

FACTORING MULTIVARIATE POLYNOMIALS OVER ALGEBRAIC NUMBER FIELDS*

ARJEN K. LENSTRA†

Abstract. We present an algorithm to factor multivariate polynomials over algebraic number fields that is polynomial-time in the degrees of the polynomial to be factored. The algorithm is an immediate generalization of the polynomial-time algorithm to factor univariate polynomials with rational coefficients.

Key words. polynomial factorization

AMS(MOS) subject classifications. 12A20, 68C25

1. Introduction. We show that the algorithm from [9] to factor univariate polynomials with rational coefficients can be generalized to multivariate polynomials with coefficients in an algebraic number field. As a result we get an algorithm that is polynomial-time in the degrees and the coefficient-size of the polynomial to be factored.

An outline of the algorithm is as follows. First the polynomial $f \in \mathbb{Q}(\alpha)[X_1, X_2, \dots, X_t]$ is evaluated in a suitably chosen integer point ($X_2 = s_2, X_3 = s_3, \dots, X_t = s_t$). Next, for some prime number p , a p -adic irreducible factor \tilde{h} of the resulting polynomial $\tilde{f} \in \mathbb{Q}(\alpha)[X_1]$ is determined up to a certain precision. We then show that the irreducible factor h_0 of f for which \tilde{h} is a p -adic factor of \tilde{h}_0 , belongs to a certain integral lattice, and that h_0 is relatively short in this lattice. This enables us to compute this factor h_0 by means of the so-called *basis reduction algorithm* (cf. [9, § 1]).

As [9] is easily available, we do not consider it to be necessary to recall the basis reduction algorithm here; we will assume the reader to be familiar with this algorithm and its properties.

Although the algorithm presented in this paper is polynomial-time, we do not think it is a useful method for practical purposes. Like the other generalizations of the algorithm from [9], which can be found in [10]–[13], the algorithm will be slow, because the basis reduction algorithm has to be applied to huge dimensional lattices with large entries. In practice, a combination of the methods from [8], [17] and [18] can be recommended (cf. [8]).

In [3] and [6] polynomial-time algorithms are given for similar multivariate polynomial factoring problems. These papers make use of a completely different approach. In [6] the multivariate factoring is reduced in polynomial time to univariate factoring and the latter problem is solved by the algorithm from [9]. A polynomial-time reduction to univariate factoring and multivariate factoring over finite fields is presented in [3].

All papers referred to above, and also the present paper, assumed the polynomials to be *densely* encoded. For algorithms which apply the more realistic *sparse* encoding we refer to [16].

2. Preliminaries. In this section we introduce some notation, and we derive an upper bound for the coefficients of factors of multivariate polynomials over algebraic number fields.

Let the algebraic number field $\mathbf{Q}(\alpha)$ be given as the field of rational numbers \mathbf{Q} extended by a root α of a prescribed *minimal polynomial* $F \in \mathbf{Z}[T]$ with leading coefficient equal to one, i.e., $\mathbf{Q}(\alpha) \approx \mathbf{Q}[T]/(F)$. Similarly, we define $\mathbf{Z}[\alpha] = \mathbf{Z}[T]/(F)$ as a ring of polynomials in α over \mathbf{Z} of degree less than I , where I denotes the degree δF of F .

Let $f \in \mathbf{Q}(\alpha)[X_1, X_2, \dots, X_t]$ 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 , for $1 \leq i \leq t$. We often use n instead of n_1 . We put $N_i = \prod_{k=i}^t (n_k + 1)$, and $N = N_1$. Let $lc_0(f) = f$. For $1 \leq i \leq t$ we define $lc_i(f) \in \mathbf{Q}(\alpha)[X_{i+1}, X_{i+2}, \dots, X_t]$ as the leading coefficient with respect to X_i of $lc_{i-1}(f)$, and we put $lc(f) = lc_t(f)$. Finally, we define the *content* $\text{cont}(f) \in \mathbf{Q}(\alpha)[X_2, X_3, \dots, X_t]$ of f as the greatest common divisor of the coefficients of f with respect to X_1 . Without loss of generality we may assume that $2 \leq n_i \leq n_{i+1}$ for $1 \leq i < t$, that f is *monic* (i.e. $lc(f) = 1$), and that $\delta_i \text{cont}(f) = 0$ for $2 \leq i \leq t$.

Let $d \in \mathbf{Z}_{>0}$ be such that $f \in (1/d)\mathbf{Z}[\alpha][X_1, X_2, \dots, X_t]$, and let $\text{discr}(F)$ denote the discriminant of F . It is well known (cf. [18]) that if we take $D = d|\text{discr}(F)|$, then all monic factors of f are in $(1/D)\mathbf{Z}[\alpha][X_1, X_2, \dots, X_t]$ (in fact it is sufficient to take $D = d \cdot s$, where s is the largest integer such that s^2 divides $\text{discr}(F)$, but this integer s might be too difficult to compute).

We now introduce some notation. Suppose that we are given a prime number p such that

$$(2.1) \quad p \text{ does not divide } D.$$

For $G = \sum_i a_i T^i \in \mathbf{Z}[T]$ we denote by G_l or $G \bmod p^l$ the polynomial $\sum_i (a_i \bmod p^l) T^i \in (\mathbf{Z}/p^l\mathbf{Z})[T]$, for any positive integer l . Suppose furthermore that we are given some positive integer k , and that p is chosen in such a way that a polynomial $H \in \mathbf{Z}[T]$ exists such that

$$(2.2) \quad H \text{ has leading coefficient equal to one,}$$

$$(2.3) \quad H_k \text{ divides } F_k \text{ in } (\mathbf{Z}/p^k\mathbf{Z})[T],$$

$$(2.4) \quad H_1 \text{ is irreducible in } (\mathbf{Z}/p\mathbf{Z})[T],$$

$$(2.5) \quad (H_1)^2 \text{ does not divide } F_1 \text{ in } (\mathbf{Z}/p\mathbf{Z})[T].$$

Clearly H_1 divides F_1 in $(\mathbf{Z}/p\mathbf{Z})[T]$, and $0 < \delta H \leq I$. In the sequel we will assume that conditions (2.1), (2.2), (2.3), (2.4) and (2.5) are satisfied.

By \mathbf{F}_q we denote the finite field containing $q = p^{\delta H}$ elements. From (2.4) we have $\mathbf{F}_q \approx (\mathbf{Z}/p\mathbf{Z})[T]/(H_1) \approx \{\sum_{i=0}^{\delta H-1} a_i \alpha^i : a_i \in \mathbf{Z}/p\mathbf{Z}\}$, where $\alpha_1 = T \bmod (H_1)$ is a zero of H_1 . Furthermore we put $W_k(\mathbf{F}_q) = (\mathbf{Z}/p^k\mathbf{Z})[T]/(H_k) \approx \{\sum_{i=0}^{\delta H-1} a_i \alpha_k^i : a_i \in \mathbf{Z}/p^k\mathbf{Z}\}$, where $\alpha_k = T \bmod (H_k)$ is a zero of H_k . Notice that $W_k(\mathbf{F}_q)$ is a ring containing q^k elements, and that $W_1(\mathbf{F}_q) \approx \mathbf{F}_q$. For $a \in \mathbf{Z}[\alpha]$ we denote by $a \bmod (p^l, H_l) \in W_l(\mathbf{F}_q)$ the result of the canonical mapping from $\mathbf{Z}[\alpha] = \mathbf{Z}[T]/(F)$ to $W_l(\mathbf{F}_q) = (\mathbf{Z}/p^l\mathbf{Z})[T]/(H_l)$ applied to a , for $l = 1, k$. For $\tilde{g} = \sum_i (a_i/D) X_i^i \in (1/D)\mathbf{Z}[\alpha][X_1]$ we denote by $\tilde{g} \bmod (p^l, H_l)$ the polynomial $\sum_i ((D^{-1} \bmod p^l) a_i) \bmod (p^l, H_l) X_i^i \in W_l(\mathbf{F}_q)[X_1]$ (notice that $D^{-1} \bmod p^l$ exists due to (2.1)).

We derive an upper bound for the height of a monic factor g of f . As usual, for $g = \sum_{i_1} \sum_{i_2} \dots \sum_{i_t} a_{i_1 i_2 \dots i_t} \alpha^{i_1} X_1^{i_1} X_2^{i_2} \dots X_t^{i_t} \in \mathbf{Q}(\alpha)[X_1, X_2, \dots, X_t]$, the *height* g_{\max} is defined as $\max |a_{i_1 i_2 \dots i_t}|$, and the *length* $|g|$ as $(\sum a_{i_1 i_2 \dots i_t}^2)^{1/2}$. Similarly, for a polynomial h with complex coefficients, we define its height h_{\max} as the maximum of the absolute values of its complex coefficients.

For any choice of $\alpha \in \{\alpha_1, \alpha_2, \dots, \alpha_t\}$, where $\alpha_1, \alpha_2, \dots, \alpha_t$ are the conjugates of α , we can regard g as a polynomial g_α with complex coefficients. We define $\|g\|$ as $\max_{1 \leq i \leq t} (g_{\alpha_i})_{c \max}$. From [4] we have

$$\|g\| \leq e^{\sum_{i=1}^t n_i} \|f\|.$$

In [10, § 4] we have shown that this leads to

$$(2.6) \quad g_{\max} \leq e^{\sum_{i=1}^t n_i} \|f\| I(I-1)^{(I-1)/2} |F|^{I-1} |\text{discr}(F)|^{-1/2}.$$

From [15] we know that the length $|F|$ of F is an upper bound for the absolute value of the conjugates of α , so that

$$\|f\| \leq f_{\max} \sum_{i=0}^{I-1} |F|^i,$$

which yields, combined with (2.6),

$$(2.7) \quad g_{\max} \leq e^{\sum_{i=1}^t n_i} f_{\max} I(I-1)^{(I-1)/2} |F|^{I-1} |\text{discr}(F)|^{-1/2} \sum_{i=0}^{I-1} |F|^i.$$

The upper bound for the height of monic factors of f , as given by the right-hand side of (2.7), will be denoted by B_f . Because $|\text{discr}(F)| \geq 1$, we find

$$(2.8) \quad \log B_f = O\left(\sum_{i=1}^t n_i + \log f_{\max} + I \log(I|F|)\right).$$

3. Factoring multivariate polynomials over algebraic number fields. We describe an algorithm to compute the irreducible factorization of f in $\mathbb{Q}(\alpha)[X_1, X_2, \dots, X_t]$.

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

Suppose that a polynomial $h \in \mathbb{Z}[\alpha][X_1]$ is given such that

$$(3.1) \quad \tilde{h} \text{ is monic,}$$

$$(3.2) \quad \tilde{h} \bmod (p^k, H_k) \text{ divides } \tilde{f} \bmod (p^k, H_k) \text{ in } W_k(\mathbb{F}_q)[X_1],$$

$$(3.3) \quad \tilde{h} \bmod (p, H_1) \text{ is irreducible in } \mathbb{F}_q[X_1],$$

$$(3.4) \quad (\tilde{h} \bmod (p, H_1))^2 \text{ does not divide } \tilde{f} \bmod (p, H_1) \text{ in } \mathbb{F}_q[X_1].$$

We put $l = \delta_1 \tilde{h}$, so $0 < l \leq n$. By $h_0 \in (1/D)\mathbb{Z}[\alpha][X_1, X_2, \dots, X_t]$ we denote the unique, monic, irreducible factor of f such that $\tilde{h} \bmod (p^k, H_k)$ divides $\tilde{h}_0 \bmod (p^k, H_k)$ in $W_k(\mathbb{F}_q)[X_1]$ (cf. (3.2), (3.3), (3.4)).

(3.5) Let $m = m_1, m_2, m_3, \dots, m_t$ be a t -tuple of integers satisfying $l \leq m < n$ and $0 \leq m_i \leq \delta_i l c_{i-1}(f)$ for $2 \leq i \leq t$, and let $M = 1 + I \sum_{i=1}^t m_i N_{i+1}$ (where of course $N_{t+1} = 1$). We define $L \subset (\mathbb{Z}/D)^M$ as the lattice of rank M , consisting of the polynomials $g \in (1/D)\mathbb{Z}[\alpha][X_1, X_2, \dots, X_t]$ for which

$$(i) \quad \delta_1 g \leq m \text{ and } \delta_i g \leq n_i \text{ for } 2 \leq i \leq t;$$

$$(ii) \quad \text{If } \delta_j l c_{j-1}(g) = m_j \text{ for } 1 \leq j \leq i, \text{ then } \delta_{i+1} l c_i(g) \leq m_{i+1} \text{ for } 1 \leq i < t;$$

$$(iii) \quad \text{If } \delta_i l c_{i-1}(g) = m_i \text{ for } 1 \leq i \leq t, \text{ then } l c(g) \in \mathbb{Z};$$

$$(iv) \quad \tilde{h} \bmod (p^k, H_k) \text{ divides } \tilde{g} \bmod (p^k, H_k) \text{ in } W_k(\mathbb{F}_q)[X_1].$$

Here M -dimensional vectors and polynomials satisfying conditions (i), (ii) and (iii) are identified in the usual way (cf. [10, (2.6)] and [12, (3.5)]). For notational convenience

we only give a basis for L in the case that $m_i = n_i$ for $2 \leq i \leq t$; the general case can easily be derived from this:

$$\begin{aligned} & \left\{ \frac{1}{D} p^k \alpha^j X_1^i : 0 \leq j < \delta H, 0 \leq i < l \right\} \\ & \cup \left\{ \frac{1}{D} \alpha^{j-\delta H} H(\alpha) X_1^i : \delta H \leq j < l, 0 \leq i < l \right\} \\ & \cup \left\{ \frac{1}{D} \alpha^j \tilde{h} X_1^{i-l} : 0 \leq j < l, l \leq i \leq m \right\} \\ & \cup \left\{ \frac{1}{D} \alpha^j X_1^i \prod_{r=2}^t (X_r - s_r)^{i_r} : 0 \leq j < l, 0 \leq i_1 \leq m, 0 \leq i_r \leq n_r \text{ for } 2 \leq r \leq t, \right. \\ & \quad \left. (i_2, i_3, \dots, i_t) \neq (0, 0, \dots, 0), \right. \\ & \quad \left. \text{and } (i_1, i_2, i_3, \dots, i_t) \neq (m, n_2, n_3, \dots, n_t) \right\} \\ & \cup \left\{ X_1^m \prod_{r=2}^t (X_r - s_r)^{n_r} \right\} \end{aligned}$$

(cf. [10, (2.6)], [12, (3.5)], (2.2), and (3.1)).

PROPOSITION 3.6. *Let b be a nonzero element of L and let*

$$(3.7) \quad \tilde{B}_j = f_{\max}^m b_{\max}^n (n+m)! \left(DN_2 (1 + F_{\max})^{l-1} \prod_{i=2}^j s_i^{n_i} \right)^{n+m},$$

for $1 \leq j \leq t$, where f_{\max}^m denotes $(f_{\max})^m$.

Suppose that

$$(3.8) \quad s_j \geq ((n+m)n_j + 1)^{1/2} \tilde{B}_{j-1}$$

for $2 \leq j \leq t$, and

$$(3.9) \quad p^{k\delta H} \geq |F|^{l-1} (I^{1/2} \tilde{B}_t)^l.$$

Then $\gcd(f, b) \neq 1$ in $\mathbf{Q}(\alpha)[X_1, X_2, \dots, X_t]$.

Proof. Denote by $R = R(Df, Db) \in \mathbf{Z}[\alpha][X_2, X_3, \dots, X_t]$ the resultant of Df and Db (with respect to the variable X_1). An outline of the proof is as follows. First we prove that an upper bound for $(\tilde{R}_j)_{\max}$ is given by \tilde{B}_j . Combining this with (3.8), we then see that $X_j = s_j$ cannot be a zero of \tilde{R}_{j-1} if $\tilde{R}_{j-1} \neq 0$, for $2 \leq j \leq t$. This implies that the assumption that $R \neq 0$ (i.e., $\gcd(f, b) = 1$) leads to $\tilde{R} \neq 0$. We then apply a result from [8], and we find with (3.9) that $\tilde{R} \bmod (p^k, H_k) \neq 0$. But this is a contradiction, because $\tilde{h} \bmod (p^k, H_k)$ divides both $\tilde{f} \bmod (p^k, H_k)$ and $\tilde{b} \bmod (p^k, H_k)$ in $W_k(\mathbf{F}_q)[X_1]$. We conclude that $R = 0$, so that $\gcd(f, b) \neq 1$ in $\mathbf{Q}(\alpha)[X_1, X_2, \dots, X_t]$.

If a and b are two polynomials in any number of variables over $\mathbf{Q}(\alpha)$, having l_a and l_b terms, respectively, then

$$(3.10) \quad (a \cdot b)_{\max} \leq a_{\max} b_{\max} \min(l_a, l_b) (1 + F_{\max})^{l-1}.$$

From (3.10) we easily derive an upper bound for $(\tilde{R}_j)_{\max}$, because $\tilde{R}_j \in \mathbf{Z}[\alpha][X_{j+1}, X_{j+2}, \dots, X_t]$ is the resultant of $D\tilde{f}_j$ and $D\tilde{b}_j$:

$$(3.11) \quad (\tilde{R}_j)_{\max} \leq (D\tilde{f}_j)_{\max}^m (D\tilde{b}_j)_{\max}^n (n+m)! N_{j+1}^{n+m-1} (1 + F_{\max})^{(l-1)(n+m-1)}.$$

It follows from $\tilde{f}_j = \tilde{f}_{j-1} \bmod (X_j - s_j)$, that $(\tilde{f}_j)_{\max} \leq (\tilde{f}_{j-1})_{\max}(n_j + 1)s_j^{n_j}$, so that

$$(3.12) \quad (\tilde{f}_j)_{\max} \leq f_{\max} \prod_{i=2}^j (n_i + 1)s_i^{n_i}.$$

Combining (3.11), (3.12) and a similar bound for $(\tilde{b}_j)_{\max}$, we obtain

$$(3.13) \quad (\tilde{R}_j)_{\max} < f_{\max}^m b_{\max}^n (n+m)! \left(DN_2 \prod_{i=2}^j s_i^{n_i} \right)^{n+m} (1 + F_{\max})^{(I-1)(n+m-1)},$$

for $1 \leq j < t$. (Remark that (3.13) with “<” replaced by “ \leq ” holds for $j = t$.)

Now assume, for some j with $2 \leq j \leq t$, that \tilde{R}_{j-1} is unequal to zero. We prove that $\tilde{R}_j \neq 0$. Because $\tilde{R}_j = \tilde{R}_{j-1} \bmod (X_j - s_j)$, the condition $\tilde{R}_j = 0$ would imply that all polynomials in $\mathbb{Z}[X_j]$ that result from \tilde{R}_{j-1} by grouping together all terms with identical exponents in α and X_{j+1} up to X_t , have $(X_j - s_j)$ as a factor. These polynomials have degree (in X_j) at most $(n+m)n_j$, so that we get, with the result from [14], that

$$|s_j| \leq ((n+m)n_j + 1)^{1/2} (\tilde{R}_{j-1})_{\max}.$$

Combined with (3.13) and (3.7) this is a contradiction with (3.8). We conclude that $\tilde{R}_j \neq 0$ if $\tilde{R}_{j-1} \neq 0$ for any j with $2 \leq j \leq t$, so that the assumption $\gcd(f, b) = 1$ (i.e., $R \neq 0$) leads to $\tilde{R} \neq 0$.

Assume that $H_k(T)$ divides $\tilde{R}(T) \in \mathbb{Z}[T]$ in $(\mathbb{Z}/p^k\mathbb{Z})[T]$, i.e., $\tilde{R} \bmod (p^k, H_k) = 0$. We show that this leads to a contradiction (cf. [8, proof of Thm. 2]). Consider the polynomials $T^i p^k$ for $0 \leq i < \delta H$ and $T^{j-\delta H} H_k$ for $\delta H \leq j < I + \delta \tilde{R}$. These polynomials, when regarded as $(I + \delta \tilde{R})$ -dimensional integral vectors, form a basis for an integral lattice L_H in $\mathbb{Z}^{I+\delta \tilde{R}}$. From (2.2) it follows that the determinant $\det(L_H)$ of L_H equals $p^{k\delta H}$, and that L_H can be considered as the set of polynomials in $\mathbb{Z}[T]$ of degree less than $I + \delta \tilde{R}$ which have $H_k(T)$ as a divisor when taken modulo p^k .

Because F is irreducible and $\delta \tilde{R} < \delta F = I$, we have that $\gcd(F(T), \tilde{R}(T)) = 1$. This implies that the polynomials $T^i F$ for $0 \leq i < \delta \tilde{R}$ and $T^j \tilde{R}$ for $0 \leq j < I$, when regarded as $(I + \delta \tilde{R})$ -dimensional integral vectors, form a basis for an integral lattice L_F in $\mathbb{Z}^{I+\delta \tilde{R}}$. Applying Hadamard's inequality to this basis for L_F , we see that $\det(L_F) \leq |F|^{\delta \tilde{R}} ((\delta \tilde{R} + 1)^{1/2} \tilde{R}_{\max})^I$.

Our assumption $\tilde{R} \bmod (p^k, H_k) = 0$ combined with (2.3) leads to the conclusion that all elements of L_F , when considered as polynomials in $\mathbb{Z}[T]$, have $H_k(T)$ as a divisor when taken modulo p^k , so that L_F is a sublattice of L_H , and in particular

$$p^{k\delta H} = \det(L_H) \leq \det(L_F) \leq |F|^{I-1} (I^{1/2} \tilde{R}_{\max})^I.$$

With the remark after (3.13) and (3.7) this is a contradiction with (3.9), so that $\tilde{R} \bmod (p^k, H_k) \neq 0$. As stated in the first paragraph of this proof, this is a contradiction because $\tilde{h} \bmod (p^k, H_k)$ divides both $\tilde{f} \bmod (p^k, H_k)$ and $\tilde{b} \bmod (p^k, H_k)$ in $W_k(\mathbb{F}_q)[X_1]$, so that our initial assumption $\gcd(f, b) = 1$ must be wrong. This concludes the proof of (3.6). \square

PROPOSITION 3.14. *Let b_1, b_2, \dots, b_M be a reduced basis for L (cf. [9, § 1]), where L and M are as in (3.5), and let*

$$(3.15) \quad B_j = (n+m)! (M2^{M-1})^{n/2} \left(B_j DN_2 (1 + F_{\max})^{I-1} \prod_{i=2}^j s_i^{n_i} \right)^{n+m},$$

for $2 \leq j \leq t$, where B_j is as in § 2. Suppose that

$$(3.16) \quad s_j \geq ((n+m)n_j + 1)^{1/2} B_{j-1}$$

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

$$(3.17) \quad p^{k\delta H} \geq |F|^{I-1} (I^{1/2} B_t)^I,$$

and that f does not contain multiple factors. Then

$$(3.18) \quad (b_1)_{\max} \leq (M2^{M-1})^{1/2} B_f$$

and h_0 divides b_1 , if and only if $h_0 \in L$.

Proof. If h_0 divides b_1 , then $h_0 \in L$, because $b_1 \in L$ and $\delta_1 h_0 \leq \delta_1 b_1$; this proves the "if" part.

To prove the "only if" part, suppose that $h_0 \in L$. Because h_0 is a monic factor of f , we have from (2.7) that $(h_0)_{\max} \leq B_f$. With [9, (1.11)] and $h_0 \in L$ this gives $|b_1| \leq (M2^{M-1})^{1/2} B_f$, so that (3.18) holds, because $(b_1)_{\max} \leq |b_1|$. Because of (3.18), (3.16), (3.17), (3.15), and the definition of B_f , we can apply (3.6), which yields $\gcd(f, b_1) \neq 1$.

Now suppose that h_0 does not divide b_1 . This implies that h_0 also does not divide $r = \gcd(f, b_1)$, where r can be assumed to be monic. But then $\tilde{h} \bmod (p^k, H_k)$ divides $(\tilde{f}/\tilde{r}) \bmod (p^k, H_k)$, so that Proposition 3.6 can be applied with f replaced by \tilde{f}/\tilde{r} . Conditions (3.8) and (3.9) are satisfied because $(f/r)_{\max} \leq B_f$ (cf. (2.7)) and because of (3.16), (3.17) and (3.15). It follows that $\gcd(f/r, b_1) \neq 1$, which contradicts $r = \gcd(f, b_1)$ because f does not contain multiple factors. \square

(3.19) We describe how to compute the irreducible factor h_0 of f . Suppose that f does not contain multiple factors, and that the polynomial \tilde{h} , the $(t-1)$ -tuple s_2, s_3, \dots, s_t , and the prime power p^k are chosen such that (3.1), (3.2), (3.3), (3.4), (3.16) and (3.17) are satisfied with, for (3.16) and (3.17), m replaced by $n-1$. Remember that we also have to take care that conditions (2.1), (2.2), (2.3), (2.4) and (2.5) on p and H are satisfied.

We apply the basis reduction algorithm (cf. [9, § 1]) to a sequence of M_j -dimensional lattices as in (3.5), where the $M_j = 1 + I \sum_{i=1}^t m_i N_{i+1}$ run through the range of admissible values for m_1, m_2, \dots, m_t (cf. (3.5)), in such a way that $M_j < M_{j+1}$. (So, for $m = l, l+1, \dots, n-1$, and $m_i = 0, 1, \dots, \delta_i l c_{i-1}(f)$ for $i = t, t-1, \dots, 2$ in succession.) According to (3.14), the first vector b_1 that we find that satisfies (3.18) equals $\pm h_0$ (remember that b_1 belongs to a basis for the lattice), so that we can stop if such a vector is found. If for none of the lattices a vector satisfying (3.18) is found, then h_0 is not contained in any of these lattices according to (3.14), so that $h_0 = f$.

PROPOSITION 3.20. Assume that the conditions in (3.19) are satisfied. The polynomial h_0 can be computed in $O((\delta_1 h_0 I N_2)^4 k \log p)$ arithmetic operations on integers having binary length $O(INk \log p)$.

Proof. Observing that $\log(INp^{2k}) = O(k \log p)$ (cf. (3.17), (3.15) and (2.8)), the proof immediately follows from (3.19), (3.5) and [9, (1.26), (1.37)]. \square

(3.21) We now show how s_2, s_3, \dots, s_t and p can be chosen in such a way that the conditions in (3.19) can be satisfied. The algorithm to factor f then easily follows by repeated application of (3.19).

We assume that f does not contain multiple factors, so that the resultant $R = R(df, df')$ of df and its derivative df' with respect to X_1 is unequal to zero. First we choose $s_2, s_3, \dots, s_t \in \mathbb{Z}_{>0}$ minimal such that (3.16) is satisfied with m replaced by $n-1$. It follows from (3.16), (3.15), (2.8) and $\log D = O(\log d + I \log(I|F|))$ (because $D = d | \text{discr}(F) |$), that

$$\begin{aligned} \log s_j &= O(\log((n+m)n_j) + \log B_{j-1}) \\ &= O\left(\ln N + n \left(\log B_f + \log D + I \log(1 + F_{\max}) + \sum_{i=1}^{j-1} n_i \log s_i \right) \right) \end{aligned}$$

$$= O\left(n\left(IN + \log(df_{\max}) + I \log(I|F|) + \sum_{i=1}^{j-1} n_i \log s_i\right)\right)$$

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

$$\log s_j = O\left(n(IN + \log(df_{\max}) + I \log(I|F|)) \prod_{i=2}^{j-1} (1 + nn_i)\right)$$

and

$$(3.22) \quad \sum_{i=2}^t n_i \log s_i = O(n^{t-2} N(IN + \log(df_{\max}) + I \log(I|F|))).$$

From the proof of (3.6) it follows that, for this choice of s_2, s_3, \dots, s_t , the resultant $R \in \mathbb{Z}[\alpha]$ of $d\tilde{f}$ and $d\tilde{f}'$ is unequal to zero.

Next we choose p minimal such that p does not divide D or $\text{discr}(F)$, and such that $\tilde{R} \not\equiv 0 \pmod{p}$. Clearly

$$\prod_{q \text{ Prime}, q < p} q \leq d \text{discr}(F) \tilde{R}_{\max}$$

which yields, together with

$$\prod_{q \text{ prime}, q < p} q > e^{Ap}$$

for all $p > 2$ and some constant $A > 0$ (cf. [5, § 22.2]), that

$$(3.23) \quad p = O(\log d + I \log(I|F|) + \log \tilde{R}_{\max}).$$

Similar to (3.13) we obtain

$$\tilde{R}_{\max} \leq f_{\max}^{2n-1} n^n (2n-1)! \left(dN_2 \prod_{i=2}^t s_i^{n_i}\right)^{2n-1} (1 + F_{\max})^{(I-1)(2n-2)},$$

so that we get, using (3.22)

$$\log \tilde{R}_{\max} = O(n^{t-1} N(IN + \log(df_{\max}) + I \log(I|F|))).$$

Combining this with (3.23) we conclude that

$$(3.24) \quad p = O(n^{t-1} N(IN + \log(df_{\max}) + I \log(I|F|))).$$

Notice that (2.1) is now satisfied. In order to compute a polynomial $H \in \mathbb{Z}[T]$ satisfying (2.2), (2.4), (2.5) and (2.3) with k replaced by 1, we factor $F \pmod{p}$ by means of Berlekamp's algorithm [7, § 4.6.2] and we choose H as an irreducible factor of $f \pmod{p}$ for which $\tilde{R} \pmod{(p, H_1)} \neq 0$; such a polynomial H exists because $\tilde{R} \pmod{p} \neq 0$. Conditions (2.4) and (2.3) with k replaced by 1 are clear from the construction of H , and because we may assume that H has leading coefficient equal to one, (2.2) also holds. The condition that $\text{discr}(F) \pmod{p} \neq 0$, finally, guarantees that $F \pmod{p}$ does not contain multiple factors, so that (2.5) is satisfied.

We choose k minimal such that (3.17) holds, so that

$$k \log p = O\left(I\left(InN + n \log(df_{\max}) + In \log(I|F|) + n \sum_{i=2}^t n_i \log s_i\right) + \log p\right)$$

(cf. (3.15) and (2.8)), which gives, with (3.22) and (3.24),

$$(3.25) \quad k \log p = O(In^{t-1} N(IN + \log(df_{\max}) + I \log(I|F|))).$$

Now we apply Hensel's lemma [7, Exer. 4.6.22] to modify H in such a way that (2.3) holds for this value of k (this is possible because (2.3) already holds for $k=1$), and finally we apply Berlekamp's algorithm as described in [1, § 5] and Hensel's lemma as in [17] to compute the irreducible factorization of $\tilde{f} \pmod{(p^k, H_k)}$ in $W_k(\mathbb{F})[X]$.

Condition (3.4) is satisfied for each irreducible factor $\tilde{h} \bmod (p^k, H_k)$ of $\tilde{f} \bmod (p^k, H_k)$ because $\tilde{R} \bmod (p, H_1) \neq 0$, and (3.1), (3.2) and (3.3) are clear from the construction of \tilde{h} .

We have shown how to choose s_2, s_3, \dots, s_t and p , and how to satisfy the conditions in (3.19). We are now ready for our theorem.

THEOREM 3.26. *Let f be a monic polynomial in $(1/d)\mathbb{Z}[\alpha][X_1, X_2, \dots, X_t]$ with $t \geq 2$, of degree n_i in X_i and $2 \leq n = n_1 \leq n_2 \leq \dots \leq n_t$. The irreducible factorization of f can be found in $O(n^{t-1}(IN)^5(IN + \log(df_{\max}) + I \log(I|F|)))$ arithmetic operations on integers having binary length $O(n^{t-1}(IN)^2(IN + \log(df_{\max}) + I \log(I|F|)))$, where $N = \prod_{i=1}^t (n_i + 1)$.*

Proof. If f does not contain multiple factors, then f can be factored by repeated application of (3.19). In that case (3.26) follows from (3.21), (3.20), (3.25) and the well-known estimates for the application of Berlekamp's algorithm and Hensel's lemma (cf. [1], [7] and [19]).

If f contains multiple factors, then we first have to compute the monic gcd g of f and its derivative with respect to X_1 , and the factoring algorithm is then applied to f/g . The cost of factoring f/g satisfies the same estimates as above, because $(f/g)_{\max} \leq B_f$ (cf. (2.7)), and this dominates the costs of the computation of g , which can be done by means of the subresultant algorithm (cf. [2]). \square

REFERENCES

- [1] E. R. BERLEKAMP, *Factoring polynomials over large finite fields*, Math. Comp., 24 (1970), pp. 713-735.
- [2] W. S. BROWN, *The subresultant PRS algorithm*, ACM Trans. Math. Software, 4 (1978), pp. 237-249.
- [3] A. L. CHISTOV AND D. YU. GRIGORYEV, *Polynomial-time factoring of the multivariable polynomials over a global field*, LOMI preprint E-5-82, Leningrad, 1982.
- [4] A. O. GEL'FOND, *Transcendental and Algebraic Numbers*, Dover, New York, 1960.
- [5] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford University Press, London, 1979.
- [6] E. KALTOFEN, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization*, this Journal, 14 (1985), pp. 469-489.
- [7] D. E. KNUTH, *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, sec. ed., Addison-Wesley, Reading, MA, 1981.
- [8] A. K. LENSTRA, *Lattices and factorization of polynomials over algebraic number fields*, Proc. Eurocam 82, LNCS, 144 (1982), pp. 32-39.
- [9] A. K. LENSTRA, H. W. LENSTRA, JR AND L. LOVÁSZ, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515-534.
- [10] A. K. LENSTRA, *Factoring polynomials over algebraic number fields*, Report IW 213/82, Mathematisch Centrum, Amsterdam, 1982.
- [11] ———, *Factoring multivariate polynomials over finite fields*, J. Comput. System Sci., 30 (1985), pp. 235-248; Proc. 15th Annual ACM Symp. on the Theory of Computing, pp. 189-192.
- [12] ———, *Factoring multivariate integral polynomials*, Theoretical Computer Science, 34 (1984), pp. 207-213; Proc. 10th ICALP, LNCS 154, pp. 458-465.
- [13] ———, *Factoring multivariate integral polynomials*, II, Report IW 230/83, Mathematisch Centrum, Amsterdam, 1983.
- [14] M. MIGNOTTE, *An inequality about factors of polynomials*, Math. Comp., 28 (1974), pp. 1153-1157.
- [15] J. STOER, *Einführung in die numerische Mathematik I*, Springer, Berlin, 1972.
- [16] J. VON ZUR GATHEN, *Factoring sparse multivariate polynomials*, Proc. 24th Annual Symposium on Foundations of Computer Science (1983), pp. 172-179.
- [17] P. S. WANG, *Factoring multivariate polynomials over algebraic number fields*, Math. Comp., 30 (1976), pp. 324-336.
- [18] P. J. WEINBERGER AND L. P. ROTHSCILD, *Factoring polynomials over algebraic number fields*, ACM Trans. Math. Software, 2 (1976), pp. 335-350.
- [19] D. Y. Y. YUN, *The Hensel Lemma in Algebraic Manipulation*, MIT, Cambridge, MA, 1974; reprint: Garland, New York, 1980.