A subexponential algorithm for the determination of class groups and regulators of algebraic number fields

Johannes Buchmann
FB 14-Informatik
Universität des Saarlandes
D-6600 Saarbrücken
West Germany

Abstract

A new probabilistic algorithm for the determination of class groups and regulators of an algebraic number field $\mathcal{F}$ is presented. Heuristic evidence is given which shows that the expected running time of the algorithm is $\exp(\sqrt{\log D \log\log D})^{c+o(1)}$ where D is the absolute discriminant of $\mathcal{F}$, where $c \in R_{>0}$ is an absolute constant, and where the $o(1)$-function depends on the degree of $\mathcal{F}$.

1 Introduction

Computing the class group and the regulator of an algebraic number field $\mathcal{F}$ are two major tasks of algorithmic algebraic number theory. In the last decade, several regulator and class group algorithms have been suggested (e.g. [16],[17],[18],[3]). In [2] the problem of the computational complexity of those algorithms was adressed for the first time. This question was then studied in [2] in great detail. The theoretical results and the computational experience show that computing class groups and regulators is a very difficult problem. More precisely, it turns out that even under the assumption of the generalized Riemann hypothesis (GRH) the fastest known deterministic algorithm is of complexity $D^{1/5+o(1)}$ where D is the absolute discriminant of $\mathcal{F}$. This running time is exponential in the length of the input data since this length is polynomially bounded in $\log D$.

Computationally hard problems in number theory are a very good source for secure cryptosystems as is well known for the factoring problem. Therefore, in [7], [4], [8] and [9] the use of quadratic fields in cryptology was suggested and discussed. Stimulated by this new application, Hafner and McCurley [11] invented a new probabilistic class group algorithm for imaginary quadratic fields and they proved under the assumption of the GRH that the expected running time of this new method is $L(D)^{\sqrt{2}+o(1)}$ where $L(D) = \exp\sqrt{\log D \log\log D}$. In this paper we will generalize the idea of Hafner and McCurley to arbitrary number fields. If we use an additional assumption about the number of "smooth reduced ideals", then we obtain the computational complexity $L(D)^{1.7+o(1)}$ where the $o(1)$-function depends on the degree of the field $\mathcal{F}$.

2 The idea

The algorithm of Hafner and McCurley makes use of the fact that under the GRH the class group Cl of an imaginary quadratic field $\mathcal{F}$ is generated by the prime ideals of norm below $6(\log D)^2$. By means of a probabilistic method the algorithm finds a basis for the lattice $L \subseteq \mathcal{Z}^k$ of relations for a generating system for Cl containing k elements. Since $\mathcal{Z}^k/L \cong Cl$, the knowledge of this basis implies the knowledge of the structure and the basis of Cl. The fact that a basis for the full lattice L has been found can be verified by means of the analytic class number formula by which an approximation h^* to the class number h of $\mathcal{F}$ with

$$h < h^* < 2h$$

can be determined in time polynomial in $\log D$ ([6]): A linearly independent system of k lattice vectors is a basis of L if its determinant is less than h^*.

For arbitrary number fields $\mathcal{F}$ the prime ideals of $\mathcal{F}$ whose norms do not exceed $12(\log D)^2$ will also generate Cl (see [6]) (assuming again the GRH). As we will show below, it is still possible to generate random relations among a small generating system for Cl. It is, however, not known how to verify in polynomial time that the proper class number has been found because in the general case the analytic class number formula only yields a polynomial time method for calculating a number h^* with

$$hR < h^* < 2hR$$

where h is the class number and where R is the regulator of $\mathcal{F}$.

Moreover, it seems to be more appropriate to calculate the regulator and the class number of $\mathcal{F}$ simultaneously because those two invariants are closely related.

We will, therefore, introduce a lattice L whose determinant $d(L)$ is hR. We will then explain how to find random vectors in L, how to verify that a basis for L has been found, and how to determine Cl and R if such a basis is known.

For $c \in R_{>0}$ we define

$$F_c = \{\wp | \wp \text{ prime ideal of } \mathcal{F}, N\wp \le c\}$$

where for any fractional ideal A of $\mathcal{F}$ we denote by NA the absolute norm of A. F_c is a finite set. We write

$$F_c = \{\wp_1, \wp_2, \ldots, \wp_{k(c)}\}.$$

Furthermore, we denote by A_c the set of all the non zero numbers in $\mathcal{F}$ which, considered as principal ideals, can be represented as a power product of the ideals in the *factor base* F_c, i.e.

$$A_c = \left\{ \alpha \in \mathcal{K}^\times \middle| \alpha O_F = \prod_{i=1}^{k(c)} \wp_i^{e_i} \right\}.$$

Every number in A_c represents a relation among the classes of the ideals in F_c. We are interested in the lattice of those relations and we, therefore, introduce two maps.

For $\alpha \in A_c$ with

$$\alpha O_F = \prod_{i=1}^{k(c)} \wp_i^{e_i}$$

we define

$$\varphi'_c(\alpha) = (e_1, \ldots, e_{k(c)}).$$

Moreover, using the logarithm map

$$\begin{array}{lcccl} \mathrm{Log} & : & \mathcal{F}^\times & \longrightarrow & R^r \\ & & \alpha & \longmapsto & (\log|\alpha|_1, \ldots, \log|\alpha|_r) \end{array}$$

where $r = s + t - 1$, s the number of real places of $\mathcal{F}$, t the number of complex places of $\mathcal{F}$ and where $||_i$ $(1 \le i \le m = s + t)$ are the archimedian valuations on $\mathcal{F}$, we define

$$\varphi_c(\alpha) = (e_1, \ldots, e_{k(c)}, \mathrm{Log}\,\alpha).$$

Hence, we have two maps

$$\varphi_c \colon A_c \to \mathcal{Z}^{k(c)} \times R^r$$

and

$$\varphi'_c \colon A_c \to \mathcal{Z}^{k(c)}.$$

Both maps are actually homomorphisms of the multiplicative group A_c into the additive groups $\mathcal{Z}^{k(c)} \times R^r$ or $\mathcal{Z}^{k(c)}$, respectively.

Note that for imaginary quadratic fields we have $r = 0$ and therefore, both maps coincide.

We can now define the lattice L_c.

Theorem 2.1 *Let $c \in R_{>0}, c > 12(\log D)^2$ and assume the GRH. The set $L_c = \varphi_c(A_c)$ is a $(k(c) + r)$-dimensional lattice of determinant hR. The set $L'_c = \varphi'_c(A_c)$ is a $k(c)$-dimensional lattice of determinant h and we have $\mathcal{Z}^{k(c)}/L'_c \cong Cl$.*

Proof: The set L'_c is the kernel of the homomorphism

$$\begin{array}{rcl} \mathcal{Z}^{k(c)} & \longrightarrow & Cl, \\ \underline{v} = (v_1, \ldots, v_{k(c)}) & \longmapsto & \prod_{i=1}^{k(c)} \overline{\wp_i}^{v_i} \end{array}$$

where for an ideal A of $\mathcal{F}$ we denote by $\overline{A}$ its class in the class group. Therefore, L'_c is a subgroup of $\mathcal{Z}^{k(c)}$, i.e. a lattice.

By a theorem of [1] the assumption $c > 12(\log D)^2$ implies that this map is surjective. Hence, by the homomorphism theorem, we have

$$\mathcal{Z}^{k(c)}/L'_c \cong Cl.$$

Since the class group is finite, it follows that L'_c must be of dimension $k(c)$ and of determinant $h = |Cl|$.

In order to prove the first assertion, we let $\alpha_1, \ldots, \alpha_{k(c)} \in A_c$ such that the vectors $\varphi'_c(\alpha_1), \ldots, \varphi'_c(\alpha_{k(c)})$ form a basis of L'_c. We also let $\epsilon_1, \ldots, \epsilon_r$ be a set of fundamental units of $\mathcal{F}$. We claim that $\varphi(\alpha_1), \ldots, \varphi(\alpha_{k(c)}), \varphi(\epsilon_1), \ldots, \varphi(\epsilon_r)$ is a basis for L_c.

To prove that those vectors generate L_c, we choose any $\alpha \in A_c, \alpha O_F = \prod_{i=1}^{k(c)} \wp_i^{e_i}$.

Then the vector $\varphi'_c(\alpha)$ must be representable on the basis we have chosen:

$$\varphi'_c(\alpha) = \sum_{i=1}^{k(c)} \lambda_i \varphi'_c(\alpha_i)$$

where the λ_i are rational integers. Since φ'_c is a homomorphism, we have

$$\sum_{i=1}^{k(c)} \lambda_i \varphi'_c(\alpha_i) = \varphi'_c\left(\prod_{i=1}^{k(c)} \alpha_i^{\lambda_i}\right).$$

Hence, the images of α and $\tilde{\alpha} = \prod_{i=1}^{k(c)} \alpha_i^{\lambda_i}$ under the mapping φ' are the same, which means that those numbers generate the same principal ideal. Consequently $\epsilon = \alpha/\tilde{\alpha}$ must be a unit in O_F, i.e. ϵ can be written as

$$\epsilon = \varsigma \cdot \prod_{i=1}^{r} \epsilon_i^{x_i}$$

where ς is a root of unity in O_F and were the exponents x_i are rational integers.

Applying the logarithm map we obtain

$$\operatorname{Log} \epsilon = \sum_{i=1}^{r} x_i \operatorname{Log}(\epsilon_i).$$

In view of the fact that $\varphi'(\epsilon_i) = (0, \ldots, 0)$ for $1 \le i \le r$ we finally have

$$\begin{aligned}\varphi_c(\alpha) &= \varphi_c(\tilde{\alpha}) + \varphi_c(\epsilon)\\ &= \sum_{i=1}^{r} \lambda_i \varphi_c(\alpha_i) + \sum_{i=1}^{r} x_i \varphi_c(\epsilon_i),\end{aligned}$$

which shows that $\varphi(\alpha_1), \ldots, \varphi(\alpha_{k(c)}), \varphi(\epsilon_1), \ldots, \varphi(\epsilon_r)$ is a generating system for L_c over $\mathcal{Z}$.

In order to see that this generating system is actually linearly independent, we observe that the matrix, whose columns are the elements of the generating system is of the form

$$G = \begin{pmatrix} \varphi_c'(\alpha_1), & \ldots, & \varphi_c'(\alpha_{k(c)}), & \underline{0}, & \ldots, & \underline{0} \\ \operatorname{Log}(\alpha_1), & \ldots, & \operatorname{Log}(\alpha_{k(c)}), & \operatorname{Log}(\epsilon_1), & \ldots, & \operatorname{Log}(\epsilon_r) \end{pmatrix}.$$

Hence, we have

$$|\det G| = |\det(\varphi_c'(\alpha_1), \ldots, \varphi_c'(\alpha_{k(c)}))| \cdot |\det(\operatorname{Log}\epsilon_1, \ldots, \operatorname{Log}\epsilon_r)| = hR \ne 0.$$

Hence, it follows that the generating system is linearly independent and we have proved that the determinant of the lattice L_c is, in fact, hR. $\square$

3 Determination of random relations in L_c.

We assume that $c \in R_{>0}$ is chosen such that $c > 12(\log D)^2$. This implies that the classes of the ideals in the factor base generate the class group of $\mathcal{F}$.

3.1 The idea of Hafner & McCurley

If $\mathcal{F}$ is a complex quadratic field, i.e. if $r = 0, L_c = L_c'$, then we can use the method of Hafner and McCurley [11] to produce random relations in L_c.

They suggest the following : fix a parameter $B \in \mathcal{Z}_{>0}$. Put

$$\mathcal{Z}_B = \{0, 1, \ldots, B-1\}.$$

After those preparations generate vectors in L_c as follows: Pick at random a vector $\underline{v} = (v_1, \ldots, v_{k(c)}) \in \mathcal{Z}_B^{k(c)}$. Determine the reduced ideal A' in the class of

$$A = \prod_{i=1}^{k(c)} \wp_i^{v_i}. \tag{1}$$

Try to factor A' over the factor base F_c. Suppose this factorization can be completed successfully, i.e.

$$A' = \prod_{i=1}^{k(c)} \wp_i^{v_i'} \tag{2}$$

where the exponent vector $\underline{v}' = (v'_1, \ldots, v'_{k(c)})$ has rational integer entries. Then, since A and A' belong to the same ideal class, the ideal

$$A(A')^{-1} = \prod_{i=1}^{k(c)} \wp_i^{v_i - v'_i} \tag{3}$$

is principal which means that the vector $\underline{e} = \underline{v} - \underline{v}'$ belongs to the lattice L_c.

For fields of arbitrary degree we can, in principle, adopt the method of Hafner and McCurley. We must, however, realize that reduction of an ideal is no longer unique. An ideal class can contain many reduced ideals. Nevertheless, any reduced ideal A' in the class of A can be written as

$$A' = \frac{1}{\alpha} A \tag{4}$$

with $\alpha \in A - \{0\}$. If A' can be written as in (2), then we have found

$$(v_1 - v'_1, \ldots, v_{k(c)} - v'_{k(c)}, \mathrm{Log}\,\alpha) \in L_c.$$

3.2 Reduction

What does *reduction* mean? A fractional ideal A' of $\mathcal{F}$ is called *reduced* if it is primitive and the least positive integer in A is a *minimum* in A'. A number α in a fractional ideal A of $\mathcal{F}$ is called a *minimum*, if the only number $\beta \in A$ satisfying $|\beta|_i < |\alpha|_i$ for $1 \leq i \leq m$ is $\beta = 0$. A reduced ideal in the class of A can be determined as follows. Consider the Minkowski map

$$\begin{aligned} &\mathcal{F} \to R^n \\ &\alpha \longmapsto \underline{\alpha} = (\alpha^{(1)}, \ldots, \alpha^{(s)}, Re\ \alpha^{(s+1)}, Im\ \alpha^{(s+1)}, \ldots, Re\ \alpha^{(m)}, Im\ \alpha^{(m)}) \end{aligned}$$

where $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are the algebraic conjugates of $\alpha \in \mathcal{F}$, numbered such that $\alpha^{(i)} \in R$ for $1 \leq i \leq s$ and $\alpha^{(t+i)} = \overline{\alpha^{(i)}}$ for $s+1 \leq i \leq s+t = m$.

The image $\underline{A}$ under this map is an n-dimensional lattice in R^n of determinant $\sqrt{D}\ NA$. Compute a number $\alpha \in A$ such that $\underline{\alpha}$ is a shortest non zero vector in $\underline{A}$. Then clearly, $\frac{a}{\alpha}A$ is reduced where a is the least positive integer such that $\frac{a}{\alpha}A$ is integral (see [13]).

Since computing shortest vectors in lattices is polynomial time for fixed dimension, we see that the above algorithm takes polynomial time for fixed degree n. In particular, if A is the product of two reduced ideals, then the running time of the algorithm will be polynomial in $\log D$.

3.3 The general procedure

In the general case we must find vectors

$$\underline{e} = (e_1, \ldots, e_{k(c)}, \operatorname{Log}\alpha) \in L_c$$

where $\operatorname{Log}\alpha$ is not uniquely determined by $e_1, \ldots, e_{k(c)}$. Hence, it is not sufficient to randomize $\underline{e}$ by choosing an exponent vector $\underline{v}' = (v_1, \ldots, v_{k(c)})$ and to reduce the corresponding c-smooth ideal but we choose a random vector

$$\underline{v} = (v_1, \ldots, v_{k(c)+r}) \in \mathcal{Z}_D^{k(c)+r}.$$

The last r coordinates of $\underline{v}$ will determine the last r coordinates of $\underline{e}$. We compute a reduced ideal $A' = \frac{1}{\alpha}A$ in the class of $A = \prod_{i=1}^{k(c)} \wp_i^{v_i}$. The choice of the particular reduced ideal depends on the parameters $v_{k(c)+1}, \ldots, v_{k(c)+r}$ in the following way: since A' is reduced, it follows that α is a minimum of A. the image of the set M_A under the logarithm map is discrete. More precisely, it has been shown in [2] that there are constants c_1, c_2 (all the constants c_i used in the sequel depend only on the degree of $\mathcal{F}$) such that every cube in R^r of side length $(\log D)^{-c_1}$ contains at least one logarithm vector of a minimum in A and, correspondingly, every cube in R^r of side length $(\log D)^{c_2}$ contains at most one logarithm vector of a minimum of A. Cover all R^r with cubes of side length $(\log D)^{-c_1}$. The position of each cube is uniquely determined by a r-dimensional integer vector. Our procedure finds the reduced ideal $A' = \frac{1}{\alpha}A$ such that $\operatorname{Log}\alpha$ is closest to the cube determined by $(v_{k(c)+1}, \ldots, v_{k(c)+r})$. The vector $(v_{k(c)+1}, \ldots, v_{k(c)+r})$ is called a *coordinate vector* of $\operatorname{Log}\alpha$. By means of the results in [2] this can be done in time polynomial in $\log D$. The whole procedure will be referred to as procedure PV.

3.4 Randomness of the lattice vectors

We first discuss which lattice vectors are found with positive probability by the procedure PV.

If we want to find $\underline{e} = (e_1, \ldots, e_{k(c)}, \operatorname{Log}\alpha)$ by our procedure, then we must start from a random vector $\underline{v} = (v_1, \ldots, v_{k(c)+r})$ where $(v_{k(c)+1}, \ldots, v_{k(c)+r})$ is a coordinate vector of $\operatorname{Log}\alpha$ and where $A' = \frac{1}{\alpha}A = \frac{1}{\alpha}\prod_{i=1}^{k(c)} \wp_i^{v_i}$ is a c-smooth reduced ideal. Hence, $\underline{e}$ will be found with positive probability if such a random vector exists in $\mathcal{Z}_D$.

If

$$0 \le \log|\alpha|_i \le D \cdot (\log D)^{-c_1} \quad (1 \le i \le r),$$

then it follows from the remarks of the previous section that there is a coordinate vector $(v_{k(c)+1,\ldots,}v_{k(c)+r})$ of $\operatorname{Log}\alpha$ in $\mathcal{Z}_D^r$.

Let $A' = \prod_{i=1}^{k(c)} \wp_i^{v_1}$ be any c-smooth reduced ideal. Then we know from [2] that

$$|v_i'| \le \log D \quad (1 \le i \le k(c)).$$

Hence, if

$$0 \leq e_i \leq D - \log D \qquad (1 \leq i \leq k(c)),$$

then $\underline{v} = (e_1 + v_1', \ldots, e_{k(c)} + v_{k(c)}', v_{k(c)+1,\ldots,}v_{k(c)+r}) \in \mathcal{Z}_D^{k(c)+r}$.

Put

$$\mathcal{Q}^- = [0, D - \log D]^{k(c)} \times [0, D(\log D)^{-c_1}]^r$$

and define N_c to be the number of c-smooth reduced ideals in $\mathcal{F}$.

Lemma 3.1 *Let $\underline{e} \in L_c \cap Q_D^-$ and let $N_{\underline{e}}$ be the number of choices for $\underline{v} \in \mathcal{Z}_D^{k(c)+r}$ which as input for the procedure PV yield $\underline{e}$. Then we have*

$$N_{\underline{e}} = N_c.$$

It also follows from the remarks above that any lattice vector which is computed by the procedure PV belongs to

$$\mathcal{Q}^+ = [-\log D, D + \log D]^{k(c)} \times [-(\log D)^{c_2}, D(\log D)^{-c_1} + (\log D)^{c_2}]^r.$$

Moreover, it can be deduced from the results in [2] that the number of coordinate vectors for a fixed logarithm vector is bounded by $(\log D)^{c_3}$. Hence, we have

Lemma 3.2 *Let $\underline{e} \in L_c$ and let $N_{\underline{e}}$ be the number of choices for $\underline{v} \in \mathcal{Z}_D^{k(c)+r}$ which as input for the procedure PV yield $\underline{e}$. Then $N_{\underline{e}} = 0$ for $\underline{e} \notin \mathcal{Q}^+$ and for $\underline{e} \in \mathcal{Q}^+$ we have*

$$N_{\underline{e}} \leq (\log D)^{c_3} \cdot N_c.$$

3.5 Producing a generating system

In this section we estimate how many vectors in L_c we must generate in order to obtain a generating system for L_c.

Suppose we have found the vectors $e_1, \ldots, e_j$. If $j = 0$, then we have not yet found anything. Let L_j be the lattice generated by those vectors and let d_j be its dimension and if $d_j = k(c) + r$ let $I_j = [L_c \colon L_j]$. We will estimate the probability p_{j+1} for the procedure PV to yield a vector $e_{j+1} \in L_c - L_j$.

Let $N_1 = |L_j \cap \mathcal{Q}^-|, N_2 = |L_c \cap \mathcal{Q}^-|$. Then it follows from Lemma 3.1 that

$$p_{j+1} \geq \frac{1}{D^{k(c)+r}}(N_2 - N_1).$$

Lemma 3.3 *If $d_j < k(c) + r$, then we have*

$$N_1 \leq (\log D)^{c_4} \left(3D\sqrt{k(c) + r}\right)^{d_j}.$$

Proof: Since $\mathcal{Q}^+$ contains a generating system for L_j this box also contains a basis for L_j. Denote the corresponding fundamental parallelepiped by $\mathcal{F}_j$. Also, denote by V_j the real vector space spanned by L_j. Then for every lattice vector $\underline{e} \in L_j \cap \mathcal{Q}^+$ the translated set $\underline{e} + F_j$ is contained in $2\mathcal{Q}^+ \cap V_j$. Hence

$$N_1 \leq \operatorname{vol}(2\mathcal{Q}^+ \cap V_j)/\det L_j.$$

By the methods of [2] it can be shown that

$$\det L_j \geq (\log D)^{-c_4}.$$

In order to estimate $\operatorname{vol}(2\mathcal{Q}^+ \cap V_j)$, we choose an orthonomal basis $\underline{b}_1, \ldots, \underline{b}_j$ of V_j. Let $\omega \in 2\mathcal{Q}^+ \cap V_j$. Then we can write

$$\underline{\omega} = (\omega_1, \ldots, \omega_{k(c)+r}) = \sum_{i=1}^{d_j} \lambda_1 \underline{b}_i.$$

Here we have $|\omega_i| \leq 3D$ (for sufficiently large D and $1 \leq i \leq k(c) + r$). This inequality implies

$$|\lambda_i| = |(\underline{\omega}, \underline{b}_i)| \leq ||\omega|| \leq 3D\sqrt{k(c)+r}$$

and therefore

$$\operatorname{vol}(2\mathcal{Q}^+ \cap V_j) \leq \left(3D\sqrt{k(c)+r}\right)^{d_j}.$$

This completes the proof. □

We define $\lambda(D) = \sqrt{D}(\log D)^{n-1}$.

Lemma 3.4 *If $d_j = k(c) + r$, then there is a lattice basis of L_j in $[0, c_5\lambda(D)I_j]^{k(c)+r}$.*

Proof: By a theorem of Siegel we have

$$\det L_j = h \cdot R \cdot I_j \leq c_5 \lambda(D) I_j.$$

Hence, there is a basis of L_j whose integer entries are bounded by $c_5\lambda(D)I_j$. Since the determinant of the sublattice of $\operatorname{Log} O_F^\times$ embedded in L_j is bounded by RI_j, it follows that there is a basis of that sublattice contained in $[0, c_6\lambda(D)I_j]^r$. This also implies that each vector in the basis of L_j can be modified such that its logarithm vector part belongs to $[0, c_5\lambda(D)I_j]^r$ and this concludes the proof. □

Lemma 3.5 *If $d_j = k(c) + r$, then we have*

$$N_1 \leq (D + c_5\lambda(D)I_j)^{k(c)+r}/(h \cdot R \cdot I_j).$$

Proof: Let $\mathcal{F}_j$ be the fundamental parallelepiped of the basis of Lemma 3.4. Then for every $\underline{e} \in \mathcal{Q}^+ \cap L_j$ the translated set $\underline{e} + \mathcal{F}_j$ belongs to $[0, D + c_5\lambda(D)I_j]$ and this implies the assertion. □

Lemma 3.6 *We have*

$$N_2 \geq (D - c_5\lambda(D)^{k(c)}(D(\log D)^{-c_1} - c_5\lambda(D))^r/(hR).$$

Proof: Let $\mathcal{F}$ be the fundamental parallelepiped of the basis of L_c from Lemma 3.4. Then for every $\underline{e} \in \mathcal{Q} \cap L_c$ the intersection of the box

$$[0, D - c_5\lambda(D)]^{k(c)} \times [0, D(\log D)^{-c_1} - c_5\lambda(D)]^r$$

is not empty and this implies the assertion. □

Corollary 3.1

$$p_{j+1} = p_{j+1}(D) \geq \frac{N_c}{h \cdot R} \cdot (\log D)^{-c_1}(1 - o(1)).$$

Proof: The total number of choices for exponent vectors $\underline{v}$ in procedure PV is $D^{k(c)+r}$. Hence, the assertion follows from Lemma 3.3, Lemma 3.5 and Lemma 3.6 □

For $\beta > 0$ define

$$L[\beta] = \exp\left(\sqrt{\log D \log\log D}\right)^{\beta + o(1)}$$

where for fixed n the notation $o(1)$ represents a function of D which tends to 0 as D tends to infinity.

In order to be able to determine the expected running time of the algorithm, we assume that the number $N_{L[\beta]}$ of $L[\beta]$-smooth reduced ideals is

$$N_{L[\beta]} = D^{\frac{1}{2}} L[-1/(4\beta)].$$

For imaginary quadratic fields this equation is a theorem due to Seysen [19] and it can be proved for real quadratic fields by the same method. For higher degree fields the equation the equation is still a conjecture. We will refer to it as *"smoothness assumption"* Choose $\beta > 0$ such that $C = L[\beta]$.

Theorem 3.1 *Under the GRH and the smoothness assumption a generating system for L_c consisting of $L[\beta]$ elements can be computed in expected running time $L[2\beta + \frac{1}{4\beta}]$.*

Proof: It follows from the theorem of Brauer and Siegel and from Corollary 3.1 that we have

$$p_{j+1}(D) = L\left[-\frac{1}{4\beta}\right]$$

Since $k(c) = L[\beta]$ it follows that the expected number of applications of the procedure PV before a sublattice L_o of finite index is found is $L\left[\beta + \frac{1}{4\beta}\right]$.

By Hadamards inequality we have $[L_c \colon L_0] \leq \exp(L[\beta])$. Hence the expected number of applications of procedure PV before a generating system of L_c is found is again $L\left[\beta + \frac{1}{4\beta}\right]$.

Each application of procedure PV requires $L[\beta]$ binary operations and this completes the proof. □

3.6 Finding a basis for L_c

Suppose that we know a generating system $\underline{e}_1, \ldots, \underline{e}_j$ for L_c. In order to determine the structure of the class group and the regulator of $\mathcal{F}$, we proceed as follows: First we consider the matrix E' whose columns are the vectors $\underline{e}'_1, \ldots, \underline{e}'_j$ consisting of the first $k(c)$ entries of the vectors $\underline{e}_1, \ldots, \underline{e}_j$, its entries are rational integers whose binary length is polynomially bounded in $\log D$. As in [11] we can compute both the Hermite and the Smith normal form of E' in time $L[4\beta]$ where again $\beta \in R_{>0}$ is such that $c = L(D)^\beta$. The Smith normal form will yield the class number and the structure of the class group.

According to [5] the generating system for the lattice L_c can be transformed into a basis in time $L[9\beta]$. It is, however, very likely that there is a faster way of doing this. The regulator computation therefore takes $L[9\beta]$ operations.

We can now discuss the optimal choice for β. Since the computation of the generating system requires $L[2\beta + \frac{1}{4\beta}]$ operations, optimizing β means solving the equation

$$2\beta + \frac{1}{4\beta} = 9\beta.$$

One solution of this equation is $\beta = \frac{1}{2}\frac{1}{\sqrt{7}}$ which means that the expected running time of the whole procedure is $L[1.7]$.

Theorem 3.2 *Under the assumption of the GRH and the smoothness condition the class number, the structure of the class group and the regulator of an algebraic number field of degree n and absolute discriminant D can be computed in expected running time $L(D)$ for fixed n as D tends to infinity where $L(D) = \exp(\sqrt{\log D \log\log D})$.*

References

[1] E. Bach, *What to do until the witness comes*, preprint 1988.

[2] J. Buchmann, *Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper.* Habilitationsschrift, Düsseldorf, 1987.

[3] J. Buchmann, *On the computation of units and class numbers by a generalization of Lagranges' algorithm*, J. Number Theory **26** (1987), 8-30.

[4] J. Buchmann, S. Düllmann, H.C. Williams, *On the complexity and efficiency of a new key exchange system*, Proceedings EUROCRYPT'89, to appear.

[5] J. Buchmann, V. Kessler, *Computing a reduced lattice basis from a generating system with applications*, Preprint 1990.

[6] J. Buchmann, H.C. Williams, *On the computation of the class number of an algebraic number field*, Math. comp. **53** (1989), 679-688.

[7] J. Buchmann, H.C. Williams, *A key exchange system based on imaginary quadratic fields,* J. Cryptology **1** (1988), 107-118.

[8] J. Buchmann, H.C. Williams, *A key exchange system based on real quadratic fields*, Proceedings CRYPTO 89, to appear.

[9] J. Buchmann, H.C. Williams, *Quadratic fields and cryptology*, to appear.

[10] P.D. Domich, R. Kannan, L.E. Trotter, *Hermite normal form computation using modulo determinant arithmetic*, Math. Op. Res. **12** (1987), 50-59.

[11] J.L. Hafner, K.S. McCurley, *A rigorous subexponential algorithm for computation of class groups,* Journal AMS, to appear.

[12] A.K. Lenstra, H.W. Lenstra, L. Lowasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 513-534.

[13] H.W. Lenstra Jr., *Integer programming with a fixed number of variables*, Math. Op. Res. **8** (1983), 538-548.

[14] K.S. McCurley, *Cryptographic key distribution and computation in class groups*, Proceedings of NATO ASI Number Theory and Applications, Kluwer Academic Publishers 1989, 459-479.

[15] M. Pohst, *A modification of the LLL reduction algorithm*, J. Symbolic Computation **4** (1987), 123-127.

[16] M. Pohst, P. Weiler und H. Zassenhaus, *On effective computation of fundamental units I,II,* Math. Comp. **38** (1982), 275-329.

[17] M. Pohst, H. Zassenhaus, *Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper*, J. Reine angew. Math. **361** (1985), 50-72.

[18] M. Pohst, H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[19] M. Seysen, *A Probabilistic Factorization algorithm with quadratic Forms of Negative Discriminant*, Math. Comp **48**, 1987,737-780.

[20] D. Shanks, *Class number, a theory of factorization and genera,* Proc. Symp. Pure Math. **20** (1969 Institute on number theory), Amer. Math. Soc., Providence, 1971, 415-440.

[21] D. Shanks, *Five number theoretic algorithms,* Proc. Second Manitoba Conference on Numerical Math., 1972, 51-70.