*J. Symbolic Computation* (2002) **11**, 1–14

# Polynomial Factorization Algorithms over Number Fields

Xavier-François Roblot

roblot@euler.univ-lyon1.fr

*Institut Girard Desargues, Université Claude Bernard, Lyon, FRANCE*

*This research was conducted while the author was a member of the Laboratoire A2X, Université Bordeaux I, FRANCE*

*(Received 14 June 2002)*

The aim of this paper is to describe two new factorization algorithms for polynomials. The first factorizes polynomials modulo the prime ideal of a number field. The second factorizes polynomials over a number field.

## 1. Introduction

Factorization algorithms over $\mathbb{Q}[X]$ and $\mathbb{F}_p[X]$ are key tools of computational number theory. Many algorithms over number fields rely on the possibility of factoring polynomials in those fields. Because of the recent development of relative methods in computational number theory, see for example (Cohen *et al.* 1998, Daberkow and Pohst 1995), efficient generalizations of factorization algorithms to the relative case are necessary. The aim of this paper is to describe two new such algorithms.

The first algorithm factors polynomials modulo a prime ideal of a number field. It generalizes the algorithm of Berlekamp over $\mathbb{F}_p$. The second factors polynomials over a number field. Note that there already exist algorithms performing this task, see (Trager 1976, Weinberger and Rothschild 1976, Lenstra 1982, Geddes *et al.* 1992). In fact, the method described in this paper can be viewed as a combination of the methods of Lenstra (1982) and Weinberger and Rothschild (1976).

Notations and definitions are given in the first section. The second section is devoted to the factorization modulo a prime ideal, and the third to the description of the factorization algorithm over a number field. In the last section we give an example, several applications and some comparison timings.

## 2. Notations and definitions

Let $K$ be a number field. Let $d_K$ and $\mathcal{O}_K$ denote respectively its discriminant and its ring of integers. Let $(r_1, r_2)$ be the signature of $K$ and $N$ its absolute degree, so $N = r_1 + 2r_2$.

Let $\sigma_1, ..., \sigma_N$ be the embeddings of $K$ into $\mathbb{C}$ with the usual convention: $\sigma_1, ..., \sigma_{r_1}$ are

0747–7171/90/000000 + 00 $03.00/0 © 2002 Academic Press Limited

real, and $\sigma_{r_1+1}, ..., \sigma_N$ are complex with $\overline{\sigma}_{r_1+i} = \sigma_{r_1+r_2+i}$ for $1 \leq i \leq r_2$. The field $K$ can be embedded in $\mathbb{R}^N$ in the following way. An element $\theta \in K$ is sent to the vector whose first $r_1$ components are $\sigma_i(\theta)$ for $1 \leq i \leq r_1$, and last $2r_2$ components are the pairs $(\Re\sigma_j(\theta) + \Im\sigma_j(\theta), \Re\sigma_j(\theta) - \Im\sigma_j(\theta))$ for $1 \leq j \leq r_2$. This embedding maps the ring of integers (or any fractional ideal of $K$) to a lattice in $\mathbb{R}^N$, *i.e.*, a free additive subgroup of $\mathbb{R}^N$ of maximal rank. From now on, we identify $K$ with its image in $\mathbb{R}^N$. Thus, the square of the Euclidean distance on $\mathbb{R}^N$ yields a quadratic form on $K$, the so-called $T_2$-norm, defined by

$$T_2(\theta) := \sum_{i=1}^{N} |\sigma_i(\theta)|^2.$$

Let $n \geq 1$ be an integer and let $L$ be a lattice in $\mathbb{R}^n$, see (Conway and Sloane 1988). Denote by $\mathcal{B} = \{b_1, ..., b_n\}$ a basis of the lattice $L$. The fundamental domain of $\mathcal{B}$ is

$$D_{\mathcal{B}} := \left\{ (x_1 b_1, ..., x_n b_n) \text{ where } -\frac{1}{2} < x_i \leq \frac{1}{2} \text{ for all } i \right\}.$$

The origin is the only point of $L$ contained in this domain and every point $x \in \mathbb{R}^n$ can be uniquely written as $x = y + l$ where $l \in L$ and $y \in D_{\mathcal{B}}$. The volume of the lattice $V(L)$ is defined to be the volume of the fundamental domain. It does not depend on the choice of the basis. The defect of orthogonality of the basis $\mathcal{B}$ is defined by

$$\delta_{\mathcal{B}} := \frac{\prod_{i=1}^{n} |b_i|}{V(L)},$$

where $|.|$ denotes the length. This defect is $\geq 1$ by Hadamard's inequality, and in fact it is equal to 1 if and only if the basis is orthogonal. For an LLL-reduced basis $\mathcal{B}$ of $L$, as defined in (Lenstra *et al.* 1982), one gets

$$\delta_{\mathcal{B}} \leq 2^{n(n-1)/4}.$$

Finally, for a vector $x \in \mathbb{R}^n$, we denote by $\lfloor x \rceil$ the vector of $\mathbb{Z}^n$ that one obtains by rounding each component of $x$ to the nearest integer (with the convention that $m + \frac{1}{2}$ rounds to $m + 1$ for $m \in \mathbb{Z}$).

## 3. Factorization of polynomials modulo a prime ideal

Let $\mathfrak{p}$ be a prime ideal of $K$ dividing the rational prime $p$. Let $\mathbb{F}_{\mathfrak{p}}$ denote the residual field

$$\mathbb{F}_{\mathfrak{p}} := \frac{\mathcal{O}_K}{\mathfrak{p}}.$$

This field is isomorphic to the finite field $\mathbb{F}_q$ where $q := \mathcal{N}\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. Let $S(X)$ be a polynomial with coefficients in $\mathbb{F}_{\mathfrak{p}}$. The following method factors $S$ using a generalization of the method of Berlekamp (1970) as described in (Cohen 1993, section 3.4). Another method to factorize polynomials over finite fields can be found in (Cantor and Zassenhaus 1981).

The first step is to compute a polynomial $S_0(X)$ that is monic, square-free, and divisible exactly by the same irreducible factors as $S(X)$. We include the algorithm to do so for the sake of completeness and refer the reader to (Cohen 1993, section 3.4.2) for the proof of its validity.

ALGORITHM 3.1. *Squarefree factorization of a polynomial* $S(X) \in \mathbb{F}_{\mathfrak{p}}[X]$.

1. *Set* $T_0 \leftarrow S$ *and* $S_0 \leftarrow 1$.
2. *If* $T_0$ *is constant, output* $S_0$ *and terminate the algorithm.*
3. *Set* $T \leftarrow \mathrm{GCD}(T_0, T_0')$, $V \leftarrow T_0/T$ *and* $k \leftarrow 0$.
4. *If* $V$ *is constant, it is of the form*

$$T(X) = \sum_{p|j} t_j X^j,$$

   *then set* $T_0 \leftarrow \sum_{p|j} t_j X^{j/p}$ *and go to step* **2.**
5. *Set* $k \leftarrow k+1$. *If* $p$ *divides* $k$ *then set* $T \leftarrow T/V$ *and* $k \leftarrow k+1$.
6. *Set* $W \leftarrow \mathrm{GCD}(T, V)$, $A \leftarrow V/W$, $V \leftarrow W$ *and* $T \leftarrow T/V$. *If* $A$ *is not constant then set* $S_0 \leftarrow S_0 A$. *Go to step* **4.**

We now assume without loss of generality that $S$ is a monic square-free polynomial. Let $m$ denote its degree. The key result is the following theorem of Berlekamp (1970).

THEOREM 3.2. *Let*

$$S(X) = \prod_{i=1}^{g} S_i(X)$$

*be the irreducible factorization of* $S$. *Then, for any* $A(X) \in \mathbb{F}_{\mathfrak{p}}[X]$ *of degree* $< m$, *the following assertions are equivalent:*

(i) *There exist elements* $\alpha_i \in \mathbb{F}_{\mathfrak{p}}$ *such that* $A(X) \equiv \alpha_i \pmod{S_i}$ *for all* $i$.
(ii) *The polynomial* $A$ *satisfies* $A(X)^q \equiv A(X) \pmod{S}$.

(*Recall that* $q$ *is the absolute norm of* $\mathfrak{p}$).

Using the Chinese Remainder Theorem, one easily proves that there exists for each $g$-tuple $(\alpha_i)_i \in {\mathbb{F}_{\mathfrak{p}}}^g$ a unique polynomial $A(X)$ satisfying assertion (i). Hence the solutions of theorem 3.2 span an $\mathbb{F}_{\mathfrak{p}}$-vector space of dimension $g$.

Now, let $A(X) := \sum_{i=0}^{m-1} a_i X^i$ satisfy the conditions of the theorem. Then the coefficients of $A$ satisfy

$$a_i = \sum_{j=0}^{m-1} a_j r_{i,j},$$

where the $r_{i,j}$'s are defined by

$$X^{jq} = \sum_{i=0}^{m-1} r_{i,j} X^i \pmod{S}.$$

Thus the computation of a basis of the solutions of theorem 3.2 boils down to the kernel computation of the matrix $R - I_m$ where $R$ is the matrix with entries $r_{i,j}$, and $I_m$ is the identity matrix of dimension $m$. Note that the number of irreducible factors of $S$ is exactly the rank of this kernel. Therefore, if this rank is 1, the polynomial $S$ is irreducible and the factorization is done. Hence, we suppose from now on that the polynomial $S$ is reducible and we let $g$ denote the number of irreducible factors of $S$, so $g \geq 2$.

Assume that we can find a solution $A(X)$ such that $\alpha_1 \neq \alpha_2$ (with the notation of the theorem 3.2). Then $S_1(X)$ divides $A(X)-\alpha_1$ but $S_2(X)$ does not. Therefore, the GCD of $A(X)-\alpha_1$ and $S(X)$ yields a non-trivial factor of $S$. And we may repeat this process until $S(X)$ is broken into $g$ factors which are then known to be irreducible. Unfortunately, the drawback of the above method is that we need to find such a polynomial $A(X)$ and the corresponding element $\alpha_1$. And this is definitely a hard task when the field $\mathbb{F}_\mathfrak{p}$ is large.

We use instead the following method.

PROPOSITION 3.3. *Let $(A_i)_i$ be a basis of the solutions of theorem 3.2, and let $A(X) := \sum_i b_i A_i(X)$ be a random linear combination of the $A_i$'s. If $p = 2$, set*

$$D(X) := A(X) + A(X)^2 + A(X)^4 + ... + A(X)^{q/2};$$

*otherwise set*

$$D(X) := A(X)^{(q-1)/2} - 1.$$

*Then the* GCD *of $S(X)$ and $D(X)$ yields a non-trivial factorization of $S$ with a probability of a least $4/9$.*

PROOF. For each $i$, let $\alpha_i$ be the element of $\mathbb{F}_\mathfrak{p}$ such that $S_i$ divides $A(X) - \alpha_i$. First, suppose that $p = 2$ and set $B(X) := X + X^2 + X^4 + ... + X^{q/2}$. Then $B(X)(B(X)+1) = X^q + X$ and the field $\mathbb{F}_\mathfrak{p}$ is the disjoint union of the set of the $q/2$ roots of $B(X)$ and the set of the $q/2$ roots of $B(X) + 1$. Denote by $\mathcal{R}$ the set of roots of $B(X)$. Then

$$D(X) = \prod_{\rho \in \mathcal{R}} (A(X) - \rho).$$

Thus the GCD of $S(X)$ and $D(X)$ is equal to a constant if and only if none of the $\alpha_i$'s are in $\mathcal{R}$. This event has a probability of $1/2^g$. On the other hand, the GCD of $S(X)$ and $D(X)$ is equal to $S(X)$ if and only if all the $\alpha_i$'s belong to $\mathcal{R}$. And, this event has also a probability of $1/2^g$. Hence, this GCD is non-trivial with a probability of $1-1/2^{g-1} \geq 1/2$.

The case where $p$ is an odd prime is similar, with $\mathcal{R}$ being the set of square elements of $\mathbb{F}_\mathfrak{p}^\times$. Then the GCD of $S(X)$ and $D(X)$ is non-trivial with a probability of $1 - \left(\frac{q-1}{2q}\right)^g - \left(\frac{q+1}{2q}\right)^g \geq 4/9$. □

Putting all these results together, we obtain the following probabilistic algorithm.

ALGORITHM 3.4. *Factorization of a polynomial $S(X) \in \mathbb{F}_\mathfrak{p}[X]$.*

1. *Using algorithm 3.1, compute a monic square-free polynomial $S_0$ with the same irreducible factors as $S$.*
2. *Compute the coefficients $r_{i,j}$ such that $X^{jq} = \sum_i r_{i,j} X^i \pmod{S_0}$ and set $R \leftarrow (r_{i,j})_{i,j}$.*
3. *Compute the kernel of the matrix $R - I_m$ and denote its rank by $g$. If $g > 1$, compute also a basis $A_1(X), ..., A_g(X)$ of the solutions of theorem 3.2.*
   *Set $\mathcal{F} \leftarrow \{S_0(X)\}$ and $k \leftarrow 1$.*
4. *If $k = g$ then go to step **6**.*
   *Let $b_1, ..., b_g$ be random elements of $\mathbb{F}_\mathfrak{p}$. Set*

$$A(X) \leftarrow \sum_{i=1}^{g} b_i A_i(X).$$

*Set also*

$$D(X) \leftarrow A(X) + A(X)^2 + ... + A(X)^{q/2}$$

*if $q$ is even, or*

$$D(X) \leftarrow A(X)^{(q-1)/2} - 1$$

*otherwise. Set $\mathcal{G} \leftarrow \emptyset$.*

**5.** *Pick up a polynomial $B(X) \in \mathcal{F}$ and set $\mathcal{F} \leftarrow \mathcal{F} \setminus \{B(X)\}$. Compute $C(X) \leftarrow \mathrm{GCD}(B(X), D(X))$. If $0 < \deg C < \deg B$, then set $\mathcal{G} \leftarrow \mathcal{G} \cup \{C(X), B(X)/C(X)\}$, and set $k \leftarrow k+1$. Otherwise, set $\mathcal{G} \leftarrow \mathcal{G} \cup \{B(X)\}$. Finally, if $\mathcal{F} \neq \emptyset$ then go to step **5**; otherwise set $\mathcal{F} \leftarrow \mathcal{G}$ and go back to step **4**.*

**6.** *For each polynomial $S_i(X) \in \mathcal{F}$, compute the greatest positive integer $e_i$ such that $S_i(X)^{e_i}$ divides $S(X)$. Output the factorization*

$$S(X) = s \prod_{i=1}^{g} S_i(X)^{e_i}$$

*where $s$ is the leading coefficient of $S$, and terminate the algorithm.*

## 4. Factorization of polynomials over a number field

We first recall how one factorizes polynomials over $\mathbb{Q}$ as explained in (Cohen 1993, section 3.5). Let $S(X)$ be a polynomial with rational coefficients. Without loss of generality, we can assume that $S$ is a square-free polynomial with coefficients in $\mathbb{Z}$. To simplify the description of the method, we also assume that $S$ is monic. In order to factor $S$, one first factors it modulo a "well-chosen" rational prime number $p$. Then, using a result of Mignotte (1974), one computes an explicit bound $C$ on the absolute value of the coefficients of any non-trivial divisor of $S(X)$. Finally, one uses Hensel lemma to lift this factorization modulo $p^e$ where $p^e > 2C$. Then every factor of $S$ in $\mathbb{Q}[X]$ is the lift of a divisor of $S$ modulo $p^e$ where the lift is chosen with coefficients in the interval $]-p^e/2, p^e/2]$. Therefore, one recovers all the factors of $S$ in $\mathbb{Q}[X]$ from the factors of $S$ modulo $p^e$ (and in particular all the irreducible factors).

Similarly, the steps for the relative algorithm are the following. Given a polynomial $S(X)$ with coefficients in a number field $K$, we first find a square-free polynomial with the same irreducible factors and with integral coefficients. We factor this polynomial modulo a "well-chosen" prime ideal $\mathfrak{p}$ of $K$. Then, using a generalization of Mignotte's bounds, we compute a bound for the $T_2$-norm of the coefficients of any non-trivial factor of $S(X)$, and lift this factorization using Hensel lemma. Eventually, we recover the irreducible factors in $K[X]$ from this lifted factorization. Note that this final step is not as straightforward as in the absolute case.

Let $S(X)$ be a polynomial with coefficients in $K$. If $S$ is not square-free, we may also replace $S$ by $S/\mathrm{GCD}(S, S')$, that is, a square-free polynomial with exactly the same irreducible factors.

We now assume without loss of generality that $S$ is a square-free polynomial, and multiplying if necessary this polynomial by some well-chosen element in $K^\times$, we can also assume that it has coefficients in $\mathcal{O}_K$, and that its leading coefficient is a rational integer $s$. However, we cannot talk of factorization in this ring since $\mathcal{O}_K$ may not be principal.

Let $\mathfrak{p}$ be a prime ideal of $K$ such that $\mathfrak{p}$ does divide neither the discriminant of $S$ nor

its leading coefficient $s$. The reduction of $S$ modulo $\mathfrak{p}$ is a square-free polynomial of the same degree. We use the result of the last section to obtain the factorization

$$S(X) \equiv s \prod_{i=1}^{g} S_i(X) \pmod{\mathfrak{p}}.$$

If $g = 1$ then the polynomial $S$ is irreducible modulo $\mathfrak{p}$, therefore it is also irreducible in $K[X]$ and the factorization is done. From now on, assume that $S$ is reducible, so $g \geq 2$.

We need to lift this factorization modulo $\mathfrak{p}^e$ where the value of the exponent $e$ will be discussed below. As we said before, we use Hensel lifting which is a classic result that can be found in any textbook about algebraic number theory. We refer to (Cohen 1993) for an algorithmic version. We only quote here the result. Note that this theorem is proved in a more general case in (Pohst and Zassenhaus 1989).

THEOREM 4.1. *Let $S$ be a square-free polynomial in $\mathcal{O}_K[X]$, and let $\mathfrak{p}$ be a prime ideal of $K$ such that $\mathfrak{p}$ does divide neither the discriminant of $S$ nor its leading term. Let*

$$S(X) \equiv s \prod_{i=1}^{g} S_i(X) \pmod{\mathfrak{p}}$$

*denote the irreducible factorization of $S$ in $\mathbb{F}_{\mathfrak{p}}[X]$. Then, for every integer $e \geq 1$, there exist polynomials $S_{i,e}(X) \in \mathcal{O}_K[X]$ such that*

$$S(X) \equiv s \prod_{i=1}^{g} S_{i,e}(X) \pmod{\mathfrak{p}^e}$$

*and $S_{i,e}(X) \equiv S_i(X) \pmod{\mathfrak{p}}$. Furthermore, these polynomials are unique modulo $\mathfrak{p}^e$.*

In order to find a suitable value for the exponent $e$, we need to know more about the size of the $T_2$-norm of the coefficients of a divisor of $S$. This theorem is a generalization of a result of Mignotte (1974).

THEOREM 4.2. *Let $S(X) = \sum_{i=0}^{m} s_i X^i$ with leading coefficient $s = s_m \in \mathbb{Z} \setminus \{0\}$. Define $T_2(S) := \sum_{i=0}^{m} T_2(s_i)$. Then, for every monic divisor $D(X) := X^l + \sum_{j=0}^{l-1} d_j X^j$ of $S(X)$ in $K[X]$, we have*

$$T_2(d_j) \leq T_2(S) \left[ \binom{l-1}{j} + \binom{l-1}{j-1} \right]^2$$

*for $0 \leq j \leq n-1$.*

PROOF. For each embedding $\sigma$ of $K$ into $\mathbb{C}$, the monic polynomial $\sigma(D)$ divides the polynomial $\sigma(S)$ in $\mathbb{C}[X]$ and its leading term is smaller (in absolute value) than the leading term of $S$. Thus, by Mignotte's bounds, it follows that

$$|\sigma(d_j)| \leq \binom{l-1}{j} |\sigma(S)| + \binom{l-1}{j-1} |s|$$

where $|\sigma(S)| := \left( \sum_{i=0}^{m} |\sigma(s_i)|^2 \right)^{1/2}$. Now, using the fact that $|s| \leq |\sigma(S)|$, squaring this expression, and summing over all the embeddings of $K$ gives the result. □

Denote by $C$ an upper bound for the $T_2$-norm of every coefficient of such a non-trivial divisor of $S$. We use this bound by means of the following two results.

PROPOSITION 4.3. *Let $\pi$ be a non-zero element of $\mathfrak{p}^e$ where $e \geq 1$. Then*

$$T_2(\pi) \geq N\, q^{2e/N}.$$

PROOF. The inequality between arithmetic mean and geometric mean gives

$$\frac{1}{N}\sum_{i=1}^{N} |\sigma_i(\pi)|^2 \geq \left(\prod_{i=1}^{N} |\sigma_i(\pi)|^2\right)^{1/N}$$

or equivalently $T_2(\pi) \geq N|N_{K/\mathbb{Q}}(\pi)|^{2/N}$. Since $\pi$ is a non-zero element of $\mathfrak{p}^e$, its norm is divisible by $q^e$ and the result follows. □

COROLLARY 4.4. *Let $e$ be an positive integer such that*

$$e \geq \frac{N}{2}\frac{\log(4s^2C/N)}{\log q}$$

*and denote by $\widetilde{D}(X)$ any monic divisor of $S(X)$ modulo $\mathfrak{p}^e$. Then there exists at most one polynomial $D(X) \in \mathcal{O}_K[X]$ with leading coefficient $s$, and such that $D(X) \equiv s\,\widetilde{D}(X)$ (mod $\mathfrak{p}^e$) and $D$ divides $S$ in $K[X]$.*

PROOF. Let $\widetilde{\delta}$ be any coefficient of $\widetilde{D}(X)$ and let $\delta$ be the corresponding coefficient of $D(X)$. Then $\delta \equiv s\,\widetilde{\delta}$ (mod $\mathfrak{p}^e$), and $T_2(\delta) < s^2C$ since $s^{-1}D$ satisfies the condition of proposition 4.2. To prove the corollary, it is enough to prove that there exists at most one algebraic integer in $\mathcal{O}_K$ satisfying these two conditions. Now, suppose that $\delta'$ is another algebraic integer which satisfies these conditions. Set $\pi := \delta - \delta'$. Then, $\pi \in \mathfrak{p}^e$ and $T_2(\pi) < 4s^2C \leq Nq^{2e/N}$, thus $\pi = 0$ by the proposition. Therefore $\delta = \delta'$ and the result is proved. □

Let $e$ be an integer satisfying the hypothesis of the corollary. We need to be able to compute, if it exists, the polynomial $D$ corresponding to a divisor $\widetilde{D}$ of $S$ modulo $\mathfrak{p}^e$. In order to do so, we need to work with a larger exponent $e$. We use the following procedure given in (Lenstra 1982).

PROPOSITION 4.5. *Let $\mathcal{B}$ be a basis of a lattice $L$ in $\mathbb{R}^N$. Then, the fundamental domain of $\mathcal{B}$ contains a ball centered on the origin of radius*

$$R_{\mathcal{B}} > \frac{m_{\mathcal{B}}}{2\delta_{\mathcal{B}}}$$

*where $m_{\mathcal{B}}$ is the minimum length of the elements of $\mathcal{B}$.*

*In particular, if $\mathcal{B}$ is an LLL-reduced basis of $\mathfrak{p}^e$, then every element $\theta \in \mathcal{O}_K$ that does not belong to the fundamental domain of $\mathcal{B}$ satisfies*

$$T_2(\theta) > \frac{N}{4}\frac{q^{2e/N}}{4^{N(N-1)/4}}.$$

Let $e$ be an integer such that

$$e > \frac{N}{2} \frac{\log(s^2 C/N) + \left(\frac{N(N-1)}{4} + 1\right) \log 4}{\log q}. \qquad (\dagger)$$

Let $\mathcal{B}$ denote an LLL-reduced basis (for the $T_2$-norm) of $\mathfrak{p}^e$. Let $\widetilde{D}$ be a monic divisor of $S$ modulo $\mathfrak{p}^e$. With the notations of 4.4, we want to compute (if it exists) the polynomial $D(X)$ congruent to $s\,\widetilde{D}(X)$ modulo $\mathfrak{p}^e$ dividing $S$. Assume $D$ exists, let $\widetilde{\delta}$ be a lift in $\mathcal{O}_K$ of any coefficient of $\widetilde{D}$, and let $\delta$ be the corresponding coefficient of $D$. Then $\delta$ is the only algebraic integer congruent to $s\,\widetilde{\delta}$ contained in the fundamental domain of $\mathcal{B}$. Indeed, any other algebraic integer $\delta'$ congruent to $s\,\widetilde{\delta}$ modulo $\mathfrak{p}^e$ is outside the fundamental domain, and so must satisfies $T_2(\delta') > s^2 C$ by proposition 4.5 and inequality (†). Thus, we have $\delta = s\,\widetilde{\delta} - \lambda$ where $\lambda$ is the point of the lattice that is the closest to $s\,\widetilde{\delta}$. This point can be computed in the following way. Fix an integral basis $\Omega := \{\omega_1, ..., \omega_N\}$ of $K$, and let $M$ be the matrix expressing the $\mathbb{Z}$-basis $\mathcal{B}$ with respect to $\Omega$. Let $\widetilde{\mathbf{d}} := (\widetilde{d}_1, ..., \widetilde{d}_N) \in \mathbb{Z}^N$ be such that $s\,\widetilde{\delta} = \sum_i \widetilde{d}_i \omega_i$. Then $\lambda = \sum_i l_i \omega_i$ where $\mathbf{l} = (l_1, ..., l_N)$ is given by

$$\mathbf{l} = M \left\lfloor M^{-1} \widetilde{\mathbf{d}} \right\rceil.$$

We are now ready to give the complete algorithm.

ALGORITHM 4.6. *Factorization of a polynomial $S(X) \in K[X]$.*

1. *Set $S_0 \leftarrow S/\mathrm{GCD}(S, S')$, and $U \leftarrow d\,S_0$ where $d$ is a non-zero element of $K$ such that $d\,S_0(X) \in \mathcal{O}_K[X]$ and the leading term $u$ of $U$ is a rational integer. Let $\mathfrak{p}$ be a prime ideal of $K$ that does divide neither the discriminant of $U$ nor its leading term $u$. Note that prime ideals can be computed using algorithm 6.2.9 of Cohen (1993).*
2. *Let $e$ be an integer satisfying (†). Compute the factorization*

$$U(X) \equiv u \prod_{i=1}^{g} U_i(X) \pmod{\mathfrak{p}}$$

*by algorithm 3.4. If $g > 1$ then lift this factorization modulo $\mathfrak{p}^e$ using Hensel's lemma, and let $\widetilde{U}_i$ denote the factors obtained. Otherwise, i.e. if $g = 1$, set $\mathcal{F} \leftarrow \{u^{-1}U\}$, and go to step **6**.*
3. *Compute an LLL-reduced basis $\mathcal{B}$ of the ideal $\mathfrak{p}^e$. Set $r \leftarrow 1$, $\mathcal{E} \leftarrow \{\widetilde{U}_1, ..., \widetilde{U}_g\}$ and $\mathcal{F} \leftarrow \emptyset$.*
4. *For every product $\widetilde{D}(X) := E_1(X)...E_r(X)$ of $r$ (distinct) elements of $\mathcal{E}$, compute the polynomial $D$ congruent to $u\,\widetilde{D}$ modulo $\mathfrak{p}^e$ using the method explained above. If $D(X)$ divides $U(X)$, then remove from $\mathcal{E}$ the factors $E_i$, set $\mathcal{F} \leftarrow \mathcal{F} \cup \{\hat{D}\}$ where $\hat{D}$ is the monic polynomial obtained by dividing $D$ by its leading term and set $U \leftarrow d\,(U/D)$ where $d$ is a non-zero element of $K$ such that $d\,(U/D) \in \mathcal{O}_K[X]$ and its leading term $u$ is a rational integer.*
   *In any case, if there exist products of $r$ (remaining) elements of $\mathcal{E}$ that has not been tested, redo this step.*
5. *Set $r \leftarrow r + 1$. If $r \leq (\deg U)/2$ then go back to step **4**. If $\deg U \geq 1$, then set $\mathcal{F} \leftarrow \mathcal{F} \cup \{u^{-1}U\}$.*
6. *For every $S_i \in \mathcal{F}$, compute the greatest integer $e_i$ such that $S_i(X)^{e_i}$ divides $S(X)$.*

*Output the factorization*

$$S(X) = s \prod_{i=1}^{h} S_i(X)^{e_i}$$

*with $s$ the leading term of $S$, and terminate the algorithm.*

REMARK 4.1. If one is only interested in the factorization in $K[X]$, but not in the factorization in $\mathbb{F}_{\mathfrak{p}}[X]$, then one can choose a prime ideal $\mathfrak{p}$ of degree 1. Then the residue field $\mathbb{F}_{\mathfrak{p}}$ is isomorphic to $\mathbb{F}_p$, with $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, and one can use a standard factorization algorithm in $\mathbb{F}_p[X]$. Furthermore, if $\mathfrak{p}$ is also unramified, one can also avoid the use of Hensel's lemma by computing directly the $p$-adic factorization in the complete field $K_{\mathfrak{p}}$ (isomorphic to $\mathbb{Q}_p$) with the precision $p^e$. Algorithms to compute factorization in $\mathbb{Q}_p$ are given in (Böffgen 1987, Böffgen and Reichert 1987, Ford *et al.* 2002).

REMARK 4.2. Several improvements to this algorithm are possible including a relative version of van Hoeij (2002), see (Belabas *et al.* 2002), and the use of the method described in (Fieker and Friedrichs 2000) to replace the use of an real LLL algorithm by an (usually faster and, in anyway, stabler) integral one.

## 5. Implementation and Applications

The two preceding algorithms have been programmed in the number theory package PARI (Batut *et al.* 2002). Polynomial factorization algorithms over number fields are also implemented in other number theory packages e.g., KANT (Pohst *et al.* 2002), SIMATH (Zimmer *et al.* 1998) using the method described in (Pohst and Zassenhaus 1989), or more general purpose packages such as MAGMA (Cannon *et al.* 2002).

### 5.1. An Example

Let $K := \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $X^3 - X^2 - 9X + 8$. We want to factorize in this field the polynomial

$$S(X) = X^3 + (6\alpha - 9)X + (5\alpha^2 - 33\alpha + 13)X - 5\alpha + 30.$$

With the notations of theorem 4.2, we have $T_2(S) = 29\,362$, and thus $C = 88\,089$ is an upper bound for the $T_2$-norm of the coefficients of any non-trivial monic divisor of $S$ in $K[X]$. The prime ideal $\mathfrak{p}$ is chosen to be the only prime ideal above 5 of residual degree 2. Using algorithm 3.4, one finds

$$S(X) \equiv X(X+2)(X+\alpha+4) \pmod{\mathfrak{p}}.$$

Inequality (†) tells us that the exponent $e$ has to be greater than 6. By Hensel's lemma, we lift the factorization modulo $\mathfrak{p}^7$ and obtain the following factors

$$\begin{aligned} \widetilde{D}_1(X) &= X + 390100\alpha + 24260, \\ \widetilde{D}_2(X) &= X + 530\alpha + 366362, \\ \widetilde{D}_3(X) &= X + \alpha + 390619. \end{aligned}$$

We compute an LLL-reduced basis $\mathcal{B}$ for the $T_2$-norm of $\mathfrak{p}^7$. The matrix of this basis over the integral basis $\{1, \alpha, \alpha^2\}$ is

$$M = \begin{pmatrix} -4055 & 1854 & 4789 \\ -5 & 1139 & -1651 \\ 140 & -642 & -647 \end{pmatrix}.$$

With the notations of corollary 4.4, we compute the polynomial $D_1(X) = X - 2271 - 579\alpha + 338\alpha^2$, and its constant term has a $T_2$-norm of 10 687 724 which is larger than $C$. Thus $D_1(X)$ cannot be a divisor of $S$. For the same reason, we find that the polynomial $D_2$ cannot divides $S$. However, the last polynomial is $D_3(X) = X + \alpha - 6$ and it does divide $S(X)$. We obtain

$$S(X) = (X + \alpha - 6)(X^2 + (-3 + 5\alpha)X - 5).$$

Finally, we know that this second factor is irreducible since, otherwise, its factorization will be given by the lift of $\widetilde{D}_1$ and $\widetilde{D}_2$. Therefore, this is the complete factorization of $S$ in $K[X]$.

The defect of orthogonality of the LLL-reduced basis $\mathcal{B}$ given by $M$ is $\delta_{\mathcal{B}} \simeq 1.094$ and the value of $m_{\mathcal{B}}$ is approximately 5 573.6. Thus, the fundamental domain of this basis contains a ball centered on the origin of radius $R_{\mathcal{B}} \geq 2\,546$ and every algebraic integer of $K$ which is not contained in this domain has a $T_2$-norm greater than 6 486 381.

### 5.2. Applications of the polynomial factorization over a number field

We use the following notations: $K := \mathbb{Q}(\alpha)$ and $L := \mathbb{Q}(\beta)$ are two number fields where $\alpha$ (resp. $\beta$) is the root of the irreducible integral polynomials $A(X)$ (resp. $B(X)$).

#### 5.2.1. Subfield test

The field $K$ is conjugate to a subfield of $L$ if and only if the polynomial $A$ has a linear factor in $L[X]$. If it is so, this factor gives also an expression of $\alpha$ (up to isomorphism) as a polynomial in $\beta$. Now, if $\alpha$ and $\beta$ are known as complex numbers, one can test if $K \subset L$ (not only up to isomorphism) by computing a precise enough value of the root of this linear factor.

#### 5.2.2. Relative minimal polynomial

If $K$ is known to be conjugate to a subfield of $L$, then the irreducible factors of $B(X)$ in $K[X]$ are the minimal polynomials over $K$ of the conjugates of $\beta$ by the $\mathbb{Q}$-isomorphisms of $K$. Once again, it is possible to find exactly which is the minimal polynomial of $\beta$ over $K$ by using complex approximations.

#### 5.2.3. Field automorphisms

Every linear factor in the factorization of $B(X)$ in $L[X]$ yields a $\mathbb{Q}$-automorphism of $L$, and this automorphism is explicitly expressed as a polynomial in $\beta$ (note that one always obtains the trivial factor $X - \beta$ corresponding to the identity automorphism). Similarly, if one factors in $L[X]$ the relative minimal polynomial $B_K(X)$ of $\beta$ over a subfield $K$, then one obtains explicitly all the $K$-automorphisms of $L$.

#### 5.2.4. Galois closure and Galois group

Assume that the polynomial $B$ splits totally over $L[X]$. Then $L/\mathbb{Q}$ is a Galois extension. In a similar way, if the factorization of $B_K$ in $L[X]$ has only linear factors, then $L/K$ is a Galois extension. Conversely, if the polynomial $B$ (resp. $B_K$) does not split completely, then the extension is not Galois, and any root $\theta$ of a non-linear factor of $B$ (resp. $B_K$) yields an new extension $L(\theta)/\mathbb{Q}$ (resp. $L(\theta)/K$) that is contained in the Galois closure of $L/\mathbb{Q}$ (resp. $L/K$). By factoring $B$ (resp. $B_K$) in this new field, one can test if this field is indeed the Galois closure. If not, one has to consider the field generated over $L(\theta)$ by a root of any non-linear factor. Using this method, one obtains finally the Galois closure of $L$, and may even be able to recover its Galois group by a close look at the factors encountered, especially when this group is solvable, see (Landau and Miller 1985).

#### 5.2.5. $n$-th roots of an algebraic number

Let $\theta$ be an algebraic number in $K$, and let $n \geq 2$ be an integer. Then, one obtains all the $n$-th roots of $\theta$ in $K$ by factoring the polynomial $X^n - \theta$ in $K[X]$. In particular, when $\theta = 1$, one can use this method, or a refined version as described in the algorithm 4.9.10 of Cohen (1993), to compute all the roots of unity contained in $K$.

### 5.3. Applications of polynomial factorization modulo a prime ideal

We keep the same notations. We assume also from now on that $K$ is a subfield of $L$.

#### 5.3.1. Relative Dedekind Criterion

Let $\mathfrak{p}$ be a prime ideal of $K$, and let $\theta$ be an algebraic integer of $L$ such that $L = K(\theta)$. This criterion tells us if the order $\mathcal{O}_K[\theta]$ is $\mathfrak{p}$-maximal (recall that this order is said to be $\mathfrak{p}$-maximal, if $\mathfrak{p}$ does not divide the index $(\mathcal{O}_L : \mathcal{O}_K[\theta])$). Furthermore, if it this order is not $\mathfrak{p}$-maximal, then the criterion defines a new order $\mathcal{O}'$, strictly larger than $\mathcal{O}_K[\theta]$. We quote the result without proof, and refer to (Roblot 1997) for the proof. We also refer the reader to theorem 6.1.4 of Cohen (1993) for the absolute version of the criterion. We denote by $T(X)$ the minimal polynomial of $\theta$ over $K$.

Theorem 5.1. *Let $\tau$ be an element of $K$ such that $v_{\mathfrak{p}}(\tau) = -1$ and $v_{\mathfrak{q}}(\tau) \geq 0$ for any prime ideal $\mathfrak{q} \neq \mathfrak{p}$. For any $P(X) \in \mathcal{O}_K[X]$, let $\overline{P}$ denote its reduction modulo $\mathfrak{p}$. Let*

$$\overline{T}(X) = \prod_{i=1}^{r} \overline{T_i}(X)^{e_i}$$

*be the irreducible factorization of $T$ in $\mathbb{F}_{\mathfrak{p}}[X]$. Let $g(X) := \prod_i T_i(X)$, and let $h(X)$ be any lift of $\overline{T/g}$ of the same degree. We define*

$$f(X) := \tau\,(g(X)h(X) - T(X)) \in \mathcal{O}_K[X].$$

*(i) The order $\mathcal{O}_K[\theta]$ is $\mathfrak{p}$-maximal if and only if $\mathrm{GCD}(\overline{f}, \overline{g}, \overline{h}) = \overline{1}$.*
*(ii) Let $U(X)$ be any lift of $\overline{T}/\mathrm{GCD}(\overline{f}, \overline{g}, \overline{h})$ of the same degree. Define the following module*

$$\widetilde{\mathcal{O}} := \mathcal{O}_K[\theta] + U(\theta)\mathfrak{p}^{-1}\mathcal{O}_K[\theta].$$

*Then, $\widetilde{\mathcal{O}}$ is an order of $L$ containing $\mathcal{O}_K[\theta]$, and $(\mathcal{O} : \mathcal{O}_K[\theta]) = \mathfrak{p}^m$ where $m$ is the degree of* $\mathrm{GCD}(\overline{f}, \overline{g}, \overline{h})$.

### 5.3.2. Decomposition of prime ideals

As above, let $\theta$ be an algebraic integer such that $L = K(\theta)$, and let $T(X)$ denote its minimal polynomial over $K$. Let $\mathfrak{p}$ be a prime ideal of $K$. If $\mathfrak{p}$ does not divide the index $(\mathcal{O}_L : \mathcal{O}_K[\theta])$, then the decomposition of $\mathfrak{p}$ in $L$ is given by the factorization of $T(X)$ modulo $\mathfrak{p}$. More precisely, one has the following theorem which is proved in (Pohst and Zassenhaus 1989).

Theorem 5.2. *Let*

$$T(X) \equiv \prod_{i=1}^{r} T_i(X)^{e_i} \pmod{\mathfrak{p}}$$

*be the irreducible factorization of $T$ in $\mathbb{F}_{\mathfrak{p}}[X]$, where the polynomials $T_i(X)$ are monic and belong to $\mathcal{O}_K[X]$. Then, there exist exactly $r$ prime ideals $\mathfrak{P}_i$ dividing $\mathfrak{p}\mathcal{O}_L$, and these prime ideals are given by*

$$\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_L + T_i(\theta)\mathcal{O}_L.$$

*Furthermore, the ramification index (resp. the residual degree) of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $e_i$ (resp. the degree of the polynomial $T_i$).*

### 5.3.3. The relative Round 4 algorithm

The absolute Round 4 algorithm is used to compute the maximal order of a $p$-adic fields. It is also used to compute the ring of integers of a number field as a $\mathbb{Z}$-module. It is described in (Ford 1978, Ford 1987, Ford and Letard 1994, Böffgen 1987, Böffgen and Reichert 1987, Ford *et al.* 2002). Since this algorithm deals only with $p$-adic computations, one can generalize this algorithm to the relative case using $\mathfrak{p}$-adic computations. However, this is a difficult and complicated algorithm, thus we will not give any details here and the interested reader can refer to (Roblot 1997).

## 5.4. Comparison timings

We have compared the implementation in PARI (v. 2.2.4) of the algorithm described in section 4 to the algorithm available in KASH (v. 2.2) (Pohst *et al.* 2002) which uses a norm-based factorization. We have considered random polynomials over random number fields of various degrees. These were constructed in the following way.

We take the polynomials defining the number fields as random monic irreducible polynomials with integral coefficients in the interval $[-5; 5]$. For $T$ such a polynomial of degree $n$, let $K$ be the number field defined by one of its roots, $\mathcal{O}_K$ be the ring of integers of $K$ and $\{\omega_1 = 1, \dots, \omega_n\}$ be an integral basis of $\mathcal{O}_K$.

Now, we choose a random integer $t$ in $[2, 6]$, and produce $t$ random polynomials in $\mathcal{O}_K[X]$ of degree between 1 and 7 with coefficients

$$\lambda_1\omega_1 + \cdots \lambda_n\omega_n \in \mathcal{O}_K$$

where the $\lambda_i$'s are random integers in the interval $]-500; 500[$. Multiplying these $t$ polynomials together gives us the polynomial we want to factorize.

For $2 \leq n \leq 7$, we have constructed in this way 10 random polynomials over 15 random number fields of degree $n$, and factorized these polynomials using the two packages. The corresponding timings are given in the following table. Note that the computation time of the new algorithm is largely dominated by the LLL-reduction step when the degree of the number field is large.

The computation were performed on a Pentium III with 1000MHz and 1GB of RAM running Linux 2.4.3.

| $n$ | KANT | PARI | $n$ | KANT | PARI |
|---|---|---|---|---|---|
| 2 | $7.1s$ | $2.7s$ | 5 | $80s$ | $38s$ |
| 3 | $20s$ | $6.5s$ | 6 | $136s$ | $63s$ |
| 4 | $39s$ | $13s$ | 7 | $279s$ | $206s$ |

## References


Batut, C., Belabas, K., Bernardi, D., Cohen, H., Olivier, M. (2002). Number theory package PARI, v.2.2.4 (development). `http://www.parigp-home.de/`.

Belabas, K., Hanrot, G., Zimmermann, P. (2002) A relative version of van Hoeij algorithm, work in progress with a pilot implementation in PARI/GP.

Berlekamp, E. (1970). Factoring polynomials over large finite fields. *Math. Comp.* **24**, 713–735.

Böffgen, R. (1987). Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren. *Ann. Univ. Saraviensis, Ser. Math.* **1**, 60–129.

Böffgen, R., Reichert, M. A. (1987). Computing the decomposition of primes $p$ and $p$-adic absolute values in semi-simple algebras over $\mathbb{Q}$. *J. Symb. Comp.* **4**, 3–10.

Cannon, J. *et al.* (2002). The Magma Computational Algebra System for Algebra, Number Theory and Geometry, v.2.9. `http://magma.maths.usyd.edu.au/magma/`.

Cantor, D. G., Zassenhaus, H. (1981). A new algorithm for factoring polynomials over finite fields. *Math. Comp.* **36**, 587–592.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Math.* Springer-Verlag.

Cohen, H., Diaz y Diaz, F., Olivier, M. (1998). Computing ray class groups, conductors and discriminants. *Math. Comp.* **67**, 773–795.

Conway, J., Sloane, N. (1988). *Sphere Packing, Lattices and Groups*, volume 290 of *Grundlehren der math. Wiss.*, Springer-Verlag.

Daberkow, M., Pohst, M. (1995). Computations with relative extensions of number fields with an application to the construction of Hilbert class fields. In *Proc. ISAAC'95.*

Fieker, C., Friedrichs, C. (2000). On reconstruction of algebraic numbers. In *Algorithmic number theory* ANTS-IV (Leiden), Lecture Notes in Comp. Sci. **1838**, Springer, 285–296

Ford, D. (1978). *On the Computation of the Maximal Order in a Dedekind Domain.* PhD thesis, Ohio State University.

Ford, D. (1987). The construction of maximal orders over a Dedekind domain. *J. Symb. Comp.* **4**, 69–75.

Ford, D., Letard, P. (1994). Implementing the Round Four maximal order algorithm. *Sém. Th. Nombres de Bordeaux* **6**, 39–80.

Ford, D., Pauli, S., Roblot, X.-F. (2002). A fast algorithm for polynomial factorization over $\mathbb{Q}_p$, to appear in *Journal de Théorie des Nombres de Bordeaux.*

Geddes, K., Czapor, S., Labahn, G. (1992). *Algorithms for Computer Algebra.* Kluwer Academic Press.

van Hoeij, M. (2002). Factoring polynomials and the knapsack problem, to appear in *Journal of Number Theory.*

Landau, S., Miller, G. L. (1985). Solvability by radicals is in polynomial time. *J. Comput. Syst. Sci.* **30**, 179–208.

Lenstra, A. K. (1982). Factoring polynomials over algebraic number fields. *LN in Comp. Sci.* **144**, 32–39.

Lenstra, A. K., Lenstra, H. W., Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math. Ann.* **261**, 515–534.

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

Pohst, M., Zassenhaus, H. (1989). *Algorithmic Algebraic Number Theory.* Cambridge Univ. Press.

Pohst, M. *et al.* (2002). Number theory package KANT, v.2.2. `http://www.math.tu-berlin.de/~kant/`.

Roblot, X.-F. (1997). *Algorithmes de Factorisation dans les Extensions Relatives et Applications de la Conjecture de Stark à la Construction des Corps de Classes de Rayon.* PhD thesis, Laboratoire A2X, Université Bordeaux I.

Trager, B. (1976). Algebraic factoring and rational function integration. In *Proc. of SYMSAC'76*, 219–226.

Weinberger, P.J., Rothschild, L.P. (1976). Factoring polynomials over algebraic number fields. *ACM Transactions on Math. Software* **2**, 335–350.

Zimmer, H. G. *et al.* (1998). Number theory package SIMATH. `http://www.math.uni-sb.de/~simath/`.