stichting
mathematisch
centrum

MC

AFDELING INFORMATICA
(DEPARTMENT OF COMPUTER SCIENCE)

IW 230/83 JUNI

A.K. LENSTRA

FACTORING MULTIVARIATE INTEGRAL POLYNOMIALS, II

Preprint

kruislaan 413 1098 SJ amsterdam

Printed at the Mathematical Centre, Kruislaan 413, Amsterdam, The Netherlands.

The Mathematical Centre, founded 11 February 1946, is a non-profit institution for the promotion of pure and applied mathematics and computer science. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

1980 Mathematics subject classification: 12A20, 68C25

1982 CR. Categories: F.2.1, I.1.2

Factoring multivariate integral polynomials, II *)

by

A.K. Lenstra

ABSTRACT

We show that the problem of factoring multivariate integral polynomials can be reduced in polynomial-time to the univariate case. Our reduction makes use of lattice techniques as introduced in [3].

KEY WORDS & PHRASES: *polynomial algorithm, polynomial factorization*

---

*) This report will be submitted for publication elsewhere.

1. Introduction.

In [5] we presented a polynomial-time algorithm to factor polynomials in $\mathbb{Z}[X,Y]$, and we pointed out how to generalize the algorithm to $\mathbb{Z}[X_1, X_2, \ldots, X_t]$ for $t \geq 3$. A nice feature of this algorithm is that it doesn't depend on the polynomial-time algorithm to factor in $\mathbb{Z}[X]$ (cf. [3]). Instead of working out the details of this direct approach for $t \geq 3$ (this will be done for $\mathbb{Q}(\alpha)[X_1, X_2, \ldots, X_t]$ in a forthcoming paper [6]), we here simplify the method from [5] somewhat, which results in a polynomial-time reduction from factoring in $\mathbb{Z}[X_1, X_2, \ldots, X_t]$ to factoring in $\mathbb{Z}[X]$. This reduction is similar to the reduction from $\mathbb{F}_q[X_1, X_2, \ldots, X_t]$ to $\mathbb{F}_q[X,Y]$ that was given in [4].

An outline of our reduction is as follows. First we evaluate the polynomial $f \in \mathbb{Z}[X_1, X_2, \ldots, X_t]$ in a suitably chosen integer point $(X_2 = s_2, X_3 = s_3, \ldots, X_t = s_t)$, to obtain a polynomial $\bar{f} \in \mathbb{Z}[X_1]$. Using the algorithm from [3] we then compute an irreducible factor $\bar{h} \in \mathbb{Z}[X_1]$ of $\bar{f}$. Next we construct an integral lattice containing the factor h_0 of f that corresponds to $\bar{h}$, and we prove that h_0 is the shortest vector in this lattice. As usual, this enables us to compute h_0 by means of the so-called *basis reduction algorithm* (cf. [3: Section 1]; in the sequel we will assume the reader to be familiar with this basis reduction algorithm and its properties).

2. Factoring multivariate integral polynomials.

Let $f \in \mathbb{Z}[X_1, X_2, \ldots, X_t]$ be the polynomial to be factored, with the number of variables $t \geq 2$. By $\delta_i f = n_i$ we denote the degree of f in X_i. We often use n instead of n_1. We put $N_i = \prod_{k=i}^{t}(n_i+1)$, and $N = N_1$. The *content* $\mathrm{cont}(f) \in \mathbb{Z}[X_2, X_3, \ldots, X_t]$ of f is defined as the greatest common divisor of the coefficients of f with respect to X_1; we say that f is *primitive* if $\mathrm{cont}(f) = 1$.

Without loss of generality we may assume that $2 \le n_i \le n_{i+1}$ for $1 \le i < t$, and that the gcd of the integer coefficients of f equals one.

We present an algorithm to factor f into its irreducible factors in $\mathbb{Z}[X_1, X_2, \ldots, X_t]$ that is polynomial-time in N and the size of the integer coefficients of f.

Let $s_2, s_3, \ldots, s_t \in \mathbb{Z}_{>0}$ be a (t-1)-tuple of integers. For $g \in \mathbb{Z}[X_1, X_2, \ldots, X_t]$ we denote by $\tilde{g}_j$ the polynomial g modulo$((X_2-s_2), (X_3-s_3), \ldots, (X_j-s_j)) \in \mathbb{Z}[X_1, X_{j+1}, X_{j+2}, \ldots, X_t]$; i.e. $\tilde{g}_j$ is g with s_i substituted for X_i for $i = 2, 3, \ldots, j$. Notice that $\tilde{g}_1 = g$, and that $\tilde{g}_j = \tilde{g}_{j-1}$modulo (X_j-s_j). We put $\tilde{g} = \tilde{g}_t$.

Suppose that an irreducible, primitive factor $\tilde{h} \in \mathbb{Z}[X_1]$ of $\tilde{f}$ is given such that

(2.1) $\tilde{h}^2$ doesn't divide $\tilde{f}$ in $\mathbb{Z}[X_1]$, and $\delta_1\tilde{h} > 0$.

This condition implies that there exists an irreducible factor $h_0 \in \mathbb{Z}[X_1, X_2, \ldots, X_t]$ of f such that $\tilde{h}$ divides $\tilde{h}_0$ in $\mathbb{Z}[X_1]$, and that this polynomial h_0 is unique up to sign.

(2.2) Let m be an integer with $\delta_1\tilde{h} \le m < n$. We define L as the collection of polynomials g in $\mathbb{Z}[X_1, X_2, \ldots, X_t]$ such that

(i) $\delta_1 g \le m$, and $\delta_i g \le n_i$ for $2 \le i \le t$,

(ii) $\tilde{h}$ divides $\tilde{g}$ in $\mathbb{Z}[X_1]$.

This is a subset of the $(m+1)N_2$-dimensional real vector space $\mathbb{R} + \mathbb{R}X_t + \ldots +$

$\mathbb{R}X_1^m X_2^{n_2} \dots X_t^{n_t}$. We put $M = (m+1)N_2$. This vector space can be identified with $\mathbb{R}^M$ by identifying the polynomial $\Sigma_{i=0}^{m} \Sigma_{j=0}^{n_2} \dots \Sigma_{k=0}^{n_t} a_{ij\dots k} X_1^i X_2^j \dots X_t^k \in \mathbb{R}[X_1, X_2, \dots, X_t]$ with the M-dimensional vector $(a_{00\dots 0}, a_{00\dots 1}, \dots, a_{mn_2\dots n_t})$. The collection L is a lattice in $\mathbb{Z}^M$ of rank $M - \delta_1 \tilde{h}$, and a basis for L is given by

$$\{X_1^i \Pi_{j=2}^t (X_j - s_j)^{i_j}: \ 0 \le i \le m, \ 0 \le i_j \le n_j \ \text{ for } \ 2 \le j \le t, \ \text{ and } \ (i_2, i_3, \dots, i_t) \ne (0, 0, \dots, 0)\}$$

$$\cup \ \{\tilde{h} X_1^{i-\delta_1 \tilde{h}}: \ \delta_1 \tilde{h} \le i \le m\}$$

(cf. [4: (3.2)]).

We define the *length* $|g|$ of the vector associated with the polynomial g as the ordinary Euclidean length of this vector. The *height* g_{max} is defined as the largest absolute value of any of the integer coefficients of g.

<u>(2.3) Proposition</u>. *Suppose that* b *is a non-zero element of* L *such that*

(2.4) $$s_j \ge f_{max}^m b_{max}^n (n+m)! \, (N_2 \Pi_{i=2}^{j-1} s_i^{n_i})^{n+m}$$

for $2 \le j \le t$. *Then* $\gcd(f,b) \ne 1$ *in* $\mathbb{Z}[X_1, X_2, \dots, X_t]$.*)

<u>Proof</u>. Suppose on the contrary that $\gcd(f,b) = 1$. This implies that the resultant $R = R(f,b) \in \mathbb{Z}[X_2, X_3, \dots, X_t]$ of f and b (with respect to the variable X_1) is unequal to zero.

We derive an upper bound for $(\tilde{R}_j)_{max}$. Because $\tilde{R}_j$ is the resultant of $\tilde{f}_j$ and $\tilde{b}_j$ we have

(2.5) $$(\tilde{R}_j)_{max} \le (\tilde{f}_j)_{max}^m (\tilde{b}_j)_{max}^n (n+m)! \, N_{j+1}^{n+m-2}$$

*) Here, and in the sequel, f_{max}^m denotes $(f_{max})^m$.

as is easily verified. Because $\tilde{b}_j = \tilde{b}_{j-1} \text{modulo}(X_j - s_j)$, we have

$$(\tilde{b}_j)_{max} \le (\tilde{b}_{j-1})_{max}(n_j+1)\, s_j^{n_j},$$

so that

$$(2.6) \qquad (\tilde{b}_j)_{max} \le b_{max}\Pi_{i=2}^{j}(n_i+1)s_i^{n_i},$$

and similarly

$$(2.7) \qquad (\tilde{f}_j)_{max} \le f_{max}\Pi_{i=2}^{j}(n_i+1)s_i^{n_i}.$$

Combining (2.5), (2.6), and (2.7), we obtain

$$(2.8) \qquad (\tilde{R}_j)_{max} < f_{max}^m\, b_{max}^n\, (n+m)!\, (N_2\, \Pi_{i=2}^{j}\, s_i^{n_i})^{n+m},$$

for $1 \le j < t$.

Because $\tilde{h}$ divides both $\tilde{f}$ and $\tilde{b}$ ((2.2)(ii)), we have that $\tilde{R} = 0$. But also $R \ne 0$, so there must be an index j with $2 \le j \le t$ such that s_j is a zero of $\tilde{R}_{j-1}$. This implies that

$$|s_j| \le (\tilde{R}_{j-1})_{max}$$

for some j with $2 \le j \le t$, which yields, combined with (2.4) and (2.8), a contradiction. We conclude that $\gcd(f,b) \ne 1$. □

<u>(2.9) Proposition</u>. *Let* $b_1, b_2, \ldots, b_M$ *be a reduced basis for* L *(cf.* [3: Section 1]*), where* L *and* M *are defined as in* (2.2). *Suppose that*

$$(2.10) \qquad s_j \ge f_{max}^m((M\,2^{M-1})^{\frac{1}{2}} f_{max})^n\, (n+m)!\left(e^{\Sigma_{i=1}^{t} n_i}\, N_2\, \Pi_{i=2}^{j-1}\, s_i^{n_i}\right)^{n+m}$$

for $2 \le j \le t$, *and that* f *doesn't contain multiple factors. Then*

(2.11) $$(b_1)_{max} \le (M\,2^{M-1})^{\frac{1}{2}} e^{\sum_{i=1}^{t} n_i} f_{max}$$

and h_0 *divides* b_1, *if and only if* $\delta_1 h_0 \le m$.

Proof. If h_0 divides b_1, then $\delta_1 h_0 \le \delta_1 b_1 \le m$; this proves the "only if"-part.

We prove the "if"-part. Suppose that $\delta_1 h_0 \le m$. The polynomial h_0 is a divisor of f, so that

$$(h_0)_{max} \le e^{\sum_{i=1}^{t} n_i} f_{max}$$

according to [2]. With $\delta_1 h_0 \le m$ and $\delta_i h_i \le n_i$ for $2 \le i \le t$ we get

$$|h_0| \le M^{\frac{1}{2}} e^{\sum_{i=1}^{t} n_i} f_{max},$$

so that [3: (1.11)] combined with $h_0 \in L$ (this follows from $\delta_1 h_0 \le m$) yields

$$|b_1| \le (M\,2^{M-1})^{\frac{1}{2}} e^{\sum_{i=1}^{t} n_i} f_{max}.$$

This proves (2.11) because $(b_1)_{max} \le |b_1|$. With (2.10) and (2.3) we now have that $\gcd(f,b_1) \ne 1$. Suppose that h_0 doesn't divide $r = \gcd(f,b_1)$. Then $\tilde{h}$ divides $\tilde{f}/\tilde{r}$, so that, with

$$(f/r)_{max} \le e^{\sum_{i=1}^{t} n_i} f_{max},$$

and (2.10), (2.11), and (2.3), we get that $\gcd(f/r,b_1) \ne 1$. This is a contradiction with $r = \gcd(f,b_1)$, because f doesn't contain multiple factors. □

(2.12) Suppose that f doesn't contain multiple factors and that f is primitive. Let $s_2, s_3, \ldots, s_t$ and $\tilde{h}$ be chosen such that (2.10) with m replaced by $n-1$ and (2.1) are satisfied. The divisor h_0 of f can be determined in the following way.

For the values $m = \delta_1\tilde{h}, \delta_1\tilde{h}+1, \ldots, n-1$ in succession we apply the basis reduction algorithm (cf. [3: Section 1]) to the lattice L as defined in (2.2). We stop as soon as a vector b_1 is found satisfying (2.11). It is not difficult to see that the first vector b_1 satisfying (2.11) that we encounter, also satisfies $b_1 = \pm h_0$ (here we apply [3: (1.37)] and (2.9)). If no vector satisfying (2.11) is found, then $\delta_1 h_0 > n-1$, so that $h_0 = f$; this follows from (2.9).

(2.13) Proposition. *Assume that the conditions in* (2.12) *are satisfied. The polynomial* h_0 *can be computed in* $O((\delta_1 h_0 N_2)^4 \log B)$ *arithmetic operations on integers having binary length* $O(N \log B)$, *where*

$$\log B = O(\log f_{max} + n + \log N_2 + \Sigma_{i=2}^{t} n_i \log s_i).$$

Proof. Combining

$$|\tilde{h}| \leq \binom{2n}{n}^{\frac{1}{2}} |\tilde{f}|$$

(cf. [7]) and (2.7), we find that

$$|\tilde{h}| \leq f_{max}((n+1)\binom{2n}{n})^{\frac{1}{2}} \Pi_{i=2}^{t} (n_i+1) s_i^{n_i}.$$

The proof follows now immediately from (2.2), [3: (1.26)] and [3: (1.37)]. □

(2.14) We describe an algorithm to compute the irreducible factors of f in $\mathbb{Z}[X_1, X_2, \ldots, X_t]$. Assume that f is primitive.

First we compute the resultant $R = R(f,f') \in \mathbb{Z}[X_2, X_3, \ldots, X_t]$ of f and its derivative f' with respect to X_1, using the subresultant algorithm from [1]. We may assume that $R \neq 0$, i.e. f doesn't contain multiple factors. (In the case that $R = 0$, the greatest common divisor g of f and f' is also computed by the subresultant algorithm, and the factoring algorithm can be applied to f/g.)

Next we determine $s_2, s_3, \ldots, s_t \in \mathbb{Z}$ such that $\tilde{R} \neq 0$ and such that (2.10) is satisfied with m replaced by $n-1$:

$$(2.15) \qquad s_j \geq (n\, N_2\, 2^{nN_2-1})^{n/2}\, (2n-1)!\, (e^{\sum_{i=1}^{t} n_i} f_{max}\, N_2 \prod_{i=2}^{j-1} s_i^{n_i})^{2n-1}$$

for $2 \leq j \leq t$. It follows from the reasoning in the proof of (2.3) that if we take $s_j \in \mathbb{Z}_{>0}$ minimal such that (2.15) is satisfied, then $\tilde{R} \neq 0$.

By means of the algorithm from [3] we compute the irreducible and primitive factors of $\tilde{f}$ of degree > 0 in X_1. The condition $\tilde{R} \neq 0$ implies that (2.1) holds for every irreducible factor $\tilde{h}$ of $\tilde{f}$ thus found.

Finally, the factorization of f is determined by repeated application of the algorithm described in (2.12).

<u>(2.16) Theorem</u>. *Let* f *be a polynomial in* $\mathbb{Z}[X_1, X_2, \ldots, X_t]$ *with* $t \geq 2$, $\delta_i f = n_i$, *and* $2 \leq n = n_1 \leq n_2 \leq \ldots \leq n_t$. *The irreducible factorization of* f *can be found in* $O(n^{t-2}(N^6 + N^5 \log f_{max}))$ *arithmetic operations on integers having binary length* $O(n^{t-2}(N^3 + N^2 \log f_{max}))$, *where* $N = \prod_{i=1}^{t}(n_i+1)$.

<u>Remark</u>. Because $n^t = O(N)$, Theorem (2.16) implies that f can be factored in time polynomial in N and $\log f_{max}$.

<u>Proof of (2.16)</u>. First assume that f is primitive. The resultant R can be computed in $O(n^{3t-1} N_2^2)$ arithmetic operations on integers having binary length $O(n^2 \log(f_{max} N_2))$ (cf. [1]).

From the choice of s_j (cf. (2.15)) we derive

$$\log s_j = O(n^2 N_2 + n \log f_{max} + \Sigma_{i=2}^{j-1} n\, n_i \log s_i)$$

for $2 \leq j \leq t$, so that

$$\log s_j = O((n^2 N_2 + n \log f_{max}) \Pi_{i=2}^{j-1} (1+n\, n_i)).$$

This yields

(2.17) $$\Sigma_{i=2}^{t} n_i \log s_i = O(n^{t-2}(N^2 + N \log f_{max})),$$

which gives, combined with (2.7),

(2.18) $$\log \bar{f}_{max} = O(n^{t-2}(N^2 + N \log f_{max})).$$

The polynomial $\bar{f}$ can be factored in $O(n^6 + n^5 \log \bar{f}_{max})$ arithmetic operations on integers having binary length $O(n^3 + n^2 \log \bar{f}_{max})$, according to [3: (3.6)]. With (2.18) this becomes

$$O(n^{t+3}(N^2 + N \log f_{max}))$$

arithmetic operations on integers having binary length

$$O(n^{t}(N^2 + N \log f_{max})).$$

According to (2.13) and (2.17), repeated application of the algorithm described in (2.12) takes

$$O(n^{t-2}(N^6 + N^5 \log f_{max}))$$

arithmetic operations on integers having binary length

$$O(n^{t-2}(N^3 + N^2 \log f_{max})).$$

The cost of applying (2.12) therefore dominates the costs of the computation of R and the factorization of $\bar{f}$.

The same estimates are valid in the case that $R=0$. In this case we have that

$$(f/g)_{max} \le e^{\sum_{i=1}^{t} n_i} f_{max}$$

(cf. [2]), so that the same estimates as above are valid for the computation of the factorization of f/g.

Finally, we consider the case that the content of f is unequal to one. The computation of $\text{cont}(f)$ can be done in $O(n\, n_2^{3t-4} N_3^2)$ arithmetic operations on integers having binary length $O(n_2^2 \log(f_{max} N_3))$ (cf. [1]). Because $\delta_i f = \delta_i \text{cont}(f) + \delta_i (f/\text{cont}(f))$ for $2 \le i \le t$, the proof follows by repeated application of the above reasoning. □

(2.19) Remark. As mentioned in the introduction, a somewhat more complicated but similar approach leads to an algorithm that doesn't depend on the polynomial-time algorithm for factoring in $\mathbb{Z}[X]$. Instead, it can be seen as a direct generalization of the $\mathbb{Z}[X]$-algorithm. We won't give a detailed description of this alternative method here, we only indicate the main differences.

The divisor $\bar{h} \in \mathbb{Z}[X_1]$ of $\bar{f}$ is replaced by a divisor $(\bar{h} \bmod p^k) \in (\mathbb{Z}/p^k\mathbb{Z})[X_1]$ of $(\bar{f} \bmod p^k)$, for some suitably chosen prime power p^k. Condition (2.2)(ii) is therefore replaced by the condition that $(\bar{h} \bmod p^k)$ divides $(\bar{g} \bmod p^k)$ in $(\mathbb{Z}/p^k\mathbb{Z})[X_1]$. The lattice $L \subset \mathbb{Z}^M$ now has rank M, and a basis for L is given by

$$\{p^k X_1^i : \ 0 \le i < \delta_1 \bar{h}\}$$

$$\cup \{(\tilde{h} \bmod p^k) X_1^{i-\delta_1 \tilde{h}} : \delta_1 \tilde{h} \le i \le m\}$$

$$\cup \{X_1^i \prod_{j=2}^t (X_j - s_j)^{i_j} : 0 \le i \le m, \quad 0 \le i_j \le n_j \quad \text{for} \quad 2 \le j \le t, \quad \text{and}$$

$$(i_2, i_3, \ldots, i_t) \ne (0, 0, \ldots, 0)\}.$$

Again, it can be proven that, if $s_2, s_3, \ldots, s_t$ and p^k are sufficiently large, then the irreducible factor of f that corresponds to $(\tilde{h} \bmod p^k)$ is the shortest vector in L. This factor can therefore be found by means of the basis reduction algorithm, and the resulting algorithm appears to be polynomial-time. For $f \in \mathbb{Z}[X,Y]$ the details are given in [5], and for $f \in \mathbb{Q}(\alpha)[X_1, X_2, \ldots, X_t]$ in [6].

References.

1. W.S. Brown, The subresultant PRS algorithm. ACM Transactions on mathematical software 4 (1978), 237-249.
2. A.O. Gel'fond, Transcendental and algebraic numbers, Dover Publ., New York 1960.
3. A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), 515-534.
4. A.K. Lenstra, Factoring multivariate polynomials over finite fields, Report IW 221/83, Mathematisch Centrum, Amsterdam 1983 (also Proceedings 15th STOC).
5. A.K. Lenstra, Factoring multivariate integral polynomials, Report IW 229/83, Mathematisch Centrum, Amsterdam 1983 (also Proceedings 10th ICALP).

6. A.K. Lenstra, Factoring multivariate polynomials over algebraic number fields, to appear.

7. M. Mignotte, An inequality about factors of polynomials, Math. Comp. 28 (1974), 1153-1157.