stichting
mathematisch
centrum

MC

AFDELING INFORMATICA IW 190/81 DECEMBER
(DEPARTMENT OF COMPUTER SCIENCE)

A.K. LENSTRA

LATTICES AND FACTORIZATION OF POLYNOMIALS

Preprint

kruislaan 413 1098 SJ amsterdam

Printed at the Mathematical Centre, 413 Kruislaan, Amsterdam.

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

1980 Mathematics subject classification: 10M05, 10E05, 68C25

Lattices and factorization of polynomials [*)]

by

A.K. Lenstra

ABSTRACT

We present a new algorithm to factorize polynomials over an algebraic number field. Unlike other algorithms the efficiency of our method does not depend on the irreducibility of the minimal polynomial modulo some prime. The algorithm is based on a theorem on integral lattices and a lower bound for the length of a polynomial having modulo p^k a non-trivial common divisor with the minimal polynomial. These theorems also enable us to formulate a new algorithm for factoring polynomials over the integers.

KEY WORDS & PHRASES: *Polynomial factorization, lattice theory, reduced basis, shortest vector*

[*)] This report will be submitted for publication elsewhere.

1. INTRODUCTION AND NOTATION

We present a new algorithm to factorize polynomials over an algebraic number field. The algebraic number field is given as the field of rational numbers extended by a root of a prescribed minimal polynomial. Unlike other algorithms the efficiency of our method does not depend on the irreducibility of the minimal polynomial modulo some prime.

A brief outline of our algorithm is as follows. First, we factorize the polynomial to be factored over a large enough ring determined by a prime power p^k and an irreducible factor of the minimal polynomial modulo p^k, using for instance the well-known Berlekamp-Hensel technique. We then construct a lattice such that the coefficients of the factors over the algebraic number field are congruent,modulo this lattice,to the coefficients of the factors over the ring. Using a theorem stating that these coefficients in the algebraic number field are the shortest-length vectors with this property, we are able to compute them, if a sufficiently orthogonal basis of the lattice can be found. That such a basis can be effectively constructed is a result of H.W. LENSTRA [3].

From the same theorem it follows that an irreducible polynomial over the integers with a given maximal length is uniquely determined by a factor modulo p^k, if k is sufficiently large. As a consequence we can compute this irreducible polynomial as the shortest-length vector in a lattice defined by p^k and the factor modulo p^k. This gives us a new algorithm to factorize polynomials over the integers.

The result from [3] on the computation of a reduced basis of a lattice is presented in Section 2, together with a number of elementary remarks about lattices. In Section 3 we prove a theorem giving a lower bound for the length of a polynomial having modulo p^k a non-trivial common divisor with an irreducible polynomial. As an application of this theorem we describe the new algorithms for factorization of polynomials over the integers and over algebraic number fields in Sections 4 and 5 respectively. The algorithm from Section 5 has been implemented in Algol 68 on a CDC-Cyber 170-750 computer; we include some machine examples with timings.

Throughout this paper we make no distinction between vectors and polynomials; an $(\ell+1)$-dimensional vector $v = (v_0,\ldots,v_\ell)^T$ corresponds to the polynomial $v(X) = \sum_{i=0}^{\underline{d}v} v_i X^i$, where $\underline{d}v$ denotes the degree of the polynomial v (here $\underline{d}v = -1$ if $v_i = 0$ for $i = 0,\ldots,\ell$, and $\underline{d}v = \max\{i \mid v_i \neq 0\}$ otherwise). Conversely a polynomial $v(X) = \sum_{i=0}^{n} v_i X^i$ corresponds to an $(\ell+1)$-dimensional vector $v = (v_0,\ldots,v_n,0,\ldots,0)^T$ for all $\ell \geq n$.

If $v = (v_0,\ldots,v_n) \in \mathbb{R}^{n+1}$, we denote by $[v]$ the vector $w = (w_0,\ldots,w_n) \in \mathbb{Z}^{n+1}$, such that w_i is the integer nearest to v_i for $i = 0,\ldots,n$, and where halves are rounded upwards, e.g. $[0.5] = 1$. Furthermore we put

$$\|v\| = (\sum_{i=0}^{n} v_i^2)^{1/2}$$

the *length* of v,

$$\ell c(v) = v_{\underline{d}v},$$

the *leading coefficient* of v (with $\ell c(v) = 0$ if $\underline{d}v = -1$), and if $v \in \mathbb{Z}^{n+1}$,

$$\mathrm{cont}(v) = \gcd(v_0,\ldots,v_n)$$

the *content* of v, and

$$pp(v) = v/\mathrm{cont}(v) = (v_0/\mathrm{cont}(v),\ldots,v_n/\mathrm{cont}(v))$$

the *primitive part* of v.

2. LATTICES

Let $b_0,\ldots,b_m \in \mathbb{Z}^{m+1}$ be $m+1$ linearly independent vectors for some positive integer m. The *lattice* L with basis $b_0,\ldots,b_m$ is defined as $L = \sum_{j=0}^{m} \mathbb{Z}\, b_j$. This lattice is uniquely determined by the basis $b_0,\ldots,b_m$; the converse however is not true as is illustrated in Figure 1.

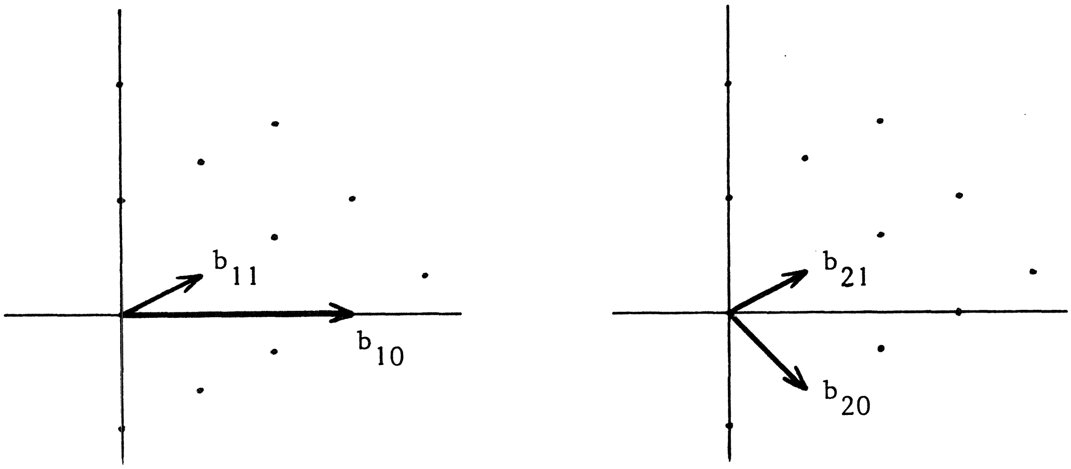

Figure 1. Two different bases generating the same lattice. $b_{10} = (6,0)^T$, $b_{11} = (2,1)^T$ and $b_{20} = (2,-2)^T$, $b_{21} = (2,1)^T$.

The *determinant* of a lattice is defined as $d(L) = |\det((b_i,b_j)_{i,j=0}^m)|^{\frac{1}{2}}$; its value is independent of the choice of the basis of L. By the *fundamental domain* of a basis $b_0,\ldots,b_m$ we mean the set

$$\{x \in \mathbb{R}^{m+1} \mid \exists c_j \in [-\tfrac{1}{2},\tfrac{1}{2}),\ j = 0,\ldots,m, \text{ such that } x = \textstyle\sum_{j=0}^m c_j b_j\}.$$

Clearly it is possible to determine for all $\tilde{x} \in \mathbb{R}^{m+1}$ a unique element x in the fundamental domain, such that $\tilde{x}$ and x are congruent modulo L. Putting $M = (b_0|\ldots|b_m)$, the $(m+1)\times(m+1)$ matrix with b_i, $i = 0,\ldots,m$, as columns, it is easily shown that $x = \tilde{x} - M\cdot[M^{-1}\cdot\tilde{x}]$ (cf. Figure 2).

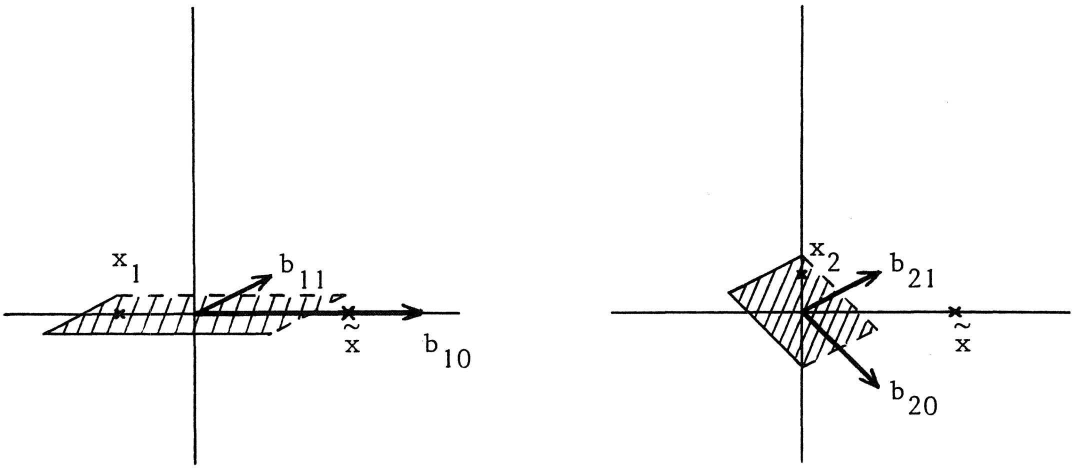

Figure 2. $\tilde{x} = (4,0)^T$, $x_1 = (-2,0)^T$, $x_2 = (0,1)^T$.

Remark that the volume of the fundamental domain equals d(L).

In the sequel the quotient $(\prod_{j=0}^{m}\|b_j\|)/d(L) = OD((b_0,\ldots,b_m)) = OD$ (where OD stands for *Orthogonality Defect*) will play an important role. By Hadamard's inequality we know that OD is always ≥ 1; there is however not an a priori upperbound for this quotient. The constructive proof of the following theorem from [3] provides us with an algorithm to construct a basis $b_0,\ldots,b_m$ of an arbitrary lattice, such that $OD((b_0,\ldots,b_m))$ is bounded from above by a constant depending only on the dimension of the lattice.

<u>THEOREM 1</u>. (Reduction Algorithm)
For any choice of $z \in (0,\frac{1}{2}\sqrt{3})$ *we can reduce an arbitrary basis of an* (m+1)-*dimensional lattice* L *to a basis* $b_0,\ldots,b_m \in \mathbb{Z}^{m+1}$ *of* L *satisfying*

$$1 \leq OD((b_0,\ldots,b_m)) \leq \left(\frac{4z^2+1}{4z^2}\right)^{\frac{(m+1)\cdot m}{4}} .$$

Unfortunately there is till now no better bound on the degree of the polynomial bounding the running time of the algorithm resulting from the proof of this theorem than an exponential function of the dimension of the lattice. For small dimensions (i.e. ≤ 10) however this appears to be no serious drawback. In the sequel we put

$$C = C(z,m+1) = \left(\frac{4z^2+1}{4z^2}\right)^{\frac{(m+1)\cdot m}{4}} .$$

In practice the value for z doesn't matter too much; all our applications of Theorem 1 resulted in bases satisfying $\mathrm{OD} \leq 2$. There exist lattices however for which the orthogonality defect is bounded from below by an exponential function of the dimension [5].

In Section 4 we need a method to determine the shortest vector $\neq 0$ in a given lattice. The algorithm given by DIETER [1] performs very well in practice, if the dimension of the lattice is reasonably small. For higher dimensions (i.e. ≥ 15) however the running time of this shortest vector algorithm becomes prohibitively long.

In Section 5 we have to do with lattices containing only large vectors $\neq 0$; we want to be able to construct a basis for such a lattice, such that the fundamental domain of this basis contains a sphere about the origin with a comparably large radius. That this is possible follows from Theorem 1 in combination with the following lemma.

LEMMA 1. *Let* L *be an*(m+1)*-dimensional lattice with bases* $b_0,\ldots,b_m$, *and let* $0 < B < \min_{0\leq j\leq m} \|b_j\|$. *Then the fundamental domain of* $b_0,\ldots,b_m$ *contains an* (m+1)*-dimensional sphere about the origin with radius* $> B/(2\cdot\mathrm{OD})$, *and all vectors* $\neq 0$ *in* L *have length* $> B/\mathrm{OD}$.

PROOF. Define for $i = 0,\ldots,m$ the m-dimensional lattice L_i in the m-dimensional hyperplane $V_i = \sum_{j=0,j\neq i}^{m} \mathbb{R}\, b_j$ as $L_i = \sum_{j=0,j\neq i}^{m} \mathbb{Z}\, b_j$. Let d_i denote the distance of V_i to V_i+b_i, then clearly we have $d_i = d(L)/d(L_i)$. By Hadamard's inequality we obtain

$$d(L_i) \leq \prod_{j=0,j\neq i}^{m} \|b_j\|,$$

and therefore

$$d_i \geq \|b_i\|\cdot d(L)/(\textstyle\prod_{j=0}^{m} \|b_j\|) > B/\mathrm{OD}((b_0,\ldots,b_m)).$$

Let $x = \sum_{i=0}^{m} c_i b_i$ be such that $\|x\| < d_i/2$ for $i = 0,\ldots,m$. This implies that $c_i < 1/2$ for $i = 0,\ldots,m$, so that x is contained in the fundamental domain of $b_0,\ldots,b_m$. The fundamental domain therefore contains a sphere about the origin with radius $> B/(2\cdot OD)$.

Suppose that there exists a non-zero v in L with $\|v\| < B/OD$. Then $-v/2$ and $v/2$ are both contained in the fundamental domain and congruent modulo L, which is a contradiction. □

Now, if we know that all vectors $\neq 0$ in a lattice have length $> B$, then we have a sphere with radius $> B/(2\cdot OD)$. Using Theorem 1, we get a theoretical lowerbound $B/(2\cdot C)$ and, in most cases, a practical lowerbound $B/4$ for the radius of the sphere contained in the fundamental domain of the reduced basis of the lattice.

In Section 4 we will see that the following simple corollary of Lemma 1 provides us with an alternative way to calculate in certain cases the shortest vector in a lattice.

COROLLARY 1. *If there exists a vector* $\neq 0$ *with length* $\leq B$ *in a lattice with basis* $b_0,\ldots,b_m$, *then there is a basis vector with length* $\leq B\cdot OD$.

PROOF. Suppose that $b_i > B\cdot OD$ for $i = 0,\ldots,m$. Then all vectors $\neq 0$ in L have length $> B\cdot OD/OD = B$ according to Lemma 1, which clearly gives a contradiction. □

If we know that all vectors $\neq 0$, linearly independent of the shortest vector v, have length $> \|v\|\cdot OD((b_0,\ldots,b_m))$, for some basis $b_0,\ldots,b_m$, then the basis vector with length $\leq \|v\|\cdot OD$ equals $\pm$ v.

3. A LOWER BOUND THEOREM

Let $g \in \mathbb{Z}[X]$ be an arbitrary polynomial of degree $n_1 \geq 1$, and let $v_k \in (\mathbb{Z}/p^k\mathbb{Z})[X]$, $k = 1,2,\ldots$, with $\underline{d}\, v_k = n_2 \geq 1$, where p is a prime. Suppose that g and v_k are relatively prime over $\mathbb{Z}$, but that there exists an integer $n \geq 1$ such that g and v_k have a monic common divisor of degree at least n modulo p^k, $k = 1,2,\ldots$.

We want to be able to give a lower bound for the length of the polynomials v_k, i.e. we want to prove that for all $B > 0$ we can find an index $k_0 = k_0(B)$ such that $\|v_k\| > B$ for all $k > k_0$. Furthermore, the proof has to give us a way to compute $k_0 = k_0(B)$, given a value for B. We do this by proving that

$$p^{k \cdot n} \leq \|g\|^{n_2} \cdot \|v_k\|^{n_1}, \quad k = 1,2,\ldots \; . \qquad (*)$$

Clearly this suffices for what we want, because given a value for B, we take

$$k_0 = k_0(B) = \lfloor \ell n(\|g\|^{n_2} \cdot \|B\|^{n_1})/(n \cdot \ell n(p)) \rfloor,$$

so that for $k > k_0$ we find

$$\|v_k\| \geq \left(\frac{p^{k \cdot n}}{\|g\|^{n_2}}\right)^{\frac{1}{n_1}} > \left(\frac{\|g\|^{n_2} \cdot \|B\|^{n_1}}{\|g\|^{n_2}}\right)^{\frac{1}{n_1}} = B.$$

Remark that from (*) it also follows that an irreducible polynomial over the integers with a given maximal length is uniquely determined by a factor modulo p^k, if k is sufficiently large. Namely, let g_1 and g_2 be two unequal irreducible polynomials with lengths $< B$ for some $B > 0$. Then g_1 and g_2 cannot have a monic common divisor of degree $n \geq 1$ modulo p^k for all k, because this would imply that

$$p^{k \cdot n} \leq \|g_1\|^{\underline{d}g_2} \cdot \|g_2\|^{\underline{d}g_1} \leq B^{\underline{d}g_1 + \underline{d}g_2} \quad \text{for } k = 1,2,\ldots,$$

which clearly is impossible. Therefore, g_1 is uniquely determined by a monic factor modulo p^k, if k is sufficiently large. We use this observation in Section 4.

We now formulate and proof our lower bound theorem.

<u>THEOREM 2</u>. *Let* f_1 *and* f_2 *be two relatively prime polynomials in* $\mathbb{Z}[X]$ *with* $n_1 = \underline{d}f_1 \geq n_2 = \underline{d}f_2 \geq 1$. *Let* p^k *be a prime power and* $n \geq 1$ *an integer such*

that f_1 *and* f_2 *have a monic common divisor* h_k *of degree* n, $1 \le n \le n_2$, *modulo* p^k. *Then* $p^{k \cdot n} \le \|f_1\|^{n_2} \cdot \|f_2\|^{n_1}$.

PROOF. Since $\gcd(f_1, f_2) = 1$ over $\mathbb{Z}$, we have that $a \cdot f_1 + b \cdot f_2 = 0$ if and only if $a = b = 0$, where $a, b \in \mathbb{Z}[X]$ and $\underline{d}a < n_2$, $\underline{d}b < n_1$. This implies that the collection

$$\tilde{b}_i = f_1 \cdot X^i \quad, \quad i = 0, \ldots, n_2-1,$$
$$\tilde{b}_i = f_2 \cdot X^{i-n_2}, \quad i = n_2, \ldots, n_1+n_2-1,$$

constitutes a basis of an (n_1+n_2)-dimensional lattice L contained in $\{\mathbb{Z} + \mathbb{Z} \cdot X + \ldots + \mathbb{Z} \cdot X^{n_1+n_2-1}\}$ with $d(L) \le \|f_1\|^{n_2} \cdot \|f_2\|^{n_1}$ (Hadamard's inequality). We define the (n_1+n_2)-dimensional lattice L_k as the lattice with the following basis:

$$b_i = p^k \cdot X^i \quad, \quad i = 0, \ldots, n-1,$$
$$b_i = h_k\, X^{i-n}, \quad i = n, \ldots, n_1+n_2-1.$$

It is clear that $b_0, \ldots, b_{n_1+n_2-1}$ are linearly independent and that $d(L_k) = p^{k \cdot n}$. Now remark that L_k equals the set of polynomials of degree $\le n_1+n_2-1$ having h_k as a factor modulo p^k, so that L is a sublattice of L_k. Therefore $d(L_k) \le d(L)$, which proves the theorem. □

4. FACTORIZATION OF POLYNOMIALS OVER THE INTEGERS

Let f be a squarefree polynomial over $\mathbb{Z}$. We present a method to determine irreducible factors of f over $\mathbb{Z}$, based on the results from the previous sections. First let us recall the well-known Berlekamp-Hensel algorithm to factorize f completely over $\mathbb{Z}$.

Algorithm 1. (Complete factorization in $\mathbb{Z}[X]$)

- Determine the irreducible factorization of f over a ring $\mathbb{Z}/p^k\mathbb{Z}$, for some prime $p \nmid \ell c(f) \cdot \mathrm{Discr}(f)$ and some sufficiently large integer k,

$$f \equiv \ell c(f) \cdot \Pi_{i=1}^{r}\, h_i \bmod p^k.$$

- For all subsets $S \subset \{1,2,\ldots,r\}$ test whether $pp((\ell c(f) \cdot \Pi_{i \in S} h_i) \bmod p^k)$ is a factor of f over $\mathbb{Z}$.

In practice this method performs very well, but since r, the number of irreducible factors modulo p, can be as large as $\underline{d}f$, the number of trial divisions in the second step can become exponential in the degree of f. This is due to the fact that in order to determine a factor over $\mathbb{Z}$, the right combination of factors modulo p^k has to be found. We present a method to determine an irreducible factor of f over $\mathbb{Z}$ using only one factor of f over some ring $\mathbb{Z}/p^k\mathbb{Z}$.

Let $h_k \in (\mathbb{Z}/p^k\mathbb{Z})[X]$ be a monic irreducible polynomial of degree n such that $h_k | f$ modulo p^k. Clearly, if $n = \underline{d}f$ then f is irreducible; therefore let $n < \underline{d}f$. If f is reducible over $\mathbb{Z}$, there exists for some $m \geq n$ an irreducible polynomial $g \in \mathbb{Z}[X]$ of degree m, such that $g|f$ over $\mathbb{Z}$ and $h_k | g$ modulo p^k. Now suppose that this g of degree m exists. We will see how we can construct g using only the factor h_k modulo p^k, if k is chosen sufficiently large. First we define a lattice L_k, such that g is contained in L_k. We then prove that it is possible to choose k in such a way that g is the shortest-length non-zero vector in L_k.

Define the (m+1)-dimensional lattice L_k generated by h_k and p^k as the lattice with the following basis:

$$b_i = p^k \cdot X^i, \qquad i = 0,\ldots,n-1,$$
$$b_i = h_k \cdot X^{i-n}, \qquad i = n,\ldots,m,$$

where the polynomials b_i for $i = 0,\ldots,m$ are regarded as (m+1)-dimensional vectors. Clearly $b_0,\ldots,b_m$ are linearly independent and $d(L_k) = p^{k \cdot n}$ (remember that h_k is monic).

It is clear from this definition that L_k equals the set of polynomials of degree $\leq m$ having h_k as a factor modulo p^k, and therefore g is contained in L_k.

Since $g|f$ over $\mathbb{Z}$, we know from MIGNOTTE [4] that, if $g = \sum_{i=0}^{m} g_i X^i$, then

$$|g_i| \leq \binom{m}{i} \cdot \|f\|, \qquad i = 0,\ldots,m,$$

and therefore

$$\|g\| \leq \left(\sum_{i=0}^{m}\binom{m}{i}^{2}\cdot\|f\|^{2}\right)^{\frac{1}{2}} = \sqrt{\binom{2m}{m}}\cdot\|f\| = B.$$

If we take k such that

$$B^{2\cdot m} < p^{k\cdot n} \qquad (*)$$

then we know from Theorem 2 that every polynomial in L_k that is not an integral multiple of g, has length > B. Namely, for $v \in L_k$ with $\gcd(g,v_k) = 1$, we have

$$\|v\| \geq \left(\frac{p^{k\cdot n}}{\|g\|^{\underline{d}v}}\right)^{\frac{1}{m}} > \left(\frac{B^{2\cdot m}}{B^{m}}\right)^{\frac{1}{m}} = B.$$

Therefore g is the shortest-length vector $\neq 0$ in L_k, and therefore g can be determined by a shortest vector algorithm.

Several remarks can be made on the above method. Since the value of m is unknown, it is possible to apply a shortest vector algorithm for $m = n, n+1, \ldots, \underline{d}f-1$ to the (m+1)-dimensional lattice generated by h_k and p^k, where k satisfies (*). If a vector is found with length $\leq B$, we test whether or not this vector is a factor of f over $\mathbb{Z}$; if there is no such vector, we know from the above reasoning that the guess for m is wrong. However, it is possible to choose for a given value of m a value for k, such that every vector $v \neq 0$ with length $\leq B$, that might be found, will satisfy $\gcd(f,v) \neq 1$. Furthermore g or some multiple of g will be determined as shortest vector, if the irreducible polynomial g with $h_k | g$ modulo p^k and $g|f$ over $\mathbb{Z}$ has degree $\leq m$. This follows by the same reasoning as above. It is therefore not necessary to guess the correct value for m; it is sufficient to choose a large enough m, and to use a sufficiently large k.

Another interesting remark is that we can apply Theorem 1 and Corollary 1 from Section 2. If we take k such that

$$B^{2\cdot m}\cdot C(z,m+1)^{m} < p^{k\cdot n},$$

for some choice of $z \in (0,\frac{1}{2}\sqrt{3})$, then every polynomial in L_k that is not an integral multiple of g has length $> C \cdot B$ (Theorem 2). Since L_k contains a vector $g \neq 0$ with length $\leq B$, we can effectively construct a basis of L_k containing a vector $b \neq 0$ with length $\leq C \cdot B$, according to Theorem 1 and Corollary 1. Therefore b is an integral multiple of g, and because b is an element of the basis of L_k, we have $b = \pm g$.

Experiments have shown that for small dimensions (i.e. ≤10) the running times of Dieter's shortest vector algorithm and of the reduction algorithm (Theorem 1) are almost equal. For larger dimensions however, the use of the shortest vector algorithm is preferable.

What can we say about the practical importance of this new factorization algorithm? Determination of a large degree irreducible factor requires the application of a shortest vector algorithm (or of the reduction algorithm) to a high-dimensional lattice; in Section 2 we have seen that it is not advisable to use these algorithms in that case. Therefore this method will in general not be very efficient.

On the other hand, suppose that we are given some polynomial f, and that we want to know all irreducible factors of f of degree ≤ m, for a certain value of m. First we compute the irreducible factorization of f modulo p^k for a prime p and a sufficiently large k (Berlekamp and quadratic Hensel). If we use the old 'combine and try' method, like in Algorithm 1, to determine the irreducible factors of degree ≤ m, then the computing time will be approximately $\Omega((\underline{d}f)^m)$ in the worst case. The new method, however, is linear in $\underline{d}f$; it takes at most $\underline{d}f$ applications of a shortest vector algorithm to an(m+1)-dimensional lattice. This implies that the new method is preferable if $\underline{d}f$ is large and m is small. There are other, similar examples where the above algorithm is of some practical importance.

We conclude this section with an example. Let

$$f = 96X^8 + 80X^7 - 156X^6 - 58X^5 + 101X^4 - 39X^3 - 29X^2 + 8X - 24.$$

Algorithm 1 will factorize f without problems into irreducible factors:

$$f = (12X^4+10X^3-9X^2+8)\cdot(8X^4-7X^2+X-3).$$

We show how we can get a factor of f using only one factor over $\mathbb{Z}/p^k\mathbb{Z}$. For instance, for $p = 5$ we find a factor $X+2$ over $\mathbb{Z}/5\mathbb{Z}$. We take for the example $k = 10$, so that we get a factor $X - 515858$ over $\mathbb{Z}/5^{10}\mathbb{Z}$. The initial basis of the 5-dimensional lattice generated by $X - 515858$ and 5^{10} is given by:

$$b_0 = \begin{pmatrix} 5^{10} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, b_1 = \begin{pmatrix} -515858 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, b_2 \begin{pmatrix} 0 \\ -515858 \\ 1 \\ 0 \\ 0 \end{pmatrix}, b_3 = \begin{pmatrix} 0 \\ 0 \\ -515858 \\ 1 \\ 0 \end{pmatrix}, b_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -515858 \\ 1 \end{pmatrix}.$$

We apply the reduction algorithm from Theorem 1 to this basis and we obtain:

$$b_0 = \begin{pmatrix} 0 \\ 23 \\ 5 \\ -43 \\ -3 \end{pmatrix}, b_1 = \begin{pmatrix} -24 \\ 5 \\ 16 \\ 13 \\ -1 \end{pmatrix}, b_2 = \begin{pmatrix} 19 \\ 12 \\ 7 \\ -2 \\ 16 \end{pmatrix}, b_3 = \begin{pmatrix} -3 \\ 1 \\ -7 \\ 0 \\ 8 \end{pmatrix}, b_4 = \begin{pmatrix} -5 \\ -8 \\ 13 \\ -10 \\ 17 \end{pmatrix}.$$

The shortest basis vector b_3 is indeed a factor of f over $\mathbb{Z}$. For $p = 23$, we find the factor $X^2 + 9X + 9$ of f modulo 23. Here we take $k = 5$, and the factor modulo $p^k = 23^5$ becomes $X^2 - 162095X + 1783475$. For the example we will have a look at the 6-dimensional lattice generated by $X^2 - 162095X + 1783475$ and 23^5; the initial basis is given by:

$$b_0 = \begin{pmatrix} 23^5 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, b_1 = \begin{pmatrix} 0 \\ 23^5 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, b_2 = \begin{pmatrix} 1783475 \\ -162095 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, b_3 = \begin{pmatrix} 0 \\ 1783475 \\ -162095 \\ 1 \\ 0 \\ 0 \end{pmatrix}, b_4 = \begin{pmatrix} 0 \\ 0 \\ 1783475 \\ -162095 \\ 1 \\ 0 \end{pmatrix},$$

$$b_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1783475 \\ -162095 \\ 1 \end{pmatrix}.$$

The reduced basis has the form:

$$b_0 = \begin{pmatrix} 285 \\ 327 \\ -197 \\ 186 \\ -487 \\ 339 \end{pmatrix}, b_1 = \begin{pmatrix} 8 \\ 0 \\ -9 \\ 10 \\ 12 \\ 0 \end{pmatrix}, b_2 = \begin{pmatrix} 0 \\ 8 \\ 0 \\ -9 \\ 10 \\ 12 \end{pmatrix}, b_3 = \begin{pmatrix} 114 \\ -287 \\ -431 \\ -275 \\ -184 \\ 139 \end{pmatrix}, b_4 = \begin{pmatrix} -296 \\ -378 \\ 154 \\ 179 \\ 149 \\ 271 \end{pmatrix}, b_5 = \begin{pmatrix} 296 \\ -40 \\ 269 \\ -8 \\ 16 \\ 5 \end{pmatrix},$$

and we see that we have found two equally short basis vectors b_1 and b_2, corresponding to a factor and a shifted factor of f respectively. In practice we modify the reduction algorithm in such a way that it stops as soon as a short enough basis vector is found. Remark that we could have used also a shortest vector algorithm.

5. FACTORIZATION OF POLYNOMIALS OVER ALGEBRAIC NUMBER FIELDS

Let $\mathbb{Q}(\alpha)$ be an algebraic number field where α denotes a zero of a monic irreducible polynomial F of degree m over $\mathbb{Z}$. The efficiency of existing methods to factorize polynomials over algebraic number fields strongly depends on the behaviour of the minimal polynomial F modulo some prime p. If a prime p can be found such that F is irreducible modulo p, and such that a few other, more trivial, conditions are met, there are no problems. In this case the algorithms are similar to algorithm 1 from Section 4; we will not discuss this case here (see [6] and [7]).

It can occur however, that the minimal polynomial factorizes modulo p for any prime p. This implies that the set

$$\left\{\sum_{i=0}^{m-1} a_i\alpha^i \mid a_i \in \mathbb{Z}/p\,\mathbb{Z}\, ,\ i = 0,\dots,m-1\right\}$$

cannot be regarded as the finite field $\mathbb{F}_{p^m}$, which gives considerable problems while factoring a polynomial f over $\mathbb{Q}(\alpha)$. WANG [6] solves these problems by transforming the factorization of f over $\mathbb{Q}(\alpha)$ into the factorization over $\mathbb{Z}$ of a multivariate polynomial of much higher degree. WEINBERGER and ROTHSCHILD [7] use the factorization of the minimal polynomial modulo p to define a number of finite fields over which f is factored using Berlekamp's methods. These factorizations of f are then combined using the Chinese Remainder Algorithm. If f has degree n and F has t factors modulo p, the worst case running time of this algorithm is $\Omega(2^{n\cdot t})$. We show that we can eliminate the use of the Chinese Remainder Algorithm at the cost of one reduction of an m-dimensional lattice. Besides the time necessary for this lattice reduction, the term $\Omega(2^{n\cdot t})$ in the running time then reduces to $\Omega(2^n)$. Although we know from Section 2 that the running time of the reduction algorithm increases extremely fast with growing dimension, it might be preferable to use it even for large dimensions, depending on the values of n and t.

Let $f \in (\mathbb{Q}(\alpha))[X]$ be the squarefree monic polynomial to be factored over $\mathbb{Q}(\alpha)$, and let $H_k \in (\mathbb{Z}/p^k\mathbb{Z})[X]$ be a monic irreducible non-trivial factor of the minimal polynomial F modulo p^k, for some prime $p \nmid \mathrm{Discr}(F)$ and $k = 1,2...$, such that $H_1 = H_k \bmod p$ for $k = 1,2,...$. We denote by α_k a zero of H_k for $k = 1,2,...$. The set

$$\left\{ \sum_{i=0}^{dH_1-1} a_i\alpha_1^i \mid a_i \in \mathbb{Z}/p\mathbb{Z}\ ,\ i = 0,\dots,\underline{d}H_1-1 \right\}$$

can be regarded as the finite field $\mathbb{F}_q$, where $q = p^{\underline{d}H_1}$. Using Berlekamp's algorithm for factorization of polynomials over finite fields, and the quadratic Hensel construction to lift a factorization, we get the complete factorization of f over $W_k(\mathbb{F}_q)$ for arbitrary $k \geq 1$ in, say, r irreducible factors, where

$$W_k(\mathbb{F}_q) = \left\{ \sum_{i=0}^{\underline{d}H_k-1} a_i\alpha_k^i \mid a_i \in \mathbb{Z}/p^k\mathbb{Z},\ i = 0,\dots,\underline{d}H_k-1 \right\}.$$

We use these r irreducible factors in $(W_k(\mathbb{F}_q))[X]$ to construct the irreducible factors of f over $\mathbb{Q}(\alpha)$.

Let $g \in (\mathbb{Q}(\alpha))[X]$ be one of the unknown irreducible factors of f over $\mathbb{Q}(\alpha)$. Without loss of generality we can assume that f and g are monic and in $(\frac{1}{D}\mathbb{Z}[\alpha])[X]$ for some integer $D \geq 1$ (D can be effectively computed using a method from [7]). For simplicity we take $D = 1$. From for instance WEINBERGER and ROTHSCHILD [7] we know that, if $g = \sum_{i=0}^{dg} v_iX^i \in (\mathbb{Z}[\alpha])[X]$, then there exists a constant $B > 0$, depending on f and F only, such that $\|v_i\| \leq B$ for $i = 0,\dots,\underline{d}g$ (here and in the sequel we regard coefficients in $\mathbb{Z}[\alpha]$ as polynomials in α). Of course, we can also use a heuristic bound on $\|v_i\|$ (see [6]). Furthermore, there exists among the 2^r factors of f modulo

H_k and p_k, which can be constructed (by multiplication over $W_k(\mathbb{F}_q)$), from the r irreducible factors of f over $(W_k(\mathbb{F}_q))[X]$, some factor g_k, such that $g_k = g \bmod(H_k,p^k) \in (W_k(\mathbb{F}_q))[X]$ (remark that we make here no distinction between α and α_k, and that we regard H_k as a polynomial in α). We now describe a mapping τ from $(W_k(\mathbb{F}_q))[X]$ to $(\mathbb{Z}[\alpha])[X]$, such that $\tau(g_k) = g$, if k is chosen sufficiently large. It follows that we can determine the complete factorization of f over $\mathbb{Q}(\alpha)$ by trying for all 2^r factors h of f modulo H_k and p^k whether or not $\tau(h)|f$ over $\mathbb{Q}(\alpha)$.

Let $v \in \mathbb{Z}[\alpha]$ be the i-th coefficient of g, so $\underline{d}v < m$, and let v_k be the i-th coefficient of g_k, for some $i \in \{0,\ldots,\underline{d}g\}$. Then $\|v\| \leq B$ and $v_k = v \bmod(H_k,p^k)$. Clearly, to define our mapping τ, it suffices to give a method to construct v given B and v_k. From $v_k = v \bmod(H_k,p^k)$ it follows that there exist polynomials w_1 and w_2 in $\mathbb{Z}[\alpha]$ such that

$$v = v_k + w_1 \cdot H_k + p^k \cdot w_2,\ \underline{d}w_1 = \underline{d}v - \underline{d}H_k \leq m - 1 - \underline{d}H_k,\ \underline{d}w_2 < \underline{d}H_k.$$

Therefore, v and v_k are congruent modulo the m-dimensional lattice L_k generated by H_k and p^k (see Section 4).

Now suppose that we can determine a basis $b_0,\ldots,b_{m-1}$ of L_k such that the fundamental domain of this basis contains an m-dimensional sphere about the origin with radius at least B. Together with $\|v\| \leq B$ this would imply that

$$v = v_k - M \cdot [M^{-1} \cdot v_k],$$

where $M = (b_0|\ldots|b_{m-1})$, because $v_k - M \cdot [M^{-1} \cdot v_k]$ is the unique element in the fundamental domain of $b_0,\ldots,b_{m-1}$ congruent to v_k modulo L_k (see Section 2).

We now prove that we indeed can construct such a basis of L_k, if k is chosen sufficiently large. Choose a value for $z \in (0,\frac{1}{2}\sqrt{3})$ and choose k such that

$$\|F\|^{m-1} \cdot (2 \cdot C(z,m+1) \cdot B)^m < p^{k \cdot \underline{d}H_k} \qquad (*)$$

Next apply Theorem 1 (the reduction algorithm) to L_k to obtain a basis

$b_0,\ldots,b_{m-1}$ of L_k satisfying

$$OD((b_0,\ldots,b_{m-1})) \leq C(z,m).$$

Let $w \neq 0$ be an arbitrary vector in L_k, then $\gcd(F,w) = 1$ over $\mathbb{Z}$ (remember that $\underline{d}H_k < m$ and that F is irreducible). Therefore Theorem 2 applies to F and w, so that

$$p^{k\cdot\underline{d}H_k} \leq \|F\|^{m-1}\cdot\|w\|^m.$$

Together with (*) this implies that $\|w\| > 2\cdot C\cdot B$. Clearly this lower bound also holds for b_j, $j = 0,\ldots,m-1$, so that application of Lemma 1 yields that the fundamental domain of $b_0,\ldots,b_{m-1}$ contains a sphere about the origin with radius $> 2\cdot C\cdot B/(2\cdot OD) \geq B$. This finishes our proof.

It is clear now how to define the mapping τ from $(W_k(\mathbb{F}_q))[X]$ to $(\mathbb{Z}[\alpha])[X]$; just apply the above construction to each of the coefficients of the polynomial in $(W_k(\mathbb{F}_q))[X]$.

Remark that the reduction algorithm from Theorem 1 has to be applied only once to compute the matrix M. Therefore, the computation of M, and of the first $\underline{d}H_k$ columns of M^{-1}, can be regarded as merely preprocessing.

In practice it is often possible to choose k considerably smaller than the theoretical value given by (*). This is due to the fact that the radius of the sphere contained in the fundamental domain of the reduced basis is almost always much larger than its theoretical lower bound. Therefore it is advisable to compute the orthogonality defect of the reduced basis of L_k for a reasonable value of k; if $\min_{j=0,\ldots,m-1}\|b_j\|/(2\cdot OD) > B$ the guess for k is correct, otherwise take a larger k. A reasonable guess is to take k such that

$$p^{(k\cdot\underline{d}H_k)/m} > 4\cdot B.$$

This follows from the following observations. In practice the vectors of the reduced basis $b_0,\ldots,b_{m-1}$ of L_k will have approximately the same length. The product of these lengths is bounded from below by $d(L_k) = p^{k\cdot\underline{d}H_k}$ (Hadamard's inequality), so $p^{(k\cdot\underline{d}H_k)/m}$ is a reasonable lower bound for the length of $b_j, j = 0,\dots,m-1$. Furthermore, we have seen in Section 2 that the reduced basis often satisfies $OD((b_0,\dots,b_{m-1})) \leq 2$. Combining these bounds with Lemma 1 we obtain a sphere with radius $p^{(k\cdot \underline{d}H_k)/m}/(2\cdot OD) \cong p^{(k\cdot \underline{d}H_k)/m}/4$. This radius is > B if k is chosen such that $p^{(k\cdot \underline{d}H_k)/m}/4 > B$. Remark here and in (*) the trade off between $\underline{d}H_k$ and k; a small degree factor of the minimal polynomial leads to a large value for k.

As an example we factorize a polynomial from Weinberger and Rothschild using the lattice algorithm (LA). Let

$$F(T) = T^6 + 3T^5 + 6T^4 + T^3 - 3T^2 + 12T + 16,$$

and let

$$f = X^3 - 3 \in (\mathbb{Q}(\alpha))[X],$$

where α denotes a zero of F. The minimal polynomial F has an irreducible factor $T^3 + T^2 - 2T + 3$ modulo 7. For the example we take k = 8, and we find a factor $T^3 - 1399040\ T^2 - 1399043\ T - 4$ of F modulo 7^8. Application of Berlekamp's factorization algorithm and of the quadratic-Hensel construction yields

$$\begin{aligned} f \equiv\ & (X-2387947\alpha-2387948)\cdot(X+2387948\alpha+1)\cdot \\ & (X-\alpha+2387947) \text{ modulo } (\alpha^3-1399040\alpha^2-1399043\alpha-4, 7^8). \end{aligned}$$

The initial basis of the 6-dimensional lattice generated by $\alpha^3 - 1399040\alpha^2 - 1399043\alpha - 4$ and $7^8 = 5764801$ is given by

$$\begin{pmatrix} 5764801 & 0 & 0 & -4 & 0 & 0 \\ 0 & 5764801 & 0 & -1399043 & -4 & 0 \\ 0 & 0 & 5764801 & -1399040 & -1399043 & -4 \\ 0 & 0 & 0 & 1 & -1399040 & -1399043 \\ 0 & 0 & 0 & 0 & 1 & -1399040 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Orthogonalization of this basis yields the following matrix:

$$\begin{pmatrix} 1265 & -1265 & -1059 & -1265 & 0 & -103 \\ 479 & -273 & -547 & 683 & 2530 & 34 \\ 547 & 547 & -137 & -34 & 752 & 1641 \\ -752 & -2017 & 2359 & -752 & 0 & -171 \\ -957 & -205 & -957 & -1231 & 1265 & 205 \\ -1299 & -1299 & -376 & 2051 & -752 & 376 \end{pmatrix} = M.$$

The highest power of α in the above factorization of f is one, so we have to compute only the first two columns of the inverse of M:

$$\begin{pmatrix} 2.5500\ 10^{-4} & 1.3045\ 10^{-4} & * & * & * & * \\ -2.8466\ 10^{-4} & -0.7112\ 10^{-4} & * & * & * & * \\ -1.8977\ 10^{-4} & 0.2996\ 10^{-4} & * & * & * & * \\ -0.9487\ 10^{-4} & 1.8977\ 10^{-4} & * & * & * & * \\ -0.9487\ 10^{-4} & 3.2022\ 10^{-4} & * & * & * & * \\ 0.3556\ 10^{-4} & -1.6011\ 10^{-4} & * & * & * & * \end{pmatrix} = M^{-1}.$$

Like Weinberger and Rothschild we use 12 as the denominator of the factors of f over $\mathbb{Q}(\alpha)$. The factorization of f modulo $\alpha^3 - 1399040\alpha^2 - 1399043\alpha - 4$ and 7^8 then becomes

$$f \equiv (X+(168641\alpha+168629)/12)\cdot(X-(168629\ -12)/12)\cdot$$
$$(X-(12\alpha+168641)/12).$$

Taking $v_k = 168641\alpha + 168629$, we compute $v = \tau(v_k)$ by putting $v = v_k - M\cdot[M^{-1}\cdot v_k]$. This gives $v = -\alpha^5 - 3\alpha^4 - 6\alpha^3 - 5\alpha^2 + 3\alpha - 12$, and $X-(\alpha^5+3\alpha^4+6\alpha^3+5\alpha^2-3\alpha+12)/12$ is a factor of f over $\mathbb{Q}(\alpha)$. In the same way we get $\tau(168629\alpha-12) = -2\alpha^5 - 4\alpha^4 - 8\alpha^3 + 2\alpha^2 - 8\alpha - 28$ and $\tau(12+168641) = \alpha^5 + \alpha^4 + 2\alpha^3 - 7\alpha^2 + 11\alpha + 16$, so that the complete factorization of f over $\mathbb{Q}(\alpha)$ becomes

$$\begin{aligned} f = {} & (X-(\alpha^5+3\alpha^4+6\alpha^3+5\alpha^2-3\alpha+12)/12)\cdot \\ & (X+(\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)/6)\cdot \\ & (X-(\alpha^5+\alpha^4+2\alpha^3-7\alpha^2+11\alpha+16)/12). \end{aligned}$$

Experiments have shown that the LA performs very well in practice. As we expected the use of this algorithm can be recommended, as long as the degree of the minimal polynomial is not too large. We compared it with a slightly modified (unpublished) version of the Weinberger-Rothschild algorithm (WRA) in the following way. To apply the LA we first determine a small prime p, such that the minimal polynomial F has an irreducible factor modulo p of small degree (i.e. 1 or 2); such a prime can easily be found. In contrast, for the WRA we look for a small prime p, such that F is irreducible modulo p. It is possible, however, that such a prime can not be found [2]; in that case we take p such that the number of irreducible factors of F modulo p is small (and $p \nmid \mathrm{Discr}(F)$). If $F_1,\dots,F_t$, with $\underline{d}F_1 \le \underline{d}F_2 \le \dots \le \underline{d}F_t$, are the irreducible factors of F modulo p^k, and f is the polynomial to be factored over $\mathbb{Q}(\alpha)$, it is often possible to derive a partial factorization of f modulo F_i and p^k for $i = 2,\dots,t$, from the factorization of f modulo F_1 and p^k. This is done by looking for a linear factor of F_1 modulo F_i and p^k for $i = 2,\dots,t$. This modification can decrease the running time of the WRA considerably.

In the examples below we denote by "new time" and "old time" the time taken by the LA and the time taken by this modified version of the WRA respectively; they both include the time taken to determine the value for p. Here we have to remark that we did not use the extremely large theoretical values for k, but a reasonable heuristic one. Examples number 1 and 4 come from Wang, numbers 8 and 9 come from a paper by KALTOFEN et al. [2].

EXAMPLES.

1) $f = X^2 + X - 1, \quad \alpha^2 - 5 = 0.$

$\alpha-4 \equiv 0$ modulo 11: new time 50 msec,
irreducible modulo 3: old time 124 msec.
factorization over $\mathbb{Q}(\alpha)$:

$$\frac{(2X+\alpha+1)\cdot(2X-\alpha+1)}{4}.$$

2) $f = \dfrac{47X^6+21X^5+598X^4+1561X^3+1198X^2+261X+47}{47}$, $\alpha^2 - \alpha + 3 = 0$.

$\alpha - 1 \equiv 0$ modulo 3: new time 143 msec,

irreducible modulo 7: old time 676 msec.

factorization over $\mathbb{Q}(\alpha)$:

$$\frac{(47X^3-(121\alpha-71)X^2-(121\alpha+70)X-47)\cdot(47X^3+(121\alpha-50)X^2+(121\alpha-191)X-47)}{2209} .$$

3) $f = X^6 - 2X^5 + 2X^3 - X - 1$, $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$.

$\alpha + 3 \equiv 0$ modulo 13: new time 183 msec,

irreducible modulo 2: old time 844 msec.

factorization over $\mathbb{Q}(\alpha)$:

$(X^2-(\alpha+1)X+\alpha^2+\alpha-1)\cdot(X^2+(\alpha^2+\alpha-2)X-\alpha^2+2)\cdot(X^2-(\alpha^2-1)X-\alpha)$.

4) $f = \dfrac{16X^6-1}{16}$, $\alpha^3 + 2 = 0$.

$\alpha^2 + 2\alpha - 1 \equiv 0$ modulo 5: new time 431 msec,

irreducible modulo 7: old time 511 msec.

factorization over $\mathbb{Q}(\alpha)$:

$$\frac{(4X^2+2\alpha X+\alpha^2)\cdot(4X^2-2\alpha X+\alpha^2)\cdot(2X-\alpha)\cdot(2X+\alpha)}{64} .$$

5) $f = X^8 - X^7 - X^6 + X^4 - X^2 + X + 1$, $\alpha^4 - \alpha + 1 = 0$.

$\alpha^3 - \alpha^2 + \alpha + 1 \equiv 0$ modulo 3: new time 1347 msec,

$\alpha + 1 \equiv 0$ modulo 3: new time 235 msec,

irreducible modulo 7: old time 2038 msec.

factorization over $\mathbb{Q}(\alpha)$:

$(X^6-(\alpha^3+\alpha^2+\alpha)X^5+(2\alpha^3+\alpha^2-3)X^4+(\alpha^3+2\alpha^2+2\alpha)X^3-(2\alpha^3+\alpha^2-3)X^2$
$-(\alpha^3+\alpha^2+\alpha)X-1)\cdot(X^2+(\alpha^3+\alpha^2+\alpha-1)X-1)$.

6) $f = X^5 - X^4 - 3X^3 + X^2 + 2X - 1$, $\alpha^5 + \alpha^3 - \alpha^2 + \alpha - 1 = 0$.

$\alpha^2 + \alpha - 1 \equiv 0$ modulo 3: new time 352 msec,

$\alpha + 1 \equiv 0$ modulo 5: new time 292 msec,

irreducible modulo 2: old time 1152 msec.

factorization over $\mathbb{Q}(\alpha)$:

$(X^4+(\alpha^4+\alpha^2)X^3+(\alpha^3+\alpha^2-2)X^2 - (\alpha^4-\alpha^3+\alpha^2-\alpha+1)X -\alpha^3+1)\cdot(X-\alpha^4-\alpha^2-1)$.

7) $f = X^3 - 3$, $\alpha^6 + 3\alpha^5 + 6\alpha^4 + \alpha^3 - 3\alpha^2 + 12\alpha + 16 = 0$.
$\alpha^2 - 2\alpha - 1 \equiv 0$ modulo 5: new time 564 msec,
2 factors modulo 7: old time 814 msec.
factorization over $\mathbb{Q}(\alpha)$:

$$\frac{(12X-\alpha^5-3\alpha^4-6\alpha^3-5\alpha^2+3\alpha-12)\cdot(6X+\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)\cdot(12X-\alpha^5-\alpha^4-2\alpha^3+7\alpha^2-11\alpha-16)}{864}.$$

8) $f = X^6 + 9X^5 + 36X^4 + 77X^3 + 90X^2 + 63X + 31$,
$\alpha^6 + 3\alpha^5 + 6\alpha^4 + 3\alpha^3 + 9\alpha + 9 = 0$.
$\alpha^2 - \alpha + 2 \equiv 0$ modulo 5: new time 1191 msec,
2 factors modulo 7: old time 2789 msec.
factorization over $\mathbb{Q}(\alpha)$:
$(X^5+(\alpha+8)X^4+(\alpha^2+7\alpha+28)X^3+(\alpha^3+6\alpha^2+21\alpha+49)X^2+(\alpha^4+5\alpha^3+15\alpha^2+28\alpha+41)X +$
$\alpha^5+4\alpha^4+10\alpha^3+13\alpha^2+13\alpha+22)\cdot(X-\alpha+1)$.

9) $f = X^9 + 9X^8 + 36X^7 + 69X^6 + 36X^5 - 99X^4 - 303X^3 - 450X^2 - 342X - 226$,
$\alpha^9 - 15\alpha^6 - 87\alpha^3 - 125 = 0$
$\alpha^3 - \alpha + 2 \equiv 0$ modulo 7: new time 2816 msec,
3 factors modulo 7: old time 59183 msec,
factorization over $\mathbb{Q}(\alpha)$:
$(X^6+6X^5+15X^4+(\alpha^3+5)X^3+(3\alpha^3-30)X^2+(3\alpha^3-39)X+\alpha^6-14\alpha^3-101)\cdot(X^2+(\alpha+2)X+\alpha^2+\alpha+1)\cdot$
$(X-\alpha+1)$.

10) $f = X^8 - 2X^7 + X^6 + 3X^5 - 4X^4 + X^3 + 2X^2 - 2X + 1$,
$\alpha^8 - 2\alpha^7 + 3\alpha^6 - 3\alpha^5 + \alpha^4 + 1 = 0$.
$\alpha^3 + \alpha^2 - 2\alpha - 3 \equiv 0$ modulo 7: new time 2011 msec,
irreducible modulo 5: old time 6295 msec.
factorization over $\mathbb{Q}(\alpha)$:
$(X^7-(\alpha^7-2\alpha^6+2\alpha^5-2\alpha^4+\alpha^2+2)X^6+(\alpha^7-3\alpha^6+4\alpha^5-4\alpha^4+\alpha^3+2\alpha^2-2\alpha+1)X^5 -$
$(\alpha^5-\alpha^4+\alpha^2-3\alpha-1)X^4-(\alpha^7-3\alpha^6+3\alpha^5-4\alpha^4+2\alpha^3+\alpha+2)X^3+(\alpha^7-3\alpha^6+5\alpha^5-6\alpha^4+3\alpha^2-2\alpha+1)X^2$
$-(\alpha^7-2\alpha^6+4\alpha^5-4\alpha^4+2\alpha^3-2\alpha)X+\alpha^5-\alpha^4+\alpha^3-\alpha)\cdot(X+\alpha^7-2\alpha^6+2\alpha^5-2\alpha^4+\alpha^2)$.

The new algorithm is on the average more than two times as fast as the WRA, even in the case that the minimal polynomial is irreducible modulo some small prime. This is due to the fact that the costs of elementary operations like +,-,* and of the algorithms for factorization of polynomials over finite fields (Berlekamp, Rabin) grow rapidly with the size of the field. In the LA we choose the prime in such a way that we only have to do with small finite fields; in the WRA we have either a number (>1) of (small) finite fields, or we have one large finite field.

In Section 4 we used a shortest vector algorithm to determine factors over $\mathbb{Z}$; here we use a shortest congruent algorithm to determine coefficients of factors over $\mathbb{Q}(\alpha)$. Notice however, that factors in $(\mathbb{Q}(\alpha))[X]$ can also be found using a shortest vector algorithm. We illustrate this with an example. Let $H(T) = T^2 + t_1T + t_0$ be an irreducible factor of $F(T)$ modulo p^k, with $\underline{d}F = 4$. Furthermore, let $h(X) = X^2 + (x_{11}\alpha+x_{10})X + x_{01}\alpha+x_{00}$ be an irreducible factor of f modulo $H(\alpha)$ and p^k. Suppose that f has over $\mathbb{Q}(\alpha)$ an irreducible factor of degree 3 with divisor $h(X)$ modulo $H(\alpha)$ and p^k. This factor can then be determined as the shortest vector in the following lattice, if k is chosen sufficiently large:

$$\begin{pmatrix}
p^k & 0 & t_0 & 0 & 0 & \cdots & \cdots & 0 & x_{00} & 0 & 0 & \cdots & 0 \\
0 & p^k & t_1 & t_0 & \vdots & & & \vdots & x_{01} & x_{00} & \vdots & & \vdots \\
\vdots & \ddots & 1 & t_1 & \vdots & & & \vdots & 0 & x_{01} & \vdots & & \vdots \\
\vdots & & \ddots & 1 & 0 & \cdots & \cdots & 0 & 0 & 0 & \vdots & 0 & 0 \\
\vdots & & & \ddots & p^k & 0 & t_0 & 0 & x_{10} & 0 & \vdots & \vdots & x_{00} \\
\vdots & & & & \ddots & p^k & t_1 & t_0 & x_{11} & x_{10} & \vdots & \vdots & x_{01} \\
\vdots & & & & & \ddots & 1 & t_1 & 0 & x_{11} & \vdots & \vdots & 0 \\
\vdots & & & & & & \ddots & 1 & 0 & 0 & 0 & 0 & 0 \\
\vdots & & & & & & & \ddots & 1 & 0 & t_0 & 0 & x_{10} \\
\vdots & & & & & & & & \ddots & 1 & t_1 & t_0 & x_{11} \\
\vdots & & & & & & & & & \ddots & 1 & t_1 & 0 \\
\vdots & & & & & & & & & & \ddots & 1 & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1
\end{pmatrix}$$

If n is the degree of the factor we are looking for, then $n\cdot\underline{d}F + 1$ is the dimension of this lattice ($(n+1)\cdot\underline{d}F$ if we are looking for a non-monic factor). Clearly this method is rather impractical if n or $\underline{d}F$ is large.

Throughout Section 5 we have restricted ourselves to univariate polynomials ; remark that the lattice approach equally well applies to the multivariate case (see for instance WANG [6]).

Acknowledgement

I am indebted to H.W. LENSTRA Jr., who suggested the lattice approach to me, and to P. VAN EMDE BOAS for his many helpful comments.

REFERENCES

[1] DIETER, U., *How to calculate shortest vectors in a lattice,* Math. Comp. 29 (1975), 827-833.

[2] KALTOFEN, E., D.R. MUSSER, B.D. SAUNDERS, *A generalized class of polynomials that are hard to factor,* Proc. of ACM Symposium on Symbolic and Algebraic Computation, Snowbird, Utah, August 5-7, 1981.

[3] LENSTRA, H.W. Jr., *Integer programming with a fixed number of variables,* University of Amsterdam, Department of Mathematics, Report 81-03.

[4] MIGNOTTE, M., *An inequality about factors of polynomials*, Math. Comp. 28 (1974), 1153-1157.

[5] MILNOR, J., D. HUSEMOLLER, *Symmetric Bilinear Forms*, Springer Ergebnisse der Mathematik und ihr Grenzgebiete 73 Berlin etc. 1973.

[6] WANG, P.S., *Factoring multivariate polynomials over algebraic number fields,* Math. Comp. 30 (1976), 324-336.

[7] WEINBERGER, P.J., L.P. ROTHSCHILD, *Factoring polynomials over algebraic number fields*, ACM Transactions on Mathematical Software 2 (1976), 335-350.