Factoring polynomials over algebraic number fields

A.K. Lenstra
Mathematisch Centrum
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

Abstract.

We present a polynomial-time algorithm for the factorization of univariate polynomials over algebraic number fields. Our algorithm is a direct generalization of the polynomial-time algorithm for the factorization of univariate polynomials over the rationals [7].

1. Introduction.

In [7] a polynomial-time algorithm was given to factor polynomials in one variable with rational coefficients. In this paper we generalize this result to polynomials in one variable with coefficients in an algebraic number field.

The existence of a polynomial-time algorithm for this problem is not surprising in view of [7]. Kronecker's idea of using norms reduced the problem to the factorization of univariate polynomials with rational coefficients, and in [5] it is shown that this reduction is polynomial-time. Here we pursue a direct approach to the factorization of polynomials over algebraic number fields. As suggested in [6: Section 5] we regard the irreducible factor we are looking for as an element of a certain integral lattice, and we prove that it is the 'smallest' element in this lattice. As we have seen in [7] this enables us to effectively compute this factor by means of a basis reduction algorithm for lattices.

The practical importance of our algorithm should not be overstated. This is mainly due to the rather slow basis reduction algorithm. For practical purposes we recommend the algorithm from [6], where the ideas of the lattice approach are combined with the well-known exponential-time factoring algorithm. In the algorithm from [6] the algebraic numbers are represented by their residues modulo a certain prime-power p^k. In the last step (trial divisions to determine the true factors), the algebraic num-

bers are restored in a unique way by means of a reduced basis of a certain integral lattice. Experiments have shown that this greatly reduces the running time (cf. [6]).

This paper is organized as follows. Section 2 contains some notation and definitions; furthermore we recall there some results from [7: Section 1]. Section 3 deals with the connection between factors and lattices; it generalizes the first part of [7: Section 2]. In Section 4 we give a global description of the factoring algorithm and we analyze its running time.

For a polynomial f we denote by δf the *degree* of f, by $\ell c(f)$ the *leading coefficient* of f, and f is said to be *monic* if $\ell c(f) = 1$.

2. Preliminaries.

Let the algebraic number field $\mathbb{Q}(\alpha)$ be given as the field of rational numbers $\mathbb{Q}$ extended by a root α of a prescribed monic irreducible polynomial $F \in \mathbb{Z}[T]$, i.e. $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[T]/(F)$. This implies that the elements of $\mathbb{Q}(\alpha)$ can be represented as polynomials in α over $\mathbb{Q}$ of degree $< \delta F$. We may assume that the degree of the *minimal polynomial* F is at least 2.

Similarly, we define $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[T]/(F)$ as the ring of polynomials in α over $\mathbb{Z}$ of degree $< \delta F$, where multiplication is done 'modulo F'.

Let f be a monic polynomial in $\mathbb{Q}(\alpha)[X]$. In Section 4 we will describe how to choose a positive integer D such that

(2.1) $\quad f$ and all monic factors of f in $\mathbb{Q}(\alpha)[X]$ are in $\frac{1}{D}\mathbb{Z}[\alpha][X]$.

The algorithm to determine the irreducible factors of f in $\mathbb{Q}(\alpha)[X]$ that we will present, is very similar to the algorithm for factorization in $\mathbb{Z}[X]$ as described in [7]: first determine the factorization of f over some finite field ($\mathbb{Z}/p\mathbb{Z}$ in [7]), next extend this factorization to a factorization over a large enough ring ($\mathbb{Z}/p^k\mathbb{Z}$ in [7]), and finally use a lattice reduction algorithm to determine the factors over $\mathbb{Q}(\alpha)$. Therefore we first describe how to choose this finite field and this ring.

Let p be a prime number such that

(2.2) $\quad p$ does not divide D,

and let k be a positive integer. For $G = \Sigma_i a_i T^i \in \mathbb{Z}[T]$ and some integer ℓ we denote by G_ℓ or $(G \bmod p^\ell)$ the polynomial $\Sigma_i (a_i \bmod p^\ell) T^i \in (\mathbb{Z}/p^\ell\mathbb{Z})[T]$. In Section

4 we will see that we are able to determine p in such a way that we can compute a polynomial $H \in \mathbb{Z}[T]$ such that:

(2.3) H is monic,

(2.4) H_k divides F_k in $(\mathbb{Z}/p^k\mathbb{Z})[T]$,

(2.5) H_1 is irreducible in $(\mathbb{Z}/p\mathbb{Z})[T]$,

(2.6) $(H_1)^2$ does not divide F_1 in $(\mathbb{Z}/p\mathbb{Z})[T]$.

It follows that H_1 divides F_1 in $(\mathbb{Z}/p\mathbb{Z})[T]$, and that $0 < \delta H \leq \delta F$.

This polynomial H, together with the prime number p and the integer k, gives us the possibility to construct the finite field and the ring we were looking for. We denote by q the prime-power $p^{\delta H}$ and by $\mathbb{F}_q$ the finite field containing q elements. From (2.5) we derive that $\mathbb{F}_q \simeq (\mathbb{Z}/p\mathbb{Z})[T]/(H_1)$. Remark that $\mathbb{F}_q \simeq \{\Sigma_{i=0}^{\delta H-1} a_i \alpha_1^i : a_i \in \mathbb{Z}/p\mathbb{Z}\}$ where $\alpha_1 = (T \bmod (H_1))$ is a zero of H_1. This enables us to represent the elements of $\mathbb{F}_q$ as polynomials in α_1 over $\mathbb{Z}/p\mathbb{Z}$ of degree $< \delta H$. The finite field $\mathbb{F}_q$ corresponds to $\mathbb{Z}/p\mathbb{Z}$ in [7]; we now define the ring that will play the role of $\mathbb{Z}/p^k\mathbb{Z}$ in [7]. Let $W_k(\mathbb{F}_q) = (\mathbb{Z}/p^k\mathbb{Z})[T]/(H_k)$ be a ring containing q^k elements. We have that $W_k(\mathbb{F}_q) = \{\Sigma_{i=0}^{\delta H-1} a_i \alpha_k^i : a_i \in \mathbb{Z}/p^k\mathbb{Z}\}$ where $\alpha_k = (T \bmod (H_k))$ is a zero of H_k. So elements of $W_k(\mathbb{F}_q)$ can be represented as polynomials in α_k over $\mathbb{Z}/p^k\mathbb{Z}$ of degree $< \delta H$, and $W_k(\mathbb{F}_q)$ can be mapped onto $\mathbb{F}_q$ by reducing the coefficients of these polynomials modulo p. For $a \in W_k(\mathbb{F}_q)[X]$ we denote by $(a \bmod p) \in \mathbb{F}_q[X]$ the result of applying this mapping coefficient-wise to a. Remark that $W_1(\mathbb{F}_q) \simeq \mathbb{F}_q$.

We now show how we map polynomials in $\frac{1}{D}\mathbb{Z}[\alpha][X]$ to polynomials in $\mathbb{F}_q[X]$ and $W_k(\mathbb{F}_q)[X]$ respectively. Clearly, the canonical mapping from $\mathbb{Z}[T]/(F)$ to $(\mathbb{Z}/p^\ell\mathbb{Z})[T]/(H_\ell)$ defines a mapping from $\mathbb{Z}[\alpha]$ to $W_\ell(\mathbb{F}_q)$, for $\ell = 1, k$. (Informally, this mapping works by reducing the polynomial in α modulo p^ℓ and $H_\ell(\alpha)$.) For $a \in \mathbb{Z}[\alpha]$ we denote by $(a \bmod (p^\ell, H_\ell)) \in W_\ell(\mathbb{F}_q)$ the result of this mapping. Finally, for $g = \Sigma_i \frac{a_i}{D} X^i \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ we denote by $(g \bmod (p^\ell, H_\ell))$ the polynomial $\Sigma_i (((D^{-1} \bmod p^\ell) a_i) \bmod (p^\ell, H_\ell)) X^i \in W_\ell(\mathbb{F}_q)[X]$. Notice that $D^{-1} \bmod p^\ell$ exists due to (2.2).

We conclude this section with a result from [7: Section 1] that we will need here. Let $b_1, b_2, \ldots, b_n \in (\frac{\mathbb{Z}}{D})^n$ be linearly independent; we restrict ourselves to the case that the $n \times n$ matrix having $b_1, b_2, \ldots, b_n$ as columns is upper-triangular. The i-dimensional lattice $L_i \subset (\frac{\mathbb{Z}}{D})^i$ with basis $b_1, b_2, \ldots, b_i$ is defined as $L_i = \Sigma_{j=1}^i \mathbb{Z} b_j = \{\Sigma_{j=1}^i r_j b_j : r_j \in \mathbb{Z}\}$; we put $L = L_n$.

(2.7) Proposition. (cf. [7: (1.11), (1.26), (1.37)]) Let $B \in \mathbb{Z}_{\geq 2}$ be such that $|Db_j|^2 \leq B$ for $1 \leq j \leq n$, where $|\ |$ denotes the ordinary Euclidean length. There is an algorithm that determines a vector $\tilde{b} \in L$ such that $\tilde{b}$ belongs to a basis for L, and such that $|\tilde{b}|^2 \leq 2^{n-1}|x|^2$ for every $x \in L$, $x \neq 0$; this algorithm takes $O(n^4 \log B)$ elementary operations on integers having binary length $O(n \log B)$. Furthermore, during the first $O(i^4 \log B)$ operations (on integers having binary length $O(i \log B)$), vectors $\tilde{b}_i$, belonging to a basis for L_i, are determined such that $|\tilde{b}_i|^2 \leq 2^{i-1}|x_i|^2$ for every $x_i \in L_i$, $x_i \neq 0$, for $1 \leq i \leq n$. □

Informally, (2.7) states that we can find a reasonable approximation of the shortest vector in L in polynomial-time. Furthermore, during this computation, we find approximations of the shortest vectors of the lattices L_i without any time loss.

3. Factors and lattices.

This section is similar to the first part of [7: Section 2]. We formulate the generalizations of [7: (2.5), (2.6), (2.7), (2.13)] to polynomials over algebraic number fields. Let f, D, p, k, F, and H be as in Section 1. We put $n = \delta f$; we may assume that $n > 0$.

Suppose that we are given a polynomial $h \in \mathbb{Z}[\alpha][X]$ such that

(3.1) h is monic,

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

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

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

We put $\ell = \delta h$; so $0 < \ell \leq n$. In Section 4 we will see which extra conditions have to be imposed on p so that h can be determined.

Let $h_0 \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ be the unique monic irreducible factor of f for which $(h \bmod (p, H_1))$ divides $(h_0 \bmod (p, H_1))$ in $\mathbb{F}_q[X]$ (or equivalently $(h \bmod (p^k, H_k))$ divides $(h_0 \bmod (p^k, H_k))$ in $W_k(\mathbb{F}_q)[X]$, cf. [7: (2.5)]).

(3.5) In the remainder of this section we fix an integer m with $\ell \leq m < n$. We define L as the collection of polynomials $g \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ such that:

(i) $\delta g \leq m$,

(ii) if $\delta g = m$, then $\ell c(g) \in \mathbb{Z}$,

(iii) $(h \bmod (p^k, H_k))$ divides $(g \bmod (p^k, H_k))$ in $W_k(\mathbb{F}_q)[X]$.

We identify such a polynomial $g = \sum_{i=0}^{m-1} \sum_{j=0}^{\delta F-1} a_{ij}\alpha^j X^i + a_{m0}X^m$ with the $(m\,\delta F + 1)$-dimensional vector $(a_{00}, a_{01}, \ldots, a_{0\,\delta F-1}, \ldots, a_{m-1\,\delta F-1}, a_{m0})$. Using this identification it is not difficult to see that L is a lattice in $(\frac{\mathbb{Z}}{D})^{m\delta F+1}$. From the fact that H and h are monic ((2.3) and (3.1)) it follows that an upper-triangular basis for L is given by:

$$\{\tfrac{1}{D}p^k\alpha^j X^i:\ 0 \le j < \delta H,\ \ 0 \le i < \ell\} \ \cup$$
$$\{\tfrac{1}{D}\alpha^{j-\delta H}H(\alpha)\,X^i:\ \delta H \le j < \delta F,\ \ 0 \le i < \ell\} \ \cup$$
$$\{\tfrac{1}{D}\alpha^j h\,X^{i-\ell}:\ 0 \le j < \delta F,\ \ \ell \le i < m\} \ \cup$$
$$\{h\,X^{m-\ell}\}.$$

We define the *length* $|g|$ of g as the ordinary Euclidean length of the vector identified with g; the *height* g_{max} of g is defined as $\max\{|a_{ij}|\}$. Similarly we define the length and the height of polynomials in $\mathbb{Z}[T]$.

(3.6) Proposition. Let $b \in L$ satisfy

$$p^{k\ell\delta H/\delta F} > \left(Df_{max}((n+1)\delta F(1+F_{max})^{\delta F-1})^{\frac{1}{2}}\right)^m \left(Db_{max}((m+1)\delta F(1+F_{max})^{\delta F-1})^{\frac{1}{2}}\right)^n. \tag{3.7}$$

Then b is divisible by h_0 in $\mathbb{Q}(\alpha)[X]$ and in particular $\gcd(f, b) \neq 1$.

Proof. The proof is similar to the proof of [7: (2.7)]; we therefore omit the details. Put $g = \gcd(f, b)$, and $e = \delta g$. Identify the polynomials

$$\{\alpha^j X^i f:\ 0 \le j < \delta F,\ \ 0 \le i < \delta b - e\} \cup \{\alpha^j X^i b:\ 0 \le j < \delta F,\ \ 0 \le i < n - e\} \tag{3.8}$$

with $(\delta F(n+\delta b-e))$-dimensional vectors. The projections of these vectors on $\frac{1}{D}\mathbb{Z}X^e + \frac{1}{D}\mathbb{Z}\alpha X^e + \ldots + \frac{1}{D}\mathbb{Z}\alpha^{\delta F-1}X^e + \frac{1}{D}\mathbb{Z}X^{e+1} + \ldots + \frac{1}{D}\mathbb{Z}\alpha^{\delta F-1}X^{n+\delta b-e-1}$ form a basis for a $(\delta F(n+\delta b-2e))$-dimensional lattice M'. Using induction on j one proves that

$$(\alpha^j X^i f)_{max} = (\alpha^j f)_{max} \le f_{max}(1 + F_{max})^j,$$

so that, for $0 \le j < \delta F$ and $0 \le i < \delta b - e$,

$$|\alpha^j X^i f| \le f_{max}((n+1)\delta F)^{\frac{1}{2}}(1 + F_{max})^j.$$

With Hadamard's inequality, and a similar bound on $|\alpha^j X^i b|$ we get

$$d(M') \le \left((f_{max}((n+1)\delta F(1+F_{max})^{\delta F-1})^{\frac{1}{2}})^m (b_{max}((m+1)\delta F(1+F_{max})^{\delta F-1})^{\frac{1}{2}})^n\right)^{\delta F},$$

where $d(M')$ denotes the determinant of M'. With (3.7) this gives

$$d(M') < \frac{p^{k\ell\delta H}}{D^{(n+m)\delta F}}. \tag{3.9}$$

It is easy to prove that h_0 divides g in $\mathbb{Q}(\alpha)[X]$ if and only if $(h \bmod (p, H_1))$ divides $(g \bmod (p, H_1))$ in $\mathbb{F}_q[X]$ (cf. [7: (2.5)]). So assume that the latter is not

the case; we will derive a contradiction from this.

Let $v \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ be some integral linear combination of the polynomials in (3.8) such that $\delta v < e + \ell$. It follows from our assumption that $(v \bmod (p^k, H_k)) = 0$ in $W_k(\mathbb{F}_q)[X]$ (cf. [7: (2.7)]). Therefore, if we regard $\ell c(v)$ as a polynomial in α, we have

(3.10) $\quad \ell c(\ell c(v)) \equiv 0 \text{ modulo } p^k \text{ if } \delta \ell c(v) < \delta H.$

Now choose a basis $b_{e0}, b_{e1}, \dots, b_{e\,\delta F-1}, b_{e+1\,0}, \dots, b_{n+\delta b-e-1\,\delta F-1}$ for M' such that $\delta b_{ij} = i$ and $\delta \ell c(b_{ij}) = j$ for $e \le i < n+\delta b-e$ and $0 \le j < \delta F$, where $\ell c(b_{ij})$ is regarded as a polynomial in α. From (3.10) we derive that $\ell c(\ell c(b_{ij})) \equiv 0 \bmod p^k$ for $0 \le j < \delta H$ and $e \le i < e+\ell$. Since $\ell c(\ell c(b_{ij})) \in \frac{\mathbb{Z}}{D}$, we obtain $|\ell c(\ell c(b_{ij}))| \ge \frac{p^k}{D}$ for $0 \le j < \delta H$ and $e \le i < e+\ell$ and $|\ell c(\ell c(b_{ij}))| \ge \frac{1}{D}$ for $\delta H \le j < \delta F$ or $e+\ell \le i < n+\delta b-e$. The determinant of M' equals the product of $|\ell c(\ell c(b_{ij}))|$, so that

$$d(M') \ge \frac{p^{k\ell\delta H}}{D^{(n+\delta b-2e)\delta F}} \ge \frac{p^{k\ell\delta H}}{D^{(n+m)\delta F}}.$$

Combined with (3.9) this is the desired contradiction. □

(3.11) Proposition. (cf. [7: (2.13)]) Suppose that

$$(3.12) \quad p^{k\ell\delta H/\delta F} > \Big(2^{n(m\delta F+1)}(n+1)^{n+m}(m+1)^n\binom{2m}{m}^n \delta F^{4n+m}(\delta F-1)^{n(\delta F-1)} (1+F_{max})^{(n+m)(\delta F-1)} |\mathrm{discr}(F)|^{-n}\Big)^{\frac{1}{2}} \cdot (Df_{max})^{n+m} |F|^{2n(\delta F-1)},$$

where $\mathrm{discr}(F)$ denotes the discriminant of F. Then we have $\delta h_0 \le m$ if and only if (3.7) is satisfied with b replaced by $\tilde{b}$, where $\tilde{b}$ results from applying (2.7) to L.

Proof. In [8] we show that the method sketched in [10] combined with results from [9] gives the following upper bound for the length of a monic factor of degree $\le m$ of f in $\frac{1}{D}\mathbb{Z}[\alpha][X]$:

$$f_{max}(2(n+1)\delta F^3(\delta F-1)^{\delta F-1}\binom{2m}{m})^{\frac{1}{2}}|F|^{2(\delta F-1)}|\mathrm{discr}(F)|^{-\frac{1}{2}}.$$

With (3.6) the proof follows immediately. □

4. Description of the algorithm.

We describe how the results from the previous sections can be used to formulate a polynomial-time algorithm to factor $f \in \mathbb{Q}(\alpha)[X]$. First we present an algorithm that determines h_0, given D, p, H and h. Let d be such that $f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$.

(4.1) Suppose that a positive integer D, a prime number p, and polynomials $H \in \mathbb{Z}[T]$ and $h \in \mathbb{Z}[\alpha][X]$ are given such that (2.1), (2.2), (2.3), (2.5), (2.6), (3,1), (3.3) and (3.4), and (2.4) and (3.2) with k replaced by 1, are satisfied. We describe an algorithm that determines h_0, the monic irreducible factor of f for which $(h \bmod (p,H_1))$ divides $(h_0 \bmod (p,H_1))$ in $\mathbb{F}_q[X]$.

Put $\ell = \delta h$; we may assume that $\ell < n$. We calculate the least positive integer k for which (3.12) holds with m replaced by $n-1$:

$$(4.2)\qquad p^{k\ell\delta H/\delta F} > \left(2^{n((n-1)\delta F+1)}(n+1)^{2n-1}n^n\binom{2(n-1)}{n-1}^n\delta F^{5n-1}(\delta F-1)^{n(\delta F-1)}\right.$$
$$\left.(1+F_{max})^{(2n-1)(\delta F-1)}|\mathrm{discr}(F)|^{-n}\right)^{\frac{1}{2}}\cdot(Df_{max})^{2n-1}|F|^{2n(\delta F-1)}.$$

Next we modify H in such a way that (2.4) holds for the value of k just calculated. The factor $H_k = (H \bmod p^k)$ of $(F \bmod p^k)$ gives us the possibility to compute in $W_k(\mathbb{F}_q)$. Therefore we now modify h, without changing $(h \bmod (p,H_1))$, in such a way that (3.2) holds for the above value of k. The computations of the new H and h can both be done by means of Hensel's lemma [4: exercise 4.6.22; 11]; notice that Hensel's lemma can be applied because of (2.6) and (3.4).

Now apply Proposition (2.7) to the $(m\delta F + 1)$-dimensional lattice L as defined in (3.5), for each of the values of $m = \ell, \ell+1, \ldots, n-1$ in succession; but we stop as soon as for one of these values of m we find a vector $\tilde{b}$ in L such that (3.7) is satisfied with b replaced by $\tilde{b}$. If such a vector is found for a certain value m_0 of m, then we know from (3.11) that $\delta h_0 \le m_0$. Since we try the values $m = \ell, \ell+1, \ldots, n-1$ in succession we also know that $\delta h_0 > m_0 - 1$, so $\delta h_0 = m_0$. By (3.6) h_0 divides $\tilde{b}$ in $\mathbb{Q}(\alpha)[X]$ which implies, together with $\delta\tilde{b} \le m_0$, that $\delta\tilde{b} = m_0$. From (3.5)(ii) and from the fact that h_0 is monic we find that $\tilde{b} = ch_0$, for some constant $c \in \mathbb{Z}$. Using that $h_0 \in L$ and that $\tilde{b}$ belongs to a basis for L, we conclude that $c = \pm 1$, so that $\tilde{b} = \pm h_0$.

If on the other hand we did not find such a vector $\tilde{b}$ in any of the lattices, then we know from (3.11) that $\delta h_0 > n-1$. This implies that $h_0 = f$. This finishes the description of Algorithm (4.1).

(4.3) Proposition. Denote by $m_0 = \delta h_0$ the degree of the irreducible factor h_0 of f that is found by Algorithm (4.1). Then the number of arithmetic operations needed by Algorithm (4.1) is $O(m_0(n^5\delta F^6 + n^4\delta F^6\log(\delta F|F|) + n^4\delta F^5\log(Df_{max}) + n^3\delta F^4\log p))$ and

the integers on which these operations are performed each have binary length $O(n^3\delta F^3 + n^2\delta F^3 \log(\delta F|F|) + n^2\delta F^2 \log(Df_{max}) + n\delta F \log p)$.

Proof. Let m_1 be the largest value of m for which Proposition (2.7) is applied; so $m_1 = m_0$ or $m_1 = m_0 - 1$. From (2.7) it follows that during the application of (2.7) to the $(m_1 \delta F + 1)$-dimensional lattice, also approximations of shortest vectors were obtained for the $(m \delta F + 1)$-dimensional lattices, for $\ell \le m < m_1$. Therefore the number of arithmetic operations needed for the applications of (2.7) for $\ell \le m \le m_1$ is equal to the number of operations needed for $m = m_1$ only.

To analyze the latter we derive a bound B for the length of the vectors in the initial basis for L (cf. (3.5)). Assuming that the coordinates of the initial basis are reduced modulo p^k, we derive from (4.2), $|\mathrm{discr}(F)| \ge 1$, $\delta H \ge 1$ and $\ell \ge 1$ that $\log B = O(n^2\delta F^2 + n\delta F^2 \log(\delta F|F|) + n\delta F \log(Df_{max}) + \log p)$. Combined with $m_1 = O(m_0)$ and (2.7) this yields the estimates given in (4.3).

It is straightforward to verify that the same estimates are valid for both applications of Hensel's lemma and for the computation of $\mathrm{discr}(F)$ (cf. [2], [11]). □

(4.4) We now describe how to choose D, p, H and h in such a way that Algorithm (4.1) can be applied. The algorithm to factor f into its monic irreducible factors in $\mathbb{Q}(\alpha)[X]$ then easily follows.

First we choose a positive integer D such that (2.1) holds, i.e. f and all monic factors of f in $\mathbb{Q}(\alpha)[X]$ are in $\frac{1}{D}\mathbb{Z}[\alpha][X]$. From [10] it follows that we can take $D = dc$, where d is such that $f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$, and c is the largest integer such that c^2 divides $\mathrm{discr}(F)$. This integer c however might be difficult to compute; therefore we take $D = d|\mathrm{discr}(F)|$ as denominator, which clearly also suffices.

We may assume that the resultant $R(f,f') \in \mathbb{Q}(\alpha)$ of f and its derivative f' is unequal to zero, i.e. f has no multiple factors in $\mathbb{Q}(\alpha)[X]$. We determine p as the smallest prime number not dividing $D \cdot \mathrm{discr}(F) \cdot R(f,f')$; so (2.2) is satisfied.

Using Berlekamp's algorithm [4: Section 4.6.2] we compute the irreducible factorization $(F \bmod p) = \prod_{i=1}^{t} (G_i \bmod p)$ of $(F \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. This factorization does not contain multiple factors because $\mathrm{discr}(F) \not\equiv 0 \bmod p$. Combined with $R(f,f') \not\equiv 0 \bmod p$ this implies that there exists an integer $i_0 \in \{1, 2, \ldots, t\}$ such that $(R(f,f') \bmod (p, (G_{i_0} \bmod p))) \neq 0$; let H be such a polynomial G_{i_0}. We may assume

that H is monic, so that (2.3), (2.5), (2.6) and (2.4) with k replaced by 1 are satisfied.

Next we determine the irreducible factorization of $(f \bmod (p,H_1))$ in $\mathbb{F}_q[X]$ by means of Berlekamp's algorithm [1: Section 5], where $q = p^{\delta H}$ and $\mathbb{F}_q \simeq (\mathbb{Z}/p\mathbb{Z})[T]/(H_1)$. (Notice that we use a modified version of Berlekamp's algorithm here, one that is polynomial-time in p and δH rather than polynomial-time in the number of elements of the finite field.)

Since f is monic the resultant $R(f,f')$ is, up to sign, equal to the discriminant of f, so that it follows from the construction of H that the discriminant of f is unequal to zero in $\mathbb{F}_q$. Therefore (3.4) holds for all irreducible factors $(h \bmod (p,H_1))$ of $(f \bmod (p,H_1))$ in $\mathbb{F}_q[X]$; we may assume that these factors are monic.

The algorithm to factor f now follows by repeated application of Algorithm (4.1).

(4.5) Theorem. The algorithm sketched above computes the irreducible factorization of any monic polynomial $f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$ of degree $n > 0$. The number of arithmetic operations needed by the algorithm is $O(n^6\delta F^6 + n^5\delta F^6 \log(\delta F|F|) + n^5\delta F^5 \log(df_{max}))$, and the integers on which these operations are performed each have binary length $O(n^3\delta F^3 + n^2\delta F^3 \log(\delta F|F|) + n^2\delta F^2 \log(df_{max}))$.

Proof. It follows from [2] that the calculations of $R(f,f')$ and $\mathrm{discr}(F)$ satisfy the above estimates. From Hadamard's inequality we obtain $|\mathrm{discr}(F)| \le \delta F^{\delta F} |F|^{2\delta F-1}$; it follows that

$$\log D = O(\log d + \delta F \log(\delta F|F|)).$$

In order to give an upper bound for the height of $R(f,f')$, we use the result from [3]. Let A be a matrix having entries $A_{ij} = \sum_{\ell=0}^{\delta F-1} a_{ij\ell} T^{\ell} \in \mathbb{Z}[T]$, for $1 \le i,j \le m$, and some positive integer m. The determinant $d(A)$ of A is a polynomial of degree $\le m(\delta F-1)$ in $\mathbb{Z}[T]$. According to [3] the length, and therefore the height, of $d(A)$ is bounded from above by

$$(\prod_{j=1}^{m} \sum_{i=1}^{m} (\sum_{\ell=0}^{\delta F-1} |a_{ij\ell}|)^2)^{\frac{1}{2}}.$$

Using this bound it is easily proved that the height of $d(A)$ modulo F is bounded by

$$(\prod_{j=1}^{m} \sum_{i=1}^{m} (\sum_{\ell=0}^{\delta F-1} |a_{ij\ell}|)^2)^{\frac{1}{2}} (1+F_{max})^{(m-1)(\delta F-1)}.$$

It follows that

$$(R(f,f'))_{max} \le (\sqrt{n+1}\delta F f_{max})^{n-1} (\sqrt{n}\delta F n f_{max})^{n} (1+F_{max})^{(2n-2)(\delta F-1)},$$

where $R(f,f')$ is regarded as a polynomial in α. We find from the definition of D and p that

$$\prod_{q \text{ prime}, q<p} q \le d|\mathrm{discr}(F)|\,(R(df,df'))_{max}$$

and this yields in a similar way as in [7] that

$$p = O(\log d + n\delta F \log(\delta F|F|) + n\log n + n\log(df_{max})).$$

This implies that the computation of the prime number p, and the computation of the factorizations of $(F \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$ and $(f \bmod (p,H_1))$ in $\mathbb{F}_q[X]$ satisfy the estimates in (4.5). Theorem (4.5) now easily follows from the bounds on $\log D$ and p, and from the observation that a monic factor g of f in $\mathbb{Q}(\alpha)[X]$ satisfies $\log(g_{max}) = O(\delta F \log(\delta F|F|) + n + \log(f_{max}))$ (this follows from a bound similar to the one given in the proof of (3.11)). □

References.

1. E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comp. 24 (1970), 713-735.
2. W.S. Brown, The subresultant PRS algorithm, ACM Transactions on mathematical software 4 (1978), 237-249.
3. A.J. Goldstein, R.L. Graham, A Hadamard-type bound on the coefficients of a determinant of polynomials, SIAM Rev. 16 (1974), 394-395.
4. D.E. Knuth, The art of computer programming, vol. 2, Seminumerical algorithms, Addison Wesley, Reading, second edition 1981.
5. S. Landau, Factoring polynomials over algebraic number fields is in polynomial-time, unpublished manuscript, 1982.
6. A.K. Lenstra, Lattices and factorization of polynomials over algebraic number fields, Proceedings Eurocam 82, LNCS 144, 32-39.
7. A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), 515-534.
8. A.K. Lenstra, Factoring polynomials over algebraic number fields, Report IW 213/82, Mathematisch Centrum, Amsterdam 1982.
9. M. Mignotte, An inequality about factors of polynomials, Math. Comp. 28 (1974), 1153-1157.
10. P.J. Weinberger, L.P. Rothschild, Factoring polynomials over algebraic number fields, ACM Transactions on mathematical software 2 (1976), 335-350.
11. D.Y.Y. Yun, The Hensel lemma in algebraic manipulation, MIT, Cambridge 1974; reprint: Garland Publ. Co., New York 1980.