

On the Complexity of the Montes Ideal Factorization Algorithm

David Ford and Olga Veres

Concordia University, Montréal

Introduction

Suppose we have the following.

- K : algebraic number field
- \mathcal{O}_K : ring of integers
- p : prime
- \mathbf{Q}_p : field of p -adic numbers
- α : element of \mathcal{O}_K such that $K = \mathbf{Q}(\alpha)$

- Factorization of $p\mathcal{O}_K$ can be determined via polynomial factorization over \mathbf{Q}_p .
- **If** $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ **then** factorization modulo p (plus Hensel lifting) suffices.

Complications arise when $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

- Zassenhaus —
 - Round Two (1965): *If an order is not p -maximal then it is a proper sub-order of its (p -local) coefficient ring.*
 - Round Four (1975): *Reducibility of a polynomial in $\mathbf{Q}_p[X]$ is revealed when the π -adic expansion of a root becomes ambiguous.*
 - “one-element” variation: MAPLE, PARI
 - “two-element” variation: Magma
- Montes —
 - Berwick (1927), Ore (1928): *Partial factorizations of ideals via Newton polygons*
 - MacLane (1936): *Characterization of valuations of polynomial rings*
 - Montes (1999), Guàrdia, Montes, Nart (2008): *Exploitation of “higher order” Newton polygons to produce a complete ideal factorization algorithm*

Elements of the Algorithm

The monic irreducible polynomial $f(X)$ in $\mathbf{Z}[X]$ is given.

Level 0. Standard use of Newton polygons to find the p -adic valuations of roots of $f(X)$.

Level r ($r \geq 1$). Successive construction of the following:

- an irreducible monic polynomial $\varphi_r(X)$ in $\mathbf{Z}_p[X]$;
- a valuation V_r of $\mathbf{Q}_p[X]$;
- the φ_r -adic expansion of $f(X)$;
- a finite field \mathbf{F}_{q_r} ;
- the Newton polygon $\mathcal{N}_r(f)$ of f 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 $\mathcal{N}_r(f)$;
- the "associated polynomial" $\psi_{r,\Phi}^{(r)}(Y) \in \mathbf{F}_{q_r}[Y]$ for each segment \mathcal{S} of $\mathcal{N}_r(f)$;
- a monic irreducible factor ψ_r of $\psi_{r,\Phi}^{(r)}$ 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 $\varphi_{r+1}(X) \in \mathbf{Z}_p[X]$.

Reducibility. The polynomial $f(X)$ is reducible if, for some $r \geq 0$,

- $\mathcal{N}_r(f)$ has two or more edges, or
- $\mathcal{S}_{\Phi}^{(r)}(Y)$ has two or more irreducible factors in $\mathbf{F}_{q^r}[Y]$.

Worst case. The polynomial $f(X)$ is irreducible in $\mathbf{Q}_p(X)$.

- The Newton polygon at each level is a single segment.
- The algorithm reaches the maximum level.
- Veres (2009): complexity is $O(n_{\Phi}^{3+\epsilon} \delta_{\Phi}^{2+\epsilon})$, with $n_{\Phi} = \deg f$ and $\delta_{\Phi} = v_p(\text{disc } f)$.
- Ford & Veres (2010): complexity is $O(n_{\Phi}^{3+\epsilon} \delta_{\Phi} + n_{\Phi}^{2+\epsilon} \delta_{\Phi}^{2+\epsilon})$.

Definitions and Notation

Definition. 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

$$V_r(K) = \min \{ e_{r-1}V_{r-1}(A_{r-1,k}) + kV_r(\varphi_{r-1}) \mid 0 \leq k \leq n \}$$

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

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

and if $\deg K < \deg \varphi_r$ then

$$\mathcal{N}_r(K) = \{(0, V_r(K))\}, \quad V_{r+1}(K) = e_r V_r(K).$$

Definition. For $r \geq 1$ 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. For positive integers r and ν we define

$$\alpha_{r,\nu} = \nu d_r^{-1} \bmod e_r, \quad \beta_{r,\nu} = (\nu - \alpha_{r,\nu} d_r)/e_r, \quad \mathcal{T}_{r,\nu} = \{ (\alpha_{r,\nu} + \lambda e_r, \beta_{r,\nu} - \lambda d_r) \mid 0 \leq \lambda \leq \lfloor \beta_{r,\nu}/d_r \rfloor \}.$$

Remark. 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. For $r \geq 0$ we define

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

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

Associated Polynomial

Definition. Let $r \geq 0$, 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 $r \geq 1$ and $k \geq 0$ define

$$m_r = (1/d_r) \bmod e_r, \quad \Theta(\mathcal{S}, r, k) = \left\lfloor m_{r-1} \frac{(\beta - kd_r) - (\alpha + ke_r) \bar{\nu}_r}{e_{r-1}} \right\rfloor,$$

$$\Omega_r = \begin{cases} 1 & \text{if } r = 1, \\ \Omega_{r-1}^{e_{r-1} f_{r-1}} \xi_{r-1}^{m_{r-1} f_{r-1} \bar{\mu}_r} & \text{if } r > 1, \end{cases} \quad \Gamma_{\mathcal{S}, r, k} = \Omega_r^{\alpha + ke_r} \xi_{r-1}^{\Theta(\mathcal{S}, r, k)} \in \mathbf{F}_{q_r}.$$

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 $d_r j + e_r V_r(A_j \varphi_r^j) \geq d_r \alpha + e_r \beta$ for $j = 0, \dots, n$ and let

$$J = \{ k \mid 0 \leq k \leq \lfloor (n - \alpha)/e_r \rfloor, (\alpha + ke_r, V_r(A_{\alpha + ke_r} \varphi_r^{\alpha + ke_r})) \in \mathcal{S} \}.$$

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

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

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

$$\eta_k = \begin{cases} \bar{A}_{\alpha + ke_0} & \text{if } r = 0, \\ \bar{B}_k(\xi_0), & \text{with } B_k(X) = A_{\alpha + ke_1}(X) / p^{\beta - kd_1}, \text{ if } r = 1, \\ \Gamma_{\mathcal{S}, r, k}^{-1} \Psi_{\mathcal{I}_{r-1, \nu_k, A_{\alpha + ke_r}}}^{(r-1)}(\xi_{r-1}), & \text{with } \nu_k = V_r(A_{\alpha + ke_r}), \text{ if } r \geq 2. \end{cases}$$

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

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

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

Outline of the Restricted Algorithm

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

M₀: 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 $\varphi_0(X) = X$,

$$\begin{aligned} n_0 &= 1, & \psi_0 &= \psi_{0,1}, \\ d_0 &= 0, & f_0 &= \deg \psi_0, \\ e_0 &= 1, & \xi_0 &\text{ a root of } \psi_0. \end{aligned}$$

4. Initialize $r \leftarrow 1$.

M₁: 5. If $r = 1$ let $\varphi_1(X)$ be a monic polynomial in $\mathbf{Z}[X]$ such that $\bar{\varphi}_1 = \psi_0$.

If $r > 1$ construct H_{r-1} according to the algorithm 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 $r \leftarrow r - 1$.

M₂: 8. If $\varphi_r = \Phi$ then **return** TRUE.

If $\varphi_r \mid \Phi$ and $\varphi_r \neq \Phi$ then **return** FALSE.

9. Let $\mathcal{S}_{r,1}, \dots, \mathcal{S}_{r,\lambda_r}$ 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 $k = 1, \dots, \lambda_r$.

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

$$\tilde{\Psi}_{\Phi}^{(r)}(Y) \in \mathbf{F}_{q_r}[Y].$$

12. Factorize

$$\tilde{\Psi}_{\Phi}^{(r)} = c_r \psi_{r,1}^{a_{r,1}} \cdots \psi_{r,\kappa_r}^{a_{r,\kappa_r}}$$

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 **M₁**.

Complexity of the Restricted Algorithm

Sequences

$$\tilde{M}_m \equiv M_0(\) \rightarrow M_1(1) \rightarrow M_2(1) \rightarrow M_1(2) \rightarrow M_2(2) \rightarrow \cdots \rightarrow M_1(m) \rightarrow M_2(m)$$

$$\hat{M}_r \equiv M_1(r) \rightarrow M_2(r-1) \rightarrow M_1(r) \quad (\text{when } e_{r-1}f_{r-1} = 1)$$

Remarks

- $n_\Phi = \deg \quad$.
- $\delta_\Phi = v_p(\text{disc } \quad)$.
- $n_r = \deg \varphi_r = e_{r-1}f_{r-1}n_{r-1} \geq 2^r \implies r \in O(\ln n_r)$.
- $\quad_\Phi = \text{cost of an arithmetic operation in } \mathbf{Z}_p \in O(\delta_\Phi^{1+\epsilon})$.
- [Pauli, 2001] $\implies \hat{M}_r$ occurs at most $2v_p(\text{disc } \quad)$ times

Execution Costs

Newton Polygon

$$\langle V_r(\) \rangle_{\mathbf{F}_p} = 0$$

$$\langle V_r(\) \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \ \Phi)$$

$$\langle \mathcal{N}_r(\) \rangle_{\mathbf{F}_p} = 0$$

$$\langle \mathcal{N}_r(\) \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \ \Phi)$$

$$\varphi_r \leftarrow \varphi_{r-1}^{e_{r-1}f_{r-1}} + \mathbf{H}_{r-1}$$

$$\langle \varphi_{r-1}^{e_{r-1}f_{r-1}} \rangle_{\mathbf{F}_p} = 0$$

$$\langle \varphi_{r-1}^{e_{r-1}f_{r-1}} \rangle_{\mathbf{Q}} \in O(n_r^{1+\epsilon} \ \Phi)$$

$$\langle \mathbf{H}_{r-1} \rangle_{\mathbf{F}_p} \in O(rn_r^{3+\epsilon})$$

$$\langle \mathbf{H}_{r-1} \rangle_{\mathbf{Q}} \in O(rn_r^{1+\epsilon} \ \Phi)$$

$$\langle \varphi_r \rangle_{\mathbf{F}_p} \in O(rn_r^{3+\epsilon})$$

$$\langle \varphi_r \rangle_{\mathbf{Q}} \in O(rn_r^{1+\epsilon} \ \Phi)$$

Associated Polynomial

$$\langle \widetilde{\ }_{\Phi}^{(r)} \rangle_{\mathbf{F}_p} \in O(n_{\Phi}^{2+\epsilon})$$

$$\langle \widetilde{\ }_{\Phi}^{(r)} \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \ \Phi)$$

Phase \mathbf{M}_0

$$\langle \mathbf{M}_0 \rangle_{\mathbf{F}_p} \in O(n_{\Phi}^{2+\epsilon})$$

$$\langle \mathbf{M}_0 \rangle_{\mathbf{Q}} \in O(1)$$

Phase \mathbf{M}_1

$$\langle \mathbf{M}_1(r) \rangle_{\mathbf{F}_p} \in O(rn_r^{3+\epsilon})$$

$$\langle \mathbf{M}_1(r) \rangle_{\mathbf{Q}} \in O(rn_r^{1+\epsilon} \ \Phi)$$

Phase \mathbf{M}_2

$$\langle \mathbf{M}_2(r) \rangle_{\mathbf{F}_p} \in O(n_{\Phi}^{3+\epsilon})$$

$$\langle \mathbf{M}_2(r) \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \ \Phi)$$

Sequence $\widetilde{\mathbf{M}}_m$

$$\langle \widetilde{\mathbf{M}}_m \rangle_{\mathbf{F}_p} \in O(n_{\Phi}^{3+\epsilon})$$

$$\langle \widetilde{\mathbf{M}}_m \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \ \Phi)$$

Sequence $\widehat{\mathbf{M}}_r$

$$\langle \widehat{\mathbf{M}}_r \rangle_{\mathbf{F}_p} \in O(n_{\Phi}^{3+\epsilon})$$

$$\langle \widehat{\mathbf{M}}_r \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \ \Phi)$$

$\widetilde{\mathbf{M}}_m + 2\delta_{\Phi}\widehat{\mathbf{M}}_r$

$$\langle \mathbf{M} \rangle_{\mathbf{F}_p} \in O(n_{\Phi}^{3+\epsilon} \delta_{\Phi})$$

$$\langle \mathbf{M} \rangle_{\mathbf{Q}} \in O(n_{\Phi}^{2+\epsilon} \delta_{\Phi}^{2+\epsilon})$$

Construction of $H_{t,\nu,\delta}$

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

- *an integer t in the range $1 \leq t \leq r$,*
- *an integer $\nu \geq \bar{\nu}_{t+1}$,*
- *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

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

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

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

For $i \in J_\delta$ construct $K_i(X)$ as follows.

- 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

$$\delta_i(\xi_{t-1}) = \tau_{t,\nu,t,i} \zeta_i.$$

- If $t = 1$ 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 set

$$K_i(X) = p^{\beta_{1,\nu}-id_1} P_i(X).$$

- If $t \geq 2$ let

$$\nu_i = (\beta_{t,\nu} - id_t) - (\alpha_{t,\nu} + ie_t) \overline{\nu}_t$$

and set

$$K_i(X) = H_{t-1,\nu_i,\delta_i}(X).$$

Having constructed $K_i(X)$ for $i \in J_\delta$, set

$$H_{t,\nu,\delta}(X) = \sum_{i \in J_\delta} K_i(X) \varphi_t(X)^{\alpha_{t,\nu} + ie_t}.$$

□

Properties of φ_r

Theorem (Montes). *Let $d_s, e_s, f_s, \varphi_s, \psi_s$, etc., be given for $1 \leq s \leq r-1$ and let*

$$\gamma_{r-1}(Y) = \frac{-e_{r-1}f_{r-1}}{r-1}(\psi_{r-1}(Y) - Y^{f_{r-1}}),$$

$$\varphi_r(X) = \varphi_{r-1}(X)^{e_{r-1}f_{r-1}} + H_{r-1, \bar{v}_r, \gamma_{r-1}}(X).$$

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 $\mathcal{S}_{r-1, \varphi_r}$.
- $V_r(\varphi_r) = \bar{v}_r$.
- $\tilde{\varphi}_r^{(r-1)}(Y) = \frac{-e_{r-1}f_{r-1}}{r-1}\psi_{r-1}(Y)$.
- φ_r is irreducible over \mathbf{Z}_p .

MAPLE: <http://www.mathstat.concordia.ca/faculty/ford/Student/Veres/mptest.mpl>

Thesis: <http://www.mathstat.concordia.ca/faculty/ford/Student/Veres/vthp.pdf>