Factoring Polynomials over Local Fields II

Sebastian Pauli

Department of Mathematics and Statistics
University of North Carolina at Greensboro, Greensboro, NC 27412, USA
s_pauli@uncg.edu

Abstract. We present an algorithm for factoring polynomials over local fields, in which the Montes algorithm is combined with elements from Zassenhaus Round Four algorithm. This algorithm avoids the computation of characteristic polynomials and the resulting precision problems that occur in the Round Four algorithm.

1 Introduction

Polynomial factorization is fundamental in working with local fields. In addition to the irreducible factors of a given polynomial, computer algebra systems that support extensions of local fields (*e.g.*, Magma [1], Sage [16]) require explicit representations of the unramified and totally ramified parts of the extensions generated by arbitrary irreducible polynomials, as these systems represent such extensions as a tower of unramified and totally ramified extensions. Moreover, there are many applications of global fields that include the construction of integral bases, decomposition of ideals, and the computation of completions.

The algorithms [2, 4, 7, 14] for factoring a polynomial $\Phi(x)$ over a local field find successively better approximations to the irreducible factors of $\Phi(x)$ until gaining sufficient precision to apply Hensel lifting. The algorithms differ in how the approximations are computed.

Algorithms based on the Zassenhaus Round Four algorithm (*e.g.* [3, 4, 14]) suffer from loss of precision in computing characteristic polynomials and approximating greatest common divisors. The Montes algorithm [10, 11, 7, 8] avoids the computation of characteristic polynomials by exploiting Newton polygons of higher order. Here the most expensive operations are division with remainder and polynomial factorization over finite fields.

We present the algorithm of Montes in the terminology of [14] and use the techniques of the Round Four algorithm to derive a factorization when a breaking element is found. We also give a complexity analysis.

Notation

Let K be a field complete with respect to a non-archimedean exponential valuation ν with finite residue class field $\underline{\mathsf{K}} \cong \mathbb{F}_q$ of characteristic p; we call K a *local field.* Assume ν is normalized with $\nu(\pi) = 1$ for the uniformizing element

π in the valuation ring $\mathcal{O}_{\mathsf{K}}$ of K. For $\gamma \in \mathcal{O}_{\mathsf{K}}$ denote by $\underline{\gamma}$ the class $\gamma + (\pi)$ in $\underline{\mathsf{K}}$. The unique extension of ν to an algebraic closure $\overline{\mathsf{K}}$ of K (or to any intermediate field) is also denoted ν.

In our algorithm we will be concerned with the first non-zero coefficient of the expansion of an element in a finite subextension of $\overline{\mathsf{K}}/\mathsf{K}$. We introduce an equivalence relation on the elements of $\overline{\mathsf{K}}$ which reflects this (also see [9]).

Definition 1 For $\gamma \in \overline{\mathsf{K}}^*$ and $\delta \in \overline{\mathsf{K}}^*$ we write $\gamma \sim \delta$ if

$$\nu(\gamma - \delta) > \nu(\gamma)$$

and make the supplementary assumption $0 \sim 0$. For $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i$ and $\vartheta(x) = \sum_{i=0}^{n} \vartheta_i x^i$ in $\overline{\mathsf{K}}[x]$ we write $\varphi(x) \sim \vartheta(x)$ if

$$\min_{0 \le i \le n} \nu(\varphi_i - \vartheta_i) \ > \ \min_{0 \le i \le n} \nu(\varphi_i).$$

Let L be a finite extension of K with uniformizing element π_{L}. Two elements $\gamma = \gamma_0 \pi_{\mathsf{L}}^v \in \mathsf{L}$ and $\delta = \delta_0 \pi_{\mathsf{L}}^w \in \mathsf{L}$ with $\nu(\gamma_0) = \nu(\delta_0) = 0$ are equivalent with respect to $\sim$ if and only if $v = w$ and $\gamma_0 \equiv \delta_0 \bmod (\pi_{\mathsf{L}})$. It follows immediately that the relation $\sim$ is symmetric, transitive, and reflexive.

2 Reducibility

Assume we want to factor a polynomial $\Phi \in \mathcal{O}_{\mathsf{K}}[x]$ of degree N. If $\Phi(x)$ splits into the product of two co-prime factors over the residue class field $\underline{\mathsf{K}}$ of K, say $\underline{\Phi}(x) = \underline{\Phi}_1(x) \cdot \underline{\Phi}_2(x)$, then Hensel lifting yields a factorization of $\Phi(x)$ to any given precision. In addition to this classic situation we give two further situations that we can exploit to obtain a factorization of $\Phi(x)$.

We consider a polynomial $\vartheta(x) \in \mathcal{O}_{\mathsf{K}}[x]$ as a representative of an element in the algebra $\mathsf{K}[x]/(\Phi(x))$ and determine a polynomial $\chi_\vartheta(x) \in \mathsf{K}[x]$ from $\vartheta(x)$ such that $\chi_\vartheta(\vartheta(\xi)) = 0$ for all roots ξ of $\Phi(x)$.

Definition 2 Let $\Phi(x) = \prod_{j=1}^{N}(x - \xi_j) \in \mathcal{O}_{\mathsf{K}}[x]$, where $\xi_j \in \overline{\mathsf{K}}$ for $1 \le j \le N$ and $\vartheta(x) \in \mathsf{K}[x]$. Then we set

$$\chi_\vartheta(y) := \prod_{i=1}^{N}(y - \vartheta(\xi_i)) = \mathrm{res}_x(\Phi(y), y - \vartheta(x)).$$

Assume we find $\vartheta \in \mathsf{K}[x]$ such that $\chi_\vartheta(y) = \chi_1(y)\chi_2(y)$ with $\gcd(\chi_1, \chi_2) = 1$. Reordering the roots ξ_i $(1 \le i \le N)$ of $\Phi(x)$ if necessary, we may write

$$\chi_1(y) = (y - \vartheta(\xi_1)) \cdots (y - \vartheta(\xi_r)) \text{ and } \chi_2(y) = (y - \vartheta(\xi_{r+1})) \cdots (y - \vartheta(\xi_N)),$$

where $1 \le r < N$ and obtain a proper factorization of $\Phi(x)$:

$$\Phi(x) = \gcd(\Phi(x), \chi_1(\vartheta(x))) \cdot \gcd(\Phi(x), \chi_2(\vartheta(x))). \tag{1}$$

Definition 3 We say a polynomial $\vartheta(x) \in \mathsf{K}[x]$ with $\chi_\vartheta(t) \in \mathcal{O}_\mathsf{K}[t]$ passes the *Hensel test* if $\underline{\chi}_\vartheta(t) = \underline{\rho}(t)^g$ for some irreducible polynomial $\underline{\rho}(t) \in \underline{\mathsf{K}}[t]$.

If $\vartheta(x) \in \mathsf{K}[x]$ fails the Hensel test, that is, $\chi_\vartheta(y)$ splits into two co-prime factors over $\underline{\mathsf{K}}$, say $\underline{\chi}_\vartheta(y) = \underline{\chi}_1(y)\underline{\chi}_2(y)$, then Hensel lifting yields a factorization $\chi_\vartheta(y) = \chi_1(y)\chi_2(y)$ and equation (1) gives a proper factorization of $\Phi(x)$.

Definition 4 For $\vartheta \in \mathsf{K}[x]$ we set $v^*_\Phi(\vartheta) := \min_{\Phi(\xi)=0} \nu(\vartheta(\xi))$ and say the polynomial $\vartheta(x)$ passes the *Newton test* if $\nu(\vartheta(\xi)) = \nu(\vartheta(\xi'))$ for all roots ξ and ξ' of $\Phi(x)$.

If $\varphi(x) \in \mathsf{K}[x]$ fails the Newton test, the Newton polygon of $\chi_\varphi(y)$ consists of at least two segments. Let $h/e = v^*_\Phi(\varphi)$ be the minimum of the valuations $\nu(\varphi(\xi_i))$ $(1 \le i \le N)$ in lowest terms. Then $-h/e$ is the gentlest slope of the segments of the Newton polygon of $\chi_\varphi(y)$. We set $\vartheta(x) := \varphi(x)^e/\pi^h$ and obtain $\nu(\vartheta(\xi)) = 0$ for all roots ξ of $\Phi(x)$ with $\nu(\varphi(\xi)) = h/e$ and $\nu(\vartheta(\xi)) > 0$ for all roots ξ of $\Phi(x)$ with $\nu(\varphi(\xi)) > h/e$. Thus $\underline{\chi}_\vartheta(t)$ splits into two co-prime factors and the considerations above yield a proper factorization of $\Phi(x)$.

3 Irreducibility and the Sequence $\big(\varphi_t(x)\big)_t$

In the polynomial factorization algorithm we construct a sequence of polynomials $\varphi_t(x) \in \mathcal{O}_\mathsf{K}[x]$ such that $\nu(\varphi_{t+1}(\xi)) > \nu(\varphi_t(\xi))$ for all roots ξ of $\Phi(x)$ until we either find a polynomial that fails the Newton test, which leads to a factorization of $\Phi(x)$ or we have established the irreducibility of $\Phi(x)$. If we assure that the degrees of the polynomials $\varphi_t(x)$ are less than or equal to the degree of all irreducible factors of $\Phi(x)$, we either obtain a factorization of $\Phi(x)$ or we establish the irreducibility of $\Phi(x)$ in finitely many steps [14]:

Theorem 5 *Let $\xi_1, \ldots, \xi_N$ be elements of an algebraic closure of a local field K and assume the following hypotheses hold.*

- *$\Phi(x) = \prod_{j=1}^N (x - \xi_j)$ is a square-free polynomial in $\mathcal{O}_\mathsf{K}[x]$.*
- *$\varphi(x) \in \mathsf{K}[x]$.*
- *$N\nu(\varphi(\xi_j)) > 2\nu(\operatorname{disc}\Phi)$ for $1 \le j \le N$.*
- *The degree of any irreducible factor of $\Phi(x)$ is greater than or equal to $\deg\varphi$.*

Then $N = \deg\varphi$ and $\Phi(x)$ is irreducible over K.

While we construct the sequence of polynomials $\varphi_t(x)$ we gather information about the extensions generated by the irreducible factors of $\Phi(x)$. In particular we will at all times know divisors E_t and F_t of the ramification index and inertia degree of these extensions respectively. If we find that not all of these extensions have the same inertia degree and ramification index, we will have encountered a polynomial that fails the Hensel or the Newton test. On the other hand if $E_t \cdot F_t = \deg\Phi$ we know that $\Phi(x)$ is irreducible.

Definition 6 Let $\Phi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be irreducible and let ξ be a root of $\Phi(x)$. We call a pair of polynomials $\Pi(x) \in \mathsf{K}[x]$ and $\Gamma(x) \in \mathsf{K}[x]$ with $\nu(\Pi(\xi)) = 1/E$ and $F = \left[\underline{\mathsf{K}}\big(\underline{\Gamma(\xi)}\big) : \underline{\mathsf{K}}\right]$ such that $E \cdot F = \deg \Phi$ a *two element certificate* for the irreducibility of $\Phi(x)$.

Remark 7 If a two element certificate exists then $\Phi(x)$ is irreducible and an integral basis of the extension of $\mathsf{K}(\xi)/\mathsf{K}$ generated by a root ξ of $\Phi(x)$ is given by the elements $\Gamma(\xi)^i \Pi(\xi)^j$ with $0 \le i \le F-1$ and $0 \le j \le E-1$.

In the polynomial factorization algorithm we construct a sequence of polynomials $(\varphi_t(x))_{t\in\mathbb{N}}$ where $\varphi_t \in \mathcal{O}_{\mathsf{K}}[x]$ such that

1. $\nu(\varphi_{t+1}(\xi)) > \nu(\varphi_t(\xi))$ for all roots ξ of $\Phi(x)$,
2. $\nu(\varphi_t(\xi)) = \nu(\varphi_t(\xi'))$ for all roots ξ and ξ' of $\Phi(x)$, and
3. the degree of $\varphi_t(x)$ is less than or equal to the degree of any irreducible factor of $\Phi(x)$.

In the following we assume that all polynomials that occur in our constructions pass the Hensel and Newton tests, as we can otherwise derive a factorization of $\Phi(x)$. For convenience of notation we define:

Definition 8 If $v^*_\Phi(\varphi - \vartheta) > v^*_\Phi(\varphi)$ for polynomials $\varphi(x) \in \overline{\mathsf{K}}[x]$ and $\vartheta(x) \in \overline{\mathsf{K}}[x]$ we write $\varphi \underset{\Phi}{\sim} \vartheta$. For polynomials $\chi(y) = \sum_{i=0}^n a_i(x) y^i \in \mathsf{K}[x][y]$ and $\tau(y) = \sum_{i=0}^n b_i(x) y^i \in \mathsf{K}[x][y]$ we write $\chi(y) \underset{\Phi}{\sim} \tau(y)$ if

$$\min_{0 \le i \le n} v^*_\Phi(a_i - b_i) > \min_{0 \le i \le n} v^*_\Phi(a_i).$$

4 The First Iteration

Let $\Phi(x) = \sum_{i=0}^N c_i x^i$ and $\varphi_1(x) := x \in \mathcal{O}_{\mathsf{K}}[x]$. Assume the Newton polygon of $\Phi(x)$ consists of one segment and let $-h_1/E_1$ be its slope in lowest terms. Then $\nu(\varphi_1(\xi)) = \nu(\xi) = h_1/E_1$ for all roots ξ of $\Phi(x)$. This implies that the ramification index of all extension generated by irreducible factors of $\Phi(x)$ is divisible by E_1. Let $\beta \in \overline{\mathsf{K}}$ with $\beta^{E_1} = \pi^{h_1}$ where π is the uniformizing element of K. We flatten the Newton polygon of $\Phi(x)$ so that it lies on the x-axis:

$$\Phi^\flat(y) := \frac{\Phi(\beta y)}{\beta^N} = \sum_{i=0}^N c_i \beta^{i-N} y^i.$$

Because we can only have $\nu(c_i \beta^{i-N}) = 0$ when $E_1 \mid i$, we have

$$\Phi^\flat(y) \sim \sum_{j=0}^{N/E_1} c_{j\cdot E_1} \pi^{h_1(j-N/E_1)} y^{j\cdot E_1}.$$

Replacing y^{E_1} by z yields

$$A_1(z) := \sum_{j=0}^{N/E_1} c_{j\cdot E_1}\pi^{h_1(j-N/E_1)}z^j.$$

The polynomial $\underline{A}_1(z) \in \underline{\mathsf{K}}[z]$ is called the *associated polynomial* [11, 10] or *residual polynomial* [7, 8] of $\Phi(x)$ with respect to $\varphi_1(x)$. Assume that $\underline{A}_1(z) = \underline{\rho}_1(z)^r$ for some irreducible polynomial $\underline{\rho}_1 \in \underline{\mathsf{K}}$. Otherwise $\varphi_1(x)^{E_1}/\pi^{h_1} = x^{E_1}/\pi^{h_1}$ would fail the Hensel test and (1) would yield a factorization of $\Phi(x)$. All fields $\mathsf{K}(\xi)$, where ξ is a root of $\Phi(x)$, contain an element ξ^{E_1}/π^{h_1}, whose minimal polynomial is a power of $\underline{\rho}_1(z)$ over $\underline{\mathsf{K}}[z]$; therefore their ramification indices are divisible by $F_1 := \deg \underline{\rho}_1$. Let $\gamma_1 \in \overline{\mathsf{K}}$ be a root of a lift $\rho_1(z) \in \mathcal{O}_{\mathsf{K}}[z]$ of $\underline{\rho}_1(z)$. In the unramified extension $\mathsf{K}_1 := \mathsf{K}(\gamma_1)$ we have the relation $x^{E_1} \underset{\Phi}{\sim} \pi^{h_1} \cdot \gamma_1$. Since $\nu\big(\rho_1(\varphi_1(\xi)^{E_1}/\pi^{h_1})\big) > 0$ for all roots ξ of $\Phi(x)$, we get

$$\nu\left(\pi^{h_1F_1}\rho_1\left(\frac{\varphi_1(\xi)^{E_1}}{\pi^{h_1}}\right)\right) > \nu(\pi^{h_1}) = \nu\big(\varphi_1^{E_1}(\xi)\big) > \nu\big(\varphi_1(\xi)\big) = \nu(\xi).$$

We set $\varphi_2(x) := \pi^{h_1F_1}\rho_1(\varphi_1(x)^{E_1}/\pi^{h_1})$ and continue the construction of our sequence of polynomials $(\varphi_t)_t$. Obviously $\deg \varphi_2 = E_1F_1$, which divides the degree of every irreducible factor of $\Phi(x)$.

Remark 9 Because the Newton polygon of $\varphi_2(x)$ consists of one segment of slope $-h_1/E_1$ with $\gcd(h_1, E_1) = 1$ and its associated polynomial with respect to x is $\underline{\rho}_1(z)$ of degree F_1, the extensions $\mathsf{K}(\alpha)$, where α is a root of $\varphi_2(x)$, have inertia degree F_1 and ramification index E_1. Hence $\varphi_2(x)$ with $\deg \varphi_2 = E_1F_1$ is irreducible.

5 The Second Iteration

Definition 10 Let $\Phi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ of degree N and $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ of degree n be monic polynomials and assume $n \mid N$. We call

$$\Phi(x) = \sum_{i=0}^{N/n} a_i(x)\varphi^i(x)$$

with $\deg(a_i) < \deg(\varphi)$ the φ-expansion of $\Phi(x)$.

We use the φ_2-expansion of $\Phi(x)$ to find the valuations $\nu(\varphi_2(\xi))$. Set $n_2 := \deg \varphi_2$ and let $\Phi(x) = \sum_{i=0}^{N/n_2} a_i(x)\varphi_2^i(x)$ be the φ_2-expansion of $\Phi(x)$. For each root ξ of $\Phi(x)$ we have

$$0 = \Phi(\xi) = \sum_{i=0}^{N/n_2} a_i(\xi)\varphi_2^i(\xi).$$

Hence

$$\chi_{2,\xi}(y) = \sum_{i=0}^{m} a_i(\xi) y^i \in \mathcal{O}_{\mathsf{K}(\xi)}[y]$$

with $m = N/n_2 = \deg(\Phi)/\deg(\varphi_2)$ is a polynomial with root $\varphi_2(\xi)$. Assume that $a_i(x) = \sum_{j=0}^{n_2-1} a_{i,j} x^j$. As the valuations

$$v_\Phi^*(\varphi_1) = \frac{h_1}{E_1}, \dots, v_\Phi^*(\varphi_1^{E_1-1}) = \frac{(E_1-1)h_1}{E_1}$$

are distinct (and not in $\mathbb{Z}$) and

$$1, \frac{\varphi_1(x)^{E_1}}{\pi^{h_1}} \underset{\Phi}{\sim} \gamma_1, \dots, \left(\frac{\varphi_1(x)^{E_1}}{\pi^{h_1}}\right)^{F_1-1} \underset{\Phi}{\sim} \gamma_1^{F_1-1}$$

are linearly independent over K, we have

$$v_\Phi^*(a_i) = \min_{0\le j\le n_2-1} \nu(a_{i,j})(h_1/E_1)j.$$

If the Newton polygon of $\chi_{2,\xi}(y)$ consists of more than one segment then $\varphi_2(x)$ fails the Newton test and we can derive a factorization of $\Phi(x)$. Otherwise let $-h_2/e_2$ be the slope of the Newton polygon of $\chi_{2,\xi}(y)$ in lowest terms. Then $\nu(\varphi_2(\xi)) = h_2/e_2$ for all roots ξ of $\Phi(x)$. We set $E_2^+ := e_2/\gcd(E_1, e_2)$. For all roots ξ of $\Phi(x)$ the ramification index of $\mathsf{K}(\xi)$ is divisible by $E_2 := E_1 \cdot E_2^+$. Because the denominator of $E_2^+ h_2/e_2$ is a divisor of E_1 there is

$$\psi_2(x) := \pi^{s_\pi} \varphi_1(x)^{s_1} = \pi^{s_\pi} x^{s_1} \in \mathsf{K}[x]$$

with $s_1 \in \{0, \dots, E_1-1\}$ and $s_\pi \in \mathbb{Z}$ such that $v_\Phi^*(\psi_2) = E_2^+ h_2/e_2$.

We flatten the Newton polygon of $\chi_{2,\xi}(y)$. Let $\beta \in \overline{\mathsf{K}}$ with $\beta^{E_2^+} = \psi_2(x)$ and consider the polynomial $\chi_{2,\xi}^\flat(y) := \chi_{2,\xi}(\beta y)/\beta^m$. As only the valuations of the coefficients of $y^{i\cdot E_2^+}$ $(0 \le i \le m/E_2^+)$ can be zero we get

$$\begin{aligned}\underline{\chi}_{2,\xi}^\flat(y) &= \sum_{i=0}^{m/E_2^+} \underline{a_{i\cdot E_2^+}(\xi)\beta^{i\cdot E_2^+ - m}}\, y^{i\cdot E_2^+} \\ &= \sum_{i=0}^{m/E_2^+} \underline{a_{i\cdot E_2^+}(\xi)\psi_2(\xi)^{i-m/E_2^+}}\, y^{i\cdot E_2^+} \in \underline{\mathsf{K}}_2[y].\end{aligned}$$

Using the relation $x^{E_1} \underset{\Phi}{\sim} \pi^{h_1}\cdot\gamma_1$, which is independent of ξ, we find coefficients $\widehat{a}_i \in \mathsf{K}_1$ with $\widehat{a}_i \underset{\Phi}{\sim} a_{i\cdot E_2^+}(x)\psi_2^{i-m/E_2^+}(x)$. We set

$$A_2(z) := \sum_{i=0}^{m/E_2^+} \widehat{a}_i z^i \underset{\Phi}{\sim} \sum_{i=0}^{m/E_2^+} a_{i\cdot E_2^+}(x)\psi_2^{i-m/E_2^+}(x) z^i$$

and obtain the *associated polynomial* $\underline{A}_2(z) \in \underline{\mathsf{K}}_1[z]$ of $\Phi(x)$ with respect to $\varphi_2(x)$.

If $\underline{A}_2(y)$ splits into two or more co-prime factors over $\underline{\mathsf{K}}_1 = \underline{\mathsf{K}}(\gamma_1)$, we can derive a factorization of $\Phi(x)$: Since $\deg \psi_2(x)$ is less than the degree of any irreducible factor of $\Phi(x)$ we have $\gcd(\psi_2(x), \Phi(x)) = 1$ and the extended Euclidean algorithm yields $\psi_2^{-1}(x) \in \mathcal{O}_{\mathsf{K}_1}[x]$ such that $\psi_2(x) \cdot \psi_2^{-1}(x) \equiv 1 \mod \Phi(x)$. The polynomial $\varphi_2^{E_2^+}(x) \cdot \psi_2^{-1}(x)$ fails the Hensel test.

Otherwise $\underline{A}_2(z) = \underline{\rho}_2(z)^{r_2}$ for some irreducible polynomial $\underline{\rho}_2(z) \in \underline{\mathsf{K}}_1[z]$. We set $\mathsf{K}_2 := \mathsf{K}(\gamma_2)$ where γ_2 is a root of a lift $\rho_2(z) \in \mathcal{O}_{\mathsf{K}_1}[z]$ of $\underline{\rho}_2(z) \in \underline{\mathsf{K}}_1[z]$, let $F_2^+ := \deg \rho_2$, and obtain $\varphi_2(x)^{E_2^+} \underset{\Phi}{\sim} \gamma_2 \psi_2(x)$.

Next we construct $\varphi_3(x) \in \mathcal{O}_{\mathsf{K}}[x]$ with $v_\Phi^*(\varphi_3) > v_\Phi^*(\varphi_2)$ and $\deg \varphi_3 = E_2 F_2$. The coefficients of $\rho_2(z) \in \mathcal{O}_{\mathsf{K}_1}$ can be written as polynomials in $\gamma_1 \underset{\Phi}{\sim} x^{E_1}/\pi^{h_1}$, say

$$\rho_2(z) = \sum_{i=0}^{F_2^+} \sum_{j=0}^{F_1-1} r_{i,j} \gamma_1^j z^i$$

where $r_{i,j} \in \mathcal{O}_{\mathsf{K}}$. We are looking for

$$\varphi_3(x) \underset{\Phi}{\sim} \psi_2(x)^{F_2^+} \rho_2 \left(\frac{\varphi_2(x)^{E_2^+}}{\psi_2(x)} \right) = \sum_{i=0}^{F_2^+} \sum_{j=0}^{F_1-1} r_{i,j} \left(\frac{x^{E_1}}{\pi^{h_1}} \right)^j \psi_2(x)^{F_2^+ - i} \varphi_2(x)^{iE_2^+}$$

with $\deg \varphi_3 = E_2 F_2 = E_2^+ F_2^+ E_1 F_1$. We have $v_\Phi^*\big(\rho_1(x^{E_1}/\pi^{h_1})\big) > 0$. If we write $\rho_1(z) = z^{F_1} + \rho_1^*(z)$ with $\deg(\rho_1^*) < F_1$ this implies

$$\varphi_1^{E_1 F_1} \underset{\Phi}{\sim} -(\pi^{h_1})^{F_1} \rho_1^* \left(\frac{x^{E_1}}{\pi^{h_1}} \right).$$

It follows that we can find a polynomial $R_{i,j}(x)$ with $\deg R_{i,j} < E_1 F_1$ such that

$$R_{i,j}(x) \underset{\Phi}{\sim} r_{i,j} \left(\frac{x^{E_1}}{\pi^{h_1}} \right)^j \psi_2(x)^{F_2^+ - i} = r_{i,j} \left(\frac{x^{E_1}}{\pi^{h_1}} \right)^j (\pi^{s_\pi} x^{s_1})^{F_2^+ - i}.$$

Thus the polynomial

$$\varphi_3(x) = \varphi_2(x)^{E_2^+ F_2^+} + \sum_{i=0}^{F_2^+ - 1} \sum_{j=0}^{F_1 - 1} R_{i,j}(x) \varphi_2(x)^{iE_2^+}$$

has the desired properties $v_\Phi^*(\varphi_3) > v_\Phi^*(\varphi_2)$ and $\deg \varphi_3 = E_2 F_2$.

Remark 11 $\varphi_3(x) \in \mathcal{O}_{\mathsf{K}}[x]$ is irreducible.

6 Data and Relations

In the algorithm we continue the construction of the sequence of polynomials $(\varphi_t)_t$ from the previous two sections. In the following steps the computation of $\psi_t(x)$, the valuation of the coefficients $a_i(x)$ of the φ_t-expansion of $\mathit{\Phi}(x)$, the coefficients of the associated polynomial, and φ_{t+1} becomes more involved and relies on the data computed in the previous iteration. We initially set

$$\mathsf{K}_0 := \mathsf{K}, \quad \varphi_1 := x, \quad E_0 := 1, \quad F_0 := 1$$

and compute the following data in every iteration:

$\varphi_t(x) \in \mathcal{O}_{\mathsf{K}}[x]$	with $v^*_{\mathit{\Phi}}(\varphi_t) > v^*_{\mathit{\Phi}}(\varphi_{t-1})$ and $n_t = \deg(\varphi_t) = E_{t-1}F_{t-1}$; an approximation to an irreducible factor of $\mathit{\Phi}(x)$
$h_t/e_t = v^*_{\mathit{\Phi}}(\varphi_t)$	with $\gcd(h_t, e_t) = 1$
$E_t^+ = \dfrac{e_t}{\gcd(E_{t-1}, e_t)}$	the increase of the maximum known ramification index
$E_t = E_t^+ \cdot E_{t-1}$	the maximum known ramification index
$\psi_t(x) = \pi^{s_\pi} \prod_{i=1}^{t-1} \varphi_i^{s_i}$	with $s_\pi \in \mathbb{Z}$ and $0 \le s_i < E_i^+$ such that $v^*_{\mathit{\Phi}}(\psi_t) = v^*_{\mathit{\Phi}}(\varphi_t^{E_t^+})$
$\underline{A}_t(y) \in \underline{\mathsf{K}}_{t-1}[y]$	the associated polynomial of $\mathit{\Phi}(x)$ with respect to $\varphi_t(x)$
$\underline{\rho}_t(y) \in \underline{\mathsf{K}}_{t-1}[y]$	irreducible with $\underline{\rho}_t^{r_t}(y) = \underline{A}_t(y)$
$\gamma_t \in \mathsf{K}_t$	such that $\varphi_t^{E_t^+} \underset{\mathit{\Phi}}{\sim} \gamma_t \psi_t$
$\mathsf{K}_t = \mathsf{K}_{t-1}(\gamma_t)$	the maximum known unramified subfield
$F_t^+ = [\mathsf{K}_t : \mathsf{K}_{t-1}]$	the increase of the maximum known inertia degree
$F_t = F_t^+ \cdot F_{t-1}$	the maximum known inertia degree

7 The u-th iteration

Assume we have computed the data and relations given above for t up to $u-1$ and that $\varphi_u(x)$ of degree $n_u = E_u F_u$ is the best approximation to an irreducible factor of $\mathit{\Phi}(x)$ found so far. We compute the φ_u-expansion $\mathit{\Phi}(x) = \sum_{i=0}^{N/n_u} a_i(x)\varphi_u(x)^i$ of $\mathit{\Phi}(x)$ and set $\chi_u(y) := \sum_{i=0}^{N/n_u} a_i(x) y^i$.

Definition 12 Let $a(x) \in \mathcal{O}_{\mathsf{K}}[x]$ with $\deg a < E_{t-1}F_{t-1}$. We call

$$a(x) = \sum_{j_{t-1}=0}^{E^+_{t-1}F^+_{t-1}-1} \varphi_{t-1}^{j_{t-1}}(x) \cdots \sum_{j_2=0}^{E_2^+F_2^+-1} \varphi_2^{j_2}(x) \sum_{j_1=0}^{E_1F_1-1} x^{j_1} \cdot a_{j_1,\dots,j_{t-1}},$$

where $a_{j_1,\dots,j_{t-1}} \in \mathcal{O}_{\mathsf{K}}$ $(0 \le j_i \le E_i,\ 0 \le i \le t)$, the $(\varphi_1, \dots, \varphi_{t-1})$-expansion of $a(x)$.

From the $(\varphi_1, \dots, \varphi_{u-1})$-expansion of $a_i(x)$ we obtain the valuations of $a_i(\xi)$ and see that they are independent of the choice of the root ξ of $\Phi(x)$. Since, by construction, the values

$$v_\Phi^*(\varphi_1), \dots, v_\Phi^*(\varphi_1^{E_1-1}), v_\Phi^*(\varphi_2), \dots, v_\Phi^*(\varphi_2^{E_2^+-1}), v_\Phi^*(\varphi_3), \dots\dots, v_\Phi^*(\varphi_{u-1}^{E_{u-1}^+-1})$$

are distinct (and not in $\mathbb{Z}$) and for $0 \le t \le u-1$ the elements

$$1, \gamma_t \underset{\Phi}{\sim} \varphi_t(x)^{E_t^+}/\psi_t(x), \dots, \gamma_t^{F_t^+-1} \underset{\Phi}{\sim} \left(\varphi_t(x)^{E_t^+}/\psi_t(x)\right)^{F_t^+-1}$$

are linearly independent over $\mathsf{K}_{t-1} = \mathsf{K}(\gamma_1, \dots, \gamma_{t-1})$ we have (see [7, Lemma 4.21]):

Lemma 13 *Let $a(x) \in \mathcal{O}_\mathsf{K}[x]$ with $\deg a < E_{t-1}F_{t-1}$ and let $a_{j_1,\dots,j_{t-1}}$, with $0 \le j_i < E_i^+F_i^+ - 1$, be the coefficients of the $(\varphi_1, \dots, \varphi_{t-1})$-expansion of $a(x)$. Then*

$$v_\Phi^*(a) = \min_{\substack{1 \le i \le t-1 \\ 1 \le j_i < E_i^+}} v_\Phi^*\big(\varphi_{t-1}^{j_{t-1}}(x) \cdots \varphi_2^{j_2}(x) \cdot x^{j_1} \cdot a_{j_1,\dots,j_{t-1}}\big).$$

If the Newton polygon of $\chi_t(y)$ consists of one segment, say of slope $-h_u/e_u$, with $\gcd(h_u, e_u) = 1$, then $\varphi_t(x)$ passes the Newton test. We set $E_u^+ := \frac{e_u}{\gcd(E_{u-1}, e_u)}$ and construct

$$\psi_u(x) = \pi^{s_\pi} \prod_{t=1}^{u-1} \varphi_t(x)^{s_t}$$

with $s_\pi \in \mathbb{Z}$ and $0 \le s_t < E_t^+$ $(1 \le t < u)$ such that $v_\Phi^*(\psi_u) = E_u^+ h_u/e_u$ using the following algorithm. For $q \in \mathbb{Q}$ we denote by $\mathrm{den}(q)$ the denominator of q in lowest terms.

Algorithm 14 (Psi)

Input: $v_\Phi^*(\varphi_i)$ and E_i^+ for $0 \le i \le t$, $E = E_0^+ \cdots E_t^+$, $v \in \mathbb{Q}$ with $E \,|\, \mathrm{den}(v)$.
Output: $s_\pi \in \mathbb{Z}$, $0 \le s_i \le E_i^+$ $(1 \le i \le t)$ such that $v_\Phi^*(\pi^{s_\pi}\varphi_0^{s_0} \cdots \varphi_t^{s_t}) = v$.

```
– $d \leftarrow E$, $i \leftarrow t$
– for $i$ from $t$ to 1 by $-1$:
    • $d \leftarrow d/E_i^+$, $v' \leftarrow v \cdot d$, $e \leftarrow v_\Phi^*(\varphi_i) \cdot d$
    • Find $s_i$ such that $e \cdot s_i \equiv v' \mod \mathrm{den}(d \cdot e)$
    • $v \leftarrow v - s_i v_\Phi^*(\varphi_i)$
– $s_\pi \leftarrow v$
– return $s_\pi, s_1, \dots, s_t$
```

Next we determine the associated polynomial $\underline{A}_u(y)$ of $\varPhi(x)$ with respect to $\varphi_u(x)$. Because we have representations of $a_i(x)$ $(0 \le i \le N/n_i)$ and $\psi_u(x)$ by power products of $\pi, \varphi_1, \ldots, \varphi_{u-1}$ we can use the relations $\varphi_t(x)^{E_t^+} \underset{\varPhi}{\sim} \gamma_t \psi_t(x)$ to find the coefficients $\widehat{a}_i \in \mathsf{K}_{u-1}$ such that $\widehat{a}_i \underset{\varPhi}{\sim} a_{i \cdot E_u^+}(x) \psi_u(x)^{i-m/E_u^+}$. We get the associated polynomial

$$\underline{A}_u(z) = \sum_{i=0}^{m/E_u^+} \underline{\widehat{a}}_i z^i$$

where $m = N/n_u$. Assume that $\underline{A}_u(z) = \underline{\rho}_u(z)^r$ for some irreducible polynomial $\underline{\rho}_u(z) \in \underline{\mathsf{K}}_{u-1}(z)$. Otherwise we can find $\vartheta(x) \in \mathsf{K}[x]$ with $\vartheta(x) \underset{\varPhi}{\sim} \varphi_u(x)^{E_u^+}/\psi_u(x)$ that fails the Hensel test, which yields a factorization of $\varPhi(x)$. Let $\rho_u(z) \in \mathsf{K}_{u-1}$ be a lift of $\underline{\rho}_u(z)$, and set $F_u^+ := \deg \rho_u$.

Finally we construct $\varphi_{u+1}(x) \in \mathcal{O}_{\mathsf{K}}[x]$ of degree $E_u F_u = E_u^+ F_u^+ E_{u-1} F_{u-1}$ such that

$$\varphi_{u+1}(x) \underset{\varPhi}{\sim} \sum_{i=0}^{F_u^+} \vartheta_i(x) \varphi_u(x)^{iE_u^+} = \psi_u(x)^{F_u^+} \rho_u(\varphi_u^{E_u^+}(x)/\psi_u(x)), \tag{2}$$

where the $\vartheta_i(x)$ are sums of power products of $\pi, \varphi_1, \ldots, \varphi_{u-1}$. For $t = u-1, u-2, \ldots, 0$ we recursively apply

$$v_{\varPhi}^* \left(\rho_t \left(\frac{\varphi_t^{E_t^+}}{\psi_t} \right) \right) > 0$$

to reduce the maximum exponent of $\varphi_t(x)$ to $E_t^+ F_t^+ - 1$, such that the degree of the $\varphi_t(x)$ term is at most $\deg(\varphi_t(x)^{E_t^+ F_t^+ - 1}) = (E_{t-1} F_{t-1})(E_t^+ F_t^+ - 1)$. Thus we can find a $\varphi_{u+1}(x)$ that fulfills the degree condition $\deg \varphi_{u+1} = E_u F_u$. Furthermore

$$v_{\varPhi}^*(\varphi_{u+1}) = v_{\varPhi}^* \left(\psi_u^{F_u^+} \rho_u \left(\frac{\varphi_u(x)^{E_u^+}}{\psi_u(x)} \right) \right) > v_{\varPhi}^* \left(\psi_u^{F_u^+} \right) \ge v_{\varPhi}^*(\varphi_u).$$

As a preparation for the next iteration we set $\mathsf{K}_u := \mathsf{K}_{u-1}(\gamma_u)$ with γ_u a root of $\rho_u(z)$ and obtain the relation $\varphi^{E_u^+}(x) \underset{\varPhi}{\sim} \gamma_u \psi_u(x)$.

Remark 15 $\varphi_{u+1}(x) \in \mathcal{O}_{\mathsf{K}}[x]$ is irreducible.

8 The Algorithm

We summarize the steps for the construction of the sequence $(\varphi_t(x))_t$ in an algorithm. Although we use the unramified extensions K_t/K above and in the algorithm, in practice the γ_i are represented as elements in the residue class field

$\underline{\mathsf{K}}_t$. Furthermore, many of the manipulations in the algorithm can be conducted on the representations of $\psi_t(x)$ as power products of $\pi, \varphi_1(x), \ldots, \varphi_{t-1}(x)$ and of $a_i(x)$ as sums of power products of $\pi, \varphi_1(x), \ldots, \varphi_{t-1}(x)$ thus reducing these operations to operations of vectors of integers.

Algorithm 16 (Polynomial Factorization)

```
Input:   a monic, separable, squarefree polynomial $\varPhi(x)$ over a local field $\mathsf{K}$.
Output:  a proper factorization of $\varPhi(x)$ if one exists,
         a two-element certificate for $\varPhi(x)$ otherwise.

(1) Initialize $t \leftarrow 1$, $\varphi_1(x) \leftarrow x$, $E_0 = 1$, $F_0 = 1$, $\mathsf{K}_0 = \mathsf{K}$.
(2) Repeat:
    (a) Find the $\varphi_t$ expansion $\varPhi(x) = \sum_{i=1}^{N/\deg\varphi_t} a_i(x)\varphi(x)^i$ of $\varPhi(x)$.
    (b) Find $v_{\varPhi}^*(a_i)$ for $0 \le i \le N/\deg\varphi_t$.
    (c) If $\varphi_t(x)$ fails the Newton test: return a proper factorization of $\varPhi(x)$.
    (d) $h_t/e_t \leftarrow v_{\varPhi}^*(\varphi)$ with $\gcd(h_t, e_t) = 1$; $E_t^+ \leftarrow \frac{e_t}{\gcd(e_t, E)}$; $E_t \leftarrow E_t^+ \cdot E_{t-1}$.
    (e) Construct $\psi_t(x) = \pi^{s_\pi} \prod_{i=1}^{t-1} \varphi_i(x)^{s_i}$ with $v_{\varPhi}^*(\psi_t) = E_t^+ v_{\varPhi}^*(\varphi_t)$, $s_\pi \in \mathbb{N}$,
        $0 \le s_i < E_i^+$ $(1 \le i \le t-1)$, $\deg\psi_t < E_i F_i$.
    (f) Compute the associate polynomial $\underline{A}_t(z)$.
    (g) Find a factorization of $\underline{A}_t(z) \in \mathsf{K}_t(z)$.
    (h) If $\underline{A}_t(z)$ has two co-prime factors: return a proper factorization of $\varPhi(x)$.
    (i) $F_t^+ \leftarrow \deg\underline{\rho}$ where $\underline{\rho}_t(z)^r = \underline{A}_t(z)$, $\underline{\rho}_t(z) \in \underline{\mathsf{K}}_{t-1}[z]$ irreducible; $F_t \leftarrow$
        $F_t^+ \cdot F_{t-1}$, $\mathsf{K}_t \leftarrow \mathsf{K}[x]/(\rho_t(x))$.
    (j) If $E_t F_t = \deg\varPhi$: return a two-element certificate for $\varPhi(x)$.
    (k) Find $\varphi_{t+1}(x) \underset{\varPhi}{\sim} \rho_t\bigl(\varphi_t(x)^{E_t^+} / \psi_t(x)^{\deg(\rho)}\bigr)$ of degree $n_{t+1} = E_t F_t$ in $\mathcal{O}_{\mathsf{K}}[x]$.
    (l) $t \leftarrow t + 1$.
```

Certificates for Irreducibility

If $\varPhi(x)$ is irreducible we will have $E_t F_t = N$ for some t. We obtain the two element certificate (Definition 6) for the irreducibility of $\varPhi(x)$ as follows. A polynomial $\varPi(x) \in \mathsf{K}[x]$ with $v_{\varPhi}^*(\varPi) = 1/E_t$ can be found using Algorithm 14. If $F_t = 1$ we can choose $\varGamma(x) = x$. If $F_t \neq 1$, let i be maximal with $F_i^+ \neq 0$. We find $\varGamma(x) \in \mathsf{K}[x]$ with $\varGamma(x) \underset{\varPhi}{\sim} \varphi_i(x)^{E_i^+}/\psi_i(x)$.

9 Complexity

We restrict our analysis of the complexity of the algorithm to the main loop. The first complexity estimate for the Montes algorithm, restricted to irreducibility testing, was given by Veres [17] and improved by Ford and Veres [5]. The complexity estimate for determining the irreducibility of a polynomial $\varPhi(x) \in \mathbb{Z}_p[x]$ of degree N using this algorithms is $O(N^{3+\varepsilon}\nu(\operatorname{disc}\varPhi) + N^{2+\varepsilon}\nu(\operatorname{disc}\varPhi)^{2+\varepsilon})$. The running time of the Round Four algorithm is analyzed in [14], but without taking into account the precision loss in the computation of greatest common divisors. Both estimates rely on Theorem 5 to bound the number of iterations and the required precision and only differ slightly in the exponent of the discriminant of $\Phi(x)$.

Lemma 17 *Let $\Phi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be of degree N and let $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be monic of degree n. Then the φ-expansion of $\Phi(x)$ can be computed in $O(N^2)$ operations in $\mathcal{O}_{\mathsf{K}}$.*

Proof. In order to determine the φ-expansion $\Phi(x) = \sum_{i=1}^{N/n} a_i(x)\varphi(x)^i$ we first compute $q_0(x), a_0(x) \in \mathcal{O}_{\mathsf{K}}[x]$ with $\Phi(x) = \varphi(x)q_0(x) + a_0(x)$, which can be done in $O((N-n)n)$ operations in $\mathcal{O}_{\mathsf{K}}[x]$. Next we determine $q_1(x), a_1(x) \in \mathcal{O}_{\mathsf{K}}[x]$ with $q_0(x) = \varphi(x)q_1(x) + a_1(x)$ ($O((N-2n)n)$ operations in $\mathcal{O}_{\mathsf{K}}[x]$), and so on. Therefore the φ-expansion of $\Phi(x)$ can be computed in

$$O((N-n)n)+O((N-2n)n)+\cdots+O((2n)n) = O\left(n\left(\frac{N^2}{n} - n\sum_{i=0}^{N/n} i\right)\right) = O(N^2)$$

operations in $\mathcal{O}_{\mathsf{K}}$.

The computation of the $(\varphi_1, \dots, \varphi_{t-1})$-expansion of a polynomial $a(x) \in \mathcal{O}_{\mathsf{K}}[x]$ of degree $m \le \deg\varphi_t - 1$ consists of the recursive computation of φ_{t-1}, φ_{t-2}, $\dots$, φ_2, and φ_1-expansions. Let $n_i = \deg\varphi_i$ $(1 \le i \le t)$. The φ_{t-1}-expansion of $a(x)$ yields up to m/n_{t-1} polynomials of degree less than n_t. The φ_{t-2}-expansions of these polynomials yield up to $m/n_{t-1} \cdot n_{t-1}/n_{t-2} = m/n_{t-2}$ of degree less than n_{t-2}. Thus the $(\varphi_1, \dots, \varphi_{t-1})$-expansion of $a(x)$ can be computed in

$$O\left(m^2\right) + O\left(\tfrac{m}{n_t}{n_t}^2\right) + O\left(\tfrac{m}{n_{t-1}}n_{t-1}^2\right) + \cdots + O\left(\tfrac{m}{n_1}n_1^2\right) + O(m)$$

operations in $\mathcal{O}_{\mathsf{K}}$. Because $n_{i+1}/n_i \ge 2$ this is less than

$$O\left(m^2\right) + O\left(\tfrac{m^2}{2}\right) + \cdots + O\left(\tfrac{m^2}{2^{t-1}}\right) + O(m) = O\left(m^2 \textstyle\sum_{i=0}^{\lfloor \log_2 m \rfloor} 2^{-i}\right) = O(m^2).$$

Lemma 18 *The $(\varphi_0, \dots, \varphi_{t-1})$-expansion of $a(x) \in \mathcal{O}_{\mathsf{K}}[x]$ with $m = \deg a \le \deg\varphi_t - 1$ can be computed in $O(m^2)$ operations in $\mathcal{O}_{\mathsf{K}}$.*

By Theorem 5 the polynomial $\Phi(x)$ is irreducible, if $Nv_\Phi^*(\varphi_t) > 2\nu(\operatorname{disc}\Phi)$ for some $t \in \mathbb{N}$. In every iteration the increase from $v_\Phi^*(\varphi_t)$ to $v_\Phi^*(\varphi_{t+1})$ is at least $2/N$, unless $E = N$, but that would imply irreducibility. Thus the algorithm terminates after at most $\nu(\operatorname{disc}\Phi)$ iterations.

In our analysis of the cost of the steps in the main loop we exclude the cost of finding a proper factorization to a desired precision using the methods of section 2 in steps **(c)** and **(h)**. We assume that two polynomials of degree up to n can be multiplied in $O(n \log n \log\log n) = O(n^{1+\varepsilon})$ operations in their coefficient ring [15].

(a,b,c,d) By Lemma 18 the φ_t-expansion

$$\Phi(x) = \varphi_t(x)^{N/n_t} + \sum_{i=0}^{N/n_t-1} a_i(x)\varphi_t(x)^i$$

of $\Phi(x)$ and the $(\varphi_1, \ldots, \varphi_t)$-expansion of the $a_i(x)$ can be computed in $O(N^2)$ operations in $\mathcal{O}_{\mathsf{K}}$.

(e) The exponents $s_\pi, s_1, \ldots, s_{t-1}$ in $\psi_t(x) = \pi^{s_\pi}\varphi_1(x)^{s_0} \cdots \varphi_{t-1}(x)^{s_{t-1}}$ with $v^*_\Phi(\psi) = h_t/e_t$ can be computed with Algorithm 14. The most expensive computation is the extended Euclidean construction, which for integers less than N runs in time $O((\log N)^2)$, at most $\log_2 N$ times.

(f) We have a representation of $a_i(x)\psi_t(x)^{i-(N/n_t)}$ $(1 \le i \le N/n_t)$ as n_t sums of power products of $\pi, \varphi_1(x), \ldots, \varphi_{t-1}(x)$. In this representation only the exponents of $\varphi_i(x)$ where $E_i^+ F_i^+ \neq 1$ are non-zero. There are at most $\log_2 N$ such indices i. Let m_t be the number of $i < t$ with $E_i^+ F_i^+ \neq 1$. Reducing the coefficients of the associated polynomial in this representation using the relations $\varphi_i(x)^{E_i^+}/\psi_i(x) \underset{\Phi}{\sim} \gamma_i$ $(1 \le i \le m_t)$ takes at most $N\sum_{i=1}^{m_t} i = O(N(\log N)^2)$ integer additions and $N(t-1) = O(N \log N)$ multiplications in the finite field $\underline{\mathsf{K}}_t$ with q^F elements.

(g,h) The factorization of a polynomial of degree at most N/F over a finite field with at most q^F elements can be done in $O((N/F)^2 \log q^F)$ bit operations [6].

(j) The cost of finding the exponents for the representation of $\Pi(x) \in \mathsf{K}[x]$ with $v^*_\Phi(\Pi) = 1/E$ as a power product of $\pi, \varphi_1(x), \ldots, \varphi_t(x)$ is the same as the cost of finding $\psi(x)$ in step **(f)**. The polynomial $\Gamma(x)$ can be computed in the same way as the coefficients $\vartheta_i(x)$ in step **(l)**.

(k) The polynomial $\varphi_{t+1}(x)$ is constructed as a polynomial in $\varphi_t(x)^{E_t^+}$ of degree F_t^+ with coefficients $\vartheta_i(x)$, $0 \le i \le F_t^+$, (see (2)), obtained from the representations of the elements γ_u as $\varphi_u(x)^{E_u}/\psi_u(x)$ and

$$v^*_\Phi\big(\rho_u(\varphi_u(x)^{E_u}/\psi_u(x))\big) > 0$$

for $1 \le u \le t-1$. This is done by manipulating the exponents in the representation of the polynomials as sums of power products of $\pi, \varphi_1(x), \ldots, \varphi_t(x)$. The computation of $\varphi_t(x)^{E_t^+}$ takes $\log_2 E_t$ multiplications of polynomials of degree up to $E_t^+ E_{t-1} F_{t-}t < N$. For $2 \le j \le F_t^+$ the polynomial $\big(\varphi_t(x)^{E_t^+}\big)^j$ can be computed in F_t^+ multiplications of polynomials of degree up to $E_t F_t < N$. For $1 \le t-2$ the exponent of $\varphi_i(x)$ in the representation of $\vartheta_i(x)$ as a power product of $\varphi_1(x), \ldots, \varphi_{t-1}(x)$ is less than $E_i^+ F_i^+$. This gives less than $\log N$ multiplications of polynomials of degree less than N. As in (e) the exponents of at most $\log N$ of the $\varphi_i(x)$ are nonzero. Therefore in total this step can be conducted in $O(N^{2+\varepsilon})$ operations in $\mathcal{O}_{\mathsf{K}}[x]$.

By Theorem 5 the maximum of the valuations $\nu(v^*_\Phi(\xi))$, where ξ is a root of $\Phi(x)$, is less than $2\big(\nu(\operatorname{disc}\Phi)\big)/N$. This is also the maximal (absolute) slope of the Newton polygon of the polynomials under consideration. Therefore a precision of $2\nu(\operatorname{disc}\Phi)$ is sufficient for all operations in the main loop.

Theorem 1. *Let p be a fixed prime. We can find a breaking element or a two element certificate for the irreducibility of a polynomial $\Phi(x) \in \mathbb{Z}_p[x]$ in at most $O(N^{2+\varepsilon}\nu(\operatorname{disc}\Phi)^{2+\varepsilon})$ operations of integers less than p.*

10 Example

We show that $\Phi(x) = x^{32} + 16 \in \mathbb{Z}_2[x]$ is irreducible using Algorithm 16.

Initially we set $\varphi_1(x) = x$, $E_0 = 1$, $F_0 = 1$, $\mathsf{K}_0 = \mathbb{Q}_2$.

(a) The φ_1-expansion of $\Phi(x)$ is $\Phi(x) = \sum_{i=0}^{32} a_i(x)\varphi_0(x)^i = x^{32} + 16$.
(b) The valuations of the coefficients are $v_\Phi^*(a_0) = 4$, $v_\Phi^*(a_i) = \infty$ for $1 \le i \le 31$, and $v_\Phi^*(a_{32}) = 0$.
(c,d) $\varphi_1(x)$ passes the Newton test; we get $v_\Phi^*(\varphi_1) = \frac{h_1}{e_1} = \frac{4}{32} = \frac{1}{8}$, so $E_1^+ = 8$ and $E_1 = 8$.
(e) We set $\psi_1(x) = 2$ as $v_\Phi^*(\varphi_1^{E_1^+}) = v_\Phi^*(x^8) = 1$.
(f,g) $A_1(z) = z^4 + 1$ with $\underline{A}_1(z) = (z-1)^4$ in $\mathbb{F}_2[z]$.
(h,i) $\frac{\varphi_1(x)^8}{\psi_1(x)}$ passes the Hensel test; we get $F_1^+ = 1$, $\mathsf{K}_1 = \mathbb{Q}_2$, $F_1 = 1$.
(k) We obtain the next approximation of an irreducible factor of $\Phi(x)$:

$$\varphi_2(x) = 2\left(\frac{x^8}{2} - 1\right) = x^8 - 2.$$

Second iteration:

(a) The φ_2-expansion of $\Phi(x)$ is

$$\Phi(x) = \varphi_2(x)^4 + 8\varphi_2(x)^3 + 24\varphi_2(x)^2 + 32\varphi_2(x) + 32.$$

(b) The valuations of the coefficients are $v_\Phi^*(32) = 5$, $v_\Phi^*(24) = 3$, $v_\Phi^*(8) = 3$, and $v_\Phi^*(1) = 0$.
(c,d) $\varphi_2(x)$ passes the Newton test; we get $\frac{h_2}{e_2} = \frac{5}{4}$, so $E_2^+ = 1$, $E_2 = 8$.
(e) We set $\psi_2(x) = \frac{x^2}{2}$, so that $v_\Phi^*(\psi_2) = \frac{5}{4}$.
(f,g) The associated polynomial with respect to $\varphi_2(x)$ is $A_2(z) = z^4 + 1 = (z-1)^4 \in \mathbb{F}_2[z]$.
(h,i) $\frac{\varphi_2(x)}{\psi_2(x)}$ passes the Hensel test, we get $F_2^+ = 1$, $\mathsf{K}_2 = \mathbb{Q}_2$, $F_2 = 1$.
(l) We set

$$\varphi_3(x) = \psi_2(x)\left(\frac{\varphi_2(x)}{\psi_2(x)} - 1\right) = x^8 - 2x^2 - 2.$$

Third iteration:

(a) The φ_3-expansion of $\Phi(x)$ is

$$\Phi(x) = \varphi_3(x)^4 + a_3(x)\varphi_3(x)^3 + a_2(x)\varphi_3(x)^2 + a_1(x)\varphi_3(x) + a_0(x)$$

where $a_3(x) = 8x^2 + 8$, $a_2(x) = 24x^4 + 48x^2 + 24$, $a_1(x) = 32x^6 + 96x^4 + 96x^2 + 48$, $a_0(x) = 64x^6 + 96x^4 + 96x^2 + 64$.

(b) The valuations of the coefficients are $v^*_\Phi(a_0) = \frac{21}{4}$, $v^*_\Phi(a_1) = 4$, $v^*_\Phi(a_2) = 3$, $v^*_\Phi(a_3) = 3$, and $v^*_\Phi(1) = 0$.
(c,d) $\varphi_3(x)$ passes the Newton test; we get $v^*_\Phi(\varphi_3) = \frac{h_3}{e_3} = \frac{21}{16}$, $E_3^+ = 2$, $E_3 = 16$.
(e) We find $\psi_3(x) = 2^2x^5$; so that $v^*_\Phi(\psi_3) = v^*_\Phi(\varphi_3^{E_3^+}) = \frac{21}{8}$.
(f,g) The associated polynomial with respect to $\varphi_3(x)$ is $\underline{A}_2(z) = z^2 + 3 = (z-1)^3 \in \mathbb{F}_2[z]$.
(h,i) $\frac{\varphi_3(x)}{\psi_3(x)}$ passes the Hensel test; we get $F_3^+ = 1$, $\mathsf{K}_3 = \mathbb{Q}_2$, $F_3 = 1$.
(l) We set

$$\varphi_4(x) = x^{16} - 4x^{10} - 4x^8 - 4x^5 + 4x^4 + 8x^2 + 4.$$

Fourth iteration:

(a) Let $\Phi(x) = \varphi_4(x)^2 + a_1(x)\varphi_4(x) + a_0(x)$ be the φ_4-expansion of $\Phi(x)$.
(b) We have $v^*_\Phi(a_0) = 85/16$ and $v^*_\Phi(a_1) = 3$.
(c,d) $\varphi_4(x)$ passes the Newton test; we get $\frac{h_4}{e_4} = \frac{85}{32}$, $E_4^+ = 2$, $E_4 = 32$.
(g) Now $E_4F_4 = 32 = \deg\Phi$ which implies the irreducibility of $\Phi(x) = x^{32} + 16$.

11 Acknowledgments

The author would like to thank the anonymous referees and David Ford for their numerous comments. He apologizes to them for the large number of small mistakes.

References

1. J.J. Cannon et al., *The computer algebra system Magma*, University of Sydney (2010) `http://magma.maths.usyd.edu.au/magma/`.
2. D. G. Cantor and D. Gordon, *Factoring polynomials over p-adic fields* in *Algorithmic Number Theory, 9th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2000*, LNCS 1838, Springer Verlag 2000.
3. D. Ford and P. Letard, *Implementing the Round Four maximal order algorithm*, Journal de Théorie des Nombres de Bordeaux **6** (1994), 39–80.
4. D. Ford, S. Pauli, and X.-F. Roblot, *A Fast Algorithm for Polynomial Factorization over $\mathbb{Q}_p$*, Journal de Théorie des Nombres de Bordeaux **14** (2002), 151–169.
5. D. Ford and O. Veres, *On the Complexity of the Montes Ideal Factorization Algorithm*, in G. Hanrot and F. Morain and E. Thomé, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010*, LNCS, Springer Verlag 2010.
6. E. Kaltofen and V. Shoup, *Subquadratic-time factoring of polynomials over finite fields*, Math. Comp. **67** (1998).
7. J. Guardia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, `arXiv:0807.2620` (2008).
8. J. Guardia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, `arXiv:0807.4065` (2008).
9. S. MacLane, *A Construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. 40 (1936), 363–395.

10. J. Montes and E. Nart, *On a Theorem of Ore*, Journal of Algebra **146** (1992), 318–334.
11. J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.
12. Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann **99** (1928), 84–117.
13. PARI/GP, version `2.3.4`, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr/`.
14. S. Pauli, *Factoring polynomials over local fields*, J. Symb. Comp. **32** (2001), 533–547.
15. A. Schönhage and V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing **7** (1971), 281–292.
16. W. Stein et al, *SAGE: Software for Algebra and Geometry Experimentation*, 2007, `http://www.sagemath.org`.
17. O. Veres, *On the Complexity of Polynomial Factorization over p-adic Fields*, PhD Dissertation, Concordia University, Montreal, 2009.