]$ over the classes of prime ideals of the form*

$$\mathfrak{q} = q\mathcal{O} + (\theta - v_q)\mathcal{O},$$

where $v_q \in \mathbb{Z}$ and $\mathcal{N}(\mathfrak{q}) \leq |\Delta|$, in expected time bounded by $L_\Delta(1/3, o(1))$.

Proof. We apply the same procedure as in Algorithm 2 with the parameter $k = \log(|\Delta|)^{1/3-\varepsilon}$ for an arbitrarily small $\varepsilon > 0$. This way, the reduced ideals $\mathfrak{b}$ satisfy $\mathcal{N}(\mathfrak{b}) \leq |\Delta|^{O(1)}$ and are derived in time $L_\Delta(1/3, o(1))$. According to Corollary 2.1, only $L_\Delta(1/3, o(1))$ of them need to be drawn until one which is $|\Delta|$-smooth is found, and under Heuristic 1, we can assume this decomposition to only include prime ideals of inertia degree 1. □

Algorithm 3 First decomposition

```
Require: Ideal $\mathfrak{a}$
Ensure: Primes $\mathfrak{q}_i$ of inertia degree 1 and $\phi \in K$ such that $\mathfrak{a} = (\phi)\prod_i \mathfrak{q}_i$.
$k \leftarrow \log(|\Delta|)^{\varepsilon}$.
$\mathfrak{a} \leftarrow (\phi_1)\mathfrak{a}$ where $\phi_1$ is the output of Algorithm 1 on $(\mathfrak{a}, k)$.
found $\leftarrow$ false
while found = false do
    $(\mathfrak{q}_i)_{i \leq N} \leftarrow$ random inertia degree 1 prime ideals with $\mathcal{N}(\mathfrak{q}_i) \leq 48\log(|\Delta|)^2$.
    $\mathfrak{a}' \leftarrow (\phi_i) \cdot \mathfrak{a}\prod_i \mathfrak{q}_i^{-1}$ where $\phi_2$ is the output of Algorithm 1 on $(\mathfrak{a} \cdot \prod_i \mathfrak{q}_i^{-1}, k)$.
    if $\mathfrak{a}'$ is $|\Delta|$-smooth with respect to the prime ideals of inertia degree 1 then
        found $\leftarrow$ true
        Let $\beta$ and $(\mathfrak{p}_j)$ such that $\mathfrak{a}' = (\beta)\prod_j \mathfrak{p}_j$.
    end if
end while
return $\{(\mathfrak{q}_i)_{i \leq N}, (\mathfrak{p}_j)\}$, $\phi_1 \cdot \phi_2 \cdot \beta$
```

3.2 Analysis of the $\mathfrak{q}$-descent algorithm

In this section, we assume we are looking for relations in an order $\mathcal{O} \in \mathcal{C}_{n_0,d_0}$ for some n_0, d_0. Once the first decomposition is done, the prime ideals occurring in the decomposition of $\mathfrak{a}$ are recursively decomposed as power-products of prime ideals of lower norm. For that, we enumerate elements $\phi \in \mathfrak{q} = q\mathcal{O} + (\theta - v_q)\mathcal{O}$ of the form $\phi = A(\theta)$ until one is smooth.

Theorem 3.3 (GRH-Heuristic 1)**.** *We can find a $\mathcal{B}$-smooth ideal equivalent to any ideal $\mathfrak{a}$ of $\mathcal{O} \in \mathcal{C}_{n_0,d_0}$ for some n_0, d_0 in time*

$$L_\Delta(1/3, b + \varepsilon),$$

with $b = \sqrt[3]{\frac{24\kappa}{9}}$ and any $\varepsilon > 0$.

Proof. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. From Lemma 3.2, we know how to find $\mathfrak{a}'$ equivalent to $\mathfrak{a}$ that splits over the prime ideals of the form $\mathfrak{q} = q\mathcal{O} + (\theta - v_q)\mathcal{O}$ and of norm bounded in $O(|\Delta|)$. We proceed recursively, starting from the primes of the first decomposition. At each stage, $\mathfrak{q} = q\mathcal{O} + (\theta - v)\mathcal{O}$ is an ideal of norm bounded by $L_\Delta(1/3 + \tau, c)$ for some $c > 0$ and $0 \leq \tau \leq 2/3$. At the beginning we have $\tau = 2/3$ and $c = 1$. We search $\phi \in \mathfrak{q}$ such that $(\phi)/\mathfrak{q}$ is $L_\Delta(1/3 + \tau/2, c')$-smooth for a c' depending on c. Such a ϕ satisfies $\mathfrak{q} \mid (\phi)$ and thus $[\mathfrak{q}]$ can be decomposed as a power product of classes of prime ideals involved in the decomposition of (ϕ). We repeat this process until we obtain a decomposition involving only classes of elements of $\mathcal{B}$. At each stage, we consider the ϕ belonging to the lattice of polynomials in θ of degree bounded by

$$k := \left\lfloor \sigma \frac{n}{(\log|\Delta|/\log\log|\Delta|)^{1/3-\tau/2}} \right\rfloor,$$

where $\sigma > 0$ is a constant to be determined later. These ϕ form a $\mathbb{Z}$-lattice generated by

$$(v_0, \theta - v_1, \ldots, \theta^k - v_k),$$

with $v_0 = q$ and $v_i = v_q^i \mod q$ for $i \geq 1$. We want to spend the same time $L_\Delta(1/3, e + o(1))$ at each smoothing step for $e > 0$ to be optimized later. The search space has to be of the same size. We thus look for $L_\Delta(1/3, e+o(1))$ distinct $(k+1)$-tuples $(\alpha_1, \ldots, \alpha_{k+1}) \in \mathbb{Z}^{k+1}$. Using Lemma 3.4, for every integer z, we can find e^{kz} such tuples satisfying $\log|\alpha_i| \leq D/k + z$ for $i \leq k+1$ and $\log|\sum_i \alpha_i v_i| \leq D/k + z$. We adjust the value of z to make sure that all the $L_\Delta(1/3, e + o(1))$ tuples obtained during the search phase satisfy this property by solving $e^{kz} = L_\Delta(1/3, e + o(1))$. This yields

$$z = \frac{1}{n} \log L_\Delta(2/3 - \tau/2, e/\sigma + o(1)).$$

From [2, Lem. 2], $\log(\mathcal{N}(\phi)) \leq n(D/k + z) + dk + d\log(k) + k\log(n)$, therefore

$$\mathcal{N}(\phi) \leq L_\Delta(2/3 + \tau/2, (c+e)/\sigma + o(1)).$$

Let $\mathfrak{q}'$ be the ideal such that $(\phi) = \mathfrak{q} \cdot \mathfrak{q}'$. Its norm is also bounded:

$$\mathcal{N}(\mathfrak{q}') \leq L_\Delta(2/3 + \tau/2, (c+e)/\sigma + o(1)).$$

From Heuristic 1 and Corollary 2.1 we expect to find at least one $L_\Delta(1/3 + \tau/2, c')$-smooth $\mathfrak{q}'$ for

$$c' = \frac{1}{3e}((c+e)/\sigma + \sigma\kappa).$$

Once this is achieved, we can write $\mathfrak{q} = (\phi)\mathfrak{q}'^{-1}$, thus rewriting $[\mathfrak{q}]$ as a power product of classes of prime ideals of norm bounded by $L_\Delta(1/3 + \tau/2, c')$. The value of c' is minimized by $\sigma = \sqrt{(c+e)/\kappa}$, which yields

$$c' = \frac{2\sqrt{\kappa}}{3e}\sqrt{c+e}.$$

Starting with $\tau_0 = 2/3$ and $c_0 = 1$, we obtain a power-product of prime ideals of norm bounded by $L_\Delta(1/3 + \tau_1, c_1)$ with $\tau_1 = 1/3$ and $c_1 = 2\sqrt{\kappa(c_0 + e)}/3e$. After i steps, we get an ideal which is $L_\Delta(1/3 + 1/(3 \cdot 2^{i-1}), c_i) = L_\Delta(1/3, c_i \cdot \mathcal{M}^{\frac{1}{3\cdot 2^{i-1}}})$-smooth, where

$$\tau_i = \frac{1}{3 \cdot 2^{i-1}}, \quad c_i = \frac{2\sqrt{\kappa}}{3e}\sqrt{c_{i-1} + e}, \quad \mathcal{M} = \left(\frac{\log(|\Delta|)}{\log\log(|\Delta|)}\right).$$

The sequence c_i converges to a finite limit c_∞ given by

$$c_\infty = \chi/2\left(\chi + \sqrt{\chi^2 + 4e}\right),$$

where $\chi = 2\sqrt{\kappa}/3e$. Let $\xi > 0$ be an arbitrary constant. After a number of steps only depending on e, κ and ξ, we have $c_i < c_\infty(1 + \xi)$, and after $O(\log\log|\Delta|)$ steps $\mathcal{M}^{\frac{1}{3\cdot 2^{i-1}}} < (1 + \xi)$. We can thus decompose $[\mathfrak{a}']$ as a power-product of classes of prime ideals of norm bounded by

$$L_\Delta(1/3, c_\infty(1 + \xi)).$$

At each step, the decomposition involves $O(\log|\Delta|)$ ideals, and we need to perform $O(\log\log|\Delta|)$ steps. Indeed, we want to decompose $[\mathfrak{a}']$ as a power product of classes of prime ideals of norm bounded by $L_\Delta(1/3, \rho)$ for some $\rho > 0$. Let us compute the effort to reach $c_\infty(1+\xi) = \rho$. As in [12, Th. 8], we write $9e^3 = E\kappa$ with E to be determined later. The equation $\rho = c_\infty$ simplifies as

$$\left(\frac{3}{E}\right)^{1/3} = \frac{2}{E}(1 + \sqrt{1+E}).$$

The least non negative solution E_0 satisfies $E_0 = 24$, which yields

$$e = \sqrt[3]{\frac{24\kappa}{9}} =: b.$$

□

Algorithm 4 $\mathfrak{q}$-descent

```
Require: Ideal $\mathfrak{a}$, $\mathcal{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$
Ensure: Primes $(\mathfrak{q}_i)_{i\leq l} \in \mathcal{B}$, integers $(e_i)$ and $(\phi_j)_{j\leq k} \in K$ such that $\mathfrak{a} = \prod_{j\leq k}(\phi_j) \cdot \prod_{i\leq l} \mathfrak{q}_i^{e_i}$
Find prime ideals $(\mathfrak{q}_i)_{i\leq l}$ of norm bounded by $|\Delta|$ and $\phi_1$ with $\mathfrak{a} = (\phi)\cdot\prod_i \mathfrak{q}_i$ using Algorithm 3

genList ← $[\phi_1]$, primeList ← $[\mathfrak{q}_1, \dots, \mathfrak{q}_l]$, expList ← $[1, \cdots, 1]$.
while there is $\mathfrak{q} \notin \mathcal{B}$ in the decomposition of $[\mathfrak{a}]$ do
    Find $(\mathfrak{q}_i)_{i\leq l}$, $(e_i)_{i\leq l}$ and $\phi_k$ such that $\mathfrak{q} = (\phi_k)\prod_{i\leq l}\mathfrak{q}_i^{e_i}$ as in Theorem 3.3
    genList ← genList ∪ $[\phi_k]$, primeList ← primeList ∪ $[\mathfrak{q}_1, \dots, \mathfrak{q}_l]$.
    expList ← expList ∪ $[e_1, \cdots, e_l]$.
end while
return genList, primeList, expList.
```

3.3 Finding short elements in $\mathfrak{q}$

In Algorithm 4 described in Section 3.2, we draw elements $\phi \in \mathfrak{q} = q\mathcal{O} + (\theta - v_q)\mathcal{O}$ in the $\mathbb{Z}$-lattice generated by $(v_0, \theta - v_1, \dots, \theta^k - v_k)$ where $v_0 = q$ and $v_i = v_q^i \bmod q$. In the proof of Theorem 3.3 we rely on the fact that there are sufficiently many small elements in a bounded hypercube of this lattice. Note that in section again, $\mathcal{O} \in \mathcal{C}_{n_0,d_0}$ for some n_0, d_0.

Lemma 3.4. *Let $\sigma, \tau, c > 0$, and some integers D and k defined by*

$$k := \left\lfloor \sigma \frac{n}{(\log|\Delta| / \log\log|\Delta|)^{1/3-\tau/2}} \right\rfloor \;,\; D := \log\left(L_\Delta(1/3+\tau, c)\right).$$

Let $v_1, \dots, v_{k+1}$ be integers satisfying $\log|v_i| \leq D$. Then, for any integer z, there exist at least e^{kz} tuples $(\alpha_1, \dots, \alpha_{k+1}) \in \mathbb{Z}^{k+1}$ satisfying

$$\log|\alpha_i| \leq D/k + z$$
$$\log\left|\sum_i \alpha_i v_i\right| \leq D/k + z.$$

Proof. Let us define the $k+1$ dimensional lattice Λ generated by the rows of

$$A := \begin{pmatrix} 1 & 0 & \dots & 0 & v_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & v_{k+1} \end{pmatrix}.$$

For any element $x \in \Lambda$, there exists $(\alpha_1, \ldots, \alpha_{k+1}) \in \mathbb{Z}^{k+1}$ such that

$$x = \left(\alpha_1, \ldots, \alpha_{k+1}, \sum_i \alpha_i v_i\right).$$

The determinant $d(\Lambda)$ of Λ satisfies

$$d(\Lambda) = \sqrt{\det\left(AA^T\right)} = \sqrt{\sum_{i \leq k+1} v_i + \sum_{i \leq k+1} v_i v_{k+1-i}} \leq \left(\sqrt{2k+1}\right) e^D.$$

Let $X \subset \mathbb{R}^{k+2}$ be the symmetric and convex set of points defined by

$$X = \left\{(x_1, \ldots, x_{k+2}) \mid \forall i \ |x_i| \leq D/k + z\right\}.$$

The volume $V(X)$ equals $2^{k+2} e^{(k+2)(D/k+z)}$, and from Theorem II of III.2.2 in [10] we know that if

$$V(X) > m 2^{k+2} d(\Lambda),$$

then X intersect Λ in at least m pairs of points $\pm x \in \mathbb{R}^{k+2}$. It thus suffices to prove that

$$e^{kz} < \frac{e^{(k+2)(\frac{D}{k}+z)}}{\sqrt{2k+1} e^D} = e^{kz} . \frac{e^{2\frac{D}{k}+2z}}{\sqrt{2k+1}},$$

which is satisfied since

$$\frac{D}{k} = \frac{c}{\sigma} \log |\Delta|^{2/3-\alpha+\tau/2} \log\log |\Delta|^{1/3-\tau/2} \gg \log(2k+1).$$

□

These short vectors need to be found via an enumeration algorithm of short vectors. This is exponential in the dimension of the lattice, which itself is bounded by n. We use the method described in [17] to perform this search.

Proposition 3.5. *The search for the solution of the vectors solution to the restrictions described in Lemma 3.4 takes time bounded by* $L_\Delta(1/3, e + o(1))$.

Proof. Enumerating vectors of length bounded by $A = e^{D/k+z}$ with [17, Alg. 10] takes

$$2^{O(k)} \frac{A^k}{k^{k/2} d(\Lambda)} \leq 2^{O(k)} \frac{e^{D+kz}}{k^{k/2} e^D} \leq 2^{O(k)} L_\Delta(1/3, e + o(1)).$$

Furthermore, since $k \sim \log(|\Delta|)^{1/3-\varepsilon}$ for some $\varepsilon > 0$, we have $2^{O(k)} = L_\Delta(1/3, o(1))$ which concludes the proof. □

4 Applications

An important motivation for finding relations in $\mathrm{Cl}(\mathcal{O})$ where $\mathcal{O}$ is an order in a number field is the computation of the structure of $\mathrm{Cl}(\mathcal{O})$ and of a system of fundamental units of $\mathcal{O}$. This is an essential task in computational number theory. It allows us in particular to provide numerical evidence in favor of unproven conjectures such as the heuristics of Cohen and Lenstra [11] on the ideal class group of a quadratic number field, Littlewood's bounds [24] on $L(1, \chi)$, or Bach's bound on the minimal B such that ideals of norm at most B generate the ideal class group. These methods can also be used to solve Diophantine equations. For example, the computation of the fundamental unit of a number field is equivalent to solving the Pell equation $T^2 - \Delta U^2 = 1, \ T, U \in \mathbb{Z}$, associated to the discriminant Δ of the field in question (see [19]). Other Diophantine equations such as the Schäffer equation $y^2 = 1^k + 2^k + \ldots + (x-1)^k, \quad k \geq 2$, can be solved using solutions to the Pell equation [18] , which is itself a special case of norm equations of the form $\mathcal{N}(\phi) = 1$.

The subexponential method for computing $\mathrm{Cl}(\mathcal{O})$ and a system of fundamental units of $\mathcal{O}$ shares a lot of similarities with algorithms with cryptographic relevance. For example, rewriting the class of a given ideal $\mathfrak{a} \subseteq \mathcal{O}$ as the class of a power product of prime ideals of short norm can be used to solve the discrete logarithm problem in $\mathrm{Cl}(\mathcal{O})$. Although not used in practice, cryptosystems relying on the hardness of the discrete logarithm problem in $\mathrm{Cl}(\mathcal{O})$ [9, 8, 4, 7, 26] may be a viable alternative to schemes relying on the hardness of factorization or of the discrete logarithm in other groups. More recently, after Gentry described the first fully homomorphic encryption scheme [13, 14], finding short vectors in ideal lattices became an essential topic in public key cryptography. In particular, finding a short generator of a principal ideal (for $\| \sum_i x_i \theta^i \|_\infty := \max_i |x_i|$) allows to break some variations of Gentry's scheme (for example, the cryptosystem of Vercauteren and Smart [29]). We show in Section 4.3 how our relation generation method applies to this problem. Finally, decomposing the class of an ideal into a power-product of ideals of smaller norm applies to the evaluation of the action of $\mathrm{Cl}(\mathcal{O})$ on curves having complex multiplication by $\mathcal{O}$, as shown by Jao in the case of elliptic curves [20].

4.1 Class group and unit group computation of $\mathcal{O}$

The subexponential method due to Buchmann [6] is a generalization of the algorithm of Hafner and McCurley [16] for quadratic number fields, and its complexity is subexponential bounded by $L_\Delta(1/2, c)$ for some $c > 0$ for classes of number fields with fixed degree. Let $\mathcal{B} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of prime ideals of $\mathcal{O}$ whose classes generate $\mathrm{Cl}(\mathcal{O})$. We have a surjective morphism

$$\begin{tikzcd}
\mathbb{Z}^N \arrow[r, "\varphi"] & \mathcal{I} \arrow[r, "\pi"] & \mathrm{Cl}(\mathcal{O}) \\
(e_1, \ldots, e_N) \arrow[r] & \prod_i \mathfrak{p}_i^{e_i} \arrow[r] & \prod_i [\mathfrak{p}_i]^{e_i}
\end{tikzcd},$$

and the class group is given by $\mathrm{Cl}(\mathcal{O}) \simeq \mathbb{Z}^N / \ker(\pi \circ \varphi)$. Therefore, computing the class group boils down to computing $\ker(\pi \circ \varphi)$, which is given by the lattice of $(e_1, \ldots, e_N) \in \mathbb{Z}^N$ such that

$$\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_N^{e_N} = (\phi),$$

where $\phi \in \mathcal{O}$. We collect many relations of the form $\prod_i \mathfrak{p}_i^{e_i^{(j)}} = (\phi_j)$ and put them in the rows of the relation matrix $M := (e_i^{(j)})$. Once the rows of M generate the lattice of all the relation, the quotient $\mathbb{Z}^N / \ker(\pi \circ \varphi)$ is derived from the Smith Normal Form (SNF) of this M. Meanwhile, every vector $X := (x_1, \cdots, x_N)$ of the left kernel of M yields a unit

$$\gamma_X := \alpha_1^{x_1} \cdots \alpha_N^{x_N},$$

since the principal ideals that it generates satisfies

$$(\gamma_X) = \mathfrak{p}_1^{\sum_i x_i e_i^{(1)}} \cdots \mathfrak{p}_N^{\sum_i x_i e_i^{(N)}} = \mathfrak{p}_1^0 \cdots \mathfrak{p}_N^0 = (1) = \mathcal{O}.$$

This allows us to iteratively compute the unit group U by finding kernel vectors of the relation matrix M. We give a high-level description of the computation of $\mathrm{Cl}(\mathcal{O})$ and $U(\mathcal{O})$ in Algorithm 5.

Computing relations between ideals of $\mathcal{B}$ is an essential ingredient of Algorithm 5. From the properties of the subexponential function, if one can find a $L_\Delta(\alpha, c_1)$-smooth relation in time $L_\Delta(\alpha, c_2)$ for some $0 < \alpha < 1$, then the time to find $L_\Delta(\alpha, c_1 + o(1))$ relations (which bounds the size of the factor base $|\mathcal{B}|$) is bounded by $L_\Delta(\alpha, c_1 + c_2 + o(1))$. By BKZ-reducing random power products of elements in $\mathcal{B}$ with Algorithm 1, we can achieve an $L_\Delta(2/3 + \varepsilon, c_1)$ algorithm to find $|\mathcal{B}|$ relations in the general case and an $L_\Delta(1/2, c_2)$ algorithm when $n \leq \log(|\Delta|)^{3/4 - \varepsilon'}$ for some

Algorithm 5 Class group and unit group of $\mathcal{O}$

```
Require: $\mathcal{O}$, $K$, $\mathcal{B} = \{\mathfrak{p} \subseteq \mathcal{O} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$ that generates $\mathrm{Cl}(\mathcal{O})$.
Ensure: Class group and unit group of $\mathcal{O}$.
Derive a generating set of the relations in $\mathrm{Cl}(\mathcal{O})$ between elements of $\mathcal{B}$.
Let $M$ be the matrix of a basis for the $\mathbb{Z}$-lattice $\mathcal{L}$ of the relations.
Compute $\mathrm{Cl}(\mathcal{O})$ from the SNF of $M$.
for $X_i \in \ker(M)$ do
    Let $\gamma_i$ be the unit corresponding to $X_i$.
end for
Find $U(\mathcal{O})$ from the $(\gamma_i)$.
```

$c_1, c_2 > 0$ and arbitrarily small $\varepsilon, \varepsilon' > 0$. By performing a $\mathfrak{q}$-descent on random power-products of elements in $\mathcal{B}$, we even achieve an $L_\Delta(1/3, c_3)$ algorithm to find $|\mathcal{B}|$ relations when $n \sim \log(|\Delta|)^{1/3}$. However, more work needs to be done to state that this allows subexponential methods of the computation of the class group and unit group of $\mathcal{O}$. The randomization of the relation needs to be addressed, and will most likely rely on some heuristics as it is the case in [2]. In addition, a careful analysis of the computation of the unit group also has to be done. It needs to take into account the precision of the representation of the units that is chosen. In [2], they are vectors of fixed point approximations of Archimedian valuations while in [3] their p-adic approximations were used.

4.2 Discrete logarithm in $\mathrm{Cl}(\mathcal{O})$

Calculating the group structure of $\mathrm{Cl}(\mathcal{O})$ allows to solve the discrete logarithm problem between two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$ by decomposing them as a power-product of the generators of $\mathrm{Cl}(\mathcal{O})$, either by the means of a $\mathfrak{q}$-descent or by multiplying them by random power-products or small ideals and testing them for smoothness.

Solving the discrete logarithm problem in $\mathrm{Cl}(\mathcal{O})$ can also be done without the knowledge of the structure of $\mathrm{Cl}(\mathcal{O})$, as described by Vollmer [30]. Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, we wish to compute x such that $[\mathfrak{b}] = [\mathfrak{a}]^x$. We enlarge the factor base with $\mathfrak{a}$ and $\mathfrak{b}$ and let $\mathcal{B}' = \mathcal{B} \cup \{\mathfrak{a}, \mathfrak{b}\}$. Then we use the methods of either Algorithm 2 or Algorithm 4 to find a relation matrix $M \in \mathbb{Z}^{N' \times N}$ whose rows generate the possible relations between elements of $\mathcal{B}$ and to decompose $[\mathfrak{a}]$ and $[\mathfrak{b}]$ over classes of elements in $\mathcal{B}$, thus creating two extra relations over $\mathcal{B}'$

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_N^{e_N} \mathfrak{a} = (\phi_\mathfrak{a}), \quad \mathfrak{p}_1^{f_1} \dots \mathfrak{p}_N^{f_N} \mathfrak{b} = (\phi_\mathfrak{b}). \tag{5}$$

Let $\vec{v_\mathfrak{a}} := (e_1, \dots, e_N)$ and $\vec{v_\mathfrak{b}} := (f_1, \dots, f_N)$. Let $X \in \mathbb{Z}^{N'+2}$ be a solution to the system $XA = \vec{v}$ where

$$A := \left(\begin{array}{c|c} M & (0) \\ \hline \vec{v_\mathfrak{b}} & 1 \\ \vec{v_\mathfrak{a}} & 0 \end{array} \right) \quad \text{and} \quad \vec{v} = (0, \dots, 0, 1).$$

Then, with the same definition of the $(\phi_i)_{i \leq N'}$ as for the computation of $\mathrm{Cl}(\mathcal{O})$, we have

$$\prod_{i \leq N'} (\phi_i)^{x_i} \cdot (\phi_\mathfrak{a})^{x_{N'+1}} \cdot (\phi_\mathfrak{b})^{x_{N'+2}} = \mathfrak{p}_1^0 \cdots \mathfrak{p}_N^0 \cdot \mathfrak{a} \cdot \mathfrak{b}^{x_{N'+2}},$$

which solves the discrete logarithm problem. We summarize in Algorithm 6 the algorithms for solving the discrete logarithm problem given $[\mathfrak{a}]$ and $[\mathfrak{b}]$ in $\mathrm{Cl}(\mathcal{O})$.

Algorithm 6 Discrete logarithm algorithm

```
Require: Ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that there exists $x \in \mathbb{Z}$ satisfying $[\mathfrak{b}] = [\mathfrak{a}]^x$
Ensure: $x'$ such that $[\mathfrak{b}] = [\mathfrak{a}]^{x'}$
  Construct the factor base $\mathcal{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$
  Construct $M \in \mathbb{Z}^{(N') \times N}$ whose rows span all the relations between the $\mathfrak{p}_i \in \mathcal{B}$.
  $\vec{v_\mathfrak{a}} \leftarrow (e_1, \dots, e_N)$ with $[\mathfrak{p}_1]^{e_1} \dots [\mathfrak{p}_N]^{e_N} [\mathfrak{a}] = (1)$ using Algorithm 4
  $\vec{v_\mathfrak{b}} \leftarrow (f_1, \dots, f_N)$ with $[\mathfrak{p}_1]^{f_1} \dots [\mathfrak{p}_N]^{f_N} [\mathfrak{b}] = (1)$ using Algorithm 4
  Solve $XA = \vec{v}$ where
      $A := \left(\begin{array}{c|c} M & (0) \\ \hline \vec{v_\mathfrak{b}} & 1 \\ \vec{v_\mathfrak{a}} & 0 \end{array}\right)$ and $\vec{v} = (0, \dots, 0, 1)$.
  return $x' = -X_{N'+2}$
```

4.3 Principal ideal problem in $\mathcal{O}$

Now let us study how we can decide whether a given arbitrary ideal $\mathfrak{a}$ is principal, and if so compute α such that $\mathfrak{a} = (\phi)$. To this end, we first decompose $[\mathfrak{a}]$ over $\mathcal{B}$ using either Algorithm 2 or Algorithm 4. We obtain a vector $b \in \mathbb{Z}^N$ representing the decomposition of $[\mathfrak{a}]$ over $\mathcal{B}$. Using Algorithm 2 or Algorithm 4, we also compute $M \in \mathbb{Z}^{N' \times N}$ whose rows generate all the possible relations between elements of $\mathcal{B}$. This means that the vector b belongs to the lattice spanned by the rows of M if and only if $\mathfrak{a}$ is principal. Therefore, solving $XM = b$ allows us to decide whether $\mathfrak{a}$ is principal. We summarize in Algorithm 7 the algorithm for solving the principal ideal problem relatively to an ideal $\mathfrak{a} \subseteq \mathcal{O}$.

Algorithm 7 Principality testing algorithm

```
Require: Ideal $\mathfrak{a} \subseteq \mathcal{O}$.
Ensure: false or $(x_1, \dots, x_g)$ and $(\beta_1, \dots, \beta_g)$ such that $\mathfrak{a} = (\prod_i \beta_i^{x_i})$
  Construct the factor base $\mathcal{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$
  Construct $M \in \mathbb{Z}^{N' \times N}$ whose rows span all the relations between the $\mathfrak{p}_i \in \mathcal{B}$.
  $(\phi_1, \cdots, \phi_{N'}) \leftarrow$ generators of the principal ideals in the relations of $M$.
  $\vec{v} \leftarrow (e_1, \dots, e_N)$ where $\mathfrak{a} = (\phi) \cdot \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N}$ and $\phi \in K$ using Algorithm 2 or Algorithm 4.
  Solve $XM_\mathbb{Z} = \vec{v}$.
  return false if no solution or $(1, x_1, \dots, x_{N'})$ and $(\phi, \phi_1, \dots, \phi_{N'})$.
```

Computing a generator of a principal ideal directly applies to the cryptanalysis of some homomorphic encryption schemes based on ideal lattices such as the one of Vercauteren and Smart [29]. The secret key is a small generator of the principal ideal, which is broadcasted using its $\mathbb{Z}$-basis. Vercauteren and Smart claim that the subexponential method of Buchmann, which corresponds to Algorithm 7 is exponential in the degree n of the number field. Using either Algorithm 2 or Algorithm 4, we can derive a relation matrix and decompose the class of $\mathfrak{a}$ over the factor base in subexponential time. The subsequent resolution of a linear system can easily be shown to run in subexponential time. Therefore, this shows that the security assumption made in [29] about the principal ideal problem is no longer true. Algorithm 7 allows us to retrieve one of the generators of a given principal ideal $\mathfrak{a} \subseteq \mathcal{O}$. If this generator was known to have a small representation over the $\mathbb{Z}$-basis of $\mathcal{O}$, then the power-product could be evaluated modulo some reasonably sized primes and recovered by the Chinese Remainder Theorem. Unfortunately, Algorithm 7 does not necessarily provide us with a small generator. If $\mathfrak{a} = (\phi)$ and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ is the unit group of $\mathcal{O}$, then

$$\forall(e_1,\cdots,e_r)\in\mathbb{Z}^r,\ \mathfrak{a}=(\varepsilon_1^{e_1},\cdots,\varepsilon_r^{e_r}\phi).$$

When the unit group has rank 1, we find $e\in\mathbb{Z}$ such that $\log|\phi|-e\log|\varepsilon|$ has the desired size. When U has rank $r>1$, let $\vec{v}_x=(\log|x|_1,\cdots,\log|x|_r)\in\mathbb{R}^r$ be the vector of Archimedian valuation of $x\in\mathcal{O}$. Finding a short generator of $\mathfrak{a}$ boils down to finding a vector $(e_1,\cdots,e_r)$ such that $\|\vec{\phi}+\sum_i e_i\vec{\varepsilon_i}\|_2$ is small. As the algorithms for solving the shortest vector problem run in exponential time with respect to the dimension of the lattice, Algorithm 7 does not allow to break homomorphic encryption schemes, despite the fact that it contradicts the security assumption as stated in [29].

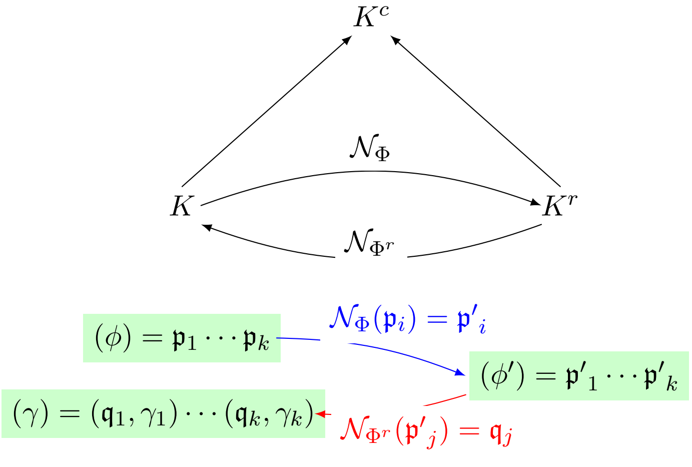
4.4 Relations in $\mathfrak{C}(\mathcal{O})$

The study of isogenies is an important topic in mathematical cryptology. It occurs in particular in point counting and in the resolution of the discrete logarithm problem. A given Abelian variety over a finite field q is said to have complex multiplication by an order $\mathcal{O}$ in a CM field K if its endomorphism ring $\mathrm{End}(V)$ is isomorphic to $\mathcal{O}$. In the case of elliptic curves, the class of an ideal $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of elliptic curves via a degree-$\mathcal{N}(\mathfrak{a})$ isogeny. The action of the class of $\mathfrak{a}$ is harder to evaluate as $\mathcal{N}(\mathfrak{a})$ gets large. The method used by Jao [20] to obtain a subexponential time algorithm was to find a relation $\mathfrak{a}=(\phi)\mathfrak{p}_1\cdots\mathfrak{p}_N$ where $\mathcal{N}(\mathfrak{p}_i)\le B$ for a subexponential value B. In general, we only know how to explicitly evaluate isogenies arising from the action of polarized ideals, that is pairs of the form $(\mathfrak{a},\gamma)$ where $\mathfrak{a}\bar{\mathfrak{a}}=(\gamma)$, $\gamma\in K_+$ totally positive and K_+ is the totally real subfield of K. We therefore look for relations in the polarized class group $\mathfrak{C}(\mathcal{O})$ which is defined as

$$\mathfrak{C}(\mathcal{O}):=\{\text{Polarized ideals of }\mathcal{O}\}/\{\text{Principal polarized ideals of }\mathcal{O}\}.$$

A given relation between ideals of $\mathcal{O}$ is unlikely to involve only polarized ideals. However, as described in Bisson's doctoral thesis [5], one can send a relation to the reflex field K^r of K via the type norm map and send it back to K via the reflex type norm map. Ideals arising as the image of an ideal of K^r via the reflex type norm are polarized. We illustrate this method in Figure 1.

Figure 1: Map between K and K^r


K^c
K
K^r
$\mathcal{N}_\Phi$
$\mathcal{N}_{\Phi^r}$
$(\phi)=\mathfrak{p}_1\cdots\mathfrak{p}_k$
$\mathcal{N}_\Phi(\mathfrak{p}_i)=\mathfrak{p}'_i$
$(\phi')=\mathfrak{p}'_1\cdots\mathfrak{p}'_k$
$(\gamma)=(\mathfrak{q}_1,\gamma_1)\cdots(\mathfrak{q}_k,\gamma_k)$
$\mathcal{N}_{\Phi^r}(\mathfrak{p}'_j)=\mathfrak{q}_j$

Therefore, relations in $\mathfrak{C}(\mathcal{O})$ can be obtained from relations in $\mathrm{Cl}(\mathcal{O})$. The complexity of our algorithms for computing relations in $\mathrm{Cl}(\mathcal{O})$ depends on the properties of the defining polynomial of K. Let χ be a q-Weil polynomial defining the CM field K in which we work, and $(\alpha_i)_{i\leq 2g}$ such that $\chi = \prod_i (X - \alpha_i)$. We have $|\alpha_i| = \sqrt{q}$ and

$$|\operatorname{Disc}(\chi)| = \prod_{i\neq j} |\alpha_i - \alpha_j| \leq (2\sqrt{q})^{\binom{2g}{2}}. \tag{6}$$

The conditions of Theorem 3.3 and Proposition 3.1 on the degree and the height of the defining polynomial of K translate into conditions on the dimension g and the cardinality q of the field of definition $\mathbb{F}_q$ of the Abelian varieties having complex multiplication by $\mathcal{O}$. From (6), we see that $\log(|\operatorname{Disc}(\chi)|) \leq O(g^2 \log(q)(1 + o(1))$. In most cases, the quantity $g^2\log(q)$ also gives a lower bound on $\log(|\operatorname{Disc}(\chi)|)$ when $g \sim \log(q)^\delta$ for some $\delta > 0$. For this, we need the roots of χ to be reasonably spaced. More precisely, if for some $1/2 > \varepsilon > 0$ we have $|e^{i\theta_j} - e^{i\theta_k}| \geq \frac{1}{p^\varepsilon}$, then $\log(|\operatorname{Disc}(\chi)|) \geq O(g^2 \log(q)(1 + o(1))$. The probability that two complex numbers $e^{i\theta_j}, e^{i\theta_k}$ on the unit circle satisfy $|e^{i\theta_j} - e^{i\theta_k}| < \frac{1}{p^\varepsilon}$ is asymptotically the same has the probability for having $|\theta_j - \theta_k| < \frac{1}{p^\varepsilon}$. Therefore, if $(\theta_j)_{j\leq 2g}$ are equidistributed then we have

$$\Pr\left(\forall j,k,\ |e^{i\theta_j} - e^{i\theta_k}| \geq \frac{1}{p^\varepsilon}\right) = \prod_{l\leq 2g}\left(1 - l\cdot\frac{1}{p^\varepsilon}\right) \to 1. \text{ when } g \to \infty.$$

An interesting special case is the restriction to families of Abelian varieties that are Jacobian varieties of curves. In this case, it is not guarantied that the $(\theta_j)_{j\leq 2g}$ are equidistributed. However, there is a result of Katz and Sarnak [22] that ensures that even with such a statistical bias, the distribution of eigenangles remains close to uniform.

Theorem 4.1 (Katz-Sarnak)**.** *Let $\mathcal{M}_g(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-isomorphism classes of genus-g curves over $\mathbb{F}_q$ and* $\operatorname{discrep}(\mu,\nu) := \operatorname{Sup}_{s\in\mathbb{R}} |\operatorname{CDF}_\mu(s) - \operatorname{CDF}_\nu(s)|$, *where* $\operatorname{CDF}_\mu(s) := \int_{]-\infty,s]} d\mu$. *Then*

$$\lim_{g\to\infty}\lim_{q\to\infty}\left(\frac{1}{|\mathcal{M}_g(\mathbb{F}_q)|}\right)\sum_{\mathcal{C}\in\mathcal{M}_g(\mathbb{F}_q)} \operatorname{discrep}(\mu(univ), \mu(\mathcal{C}/\mathbb{F}_q)) = 0,$$

where μ is the spacing measure and $\mu(univ)$ is the limit of $\mu(U(N))$ as N grows to infinity where $U(N)$ is the unitary group of size N.

Asymptotically, when $g \sim \log(q)^\delta$ for some $\delta > 0$, we have $\log(|\operatorname{Disc}(\chi)|) = \Theta(g^2\log(q)(1 + o(1))$ with probability 1. We can apply Algorithm 2 and Algorithm 4 from the perspective of an Abelian variety.

Proposition 4.2 (GRH-Heuristic 1)**.** *Let $\mathcal{F}$ be an infinite family of dimension g CM Abelian varieties over $\mathbb{F}_q$ such that $g \sim \log(q)^\delta$ for some $\delta > 0$, and let $\mathcal{O}$ be an order in the center K of $\mathbb{Q}\otimes\operatorname{End}(V)$ for some $V \in \mathcal{F}$. Then there is an algorithm that returns a B-smooth decomposition of an ideal $\mathfrak{a} \subseteq \mathcal{O}$ in time*

$$\log(\mathcal{N}(\mathfrak{a}))^{1+o(1)} L_{g^2\log(q)}(\alpha, c_1) \text{ where } B = L_{g^2\log(q)}(\alpha, c_2) \text{ for some } c_1, c_2 > 0.$$

The value of α is

- *$\alpha = 1/2$ in the general case.*
- *$\alpha = 1/3$ when $\delta = 1$.*

Furthermore, with asymptotic probability 1 we have

$$g^2\log(q) = \Theta(\log(|\operatorname{Disc}(\chi)|)(1 + o(1)),$$

even if we restrict ourselves to families of Jacobians of curves.

Proof. When $g \sim \log(q)^{\delta}$, then $g \sim \left(g^2 \log(q)\right)^{\alpha}$ for some $\alpha \leq 1/2$, thus falling in the range of applicability of the $L(1/2)$ algorithm. In addition, $g \sim \left(g^2 \log(q)\right)^{1/3}$ happens when $g \sim \log(q)^{1/3}$, thus ensuring that Algorithm 4 runs in heuristic expected time $L_{g^2 \log(q)}(1/3, c)$ for some $c > 0$. The relation between $g^2 \log(q)$ and $\log\left(|\operatorname{Disc}(\chi)|\right)$ results from the above discussion. □

Once a relation between classes of ideals of reasonably small norm is found in $\mathfrak{C}(\mathcal{O})$, the evaluation of its action boils down to the evaluation of the action of all the ideals in the relation. If $\mathfrak{a} \sim \mathfrak{p}_1 \cdots \mathfrak{p}_k$ in $\mathfrak{C}(\mathcal{O})$, then evaluating the action of $\mathfrak{a}$ (via a degree $\mathcal{N}(\mathfrak{a})$ isogeny) boils down to evaluating that of all the $\mathfrak{p}_i$ for $i \leq k$. Evaluating an isogeny corresponding to a given ideal $\mathfrak{p}$ of norm l (i.e. an $(\mathbb{Z}/l\mathbb{Z})^g$-isogeny) between Abelian varieties expressed in a system of theta coordinates can be done following the approach of Lubicz and Robert [25]. When the l-torsion is known, evaluating an $(\mathbb{Z}/l\mathbb{Z})^g$-isogeny can be done in time $l^{O(g)}$. Although exponential in g, this is still subexponential in $e^{g^2 \log(q)}$. The main obstruction for a direct application of Proposition 4.2 to a generalization of Jao's subexponential method for the computation of a large degree isogeny [20] is the computation of the l-torsion. Indeed, the classical approach involves drawing points at random, which is computationally very expensive since a dimension-g Abelian variety is represented by equations between at least 4^g coordinates (in the case of a representation by level 4 theta coordinates).

5 Conclusion and future perspectives

We presented an algorithm to derive an $L_{\Delta}(\alpha, c_1)$-smooth relation in heuristic expected time $L_{\Delta}(\alpha, c_2)$ in $\mathrm{Cl}(\mathcal{O})$ for some order in a number field, where $c_1, c_2 > 0$ and $0 < \alpha < 1$. We achieve a subexponential complexity even in classes of number field of degree growing to infinity, which is a significant improvement over the Buchmann method [6], and we are able to work with ideals in any non-maximal order unlike in [2] where we restricted ourselves to the equation order. We showed direct applications of Algorithm 2 and Algorithm 4 to computational number theory and cryptology.

Our decomposition algorithms could be generalized to find $L_{\Delta}(\alpha, c_1)$-smooth relations in heuristic expected time $L_{\Delta}(\beta, c_2)$ for $\alpha \neq \beta$. This would be useful in particular in the context of isogeny evaluation where one might want to spend more time to get a decomposition over ideals of smaller norm. Indeed, when evaluating an isogeny, we need to account for the cost action of the ideals occurring the relations. The $\mathfrak{q}$-descent could also be generalized to wider classes of number field to derive relations in time $L_{\Delta}(\alpha, c)$ for $1/2 > \alpha > 1/3$. It would be interesting to have a panorama of the classes of number fields for which Algorithm 4 outperforms Algorithm 2. Finally, improving the the enumeration of short lattice vectors would result in a significant improvement to the $\mathfrak{q}$-descent since it is a bottleneck that forces us to restrict the classes of number fields to which it applies.

Acknowledgments

The author thanks the organizers of the GEOCRYPT 2013 conference. We are also grateful to Gaetan Bisson and Damien Robert for providing us with valuable insight on the evaluation of isogenies between Abelian varieties represented by a system of theta coordinates. Finally, we thank Damien Stehlé for his comments on problems relevant to the geometry of numbers.

References

[1] L. Adleman and J. DeMarrais, *A subexponential algorithm for discrete logarithms over all finite fields*, Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology

Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings (D. Stinson, ed.), Lecture Notes in Computer Science, vol. 773, 1993, pp. 147–158.

[2] J-F. Biasse, *An $L(1/3)$ algorithm for ideal class group and regulator computation in certain number fields*, To appear in *Mathematics of Computation.*

[3] J.-F. Biasse and C. Fieker, *New techniques for computing the ideal class group and a system of fundamental units in number fields*, CoRR **abs/1204.1294** (2012).

[4] I. Biehl, J. Buchmann, S. Hamdy, and A. Meyer, *A signature scheme based on the intractability of computing roots*, Des. Codes Cryptography **25** (2002), no. 3, 223–236.

[5] G. Bisson, *Endomorphism rings in cryptography*, Ph.D. thesis, LORIA, Nancy, France, 2011.

[6] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–1989 (Boston) (Catherine Goldstein, ed.), Progress in Mathematics, Birkhäuser, 1990, pp. 27–41.

[7] J. Buchmann and S. Paulus, *A one way function based on ideal arithmetic in number fields*, CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (London, UK), Springer-Verlag, 1997, pp. 385–394.

[8] J. Buchmann and H. C. Williams, *A key-exchange system based on real quadratic fields*, CRYPTO '89, Lecture Notes in Computer Science, vol. 435, 1989, pp. 335–343.

[9] Johannes Buchmann and Ulrich Vollmer, *Binary quadratic forms: An algorithmic approach*, Algorithms and Computation in Mathematics, vol. 20, Springer-Verlag, 2007.

[10] J. Cassels, *An introduction to the geometry of numbers*, Classics in Mathematics, Springer-Verlag, Berlin, 1997, Corrected reprint of the 1971 edition.

[11] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Number Theory, Lecture notes in Math. **1068** (1983), 33–62.

[12] Andreas Enge, Pierrick Gaudry, and Emmanuel Thomé, *An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves.*

[13] C. Gentry, *A fully homomorphic encryption scheme*, Ph.D. thesis, Stanford University, 2009, crypto.stanford.edu/craig.

[14] ———, *Fully homomorphic encryption using ideal lattices*, Proceedings of the 41st annual ACM symposium on Theory of computing (New York, NY, USA), STOC '09, ACM, 2009, pp. 169–178.

[15] D. Gordon, *Discrete logarithms in GF(p) using the number field sieve*, SIAM J. Discrete Math **6** (1993), 124–138.

[16] J.L. Hafner and K.S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, Journal of American Society **2** (1989), 839–850.

[17] G. Hanrot and D. Stehlé, *Improved analysis of kannanâĂŹs shortest lattice vector algorithm*, Advances in Cryptology - CRYPTO 2007 (A. Menezes, ed.), Lecture Notes in Computer Science, vol. 4622, Springer Berlin Heidelberg, 2007, pp. 170–186.

[18] M. Jacobson, Á. Pintér, and P. Walsh, *A computational approach for solving $y^2 = 1^k + 2^k + ... + x^k$*, Mathematics of computation **72** (2003), 2099–2110.

[19] M. Jacobson and H.C. Williams, *Solving the pell equation*, CMS Books in Mathematics, Springer-Verlag, 2009.

[20] D. Jao and V. Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, Algorithmic Number Theory (G. Hanrot, F. Morain, and E. Thomé, eds.), Lecture Notes in Computer Science, vol. 6197, Springer Berlin Heidelberg, 2010, pp. 219–233.

[21] A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren, *The number field sieve in the medium prime case*, Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings (Cynthia Dwork, ed.), Lecture Notes in Computer Science, vol. 4117, Springer, 2006, pp. 326–344.

[22] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues and monodromy*, Colloquium Publications, American Mathematical Society, 1998.

[23] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, *The number field sieve*, STOC '90: Proceedings of the twenty-second annual ACM symposium on Theory of computing (New York, NY, USA), ACM, 1990, pp. 564–572.

[24] J.E. Littlewood, *On the class number of the corpus* $p(\sqrt{k})$, Proc. London Math.Soc **27** (1928), 358–372.

[25] D. Lubicz and D. Robert, *Computing isogenies between abelian varieties.*, Compositio Mathematica **148** (2012), no. 5, 1483–1515 (English).

[26] A. Meyer, S. Neis, and T. Pfahler, *First implementation of cryptographic protocols based on algebraic number fields*, ACISP '01: Proceedings of the 6th Australasian Conference on Information Security and Privacy (London, UK), Springer-Verlag, 2001, pp. 84–103.

[27] C.P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoretical Computer Science **53** (1987), no. 2âĂŞ3, 201 – 224.

[28] E. Scourfield, *On ideals free of large prime factors*, Journal de Théorie des Nombres de Bordeaux **16** (2004), no. 3, 733–772.

[29] N. Smart and F. Vercauteren, *Fully homomorphic encryption with relatively small key and ciphertext sizes*, Public Key Cryptography âĂŞ PKC 2010 (P. Nguyen and D. Pointcheval, eds.), Lecture Notes in Computer Science, vol. 6056, Springer Berlin Heidelberg, 2010, pp. 420–443.

[30] U. Vollmer, *Asymptotically fast discrete logarithms in quadratic number fields*, Algorithmic Number Theory — ANTS-IV, Lecture Notes in Computer Science, vol. 1838, 2000, pp. 581–594.