Some remarks concerning the complexity of computing class groups of quadratic fields

Johannes A. Buchmann
FB-10 Informatik
Universität des Saarlandes
6600 Saarbrücken
West Germany

Hugh C. Williams
Department of Computer Science
University of Manitoba
Winnepeg, Manitoba
Canada, R3T2N2

August 10, 1993

Abstract

Let O be an order of a quadratic number field. In this paper we show that under the assumption of the generalized Riemann hypothesis the following decision problems are in NP $\cap$ co-NP:

1. Is a given ideal A of O principal?
2. Given ideals $A_1, \ldots, A_k$ of O, do their equivalence classes generate the class group of O.
3. Given ideals $A_1, \ldots, A_k$ of O, do their equivalence classes form a basis for the class group of O?

1 Introduction

Let Δ be a rational integer which is not a perfect square, $\Delta \equiv 0, 1 \mod 4$.

Then

$$O = \mathbf{Z} + \mathbf{Z}\frac{\Delta + \sqrt{\Delta}}{2}$$

is the *quadratic order* of *discriminant* Δ.

In McCurley [3] and Buchmann/Williams [1] it was shown that the following decision problems belong to the complexity class NP.

(P) Is a given ideal A in O principal?

(h) Is $h' \in \mathbf{Z}_{\geq 1}$ equal to the *class number* h of O?

We remark that (h) could be proved to be in NP only under the assumption of the the generalized Rieman Hypothesis (GRH). In addition, we consider in this paper the following decision problems.

(G) Given ideals $A_1, \ldots, A_k$ of O. Do their equivalence classes $\overline{A}_1, \ldots, \overline{A}_k$ generate the *class group* Cl of O?

(B) Given ideals $A_1, \ldots, A_k$ of O. Do their equivalence classes form a basis of Cl?

(O) Given an ideal A of O and $\lambda \in \mathbf{Z}_{\geq 1}$. Is λ the order of $\overline{A}$ in Cl?

We will prove in this paper

Theorem 1.1 *Under the assumption of the GRH the problems (P),(G),(B),(h) and (O) belong to the complexity class NP $\cap$ co-NP.*

2 The proofs

Let $A_1. \ldots, A_k$ be ideals of O. Assume that their equivalence classes generate Cl and that a prover P wants to demonstrate this to a verifier V in polynomial time. Under the assumption of the GRH the equivalence classes of those principal ideals $\mathcal{P}_1, \ldots, \mathcal{P}_n$ whose norm does not exceed $C_1(\log|\Delta|)^2$, where C_1s an absolute constant, generate Cl (see Bach [2]). P may, therefore, assume that V knows this generating system which is of polynomial length. All he need give to V in order to prove that $S = \{\overline{A}_1, \ldots, \overline{A}_k\}$ generates Cl is the representation of the generators $\overline{\mathcal{P}}_1, \ldots, \overline{\mathcal{P}}_n$ on this system:

$$\overline{\mathcal{P}}_j = \prod_{i=1}^{k} \overline{A}_i^{v_{ij}}, \; 1 \leq j \leq n \tag{1}$$

with $v_{ij} \in \mathbf{Z}_h = \{0, 1, \ldots, h-1\}$ for $1 \leq i \leq k, 1 \leq j \leq n$ together with short proofs for (1) which exist since $(P) \in$ NP. This shows

Proposition 2.1 *$(G) \in NP$.*

Now suppose that P wants to prove to V that S even forms a basis of Cl. Then he uses

Proposition 2.2 *Let G be a finite abelian group and let $g_1, \ldots, g_k$ be a generating system for G. Then $\{g_1, \ldots, g_k\}$ is a basis of G if and only if $h' = \prod_{i=1}^{k} \operatorname{ord} g_i$ divides $|G|$ and if $\operatorname{ord} g_i > 1$ for $1 \leq i \leq k$.*

Proof: Clearly, if $\{g_1, \ldots, g_k\}$ is a basis of G, then $h' = |G|$.

Conversely, assume that $h' \mid |G|$. The vectors $\underline{v}_j = (v_{1j}, \ldots, v_{kj})$ with $v_{ij} = 0$ for $i \neq j$ and $v_{ii} = \operatorname{ord} g_i$ $(1 \leq i, j \leq k)$ form a basis of a sublattice γ' of the kernel γ of $\mathbf{Z}^k \to G, \underline{v} = (v_1, \ldots, v_k) \longmapsto \prod\limits_{i=1}^{k} g_i^{v_i}$. γ' is of finite index in γ and $\det \gamma = |G|, \det \gamma' = h'$. Hence, $h' \| G|$ implies that $h = |G|$ and that $\underline{v}_1, \ldots, \underline{v}_k$ forms a basis of γ. As a consequence, $\{g_1, \ldots, g_k\}$ must be a basis of G because for every vector $\underline{v} \in \gamma, \underline{v} = (v_1, \ldots, v_k)$ we must have $v_i \equiv 0 \mod \operatorname{ord} g_i$ for $1 \leq i \leq k$. $\square$

After having proved that S generates Cl and that h is the class number of O, P must only give the orders a_i of $\overline{A}_i$ $(1 \leq i \leq k)$ to V and short proofs for $\overline{A}_i^{a_i} = \overline{0}$ for $1 \leq i \leq k$. Then V can verify that $\operatorname{ord} \overline{A}_i | a_i$ for $1 \leq i \leq k$ and, therefore $\prod\limits_{i=1}^{k} \operatorname{ord} \overline{A}_i \; |h$ which by Proposition 2.2 means that S forms a basis of Cl. So we have proved

Proposition 2.3 *$(B) \in NP$*

We remark that the above proof also shows to V that a_i is the order of A_i for $1 \leq i \leq k$.

Once P has proved to V that S is a basis of Cl he can now give short proofs for (O). Let A be an ideal of O. Then we have

$$\overline{A} = \prod_{i=1}^{k} \overline{A}_i^{x_i} \tag{2}$$

where $x_i \in \mathbf{Z}$ is unique modulo $a_i = \operatorname{ord} \overline{A}_i$ for $1 \leq i \leq k$. We also have

$$\operatorname{ord} A = \operatorname{lcm}\left(\frac{a_1}{\gcd(a_1, x_1)}, \ldots, \frac{a_k}{\gcd(a_k, x_k)}\right). \tag{3}$$

If P gives $x_1, \ldots, x_k$ to V and a short proof for (2), then V can use (3) to check whether a given number a is the order of A.

This shows

Proposition 2.4 *$(O) \in NP \cap co\text{-}NP$*

and

Proposition 2.5 *$(P) \in NP \cap co\text{-}NP$.*

Now suppose that P wants to prove that for ideals $A_1, \ldots, A_k$ of O the system $S = \{\overline{A}_1, \ldots, \overline{A}_k\}$ is not a basis of Cl. If there is a non trivial relation among the elements of S, then P presents this relation to V together with a short proof for its correctness. P also gives the orders a_i if $\overline{A}_i$ in Cl to V $(1 \leq i \leq k)$ together with short proofs for their correctness. Then V can verify that the relation is, in fact, non trivial. But if S is a multiplicatively independent system which is not a generating system for Cl, then we must have $\prod_{i=1}^{k} a_i < h$ for which by Proposition 2.4 and by the results of [3] and [1] there exists a short proof.

Proposition 2.6 *$(B) \in co\text{-}NP$*

Finally, P wants to prove that for ideals $A_1, \ldots, A_k$ the system $\{\overline{A}_1, \ldots, \overline{A}_k\}$ does not generate Cl.

By Proposition2.3 we may assume that both P and V know a basis $B = \{\overline{B}_1, \ldots, \overline{B}_m\}$ of Cl and the orders b_i of $\overline{B}_i$ in Cl for $1 \leq i \leq m$.

If S is not a generating system for Cl, then there must be an element $\overline{B} = \prod_{i=1}^{m} \overline{B}^{\lambda_i}$ which has no representation on S. Let

$$\overline{A}_j = \prod_{i=1}^{m} \overline{B}_i^{n_{ij}} \text{ for } 1 \leq j \leq k. \tag{4}$$

If $\overline{B}$ were presentable on S, this would mean that

$$\overline{B} = \prod_{j=1}^{k} \overline{A}_j^{x_j} = \prod_{i=1}^{m} \overline{B}_i^{\sum_{j=1}^{k} n_{ij} x_j}.$$

Since S is a basis of Cl, this would mean that

$$\lambda_i = \sum_{j=1}^{k} n_{ij} x_j + x_{k+i} b_i \text{ for } 1 \leq i \leq m \tag{5}$$

with $x_{k+i} \in \mathbf{Z}$ for $1 \leq i \leq m$. P must, therefore, only present the matrix $(u_{ij})_{m \times k}$ and the vector $(\lambda_i)n$ to V. Using the method described in Knuth [4] p.327 V can then figure out the unsolvability of (5) in polynomial time. So we have

Proposition 2.7 *$(G) \in co\text{-}NP$*

3 Some remarks

The methods used in this section can be used to prove Theorem 1.1 for any finite abelian group G if the problems analogous to (P) and (h) are known to be in NP and if both P and V know the same generating system for G of polynomial length.

It is certainly an interesting question whether parts of Theorem 1.1 can be proved without assuming the GRH.

References

[1] J. Buchmann and H.C. Williams, *On the existence of a short proof for the class number of a real quadratic number field*, Proceedings of NATO-ASI on Number Theory and applications, Banff (1988) to appear.

[2] E. Bach.

[3] K.S. McCurley, *Cryptographic key distribution and computation in class groups* preprint, 1988.

[4] D. E. Knuth, *The art of computer programming, vol. 2: seminumerical algorithms*, Addison-Wesley, Reading, Ma. 1981.