

ANTS X Proceedings of the Tenth Algorithmic Number Theory Symposium

Improved techniques for computing the
ideal class group and a system of
fundamental units in number fields

Jean-François Biasse and Claus Fieker



Improved techniques for computing the ideal class group and a system of fundamental units in number fields

Jean-François Biasse and Claus Fieker

We describe improvements to the subexponential methods for computing the ideal class group, the regulator and a system of fundamental units in number fields under the generalized Riemann hypothesis. We use sieving techniques adapted from the number field sieve algorithm to derive relations between elements of the ideal class group, and p -adic approximations to manage the loss of precision during the computation of units. These improvements are particularly efficient for number fields of small degree for which a speedup of an order of magnitude is achieved with respect to the standard methods.

1. Introduction

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n and discriminant Δ . In this paper, we present improved fast methods for computing the structure of the ideal class group of the maximal order $\mathbb{O}_K$ of K , along with the regulator and a system of fundamental units of $\mathbb{O}_K$.

Class group and unit group computation are two of the four principal tasks for computational algebraic number theory postulated by Zassenhaus (together with the computation of the ring of integers and the Galois group). In particular, they occur in the resolution of Diophantine equations. For example, the Pell equation

$$T^2 - \Delta U^2 = 1, \quad T, U \in \mathbb{Z},$$

boils down to finding the fundamental unit in a real quadratic number field of discriminant Δ (see [26]). In addition, the Schäffer equation

$$y^2 = 1^k + 2^k + \cdots + (x-1)^k, \quad k \geq 2,$$

MSC2000: primary 54C40, 14E20; secondary 46E25, 20C20.

Keywords: number fields, ideal class group, regulator, units, index calculus, subexponentiality.

can be solved using solutions to the Pell equation [24]. Unit computations are key ingredients in solving almost all Diophantine equations, for example when solving Thue equations [8]. On the other hand, the computation of the ideal class group $\text{Cl}(\mathbb{O}_K)$ of a number field K allows in particular to provide numerical evidence in favor of unproven conjectures such as the heuristics of Cohen and Lenstra [14] on the ideal class group of a quadratic number field, Littlewood's bounds [32] on $L(1, \chi)$, or Bach's bound on the minimal bound B such that ideals of norm lower than B generate the ideal class group. The class group enters also into the computation of the Mordell-Weil group of elliptic curves with the descent method, or the Brauer group computations for representation theory [16].

In 1968, Shanks [41; 42] proposed an algorithm relying on the baby-step giant-step method to compute the structure of the class number and the regulator of a quadratic number field in time $O(|\Delta|^{1/4+\epsilon})$, or $O(|\Delta|^{1/5+\epsilon})$ under the extended Riemann hypothesis [30]. In 1985 Pohst and Zassenhaus [37] published an algorithm that could determine the class group of arbitrary number fields. Then, a subexponential strategy for the computation of the group structure of the class group of an imaginary quadratic field was described in 1989 by Hafner and McCurley [21]. The expected running time of this method is bounded by $L_\Delta(1/2, \sqrt{2} + o(1))$ where

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

Buchmann [11] generalized this result to the case of an arbitrary extension, the heuristic complexity being valid for fixed degree n and Δ tending to infinity. In a recent work [6], Biasse described an algorithm achieving the heuristic complexity $L_\Delta(1/3, O(1))$ for certain classes of number fields where both the discriminant and the degree tend to infinity.

In parallel with theoretical improvements, considerable efforts have been invested to make the implementations of the subexponential methods efficient. In the quadratic case, Jacobson [25] described an algorithm based on the quadratic sieve for deriving relations between elements of $\text{Cl}(\mathbb{O}_K)$. He successfully used it for computing the class group and the fundamental unit of quadratic number fields. His implementation contained some of the practical improvements described in the context of factorization such as self-initialization and the single large prime variant. This strategy was later improved by Biasse [7] who used a double large prime variant and a dedicated Gaussian elimination technique. Attempts have been made to generalize sieving techniques to general number fields [12; 34]. A variant of the number field sieve was used for deriving relations in the class group of cubic fields. On special classes of cubic number fields for which the regulator can be precomputed, it allowed the computation of the ideal class group. Promising timings were presented in [12; 34], for sizes of factor base that do not (to the best

of our knowledge) certify the result under the generalized Riemann hypothesis. In particular, a significant speedup was obtained over the standard random ideal factorization method.

Our contribution. In this paper, we present an algorithm based on sieving techniques adapted from recent implementations of the number field sieve [28] for computing $\text{Cl}(\mathbb{O}_K)$ under the generalized Riemann hypothesis (GRH) for an arbitrary number field K . We also describe a p -adic method for computing the regulator and a system of fundamental units. We show that these methods allow a significant improvement for number fields of low degree over the current state of the art based on enumeration techniques.

2. Generalities on number fields

Let K be a number field of degree d . It has $r_1 \leq d$ real embeddings $(\sigma_i)_{i \leq r_1}$ and $2r_2$ complex embeddings $(\sigma_i)_{r_1 < i \leq d}$ coming as r_2 pairs of conjugates, which we number so that $\sigma_{i+r_2} = \overline{\sigma_i}$ for $r_1 < i \leq r_1 + r_2$. The field K is isomorphic to $\mathbb{O}_K \otimes \mathbb{Q}$ where $\mathbb{O}_K$ denotes the ring of integers of K . We can embed K in $K_{\mathbb{R}} := K \otimes \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, and extend the σ_i to $K_{\mathbb{R}}$. Let T_2 be the Hermitian form on $K_{\mathbb{R}}$ defined by $T_2(x, x') := \sum_i \sigma_i(x) \overline{\sigma_i(x')}$, and let $\|x\| := \sqrt{T_2(x, x)}$ be the corresponding L_2 -norm. Choose $(\alpha_i)_{i \leq d}$ such that $\mathbb{O}_K = \bigoplus_i \mathbb{Z}\alpha_i$; then the discriminant of K is given by $\Delta = \det^2(T_2(\alpha_i, \alpha_j))$. The norm of an element $x \in K$ is defined as $\mathcal{N}(x) = \prod_i \sigma_i(x)$.

Let $\mathcal{I}$ be the group of nonzero fractional ideals of K and $\mathcal{P} \subseteq \mathcal{I}$ is the subgroup of principal fractional ideals. The norm of integral ideals is given by $\mathcal{N}(I) := [\mathbb{O}_K : I]$, which extends to fractional ideals by $\mathcal{N}(I/J) := \mathcal{N}(I)/\mathcal{N}(J)$. The norm of a principal ideal agrees with the norm of its generator: $\mathcal{N}(x\mathbb{O}_K) = |\mathcal{N}(x)|$.

The ideal class group of $\mathbb{O}_K$ is defined by $\text{Cl}(\mathbb{O}_K) := \mathcal{I}/\mathcal{P}$. We denote by $[\mathfrak{a}]$ the class of a fractional ideal $\mathfrak{a}$ in $\text{Cl}(\mathbb{O}_K)$ and by h the cardinality of $\text{Cl}(\mathbb{O}_K)$. Elements of $\mathcal{I}$ admit a unique decomposition as a power product of prime ideals of $\mathbb{O}_K$ (with possibly negative exponents). An element $x \in \mathbb{O}_K$ is said to be a unit if $(x)\mathbb{O}_K = \mathbb{O}_K$, or equivalently if $|\mathcal{N}(x)| = 1$. The units of $\mathbb{O}_K$ form a multiplicative group of the form

$$U = \mu \times \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_r \rangle,$$

where μ is the torsion subgroup of U , $r := r_1 + r_2 - 1$ and the generators γ_i of the nontorsion part are called a system of fundamental units. The regulator is an invariant of K which allows us to certify the calculation of $\text{Cl}(\mathbb{O}_K)$ and U . It is defined as $R = \text{Vol}(\Gamma)$ where Γ is the lattice generated by vectors of the form

$$(c_1 \log|\gamma_i|_1, \dots, c_{r+1} \log|\gamma_i|_{r+1}),$$

with $|x|_i := |\sigma_i(x)|$ for $i \leq r+1$, $c_1 = 1$ for $i \leq r_1$, $c_i = 2$ otherwise.

3. The subexponential strategy

The idea behind the algorithm of Buchmann [11] is to find a set of ideals $\mathcal{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$ whose classes generate $\text{Cl}(\mathbb{O}_K)$, and then consider the surjective morphism

$$\begin{aligned} \mathbb{Z}^n &\xrightarrow{\varphi} I \xrightarrow{\pi} \text{Cl}(\mathbb{O}_K) \\ (e_1, \dots, e_N) &\longmapsto \prod_i \mathfrak{p}_i^{e_i} \longmapsto \prod_i [\mathfrak{p}_i]^{e_i}. \end{aligned}$$

From the fundamental theorem of homomorphisms, the ideal class group satisfies $\text{Cl}(\mathbb{O}_K) \simeq \mathbb{Z}^N / \ker(\pi \circ \varphi)$. Therefore, the knowledge of $\ker(\pi \circ \varphi)$, which has the structure of a $\mathbb{Z}$ -lattice, enables us to derive $\text{Cl}(\mathbb{O}_K)$. In the meantime, elements of $\ker(\varphi)$ give us units as power-products of relations. From these units, we hope to derive a system of fundamental units of $\mathbb{O}_K$. The subexponential strategy can be broken down into three essential tasks: collecting relations, calculating the class group and calculating the unit group. The subexponentiality is a consequence of a careful choice of B .

3.1. Relation collection. A preliminary step to the relation collection is the choice of a generating set $\mathcal{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$ of $\text{Cl}(\mathbb{O}_K)$. We choose the set of prime ideals of norm bounded by an integer B . The use of the Minkowski bound certifies the result unconditionally, but it causes the algorithm to take a time exponential in the size of Δ . To achieve subexponentiality, many authors chose the bound of Bach [2], who proved that under GRH, $\text{Cl}(\mathbb{O}_K)$ was generated by the classes of the prime ideals $\mathfrak{p}$ satisfying $\mathcal{N}(\mathfrak{p}) \leq 12(\log |\Delta|)^2$. Although asymptotically better, in practice this bound can be larger than the one described by Belabas et al. [4] who stated that under GRH, the class group is generated by the classes of the prime ideals of norm bounded by B provided that

$$\begin{aligned} \sum_{(m, \mathfrak{p}): \mathcal{N}(\mathfrak{p}^m) \leq B} \frac{\log \mathcal{N}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p}^{m/2})} \left(1 - \frac{\log \mathcal{N}(\mathfrak{p}^m)}{\log B} \right) \\ > \frac{1}{2} \log |\Delta| - 1.9n - 0.785r_1 + \frac{2.468n + 1.832r_1}{\log B}. \end{aligned}$$

In the rest of the paper, we assume that $\mathcal{B}$ is constructed with the bound of Belabas et al. Indeed, Bach's bound enlarges the dimensions of the matrices that are processed during the computation of $\text{Cl}(\mathbb{O}_K)$, thus inducing a slow-down that is not compensated by the fact that the relations are found more rapidly.

During the relation collection phase, we collect relations of the form

$$(\phi_i) = \mathfrak{p}_1^{e_{i,1}} \cdots \mathfrak{p}_N^{e_{i,N}},$$

where $\phi_i \in K$. We progressively build the matrix $M := (e_{i,j}) \in \mathbb{Z}^{k \times N}$ where k is the number of relations collected so far. Let $\Lambda \subseteq \ker(\pi \circ \varphi)$ be the lattice generated

$$UM = \begin{pmatrix} h_{11} & 0 & \cdots & 0 \\ \vdots & h_{22} & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ * & * & \cdots & h_{NN} \\ \text{.....} \\ (0) \end{pmatrix},$$

3.2. Class group computation. Given a matrix $A \in \mathbb{Z}^{N \times N}$ whose rows generate $\ker(\pi \circ \varphi)$, unimodular transformations on both rows and columns of A yield the structure of $\text{Cl}(\mathcal{O}_K)$. More precisely, for every nonsingular matrix $A \in \mathbb{Z}^{N \times N}$, there exist unimodular matrices $U, V \in \mathbb{Z}^{N \times N}$ such that

where $d_{i+1} \mid d_i$ for all i with $1 \leq i < N$. The matrix S is called the Smith normal form (SNF) of A .

$$\mathrm{Cl}(\mathbb{O}_K) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_N\mathbb{Z}.$$

Once enough relations have been found, the rows of M generate $\ker(\pi \circ \varphi)$, and the N nonzero rows of the HNF of M are a matrix $A \in \mathbb{Z}^{N \times N}$ whose rows are a basis for $\ker(\pi \circ \varphi)$, and the SNF of A gives us $\text{Cl}(\mathbb{O}_K)$. However, finding the structure of $\text{Cl}(\mathbb{O}_K)$ can also be done by computing the SNF of a matrix which is in practice significantly smaller than A , namely the essential part of A . Indeed, for each matrix H in HNF, there exists an index l such that $h_{i,i} = 1$ for all $i > l$. The upper left $l \times l$ submatrix of H is called its essential part. As the classes of $\mathfrak{p}_i$ for $i > l$ are generated by those of the $\mathfrak{p}_j$, $j \leq l$, the SNF of the essential part of A suffices to recover $\text{Cl}(\mathbb{O}_K)$.

3.3. Regulator and fundamental units computation. Computing the regulator and a system of fundamental units of K consists of finding kernel vectors of M . Indeed, if $X = (x_1, \dots, x_k)$ satisfies $XM = 0$, then we have

$$\left(\prod_i \phi_i^{x_i}\right) \mathbb{O}_K = \mathbb{O}_K.$$

In other words, $\gamma := \prod_i \phi_i^{x_i}$ is a unit. Every kernel vector X of M yields a unit, and we want to compute the group generated by all those elements as well as the regulator of this group, defined to be zero if the group is not of full rank. So far, finding of relations between units is mostly done using real linear algebra (LLL), the core problem here being the numerical instability of the matrices. This in itself is a consequence of the well-known fact that units are very large in general: Writing the fundamental unit of a real quadratic fields explicitly with the canonical basis needs exponentially many digits while it is always possible to find a product representation of size polynomial in $\log|\Delta|$ (see [13; 43]). At the end of the procedure, we verify that the assumption we made on the completeness of the lattice of relations is true. To this end, we use an approximation of the Euler product

$$hR = \frac{|\mu| \sqrt{|\Delta|}}{2^{r_1} (2\pi)^{r_2}} \lim_{s \rightarrow 1} ((s-1)\zeta_K(s)),$$

where $\zeta_K(s) = \sum_{\mathfrak{a}} 1/\mathcal{N}(\mathfrak{a})^s$ is the usual ζ -function associated to K and $|\mu|$ is the cardinality of μ . Indeed, it allows us to derive a bound h^* in polynomial time under ERH that satisfies $h^* \leq hR < 2h^*$; see [3]. If the values $\det(\Gamma)$ and $\det(\Lambda)$ do not satisfy this inequality, then we need to collect more relations.

4. Sieving techniques

In this section, we describe sieving techniques to derive relations in $\text{Cl}(\mathbb{O}_K)$ for general number fields. This is a generalization of Jacobson's results [25] for quadratic number fields. Similar ideas were suggested in [12; 34] but the corresponding algorithms were either not implemented or are no longer available for comparison. Here we provide numerical data illustrating the considerable impact of these techniques for class group and unit group computation in the case of low degree number fields.

Given a generating set $\mathcal{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$ for $\text{Cl}(\mathbb{O}_K)$, the usual method for deriving relations consists of computing random exponents $\vec{e} := (e_1, \dots, e_N)$, $\alpha \in \mathbb{O}_K$ and a reduced ideal $I_{\vec{e}}$ such that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = (\alpha) I_{\vec{e}}.$$

Then, every time $I_{\vec{e}}$ is $\mathcal{B}$ -smooth (that is, is a power product of elements of $\mathcal{B}$), we obtain a relation. As the arithmetic of ideals is rather expensive when $n > 2$, the relation search in the computer algebra software PARI [35] and versions 2.x for $x < 18$ of Magma [9] consists of enumerating short elements of $I_{\vec{e}}$ via the Fincke-Pohst method [18].

Our method consists of deriving relations from smooth values of polynomials, thus avoiding the cost of the ideal arithmetic and of the ideal reduction. Our method for finding smooth values is based on the recent development of the number field sieve algorithm [28]. The use of trivial methods such as trial division for finding smooth values of our polynomials would yield the same theoretical complexity, but would be impractical for large discriminants. The most efficient implementation of the enumeration-based strategy for finding relations is the one of PARI. Therefore, in the following, we assess the impact of our sieving method by comparing its performance with those of PARI.

4.1. Polynomial selection. Let $\mathfrak{a}$ be a $\mathcal{B}$ -smooth ideal of $\mathbb{O}_K$. In this section, we show how to provide polynomials $P \in \mathbb{Z}[X, Y]$ of degree n derived from $\mathfrak{a}$ such that every $(x, y) \in \mathbb{Z}^2$ such that $P(x, y)$ is $\mathcal{B}$ -smooth yields a relation. Note that in theory, $\mathfrak{a}$ can be any ideal, however, we obtained the best results by choosing $\mathfrak{a} = \mathbb{O}_K$. Let α and β be two linearly independent elements of $\mathfrak{a}$. Then, we create by interpolation a $P_{\alpha, \beta} \in \mathbb{Z}[X, Y]$ such that

$$P_{\alpha, \beta}(x, y) = \mathcal{N}(x\alpha + y\beta) \quad \text{for all } x, y \in \mathbb{Z}^2.$$

Every time $\phi_{x, y} := x\alpha + y\beta$ has a smooth norm, we add the relation corresponding to the principal ideal $(\phi_{x, y})$ to the relation matrix. Before applying sieving algorithms to $P_{\alpha, \beta}$ to derive relations, we need to ensure that it is likely to yield enough smooth values. Polynomial selection is an important part of the number field sieve algorithm, and so it is in our algorithm. However, the specificities of our context prevent us from directly adapting the methods of NFS for selecting the sieving polynomial. First of all, we can afford to find relations with many different choices of α and β , whereas the choice of a sieving polynomial in the NFS algorithm is fixed. We require that our choices of α and β yield polynomials with small coefficients, and that we have a sufficient randomization at the infinite places to avoid drawing $\phi_{x, y}$ spanning the same subgroup of the unit group of $\mathbb{O}_K$.

To randomize the choice of α, β , we consider random coefficients $a_1, \dots, a_n \in \mathbb{R}^n$ such that $\sum_{i \leq n} a_i = 0$. For every such n -tuple $\vec{a}$, we define the embedding

$$\psi_{\vec{a}} : \mathfrak{a} \rightarrow \mathbb{R}^n, \quad \alpha \mapsto (a_1 \log|\alpha|_1, \dots, a_n \log|\alpha|_n).$$

For every choice of $\vec{a}$, the set of elements of the form $\psi_{\vec{a}}(\alpha)$ for $\alpha \in \mathfrak{a}$ is a lattice $\Lambda_{\vec{a}}$ of $\mathbb{R}^n$ for which we can find an LLL reduced basis for the norm

$$T_2^{\vec{a}} : (x_1, \dots, x_n) \mapsto e^{2a_1} x_1^2 + \dots + e^{2a_n} x_n^2.$$

For every choice of $\vec{a}$, the first two vectors α, β of an LLL reduced basis of $\Lambda_{\vec{a}}$ are potential candidates for the creation of a polynomial yielding smooth values. Every time we draw such a pair of elements of $\mathfrak{a}$, we need to make sure that they do not generate the same $\mathbb{Z}$ -module as another pair previously used. To prevent this from happening, every time we draw a pair α, β by the previous method, we express them in terms of the canonical $\mathbb{Z}$ -basis of $\mathbb{O}_K$. Thus, to every pair α, β corresponds the matrix $M_{\alpha, \beta} \in \mathbb{Z}^{2 \times n}$ of their coordinates. The HNF of $M_{\alpha, \beta}$ uniquely represents the $\mathbb{Z}$ -module spanned by (α, β) . Thus, to avoid duplicates, we store a hash of the HNF of $M_{\alpha, \beta}$ in a hash table every time we use a pair (α, β) to draw relations. We summarize the procedure of the selection of a sieving polynomial in Algorithm 1.

Algorithm 1 (Polynomial selection).

Input: $\mathfrak{a}, (A_1, \dots, A_n), \text{HashTable}$.

Output: Sieving polynomial $P_{\alpha, \beta}$ corresponding to $\alpha, \beta \in \mathfrak{a}$.

- 1: **while** a new α, β has not been found **do**
 - 2: Draw $|a_1| \leq A_1, \dots, |a_n| \leq A_n$ at random such that $a_1 + \dots + a_n = 0$.
 - 3: Let α and β be the first two elements of a LLL-reduced basis of $\Lambda_{\vec{a}}$ for $\vec{a} = (a_1, \dots, a_n)$.
 - 4: Compute the hash $h_{\alpha, \beta}$ of the HNF of $M_{\alpha, \beta}$.
 - 5: **if** $h_{\alpha, \beta} \notin \text{HashTable}$ **then**
 - 6: Compute by interpolation $P_{\alpha, \beta} \in \mathbb{Z}[X, Y]$ with $P_{\alpha, \beta}(x, y) = \mathcal{N}(x\alpha + y\beta)$.
 - 7: **end if**
 - 8: **end while**
 - 9: **return** $\alpha, \beta, P_{\alpha, \beta}$.
-

4.2. Line sieving. The quadratic sieve algorithm [39] used to derive smooth values of a binary quadratic form generalizes to the case of polynomials of arbitrary degree. Its design follows from the observation that if $P \in \mathbb{Z}[X, Y]$ is a polynomial of degree n , then

$$p \mid P(r_p, y_0) \quad \text{for all } y_0 \in \mathbb{Z} \quad \implies \quad p \mid P(r_p + ip, y_0) \quad \text{for all } i \in \mathbb{Z}. \quad (1)$$

Given $y_0 \in \mathbb{Z}$, we wish to find the $x \in [-I/2, I/2]$ such that $P(x, y_0)$ is B -smooth, where B is the bound on the norm of the prime ideals in the factor base. Instead of trying them all, we prefer to isolate a short list of good candidates that we test by trial division. If $p \mid P(x, y_0)$ for many $p \leq B$, then $P(x, y_0)$ is likely to be B -smooth. From (1), we know that once we have one root r_p of $P(X, y_0) \bmod p$, then we can derive all the others by translation by $(p, 0)$. Line sieving consists of initializing to zero an array S of length I whose cells represent the $x \in$

$[-I/2, I/2]$. Then, for each $p \leq B$, we compute the smallest roots $x_p \in [-I/2, I/2]$ of $P(X, y_0) \bmod p$ and repeat

$$S[x_p] \leftarrow S[x_p] + \log p, \quad x_p \leftarrow x_p + p.$$

Then, whenever $S[x] \approx \log P(x, y_0)$ for $x \in [-I/2, I/2]$, the value $P(x, y_0)$ is likely to be B -smooth. We summarize this procedure in Algorithm 2.

Algorithm 2 (Line sieving).

Input: $P \in \mathbb{Z}[X, Y]$, $I, B, y_0 \in \mathbb{Z}$.

Output: Smooth values of $P(X, y_0)$ in $[-I/2, I/2]$.

```

1:  $L \leftarrow \emptyset$ ;  $S[x] \leftarrow 0$  for all  $x \in [-I/2, I/2]$ .
2: for  $p \leq B$  do
3:   Let  $x_p$  be the smallest root of  $P(X, y_0) \bmod p$  in  $[-I/2, I/2]$ .
4:   while  $r_p \leq I/2$  do
5:      $S[x_p] \leftarrow S[x_p] + \log p$ ,  $x_p \leftarrow x_p + p$ .
6:   end while
7: end for
8: for  $x \in [-I/2, I/2]$  do
9:   if  $S[x] \approx \log P(x, y_0)$  then
10:    If  $P(x, y_0)$  is  $B$ -smooth,  $L \leftarrow L \cup \{x\}$ .
11:   end if
12: end for
13: return  $L$ .
```

4.3. Lattice sieving. Let $P_{\alpha, \beta}(X, Y) \in \mathbb{Z}[X, Y]$ be the sieving polynomial described in Section 4.1, B the bound on the norm of the ideals in the factor base, and $I, J \in \mathbb{Z}_{>0}$. Every pair $(x, y) \in [-I/2, I/2[\times [1, J]$ such that $P_{\alpha, \beta}(x, y)$ is B -smooth yields a relations. Therefore, one can repeat the line sieving operation on $P_{\alpha, \beta}(X, y_0)$ for every $y_0 \in [1, J]$. This method is efficient when sieving with primes $p < I$. but when the primes are significantly larger than I , the root computation at Step 3 of Algorithm 2 is often performed for nothing since there is a good chance that none of the $x \in [-I/2, I/2[$ will be a root of $P_{\alpha, \beta}(X, y_0) \bmod p$. A way around that is to have an array S of length IJ representing $[-I/2, I/2[$ and to fill it by line sieving methods for the primes $p < I$ and by lattice sieving for the other primes.

The lattice sieve was first described by Pollard [38]. Since then, it has been extensively studied and improved in the past 15 years, and the most recent developments of this methods yielded the factorization of RSA768 (see [28]). This strategy relies on a one-time enumeration of roots of $P_{\alpha, \beta}(X, Y) \bmod p$ in $[-I/2, I/2[\times [1, J]$. The entry $x \leq IJ$ of the array S that we use to store the logarithmic contributions

corresponds to the pair $(i, j) \in [-I/2, I/2[\times [1, J]$ where

$$i = (x - I/2) \bmod I, \quad j = (x - i - I/2)/I.$$

As in the line sieving case, every entry of S is initialized to zero, and for every $p \leq B$ and every $(i, j) \in [-I/2, I/2[\times [1, J]$ such that $p \mid P_{\alpha, \beta}(i, j)$, we want to perform the operation $S[x] \leftarrow S[x] + \log p$. Line sieving repeated on every line $j \leq J$ allows us to efficiently do this for $p < I$. For the others, we followed the approach of [19], as it is done in [28] for the factorization of RSA768. By [19, Proposition 1], we know that for every p such that we have a root r_p of $P_{\alpha, \beta}(X, 1)$ modulo p , there exists a basis $\{(a, b), (c, d)\}$ of the lattice spanned by $\{(r_p, 1), (p, 0)\}$ that satisfies

- $b > 0$ and $d > 0$;
- $-I < a \leq 0 \leq c < I$;
- $c - a \geq I$.

This basis is computed via an algorithm described in [19] that relies on the continued fraction expansion of r_p . It satisfies $p \mid P_{\alpha, \beta}(ia + jc, ib + jd)$ for all $(i, j) \in \mathbb{Z}^2$. To fill the array S , we start from $(i, j) = (0, 0)$ which is a common root modulo all primes. Then, by induction, we construct the next pair (i', j') from (i, j) by choosing

- $(i, j) + (a, b)$ if $i \geq -a$;
- $(i, j) + (c, d)$ if $i < I - c$;
- $(i, j) + (a, b) + (c, d)$ if $I - c \leq i < -a$.

4.4. Special- q . The sieving space $[-I/2, I/2[\times [1, J]$ only contains a limited number of pairs (i, j) yielding a smooth value. Enlarging I and J might cause its size to rapidly exceed single precision. For a fixed prime q , the special- q strategy consists of sieving with a polynomial P_q derived from the original sieving polynomial P such that

$$\begin{aligned} \forall (i, j) \in [-I/2, I/2[\times [1, J], \quad \exists (x, y) \in \mathbb{Z}^2, \quad P_q(i, j) &= P(x, y), \\ \forall (i, j) \in [-I/2, I/2[\times [1, J], \quad q \mid P_q(i, j). \end{aligned}$$

This strategy was used by Pollard in his original paper [38] to sieve on the rational side, but most current implementations use it on the algebraic side as well [28]. To create P_q for a given q , we need a root r_q of P modulo q . Then, we find a reduced basis $(a_0, b_0), (a_1, b_1)$ of the lattice spanned by the vectors $(q, 0), (r_q, 1)$. The polynomial P_q is then simply given by

$$P_q(i, j) = P(ia_0 + ja_1, ib_0 + jb_1).$$

The reduced basis is given by successive Gaussian reductions, as explained in [19]. Then, to sieve with a given polynomial P , we repeat the procedure described in Section 4.3 for many different polynomials of the form P_q . Fortunately, once the roots of $P \bmod p$ for all $p \leq B$ have been computed, it is possible to use these values to compute the roots of $P_q \bmod p$ for $p \leq B$. Indeed,

$$P(ia_0 + ja_1, ib_0 + jb_1) \equiv 0 \pmod{p}$$

means that there is some root r_p of $P(X, 1) \bmod p$ such that $r_p \equiv \frac{ia_0 + ja_1}{ib_0 + jb_1} \pmod{p}$. This implies that we have $P_q(r_p^q, 1) \equiv 0 \pmod{p}$ for

$$r_p^q \equiv \frac{i}{j} \equiv -\frac{a_1 - r_p b_1}{a_0 - r_p b_0} \pmod{p},$$

which gives us a root of $P_q(X, 1) \bmod p$ from $(a_0, b_0), (a_1, b_1)$ and a root of $P(X, 1) \bmod p$. We summarize our procedure to derive relations from an ideal $\mathfrak{a} \subseteq \mathbb{O}_K$ in Algorithm 3.

Algorithm 3 (Sieving procedure).

Input: $\mathfrak{a} \subseteq \mathbb{O}_K$, $\mathcal{B} = \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$, $I, J \in \mathbb{Z}_{>0}$.

- 1: Select $\alpha, \beta \in \mathbb{O}_K$ and a sieving polynomial $P_{\alpha, \beta}$ with Algorithm 1.
- 2: For all $p \leq B$, compute the roots of $P_{\alpha, \beta}(X, 1) \bmod p$.
- 3: **for** $q \leq B$ **do**
- 4: Compute P_q and its roots modulo the $p \leq B$ as in Section 4.4.
- 5: Let S be an array of size IJ initialized to 0.
- 6: **for** $p \leq I$ **do**
- 7: Do $S[x] \leftarrow S[x] + \log p$ for each x representing $(i, j) \in [-I/2, I/2[\times [1, J]$ such that $p \mid P_q(i, j)$ by repeating Algorithm 2 for each line $j \leq J$.
- 8: **end for**
- 9: **for** $p > I$ **do**
- 10: Calculate a basis $\{(a, b), (c, d)\}$ of the lattice of points in $[-I/2, I/2[\times [1, J]$ that are roots of $P_q(X, Y) \bmod p$ with the method of Section 4.3.
- 11: Do $S[x] \leftarrow S[x] + \log p$ for each x representing $(i, j) \in [-I/2, I/2[\times [1, J]$ such that $p \mid P_q(i, j)$ by using the method of Section 4.3.
- 12: **end for**
- 13: **end for**
- 14: **for** $x \leq IJ$ **do**
- 15: **if** $S[x] \approx \log P_q(i, j)$, where x represent $(i, j) \in [-I/2, I/2[\times [1, J]$ **then**
- 16: If $\log P_q(i, j)$ is B -smooth, store the corresponding relation.
- 17: **end if**
- 18: **end for**

4.5. Overall relation collection phase. A necessary condition to compute the class group and the unit group is to produce a full-rank relation matrix M . Our sieving methods allow us to derive relations in $\text{Cl}(\mathbb{O}_K)$ very rapidly, but it is hard to force a given prime to occur in a relation. The best performance is obtained by sieving with the trivial ideal $\mathbb{O}_K$. If we want to see a given prime ideal $\mathfrak{p} \mid (p)$ occur in a relation, one can use the special- q with $q = p$, or sieve with the ideal $\mathfrak{p}$. However, even after using those methods, some prime ideals still do not contribute to the rank of M . Rather than sieving in random power-products involving missing primes, one might prefer to switch to enumeration-based methods to complete the relation search. To identify the primes that need to appear in a relation, we perform an LU decomposition of the relation matrix modulo a random wordsize prime. We try to produce enough relations with sieving so that the rank of M is 97% of $\#\mathcal{B}$. Then we find additional relations with enumeration. We summarize this procedure:

Algorithm 4 (Full rank relation matrix computation).

Input: K, B .

Output: A full-rank relation matrix for the primes of norm bounded by B .

- 1: $\mathcal{B} \leftarrow \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq B\} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$.
 - 2: Derive N relations by repeating Algorithm 3 with $\mathfrak{a} = (1)$. Let M be the relation matrix.
 - 3: Perform an LU decomposition of M and let `EmptyList` be the list of zero columns.
 - 4: **for** $\mathfrak{p} \in \text{EmptyList}$ **do**
 - 5: Sieve with $\mathfrak{p}$, update M .
 - 6: **end for**
 - 7: Update `EmptyList` by updating the LU decomposition of M .
 - 8: **for** $\mathfrak{p} \in \text{EmptyList}$ **do**
 - 9: Find a relation involving $\mathfrak{p}$ by enumerating short elements in random power-products.
 - 10: **end for**
 - 11: **return** M .
-

To assess the advantage of sieving over enumeration techniques, we need to isolate its contribution to the performances of the class group and unit group computation. To do this, we used a modified version of the function `bnfinit` of the computer algebra software PARI that accepts in input a list of precomputed relations. We interfaced via Sage this version of PARI with a development version of Magma containing a function creating relations with the sieving algorithm. The Magma function tries to create enough relations so that the rank of M is 97% of $\#\mathcal{B}$ and passes it to PARI which adds new relations with enumeration methods

and calculates the class group and the unit group. We compared the performance of this approach to the traditional `bnfinit` function of PARI. There are two main reasons for using a hybrid version. The first one is that PARI's implementation of enumeration techniques is the most efficient. As these are necessary to finish the creation of the relation matrix after calling the sieving algorithm, it is interesting to see how the two perform together. Another reason for this choice is the fact that many different algorithms contribute to the computation of the class group and the unit group. In particular, we use time-consuming linear algebra methods such as the HNF computation. Our methodology avoids the risk of seeing the influence of the quality of the implementation of other algorithms occurring in the class group and unit group computation.

We performed our computations on a 2.6 GHz Opteron with 4 GB of memory. We used a branch of the development version 2.6.0 of PARI provided by Loïc Grenié and the development version of Magma, interfaced via Sage 4.7.2. We allocated 3 GB of memory to the computation made with PARI. For each size d , we drew at random 10 number fields with discriminant satisfying $\log_2|\Delta| = d$. For each discriminant, we computed the class group and the unit group with `bnfinit`, which we refer to as the PARI method, and with the hybrid version which we refer to as the PARI+Sieving method. The average timings, in CPU sec (rounded to the nearest integer), are presented in Table 1. They illustrate the impact of sieving methods for small degree number fields. It is very strong for number fields of degree 3, 4, and 5, for which we often witness a speedup by a factor at least 10, while it is rather moderate for degree-6 number fields, and negligible for number fields of degree 7 and 8. Finding smooth values of a polynomial gets more difficult when we increase its degree, but it is not the only reason why the impact of sieving decreases with the degree. Indeed, for degree 6 number field, our sieving algorithm still derives relations at a competitive pace, but there are many linear dependencies

n	$\log_2 \Delta $	PARI	PARI+Sieving	n	$\log_2 \Delta $	PARI	PARI+Sieving
3	120	76	11	5	120	33	18
3	140	694	66	5	140	295	64
3	160	6828	333	5	160	3402	378
3	180	29807	2453	5	180	16048	2342
4	120	38	7	6	120	40	111
4	140	366	24	6	140	294	161
4	160	4266	175	6	160	1709	1012
4	180	31661	1201	6	180	14549	8413

Table 1. Impact of sieving on class group and unit group computation of small degree number fields. Timings in CPU-seconds.

n	Magma 2.18	PARI	PARI+Sieving
20	0.7	0.5	0.2
30	6	5	3
40	22	44	66
45	128	271	556
50	170	593	1562
54	1453	1085	9251

Table 2. Impact of the quadratic sieve on computations in fields generated by a root of $X^2 + 4(10^n + 1)$. Timings in CPU-seconds.

whereas enumeration allows a more targeted search, thus avoiding linear dependencies. To put these improvements into perspective, we show in Table 2 the impact of Jacobson’s self-initializing quadratic sieve [25] which is implemented in Magma 2.18. The timings for PARI and PARI+Sieving are derived under the same setting as for Table 1. In addition, we added the performances of Magma 2.18 which uses different methods for linear algebra. Timings for the same series of number fields were reported by Jacobson in [25, Table A.3] on a 296-MHz Sun processor (for a fair comparison one has to take into account the verification time since the timings of Table 1 and Table 2 correspond to a certification under GRH).

5. Computing the unit group

Assume that we have created a relation matrix $(e_{i,j})$ corresponding to the relations

$$(\phi_i) = \mathfrak{p}_1^{e_{i,1}} \cdots \mathfrak{p}_N^{e_{i,N}}.$$

Every kernel vector allows us to derive a unit of $\mathbb{O}_K$. Let $\beta_1, \dots, \beta_k$ be a generating set of the units created so far. We compute a new unit β' , and we wish to find a new minimal generating set for $\langle \beta_1, \dots, \beta_k, \beta' \rangle$. Usually this is done by computing (real) logarithms of the units followed by some approximate linear algebra to find a (tentative) relation as well as the (tentative) new basis. This is then followed by some verification of the relation to guarantee correctness, by using real based computations. The difficulty comes from the fact that the entries in the real matrix differ vastly in size — by several orders of magnitude — thus making it necessary to work with a huge precision; in fact the precision is also subexponential in the discriminant for guaranteed results.

Here, we propose to use p -adic logarithms instead. The key advantage comes from the much better control of error propagation in the linear algebra: Unless division by nonunits happens, linear algebra does not increase errors. However, while the correctness is based on the unproven Leopoldt conjecture about the non-vanishing of the p -adic regulator, this is not a problem in practice: Any relation

found by the p -adic method can easily be verified unconditionally, thus a failure of the algorithm would provide a counterexample to Leopoldt's conjecture.

We start by choosing a prime p such that the p -adic splitting field K_p has moderate degree; here we allow at most degree 2. In practice, we search for the smallest prime $p > 10000$ such that the p -adic splitting field is unramified of degree ≤ 2 . Then we have n embeddings $\phi_i : K \rightarrow K_p$, and we define a map $L_p : K^* \rightarrow K_p^n$ given by $x \mapsto (\log \phi_i(x))_i$, where ϕ_i is the usual p -adic logarithm extended to K_p . In order to estimate the necessary p -adic precision, we also need the usual real logarithmic embedding, denoted by $L : K^* \rightarrow \mathbb{R}^{r+1}$. We are looking for a (rational) solution $(x_i)_i \in \mathbb{Q}^{k+1}$ to $\sum x_i L_p(\beta_i) = L_p(\beta')$. Using p -adic linear algebra we will instead get a p -adic solution (or a proof that β' is independent). Using standard rational reconstruction techniques, we derive the rational solution from the p -adic one and then the integral relation between the units. In order to estimate the p -adic precision, we bound numerator and denominator using Cramer's rule and universal lower bounds on the logarithms of units. The rational solution then also satisfies $\sum x_i L(\beta_i) = L(\beta')$. Let $(\alpha_i)_i$ be a basis for $\langle \beta_1, \dots, \beta_s, \beta' \rangle$. By Cramer's rule,

$$x_i = \det(L_p(\beta_1), \dots, L_p(\beta'), \dots, L_p(\beta_s)) / \det(L_p(\beta_1), \dots, L_p(\beta_s)).$$

Since the (unknown) (α_i) form a basis, we see that

$$\det(L_p(\beta_1), \dots, L_p(\beta'), \dots, L_p(\beta_s)) / \det(L_p(\alpha_1), \dots, L_p(\alpha_s))$$

is an integer and the same is true for L instead of L_p ; thus we can write x_i as a quotient of integers. In either case, to make sense of the determinants, we will have to select an appropriate number of rows to make the matrices square. To bound the integers, we make use of the Hadamard bound for $\det(L(\beta_1), \dots, L(\beta'), \dots, L(\beta_s))$ and some universal lower bound for $\det(L(\alpha_i))_i$. For the lower bound we use lower bounds of logarithms of nontorsion units: $\|L(\alpha_i)\|_2 \geq \frac{21}{128}(\log d)/d^2$ (see [17, 3.5]), or, if the unit group has full rank, $s = r = r_1 + r_2 - 1$, we use lower regulator bounds, possibly coming from the Euler product. Having obtained bounds from the real logarithm (L) with low precision, we calculate the p -adic precision required to find x_i using p -adic linear algebra and rational reconstruction. In the course of the computation it can happen that the p -adic determinants (p -adic regulators) have nontrivial valuation. In this case we have to restart the computation with a correspondingly higher precision to account for the loss. Since the Leopoldt conjecture has not been proved, we also need to verify the solution by computing a low-precision estimate for $\|\sum x_i L(\beta_i) - L(\beta')\|$ to compare it to the lower bound used above.

From the relation x_i we can easily obtain a presentation of the new basis α_i in terms of the β_i, β' . For optimization, we then proceed to compute a new basis $\tilde{\alpha}_i$ such that the real logarithms are (roughly) LLL-reduced. We note that we do not

rely on any LLL estimates here, so any heuristic algorithm that aims at reducing the apparent size will do. Since we do not have any LLL algorithm that will accept real input (as opposed to rational), it is important that this does not influence the correctness.

5.1. Advantages of the p -adic method. There are two core advantages of the p -adic logarithms over the ordinary, complex, ones: First, the linear algebra problems we need to solve in order to find dependencies or relations between units have a much simpler error analysis. In fact, contrary to the complex case, it is possible through the use of ring based operations to solve linear equations without any additional loss of precision. This is very important in the context of unit computation since the matrices representing the image of $L(\alpha)$ are very badly conditioned for classical numerical methods. The other advantage of the p -adic logarithms is more subtle: If we assume Leopoldt's conjecture to hold for the field(s) we are interested in, then instead of doing linear algebra over $\mathbb{R}$ with a precision of say q to find dependencies, it is sufficient to work with a real precision of $q/2$ and a p -adic precision of $q/2$ as well. Thus, assuming classical multiplication, we gain a factor of about 4 through the use of lower precision. Using fast multiplication (in high precision), the gain is smaller but still noticeable. But the most important advantage is the much easier precision control: Instead of complicated and very delicate estimates for linear algebra problems, all we need are upper bounds on linear combinations with integral coefficients — which are trivial to obtain.

We should also mention that one disadvantage of the p -adic method lies in the total lack of control over the real size of the units, thus it needs to be paired with a crude (and uncritical for correctness) size reduction algorithm. Also, it is (currently) not possible to avoid completely the use of complex (or real) logarithms, as the p -adic method is not capable to proving a unit to be torsion without knowledge of bounds on the real size.

5.2. Lower bound from Euler product. Suppose that, as in the class group algorithm, we are given an approximation of the Euler product; that is, we have a real number E such that $1/\sqrt{2} \leq hR/E \leq \sqrt{2}$. After the relation matrix has full rank, and assuming the factor base is large enough for correctness, we have an upper bound for the class number, thus a lower bound for R . This lower bound will be several orders of magnitude larger than the universal bounds available otherwise.

5.3. Saturation. After the initial steps of the algorithm, when the relation matrix has full rank, we have a tentative class number h and a tentative regulator R . Experimentally, at this point, hR does not approximate the Euler product very well — the product will be off by several orders of magnitude. However, after finding one or two more relations, the product has the same size as the Euler product;

it frequently even looks like only a factor of 2 is missing in either h or R . To find the last missing relation can easily take more time than the entire previous run, therefore we suggest using saturation methods instead. At this point in the algorithm the relations define a subgroup U of the S -unit group U_S where S is the factor basis. From the Euler product we know that the index $(U_S : U) =: b$ is small, let's say $b < B$. For any prime $p \mid b$ there is some $u \in U_S \setminus U$ such that $u^p \in U$. Let us fix the prime p . For any prime ideal $Q \notin S$ such that $p \mid \mathcal{N}(Q) - 1$ we can define the map $\phi_Q : U \rightarrow \mathbb{F}_Q^*/(\mathbb{F}_Q^*)^p$ mapping S -units into the multiplicative group of the residue class field modulo p -th powers. The Chebotarev theorem [44] guarantees that if $u \in U$ is not a p -th power, there will be some Q such that $\phi_Q(u)$ is nontrivial, that is, u is not a p -th power modulo Q . We now simply intersect $\ker \phi_Q$ for several Q until either the intersection is U^p or it does not change for five consecutive Q . We expect that any $u \in U / \bigcap \ker \phi_Q$ will have a p -th root in U_S but not in U . Therefore $v^p = u$ is a new relation that will change hR by p . Repeating this for all $p < B$ until we cannot enlarge U any more we find the missing relations. Similar techniques have been used a long time but were confined to the unit group [45; 36]. This appears to be the first time that saturation has been applied to the full relation lattice.

5.4. Representation. During the execution of the algorithm, all (S) -units are naturally represented as power products of the relations coming from the sieving (or the saturation). It is well known that the explicit representation of the units with respect to a fixed basis for the field can require exponentially large coefficients, so it is important to operate on the power products as much as possible. However, even the exponent vectors constructed for the basis of the unit group, or the saturation, will become huge, so we need to “size reduce” the power products. In particular, this happens even if the resulting element is not too large. Using ideas of [13] for compact representations and [22] for reduced divisors in function fields, we can find a representation for those elements that depends only on the logarithmic size (and the number field) rather than the execution path. For any prime p we can write any unit $u = \prod r_i^{e_i} = \prod a_i^{p^{f_i}}$ with elements such that the size of a_i depends on the discriminant and p only. The length of the product comes from $L(u)$. Furthermore, in this presentation it is easy to test for p -th powers as only a_0 needs to be tested and this is a small element.

5.5. Example. To illustrate the power of the p -adic method, we look at a totally real quartic field generated by a root of

$$x^4 + 17211x^3 + 5213x^2 - 176910463x - 4958.$$

The discriminant Δ of the maximal order has 38 digits. In the course of the computation, we found 534 relations involving prime ideals of norm up to $3000 =$

$0.4 \log^2 |\Delta|$ describing a trivial class group. We then searched for 5 further relations to obtain units u_i ($1 \leq i \leq 5$). As power products of the relations, the units are given via exponent vectors e_i with $\|e_i\|_\infty$ ranging between 10^{80} and 10^{160} and $20 < \|e_i\|_1 / \|e_i\|_\infty < 92$. So, while not uniformly large, the exponents are nonsparse, involving huge integers. Using a decimal precision of 170 digits, we establish that the logarithms of the units are roughly $\|L(u_i)\|_\infty \approx 10^{160}$. The first three units are indeed independent, giving a basis for a subgroup of full rank, the fourth is then dependent. Choosing the prime $p = 10337$ we get $\mathbb{Q}_p$ as a splitting field. Using a p -adic precision of 245 digits (that is, working in $\mathbb{Z}_p \bmod p^{245}$), we compute the dependency for the fourth unit, involving exponents of around 10^{360} . The new unit group is then tentatively LLL reduced, producing a new basis where the $\|L(\tilde{u}_i)\|_\infty$ are bounded by 10^7 only. The last unit then involves a much smaller dependency, here the exponents are only around 10^{60} .

Unfortunately, looking at the Euler product, the unit group is not complete. However, the saturation technique outlined above takes 1 sec to determine that the product of the three basis elements is (probably) a square. Finding a better representation where the exponents are all powers of 2 takes less than 1 sec and then we can enlarge the unit group easily.

Due to the implementation, the p -adic precision used was actually higher: Changing (increasing) precision is very computationally expensive, so we try to avoid this and simply double the precision. We used a precision of 320 for the p -adics and a maximal precision of 1000 for the real precision. The computation of the log is the dominating part: We spent 50 sec or 90% of the total processing time here.

6. Conclusion

We introduced new techniques to enhance the performances of the subexponential methods for computing the class group and the unit group of a number field. In particular, sieving allows a speedup of an order of magnitude for number fields of small degree. These techniques could be developed even further. Indeed, we have not taken into account all the improvements to sieving techniques described in the context of the number field sieve algorithm, such as large prime variations or cache-friendly methods. It is also notable that fast techniques for deriving relations in the class group of a small degree number field have applications in evaluating isogenies between small genus curves via complex multiplication methods. Indeed, in that case, evaluating isogenies between genus g curves involves relations in the class group of a degree $2g$ number field.

Acknowledgments

The first author is particularly grateful to Loïc Grenié for providing a special branch of PARI allowing to start the class group computation from an existing relation

matrix. He also thanks David Roe for helping with the Sage interface between Magma and PARI. The research presented in this paper was carried out while both authors were working in Sydney with the Magma group.

References

- [1] J. V. Armitage (ed.), *Journées Arithmétiques*, 1980: *Lectures from the Conference held at the University of Exeter, Exeter, April 13–19, 1980*, London Mathematical Society Lecture Note Series, no. 56, Cambridge University Press, 1982. MR 84c:10003
- [2] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR 91m:11096
- [3] ———, *Improved approximations for Euler products*, in Dilcher [15], 1995, pp. 13–28. MR 96i:11124
- [4] Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197. MR 2009c:11179
- [5] T. Beth, N. Cot, and I. Ingemarsson (eds.), *Advances in cryptology: Proceedings of the EU-ROCRYPT 84 workshop on the theory and application of cryptographic techniques held in Paris, April 9–11, 1984*, Lecture Notes in Computer Science, no. 209, Berlin, Springer, 1985. MR 86m:94003
- [6] J.-F. Biasse, *An $L(1/3)$ algorithm for ideal class group and regulator computation in certain number fields*, 2012, to appear in Math. Comp.
- [7] Jean-François Biasse, *Improvements in the computation of ideal class groups of imaginary quadratic number fields*, Adv. Math. Commun. **4** (2010), no. 2, 141–154. MR 2011e:11192
- [8] Yuri Bilu and Guillaume Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), no. 2, 373–392. MR 97k:11040
- [9] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265. MR 1484478
- [10] Wieb Bosma and Alf van der Poorten (eds.), *Computational algebra and number theory: Papers from the CANT2 Meeting held at Sydney University, November 1992*, Mathematics and its Applications, no. 325, Kluwer Acad. Publ., Dordrecht, 1995. MR 96c:00019
- [11] Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, in Goldstein [20], 1990, pp. 27–41. MR 92g:11125
- [12] Johannes Buchmann, Michael J. Jacobson, Jr., Stefan Neis, Patrick Theobald, and Damian Weber, *Sieving methods for class group computation*, in Matzat et al. [33], 1999, pp. 3–10. MR 2000a:11177
- [13] Johannes Buchmann, Christoph Thiel, and Hugh Williams, *Short representation of quadratic integers*, in Bosma and van der Poorten [10], 1995, pp. 159–185. MR 96c:11144
- [14] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, in Jager [27], 1984, pp. 33–62. MR 85j:11144
- [15] Karl Dilcher (ed.), *Number theory: Proceedings of the Fourth Conference of the Canadian Number Theory Association held at Dalhousie University, Halifax, July 2–8, 1994*, CMS Conference Proceedings, no. 15, Providence, RI, American Mathematical Society, 1995. MR 96c:11003
- [16] Claus Fieker, *Minimizing representations over number fields, II: Computations in the Brauer group*, J. Algebra **322** (2009), no. 3, 752–765. MR 2010e:20016

- [17] Claus Fieker and Michael E. Pohst, *Dependency of units in number fields*, Math. Comp. **75** (2006), no. 255, 1507–1518. MR 2007a:11168
- [18] U. Fincke and M. Pohst, *A procedure for determining algebraic integers of given norm*, in van Hulzen [23], 1983, pp. 194–202. MR 86k:11078
- [19] Jens Franke and Thorsten Kleinjung, *Continued fractions and the lattice sieving*, paper presented at the Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS) conference, Paris, February 24–25, 2005. <http://www.ruhr-uni-bochum.de/itsc/tanja/SHARCS/talks/FrankeKleinjung.pdf>
- [20] Catherine Goldstein (ed.), *Séminaire de théorie des nombres, Paris 1988–1989*, Progress in Mathematics, no. 91, Birkhäuser, Boston, 1990. MR 91k:11004
- [21] James L. Hafner and Kevin S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), no. 4, 837–850. MR 91f:11090
- [22] Florian Heß, *Zur Divisorklassengruppenberechnung in globalen Funktionenkörpern*, Ph.D. thesis, Technische Universität Berlin, 1999. http://page.math.tu-berlin.de/~kant/publications/diss/diss_FH.ps.gz
- [23] J. A. van Hulzen (ed.), *Computer algebra: Proceedings of the European computer algebra conference (EUROCAL) held in London, March 28–30, 1983*, Lecture Notes in Computer Science, no. 162, Berlin, Springer, 1983. MR 86f:68004
- [24] M. J. Jacobson, Jr., Á. Pintér, and P. G. Walsh, *A computational approach for solving $y^2 = 1^k + 2^k + \dots + x^k$* , Math. Comp. **72** (2003), no. 244, 2099–2110. MR 2004c:11241
- [25] Michael J. Jacobson, Jr., *Subexponential class group computation in quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, Aachen, Germany, 1999. <http://www.shaker.eu/shop/978-3-8265-6374-4>
- [26] Michael J. Jacobson, Jr. and Hugh C. Williams, *Solving the Pell equation*, Springer, New York, 2009. MR 2009i:11003
- [27] H. Jager (ed.), *Number theory, Noordwijkerhout 1983: Proceedings of the thirteenth Journées Arithmétiques held at Noordwijkerhout, July 11–15, 1983*, Lecture Notes in Mathematics, no. 1068, Berlin, Springer, 1984. MR 85i:11001
- [28] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann, *Factorization of a 768-bit RSA modulus*, in Rabin [40], 2010, pp. 333–350. MR 2725602
- [29] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The development of the number field sieve*, Lecture Notes in Mathematics, no. 1554, Springer, Berlin, 1993. MR 96m:11116
- [30] H. W. Lenstra, Jr., *On the calculation of regulators and class numbers of quadratic fields*, in Armitage [1], 1982, pp. 123–150. MR 86g:11080
- [31] Donald J. Lewis (ed.), *Proceedings of the 1969 Summer Institutes on Number Theory: Analytic Number Theory, Diophantine Problems, and Algebraic Number Theory; held at the State University of New York at Stony Brook, July 7–August 1, 1969*, Proceedings of Symposia in Pure Mathematics, no. 20, American Mathematical Society, Providence, R.I., 1971. MR 47 #3286
- [32] J. E. Littlewood, *On the class-number of the corpus $P(\sqrt{-k})$* , Proc. London Math. Soc. **S2-27** (1928), no. 1, 358. MR 1575396
- [33] B. Heinrich Matzat, Gert-Martin Greuel, and Gerhard Hiss (eds.), *Algorithmic algebra and number theory: Selected papers from the conference held at the University of Heidelberg, October 1997*, Springer, Berlin, 1999. MR 99h:00020

- [34] Stefan Neis, *Zur Berechnung von Klassengruppen*, Ph.D. thesis, Technische Universität Darmstadt, 2002. <http://tuprints.ulb.tu-darmstadt.de/epda/000283/>
- [35] PARI Group, Bordeaux, France, *PARI/GP, version 2.5.0*, 2011. <http://pari.math.u-bordeaux.fr/>
- [36] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, no. 30, Cambridge University Press, 1989. MR 92b:11074
- [37] Michael Pohst and Hans Zassenhaus, *Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper*, J. Reine Angew. Math. **361** (1985), 50–72. MR 87g:11147
- [38] J. M. Pollard, *The lattice sieve*, in Lenstra and Lenstra [29], 1993, pp. 43–49. MR 1321220
- [39] Carl Pomerance, *The quadratic sieve factoring algorithm*, in Beth et al. [5], 1985, pp. 169–182. MR 87d:11098
- [40] Tal Rabin (ed.), *Advances in cryptology—CRYPTO 2010: Proceedings of the 30th Annual International Conference held in Santa Barbara, CA, August 15–19, 2010*, Lecture Notes in Computer Science, no. 6223, Berlin, Springer, 2010. MR 2012c:94002
- [41] Daniel Shanks, *Class number, a theory of factorization, and genera*, in Lewis [31], 1971, pp. 415–440. MR 47 #4932
- [42] ———, *The infrastructure of a real quadratic field and its applications*, Proceedings of the Number Theory Conference (Boulder, CO), Univ. Colorado, 1972, pp. 217–224. MR 52 #10672
- [43] Christoph Thiel, *On the complexity of some problems in algorithmic algebraic number theory*, Ph.D. thesis, Universität des Saarlandes, 1995. http://www.cdc.informatik.tu-darmstadt.de/reports/reports/Christoph_Thiel.diss.pdf
- [44] N. Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95** (1926), 191–228. JFM 51.0149.04
- [45] Klaus Wildanger, *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*, master's thesis, Heinrich Heine Universität Düsseldorf, 1993. <http://page.math.tu-berlin.de/~kant/publications/diplom/wildanger.pdf>

JEAN-FRANÇOIS BIASSE: biasse@lix.polytechnique.fr

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW,
Calgary, AB T2N 1N4, Canada

CLAUS FIEKER: fieker@mathematik.uni-kl.de

Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, D-67653 Kaiserslautern,
Germany

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

The contents of this work are copyrighted by MSP or the respective authors.
All rights reserved.

Electronic copies can be obtained free of charge from <http://msp.org/obs/1>
and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.



MATHEMATICAL SCIENCES PUBLISHERS

798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org

<http://msp.org>

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS

Deterministic elliptic curve primality proving for a special sequence of numbers — Alexander Abatzoglou, Alice Silverberg, Andrew V. Sutherland, and Angela Wong	1
Imaginary quadratic fields with isomorphic abelian Galois groups — Athanasios Angelakis and Peter Stevenhagen	21
Iterated Coleman integration for hyperelliptic curves — Jennifer S. Balakrishnan	41
Finding ECM-friendly curves through a study of Galois properties — Razvan Bărbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery	63
Two grumpy giants and a baby — Daniel J. Bernstein and Tanja Lange	87
Improved techniques for computing the ideal class group and a system of fundamental units in number fields — Jean-François Biasse and Claus Fieker	113
Conditionally bounding analytic ranks of elliptic curves — Jonathan W. Bober	135
A database of elliptic curves over $\mathbb{Q}(\sqrt{5})$: a first report — Jonathan Bober, Alyson Deines, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Ashwath Rabindranath, Paul Sharaba, and William Stein	145
Finding simultaneous Diophantine approximations with prescribed quality — Wieb Bosma and Ionica Smeets	167
Success and challenges in determining the rational points on curves — Nils Bruin	187
Solving quadratic equations in dimension 5 or more without factoring — Pierre Castel	213
Counting value sets: algorithm and complexity — Qi Cheng, Joshua E. Hill, and Daqing Wan	235
Haberland's formula and numerical computation of Petersson scalar products — Henri Cohen	249
Approximate common divisors via lattices — Henry Cohn and Nadia Heninger	271
Explicit descent in the Picard group of a cyclic cover of the projective line — Brendan Creutz	295
Computing equations of curves with many points — Virgile Ducet and Claus Fieker	317
Computing the unit group, class group, and compact representations in algebraic function fields — Kirsten Eisenträger and Sean Hallgren	335
The complex polynomials $P(x)$ with $\text{Gal}(P(x) - t) \cong M_{23}$ — Noam D. Elkies	359
Experiments with the transcendental Brauer-Manin obstruction — Andreas-Stephan Elsenhans and Jörg Jahnel	369
Explicit 5-descent on elliptic curves — Tom Fisher	395
On the density of abelian surfaces with Tate-Shafarevich group of order five times a square — Stefan Keil and Remke Kloosterman	413
Improved CRT algorithm for class polynomials in genus 2 — Kristin E. Lauter and Damien Robert	437
Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent — Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling	463
Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups — Jennifer Paulhus	487
Isogeny volcanoes — Andrew V. Sutherland	507
On the evaluation of modular polynomials — Andrew V. Sutherland	531
Constructing and tabulating dihedral function fields — Colin Weir, Renate Scheidler, and Everett W. Howe	557