On the Complexity of the Montes Ideal Factorization Algorithm

David Ford and Olga Veres

Concordia University, Montréal

22-Jul-2010, 7:53 am

Introduction

Suppose we have the following.

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

- 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 $\Phi(X)$ in $\mathbf{Z}[X]$ is given.

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

Level $\boldsymbol{r}$ ($\boldsymbol{r \geq 1}$). 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 $\Phi(X)$;
- 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 $\varphi_{r+1}(X) \in \mathbf{Z}_p[X]$.

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

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

Worst case. The polynomial $\Phi(X)$ 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 $n_\Phi = \deg \Phi$ and $\delta_\Phi = v_p(\operatorname{disc} \Phi)$.
- 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

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

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

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

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

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

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

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

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

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

$$m_r = (1/d_r) \ \mathbf{mod} \ e_r \,, \qquad \Theta(\mathcal{S}, r, k) = \left\lfloor m_{r-1} \frac{(\beta - k d_r) - (\alpha + k e_r)\,\overline{\nu}_r}{e_{r-1}} \right\rfloor,$$

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

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 $j = 0, \ldots, n$ and let

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

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

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

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

$$\eta_k = \begin{cases} \overline{A}_{\alpha + k e_0} & \text{if } r = 0\,, \\ \overline{B}_k(\xi_0)\,, \qquad \text{with } B_k(X) = A_{\alpha + k e_1}(X) \big/ p^{\beta - k d_1}\,, & \text{if } r = 1\,, \\ \Gamma_{\mathcal{S},r,k}^{-1} \Psi_{\mathcal{T}_{r-1,\nu_k}, A_{\alpha + k e_r}}^{(r-1)}(\xi_{r-1})\,, \quad \text{with } \nu_k = V_r(A_{\alpha + k e_r})\,, & \text{if } r \geq 2\,. \end{cases}$$

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

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

Remark. The polynomial $\widetilde{\Psi}_K^{(r)}(Y)$ 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: $\begin{cases} \text{TRUE} & \text{if } \Phi(X) \text{ is irreducible over } \mathbf{Q}_p[X], \\ \text{FALSE} & \text{if } \Phi(X) \text{ is reducible over } \mathbf{Q}_p[X]. \end{cases}$

$\mathbf{M_0}$: 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 $\varphi_0(X) = X$,

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

4. Initialize $r \leftarrow 1$.

$\mathbf{M_1}$: 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 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 $r \leftarrow r - 1$.

$\mathbf{M_2}$: 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.

Complexity of the Restricted Algorithm

Sequences

$$\widetilde{\mathrm{M}}_m \equiv \mathrm{M}_0(\Phi) \rightarrow \mathrm{M}_1(1) \rightarrow \mathrm{M}_2(1) \rightarrow \mathrm{M}_1(2) \rightarrow \mathrm{M}_2(2) \rightarrow \cdots \rightarrow \mathrm{M}_1(m) \rightarrow \mathrm{M}_2(m)$$

$$\widehat{\mathrm{M}}_r \equiv \mathrm{M}_1(r) \rightarrow \mathrm{M}_2(r-1) \rightarrow \mathrm{M}_1(r) \qquad (\text{when } e_{r-1}f_{r-1} = 1)$$

Remarks

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

Execution Costs

Newton Polygon	$\big\langle V_r(\Phi)\big\rangle_{\mathbf{F}_p} = 0$	$\big\langle V_r(\Phi)\big\rangle_{\mathbf{Q}} \in O(n_\Phi^{2+\epsilon}\Delta_\Phi)$
	$\big\langle \mathcal{N}_r(\Phi)\big\rangle_{\mathbf{F}_p} = 0$	$\big\langle \mathcal{N}_r(\Phi)\big\rangle_{\mathbf{Q}} \in O(n_\Phi^{2+\epsilon}\Delta_\Phi)$
$\boldsymbol{\varphi_r \leftarrow \varphi_{r-1}^{e_{r-1}f_{r-1}} + H_{r-1}}$	$\big\langle \varphi_{r-1}^{e_{r-1}f_{r-1}}\big\rangle_{\mathbf{F}_p} = 0$	$\big\langle \varphi_{r-1}^{e_{r-1}f_{r-1}}\big\rangle_{\mathbf{Q}} \in O\big(n_r^{1+\epsilon}\Delta_\Phi\big)$
	$\big\langle H_{r-1}\big\rangle_{\mathbf{F}_p} \in O(r n_r^{3+\epsilon})$	$\big\langle H_{r-1}\big\rangle_{\mathbf{Q}} \in O\big(r\, n_r^{1+\epsilon}\Delta_\Phi\big)$
	$\big\langle \varphi_r\big\rangle_{\mathbf{F}_p} \in O(r n_r^{3+\epsilon})$	$\big\langle \varphi_r\big\rangle_{\mathbf{Q}} \in O\big(r\, n_r^{1+\epsilon}\Delta_\Phi\big)$
Associated Polynomial	$\big\langle \widetilde{\Psi}_\Phi^{(r)}\big\rangle_{\mathbf{F}_p} \in O(n_\Phi^{2+\epsilon})$	$\big\langle \widetilde{\Psi}_\Phi^{(r)}\big\rangle_{\mathbf{Q}} \in O\big(n_\Phi^{2+\epsilon}\Delta_\Phi\big)$
Phase $\mathbf{M_0}$	$\big\langle \mathrm{M}_0\big\rangle_{\mathbf{F}_p} \in O(n_\Phi^{2+\epsilon})$	$\big\langle \mathrm{M}_0\big\rangle_{\mathbf{Q}} \in O(1)$
Phase $\mathbf{M_1}$	$\big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{F}_p} \in O(r n_r^{3+\epsilon})$	$\big\langle \mathrm{M}_1(r)\big\rangle_{\mathbf{Q}} \in O\big(r\, n_r^{1+\epsilon}\Delta_\Phi\big)$
Phase $\mathbf{M_2}$	$\big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{F}_p} \in O(n_\Phi^{3+\epsilon})$	$\big\langle \mathrm{M}_2(r)\big\rangle_{\mathbf{Q}} \in O(n_\Phi^{2+\epsilon}\Delta_\Phi)$
Sequence $\widetilde{\mathbf{M}}_{\boldsymbol{m}}$	$\big\langle \widetilde{\mathrm{M}}_m\big\rangle_{\mathbf{F}_p} \in O\big(n_\Phi^{3+\epsilon}\big)$	$\big\langle \widetilde{\mathrm{M}}_m\big\rangle_{\mathbf{Q}} \in O\big(n_\Phi^{2+\epsilon}\Delta_\Phi\big)$
Sequence $\widehat{\mathbf{M}}_{\boldsymbol{r}}$	$\big\langle \widehat{\mathrm{M}}_r\big\rangle_{\mathbf{F}_p} \in O\big(n_\Phi^{3+\epsilon}\big)$	$\big\langle \widehat{\mathrm{M}}_r\big\rangle_{\mathbf{Q}} \in O\big(n_\Phi^{2+\epsilon}\Delta_\Phi\big)$
$\boldsymbol{\widetilde{\mathrm{M}}_m + 2\,\delta_\Phi\,\widehat{\mathrm{M}}_r}$	$\big\langle \mathrm{M}\big\rangle_{\mathbf{F}_p} \in O\big(n_\Phi^{3+\epsilon}\,\delta_\Phi\big)$	$\big\langle \mathrm{M}\big\rangle_{\mathbf{Q}} \in O\big(n_\Phi^{2+\epsilon}\,\delta_\Phi^{2+\epsilon}\big)$

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

Algorithm (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

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

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

$$\delta_i(\xi_{t-1}) = \Gamma_{\mathcal{I}_{t,\nu},t,i} \, \zeta_i .$$

- 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

$$K_i(X) = p^{\beta_{1,\nu} - i d_1} \, P_i(X) \, .$$

- If $t \geq 2$ let

$$\nu_i = (\beta_{t,\nu} - i d_t) - (\alpha_{t,\nu} + i e_t) \, \overline{\nu}_t$$

  and set

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

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

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

Properties of φ_r

Theorem (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* $\mathbf{Z}_p$.

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

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