Lattices and Factorization of Polynomials over Algebraic Number Fields

(Extended Abstract)

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

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. 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 [4], which 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 algorithm for factorization of polynomials over algebraic number fields in Section 4; we include some machine examples with timings. In Section 5 we make some final remarks on our new method, and we show that the theorem from Section 3 can also be used to formulate a new algorithm for factoring in $\mathbb{Z}[X]$.

Throughout this paper we make no distinction between vectors and polynomials; an m-dimensional vector $v = (v_0,\ldots,v_{m-1})^T$ corresponds to the polynomial $v(X) = \Sigma_{i=0}^{\underline{dv}} v_i X^i$, where $\underline{dv}$ denotes the degree of the polynomial v (here $\underline{dv} = -1$ if $v_i = 0$ for $i = 0,\ldots,m-1$, and $\underline{dv} = \max\{ i \mid v_i \neq 0 \}$ otherwise). Conversely a polynomial $v(X) = \Sigma_{i=0}^{\ell} v_i X^i$ corresponds to an m-dimensional vector $v = (v_0,\ldots,v_\ell,0,\ldots,0)^T$ for all $m > \ell$. If $v = (v_0,\ldots,v_{m-1})^T \in \mathbb{R}^m$, we denote by $[v]$ the vector $w = (w_0,\ldots,w_{m-1})^T \in \mathbb{Z}^m$, such that w_i is the integer nearest to v_i for $i = 0,\ldots,m-1$, and where halves are rounded upwards, e.g. $[0.5] = 1$. Furthermore we put $\|v\| = (\Sigma_{i=0}^{m-1} v_i^2)^{\frac{1}{2}}$, the *length* of v.

2. Lattices.

Let $b_0,\ldots,b_{m-1} \in \mathbb{Z}^m$ be m linearly independent vectors. The *lattice* L with basis $b_0,\ldots,b_{m-1}$ is defined as $L = \sum_{j=0}^{m-1} \mathbb{Z} b_j$. Putting $M = (b_0|\ldots|b_{m-1})$, the m×m matrix with b_j, $j = 0,\ldots,m-1$, as columns, we define the *determinant* of L as $d(L) = |\det((b_i,b_j)_{i,j=0}^{m-1})|^{\frac{1}{2}} = |\det(M)|$; the value of d(L) is independent of the choice of the basis of L. By the *fundamental domain* of $b_0,\ldots,b_{m-1}$ we denote the set $\{x \in \mathbb{R}^m \mid \exists c_j \in [-\frac{1}{2},\frac{1}{2}),\ j = 0,\ldots,m-1,$ such that $x = \sum_{j=0}^{m-1} c_j b_j\}$. For all $\tilde{x} \in \mathbb{R}^m$ there exists a unique element $x = \tilde{x} - M \cdot [M^{-1} \cdot \tilde{x}]$ in the fundamental domain, such that x and $\tilde{x}$ are congruent modulo L.

A measure of the orthogonality of a basis $b_0,\ldots,b_{m-1}$ is given by the *orthogonality defect* OD: $OD(b_0,\ldots,b_{m-1}) = \prod_{j=0}^{m-1} \|b_j\|/d(L)$. From Hadamard's inequality we know that $OD \geq 1$, but there is no a priori upper bound for OD. In [4] an algorithm is given to construct a basis for an arbitrary lattice such that the orthogonality defect of this basis is bounded from above by a constant depending on the dimension of the lattice only.

Theorem 1. (Reduction Algorithm) For any choice of $z \in (0,\frac{1}{2}\sqrt{3})$ we can reduce an arbitrary basis of an m-dimensional lattice L to a basis $b_0,\ldots,b_{m-1} \in \mathbb{Z}^m$ of L satisfying $1 \leq OD(b_0,\ldots,b_{m-1}) \leq (\frac{4z^2+1}{4z^2})^{m\cdot(m-1)/4}$. □

The running time of this algorithm is exponential in the dimension of the lattice; for small dimensions (i.e. ≤ 10) this appears to be no serious drawback. In the sequel we put $C = C(z,m) = (\frac{4z^2+1}{4z^2})^{m\cdot(m-1)/4}$. In practice the value for z doesn't matter too much; all our applications of Theorem 1 resulted in bases satisfying OD < 2 (which is however certainly not always possible).

It is intuitively clear that the radius of the largest sphere contained in the fundamental domain is proportional to 1/OD. The following lemma makes this more precise.

Lemma 1. Let $0 < B < \min_{0 \leq j < m} \|b_j\|$. The fundamental domain of $b_0,\ldots,b_{m-1}$ contains an m-dimensional sphere about the origin with radius > B/(2·OD), and all vectors ≠ 0 in L have length > B/OD. □

It follows that if all vectors ≠ 0 in an arbitrary lattice have length > B, we can construct a basis such that the fundamental domain of this basis contains a sphere about the origin with radius at least B/(2·C).

3. A lower bound theorem.

Let $F \in \mathbb{Z}[T]$ be an irreducible polynomial of degree m, and let $H_k \in (\mathbb{Z}/p^k\mathbb{Z})[T]$ be a monic factor of degree ℓ, $1 \leq \ell < m$, of F modulo p^k, for some prime power p^k. We define the m-dimensional lattice L_k generated by H_k and p^k as the lattice with the following basis: $b_i = p^k \cdot T^i$, $i = 0,\ldots,\ell-1$,
$b_i = H_k \cdot T^{i-\ell}$, $i = \ell,\ldots,m-1$.
Here the polynomials b_i are regarded as m-dimensional vectors. Clearly $b_0,\ldots,b_{m-1}$ are linearly independent and $d(L_k) = p^{k\cdot\ell}$. Remark that L_k equals the set of polynomials of degree < m having H_k as a factor modulo p^k.

We prove that for all B > 0 we can find an index $k_0 = k_0(B)$, such that the fundamental domain of the reduced basis of L_k contains a sphere with radius > B, for all $k \geq k_0$. We do this by proving that the lengths of the vectors ≠ 0 in L_k can be bounded from below by a monotone increasing function of k.

Theorem 2. Let $V_k \neq 0$ be an arbitrary vector in L_k, regarded as polynomial in $\mathbb{Z}[T]$ of degree $n < m$, then $p^{k\cdot\ell} \leq \|F\|^n \cdot \|V_k\|^m \leq \|F\|^{m-1} \cdot \|V_k\|^m$.

Proof. Since F is irreducible over $\mathbb{Z}$ and $n < m$, we have that $\gcd(F,V_k) = 1$ over $\mathbb{Z}$, and therefore $G_1 \cdot F + G_2 \cdot V_k = 0$ if and only if $G_1 = G_2 = 0$, where $G_1,\ G_2 \in \mathbb{Z}[T]$ and $\underline{d}G_1 < n$, $\underline{d}G_2 < m$. This implies that the collection

$\tilde{b}_i = F \cdot T^i$, $i = 0,\ldots,n-1$,
$\tilde{b}_i = V_k \cdot T^{i-n}$, $i = n,\ldots,n+m-1$,

constitutes a basis of an (n+m)-dimensional lattice L contained in $\{\mathbb{Z} + \mathbb{Z}\cdot T + \ldots + \mathbb{Z}\cdot T^{n+m-1}\}$ with $d(L) \leq \|F\|^n \cdot \|V_k\|^m$ (Hadamard's inequality). The polynomials F and V_k both have the monic polynomial H_k as a factor modulo p^k, and therefore the lattice L is a sublattice of the (n+m)-dimensional lattice L_k' generated by H_k and p^k, so that

$d(L_k') = p^{k\cdot\ell} \leq d(L) \leq \|F\|^n \cdot \|V_k\|^m$. □

Remark that up to the constant factor, the lower bound $\|F\|^{-(m-1)/m} \cdot p^{(k\cdot\ell)/m}$ for elements in L_k is the best possible. This follows from Theorem 1, namely there exists a basis $b_0,\ldots,b_{m-1}$ of L_k such that $\prod_{j=0}^{m-1} \|b_j\| \leq C(z,m) \cdot p^{k\cdot\ell}$. Therefore there is a basisvector b_i satisfying $\|b_i\| \leq C(z,m)^{1/m} \cdot p^{(k\cdot\ell)/m}$.

It follows from Theorem 2, and from the results of the previous section, that in order to obtain a sphere with radius B, we should take k such that

$$\|F\|^{m-1} \cdot (2 \cdot C(z,m) \cdot B)^m < p^{k\cdot\ell}. \qquad (*)$$

We are now able to solve the following problem. Given a value B > 0 and a polynomial $\tilde{w} \in \mathbb{Z}[T]/H_k$ where k satisfies (*), determine if possible a polynomial $w \in \mathbb{Z}[T]/F$ such that $\|w\| \leq B$ and such that $\tilde{w}$ and w are congruent modulo H_k and p^k. Clearly, if w exists then w is unique and $w = \tilde{w} - M \cdot [M^{-1} \cdot \tilde{w}]$, where M is the matrix of the reduced basis of L_k. Remark that if we have a number of polynomials $\tilde{w}$, we only have to compute M and (the first ℓ columns of) M^{-1} once.

4. Factorization in $(\mathbb{Q}(\alpha))[X]$.

We are ready to present our new algorithm for factoring 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 $\mathbb{Z}$.

Lattice algorithm (LA).
Given a square-free monic polynomial $f \in (\mathbb{Q}(\alpha))[X]$ of degree n, this algorithm computes the irreducible factors of f over $\mathbb{Q}(\alpha)$.

1) Determine $D \in \mathbb{N}$, such that f and the factors of f are in $(\frac{1}{D}\mathbb{Z}[\alpha])[X]$.
2) Choose a prime p such that
   - $p \nmid D$,

- F remains square-free modulo p,
- F has a non-trivial monic irreducible factor H_1 of degree ℓ modulo p,
- f remains square-free modulo H_1 and p.

3) Choose B such that B/D is an upper bound for the length of the coefficients (in $\frac{1}{D}\mathbb{Z}[\alpha]$) of the factors of f over $\mathbb{Q}(\alpha)$.

4) Take $k \in \mathbb{N}$ minimal such that (*) holds, and determine the monic irreducible factor H_k of degree ℓ of F modulo p^k, such that $H_k \equiv H_1$ modulo p.

5) Determine the complete factorization of f modulo H_k and p^k:
$(D^{-1} \bmod p^k)\cdot(D\cdot f) \equiv \prod_{i=1}^{r} h_i$ modulo (H_k, p^k).

6) If r = 1 then f is irreducible. Otherwise compute M, the matrix of the reduced basis of the m-dimensional lattice L_k generated by H_k and p^k. Compute the polynomial $\tilde{h} = ((D\cdot\prod_{i\in S} h_i) \text{ modulo } (H_k, p^k)) = \sum_{i=0}^{\underline{d\tilde{h}}} \tilde{v}_i X^i$ for all subsets $S \subset \{1,\ldots,r\}$ such that $\underline{d\tilde{h}} \le \lfloor n/2 \rfloor$, and test whether
$h = \frac{1}{D}\cdot(\sum_{i=0}^{\underline{dh}} (\tilde{v}_i - M\cdot[M^{-1}\cdot\tilde{v}_i])X^i) \in (\frac{1}{D}\mathbb{Z}[\alpha])[X]$
is a factor of f over $\frac{1}{D}\mathbb{Z}[\alpha]$.

The values of D and B in Steps 1) and 3) can be determined using methods from [9]. The theoretical value for B is often much too large; it is in general advisable to use a heuristic bound [3,7]. The factorization of f modulo H_k and p^k is computed in the usual way; first factorize f modulo H_1 and p using for instance the Cantor-Zassenhaus algorithm [1] for factorization over finite fields (after Step 2), exit if r = 1), next apply Zassenhaus' quadratic lift-algorithm [10,11] to obtain the factors modulo H_k and p^k. It follows from Section 3 that the fundamental domain of the reduced basis of L_k contains the coefficients of the factors of f over $\mathbb{Q}(\alpha)$ (multiplied by D). These factors can therefore be determined as described in Step 6). Remark that all integers occurring in the LA are in absolute value $< p^{2k}$.

In practice we replace C(z,m) in (*) by 2, thus obtaining a smaller value for k. If the orthogonality defect of the reduced basis of L_k turns out to be too large (i.e. $\min_{0\le j<m} \|b_j\|/(2\cdot OD(b_0,\ldots,b_{m-1})) < B$) we try again with a larger k, but in most cases OD will be small enough.

As an example we factorize a polynomial from Weinberger and Rothschild [9] using the LA. Let $F(T) = T^6+3T^5+6T^4+T^3-3T^2+12T+16$ (m = 6), and let $f = X^3-3 \in (\mathbb{Q}(\alpha))[X]$ (n = 3), where α denotes a zero of F.

1) Like Weinberger and Rothschild we use D = 12 as the denominator of the factors of f over $\mathbb{Q}(\alpha)$.

2) The prime p = 7 satisfies the conditions; we find $H_1 = T^3+T^2-2T+3$ and $\ell = 3$.

3) We know from Weinberger and Rothschild that 40/12 is an upper bound for the length of the coefficients of the factors of f, so we take B = 40.

4) We replace C(z,6) in (*) by 2 and we take k minimal such that $(\sqrt{456})^5\cdot(2\cdot2\cdot40)^6 < 7^{k\cdot3}$, so we find k = 8, and $H_8 = T^3-1399040T^2-1399043T-4$.

5) $f \equiv (X-2387947\alpha-2387948)\cdot(X+2387948\alpha+1)\cdot(X-\alpha+2387947)$ modulo $(\alpha^3-1399040\alpha^2-1399043\alpha-4,\ 7^8)$.

6) Application of Theorem 1 to L_8 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 orthogonality defect of this basis is $(\prod_{i=0}^{5}\|b_i\|)/7^{8\cdot3} = 1.4 < 2$, so k is large enough. Remark that according to Lemma 1 the radius of the sphere contained in the fundamental domain of this basis is at least $\lfloor \min_{i=0,\ldots,5} \|b_i\|/(2\cdot OD) \rfloor > 600$.

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:

$$\begin{pmatrix} 2.5500\ 10^{-4} & 1.3045\ 10^{-4} & * & * & * & * \\ -2.8466\ 10^{-4} & -0.7112\ 10^{-4} & * & * & * & * \\ -1.8977\ 10^{-4} & 0.2966\ 10^{-4} & * & * & * & * \\ -0.9489\ 10^{-4} & 1.8977\ 10^{-4} & * & * & * & * \\ -0.9489\ 10^{-4} & 3.2022\ 10^{-4} & * & * & * & * \\ 0.3556\ 10^{-4} & -1.6011\ 10^{-4} & * & * & * & * \end{pmatrix} = M^{-1}.$$

First we take $S = \{1\}$: $\tilde{h} = (12\cdot(X-2387947\alpha-2387948)) \text{ modulo } (H_8, 7^8) = 12X+168641\alpha+168629 = \tilde{v}_1X+\tilde{v}_0$. Now reduce these coefficients modulo the reduced basis of L_8: $h = \frac{1}{12}\cdot\sum_{i=0}^{1}(\tilde{v}_i - M\cdot[M^{-1}\cdot\tilde{v}_i])X^i = X-(\alpha^5+3\alpha^4+6\alpha^3+5\alpha^2-3\alpha+12)/12$, and indeed h is a factor of f over $\mathbb{Q}(\alpha)$. For $S = \{2\}$ we find the factor $X+(\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)/6$, so that the complete factorization of f over $\mathbb{Q}(\alpha)$ becomes $f = (X-(\alpha^5+3\alpha^4+6\alpha^3+5\alpha^2-3\alpha+12)/12)\cdot(X+(\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)/6)\cdot(X-(\alpha^5+\alpha^4+2\alpha^3-7\alpha^2+11\alpha+16)/12)$.

We implemented the LA and the algorithm as described by Weinberger and Rothschild [9] (WRA) in Algol 68 on a CDC-Cyber 170-750 computer (we didn't implement the methods described in [5,6,7]). Below we give a number of machine examples; we denote by "new time" and "old time" the time taken by the LA and the time taken by the WRA respectively (in milliseconds).

1) $f = \frac{1}{47}(47X^6+21X^5+598X^4+1561X^3+1198X^2+261X+47)$, $\alpha^2-\alpha+3 = 0$.
$\alpha-1 \equiv 0$ modulo 3: new time 143 msec,
irreducible modulo 7: old time 676 msec.
factorization over $\mathbb{Q}(\alpha)$:
$\frac{1}{2209}(47X^3-(121\alpha-71)X^2-(121\alpha+70)X-47)\cdot(47X^3+(121\alpha-50)X^2+(121\alpha-191)X-47)$.

2) $f = \frac{1}{16}(16X^6-1)$, $\alpha^3+2 = 0$.
$\alpha^2+2\alpha-1 \equiv 0$ modulo 5: new time 431 msec,
irreducible modulo 7: old time 511 msec.
factorization over $\mathbb{Q}(\alpha)$:
$\frac{1}{64}(4X^2+2\alpha X+\alpha^2)\cdot(4X^2-2\alpha X+\alpha^2)\cdot(2X-\alpha)\cdot(2X+\alpha)$.

3) $f = X^8-X^7-X^6+X^4-X^2+X+1$, $\alpha^4-\alpha+1 = 0$.
$\alpha^3-\alpha^2+\alpha+1 \equiv 0$ 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 $\mathbb{Q}(\alpha)$:
$(X^6-(\alpha^3+\alpha^2+\alpha)X^5+(2\alpha^3+\alpha^2-3)X^4+(\alpha^3+2\alpha^2+2\alpha)X^3-(2\alpha^3+\alpha^2-3)X^2-(\alpha^3+\alpha^2+\alpha)X-1)\cdot(X^2+(\alpha^3+\alpha^2+\alpha-1)X-1)$.

4) $f=X^3-3$, $\alpha^6+3\alpha^5+6\alpha^4+\alpha^3-3\alpha^2+12\alpha+16=0$.
$\alpha^2-2\alpha-1 \equiv 0$ modulo 5: new time 564 msec,
two factors modulo 7: old time 814 msec.
factorization over $\mathbb{Q}(\alpha)$:
$\frac{1}{864}(12X-\alpha^5-3\alpha^4-6\alpha^3-5\alpha^2+3\alpha-12)\cdot(6X+\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)\cdot(12X-\alpha^5-\alpha^4-2\alpha^3+7\alpha^2-11\alpha-16)$.

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

5. Remarks.

From the examples in the previous section we conclude that, as we expected, the use of the LA can be recommended, as long as the degree of the minimal polynomial is not too large. Even in the case that the minimal polynomial remains irreducible modulo some small prime the LA is considerably faster than the WRA.

A drawback of the LA is the rather large theoretical lower bound for p^k. This causes no difficulties in an implementation using arbitrary length integers, but in the case that fixed length integers are used (as in our implementation, where we used single-length integers of 48 bits) we can get problems. There are several ways to lower the value for p^k if the theoretical bound on p^k appears to be too large.

1) Don't care about the theoretical bound, take p^k as large as the implementation allows. If the reduced basis $b_0,\ldots,b_{m-1}$ satisfies $\min_{0\le j<m} \|b_j\|/(2\cdot OD(b_0,\ldots,b_{m-1})) > B$ then the complete factorization will be found. Otherwise just try to find factors, but no guarantee can be given that we find them all.
2) Try to find a large degree irreducible factor of the minimal polynomial.
3) Use a combination of the WRA and the LA, i.e. combine the factorizations of f modulo a number of irreducible factors of the minimal polynomial modulo p^k (WRA), and apply the LA to these combinations. Here the lattice is generated by the product of this number of factors of the minimal polynomial and p^k. The running time of this algorithm grows exponentially with the number of factors of the minimal polynomial used, but unlike the WRA we do not have to use the complete factorization of the minimal polynomial; just take a number of factors such that the sum of the degrees is large enough to lower p^k sufficiently.
4) Any combination of 1), 2) and 3).

Theorem 2 can also be used while factoring in $\mathbb{Z}[X]$ [8]. Let $G \in \mathbb{Z}[X]$, and let H_k be a monic irreducible factor of degree ℓ of G modulo p^k. We test whether H_k leads

to an irreducible factor F of degree m of G (i.e. $H_k | F$ modulo p^k and $F | G$ over $\mathbb{Z}$) by looking at the (m+1)-dimensional lattice L_k generated by H_k and p^k. A basis of this lattice is given by: $b_i = p^k \cdot X^i$, $i=0,\ldots,\ell-1$, $b_i = H_k \cdot X^{i-\ell}$, $i=\ell,\ldots,m$. If F exists then clearly $F \in L_k$, but also F is the shortest-length vector in L_k if k is chosen sufficiently large. This follows from a generalized version of Theorem 2, stating that if $V_k \in L_k$ such that $\gcd(F,V_k)=1$ over $\mathbb{Z}$, then $p^{k\cdot\ell} \le \|F\|^{dV_k} \cdot \|V_k\|^m$. We know that there exists an effectively computable bound $B>0$ such that $\|F\| < B$, so if we take k minimal such that $B^{2\cdot m} < p^{k\cdot\ell}$, then $B^{2\cdot m} < \|F\|^{dV_k} \cdot \|V_k\|^m \le B^m \cdot \|V_k\|^m$. This implies $\|V_k\| > B$, which proves that indeed F is the shortest-length vector in L_k. Using for instance the shortest-vector algorithm of Dieter [2] we can determine F. It is not difficult to see that Theorem 1 can also be used to calculate F, if we take k such that $B^{2\cdot m}\cdot C(z,m+1)^m < p^{k\cdot\ell}$.

A similar algorithm, using the computation of a shortest vector in a lattice, can be applied to factorize in $(\mathbb{Q}(\alpha))[X]$. Determination of a monic factor of degree n leads to a lattice of dimension $n\cdot m+1$, where m is the degree of the minimal polynomial. As the shortest-vector algorithms are only efficient for small-dimensional lattices this is in general not a very practical method.

In Section 4 we have restricted ourselves to univariate polynomials; remark that the LA equally well applies to the multivariate case.

References.

1. D.G. Cantor & H. Zassenhaus, A New Algorithm for Factoring Polynomials Over Finite Fields, Math. Comp. 36 (1981), pp 587-592.
2. U. Dieter, How to calculate Shortest Vectors in a Lattice, Math. Comp. 29 (1975), pp 827-833.
3. A.K. Lenstra, Lattices and Factorization of Polynomials, Mathematisch Centrum, Amsterdam, Report IW 190/81.
4. H.W. Lenstra Jr., Integer programming with a fixed number of variables, University of Amsterdam, Department of Mathematics, Report 81-03.
5. B.M. Trager, Algebraic Factoring and Rational Function Integration, Proc. SYMSAC 76, pp 219-226.
6. B.L. van der Waerden, Moderne Algebra, Springer, Berlin, 1931.
7. P.S. Wang, Factoring Multivariate Polynomials over Algebraic Number Fields, Math. Comp. 30 (1976), pp 324-336.
8. P.S. Wang, An Improved Multivariate Polynomial Factoring Algorithm, Math. Comp. 32 (1978), pp 1215-1231.
9. P.J. Weinberger & L.P. Rothschild, Factoring Polynomials over Algebraic Number Fields, ACM Transactions on Math. Software 2 (1976), pp 335-350.
10. H. Zassenhaus, On Hensel Factorization, I, J. of Number Theory 1 (1969), pp 291-311.
11. H. Zassenhaus, A Remark on the Hensel Factorization Method, Math. Comp. 32 (1978), pp 287-292.

Addendum.

Recently L. Lovász invented a polynomial time reduction algorithm. Among others, this new reduction algorithm leads to a polynomial time algorithm for factoring polynomials with rational coefficients (see Section 5). A report describing the new polynomial factorization algorithm in detail is available from the Mathematisch Centrum, Amsterdam.

A.K. Lenstra, H.W. Lenstra & L. Lovász, Factoring Polynomials with Rational Coefficients, Mathematisch Centrum, Amsterdam.