MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 207
JULY 1994, PAGES 377-387

RECOGNIZING UNITS IN NUMBER FIELDS

GUOQIANG GE

ABSTRACT. We present a deterministic polynomial-time algorithm that decides whether a power product $\prod_{i=1}^{k} \gamma_i^{n_i}$ is a unit in the ring of integers of K, where K is a number field, γ_i are nonzero elements of K and n_i are rational integers. The main algorithm is based on the factor refinement method for ideals, which might be of independent interest.

1. INTRODUCTION

A number field K is a finite field extension of the field $\mathbf{Q}$ of rational numbers ([3, 5, 8, 12]). Denote by $\mathcal{O}$ the ring of integers of K and by $\mathcal{O}^*$ the unit group of $\mathcal{O}$. The main result of the present paper is as follows.

Theorem 1.1. *There exists a polynomial-time algorithm that, given a number field K, nonzero elements $\gamma_1, \dots, \gamma_k$ of K and rational integers $n_1, \dots, n_k$, decides whether the power product $\prod_{i=1}^{k} \gamma_i^{n_i}$ is in $\mathcal{O}^*$.*

The proof of Theorem 1.1 will be given in §6. Theorem 1.1 answers a question suggested by H. W. Lenstra, Jr. in the the survey article *Algorithms in algebraic number theory* ([9, Problem 5.2]).

The problem of testing whether a power product is a unit arises from calculating the unit group $\mathcal{O}^*$ of a number field K. It is conjectured that, for an infinite sequence of real quadratic fields, the total number of digits of the coefficients of ϵ on a given basis of $\mathcal{O}$ over $\mathbf{Z}$ is as large as $\Delta^{1/2+o(1)}$, where ϵ is a fundamental unit and Δ is the discriminant of K. A different representation for ϵ is necessary since just writing down ϵ on a given basis of $\mathcal{O}$ over $\mathbf{Z}$ may be both time- and space-consuming. The algorithms that are actually used for finding units suggest that it is better to represent units in a compact form such as a power product $\prod_{i=1}^{k} \gamma_i^{n_i}$ of small nonzero elements $\gamma_1, \dots, \gamma_k$ of K with integer exponents $n_1, \dots, n_k$. Theorem 1.1 provides an efficient method of recognizing units if elements of number fields are represented as power products.

The algorithm on which the proof of our theorem is based depends on the use of basic ring theory. More specifically, Theorem 1.1 is obtained by the factor refinement method for ideals. If $K = \mathbf{Q}$, it is easy to see that Theorem 1.1 can be obtained from the results in [2]. The essential idea of the factor refinement

Received by the editor May 11, 1993.
1991 *Mathematics Subject Classification*. Primary 11Y16, 11Y40.
Key words and phrases. Number field, units, algorithm.

method for integers ([2]) is as follows: given $m = ab$, compute $d = \gcd(a, b)$ and write $m = (a/d) \cdot (d^2) \cdot (b/d)$, then continue this process until all factors are relatively prime. For the general number field K, we can efficiently calculate an order A in K. But we cannot assume that the computed order A is the ring of integers $\mathcal{O}$ of K, since finding the ring of integers of a given number field is not known to be computable in polynomial time (cf. [4, 6]). If a, b belong to the order A, then $\gcd(a, b)$ is not an element of A but is an ideal of A. The division of ideals of A cannot be carried out if the divisor is not an invertible ideal. On the other hand, if an ideal that is not invertible is found in the process of factor refinement, then an order B that is strictly larger than the order A can be found efficiently. This enlargement process will eventually stop after polynomially many steps.

The structure of this paper is as follows. In §2, we review some basic knowledge of algorithmic algebraic number theory. In §3, we recall some basic ring theory that will be used later. In §4, we give some estimates on the sizes of fractional ideals and overorders. In §5, we give the factor refinement method for ideals of an order in a number field. The proof of Theorem 1.1 will be given in §6.

Algorithms presented in this paper are not necessarily efficient from a practical point of view. Accordingly, I have not estimated the running time of the algorithms precisely.

2. Preliminaries

In this section, we review some basic knowledge of algorithmic algebraic number theory. For more details, we refer to [9]. All rings in this paper are supposed to be commutative with a unit element, subrings contain the same unit element.

A number field K of degree n is encoded as a ring. This amounts to giving a positive integer n, as well as a system of n^3 rational numbers a_{ijk} with the property that there is a $\mathbf{Q}$-vector space basis $\omega_1, \dots, \omega_n$ of K over $\mathbf{Q}$ such that $\omega_i\omega_j = \sum_{k=1}^{n} a_{ijk}\omega_k$ for all $i, j = 1, \dots, n$.

An order in K is a subring A of K of which the additive group is free of rank n. We will encode an order A in a number field K of degree n by specifying A as a ring, which amounts to giving a positive integer n and a system of n^3 integers c_{ijk} with the property that there is a free abelian group basis $e_1, \dots, e_n$ of A over $\mathbf{Z}$ such that $e_ie_j = \sum_{k=1}^{n} c_{ijk}e_k$ for all $i, j = 1, \dots, n$. It is easy to see that the same data encoding A also encode K. Given a number field K as above, one can construct an order A in K efficiently. The discriminant Δ_A of an order A with $\mathbf{Z}$-basis $e_1, \dots, e_n$ is defined to be the determinant of the matrix $(\mathrm{Tr}(e_ie_j))_{i,j}$, where $\mathrm{Tr}\colon K \to \mathbf{Q}$ is the trace map. The discriminant of any order is a nonzero integer.

Let A be an order in a number field K of degree n. By a fractional ideal of A we mean a finitely generated nonzero A-submodule of K. The additive group of a fractional ideal of A is isomorphic to $\mathbf{Z}^n$. A fractional ideal I of A is called an ideal of A if I is contained in A. An ideal I of an order A is encoded by an $n \times n$ matrix H_I over $\mathbf{Z}$ in Hermite Normal Form ([4, 7, 11]) such that the rows of the matrix H_I consist of a basis of I over $\mathbf{Z}$. Since the product of all diagonal entries in H_I is the index of I in A, it follows that all entries of the matrix H_I are bounded by the index $\langle A : I\rangle$. A fractional ideal J of A is given by means of a pair d, I, where d is the least positive integer such that $dJ \subseteq A$ and $I = dJ$ is an ideal of A of finite index. This representation is clearly unique. If I, J are fractional ideals of A, then we define $I : J = \{x \in A : xJ \subseteq I\}$; this is also a fractional ideal of A. There are polynomial-time algorithms that given an order A and fractional ideals I, J of A determine $I + J$, $I \cdot J$, $I \cap J$, and $I : J$ (cf. [4, §5]).

By an overorder of A we mean a fractional ideal of A that is a subring of K. It is clear that any overorder of A contains A. If I is a fractional ideal of A, then $I : I$ is an overorder of A. Every overorder B of A is an order in K, and it satisfies $\Delta_A = \Delta_B\langle B : A\rangle^2$. Overorders of A and their fractional ideals will be represented as fractional ideals of A.

Among all orders in K there is a unique maximal one denoted by $\mathscr{O}$, which is the integral closure of $\mathbf{Z}$ in K and is called the ring of integers of K. A subring A of $\mathscr{O}$ is an order in K if and only if it has finite additive index in $\mathscr{O}$. The discriminant of $\mathscr{O}$ is also called the discriminant of K over $\mathbf{Q}$, and denoted by Δ_K.

We will not give the precise meaning of the notions such as length of the encoding data, algorithm, running time, etc. For conventions concerning these notions we refer to [9, §2]. If O is an object (e.g., a number field, an order, a fractional ideal, etc.), then by size(O) we denote the length of the data encoding O. An algorithm is said to be a polynomial-time algorithm if its running time is polynomially bounded by the size of its input. In this case we also say that the algorithm runs in polynomial time.

3. Basic ring theory

In this section, we recall some basic ring theory that will be used later. For conventions, we refer to [1].

Let A be a domain with quotient field K, let I, J be fractional ideals of A. It is noted that in general $I(J : I)$ may not be equal to J. We recall that a fractional ideal I of A is invertible if there exists a fractional ideal J of A such that $I \cdot J = A$.

Proposition 3.1. *A fractional ideal I of A is invertible if and only if $I(A : I) = A$. In this case we have $I(J : I) = J$ and $J : I = J(A : I)$ for any fractional ideal J of A.*

Proof. The proof of the "if" part is obvious. For the "only if" part, let H be a fractional ideal of A such that $IH = A$. Let J be any fractional ideal of A; then $x \in J \Leftrightarrow xIH \subseteq J \Leftrightarrow xH \subseteq J : I \Leftrightarrow xIH \subseteq I(J : I) \Leftrightarrow x \in I(J : I)$. Hence $I(J : I) = J$, in particular $I(A : I) = A$. Furthermore, $J : I = (J : I) \cdot I(A : I) = J(A : I)$. □

Remark 3.2. It is easy to see from Proposition 3.1 that if I is invertible, then its inverse is unique and is equal to $A : I$. For any fractional ideal I of A, we define $I^0 = A$ and $I^n = (A : I)^{-n}$ if n is a negative integer.

Proposition 3.3. *Let A be a Noetherian one-dimensional domain, and let P be a nonzero prime ideal. Then $A : P$ strictly contains A.*

Proof. It is clear that $A : P$ contains A. Pick a nonzero element $x \in P$, and let H be the ideal generated by x. Since A is Noetherian, there exist prime ideals $P_1, \dots, P_n$ such that $H \subseteq P_i$ and $\prod_{i=1}^{n} P_i \subseteq H$. We may assume n is the smallest integer with these properties. Since $\prod_{i=1}^{n} P_i \subseteq H \subseteq P$ and P is prime, there exists some k, $1 \leq k \leq n$, such that $P_k \subseteq P$. In fact, we have $P_k = P$ since A is one-dimensional. Pick a $y \in \prod_{i \neq k} P_i \setminus H$; then $yP \subseteq \prod_{i=1}^{n} P_i \subseteq H = Ax$. Hence, $y/x \in A : P$ but $y/x \notin A$. This proves the proposition. □

Proposition 3.4. *Let A be a domain, and H, I, J fractional ideals of A; then $H : (I \cdot J) = (H : I) : J$.*

Proof. $x \in H : (I \cdot J) \Leftrightarrow xIJ \subseteq H \Leftrightarrow xJ \subseteq H : I \Leftrightarrow x \in (H : I) : J$. □

Proposition 3.5. *Let A be a Noetherian one-dimensional domain, and let I be a fractional ideal of A. Then I is invertible if and only if $(A : I) : (A : I) = A$.*

Proof. By Proposition 3.4, we have $(A : I) : (A : I) = A : (I \cdot (A : I))$. If I is invertible, then $I \cdot (A : I) = A$. Hence, $(A : I) : (A : I) = A : (I \cdot (A : I)) = A : A = A$. If I is not invertible, then $J = I(A : I)$ is a proper ideal of A. Let P be a maximal ideal of A containing J; then $(A : I) : (A : I) = A : (I \cdot (A : I)) = A : J \supseteq A : P$. Thus $(A : I) : (A : I) \neq A$, since $A : P$ strictly contains A by Proposition 3.3. This proves Proposition 3.5. □

Remark 3.6. The same result is proved in [4] for orders over principal ideal domains. For more details on this we refer to [4, §2].

Proposition 3.7 (Krull-Akizuki Theorem). *Let A be a Noetherian one-dimensional domain with field of fractions K, let L be a finite algebraic extension field of K, and B a ring with $A \subseteq B \subseteq L$; then B is a Noetherian domain of dimension at most one.*

Proof. See [10, p. 84]. □

Proposition 3.8. *Every order in a number field is a Noetherian one-dimensional domain.*

Proof. This is an immediate corollary of the Krull-Akizuki Theorem, since the dimension of every order is at least one. □

Proposition 3.9. *Let A be an order in a number field, and let I be a fractional ideal of A. Then I is invertible if and only if the overorder $(A : I) : (A : I)$ of A equals A.*

Proof. This immediately follows from Proposition 3.5 and Proposition 3.8. □

Proposition 3.10. *Let A be a domain, let $J_1, \dots, J_l$ be proper invertible ideals of A such that $J_j + J_{j'} = A$ for all $j \neq j'$, let $I = \prod_{1 \leq j \leq l} J_j^{e_j}$ where $e_j \in \mathbf{Z}$. Then $I \subseteq A$ if and only if $e_j \geq 0$ for all $1 \leq j \leq l$.*

Proof. The proof of the "if" part is obvious. For the "only if" part, it is enough to prove $e_1 \geq 0$. Let P be a maximal ideal containing J_1. Let H be any finitely generated fractional ideal of A; then $(H^{-1})_P = (A : H)_P = (A_P : H_P) = (H_P)^{-1}$ (cf. [1, Corollary 3.15]). So $(H^n)_P = (H_P)^n$ for any $n \in \mathbf{Z}$. Thus, $(J_j^{e_j})_P = (J_{jP})^{e_j} = A_P$ $(j \geq 2)$, since invertible ideals are finitely generated and

$J_j + P = A \ \ (j \geq 2)$. Therefore,

$$A_P \supseteq I_P = \left(\prod_{j=1}^{l} J_j^{e_j}\right)_P = \prod_{j=1}^{l}(J_j^{e_j})_P = (J_1^{e_1})_P = (J_{1P})^{e_1}.$$

Since J_{1P} is a proper invertible ideal of A_P, we have $e_1 \geq 0$.

This proves Proposition 3.10. □

Proposition 3.11. *Let A be a domain, let $J_1, \dots, J_l$ be proper invertible ideals of A such that $J_j + J_{j'} = A$ for all $j \neq j'$, let $I = \prod_{1 \leq j \leq l} J_j^{e_j}$, where $e_j \in \mathbf{Z}$. Then $I = A$ if and only if $e_j = 0$ for all $1 \leq j \leq l$.*

Proof. This follows from Proposition 3.10 by considering I and I^{-1}. □

Proposition 3.12. *Let A be an order in a number field K, and let $\mathcal{O}$ be the ring of integers of K. If I is a proper ideal of A, then $I\mathcal{O}$ is a proper ideal of $\mathcal{O}$.*

Proof. Suppose that $I\mathcal{O} = \mathcal{O}$. Let P be a maximal ideal of A containing I; then $P\mathcal{O} = \mathcal{O}$. Localize at P; we get $P_P\mathcal{O}_P = \mathcal{O}_P$. Since $\mathcal{O}_P$ is a finitely generated A_P-module and A_P is a local ring with maximal ideal P_P, we have $\mathcal{O}_P = 0$ by Nakayama's Lemma (cf. [1, p. 21]). This is a contradiction. □

4. Bounding sizes

Given a number field K as in §2, we can efficiently find an order A in K. We will represent overorders of A and their fractional ideals as fractional ideals of A. In the following, we will give some estimates on the sizes of fractional ideals and overorders of A.

Let I be a fractional ideal of A. Suppose d is the smallest positive integer such that $dI \subseteq A$. The index $\langle A : dI\rangle$ is the product of all main diagonal entries in the matrix representation H_{dI} of the ideal dI. Each entry in the matrix H_{dI} is bounded by a main diagonal entry. Hence, size(I) is polynomially equivalent to the length of the data encoding the integer d, the index $\langle A : dI\rangle$ and the order A.

Proposition 4.1. *Let A be an order in a number field, and let B be any overorder of A. Then* size(B) *is bounded by a polynomial function of* size(A). *Furthermore, if I is a fractional ideal of A, then* size(IB) *is bounded by a polynomial function of* size(I) *and* size(A).

Proof. Let B be an overorder of A, and let d be the smallest positive integer such that $dB \subseteq A$; then d divides $|\Delta_A|$ since $\langle B : A\rangle B \subseteq A$ and $\langle B : A\rangle$ divides $|\Delta_A|$. On the other hand, the index $\langle A : dB\rangle$ divides $\langle A : dA\rangle = d^n$, since $dA \subseteq dB \subseteq A$. So $\langle A : dB\rangle$ divides $|\Delta_A|^n$. Therefore, size(B) is bounded by a polynomial function of size(A). Furthermore, size(IB) is bounded by a polynomial function of size(I) and size(A), since size(IB) is polynomially bounded by size(I) and size(B). □

Proposition 4.2. *Let A be an order in a number field, and let I be a fractional ideal of A such that $I \subseteq \mathcal{O}$. Then $\log_2\langle \mathcal{O} : I\mathcal{O}\rangle$ is polynomially bounded by* size(I) *and* size(A).

Proof. Let d be the smallest positive integer such that $dI \subseteq A$; then the index $\langle \mathcal{O} : I\mathcal{O} \rangle \leq \langle \mathcal{O} : I \rangle \leq \langle \mathcal{O} : dI \rangle = \langle \mathcal{O} : A \rangle \langle A : dI \rangle \leq |\Delta_A| \langle A : dI \rangle$. So $\log_2 \langle \mathcal{O} : I\mathcal{O} \rangle$ is polynomially bounded by size(I) and size(A). □

Proposition 4.3. *Let A be an order in a number field, and let I be a fractional ideal of A such that $I \subseteq \mathcal{O}$. Let J be any fractional ideal of A such that $I \subseteq J \subseteq \mathcal{O}$. Then* size$(J)$ *is bounded by a polynomial function of* size(I) *and* size(A).

Proof. Let d be the smallest positive integer such that $d\mathcal{O} \subseteq A$, let e be the smallest positive integer such that $eJ \subseteq A$, and let f be the smallest positive integer such that $fI \subseteq A$. Since $dJ \subseteq d\mathcal{O} \subseteq A$, we have that e divides d. So $e \leq d \leq |\Delta_A|$. The index $\langle A : eJ \rangle \leq \langle A : dJ \rangle = \langle A : d\mathcal{O} \rangle \langle d\mathcal{O} : dJ \rangle \leq \langle A : dA \rangle \langle \mathcal{O} : J \rangle \leq d^n \langle \mathcal{O} : fI \rangle \leq d^n \langle \mathcal{O} : A \rangle \langle A : fI \rangle \leq |\Delta_A|^{n+1} \langle A : fI \rangle$. Therefore, size$(J)$ is bounded by a polynomial function of size(I) and size(A). □

Proposition 4.4. *Let A be an order in a number field, and let C be an overorder of A. Suppose that I_i $(1 \leq i \leq k)$ are ideals of C, J_j $(1 \leq j \leq l)$ are proper ideals of C and e_j $(1 \leq j \leq l)$ are positive integers such that*

$$\prod_{1 \leq i \leq k} I_i = \prod_{1 \leq j \leq l} J_j^{e_j}.$$

Then

$$l \leq \sum_{j=1}^{l} e_j \leq \sum_{i=1}^{k} \log_2 \langle \mathcal{O} : I_i\mathcal{O} \rangle.$$

In particular, both l and $\sum_{j=1}^{l} e_j$ are polynomially bounded by k, size(I_i) $(1 \leq i \leq k)$ *and* size(A).

Proof. Since

$$\prod_{1 \leq i \leq k} I_i = \prod_{1 \leq j \leq l} J_j^{e_j},$$

we have

$$\prod_{1 \leq i \leq k} I_i\mathcal{O} = \prod_{1 \leq j \leq l} (J_j\mathcal{O})^{e_j}.$$

Hence,

$$\prod_{1 \leq i \leq k} \langle \mathcal{O} : I_i\mathcal{O} \rangle = \prod_{1 \leq j \leq l} \langle \mathcal{O} : J_j\mathcal{O} \rangle^{e_j}.$$

By Proposition 3.12, $J_j\mathcal{O}$ is a proper ideal of $\mathcal{O}$ $(1 \leq j \leq l)$. Therefore,

$$2^{\sum_{j=1}^{l} e_j} \leq \prod_{1 \leq j \leq l} \langle \mathcal{O} : J_j\mathcal{O} \rangle^{e_j} = \prod_{1 \leq i \leq k} \langle \mathcal{O} : I_i\mathcal{O} \rangle.$$

That is,

$$\sum_{j=1}^{l} e_j \leq \sum_{i=1}^{k} \log_2 \langle \mathcal{O} : I_i\mathcal{O} \rangle.$$

By Proposition 4.2, $\log_2 \langle \mathcal{O} : I_i\mathcal{O} \rangle$ is polynomially bounded by size(I_i) $(1 \leq i \leq k)$. Therefore, both l and $\sum_{j=1}^{l} e_j$ are polynomially bounded by k, size(I_i) $(1 \leq i \leq k)$ and size(A). This proves the proposition. □

5. Factor refinement

In this section, we give the factor refinement algorithm for ideals of an order in a number field. For history and applications of the factor refinement technique, we refer to [2].

Algorithm 5.1. We describe an algorithm that, given an order A, an overorder B of A, and a fractional ideal I of B, determines an overorder C of A and an invertible fractional ideal J of C such that $B \subseteq C$ and $IC = J$.

The algorithm begins by putting $C = B$ and $J = I$, then does the following. It calculates the overorder $C' = (C : J) : (C : J)$ of A. If $C' = C$, the algorithm stops. Otherwise, it replaces C by C' and J by JC', then the algorithm iterates on the new C and J.

Proposition 5.2. *Given an order A, an overorder B of A, and a fractional ideal I of B, Algorithm* 5.1 *determines in polynomial time an overorder C of A and an invertible fractional ideal J of C such that $B \subseteq C$ and $IC = J$.*

Proof. Algorithm 5.1 iterates at most $\log_2 \langle \mathcal{O} : A \rangle$ steps, since the index $\langle C : A \rangle$ increases by a factor of at least 2 in each step. Hence the number of iterating steps is bounded by $\log_2 |\Delta_A|$. The running time of each step is bounded by a polynomial function of size(IC) and size(C), hence bounded by a polynomial function of size(I) and size(A) by Proposition 4.1. When the algorithm stops, we have $(C : J) : (C : J) = C$. Thus, J is invertible in C by Proposition 3.9. This completes the proof of Proposition 5.2. □

Algorithm 5.3. We describe an algorithm that, given an order A, an overorder B of A, and k proper ideals $I_1, \dots, I_k$ of B, determines an overorder C of A, proper invertible ideals $J_1, \dots, J_l$ of C, and positive integers e_j $(1 \le j \le l)$ such that $B \subseteq C$, $J_j + J_{j'} = C$ for all $j \neq j'$ and $\prod_{1 \le i \le k} I_i C = \prod_{1 \le j \le l} J_j^{e_j}$.

Step 1. The algorithm begins by putting $C_0 = B$. For each $i = 1, \dots, k$ we do the following. Applying Algorithm 5.1 to the ideal I_i and the overorder C_{i-1} of A, we find an overorder C_i of A and an invertible ideal $I_i C_i$.

Step 2. Put $C = C_k$, $J_i = I_i C_k$ and $e_i = 1$ $(i = 1, \dots, k)$. The algorithm works with a set S of all pairs (J_j, e_j) $(j = 1, \dots, l)$ such that $\prod_{1 \le i \le k} I_i C = \prod_{1 \le j \le l} J_j^{e_j}$, where l is the cardinality of the set S and J_j $(j = 1, \dots, l)$ are proper invertible ideals of C.

Step 3. First the algorithm searches for two members (J_j, e_j) and $(J_{j'}, e_{j'})$ of the set S such that $J_j + J_{j'} \neq C$. If these cannot be found, the algorithm stops. Suppose that (J_j, e_j) and $(J_{j'}, e_{j'})$ can be found; it calculates $H = J_j + J_{j'}$. Applying Algorithm 5.1 to C and its ideal H, we find an overorder $C' \supseteq C$ of A and an invertible ideal H' of C' with $H' = HC'$. Replace C by C', H by H', and all J_j by $J_j C'$, then remove pairs (J_j, e_j) and $(J_{j'}, e_{j'})$ from the set S and add the pairs $(J_j : H, e_j), (H, e_j + e_{j'}), (J_{j'} : H, e_{j'})$ to S except for those pairs containing C as their first entry. Next one iterates Step 3 on the new set S.

This completes the description of the algorithm.

Proposition 5.4. *Given an order A, an overorder B of A, and k proper ideals $I_1, \dots, I_k$ of B, Algorithm* 5.3 *determines in polynomial time an overorder C of A, proper invertible ideals $J_1, \dots, J_l$ of C and positive integers e_j $(1 \le j \le l)$*

such that $B \subseteq C$, $J_j + J_{j'} = C$ for all $j \neq j'$, and $\prod_{1\le i\le k} I_iC = \prod_{1\le j\le l} J_j^{e_j}$. Moreover, there are nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$ such that $I_iC = \prod_{1\le j\le l} J_j^{f_{ij}}$ for $i = 1, \ldots, k$.

Proof. When the algorithm terminates, we clearly have $B \subseteq C$, $J_j + J_{j'} = C$ for all $j \neq j'$. We also have $\prod_{1\le i\le k} I_iC = \prod_{1\le j\le l} J_j^{e_j}$ and $I_iC = \prod_{1\le j\le l} J_j^{f_{ij}}$ for some nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$, since they hold at the start of Step 3 and they are preserved after each iteration in Step 3.

Clearly, Step 1 and Step 2 can be done in polynomial time.

We refer to the process of removing (J_j, e_j) and $(J_{j'}, e_{j'})$ from S and adding pairs $(J_j : H, e_j)$, $(H, e_j + e_{j'})$, $(J_{j'} : H, e_{j'})$ to S as a *refinement step*. Let

$$m = \sum_{j=1}^{l}(e_j - 1).$$

We claim that m is increased by at least one after each refinement step. The contribution of (J_j, e_j) and $(J_{j'}, e_{j'})$ to m is $e_j + e_{j'} - 2$ before removing them. After adding $(J_j : H, e_j)$, $(H, e_j + e_{j'})$, $(J_{j'} : H, e_{j'})$ to S, the contribution of these pairs is:

$$\begin{cases} 2e_j + 2e_{j'} - 3 & \text{if } J_j : H \neq C \text{ and } J_{j'} : H \neq C; \\ 2e_j + e_{j'} - 2 & \text{if } J_j : H \neq C \text{ and } J_{j'} : H = C; \\ e_j + 2e_{j'} - 2 & \text{if } J_j : H = C \text{ and } J_{j'} : H \neq C; \\ e_j + e_{j'} - 1 & \text{if } J_j : H = C \text{ and } J_{j'} : H = C. \end{cases}$$

In all cases the contribution to m is greater than $e_j + e_{j'} - 2$.

Since each refinement step preserves

$$\prod_{1\le i\le k} I_iC = \prod_{1\le j\le l} J_j^{e_j},$$

we have by Proposition 4.4 that

$$m \le \sum_{j=1}^{l} e_j \le \sum_{i=1}^{k} \log_2\langle \mathscr{O} : I_i\mathscr{O}\rangle$$

which is polynomially bounded by k, size$(I_1), \ldots,$ size(I_k) and size(A). Therefore, the number of refinement steps is bounded by a polynomial function of k, size$(I_1), \ldots,$ size(I_k), and size(A).

All the fractional ideals (J_j and H, etc.) appearing in Step 3 have their sizes uniformly bounded by a polynomial function of size$(I_1), \ldots,$ size(I_k) and size(A) by Proposition 4.3, since each of them is contained in $\mathscr{O}$ and contains at least one I_i for some $i \in \{1, \ldots, k\}$. Since the cardinality l of the set S is polynomially bounded at any stage, each iteration in Step 3 runs in polynomial time.

Therefore, Algorithm 5.3 runs in polynomial time. □

Remark 5.5. The properness assumption on ideals $I_1, \ldots, I_k$ in Algorithm 5.3 and Proposition 5.4 is not necessary since we can apply Algorithm 5.3 to the ideals I_i that are proper in B and let $f_{ij} = 0$ for those I_i that are equal to B. We will drop this assumption in the Factor Refinement Algorithm below.

Algorithm 5.6 (Factor Refinement Algorithm). Given an order A of a number field K, an overorder B of A, and ideals $I_1, \dots, I_k$ of B. We describe an algorithm that determines an overorder C of A, proper invertible ideals $J_1, \dots, J_l$ of C, and nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$ such that $B \subseteq C$, $J_j + J_{j'} = C$ for all $j \ne j'$, and $I_iC = \prod_{1 \le j \le l} J_j^{f_{ij}}$ for $i = 1, \dots, k$.

Applying Algorithm 5.3 to order A, overorder B, and proper ideals $I_1, \dots,$ I_k of B, we find an overorder C of A and proper invertible ideals $J_1, \dots, J_l$ of C and positive integers $e_1, \dots, e_l$ such that $B \subseteq C$, $J_j + J_{j'} = C$ for all $j \ne j'$ and $\prod_{1 \le i \le k} I_iC = \prod_{1 \le j \le l} J_j^{e_j}$. Moreover, there are nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$ such that $I_iC = \prod_{1 \le j \le l} J_j^{f_{ij}}$ for $i = 1, \dots, k$.

For each $i = 1, \dots, k$, put $H_i = I_iC$, then do the following: For each $j = 1, \dots, l$, let $f_{ij} = 0$, if $H_i \subseteq J_j$, then replace H_i by $H_i : J_j$ and increase f_{ij} by 1 and continue the division process. Otherwise advance to the next j.

Proposition 5.7. *Given an order A, an overorder B of A, and ideals $I_1, \dots, I_k$ of B, Algorithm* 5.6 *determines in polynomial time an overorder C of A, proper invertible ideals $J_1, \dots, J_l$ of C, and nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$ such that $B \subseteq C$, $J_j + J_{j'} = C$ for all $j \ne j'$, and $I_iC = \prod_{1 \le j \le l} J_j^{f_{ij}}$ for $i = 1, \dots, k$.*

Proof. The number of division steps is

$$\sum_{i=1}^{k} \sum_{j=1}^{l} f_{ij} = \sum_{j=1}^{l} e_j ,$$

which is polynomially bounded. By Proposition 4.3, all the fractional ideals (J_j and H_i, etc.) appearing in the division process have their sizes uniformly bounded by a polynomial function of size$(I_1), \dots,$ size(I_k) and size(A), since each of them is contained in $\mathscr{O}$ and contains at least one I_i for some $i \in \{1, \dots, k\}$. So the running time of each division step is polynomially bounded. Therefore, Algorithm 5.6 runs in polynomial time.

This proves the proposition. □

6. Proof of Theorem 1.1

We prove Theorem 1.1 in this section.

Proposition 6.1. *There is a polynomial-time algorithm that, given an order A and a nonzero element $\gamma \in A$, determines the ideal I of A generated by γ.*

Proof. We first describe the algorithm. Let $\{e_i\}_{1 \le i \le n}$ be a **Z**-basis of A such that $e_ie_j = \sum_{k=1}^n c_{ijk}e_k$, where c_{ijk} $(1 \le i, j, k \le n)$ are the data encoding the order A (cf. §2). Let $\gamma = \sum_{i=1}^n r_ie_i$, where $r_i \in \mathbf{Z}$ for $i = 1, \dots, n$. Calculate a matrix $M = (m_{ij})$ such that $\gamma e_i = \sum_{j=1}^n m_{ij}e_j$ for $i = 1, \dots, n$, where $m_{kl} = \sum_{i=1}^n r_ic_{ikl}$ for $k, l = 1, \dots, n$. Find the Hermite Normal Form $H = (h_{ij})$ (cf. [4, 7, 11]) of the matrix M; then H is the unique matrix representation of the ideal I generated by γ.

Let $U = (u_{ij})$ be the unique $n \times n$ unimodular matrix such that $H = UM$. Let $\eta_i = \sum_{j=1}^n u_{ij}(\gamma e_j)$ for $i = 1, \dots, n$; then $\eta_i = \sum_{j=1}^n h_{ij}e_j$ for $i =$

$1, \ldots, n$. Since $\{\gamma e_i\}_{1\le i\le n}$ is a **Z**-basis of I and U is unimodular, $\{\eta_i\}_{1\le i\le n}$ is also a **Z**-basis of I. Therefore, H is the unique matrix representation of the ideal I, since the matrix H is in Hermite Normal Form. It is clear that the algorithm runs in polynomial time. This proves the proposition. □

Proposition 6.2. *There is a polynomial-time algorithm that, given an order A and nonzero elements $\gamma_1, \ldots, \gamma_k \in A$, determines an overorder C of A, proper invertible ideals $J_1, \ldots, J_l$ of C and nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$ such that $J_j + J_{j'} = C$ for all $j \ne j'$ and $\gamma_i C = \prod_{1\le j\le l} J_j^{f_{ij}}$ for $i = 1, \ldots, k$.*

Proof. Compute ideals $I_i = \gamma_i A$ by applying the algorithm in Proposition 6.1 to each $\gamma_i \in A$ $(i = 1, \ldots, k)$. Applying the Factor Refinement Algorithm (Algorithm 5.6) to the ideals I_i, we find an overorder C of A, proper invertible ideals $J_1, \ldots, J_l$ of C, and nonnegative integers f_{ij} $(1 \le i \le k, 1 \le j \le l)$ such that $J_j + J_{j'} = C$ for all $j \ne j'$ and $\gamma_i C = I_i C = \prod_{1\le j\le l} J_j^{f_{ij}}$ for $i = 1, \ldots, k$.

Apparently the algorithm runs in polynomial time since both the algorithm in Proposition 6.1 and the Factor Refinement Algorithm run in polynomial time. □

Proposition 6.3. *Let A be an order in a number field, and let $\gamma_1, \ldots, \gamma_k$ be nonzero elements in A. Let C be an overorder of A, let $J_1, \ldots, J_l$ be proper invertible ideals of C, and let f_{ij} $(1 \le i \le k, 1 \le j \le l)$ be nonnegative integers such that $J_j + J_{j'} = C$ for all $j \ne j'$ and $\gamma_i C = \prod_{1\le j\le l} J_j^{f_{ij}}$ for $i = 1, \ldots, k$. Let $n_1, \ldots, n_k$ be integers; then $\epsilon = \prod_{i=1}^k \gamma_i^{n_i} \in \mathcal{O}^*$ if and only if $\sum_{i=1}^k f_{ij} n_i = 0$ for $j = 1, \ldots, l$, and $\epsilon = \prod_{i=1}^k \gamma_i^{n_i} \in \mathcal{O}$ if and only if $\sum_{i=1}^k f_{ij} n_i \ge 0$ for $j = 1, \ldots, l$.*

Proof. Since

$$\epsilon C = \prod_{i=1}^k (\gamma_i C)^{n_i} = \prod_{i=1}^k \left(\prod_{j=1}^l J_j^{f_{ij}}\right)^{n_i} = \prod_{j=1}^l J_j^{\sum_i f_{ij} n_i},$$

we have

$$\epsilon\mathcal{O} = \prod_{j=1}^l (J_j \mathcal{O})^{\sum_i f_{ij} n_i}.$$

By Proposition 3.12, $J_j\mathcal{O}$ is a proper ideal of $\mathcal{O}$ for $j = 1, \ldots, l$. We also have $J_j\mathcal{O} + J_{j'}\mathcal{O} = \mathcal{O}$ for all $j \ne j'$, since $J_j + J_{j'} = C$. Hence, $\epsilon\mathcal{O} = \mathcal{O}$ if and only if $\sum_{i=1}^k f_{ij} n_i = 0$ for $j = 1, \ldots, l$ by Proposition 3.11, and $\epsilon\mathcal{O} \subseteq \mathcal{O}$ if and only if $\sum_{i=1}^k f_{ij} n_i \ge 0$ for $j = 1, \ldots, l$ by Proposition 3.10.

This proves the proposition. □

It is not difficult to see that Theorem 1.1 is equivalent to the following theorem up to a polynomial-time transformation. Therefore, it is enough to prove:

Theorem 6.4. *There is a polynomial-time algorithm that, given an order A, nonzero elements $\gamma_1, \ldots, \gamma_k \in A$ and integers $n_1, \ldots, n_k \in$ **Z**, decides whether $\epsilon = \prod_{i=1}^k \gamma_i^{n_i}$ is a unit, i.e., belongs to $\mathcal{O}^*$.*

Proof. Applying the algorithm in Proposition 6.2 to order A and $\gamma_1, \dots, \gamma_k \in A$, we find nonnegative integers f_{ij} $(i = 1, \dots, k, j = 1, \dots, l)$ with properties stated in Proposition 6.2.

Compute $\sum_{i=1}^{k} f_{ij} n_i$ for each $j = 1, \dots, l$. By Proposition 6.3, if all of them are zero, then ϵ is a unit, otherwise ϵ is not a unit.

Clearly this can be done in polynomial time. This completes the proof. □

ACKNOWLEDGMENTS

This paper represents part of the author's thesis. The author would like to thank his advisor, Hendrik Lenstra, for his thoughtful guidance and encouragement.

BIBLIOGRAPHY

1. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.
2. E. Bach, J. Driscoll, and J. O. Shallit, *Factor refinement*, J. Algorithms **15** (1993), 199–222.
3. Z. Borevich and I. Shafarevich, *Number theory*, Pure and Appl. Math., vol. 20, Academic Press, New York, 1966.
4. J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, in preparation.
5. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London, 1967.
6. A. L. Chistov, *The complexity of constructing the ring of integers of a global field*, Soviet Math. Dokl. **39** (1989), 597–600.
7. J. L. Hafner and K. S. McCurley, *Asymptotically fast triangularization of matrices over rings*, SIAM J. Comput. **20** (1991), 1068–1083.
8. S. Lang, *Algebraic number theory*, Graduate Texts in Math., vol. 110, Springer-Verlag, New York, 1986.
9. H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), 211–244.
10. H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Math., vol. 8, Cambridge Univ. Press, New York, 1986.
11. A. Schrijver, *Theory of linear and integer programming*, Wiley, Chichester, NY, 1986.
12. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720

Current address: Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

E-mail address: `magge@uxmail.ust.hk`