Under the Assumption of the Generalized Riemann Hypothesis Verifying the Class Number Belongs to $\mathcal{NP} \cap$ co–$\mathcal{NP}$

Christoph Thiel*

Fachbereich Informatik
Universität des Saarlandes
Postfach 151150
D-66041 Saarbrücken
Germany

Abstract. We show that under the assumption of a certain Generalized Riemann Hypothesis the problem of verifying the value of the class number of an arbitrary algebraic number field $\mathcal{F}$ of arbitrary degree belongs to the complexity class $\mathcal{NP} \cap \text{co} - \mathcal{NP}$. In order to prove this result we introduce a compact representation of algebraic integers which allows us to represent a system of fundamental units by $(2 + \log_2(\Delta))^{O(1)}$ bits, where Δ is the discriminant of $\mathcal{F}$.

1 Introduction

Let $\mathcal{F}$ be an algebraic number field, i.e. a finite field extension of the field $\mathbb{Q}$ of the rational numbers. In [21] and [11] it was shown that the problem of verifying the value of the class number h of $\mathcal{F}$ belongs to the complexity class $\mathcal{NP}$ if $\mathcal{F}$ is of degree 2 and if a certain Generalized Riemann Hyptothesis (GRH) holds. That is, assuming the GRH, there exists a nondeterministic polynomial time algorithm that accepts the set of all pairs (Δ, h), where $\Delta \in \mathbb{Z}$ is squarefree and h is the class number of $\mathbb{Q}(\sqrt{\Delta})$. We will generalize this result by showing that under the assumption of the GRH the problem of verifying the value of the class number $h_{\mathcal{F}}$ of an arbitrary algebraic number field $\mathcal{F}$ of arbitrary degree belongs to $\mathcal{NP}$. To be more precise, our main results are:

Theorem 1. *The set* PRI *of all pairs* $(\mathcal{F}, A)$, *where* $\mathcal{F}$ *is an algebraic number field and* A *is a principal ideal of the ring of integers of* $\mathcal{F}$, *belongs to* $\mathcal{NP}$. *Moreover, if we assume the GRH, then the set* $\mathcal{H}$ *of all pairs* $(\mathcal{F}, h_{\mathcal{F}})$, *where* $\mathcal{F}$ *is an arbitrary algebraic number field and* $h_{\mathcal{F}}$ *is the class number of* $\mathcal{F}$, *belongs to* $\mathcal{NP}$.

¿From our theorem and from the results of [13] we immediately obtain

Corollary 2. *Assume the GRH. Then* $\mathcal{H}$ *and* PRI *belong to the complexity class* $\mathcal{NP} \cap co - \mathcal{NP}$.

* This research was supported by the Deutsche Forschungsgemeinschaft.

The main tool used in our work is the theory of minima in ideals which will be reviewed in Sect. 3. In order to prove our results we will generalize the results of [15] and introduce in Sect. 4 a short representation of algebraic integers which allows us to represent a system of fundamental units by $(2+\log_2(\Delta))^{O(1)}$ bits where the O-constant is independent of $\mathcal{F}$. Given such a representation of a system of fundamental units we can determine in polynomial time an approximation to the regulator $R_{\mathcal{F}}$. This kind of representation solves an open problem suggested by H. W. Lenstra in [19, Problem 5.2].

After studying the binary length of short representations in Sect. 5, we will use short representations to show in Sect. 6 that there exists a short proof for the principality of a given ideal. As an application of this result we will show in Sect. 7 under the assumption of GRH: if an integer H is divisible by the class number $h_{\mathcal{F}}$, then there exists a short proof for this fact. In Sect. 8 we will use short representations of elements of a system of fundamental units to compute a rational R^* which is an approximation of $mR_{\mathcal{F}}$ for some $m \in \mathbb{Z}$. In Sect. 9 we will show how to verify that a number Θ satisfies $(6/5)h_{\mathcal{F}}R_{\mathcal{F}} \leq \Theta \leq (15/8)h_{\mathcal{F}}R_{\mathcal{F}}$. We can check that $H/h_{\mathcal{F}} = m = 1$ since $HR^* \leq \Theta$ if and only if $H/h_{\mathcal{F}} = m = 1$.

2 Preliminaries

For notions in complexity theory such as *polynomial time* or the complexity class $\mathcal{NP}$ we refer to [24]. The definitions and results in algebraic number theory used in our paper can be found for example in [22] or [18]. We use the notions of encoding data in a similar way as in [19]. For example, mathematical objects are encoded by finite sequences of rational integers (for example, a polynomial is encoded by its coefficients), which are represented in binary. The *binary length of a rational integer* $z \neq 0$ is $\operatorname{size}(z) = \lfloor \log_2 |z| \rfloor + 2$, where the extra bit encodes the sign of z. We also set $\operatorname{size}(0) = 2$. The *binary lenght* $\operatorname{size}(O)$ *of an object* O is defined to be the length of its encoding sequence. When we say that an object is input for an algorithm then this means that the appropriate encoding is its input.

An algebraic number field $\mathcal{F}$ of degree $n > 1$ is represented by a *generating polynomial* which is a monic and irreducible polynomial $f \in \mathbb{Z}[X]$ of degree n such that $\mathcal{F} \cong \mathbb{Q}[X]/f\mathbb{Q}[X]$, i.e. $\mathcal{F} = \mathbb{Q}(\rho)$ with $\rho = X + f\mathbb{Q}[X]$. The numbers $1, \rho, \rho^2, \ldots, \rho^{n-1}$ form a $\mathbb{Q}$-basis of $\mathcal{F}$ and each $\xi \in \mathcal{F}$ can be uniquely represented in the form $\xi = \frac{1}{d}\sum_{i=1}^{n} a_i \rho^{i-1}$, where $d \in \mathbb{Z}_{>0}$, $a_i \in \mathbb{Z}$ for $1 \leq i \leq n$ and $\gcd(a_1, \ldots, a_n, d) = 1$. By $\overline{\xi}$ we denote the complex conjugate of ξ.

Let $s, t, m \in \mathbb{Z}_{\geq 0}$ and let $\rho^{(1)}, \ldots, \rho^{(s)}$ be the real zeros and $\rho^{(s+1)}, \ldots, \rho^{(m)}$, $\rho^{(m+1)} = \overline{\rho^{(s+1)}}, \ldots, \rho^{(m+t)} = \overline{\rho^{(m)}}$ the non real zeros of f, then for $1 \leq j \leq n$ the mapping

$$\xi \mapsto \xi^{(j)} = \frac{1}{d}\sum_{i=1}^{n} a_i {\rho^{(j)}}^{i-1}$$

is a $\mathbb{Q}$-isomorphism. Of course, $m = s + t$ and $n = s + 2t$. For $\xi \in \mathcal{F}$ we define $|\xi|_i = |\xi^{(i)}|^{e_i}$, where $e_i = 1$, if $i \in \{1, \ldots, s\}$ and $e_i = 2$, if $i \in \{s+1, \ldots, m\}$.

The *trace* of ξ is $\mathrm{Tr}(\xi) = \sum_{i=1}^{n} \xi^{(i)}$, the *norm* of ξ is $\mathrm{N}(\xi) = \prod_{i=1}^{n} \xi^{(i)}$, and the *height* of ξ is $\mathrm{H}(\xi) = \max\{|\xi|_i \mid 1 \leq i \leq m\}$.

The integral closure of $\mathbb{Z}$ in a number field $\mathcal{F}$ is called the *maximal order* of $\mathcal{F}$. It is encoded by a multiplication table $\mathrm{MT}(\mathcal{O}) = (w_{i,j,k}) \in \mathbb{Z}^{n \times n \times n}$ with the property that there exists a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}$ such that

$$\omega_i \omega_j = \sum_{k=1}^{n} w_{i,j,k} \omega_k$$

for $1 \leq i, j \leq n$ (cf. [19]). We note, that $\mathrm{MT}(\mathcal{O})$ also encodes $\mathcal{F}$, because every $\mathbb{Z}$-basis of $\mathcal{O}$ is a $\mathbb{Q}$-basis of $\mathcal{F}$ as a vector space. The *discriminant* Δ of $\mathcal{O}$ is the determinant of the matrix

$$(\mathrm{Tr}(\omega_i \omega_j)) = \det(\omega_i^{(j)})^2 \in \mathbb{Q}^{n \times n} \quad .$$

More generally, when A is a $\mathbb{Z}$-modul in $\mathcal{F}$ with $\mathbb{Z}$-basis $a_1, \ldots, a_n$ then we call $\Delta_A = \det(a_i^{(j)})^2$ the *discriminant* of A. The problem of verifying the maximal order of a given number field belongs to $\mathcal{NP}$ (cf. [19]). Moreover, since by [19] and [14] we know that there is a multiplication table of $\mathcal{O}$ with size bounded by $(2 + \log_2(\Delta))^{O(1)} \leq (2 + \log_2(\Delta_f))^{O(1)}$ we may assume that on input $\mathcal{F}$ every nondeterministic polynomial time algorithm also knows $\mathcal{O}$.

We represent $\xi = \sum_{i=1}^{n} x_i \omega_i \in \mathcal{O}$ by the vector $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, called the *standard representation* of ξ. Given elements in standard representation we can compute in polynomial time their sums, products and their quotients. Since there is a polynomial time algorithm that given an element of $\mathcal{O}$ computes its trace (cf. [9]), there is also a polynomial time algorithm, that given $\mathcal{O}$ computes the discriminant Δ of $\mathcal{O}$.

A *(fractional) ideal* of $\mathcal{O}$ is a subset A of $\mathcal{F}$ such that dA is a non zero ideal of the ring $\mathcal{O}$ for some $d \in \mathbb{Z}_{>0}$. The *denominator* $d(A)$ of A is the minimal such d. If for two ideals A and B of $\mathcal{O}$ there is a non zero $\alpha \in \mathcal{F}$ such that $A = \alpha B$, then we write $A \sim B$. An ideal A of $\mathcal{O}$ is called *principal* if $A \sim \mathcal{O}$. In that case any $\alpha \in \mathcal{F}$ with $A = \alpha\mathcal{O}$ is called a *generator* of A.

An ideal A of $\mathcal{O}$ is uniquely encoded (with respect to $\omega_1, \ldots, \omega_n$) by the pair $(d(A), \mathrm{HNF}(A))$, where $\mathrm{HNF}(A) = (h_{i,j}) \in \mathbb{Z}^{n \times n}$ is a matrix in Hermite normal form (cf. [27, pp. 45-51]) such that the elements $\alpha_j = \sum_{i=1}^{n} h_{i,j} \omega_i$, $1 \leq j \leq n$, form a $\mathbb{Z}$-basis of $d(A)A$. We note that there are polynomial time algorithms that given $\mathcal{O}$, $\alpha \in \mathcal{O}$ and fractional ideals A, B of $\mathcal{O}$ determine AB, A^{-1} and $\alpha\mathcal{O}$ (cf. [8]). We call $\mathrm{N}(A) = [\mathcal{O} : d(A)A]/d(A)^n$ the *norm* of the ideal A. Clearly, all entries of $\mathrm{HNF}(A)$ are bounded by $\mathrm{N}(A)d(A)^n$. We know

Lemma 3. *For all ideals A of $\mathcal{O}$ and all $\alpha \in A$, $\alpha \neq 0$, we have $|\mathrm{N}(\alpha)| \geq \mathrm{N}(A)$. For all $\beta \in \mathcal{O}$, $\beta \neq 0$, we have $|\mathrm{N}(\beta)| = \mathrm{N}(\beta\mathcal{O})$.*

The set $\mathcal{I}_\mathcal{F}$ of (fractional) ideals of $\mathcal{O}$ is a multiplicative abelian group in which the set $\mathcal{P}_\mathcal{F}$ of all principal ideals of $\mathcal{O}$ is a subgroup. We call the factor group $Cl_\mathcal{F} = \mathcal{I}_\mathcal{F}/\mathcal{P}_\mathcal{F}$ the *class group* and $h_\mathcal{F} = |\mathcal{I}_\mathcal{F}/\mathcal{P}_\mathcal{F}|$ the *class number* of $\mathcal{F}$.

The *unit group* $\mathcal{O}^*$ of $\mathcal{O}$ is the set of all elements of $\mathcal{O}$ whose multiplicative inverse also belongs to $\mathcal{O}$. By Dirichlet's Unit Theorem, there is a root of unity

$\delta \in \mathcal{O}^*$ and a *system of* $r = m - 1$ *fundamental units* $\epsilon_1, \dots, \epsilon_r \in \mathcal{O}^*$ such that every unit of $\mathcal{O}$ is uniquely represented by a product of δ and of powers of the ϵ_i, $1 \leq i \leq r$. The image of $\mathcal{O}^*$ under the *logarithm map*

$$\mathrm{Log} : \mathcal{F} \setminus \{0\} \to \mathbb{R}^r, \xi \mapsto \mathrm{Log}\,\xi = (\ln|\xi|_1, \dots, \ln|\xi|_r)^T,$$

where $\ln(\cdot)$ denotes the natural logarithm, is the lattice $L_{\mathcal{F}} = \sum_{i=1}^r (\mathrm{Log}\,\epsilon_i)\mathbb{Z}$. The absolut value of the determinant of the matrix $(\mathrm{Log}\,\epsilon_1, \dots, \mathrm{Log}\,\epsilon_r)$ is called the *regulator* $R_{\mathcal{F}}$ of $\mathcal{F}$.

By $|\cdot|_\infty$ we denote the maximum modulus of all entries of a given vector. We also use the euclidean norm $|\cdot|_2$. The distinction between the euclidean norm and the archimedian valuations arises from the context.

3 Minima

The main tool used in our work is the theory of minima in ideals which was described in [3]. An element μ of an ideal A is called a *minimum* in A if there exists no $\alpha \in A$, $\alpha \neq 0$, such that $|\alpha|_i < |\mu|_i$ for $1 \leq i \leq m$. If 1 is a minimum in A, then A is called *reduced*.

Proposition 4. *Let A be an ideal. The reduced ideals equivalent to A are exactly the ideals $(1/\alpha)A$ where α is a minimum in A.*

By [1, Proposition 2.2] and [2, Lemma 3.4] we know

Theorem 5. *For all minima μ in an ideal A we have*

$$|\mathrm{N}(\mu)| \leq (2/\pi)^t \mathrm{N}(A)\sqrt{\Delta}\ .$$

Moreover, for all $z \in \mathbb{R}^r$ and for ideals A there is at least one minimum μ in A with $\mathrm{Log}\,\mu \in z + \mathcal{W}$, where $\mathcal{W} = \{x \in \mathbb{R}^r \mid |x|_\infty \leq (\log\sqrt{\Delta})/2\}$.

Lemma 6. *If A is a reduced ideal of $\mathcal{O}$, then $1/\sqrt{\Delta} \leq \mathrm{N}(A) \leq 1$.*

Proof. Since 1 is a minimum in A we know by Lemma 3 that $1 = |\mathrm{N}(1)| \geq \mathrm{N}(A)$. On the other hand we get by Theorem 5 that $1 = |\mathrm{N}(1)| \leq \mathrm{N}(A)\sqrt{\Delta}$. □

Lemma 7. *Let A be a reduced ideal of $\mathcal{O}$ and let $\mathrm{HNF}(A) = (a_{i,j})$ be the Hermite normal form of A. Then $0 \leq |a_{i,j}| \leq d(A) \leq \sqrt{\Delta}$ for $1 \leq i, j \leq n$.*

Proof. Since A is reduced, we know that $\mathcal{O} \subseteq A$. Hence $[A : O]A \subseteq \mathcal{O}$ and therefore $d(A) \leq [A : \mathcal{O}]$. By Lemma 6 and [22] we obtain

$$[A : \mathcal{O}] = \sqrt{\Delta_A}/\sqrt{\Delta} = 1/\mathrm{N}(A) \leq \sqrt{\Delta},$$

where Δ_A is the discriminant of A. To show the left inequality we note that $d(A)\omega_i \in d(A)A$, hence, by induction we see that $a_{i,i}$ divides $d(A)$ for $1 \leq i \leq n$. The assertion follows since $\mathrm{HNF}(A)$ is in Hermite normal form and therefore $|a_{i,j}| \leq |a_{i,i}|$ for $1 \leq i, j \leq n$. □

Corollary 8. *Let A be a reduced ideal of $\mathcal{O}$. Then $\mathrm{size}(A) \leq (n^2 + 1)\log_2(\sqrt{\Delta})$.*

4 Compact Representations

In this section we prove the existence of a short representation for any number in $\mathcal{O}$. In the next sections, this representation will be used to show our main results.

Let A be a reduced ideal of $\mathcal{O}$, let $u \in \mathbb{R}^r$, and let μ be a minimum in A with $\operatorname{Log} \mu \in u + \mathcal{W}$ where

$$\mathcal{W} = \left\{ x \in \mathbb{R}^r \mid |\, x\,|_\infty \le (\log \sqrt{\Delta})/2 \right\} .$$

We let $\mathrm{DOUBLE}(A, \mu, u)$ be the set of all minima β in $B = ((1/\mu))^2 A$ with $\operatorname{Log} \beta \in 2u - 2\operatorname{Log} \mu + \mathcal{W}$. By Theorem 5 the set $\mathrm{DOUBLE}(A, \mu, u)$ is not empty. Clearly, for each $\beta \in \mathrm{DOUBLE}(A, \mu, u)$ there exists a unique element $a(\beta) \in \mathcal{O}$ such that $1/\beta = a(\beta)/d(\beta)$ where $d(\beta) = d((1/\beta)B)$.

Lemma 9. *For every* $\beta \in \mathrm{DOUBLE}(A, \mu, u)$ *we have* $0 \le d(\beta) \le \sqrt{\Delta}$ *and* $\mathrm{H}(a(\beta)) \le \Delta^{3(m+2)/4}$.

Proof. Let $B = ((1/\mu))^2 A$. Since $(1/\beta)B$ is reduced, the first assertion follows from Lemma 7. Since $\operatorname{Log} \beta \in 2u - 2\operatorname{Log} \mu + \mathcal{W}$ we have $|\log |\beta|_i\,| \le (3/2) \log \sqrt{\Delta}$ for $1 \le i \le r$. Hence, $\Delta^{-3/4} \le |\beta|_i \le \Delta^{3/4}$ for $1 \le i \le r$. By Lemma 3 we have $|\,\mathrm{N}(\beta)\,| = \prod_{i=1}^m |\beta|_i \ge \mathrm{N}(B)$, thus from Lemma 6 and Theorem 5 we obtain $|\beta|_m \ge \mathrm{N}(B)/\Delta^{3(m-1)/4} \ge 1/\Delta^{3(m+1)/4}$, implying that $\mathrm{H}(1/\beta) \le \Delta^{3(m+1)/4}$. The second assertion follows. $\square$

Lemma 10. *Let A be a reduced ideal, and let ρ be a minimum in A. If we set* $u_j = (\operatorname{Log} \rho)/2^{k-j+1}$ *for* $1 \le j \le k$ *where* $k = \max\{1, \lceil \log_2(|\operatorname{Log} \rho|_\infty)\rceil + 2\}$, *then there are* $\beta_0, \ldots, \beta_k$ *with* $\beta_0 = 1$ *and* $\beta_j \in \mathrm{DOUBLE}(A, \prod_{i=0}^{j-1} \beta_i^{2^{j-i}}, u_j)$ *such that* $\rho = \prod_{j=0}^k \beta_j^{2^{k-j}}$ *and* $\prod_{i=0}^j \beta_i^{2^{j-i}}$ *is a minimum in A.*

Proof. The number 1 is a minimum in A with $\operatorname{Log} 1 \in \operatorname{Log} u_1 + \mathcal{W}$. By Theorem 5 we have for every $\beta_1 \in \mathrm{DOUBLE}(A, \beta_0, u_1)$ that $\rho_1 = \beta_1(\beta_0)^2$ is a minimum in A with $\operatorname{Log} \rho_1 \in 2u_1 + \mathcal{W} = u_2 + \mathcal{W}$. By induction on j we obtain that for every $\beta_j \in \mathrm{DOUBLE}(A, \prod_{i=0}^{j-1} \beta_i^{2^{j-i}}, u_j)$ the number $\rho_j = \beta_j(\prod_{i=0}^{j-1} \beta_i^{2^{j-i}})^2$ is a minimum in A with $\operatorname{Log} \rho_j \in u_{j+1} + \mathcal{W}$, $1 \le j \le k$. If we fix $\beta_k = \rho/(\rho_{k-1})^2$ then $\operatorname{Log} \beta_k \in 2u_k - 2\operatorname{Log} \rho_{k-1} + \mathcal{W}$. Thus $\beta_k \in \mathrm{DOUBLE}(A, \prod_{i=0}^{k-1} \beta_i^{2^{k-i}}, u_k)$ and $\rho = \prod_{j=0}^k \beta_j^{2^{k-j}}$. $\square$

Theorem 11. *For* $\alpha \in \mathcal{O}$ *there exist* $k \le \log_2(\log_2(\Delta) + (n-1)\log_2 \mathrm{H}(\alpha)) + 2$ *and* $\gamma, \alpha_j \in \mathcal{O}$ *and* $d_j \in \mathbb{Z}$, $1 \le j \le k$, *with* $\mathrm{H}(\gamma) \le |\mathrm{N}(\alpha)|^{2/n} \Delta$, $\mathrm{H}(\alpha_j) \le \Delta^{\frac{3}{4}(m+2)}$ *and* $0 < d_j \le \Delta^{1/2}$ *such that*

$$\alpha = \gamma \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j} \right)^{2^{k-j}} .$$

Moreover, for $1 \le j \le k$ *the ideal* $\prod_{i=1}^{j-1} (\alpha_i/d_i)^{2^{j-i}} \mathcal{O}$ *is reduced.*

Proof. By Minkowsky's Convex body theorem (cf. [23, pp.33-34]) and Lemma 3 there is a minimum γ in the principal ideal $\alpha\mathcal{O}$ with $\mathrm{H}(\gamma) \le |\mathrm{N}(\alpha)|^{2/n}\Delta$. If we set $\rho = \gamma/\alpha$ then by Proposition 4 we have that ρ is a minimum in $\mathcal{O}$. Since $\mathcal{O}$ is an ideal with minimum 1 we can apply Lemma 10. Using the notations of that Lemma we obtain $\rho = \prod_{j=0}^{k} \beta_j^{2^{k-j}}$.

We may assume that $k \le \log_2 |\mathrm{Log}\,\rho|_\infty + 2 \le \log_2(\log_2 \mathrm{H}(\rho)) + 2$. But $\rho = \gamma/\alpha$, thus we have

$$\mathrm{H}(\rho) \le \frac{\mathrm{H}(\gamma)(\mathrm{H}(\alpha))^{n-1}}{|\mathrm{N}(\alpha)|} \le \Delta(\mathrm{H}(\alpha))^{n-1}.$$

Hence, we have shown that $k \le \log_2(\log_2(\Delta) + (n-1)\log \mathrm{H}(\alpha)) + 2$.

If we set $\alpha_j = a(\beta_j)$ and $d_j = d(\beta_j)$ then $\alpha_j \in \mathcal{O}$ and $d_j \in \mathbb{Z}$ and by Lemma 9 it follows that $\mathrm{H}(\alpha_j) \le \Delta^{\frac{3}{4}(m+2)}$ and $0 < d_j \le \Delta^{1/2}$.

The last assertion is a direct consequence of Lemma 10. □

A representation of $\alpha \in \mathcal{O}$ as described in Theorem 11 is called a *compact representation* of α.

Proposition 12. *There is a polynomial time algorithm that given $\mathcal{O}$ and the compact representation $\gamma \prod_{j=1}^{k} (\alpha_j/d_j)^{2^{k-j}}$ of $\alpha \in \mathcal{O}$ computes the ideal $\alpha\mathcal{O}$.*

Proof. We describe the algorithm. It starts by computing $A_0 = (\alpha_0/d_0)\mathcal{O}$. Then it determines recursively $A_j = (\alpha_j/d_j)(A_{j-1})^2$ for $1 \le j \le k$. Since each A_{j-1} is reduced, from Lemma 7 follows that all these steps can be done in polynomial time. Finally, the algorithm calculates $\alpha\mathcal{O} = \gamma A_k$. It is clear that the algorithm has polynomially bounded running time. □

Corollary 13. *There is a polynomial time algorithm that given the compact representation of $\alpha \in \mathcal{O}$ decides whether α is a unit of $\mathcal{O}$ or not.*

Remark. Using methods similar to those in [10], [1], [2] and [3] it can be shown that there is a deterministic algorithm that given an ideal $\alpha\mathcal{O}$ and an appropriate approximation of $\mathrm{Log}\,\alpha$ computes a compact representation of α in running time $(n \log \Delta \lceil |\mathrm{Log}\,\alpha|_\infty \rceil)^{O(n)}$. It can also be shown that if the dimension n of the considered field $\mathcal{F}$ is fixed we can add, multiply and compare algebraic numbers given in compact representation in polynomial time. More details will be given in a subsequent paper.

5 Sizes of Algebraic Integers

Let $\mathcal{O}$ be given by the table $\mathrm{MT}(\mathcal{O}) = (w_{i,j,k}) \in \mathbb{Z}^{n\times n\times n}$ such that there is a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}$ with $\omega_i\omega_j = \sum_{k=1}^{n} w_{i,j,k}\,\omega_k$ for $1 \le i, j \le n$. Then the binary length of the standard representation of $\alpha = \sum_{i=1}^{n} x_i\omega_i \in \mathcal{O}$ with respect to that $\mathbb{Z}$-basis is

$$\mathrm{size}_s(\alpha) = \sum_{i=1}^{n} \mathrm{size}(x_i) \ .$$

The binary length of the compact representation $\gamma \prod_{i=1}^{k} (\alpha_i / d_i)^{2^{k-i}}$ of α with respect to that $\mathbb{Z}$-basis is

$$\mathrm{size}_s(\gamma) + \sum_{i=1}^{k} \big(\mathrm{size}_s(\alpha_i) + \mathrm{size}(d_i)\big),$$

since the α_i are given in standard representation. We define $\mathrm{size}_c(\alpha)$ to be the maximum of that quantity taken over all compact representations with respect to $\mathcal{O}$.

Proposition 14. *For $\alpha = \sum_{i=1}^{n} x_i \omega_i \in \mathcal{O} \setminus \{0\}$ we have*

$$|\,(x_1, \ldots, x_n)^T\,|_\infty \leq n\, 2^{4n^2} 2^{\mathrm{size}(\mathcal{O})}\, \mathrm{H}(\alpha) \;\; .$$

Proof. Let $\ell, h \in \{1, \ldots, n\}$ be such that $|\omega_\ell|_h = \max\{|\omega_j|_i \,|\, 1 \leq i, j \leq n\}$. Then

$$|\omega_\ell|_h{}^2 \leq \sum_{k=1}^{n} |\, w_{h,h,k}\,||\omega_k|_h \;\leq\; n\, |\omega_\ell|_h\; 2^{\mathrm{size}(\mathcal{O})}$$

and $|\omega_j|_i \leq n\, 2^{\mathrm{size}(\mathcal{O})}$ for $1 \leq i, j \leq n$. For $\xi \in \mathcal{F}$ we write

$$\underline{\xi} = (\xi^{(1)}, \ldots \xi^{(s)}, Re(\xi^{(s+1)}), \ldots,\; Re(\xi^{(m)}),\; Im(\xi^{(s+1)}), \ldots,\; Im(\xi^{(m)}))^T.$$

If $\underline{\Omega}$ is the matrix $(\underline{\omega_1}, \ldots, \underline{\omega_n}) \in \mathbb{R}^{n\times n}$, then we obtain by Cramer's rule and Hadamard's inequality that $\|\underline{\Omega}^{-1}\|_\infty \leq 2^{4n^2} 2^{\mathrm{size}(\mathcal{O})}$, where $\|\cdot\|_\infty$ denotes the maximum absolute value of all entries in a matrix. Thus, we have

$$|\,(x_1, \ldots, x_n)^T\,|_\infty \;=\; |\,\underline{\Omega}^{-1}\underline{\alpha}\,|_\infty \;\leq\; n \|\underline{\Omega}^{-1}\|_\infty \mathrm{H}(\alpha) \;\leq\; n\, 2^{4n^2} 2^{\mathrm{size}(\mathcal{O})}\, \mathrm{H}(\alpha) \;\; .$$

□

Corollary 15. *For $\alpha \in \mathcal{O} \setminus \{0\}$ we have*

$$\mathrm{size}_s(\alpha) \leq n\, \big(\log_2(n) + 4n^2 + \mathrm{size}(\mathcal{O}) + \log_2(\mathrm{H}(\alpha))\big),$$

$$\mathrm{size}_c(\alpha) \leq 5n^2 \big(n^2 + n \log_2(\Delta\, |\, \mathrm{N}(\alpha)\,|) + \mathrm{size}(\mathcal{O})\big) \big(3 + \log_2(\log_2(\Delta\, \mathrm{H}(\alpha)))\big) \;\; .$$

Lemma 16. *There exists a polynomial $p \in \mathbb{Z}[x, y, z]$ such that for every algebraic number field $\mathcal{F}$ and every multiplication table of its maximal order $\mathcal{O}$ there exists a system of fundamental units $\epsilon_1, \ldots, \epsilon_r$ of $\mathcal{O}$ with*

$$\mathrm{size}_c(\epsilon_i) < p\big(n, \log_2(\Delta), size(\mathcal{O})\big) \;\; .$$

Proof. By [28], there is a system of fundamental units $\epsilon_1, \ldots, \epsilon_r$ of $\mathcal{O}$ such that for $1 \leq i, j \leq r$ we have $|\ln|\epsilon_i|_j\,| < 2(5\log_2(\Delta))^{n-1}\sqrt{\Delta}$. Since $\mathrm{N}(\epsilon_i) = 1$, the assertion is an immediate consequence of Corollary 15. □

Lemma 17. *For every principal (integral) ideal A in $\mathcal{O}$ there exists a generator $\alpha \in \mathcal{O}$ of A such that $|\log_2 \mathrm{H}(\alpha)\,| \leq \log_2(|\,\mathrm{N}(A)\,|) + 2n^2(5\log_2(\Delta))^{n-1}\sqrt{\Delta}$.*

Proof. Let β be a generator of A. Let $\epsilon_1, \ldots, \epsilon_r$ be a system of fundamental units of $\mathcal{O}$. We set $T = \{\sum_{i=1}^r x_i \operatorname{Log} \epsilon_i \mid x_i \in \mathbb{R}, 0 \le x_i < 1 \text{ for } 1 \le i \le r\}$. Then there is a vector $\ell = \sum_{i=1}^r y_i \operatorname{Log} \epsilon_i \in L_{\mathcal{F}}$, where $y_i \in \mathbb{Z}$ for $1 \le i \le r$, such that $\ell' = \operatorname{Log} \beta - \ell \in T$. Thus we have $|\ell'|_2 \le r \max\{|\operatorname{Log} \epsilon_i|_2 \mid 1 \le i \le r\}$. If we set $\alpha = \beta / \prod_{i=1}^r \epsilon_i^{y_i}$, then α is a generator of A with $\operatorname{Log} \alpha = \ell'$. Since by [28] we may assume that $|\ln |\epsilon_i|_j| < 2(5\log_2(\Delta))^{n-1}\sqrt{\Delta}$ for $1 \le i, j \le r$, we have

$$|\ln |\alpha|_i| \le 2r(5\log_2(\Delta))^{n-1}\sqrt{\Delta} \ .$$

From Lemma 3 we obtain

$$\left|\ln |\alpha|_m\right| = \left|\ln |\mathrm{N}(A)| - \sum_{i=1}^r \ln |\alpha|_i\right| \le \left|\log_2 |\mathrm{N}(A)|\right| + 2r^2(5\log_2(\Delta))^{n-1}\sqrt{\Delta} \ .$$

□

Corollary 18. *There exists a fixed polynomial $q \in \mathbb{Z}[x, y, z]$ such that for every algebraic number field $\mathcal{F}$ and every multiplication table of its maximal order $\mathcal{O}$ and every principal ideal A of $\mathcal{O}$ there is a generator α of A with*

$$\operatorname{size}_c(\alpha) \le q(n, \log_2(\Delta), size(\mathcal{O}), \log_2(\mathrm{N}(A))) \ .$$

6 Principal Ideal Testing

In this section we consider the following problem: Given an algebraic number field $\mathcal{F}$ and an ideal A of the maximal order $\mathcal{O}$ is there a short proof of the principality of A? We first look at the set PRI of all pairs $(\mathcal{F}, A)$, where $\mathcal{F}$ is an algebraic number field, and A is a principal ideal in the maximal order $\mathcal{O}$. Remember that as mentioned in Sect. 2 we may assume that every nondeterministic polynomial time algorithm knows $\mathcal{O}$ on input $\mathcal{F}$.

Theorem 19. *The set* PRI *belongs to $\mathcal{NP}$.*

Proof. Let $(\mathcal{F}, A) \in$ PRI, where $\mathcal{F}$ is a number field of degree n. By Lemma 18 there exists a generator α of the ideal A such that $\operatorname{size}_c(\alpha)$ is bounded by a polynomial in $\log_2(\Delta)$ and the input size, i.e. the sizes of $\mathcal{F}$, $\mathcal{O}$ and A. By Proposition 12 there is a polynomial time algorithm, which given the compact representation $\gamma \prod_{j=1}^k (\alpha_j/d_j)^{2^{k-j}}$ of α (cf. Sect. 4) computes $\alpha\mathcal{O}$. Thus a nondeterministic polynomial time algorithm, that accepts PRI, only has to guess the compact representation of α, to compute $\alpha\mathcal{O}$ and to compare this ideal with A. □

To prove our second main result we need

Proposition 20. *Given $\mathcal{O}$, $\beta_1, \ldots, \beta_i \in \mathcal{O}$ and ideals $B_1, \ldots, B_i$ of $\mathcal{O}$, $i \in \mathbb{Z}_{>0}$, there is a polynomial time algorithm that decides whether $B_j = (1/\beta_j)(B_{j-1})^2$ for $1 \le j \le i$.*

Lemma 21. *Let $\mathcal{O}$ be the maximal order of $\mathcal{F}$, let A be an ideal of $\mathcal{O}$ and let $x = 2^i$, $i \in \mathbb{Z}_{>0}$. Then there exist $\beta_0, \beta_1, \ldots, \beta_i \in \mathcal{O}$ with*

$$\mathrm{size}_s(\beta_j) = (2 + \log_2(\Delta))^{O(1)} + \log_2(\Delta)\mathrm{size}(\mathcal{O})$$

and ideals $B_1, \ldots, B_i$ of $\mathcal{O}$ with

$$\mathrm{size}(B_j) \leq (n^2 + 1)\log_2(\sqrt{\Delta})$$

for $1 \leq j \leq i$ such that $B_j = (1/\beta_j)(B_{j-1})^2$ and $A^x \sim B_i$.

Proof. Let $B_0 = (1/\beta_0)A$ and $B_j = (1/\beta_j)(B_{j-1})^2$, $j \geq 1$, where β_0 is a minimum of A and β_j is a minimum of $(B_{j-1})^2$ with

$$\mathrm{Log}\,\beta_0, \mathrm{Log}\,\beta_j \in \left\{x \in \mathbb{R}^r \mid |x|_\infty \leq (\log\sqrt{\Delta})/2\right\} \ .$$

Thus, $B = B_i$ is reduced and $A^x \sim B$. As in the proof of Lemma 9 we can show that $\mathrm{H}(\beta_j) \leq \Delta^{3(m+1)/4}$. Thus, by Corollary 15 we obtain

$$\mathrm{size}_s(\beta_j) = (2 + \log_2(\Delta))^{O(1)} + \log_2(\Delta)\mathrm{size}(\mathcal{O}) \ .$$

Since each B_j is reduced, from Corollary 8 it follows that

$$\mathrm{size}(B_j) \leq (n^2 + 1)\log_2(\sqrt{\Delta}) \ .$$

□

Theorem 22. *The set of all tuples $(\mathcal{F}, A_0, \ldots, A_\ell, x_0, \ldots, x_\ell)$ where $\mathcal{F}$ is an algebraic number field and $A_0, \ldots, A_\ell$ are ideals of the maximal order $\mathcal{O}$ and $x_0, \ldots, x_\ell \in \mathbb{Z}$, $\ell \in \mathbb{Z}_{>0}$, such that $\prod_{i=0}^{\ell} A_i^{x_i} \sim \mathcal{O}$, belongs to $\mathcal{NP}$.*

Proof. W.l.o.g. we may assume that $x_i \geq 0$ for $1 \leq i \leq \ell$. Otherwise, we replace A_i by A_i^{-1}, which can be computed in polynomial time. Let $y_i = \lceil \log_2(x_i) \rceil + 1$ and $x_{i,j} \in \{0, 1\}$, $1 \leq j \leq y_i$, such that $x_i = \sum_{j=0}^{y_i} x_{i,j} 2^j$. Then

$$\prod_{i=0}^{\ell} A_i^{x_i} = \prod_{i=0}^{\ell} \prod_{j=0}^{y_i} (A_i^{x_{i,j}})^{2j} \ .$$

Thus, from Proposition 20 and Lemma 21 it follows that there is a nondeterministic polynomial time algorithm that guesses an ideal B with size bounded by a polynomial in the size of the input tuple and tests whether $\prod_{i=0}^{\ell} A_i^{x_i} \sim B$. Hence, the assertion follows from Theorem 19. □

7 Multiples of the Class Number

Theorem 23. *Assume the GRH. Then the set of all pairs $(\mathcal{F}, H)$, where $\mathcal{F}$ is an algebraic number field and H is a multiple of $h_{\mathcal{F}}$, belongs to $\mathcal{NP}$.*

Proof. Let $\mathcal{F}$ be a number field of degree n and let $F = \{P_1, \ldots, P_{|F|}\}$ be the set of all prime ideals of the maximal order $\mathcal{O}$ with norm not exceeding $12(\log \Delta)^2+1$. By means of the methods presented in [9] and [29] the set F can be computed in time polynomially bounded by $\mathrm{size}(\mathcal{F})$, $\mathrm{size}(\mathcal{O})$ and $\log_2(\Delta)$.

We also set

$$A = \left\{ \alpha \in \mathcal{F} \setminus \{0\} \,\middle|\, \alpha\mathcal{O} = \prod_{i=1}^{|F|} P_i^{e_i}, e_i \in \mathbb{Z} \right\},$$

and for $\alpha \in A$ with $\alpha\mathcal{O} = \prod_{i=1}^{|F|} P_i^{e_i}$ we define $\varphi'(\alpha) = (e_1, \ldots, e_{|F|}) \in \mathbb{Z}^{|F|}$. If we assume the GRH then by [4] the image $L' = \varphi'(A)$ is a $|F|$-dimensional lattice of determinant $h_{\mathcal{F}}$. Thus a number H is a multiple of $h_{\mathcal{F}}$ if and only if there is $E = (e_{i,j}) \in \mathbb{Z}^{|F|\times|F|}$ with $\det(E) = H$ satisfying

$$\prod_{j=1}^{|F|} P_j^{e_{i,j}} \sim \mathcal{O} \tag{1}$$

for each $1 \le i \le |F|$. This is true, because the vectors $e_i = (e_{i,1}, \ldots, e_{i,|F|})$ form a sublattice Λ of L' with $|L'/\Lambda| = |\det(E)|/h_{\mathcal{F}}$.

W.l.o.g. we may assume that $\|E\|_\infty \le \det(E)$. Then $\mathrm{size}(E)$ is polynomially bounded by H and a nondeterministic polynomial time algorithm which accepts the above set only has to guess E and to verify condition (1) for $1 \le i \le |F|$. By Theorem 22 this can be done in polynomial time. Since the algorithm knows $\mathcal{O}$ (see Sect. 2) this proves the theorem. □

8 Approximations

Since we can not compute with real values we sometimes have to work with approximations. For this purpose we give in this section some notations and results concerning the computation of approximations to algebraic numbers given in standard or compact representation.

Let $q \in \mathbb{Z}_{>0}$, and let z be a complex number. A number $z\{q\} \in 2^{-(q+1)}\mathbb{Z}[i]$ is called an *approximation of precision* q to z if $|z - z\{q\}| < 2^{-q}$. An approximation of precision q to a vector $\underline{v} \in \mathbb{C}^r$ or a matrix $A \in \mathbb{C}^{r\times r}$ is a vector $\underline{v}\{q\}$ or a matrix $A\{q\}$ whose entries are approximations of precision q to the corresponding entries of the original vector or matrix. We use the following technical result that can be deduced from the estimates in [5]:

Proposition 24. *Let $A \in \mathbb{C}^{\ell\times\ell}$, $\ell \in \mathbb{Z}_{>0}$, and let $A\{p\}$ be an approximation of precision $p \in \mathbb{Z}_{>0}$ to A. Then we have*

$$|\det(A) - \det(A\{p\})| \le 2^{-p}\sqrt{\ell}\, 2^{\ell-1}\ell^{\frac{\ell+1}{2}}\|A\|_\infty^{\ell-1}\ .$$

Proposition 25. *Let $x \in \mathbb{R}_{>0}$, and let $x\{q\} \in \mathbb{R}_{>0}$ be an approximation of precision q to x, where $x\{q\} > x$, $q \in \mathbb{Z}_{>0}$. Let $p \in \mathbb{Z}_{>0}$ and let $\kappa \in \mathbb{R}_{>0}$ with $\kappa > \ln(2)$. If $q > -\ln(x) + \kappa p$ then we have $|\ln(x\{q\}) - \ln(x)| < 2^{-p}$.*

Lemma 26. *There is a polynomial time algorithm that given a number field $\mathcal{F}$, the maximal order $\mathcal{O}$ of $\mathcal{F}$, the compact representation $\gamma \prod_{j=1}^{k} (\alpha_j/d_j)^{2^{k-j}}$ of an element $\alpha \in \mathcal{O}$ and an integer 2^p, where $p \in \mathbb{Z}_{>0}$, computes an approximation of precision p to $\operatorname{Log} \alpha$.*

Proof. If we set $q' = p + 2k + 2$, then

$$(\operatorname{Log} \gamma)\{q'\} + \sum_{j=1}^{k} 2^{k-j} \big((\operatorname{Log} \alpha_j)\{q'\} - (\operatorname{Log} d_j)\{q'\}\big)$$

is an approximation of precision p to $\operatorname{Log} \alpha$. Thus, the algorithm first computes upper bounds λ_j of $\mathrm{H}(\alpha_j)$ and an upper bound δ of $\mathrm{H}(\gamma)$. Then it determines for $1 \le i \le n$ approximations of precision $2(\lceil \log_2(\lambda_j) \rceil + \ln(2)q')$ to $\alpha_j^{(i)}$ respectively of precision $2(\lceil \log_2(\delta) \rceil + \ln(2)q')$ to $\gamma^{(i)}$. These steps can be performed in polynomial time (cf. [7] or [17]). Therefore, from Proposition 25 and [26] the assertion follows. □

Theorem 27. *There is a polynomial time algorithm that given $\mathcal{O}$, the compact representations of r independent units $\epsilon_1, \ldots, \epsilon_r$ of $\mathcal{O}$ and a number 2^q, $q \in \mathbb{Z}_{>0}$ computes an approximation of precision q to a multiple of $R_{\mathcal{F}}$.*

Proof. The lattice $\sum_{i=1}^{r} \operatorname{Log} \epsilon_i \mathbb{Z}$ is a sublattice of the lattice $L_{\mathcal{F}}$. Therefore the determinant of the matrix $\mathrm{REG} = (\operatorname{Log} \epsilon_1, \ldots, \operatorname{Log} \epsilon_r)$ is a multiple of $R_{\mathcal{F}}$. We describe an algorithm that approximates that determinant. First, the algorithm determines an approximation of precision 1 to the matrix REG and computes the bound $\lambda = \lceil \|\mathrm{REG}\{1\}\|_\infty \rceil + 1 \ge \|\mathrm{REG}\|_\infty$. Then it computes an approximation $\mathrm{REG}\{p\}$ of precision $p = (n(\log_2(\lambda) + n + 2) + q + 1$ to REG. Since $n > r$ we obtain from Proposition 24 that $|\det(\mathrm{REG}) - \det(\mathrm{REG}\{p\})| < 2^{-q}$. Finally, the algorithm computes the determinant of $\mathrm{REG}\{q\}$. According to Lemma 26, the algorithm only needs polynomial time. □

9 An Approximation of $h_{\mathcal{F}} R_{\mathcal{F}}$

Theorem 28. *Assume the GRH. Then there is a polynomial time algorithm that given an algebraic number field $\mathcal{F}$ and the number w of roots of unity in $\mathcal{F}$ computes a number $\Theta \in \mathbb{R}_{>0}$ such that $(6/5)h_{\mathcal{F}} R_{\mathcal{F}} \le \Theta \le (15/8) h_{\mathcal{F}} R_{\mathcal{F}}$.*

Proof. By [12] the product $h_{\mathcal{F}} R_{\mathcal{F}}$ can be expressed by means of the analytic class number formula $h_{\mathcal{F}} R_{\mathcal{F}} = C_{\mathcal{F}} \prod_{p \in P} E(p)$, where $C_{\mathcal{F}} = \frac{w\sqrt{\Delta}}{2^s (2\pi)^t}$, P is the set of rational primes and $E(p)$ is the Euler factor belonging to p. Since s and t can be determined in polynomial time from the generating polynomial f of $\mathcal{F}$, we only have to describe a method for computing an approximation of $\prod_{p\in P} E(p)$. For this purpose let $\mathbb{L}$ be the normal closure of $\mathcal{F}$. We choose $Q \in \mathbb{Z}_{>0}$ and split $\prod_{p\in P} E(p) = F(Q)T(Q)$, where

$$F(Q) = \prod_{p\in P, p\leq Q} E(p) \prod_{\substack{p\in P, p>Q \\ p \text{ ramified in } \mathbb{L}}} E(p)$$

and

$$T(Q) = \prod_{\substack{p\in P, p>Q \\ p \text{ unramified in } \mathbb{L}}} E(p).$$

Then we have $h_{\mathcal{F}} R_{\mathcal{F}} = C_F F(Q)T(Q)$. From [12] (cf. inequality (3.4) and Theorem 3.1) we obtain that $|\log(T(Q))| \leq (c_3 \log(\Delta))/\sqrt{Q}$, where $c_3 = n^{O(1)}$. Therefore, if we set

$$Q = (c_3 \log(\Delta)/\log(5/4))^2 \quad \text{and} \quad \Theta = (3/2)C_{\mathcal{F}} F(Q),$$

then $(6/5)h_{\mathcal{F}} R_{\mathcal{F}} \leq \Theta \leq (15/8)h_{\mathcal{F}} R_{\mathcal{F}}$. By the methods of [12] the value $E(p)$ can be computed in time polynomially bounded by size($\mathcal{F}$), size($\mathcal{O}$) and p for every $p \leq Q$. Hence, there is a polynomial time algorithm that computes Θ. □

10 Proof of the Main Results

Theorem 29. *Assume the GRH. Then the set $\mathcal{H}$ of all pairs $(\mathcal{F}, h_{\mathcal{F}})$ belongs to $\mathcal{NP}$.*

Proof. We describe a nondeterministic algorithm that accepts the set $\mathcal{H}$. We know that there is a nondeterministic polynomial time algorithm which guesses on input of $\mathcal{F}$ the representation of the maximal order $\mathcal{O}$ of $\mathcal{F}$ and verifies it. There also exists a nondeterministic polynomial time algorithm that guesses the compact representations of r elements $\epsilon_1, \ldots, \epsilon_r$ such that $\text{size}_c(\epsilon_i)$ satisfies the bounds of Lemma 16 for $1 \leq i \leq r$. By Corollary 13, the algorithm can test in polynomial time, if the ϵ_i are units of $\mathcal{O}$. Finally, we note that there is a nondeterministic algorithm which guesses a number $w \leq n(n+1)/2$ and w elements of $\mathcal{F}$ and tests if they are roots of unity. Since the height of that elements is 1 this can be done in polynomial time, too.

The algorithm that accepts the set $\mathcal{H}$ starts the above algorithms. After that initialization, it computes by the method described in the proof of Theorem 27 an approximation R^* of precision 10 to the absolut value of the determinant of the matrix REG $= (\operatorname{Log}\epsilon_1, \ldots, \operatorname{Log}\epsilon_r)$. From [30] we know that $R_{\mathcal{F}} > 0.05$. Thus, the units ϵ_i are independent if and only if $R^* 2^{-10}$. If the units are not independent our algorithm begins an endless loop. Otherwise, R^* is an approximation of precision 10 to a multiple of $R_{\mathcal{F}}$. Using the algorithm of Theorem 28 it computes an approximation Θ of $h_{\mathcal{F}} R_{\mathcal{F}}$ such that $(6/5)h_{\mathcal{F}} R_{\mathcal{F}} < \Theta < (15/8)h_{\mathcal{F}} R_{\mathcal{F}}$. Then the algorithm verifies according to Theorem 23 that H is a multiple of the class number $h_{\mathcal{F}}$. Obviously, $H = h_{\mathcal{F}}$ if and only if $HR^* \leq \Theta$. □

References

1. J. Buchmann, *On the Computation of Units and Class Numbers by a Generalization of Lagrange's Algorithm*, Journal of Number Theory, Vol. 26, No. 1 (1987) 8-30
2. J. Buchmann, *On the Period Length of the Generalized Lagrange Algorithm*, Journal of Number Theory, Vol. 26, No. 1 (1987) 31-37
3. J. Buchmann, *Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper*, Habiliationsschrift, Düsseldorf (1987)
4. J. Buchmann, *A subexponentional algorithm for the determination of class group and regulator of algebraic number fields,* Séminaire de Théorie des Nombres, Paris 1988-1989, Birkhäuser Verlag (1990)
5. J. Buchmann, *Reducing lattice bases by means of approximations,* in preparation.
6. J. Buchmann, *Number Theoretic Algorithms, Algebraic Number Theory,* Lecture Notes, Saarbrücken, WS 88/89.
7. J. Buchmann, *Algorithms in algebraic number theory,* Manuscript (1992)
8. J. Buchmann, H. W. Lenstra, Jr., *Approximating rings of integers in number fields,* in preparation.
9. J. Buchmann, H. W. Lenstra, Jr., *Computing maximal orders and decomposing primes in number fields,* in preparation.
10. J. Buchmann, H. C. Williams, *On Principal Ideal testing in Algebraic Number Fields*, Journal of Symbolic Computation, Vol. 4, No. 1 (1987) 11-19
11. J. Buchmann, H. C. Williams, *On the existence of a short proof for the value of the class number and regulator of a real quadratic field,* NATO Advanced Science Institutes Series C, Vol. 256, Kluwer, Dordrecht (1989) 327-345
12. J. Buchmann, H. C. Williams, *On the Computation of the Class Number of an Algebraic Number Field,* Math. Comp., v. 53 (1989) 679-688
13. J. Buchmann, H. C. Williams, *Some Remarks Concerning the Complexity of Computing Class Groups of Quadratic Fields,* Journal of Complexity **7**, (1991) 311-315
14. J. Buchmann, Oliver van Sprang, *On short representations of orders and number fields,* Manuscript (1992)
15. J. Buchmann, H. C. Williams, C. Thiel, *Short representation of quadratic integers,* to appear in Proceedings of CANT 1992.
16. H. Cohen, *A Course in Computational algebraic number theory,* Springer Verlag (1993)
17. G. Ge, *Algorithms Related to Multiplicative Representations of Algebraic Numbers*, PhD. Thesis, University of California at Berkeley (1993)
18. S. Lang, Algebraic number theory, Springer-Verlag,New York (1986)
19. H. W. Lenstra, Jr., *Algorithms in algebraic number theory,* Bulletin (New Series) of The American Mathematical Society **26** no. 4 (1992) 211-244
20. A. K. Lenstra, H. W. Lenstra Jr., L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982) 515-534
21. K. S. McCurley, *Cryptographic key distribution and computation in class groups,* NATO Advanced Science Institutes Series C, Vol. 256, Kluwer, Dordrecht (1989) 459-479
22. W. Narkiewiecz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa (1974) 70
23. J. Neukirch, *Algebraische Zahlentheorie*, Springer Verlag, Berlin (1992)
24. H. R. Lewis, C. H. Papadimitriou, *Elements of the theory of computation,* Prentice-Hall (1981)

25. A. Schönhage, *Factorization of Univariate Integer Polynomials by Diophantine Approximation and an Improved Basis Reduction Algorithm,* ICALP (1984)
26. A. Schönhage, *Numerik analytischer Funktionen und Komplexität,* Jber. d. Dt. Math. Verein **92** (1990)
27. A. Schrijver, *Theory of linear and integer programming,* Wiley&Sons Ltd., Chichester (1987) 45-51
28. C. L. Siegel, *Gesammelte Abhandlungen IV,* Berlin, New York, Heidelberg (1979) 66-81
29. D. Weber, *Ein Algorithmus zur Zerlegung von Primzahlen in Primideale*, Universität des Saarlandes, Masterthesis (1993)
30. R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung,* Invent. math. **62** (1981) 367-380