Séminaire de Théorie des Nombres
Année 1981-1982 - exposé n° 35

35-01
21 mai 1982

REDUCED BASES FOR LATTICES AND FACTORIZATION OF POLYNOMIALS

by

H. W. LENSTRA, Jr.

-:-:-:-

1. - Reduced bases for lattices

Let n be a positive integer, and $b_1, b_2, \dots, b_n$ linearly independent in a real vector space. We call $L = \sum_{i=1}^{n} \mathbb{Z} b_i$ a lattice of rank n with basis $b_1, b_2, \dots, b_n$, and its determinant is defined by $d(L) = \det((b_i, b_j))_{1 \le i, j \le n}^{\frac{1}{2}}$; this is independent of the choice of the basis of L. Hadamard's inequality asserts that

$$d(L) \le \prod_{i=1}^{n} |b_i| ,$$

the equality sign holding if and only if the b_i are pairwise orthogonal. It is a classical theorem that any lattice of rank n has a basis $b_1, b_2, \dots, b_n$ that is nearly orthogonal in the sense that

$$\prod_{i=1}^{n} |b_i| \le c_n \, d(L) ,$$

for a constant c_n only depending on n. It has recently been shown by Lovász that there exists a fast ("polynomial-time") algorithm to find such a basis with

$c_n = 2^{n(n-1)/4}$, see [3L, sec. 1]. We call such a basis reduced. If $b_1, b_2, \ldots, b_n$ is a reduced basis, then

$$\min\{|b_i| : 1 \leq i \leq n\} \leq c_n \min\{|x| : x \in L, x \neq 0\} .$$

Therefore Lovász's algorithm can be used to find small elements in a lattice, and this leads, in section 2, to an efficient factoring algorithm for polynomials. There are other applications in simultaneous diophantine approximation, generalized continued fractions, integer programming, and linear programming.

2. - Factoring polynomials

Let f be a polynomial in one variable with integer coefficients. Assume for simplicity that the leading coefficient of f equals 1. Denote by m the degree of f. We wish to factor f into irreducible factors in $\mathbb{Z}[X]$. One way to proceed is to factor f into irreducible linear and quadratic factors in $\mathbb{R}[X]$ to a certain accuracy, using methods from numerical analysis. Searching among all subproducts for polynomials with integer coefficients we can then find the desired factorization in $\mathbb{Z}[X]$. This algorithm is not a polynomial-time algorithm, because of the large number of subproducts to be tried.

A faster method is as follows. Fix one irreducible factor h_o of f in $\mathbb{R}[X]$, and look for the unique irreducible factor h of f in $\mathbb{Z}[X]$ divisible by h_o. Suppose for example that h_o is linear : $h_o = X - a$, where a is a real zero of f. Then $h(a) = 0$. From the numerical analysis we will only get an approximation $\hat{a}$ of a ; so we have to look for a factor h of f for which $h(\hat{a})$ is very small. Since we know an upper bound for the coefficients of h we can view h as a "small" element of the lattice of rank $m+1$ defined by

$$\{(g, g(\hat{a})) : g \in \mathbb{Z}[X], \deg(g) \leq m\} \subset \mathbb{Z}^{m+1} \times \mathbb{R} .$$

We can now find h by means of Lovász's algorithm.

It is likely that the above procedure, when all details are filled in, leads to a polynomial-time algorithm to factor f in $\mathbb{Z}[X]$. In [3 L] the field of real numbers is replaced by the field $\mathbb{Q}_p$ of p-adic numbers, for a suitable small prime number p. The role of the numerical analysis is then played by a combination of Berlekamp's factoring algorithm over finite fields and Hensel's lemma.

It has been shown in [3 L] that in this way one does obtain a polynomial-time algorithm to factor primitive polynomials with integer coefficients in one variable. There are generalizations to polynomials in several variables and to polynomials over algebraic number fields.

-:-:-:-

REFERENCE

[3 L] A.K. LENSTRA, H. W. LENSTRA, Jr., L. LOVÁSZ, Factoring polynomials with rational coefficients, to appear, Preliminary version : Report IW 195/82, Mathematisch Centrum, Amsterdam 1982.

(texte reçu le 7 juillet 1982)

-:-:-:-

H. W. LENSTRA, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB AMSTERDAM