On the Complexity of the Montes Ideal Factorization Algorithm

David Ford and Olga Veres

Concordia University,
1455 de Maisonneuve Boulevard West,
Montréal, Québec, Canada H3G 1J1
ford@cse.concordia.ca,
overes@mathstat.concordia.ca

Abstract. Let p be a rational prime and let $\Phi(X)$ be a monic irreducible polynomial in $\mathbf{Z}[X]$, with $n_\Phi = \deg \Phi$ and $\delta_\Phi = v_p(\operatorname{disc} \Phi)$. In [13] Montes describes an algorithm for the decomposition of the ideal $p\,\mathcal{O}_K$ in the algebraic number field K generated by a root of Φ. A simplified version of the Montes algorithm, merely testing $\Phi(X)$ for irreducibility over $\mathbf{Q}_p$, is given in [19], together with a full Maple implementation and a demonstration that in the worst case, when $\Phi(X)$ is irreducible over $\mathbf{Q}_p$, the expected number of bit operations for termination is $O(n_\Phi^{3+\epsilon}\delta_\Phi^{2+\epsilon})$. We now give a refined analysis that yields an improved estimate of $O(n_\Phi^{3+\epsilon}\delta_\Phi + n_\Phi^{2+\epsilon}\delta_\Phi^{2+\epsilon})$ bit operations. Since the worst case of the simplified algorithm coincides with the worst case of the original algorithm, this estimate applies as well to the complete Montes algorithm.

1 Introduction

In an algebraic number field K with ring of integers $\mathcal{O}_K$, factorization of the ideal $p\mathcal{O}_K$, for p prime, can be determined via polynomial factorization over the field of p-adic numbers $\mathbf{Q}_p$ [12].

If $K = \mathbf{Q}(\alpha)$ for a given $\alpha \in \mathcal{O}_K$ such that the index $\left[\mathcal{O}_K : \mathbf{Z}[\alpha]\right]$ is not divisible by p then the factorization of the ideal $p\mathcal{O}_K$ can be determined by polynomial factorization modulo p [5,6,7]. In practice, efficient techniques for polynomial factorization modulo p [1,2,4] combined with Hensel lifting [12,20] solve the problem of factoring $p\mathcal{O}_K$ in a straightforward and effective manner when p does not divide the index.

The complications arising when p divides the index $\left[\mathcal{O}_K : \mathbf{Z}[\alpha]\right]$ have been the subject of considerable study. Current ideas are derived from the "Round Four" algorithm of Zassenhaus [20], which has evolved into two main variations, the "one-element" method [8] and the "two-element" method [16]. Versions of the one-element method are used by Maple and PARI. The two-element method is used, *e.g.*, by Magma.

The algorithm of Montes [13] is in a separate category.

Given a monic irreducible polynomial $\Phi(X)$ in $\mathbf{Z}[X]$, the Montes algorithm determines the number of irreducible factors of $\Phi(X)$ in $\mathbf{Z}_p[X]$ and their respective degrees. The algorithm exploits classical results of Ore [15,14] on Newton

G. Hanrot, F. Morain, and E. Thomé (Eds.): ANTS-IX 2010, LNCS 6197, pp. 174–185, 2010.

polygons and provides an alternative to the methods based on ideas of Zassenhaus.

A familiar application of Newton polygons gives the p-adic valuations of roots of a polynomial in $\mathbf{Z}_p[X]$. If $\Phi(X) \in \mathbf{Z}_p[X]$ has two roots with different p-adic values then Hensel-lifting techniques can be applied to construct a non-trivial p-adic factorization of Φ to any desired degree of precision.

This process constitutes "level 0" of the Montes algorithm.

For each factor of Φ revealed at level 0, the algorithm proceeds to higher levels, either to discover a refined factorization or to establish irreducibility.

At level r, with $\varphi_r(X)$ an irreducible monic polynomial in $\mathbf{Z}_p[X]$ and V_r a valuation of $\mathbf{Q}_p[X]$, the algorithm constructs the φ_r-adic expansion of a given polynomial and then computes

- a finite field $\mathbf{F}_{q_r}$,
- the Newton polygon $\mathcal{N}_r(\Phi)$ of Φ with respect to the valuation V_r,
- a slope $-d_r/e_r$, with d_r and e_r coprime positive integers, of an edge of $\mathcal{N}_r(\Phi)$,
- the "associated polynomial" $\Psi^{(r)}_{\mathcal{S},\Phi}(Y) \in \mathbf{F}_{q_r}[Y]$ for each segment $\mathcal{S}$ of $\mathcal{N}_r(\Phi)$,
- a monic irreducible factor ψ_r of $\Psi^{(r)}_{\mathcal{S},\Phi}$ with ξ_r a root of ψ_r and $f_r = \deg \psi_r$,
- a valuation V_{r+1} of $\mathbf{Q}_p[X]$,
- an irreducible monic polynomial $\varphi_{r+1}(X) \in \mathbf{Z}_p[X]$.

The number of edges of $\mathcal{N}_r(\Phi)$ and the number of distinct irreducible factors of $\Psi^{(r)}_{\mathcal{S},\Phi}$ give information for the factorization of Φ; if either is greater than one then Φ is reducible.

Our goal being to give an estimate of the complexity of the worst case of the Montes algorithm, we have restricted the algorithm merely to decide the question of irreducibility of a given polynomial. When Φ is irreducible over $\mathbf{Q}_p$ the Newton polygon at each level is a single segment. It is apparent that this is the most costly case, *i.e.*, the case that reaches the highest level, for the full algorithm. So our restricted algorithm operates under the assumption that $\mathcal{N}_r(\Phi)$ has just one edge at each level r; the failure of this condition terminates the restricted algorithm.

In [19, Chapter 3] a complete Maple implementation of the restricted Montes algorithm is given, together with a demonstration that in the worst case, when Φ is irreducible over $\mathbf{Q}_p$, the expected number of bit operations for termination is $O(n_\Phi^{3+\epsilon}\delta_\Phi^{2+\epsilon})$, with $n_\Phi = \deg \Phi$ and $\delta_\Phi = v_p(\operatorname{disc} \Phi)$. In the present paper we give a refined analysis that yields an improved estimate of $O(n_\Phi^{3+\epsilon}\delta_\Phi + n_\Phi^{2+\epsilon}\delta_\Phi^{2+\epsilon})$ bit operations. Since the worst case of the simplified algorithm coincides with the worst case of the original algorithm, this estimate applies as well to the full Montes algorithm.

2 Definitions and Notation

Definition 1. *Let $\varphi_0(X) = X$ and let V_0 denote the standard p-adic valuation of $\mathbf{Q}_p$. For $K(X) \in \mathbf{Q}_p[X]$ and $r \geq 1$, the level-r Newton polygon of K, denoted*

$\mathcal{N}_r(K)$, is the Newton polygon of K with respect to the valuation V_r of $\mathbf{Q}_p[X]$, which can be defined recursively as

$$V_r(K) = \min\left\{ e_{r-1}V_{r-1}\big(A_{r-1,k}\big) + kV_r\big(\varphi_{r-1}\big) \;\big|\; 0 \le k \le n \right\}$$

with $K(X) = \sum_{k=0}^{n} A_{r-1,k}(X)\,\varphi_{r-1}(X)^k$ the φ_{r-1}-adic expansion of $K(X)$.

Remark 1. $\mathcal{N}_r(K)$ is the lower convex hull of the set

$$\{\, (k, V_r(A_{r,k}\,\varphi_r^k)) \mid 0 \le k \le n,\ A_{r,k}(X) \ne 0 \,\},$$

and if $\deg K < \deg \varphi_r$ then $\mathcal{N}_r(K) = \{(0, V_r(K))\}$ and $V_{r+1}(K) = e_r V_r(K)$.

Definition 2. *For $r \ge 1$ and $K(X)$ a nonzero polynomial in $\mathbf{Z}_p[X]$ we define $\mathcal{S}_{r,K}$ to be the segment of $\mathcal{N}_r(K)$ having slope $-d_r/e_r$.*

Definition 3. *For positive integers r and ν we define*

$$\begin{aligned}
\alpha_{r,\nu} &= \nu d_r^{-1}\ \mathbf{mod}\ e_r\,,\\
\beta_{r,\nu} &= (\nu - \alpha_{r,\nu} d_r)/e_r\,,\\
\mathcal{T}_{r,\nu} &= \{\, (\alpha_{r,\nu} + \lambda e_r,\ \beta_{r,\nu} - \lambda d_r) \mid 0 \le \lambda \le \lfloor \beta_{r,\nu}/d_r \rfloor \,\}\,.
\end{aligned}$$

Remark 2. If $\mathcal{L}$ is the line through the point $(0, \nu/e_r)$ with slope $-d_r/e_r$ then $\mathcal{T}_{r,\nu}$ is the longest segment of $\mathcal{L}$ with endpoints having nonnegative integer coordinates.

Definition 4. *For $r \ge 0$ we define*

$$\begin{aligned}
&\overline{\mu}_r = 0\,, && \overline{\nu}_r = 0\,, && \textit{if } r = 0\,,\\
&\overline{\mu}_r = d_{r-1} + e_{r-1}\overline{\nu}_{r-1}\,, && \overline{\nu}_r = e_{r-1} f_{r-1}\overline{\mu}_r\,, && \textit{if } r \ge 1\,.
\end{aligned}$$

Remark 3. For $r \ge 1$ it is easily seen that $\overline{\mu}_r = V_r(\varphi_{r-1})$ and $\overline{\nu}_r = V_r(\varphi_r)$.

Definition 5 (*Associated Polynomial*). *Let $r \ge 0$, let α and β be nonnegative integers, and let $\mathcal{S}$ be an arbitrary segment of slope $-d_r/e_r$ with left endpoint (α, β). Let $m_0 = 0$ and for $r \ge 1$ and $k \ge 0$ define*

$$\begin{aligned}
m_r &= (1/d_r)\ \mathbf{mod}\ e_r\,,\\
\Omega_r &= \begin{cases} 1 & \textit{if } r = 1\,,\\ \Omega_{r-1}^{e_{r-1} f_{r-1}}\,\xi_{r-1}^{m_{r-1} f_{r-1}\overline{\mu}_r} & \textit{if } r > 1\,,\end{cases}\\
\Theta(\mathcal{S}, r, k) &= \left\lfloor m_{r-1}\frac{(\beta - kd_r) - (\alpha + ke_r)\,\overline{\nu}_r}{e_{r-1}} \right\rfloor,\\
\Gamma_{\mathcal{S},r,k} &= \Omega_r^{\alpha + ke_r}\,\xi_{r-1}^{\Theta(\mathcal{S},r,k)} \in \mathbf{F}_{q_r}\,.
\end{aligned}$$

Let $K(X) \in \mathbf{Z}_p[X]$ have φ_r-adic expansion

$$K(X) = A_0(X) + A_1(X)\,\varphi_r(X) + \cdots + A_n(X)\,\varphi_r(X)^n$$

with $d_r j + e_r V_r(A_j \varphi_r^j) \ge d_r\alpha + e_r\beta$ *for* $j = 0, \ldots, n$ *and let*

$$J = \left\{ k \;\middle|\; 0 \le k \le \lfloor (n-\alpha)/e_r \rfloor,\ \big(\alpha + ke_r,\, V_r(A_{\alpha+ke_r}\,\varphi_r^{\alpha+ke_r})\big) \in \mathcal{S} \right\}.$$

We define the level-r associated polynomial of K with respect to $\mathcal{S}$ *to be*

$$\Psi^{(r)}_{\mathcal{S},K}(Y) = \textstyle\sum_{k\in J} \eta_k Y^k$$

with $\eta_k \in \mathbf{F}_{q_r}$ *defined as*

$$\eta_k = \begin{cases} \overline{A}_{\alpha+ke_0} & \textit{if } r = 0\,, \\ \overline{B}_k(\xi_0)\,, \qquad \textit{with } B_k(X) = A_{\alpha+ke_1}(X)\,/\,p^{\beta-kd_1}\,, & \textit{if } r = 1\,, \\ \Gamma^{-1}_{\mathcal{S},r,k}\Psi^{(r-1)}_{\mathcal{I}_{r-1,\nu_k},A_{\alpha+ke_r}}(\xi_{r-1})\,, \quad \textit{with } \nu_k = V_r(A_{\alpha+ke_r})\,, & \textit{if } r \ge 2\,. \end{cases}$$

We further define the natural level-r associated polynomial of K *to be*

$$\widetilde{\Psi}^{(r)}_K(Y) = \Psi^{(r)}_{\mathcal{S}_{r,K},K}(Y)\,.$$

Remark 4. The polynomial $\widetilde{\Psi}^{(r)}_K(Y)$ has nonzero constant term.

3 Outline of the Restricted Montes Algorithm

A complete Maple implementation of the restricted Montes algorithm, with proofs and explanatory comments interspersed, is given in [19]. Here we give an outline showing the three major phases of the algorithm. The algorithm begins in phase M_0 (level 0), then alternates between phase M_1 and phase M_2 (level r, for $r = 1, 2, \ldots$) until reaching a terminating condition.

- input: $\Phi(X) \in \mathbf{Z}[X]$ monic and irreducible, $p \in \mathbf{Z}$ prime
- output: $\begin{cases} \text{TRUE} & \text{if } \Phi(X) \text{ is irreducible over } \mathbf{Q}_p[X], \\ \text{FALSE} & \text{if } \Phi(X) \text{ is reducible over } \mathbf{Q}_p[X]. \end{cases}$

$\mathbf{M_0}$**:** 1. Factorize Φ modulo p:

$$\Phi \equiv \psi_{0,1}^{a_{0,1}} \cdots \psi_{0,\kappa_0}^{a_{0,\kappa_0}} \pmod{p}\,.$$

2. If $\kappa_0 > 1$ then **return** FALSE.
If $\kappa_0 = 1$ and $a_{0,1} = 1$ then **return** TRUE.
3. Define $\varphi_0(X) = X,\ n_0 = 1,\ d_0 = 0,\ e_0 = 1,$
$\psi_0 = \psi_{0,1},\ f_0 = \deg\psi_0,\ \xi_0$ a root of ψ_0.
4. Set $r \leftarrow 1$.

$\mathbf{M_1}$**:** 5. If $r = 1$ let $\varphi_1(X)$ be a monic polynomial in $\mathbf{Z}[X]$ such that $\overline{\varphi}_1 = \psi_0$.
If $r > 1$ construct H_{r-1} according to Algorithm 1 in Sect. 6 below and let

$$\varphi_r = \varphi_{r-1}^{e_{r-1}f_{r-1}} + H_{r-1}\,.$$

6. Define $n_r = e_{r-1} f_{r-1} n_{r-1} = \deg \varphi_r$.
7. If $r > 1$ and $e_{r-1} f_{r-1} = 1$ then replace $\varphi_{r-1} \leftarrow \varphi_r$ and $r \leftarrow r - 1$.

$\mathbf{M_2}$ **:** 8. If $\varphi_r = \Phi$ then **return** TRUE.
If $\varphi_r \mid \Phi$ and $\varphi_r \neq \Phi$ then **return** FALSE.
9. Let $\mathcal{S}_{r,1}, \ldots, \mathcal{S}_{r,\lambda_r}$ be the segments of $\mathcal{N}_r(\Phi)$ and let $\zeta_{r,k} + 1$ be the number of points on $\mathcal{S}_{r,k}$ with integer coordinates, for $k = 1, \ldots, \lambda_r$.
10. If $\lambda_r > 1$ then **return** FALSE.
If $\lambda_r = 1$ and $\zeta_{r,1} = 1$ then **return** TRUE.
11. Let $-d_r/e_r$ be the slope of $\mathcal{S}_{r,1}$, with d_r and e_r relatively prime and $e_r > 0$, and construct $\widetilde{\Psi}_{\Phi}^{(r)}(Y) \in \mathbf{F}_{q_r}[Y]$.
12. Factorize
$$\widetilde{\Psi}_{\Phi}^{(r)} = c_r\, \psi_{r,1}^{a_{r,1}} \cdots \psi_{r,\kappa_r}^{a_{r,\kappa_r}}$$
over $\mathbf{F}_{q_r}$, with $c_r \in \mathbf{F}_{q_r}$ a nonzero constant.
13. If $\kappa_r > 1$ then **return** FALSE.
If $\kappa_r = 1$ and $a_{r,1} = 1$ then **return** TRUE.
14. Define $\psi_r = \psi_{r,1}$, $f_r = \deg \psi_r$, ξ_r a root of ψ_r.
15. Replace $r \leftarrow r + 1$.
Go to M_1.

4 Complexity of Fundamental Operations

Notation. We use $\langle \texttt{alpha} \rangle_{\mathbf{F}_p}$ and $\langle \texttt{alpha} \rangle_{\mathbf{Q}}$ to denote the number of operations in $\mathbf{F}_p$ and $\mathbf{Q}$ respectively required for the execution of the procedure `alpha`. We use the notation
$$f(n) \in O(n^{k+\epsilon})$$
as an alternative to the "soft-O" notation
$$f(n) \in O^{\sim}(n^k) \;\equiv\; f(n) \in O(n^k (\ln n)^c)$$
for some positive constant c (see [9]). For $n \geq 3$ and q a prime power we define the following.
$$\mathsf{L}(n) = \ln n \ln \ln n \qquad \mathsf{F}(n,q) = n\, \mathsf{M}(n) \ln(qn)$$
$$\mathsf{M}(n) = n\, \mathsf{L}(n) \qquad \mathsf{K}(q) = \mathsf{M}(\ln q) \ln \ln q$$

We are concerned with the reducibility of the monic polynomial $\Phi(X) \in \mathbf{Z}_p[X]$ for some prime p. We let δ_Φ denote $v_p(\operatorname{disc} \Phi)$ and we let $p^{\delta^*_\Phi}$ denote the p-adic reduced discriminant of Φ [8, Appendix A]. It is clear that $\delta^*_\Phi \leq \delta_\Phi$.

Magnitude of p. To simplify the subsequent discussion we impose the condition that $p \in O(1)$, by which we mean that p is a small prime, not exceeding the magnitude of a single machine word.

Arithmetic in $\mathbf{Z}_p$. If $F(X) \in \mathbf{Z}[X]$ with $F(X) \equiv \Phi(X) \pmod{p^{2\delta^*_\Phi+1}\mathbf{Z}_p[X]}$ then $\Phi(X)$ is reducible in $\mathbf{Z}_p[X]$ if and only if $F(X)$ is reducible in $\mathbf{Z}_p[X]$. Thus in our computations p-adic integers are represented as rational approximations with $2\delta^*_\Phi + 1$ p-adic digits of precision, *i.e.*, as rational integers reduced modulo $p^{2\delta^*_\Phi+1}$.

Schönhage and Strassen have shown that the time required to perform an arithmetic operation on two rational integers of length m is $O(\mathsf{M}(m))$; see [9, Ch.8, §8.3]. It follows that if we represent p-adic integers in this fashion then the cost of an arithmetic operation is $O(\Delta_\Phi)$, with

$$\Delta_\Phi = \mathsf{M}(\delta^*_\Phi \ln p)\,.$$

Arithmetic in $\mathbf{F}_q$. By [9, Ch.14, §14.7], a single operation in $\mathbf{F}_q$ can be performed in $O(\mathsf{K}(q))$ word operations. If $q = p^{f^*}$ the assumption that $\ln p \in O(1)$ gives $\ln q = f^* \ln p \in O(f^*)$ and thus the cost of an operation in $\mathbf{F}_q$ is

$$O(\mathsf{K}(q)) = O\big(\mathsf{M}(\ln q)\ln\ln q\big) \subseteq O\big(f^*(\ln f^*)^2 \ln\ln f^*\big) \subseteq O\big(f^{*\,(1+\epsilon)}\big)\,.$$

For $\alpha \in \mathbf{F}_q$ and any integer n the cost of computing α^n is

$$O(\ln q\,\mathsf{K}(q)) \subseteq O(f^* f^{*\,(1+\epsilon)}) = O(f^{*\,(2+\epsilon)})$$

since we may assume $0 \le n \le q-1$. By [18, Theorem 10], the asymptotic cost for constructing an irreducible polynomial of degree n over the finite field $\mathbf{F}_q$ is

$$O\big((n^2 \ln n + n \ln q)\,\mathsf{L}(n)\big)\,.$$

Polynomial Arithmetic. The number of operations required to evaluate a polynomial of degree n at a given point using Horner's rule is $O(n)$. By [17] and [3], the number of operations needed to multiply two polynomials of degree at most n is $O(\mathsf{M}(n))$. It follows that the number of operations needed to compute the m^{th} power of a polynomial of degree n is

$$O\big(nm\ln^2(nm)\big) \subseteq O\big((nm)^{1+\epsilon}\big)\,.$$

By [9, Ch 14, §14.4 and §14.5], the expected number of operations in $\mathbf{F}_q$ needed to factorize a polynomial of degree n over $\mathbf{F}_q$ is

$$O(\mathsf{F}(n,q)) \subseteq O(n^{2+\epsilon}\ln q)\,.$$

Let $\varphi(X)$ be a monic polynomial in $\mathbf{Z}_p[X]$ of degree n_φ, let $f(X)$ be a polynomial in $\mathbf{Z}_p[X]$ of degree n, and let $k_\varphi = \lfloor n/n_\varphi \rfloor$. Let $E(f,k_\varphi)$ denote the number of operations in $\mathbf{Z}_p$ needed to compute the φ-adic expansion

$$f(X) = \textstyle\sum_{i=1}^{k_\varphi} a_i(X)\,\varphi^i(X)\,.$$

From [9, Ch 5, §5.11], we have

$$E(f,k_\varphi) \in O(k_\varphi(k_\varphi+1)n_\varphi^2) = O(n_\varphi^2 k_\varphi^2) = O(n^2)\,.$$

5 Complexity of the Algorithm

Finite Fields. For $r \geq 0$ the finite field $\mathbf{F}_{q_{r+1}}$ is implemented as $\mathbf{F}_p[\rho_r]$, with

- ρ_r of a root of ψ_r^*,
- $\psi_r^*(Y)$ an arbitrary irreducible monic polynomial in $\mathbf{F}_p[Y]$ of degree f_r^*,
- $f_r^* = f_0 \cdots f_r$.

Thus $\mathbf{F}_{q_{r+1}} = \mathbf{F}_{q_r}[\xi_r] = \mathbf{F}_p[\xi_0, \ldots, \xi_r] = \mathbf{F}_p[\rho_r]$ and $q_{r+1} = q_r^{f_r} = p^{f_r^*}$.

Computing the Newton Polygon. It follows from [19, Theorem 15] that the recursive computation of $V_r(\Phi)$ requires $O(n_\Phi^{2+\epsilon}\Delta_\Phi)$ operations in $\mathbf{Q}$ and that this dominates the cost of constructing $\mathcal{N}_r(\Phi)$.

Computing $\boldsymbol{\varphi_r}$. The construction of $\varphi_r = \varphi_{r-1}^{e_{r-1}f_{r-1}} + H_{r-1}$ is explained in Sect. 6 below. The cost of computing $\varphi_{r-1}^{e_{r-1}f_{r-1}}$ is

$$\big\langle \varphi_{r-1}^{e_{r-1}f_{r-1}} \big\rangle_{\mathbf{F}_p} = 0\,,$$
$$\big\langle \varphi_{r-1}^{e_{r-1}f_{r-1}} \big\rangle_{\mathbf{Q}} \in O\big((n_{r-1}e_{r-1}f_{r-1})^{1+\epsilon}\Delta_\Phi\big) = O\big(n_r^{1+\epsilon}\Delta_\Phi\big)\,.$$

A slight modification of the proof of [19, Theorem 17] shows that the cost of constructing $H_{r-1} = H_{r-1,\overline{\nu}_r,\gamma_{r-1}}$ is

$$\big\langle H_{r-1} \big\rangle_{\mathbf{F}_p} \in O\big(r f_{r-1} f_{r-2}^{*\,(3+\epsilon)}\big) \subseteq O(r n_r^{3+\epsilon})\,,$$
$$\big\langle H_{r-1} \big\rangle_{\mathbf{Q}} \in O\big(r n_r^{1+\epsilon}\Delta_\Phi\big)\,.$$

Thus the cost of computing φ_r is dominated by the cost of computing H_{r-1}.

Computing the Associated Polynomial. It follows from [19, Theorem 16] that if $r \geq 2$ then

$$\big\langle \widetilde{\Psi}_\Phi^{(r)} \big\rangle_{\mathbf{F}_p} \in O(n_\Phi n_r^{1+\epsilon}) \subseteq O(n_\Phi^{2+\epsilon})\,,$$
$$\big\langle \widetilde{\Psi}_\Phi^{(r)} \big\rangle_{\mathbf{Q}} \in O\big(n_\Phi n_r^{1+\epsilon}\Delta_\Phi\big) \subseteq O\big(n_\Phi^{2+\epsilon}\Delta_\Phi\big)\,.$$

Total Complexity. The cost of phase M_0 is dominated by the cost of factorizing Φ over $\mathbf{F}_p$. Hence

$$\big\langle \mathrm{M}_0 \big\rangle_{\mathbf{F}_p} \in O(\mathsf{F}(n_\Phi, p)) \subseteq O(n_\Phi^{2+\epsilon})\,,$$
$$\big\langle \mathrm{M}_0 \big\rangle_{\mathbf{Q}} \in O(1)\,.$$

The cost of phase M_1 is dominated by the cost of constructing φ_r. Hence

$$\big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{F}_p} \in O(rn_r^{3+\epsilon})\,,$$
$$\big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{Q}} \in O\big(rn_r^{1+\epsilon}\Delta_\Phi\big)\,.$$

The cost in **Q**-operations of phase M_2 is dominated by the construction of the Newton polygon $\mathcal{N}_r(\Phi)$ and of the associated polynomial $\widetilde{\Psi}_\Phi^{(r)}$, each of which require $O(n_\Phi^{2+\epsilon}\Delta_\Phi)$ operations in $\mathbf{Q}$. Since $\mathbf{F}_{q_{r+1}} = \mathbf{F}_p[\rho_r]$, the necessity of expressing ξ_r and ρ_{r-1} in terms of ρ_r arises. This is achieved in each case by factoring ψ^*_{r-1} over $\mathbf{F}_p[\rho_r]$, which requires $O(f_r^{*3+\epsilon}) \subseteq O(n_\Phi^{3+\epsilon})$ operations in $\mathbf{F}_p$. These are the dominant finite-field operations in M_2, hence

$$\big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{F}_p} \in O(n_\Phi^{3+\epsilon})\,,$$
$$\big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{Q}} \in O(n_\Phi^{2+\epsilon}\Delta_\Phi)\,.$$

We now estimate the number of operations required for the chain of computations

$$\mathrm{M}_0(\Phi) \to \mathrm{M}_1(1) \to \mathrm{M}_2(1) \to \mathrm{M}_1(2) \to \mathrm{M}_2(2) \to \cdots \to \mathrm{M}_1(m) \to \mathrm{M}_2(m)$$

with the algorithm terminating at level m. We note that at level r we have $n_0 < n_1 < \cdots < n_r$ with $n_0 \mid n_1 \mid \cdots \mid n_r$. Hence $2^r \le n_r$ and thus $r \in O(\ln n_r)$. It follows that $m \in O(\ln n_\Phi)$ and we have

$$\begin{aligned}
&\big\langle \mathrm{M}_0(F)\big\rangle_{\mathbf{F}_p} + \textstyle\sum_{r=1}^m \big(\big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{F}_p} + \big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{F}_p}\big)\\
&\quad = \big\langle \mathrm{M}_0(F)\big\rangle_{\mathbf{F}_p} + \textstyle\sum_{r=1}^m \big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{F}_p} + \sum_{r=1}^m \big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{F}_p}\\
&\quad \in O\big(n_\Phi^{2+\epsilon} + m^2 n_\Phi^{3+\epsilon} + m n_\Phi^{3+\epsilon}\big)\\
&\quad \subseteq O\big(n_\Phi^{3+\epsilon}\big)\,,\\
&\big\langle \mathrm{M}_0(F)\big\rangle_{\mathbf{Q}} + \textstyle\sum_{r=1}^m \big(\big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{Q}} + \big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{Q}}\big)\\
&\quad = \big\langle \mathrm{M}_0(F)\big\rangle_{\mathbf{Q}} + \textstyle\sum_{r=1}^m \big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{Q}} + \sum_{r=1}^m \big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{Q}}\\
&\quad \in O\big(n_\Phi + m^2 n_\Phi^{1+\epsilon}\Delta_\Phi + m n_\Phi^{2+\epsilon}\Delta_\Phi\big)\\
&\quad \subseteq O\big(n_\Phi^{2+\epsilon}\Delta_\Phi\big)\,.
\end{aligned}$$

From [16, Proposition 4.1] it follows that the case $e_{r-1}f_{r-1} = 1$ can occur at most

$$2\,\frac{e^*_{r-2}}{n_\Phi}\,v_p(\operatorname{disc}\Phi) \;\le\; 2\,v_p(\operatorname{disc}\Phi)$$

times. Hence the sequence

$$\mathrm{M}_1(r) \to \mathrm{M}_2(r-1) \to \mathrm{M}_1(r)$$

can occur at most $2v_p(\operatorname{disc}\Phi)$ times in the course of the computation. From the results above we have

$$\langle \mathrm{M}_1(r)\rangle_{\mathbf{F}_p} + \langle \mathrm{M}_2(r-1)\rangle_{\mathbf{F}_p} \in O(rn_r^{3+\epsilon} + n_\Phi^{3+\epsilon}) \subseteq O(n_\Phi^{3+\epsilon}),$$

$$\langle \mathrm{M}_1(r)\rangle_{\mathbf{Q}} + \langle \mathrm{M}_2(r-1)\rangle_{\mathbf{Q}} \in O(rn_r^{1+\epsilon} + n_\Phi^{2+\epsilon}\Delta_\Phi) \subseteq O(n_\Phi^{2+\epsilon}\Delta_\Phi).$$

Since $\delta_\Phi^* \le \delta_\Phi$ and $\ln p \in O(1)$ we have

$$\Delta_\Phi = \mathsf{M}(\delta_\Phi^* \ln p) \in O(\delta_\Phi^{1+\epsilon}).$$

It now follows that the expected number of operations required for the restricted Montes algorithm to terminate is

$$O\big(2\delta_\Phi(n_\Phi^{3+\epsilon} + n_\Phi^{2+\epsilon}\Delta_\Phi)\big) \subseteq O\big(n_\Phi^{3+\epsilon}\,\delta_\Phi + n_\Phi^{2+\epsilon}\,\delta_\Phi^{2+\epsilon}\big).$$

Remark 5. This is a slight improvement on the estimate $O(n_\Phi^{3+\epsilon}\delta_\Phi^{2+\epsilon})$ from [19]. By way of comparison, Pauli [16] gives an estimate of

$$O\big(n_\Phi^{3+\epsilon}\,\delta_\Phi^{1+\epsilon} + n_\Phi^{2+\epsilon}\,\delta_\Phi^{2+\epsilon}\big)$$

bit operations for factorization of a univariate polynomial over $\mathbf{Q}_p$ via the "two-element" method.

6 The Construction of φ_r

Algorithm 1 (Montes). *Given d_s, e_s, f_s, etc., for $1 \le s \le r$ and given*

- *an integer t in the range $1 \le t \le r$,*
- *an integer $\nu \ge \overline{\nu}_{t+1}$,*
- *a nonzero polynomial $\delta(Y) \in \mathbf{F}_{q_t}[Y]$ of degree less than f_t,*

to construct a polynomial $H_{t,\nu,\delta}(X) \in \mathbf{Z}_p[X]$ such that

- $\deg H_{t,\nu,\delta} < n_{t+1}$,
- $V_{t+1}(H_{t,\nu,\delta}) = \nu$,
- $\Psi^{(t)}_{\mathcal{T}_{t,\nu},\,H_{t,\nu,\delta}}(Y) = \delta(Y)$.

Construction. Let $\zeta_0, \ldots, \zeta_{f_t-1}$ in $\mathbf{F}_{q_t}$ be such that

$$\delta(Y) = \textstyle\sum_{i=0}^{f_t-1} \zeta_i\, Y^i.$$

Since $\delta(Y) \ne 0$ the set $J_\delta = \{\, i \mid 0 \le i \le f_t - 1,\ \zeta_i \ne 0 \,\}$ is not empty. For $i \in J_\delta$ we construct $K_i(X)$ as follows.

- We take $\delta_i(Y)$ to be the unique polynomial in $\mathbf{F}_{q_{t-1}}[Y]$ of degree less than f_{t-1} such that $\delta_i(\xi_{t-1}) = \Gamma_{\mathcal{T}_{t,\nu},t,i}\,\zeta_i$.

- If $t = 1$ we take $P_i(X)$ to be a polynomial in $\mathbf{Z}_p[X]$ of degree less than f_0 such that $\overline{P}_i(Y) = \delta_i(Y)$ and we set
$$K_i(X) = p^{\beta_{1,\nu} - id_1} P_i(X) .$$
- If $t \geq 2$ we let $\nu_i = (\beta_{t,\nu} - id_t) - (\alpha_{t,\nu} + ie_t)\overline{\nu}_t$ and we set
$$K_i(X) = H_{t-1,\,\nu_i,\,\delta_i}(X) .$$

Having constructed $K_i(X)$ for $i \in J_\delta$, we set
$$H_{t,\nu,\delta}(X) = \textstyle\sum_{i \in J_\delta} K_i(X)\,\varphi_t(X)^{\alpha_{t,\nu}+ie_t} . \qquad \square$$

Remark 6. It follows from [13, Proposition 3.2] that Algorithm 1 correctly constructs the polynomial $H_{t,\nu,\delta}$ with the indicated properties.

The construction of $\delta_i(Y)$ in Algorithm 1 being rather complicated, we provide some implementation details.

Computing $\boldsymbol{\Upsilon_r}$. If $r > 0$ we construct $\Upsilon_r \in \mathbf{F}_p^{f_r^* \times f_r \times f_{r-1}^*}$ such that
$$\rho_{r-1}^k\,\xi_r^j \;=\; \textstyle\sum_{h=0}^{f_r^*-1} (\Upsilon_r)_{h,j,k}\,\rho_r^h$$
for $j = 0, \ldots, f_r - 1$, $k = 0, \ldots, f_{r-1}^* - 1$. In practice we construct $\widetilde{\Upsilon}_r \in \mathbf{F}_p^{f_r^* \times f_r^*}$ and $\widetilde{M} \in \mathbf{F}_p^{f_r^*}$ such that
$$(\widetilde{\Upsilon}_r)_{1+h,1+j+kf_r} \;=\; (\Upsilon_r)_{h,j,k}\,, \quad \widetilde{M}_{1+j+kf_r} \;=\; M_{j,k}\,,$$
for $h = 0, \ldots, f_r^* - 1$, $j = 0, \ldots, f_r - 1$, $k = 0, \ldots, f_{r-1}^* - 1$.

Deriving $\boldsymbol{\delta_i}$ from $\boldsymbol{\Upsilon_{t-1}}$. Given $i \in J_\delta$ and $t \geq 2$, let
$$\Gamma_{\mathcal{T}_{t,\nu},t,i}\,\zeta_i \;=\; \kappa_{i,0} + \kappa_{i,1}\,\rho_{t-1} + \cdots + \kappa_{i,f_{t-1}^*-1}\,\rho_{t-1}^{f_{t-1}^*-1} \;\in\; \mathbf{F}_p[\rho_{t-1}] \;=\; \mathbf{F}_{q_t} .$$
For $j = 0, \ldots, f_{t-1} - 1$, $k = 0, \ldots, f_{t-2}^* - 1$, let $M_{j,k} \in \mathbf{F}_p$ satisfy
$$\textstyle\sum_{j=0}^{f_{t-1}-1} \sum_{k=0}^{f_{t-2}^*-1} (\Upsilon_{t-1})_{h,j,k}\,M_{j,k} \;=\; \kappa_{i,h}$$
for $h = 0, \ldots, f_{t-1}^* - 1$, and let
$$\delta_i(Y) \;=\; \textstyle\sum_{j=0}^{f_{t-1}-1} \big(\sum_{k=0}^{f_{t-2}^*-1} M_{j,k}\,\rho_{t-2}^k\big)\,Y^j .$$
Then $\delta_i(Y) \in \mathbf{F}_p[\rho_{t-2}][Y] = \mathbf{F}_{q_{t-1}}[Y]$ and
$$\begin{aligned}
\delta_i(\xi_{t-1}) &= \textstyle\sum_{j=0}^{f_{t-1}-1} \sum_{k=0}^{f_{t-2}^*-1} M_{j,k}\,\rho_{t-2}^k\,\xi_{t-1}^j \\
&= \textstyle\sum_{j=0}^{f_{t-1}-1} \sum_{k=0}^{f_{t-2}^*-1} M_{j,k} \sum_{h=0}^{f_{t-1}^*-1} (\Upsilon_{t-1})_{h,j,k}\,\rho_{t-1}^h \\
&= \textstyle\sum_{h=0}^{f_{t-1}^*-1} \sum_{j=0}^{f_{t-1}-1} \sum_{k=0}^{f_{t-2}^*-1} (\Upsilon_{t-1})_{h,j,k}\,M_{j,k}\,\rho_{t-1}^h \\
&= \textstyle\sum_{h=0}^{f_{t-1}^*-1} \kappa_{i,h}\,\rho_{t-1}^h \\
&= \Gamma_{\mathcal{T}_{t,\nu},t,i}\,\zeta_i .
\end{aligned}$$

The essential properties of φ_r are as follows (see [19, Proposition 9]).

Proposition 1 (Montes). *Let d_s, e_s, f_s, φ_s, ψ_s, etc., be given for $1 \le s \le r-1$ and let*

$$\gamma_{r-1}(Y) = \Omega_{r-1}^{-e_{r-1}f_{r-1}}(\psi_{r-1}(Y) - Y^{f_{r-1}}),$$
$$\varphi_r(X) = \varphi_{r-1}(X)^{e_{r-1}f_{r-1}} + H_{r-1,\overline{\nu}_r,\gamma_{r-1}}(X)\,.$$

Then $\varphi_r(X)$ is a monic polynomial in $\mathbf{Z}_p[X]$ with the following properties.

- $\deg \varphi_r = n_r$.
- $\mathcal{N}_{r-1}(\varphi_r)$ *consists of the single segment* $\mathcal{S}_{r-1,\varphi_r}$.
- $V_r(\varphi_r) = \overline{\nu}_r$.
- $\widetilde{\Psi}_{\varphi_r}^{(r-1)}(Y) = \Omega_{r-1}^{-e_{r-1}f_{r-1}}\psi_{r-1}(Y)$.
- φ_r *is irreducible over* $\mathbf{Z}_p$.

7 Supplementary Remarks

The Maple code from [19], including an example, can be found at this URL.

`http://www.mathstat.concordia.ca/faculty/ford/Student/Veres/mmtest.mpl`

Two recent monographs by Guàrdia, Montes, and Nart give a thorough revision of the theory underlying the Montes algorithm [10] and a detailed description of the algorithm [11]. Algorithm 1 and Proposition 1 in Sect. 6 above appear in [10]. A simpler choice for Ω_r (see Definition 5) is also given, but with no effect on the complexity of the algorithm.

References

1. Berlekamp, E.R.: Factoring Polynomials over Finite Fields. Bell Systems Technical Journal 46, 1853–1859 (1967)
2. Berlekamp, E.R.: Factoring Polynomials over Large Finite Fields. Math. Comp. 24, 713–735 (1970)
3. Cantor, D.G., Kaltofen, E.: On Fast Multiplication of Polynomials over Arbitrary Algebras. Acta Informatica 28(7), 693–701 (1991)
4. Cantor, D.G., Zassenhaus, H.: A New Algorithm for Factoring Polynomials Over Finite Fields. Math. Comp. 36, 587–592 (1981)
5. Dedekind, R.: Supplement X to Vorlesungen über Zahlentheorie von P.G. Lejeune Dirichlet (2nd ed.). Vieweg, Braunschweig (1871); Also Werke 3, 223–261 (1932) (in part)
6. Dedekind, R.: Sur la théorie des nombres entiers algébriques. Gauthier-Villars (1877); Also Bull. des Sci. Math. Astron. 11(1), 278–288 (1876); 1(2), 17–41, 69–92, 144–164, 207–248 (1877) and Werke 3, 263–296 (1932) (in part)
7. Dedekind, R.: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen 23, 1–23 (1878)

8. Ford, D., Pauli, S., Roblot, X.-F.: A Fast Algorithm for Polynomial Factorization over $\mathbf{Q}_p$. Journal de Théorie des Nombres de Bordeaux 14, 151–169 (2002)
9. von zur Gathen, J., Gerhard, J.: Modern computer algebra. Cambridge University Press, Cambridge (1999)
10. Guàrdia, J., Montes, J., Nart, E.: Newton polygons of higher order in algebraic number theory (2008), arXiv:0807.2620v2[math.NT]
11. Guàrdia, J., Montes, J., Nart, E.: Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields (2008), arXiv:0807.4065v3[math.NT]
12. Hensel, K.: Theorie der algebraischen Zahlen. Teubner, Leipzig (1908)
13. Montes, J.: Polígonos de Newton de orden superior y aplicaciones aritméticas. PhD thesis, Universitat de Barcelona (1999)
14. Montes, J., Nart, E.: On a theorem of Ore. Journal of Algebra 146, 318–334 (1992)
15. Ore, Ø.: Newtonsche Polygone in der Theorie der algebraischen Körper. Math. Ann. 99 (1928)
16. Pauli, S.: Factoring Polynomials over Local Fields. Journal of Symbolic Computation 32(5), 533–547 (2001)
17. Schönhage, A., Strassen, V.: Schnelle Multiplikation großer Zahlen. Computing 7, 281–292 (1971)
18. Shoup, V.: Fast Construction of Irreducible Polynomials over Finite Fields. Journal of Symbolic Computation 17, 371–394 (1994)
19. Veres, O.: On the Complexity of Polynomial Factorization over p-adic Fields. PhD Dissertation, Concordia University (2009), `http://www.mathstat.concordia.ca/faculty/ford/Student/Veres/vthp.pdf`
20. Zassenhaus, H.: On Hensel factorization II. In: Symposia Mathematica XV, Instituto Di Alta Matematica, pp. 499–513. Academic Press, New York (1975)