Factoring Polynomials over Local Fields II

Sebastian Pauli

Department of Mathematics and Statistics
University of North Carolina at Greensboro

Polynomial Factorization and Related Algorithms

- Round 4 maximal order algorithm [Ford, Zassenhaus (1976)]
- Montes Algorithm for ideal decomposition [Montes (1999)]
- Polynomial Factorization [Cantor, Gordon (2000)]

$$O\left(N^{4+\varepsilon}\nu(\operatorname{disc}\Phi)^{2+\varepsilon}\right)$$

- Polynomial Factorization [Ford, P., Roblot (2002)]
- Polynomial Factorization [P. (2001)]
- Montes Algorithm revisited [Guardia, Montes, Nart (2008–)]
- Complexity of Montes Algorithm [Ford, Veres (2010)]

$$O(N^{3+\varepsilon}\nu(\operatorname{disc}\Phi) + N^{2+\varepsilon}\nu(\operatorname{disc}\Phi)^{2+\varepsilon})$$

Notation

K	field complete with respect to a non-archimedian valuation
$\mathcal{O}_K$	valuation ring of K
π	uniformizing element in $\mathcal{O}_K$
ν	exponential valuation normalized such that $\nu(\pi) = 1$
$\overline{K}$	residue class field $\mathcal{O}_K/(\pi)$ of K with char $\overline{K} = p$

$\Phi(x) \in \mathcal{O}_K[x]$	separable, squarefree, monic: the polynomial to be factored
$\varphi(x) \in \mathcal{O}_K[x]$	monic: an approximation to an irreducible factor of $\Phi(x)$

Reducibility – Classical

Hensel's Lemma

A factorization of $\overline{\Phi}(x)$ into coprime factors over the residue class field $\overline{K}$ can be lifted to a factorization of $\Phi(x)$ over $\mathcal{O}_K$.

Reducibility – Classical

Hensel's Lemma

A factorization of $\overline{\Phi}(x)$ into coprime factors over the residue class field $\overline{K}$ can be lifted to a factorization of $\Phi(x)$ over $\mathcal{O}_K$.

Newton Polygons

Each distinct segment of the Newton Polygon of $\Phi(x)$ corresponds to a distinct factor of $\Phi(x)$.

Reducibility

Let $\Phi(x) := \prod_{i=1}^N (x-\alpha_i) \in \mathcal{O}_K[x]$ and $\vartheta(x) \in K[x]$, then we set

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

Reducibility

Let $\Phi(x) := \prod_{i=1}^{N}(x-\alpha_i) \in \mathcal{O}_K[x]$ and $\vartheta(x) \in K[x]$, then we set

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

Hensel Test

If $\chi_\vartheta(y) \in \mathcal{O}_K[y]$ and $\chi_\vartheta(y) \equiv \rho(y)^r \bmod (\pi)$ with $\overline{\rho}(y)$ irreducible in $\overline{K}$ we say $\vartheta(x)$ passes the *Hensel test*.

Reducibility

Let $\Phi(x) := \prod_{i=1}^{N}(x-\alpha_i) \in \mathcal{O}_K[x]$ and $\vartheta(x) \in K[x]$, then we set

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

Hensel Test

If $\chi_\vartheta(y) \in \mathcal{O}_K[y]$ and $\chi_\vartheta(y) \equiv \rho(y)^r \bmod (\pi)$ with $\overline{\rho}(y)$ irreducible in $\overline{K}$ we say $\vartheta(x)$ passes the *Hensel test*.

If $\vartheta(x)$ fails the Hensel Test we can derive a proper factorization of $\Phi(x)$.

Reducibility

Let $\Phi(x) := \prod_{i=1}^{N}(x-\alpha_i) \in \mathcal{O}_K[x]$ and $\vartheta(x) \in K[x]$, then we set

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

Hensel Test

If $\chi_\vartheta(y) \in \mathcal{O}_K[y]$ and $\chi_\vartheta(y) \equiv \rho(y)^r \bmod (\pi)$ with $\overline{\rho}(y)$ irreducible in $\overline{K}$ we say $\vartheta(x)$ passes the *Hensel test*.

If $\vartheta(x)$ fails the Hensel Test we can derive a proper factorization of $\Phi(x)$.

Newton Test

We set $v^*_\Phi(\varphi) := \min_{\Phi(\alpha)=0} \nu(\varphi(\alpha))$ and say the polynomial $\varphi(x)$ passes the *Newton test* if $\nu(\varphi(\alpha)) = v^*_\Phi(\varphi)$ for all roots α of $\Phi(x)$.

Reducibility

Let $\Phi(x) := \prod_{i=1}^{N}(x-\alpha_i) \in \mathcal{O}_K[x]$ and $\vartheta(x) \in K[x]$, then we set

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

Hensel Test

If $\chi_\vartheta(y) \in \mathcal{O}_K[y]$ and $\chi_\vartheta(y) \equiv \rho(y)^r \bmod (\pi)$ with $\overline{\rho}(y)$ irreducible in $\overline{K}$ we say $\vartheta(x)$ passes the *Hensel test*.

If $\vartheta(x)$ fails the Hensel Test we can derive a proper factorization of $\Phi(x)$.

Newton Test

We set $v^*_\Phi(\varphi) := \min_{\Phi(\alpha)=0} \nu(\varphi(\alpha))$ and say the polynomial $\varphi(x)$ passes the *Newton test* if $\nu(\varphi(\alpha)) = v^*_\Phi(\varphi)$ for all roots α of $\Phi(x)$.

If $\varphi(x)$ fails the Newton Test we can derive a proper factorization of $\Phi(x)$.

Irreducibility – Certificates

Let $\Phi(x) \in \mathcal{O}_K[x]$ and $\varphi(x) \in K[x]$ with $\chi_\varphi(y) \in \mathcal{O}_K[y]$.

- If $\varphi(x)$ passes the Hensel test, that is, $\overline{\chi}_\varphi(y) = \overline{\rho}(y)^r$ for some irreducible $\overline{\rho}(y) \in \overline{K}[y]$, we set $F_\varphi := \deg \overline{\rho}$.
- If $\varphi(x)$ passes the Newton test, let E_φ be the denominator of $v_\Phi^*(\varphi)$ in lowest terms.

Irreducibility – Certificates

Let $\Phi(x) \in \mathcal{O}_K[x]$ and $\varphi(x) \in K[x]$ with $\chi_\varphi(y) \in \mathcal{O}_K[y]$.

- If $\varphi(x)$ passes the Hensel test, that is, $\overline{\chi}_\varphi(y) = \overline{\rho}(y)^r$ for some irreducible $\overline{\rho}(y) \in \overline{K}[y]$, we set $F_\varphi := \deg \overline{\rho}$.
- If $\varphi(x)$ passes the Newton test, let E_φ be the denominator of $v_\Phi^*(\varphi)$ in lowest terms.

Two Element Certificates

A two-element certificate for $\Phi(x)$ is a pair $(\Gamma(x), \Pi(x)) \in K[x]^2$ such that $\chi_\Gamma(t) \in \mathcal{O}_K[t]$, $\chi_\Pi(t) \in \mathcal{O}_K[t]$, and $F_\Gamma E_\Pi = \deg \Phi$.

Irreducibility – Certificates

Let $\Phi(x) \in \mathcal{O}_K[x]$ and $\varphi(x) \in K[x]$ with $\chi_\varphi(y) \in \mathcal{O}_K[y]$.

- If $\varphi(x)$ passes the Hensel test, that is, $\overline{\chi}_\varphi(y) = \overline{\rho}(y)^r$ for some irreducible $\overline{\rho}(y) \in \overline{K}[y]$, we set $F_\varphi := \deg \overline{\rho}$.
- If $\varphi(x)$ passes the Newton test, let E_φ be the denominator of $v^*_\Phi(\varphi)$ in lowest terms.

Two Element Certificates

A two-element certificate for $\Phi(x)$ is a pair $(\Gamma(x), \Pi(x)) \in K[x]^2$ such that $\chi_\Gamma(t) \in \mathcal{O}_K[t]$, $\chi_\Pi(t) \in \mathcal{O}_K[t]$, and $F_\Gamma E_\Pi = \deg \Phi$.

If a two-element certificate exists for $\Phi(x)$ then $\Phi(x)$ is irreducible.

Termination

We construct a sequence $\varphi_1(x), \varphi_2(x), \ldots$ of approximations to a factor of $\Phi(x)$ such that $\nu(\varphi_1(\alpha)) < \nu(\varphi_2(\alpha)) < \ldots$ for all roots α of $\Phi(x)$ until we find one of the situations described above.

Termination

We construct a sequence $\varphi_1(x), \varphi_2(x), \ldots$ of approximations to a factor of $\Phi(x)$ such that $\nu(\varphi_1(\alpha)) < \nu(\varphi_2(\alpha)) < \ldots$ for all roots α of $\Phi(x)$ until we find one of the situations described above.

Theorem (P. 2001)

If $\Phi(x) \in \mathcal{O}_K[x]$ separable, squarefree, monic,

- $\varphi(x) \in \mathcal{O}_K[x]$ monic,
- $\nu(\varphi(\alpha)) > 2 \cdot \nu(\operatorname{disc} \Phi) / \deg \Phi$ for all roots α of $\Phi(x)$, and
- the degree of any irreducible factor of $\Phi(x)$ is greater than or equal to $\deg \varphi$,

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

Sketch of an Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: a proper factorization of $\Phi(x)$ or
a two-element certificate for the irreducibility of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E \leftarrow 1$, $F \leftarrow 1$.
- Repeat:
  1. If $\varphi_t(x)$ fails the Newton test: return a factorization of $\Phi(x)$.
  2. If we find more ramification: increase E.
  3. ...
  4. If we find more inertia: increase F.
  5. ...
  6. If $E \cdot F = \deg \Phi$: return a two-element certificate.
  7. Find $\varphi_{t+1}(x) \in \mathcal{O}_K[x]$ with $v^*_\Phi(\varphi_{t+1}) > v^*_\Phi(\varphi_t)$, $\deg \varphi_{t+1} = EF$.
  8. $t \leftarrow t + 1$

Main Steps

Newton Test

Round 4: Newton Polygon of the Characteristic Polynomial $\chi_\varphi(y)$ of $\varphi(x)$

Montes: φ-adic Expansion of $\Phi(x)$

Hensel Test

Round 4: Characteristic Polynomial $\chi_{\varphi^e\psi^{-1}}(y)$ of $\varphi^e(x)\psi^{-1}(x)$ where $v_\Phi^*(\psi) = v_\Phi^*(\varphi^e)$

Montes: Residual Polynomial

Construction of Next φ

The 1st Iteration – Newton Polygon

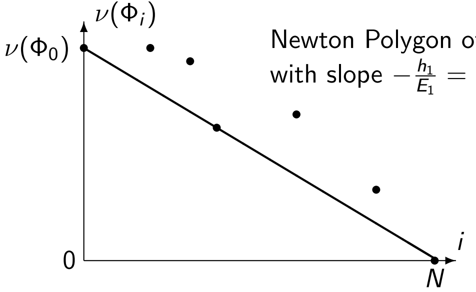
$\varphi_1(x) = x$

If the Newton polygon of $\Phi(x)$ consists of more than one segment, then we can derive a factorization of $\Phi(x)$.

Otherwise let $-\frac{h_1}{E_1}$ be the slope of the Newton polygon in lowest terms. Then $\nu(\alpha) = v^*_\Phi(x) = \frac{h_1}{E_1}$ for all roots α of $\Phi(x)$.

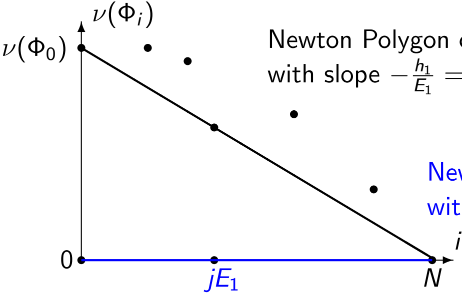
E_1 is a divisor of the ramification indices of all $K(\alpha)$ where α is a root of $\Phi(x)$.

The 1st Iteration – Residual Polynomial



Newton Polygon of $\Phi(x) = x^N + \sum_{i=0}^{N-1} \Phi_i x^i$
with slope $-\frac{h_1}{E_1} = -v_\Phi^*(x) = -\frac{\nu(\Phi_0)}{N}$ where $\gcd(h_1, E_1) = 1$

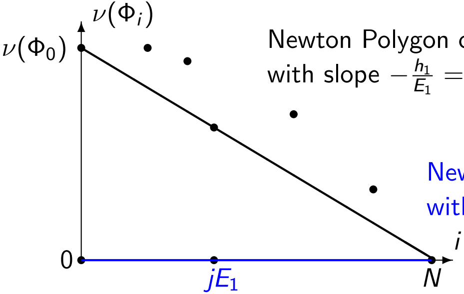
The 1st Iteration – Residual Polynomial



Newton Polygon of $\Phi(x) = x^N + \sum_{i=0}^{N-1} \Phi_i x^i$
with slope $-\frac{h_1}{E_1} = -v_\Phi^*(x) = -\frac{\nu(\Phi_0)}{N}$ where $\gcd(h_1, E_1) = 1$

Newton Polygon of $\Phi^\flat(y) := \Phi(\beta y)/\beta^N$
with β such that $\beta^{E_1} = \pi^{h_1}$

The 1st Iteration – Residual Polynomial



Newton Polygon of $\Phi(x) = x^N + \sum_{i=0}^{N-1} \Phi_i x^i$
with slope $-\frac{h_1}{E_1} = -v_\Phi^*(x) = -\frac{\nu(\Phi_0)}{N}$ where $\gcd(h_1, E_1) = 1$

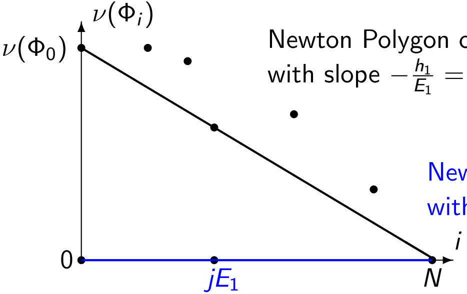
Newton Polygon of $\Phi^\flat(y) := \Phi(\beta y)/\beta^N$
with β such that $\beta^{E_1} = \pi^{h_1}$

So $\Phi^\flat(y) = \Phi(\beta y)/\beta^N = \sum_{i=0}^{N} \Phi_i \beta^{i-N} y^i$. We set

$$A_1(z) := \sum_{j=0}^{N/E_1} \Phi_{jE_1} \pi^{h_1(j-N/E_1)} z^j.$$

$\overline{A}_1(z)$ is called the *residual polynomial* of $\Phi(x)$ with respect to $\varphi_1(x) = x$.

The 1st Iteration – Residual Polynomial



Newton Polygon of $\Phi(x) = x^N + \sum_{i=0}^{N-1} \Phi_i x^i$
with slope $-\frac{h_1}{E_1} = -v_\Phi^*(x) = -\frac{\nu(\Phi_0)}{N}$ where $\gcd(h_1, E_1) = 1$

Newton Polygon of $\Phi^\flat(y) := \Phi(\beta y)/\beta^N$
with β such that $\beta^{E_1} = \pi^{h_1}$

So $\Phi^\flat(y) = \Phi(\beta y)/\beta^N = \sum_{i=0}^{N} \Phi_i \beta^{i-N} y^i$. We set

$$A_1(z) := \sum_{j=0}^{N/E_1} \Phi_{jE_1} \pi^{h_1(j-N/E_1)} z^j.$$

$\overline{A}_1(z)$ is called the *residual polynomial* of $\Phi(x)$ with respect to $\varphi_1(x) = x$.

We have $v_\Phi^*\big(A_1(x^{E_1}/\pi^{h_1})\big) > 0$.

If $A_1(y)$ splits into coprime factors modulo π then x^{E_1}/π^{h_1} fails the Hensel test.

The 1st Iteration – Next φ

Let $\overline{A}_1(z)$ be the residual polynomial, so $v_\Phi^*\big(A_1(\varphi_1^{E_1}/\pi^{h_1})\big) > 0$.

Assume $\overline{A}_1(z) = \overline{\rho}_1(z)^{r_1}$ for some irreducible $\overline{\rho}_1(z) \in \overline{K}[z]$.

$F_1 := \deg \overline{\rho}_1$ is a divisor of the inertia degrees of all extensions $K(\alpha)$.

The 1st Iteration – Next φ

Let $\overline{A}_1(z)$ be the residual polynomial, so $v_\Phi^*\big(A_1(\varphi_1^{E_1}/\pi^{h_1})\big) > 0$.

Assume $\overline{A}_1(z) = \overline{\rho}_1(z)^{r_1}$ for some irreducible $\overline{\rho}_1(z) \in \overline{K}[z]$.

$F_1 := \deg \overline{\rho}_1$ is a divisor of the inertia degrees of all extensions $K(\alpha)$.

If $E_1 F_1 = N = \deg \Phi$ then $K(\alpha)$ is an extension of degree N, which implies that $\Phi(x)$ is irreducible.

The 1st Iteration – Next φ

Let $\overline{A}_1(z)$ be the residual polynomial, so $v_\Phi^*\big(A_1(\varphi_1^{E_1}/\pi^{h_1})\big) > 0$.

Assume $\overline{A}_1(z) = \overline{\rho}_1(z)^{r_1}$ for some irreducible $\overline{\rho}_1(z) \in \overline{K}[z]$.

$F_1 := \deg \overline{\rho}_1$ is a divisor of the inertia degrees of all extensions $K(\alpha)$.

If $E_1 F_1 = N = \deg \Phi$ then $K(\alpha)$ is an extension of degree N, which implies that $\Phi(x)$ is irreducible.

As $v_\Phi^*\left(\rho_1(\varphi_1^{E_1}/\pi^{h_1})\right) > 0$ for a lift $\rho_1(z)$ of $\overline{\rho}_1(z)$ to $\mathcal{O}_K[x]$ we get

$$v_\Phi^*\big(\pi^{F_1 h_1}\rho_1(\varphi_1^{E_1}/\pi^{h_1})\big) > F_1 h_1 \geq h_1/E_1 = v_\Phi^*(\varphi_1).$$

Also $\deg\big(\rho_1(\varphi_1^{E_1}/\pi^{h_1})\big) = E_1 F_1$.

We set $\varphi_2(x) := \pi^{F_1 h_1}\rho_1\big(\varphi_1(x)^{E_1}/\pi^{h_1}\big)$.

The 1st Iteration – Next φ

Let $\overline{A}_1(z)$ be the residual polynomial, so $v_\Phi^*\big(A_1(\varphi_1^{E_1}/\pi^{h_1})\big) > 0$.

Assume $\overline{A}_1(z) = \overline{\rho}_1(z)^{r_1}$ for some irreducible $\overline{\rho}_1(z) \in \overline{K}[z]$.

$F_1 := \deg \overline{\rho}_1$ is a divisor of the inertia degrees of all extensions $K(\alpha)$.

If $E_1 F_1 = N = \deg \Phi$ then $K(\alpha)$ is an extension of degree N, which implies that $\Phi(x)$ is irreducible.

As $v_\Phi^*\left(\rho_1(\varphi_1^{E_1}/\pi^{h_1})\right) > 0$ for a lift $\rho_1(z)$ of $\overline{\rho}_1(z)$ to $\mathcal{O}_K[x]$ we get

$$v_\Phi^*\big(\pi^{F_1 h_1}\rho_1(\varphi_1^{E_1}/\pi^{h_1})\big) > F_1 h_1 \geq h_1/E_1 = v_\Phi^*(\varphi_1).$$

Also $\deg\big(\rho_1(\varphi_1^{E_1}/\pi^{h_1})\big) = E_1 F_1$.

We set $\varphi_2(x) := \pi^{F_1 h_1}\rho_1\big(\varphi_1(x)^{E_1}/\pi^{h_1}\big)$.

Remark

$\varphi_2(x)$ is irreducible.

The 1st Iteration – Data

$\varphi_1(x) = x \in \mathcal{O}_K[x]$	an approximation to an irreducible factor of $\Phi(x)$
$h_1/E_1 = v^*_\Phi(\varphi_1)$	with $\gcd(h_1, E_1) = 1$
E_1	the maximum known ramification index
$\overline{A}_1(z)$	the residual polynomial with respect to $\varphi_1(x) = x$ such that $v^*_\Phi(A_1\big(x^{E_1}/\pi^{h_1}\big) > 0$ is
$\rho_1(z) \in \mathcal{O}_K[z]$	irreducible modulo π, such that $\overline{A}_1(z) \equiv \overline{\rho}_1(z)^{r_1}$
γ_1	a root of ρ_1, so $v^*_\Phi\left((x^{E_1}/\pi^{h_1}) - \gamma_1\right) > 0$
$K_1 = K(\gamma_1)$	the maximum known unramified subfield
$F_1 = [K_1 : K]$	the maximum known inertia degree

The 2nd Iteration – Newton Polygon

Find $\nu\big(\varphi_2(\alpha)\big)$ for all roots α of $\Phi(x)$.

φ_2-expansion

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_2 = n_2$ such that

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

We have $0 = \Phi(\alpha) = \sum_{i=0}^{N/n} a_i(\alpha)\varphi_2^i(\alpha)$ for all roots α of $\Phi(x)$.

$\chi(y) = \sum_{i=0}^{N/n} a_i(\alpha)y^i = \sum_{i=0}^{N/n} \sum_{j=0}^{E_1F_1-1} a_{ij}\alpha^j y^i$ is a polynomial with root $\varphi_2(\alpha)$.

The 2nd Iteration – Newton Polygon

Find $\nu\big(\varphi_2(\alpha)\big)$ for all roots α of $\Phi(x)$.

φ_2-expansion

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_2 = n_2$ such that

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

We have $0 = \Phi(\alpha) = \sum_{i=0}^{N/n} a_i(\alpha)\varphi_2^i(\alpha)$ for all roots α of $\Phi(x)$.

$\chi(y) = \sum_{i=0}^{N/n} a_i(\alpha)y^i = \sum_{i=0}^{N/n} \sum_{j=0}^{E_1F_1-1} a_{ij}\alpha^j y^i$ is a polynomial with root $\varphi_2(\alpha)$.

As the valuations

$$\nu(\alpha) = h_1/E_1, \ \ldots\ , \ \nu(\alpha^{E_1-1}) = (E_1-1)h_1/E_1$$

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

$$1, \alpha^{E_1}/\pi^{h_1} \equiv \gamma_1 \bmod (\pi), \ \ldots\ , \left(\alpha^{E_1}/\pi^{h_1}\right)^{F_1-1} \equiv \gamma_1^{F_1-1} \bmod (\pi)$$

are linearly independent over $\mathcal{O}_K$, we have $v_\Phi^*(a_i) = \min_{0\le j\le n-1} \nu(a_{ij})(h_1/E_1)^j$.

The 2nd Iteration – Newton Polygon

Find $\nu(\varphi_2(\alpha))$ for all roots α of $\Phi(x)$.

φ_2-expansion

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_2 = n_2$ such that

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

We have $0 = \Phi(\alpha) = \sum_{i=0}^{N/n} a_i(\alpha)\varphi_2^i(\alpha)$ for all roots α of $\Phi(x)$.

$\chi(y) = \sum_{i=0}^{N/n} a_i(\alpha)y^i = \sum_{i=0}^{N/n}\sum_{j=0}^{E_1F_1-1} a_{ij}\alpha^j y^i$ is a polynomial with root $\varphi_2(\alpha)$.

Lemma

The Newton Polygon of $\chi(y)$ yields the valuations of $\varphi_2(\alpha)$ for all roots α of $\Phi(x)$

If the Newton Polygon of $\chi(y)$ is not a line then $\varphi_2(x)$ fails the Newton test and we can derive a proper factorization of $\Phi(x)$.

The 2nd Iteration – Residual Polynomial

Assume that $\varphi_2(x)$ passes the Newton Test and let $h_2/e_2 = v^*_\Phi(\varphi_2)$.
Set $E_2^+ = \frac{e_2}{\gcd(e_2,E_1)}$ and $E_2 = E_1 E_2^+$.

Find $s_\pi \in \mathbb{Z}$, $s_1 \in \mathbb{N}$ such that $\psi_2(x) = \pi^{s_\pi} x^{s_1}$ with $\nu(\psi_2(\alpha)) = \frac{E_2^+ h_2}{e_2}$.

The 2nd Iteration – Residual Polynomial

Assume that $\varphi_2(x)$ passes the Newton Test and let $h_2/e_2 = v^*_\Phi(\varphi_2)$.
Set $E_2^+ = \frac{e_2}{\gcd(e_2,E_1)}$ and $E_2 = E_1 E_2^+$.

Find $s_\pi \in \mathbb{Z}$, $s_1 \in \mathbb{N}$ such that $\psi_2(x) = \pi^{s_\pi} x^{s_1}$ with $\nu(\psi_2(\alpha)) = \frac{E_2^+ h_2}{e_2}$.

Set

$$A_2(z) := \sum_{j=0}^{m/E_2^+} a_{jE_2^+}(x)\psi_2^{j-m/E_2^+}(x)z^j$$

Now $v^*_\Phi\Big(A_2\big(\varphi_2^{E_2^+}/\psi_2\big)\Big) > 0$.

The 2nd Iteration – Residual Polynomial

Assume that $\varphi_2(x)$ passes the Newton Test and let $h_2/e_2 = v_\Phi^*(\varphi_2)$. Set $E_2^+ = \frac{e_2}{\gcd(e_2,E_1)}$ and $E_2 = E_1 E_2^+$.

Find $s_\pi \in \mathbb{Z}$, $s_1 \in \mathbb{N}$ such that $\psi_2(x) = \pi^{s_\pi} x^{s_1}$ with $\nu(\psi_2(\alpha)) = \frac{E_2^+ h_2}{e_2}$.

Set

$$A_2(z) := \sum_{j=0}^{m/E_2^+} a_{jE_2^+}(x)\psi_2^{j-m/E_2^+}(x)z^j$$

Now $v_\Phi^*\Big(A_2\big(\varphi_2^{E_2^+}/\psi_2\big)\Big) > 0$.

We use $a_{jE_2^+}(x) = \sum_{j=0}^{E_1 F_1 - 1} a_{ij}x^j$ and $\psi_2(x) = \pi^{s_\pi} x^{s_1}$ and the relation $v_\Phi^*\left(x^{E_1}/\pi^{h_1} - \gamma_1\right) > 0$, where $\gamma_1 \in K_1$ to find $\overline{A}_2(z) \in \overline{K}_1[z]$.

The 2nd Iteration – Residual Polynomial

Assume that $\varphi_2(x)$ passes the Newton Test and let $h_2/e_2 = v^*_\Phi(\varphi_2)$.
Set $E_2^+ = \frac{e_2}{\gcd(e_2,E_1)}$ and $E_2 = E_1 E_2^+$.

Find $s_\pi \in \mathbb{Z}$, $s_1 \in \mathbb{N}$ such that $\psi_2(x) = \pi^{s_\pi} x^{s_1}$ with $\nu(\psi_2(\alpha)) = \frac{E_2^+ h_2}{e_2}$.

Set

$$A_2(z) := \sum_{j=0}^{m/E_2^+} a_{jE_2^+}(x)\psi_2^{j-m/E_2^+}(x)z^j$$

Now $v^*_\Phi\Big(A_2\big(\varphi_2^{E_2^+}/\psi_2\big)\Big) > 0$.

We use $a_{jE_2^+}(x) = \sum_{j=0}^{E_1F_1-1} a_{ij}x^j$ and $\psi_2(x) = \pi^{s_\pi}x^{s_1}$ and the relation $v^*_\Phi\left(x^{E_1}/\pi^{h_1} - \gamma_1\right) > 0$, where $\gamma_1 \in K_1$ to find $\overline{A}_2(z) \in \overline{K}_1[z]$.

Definition

$\overline{A}_2(z)$ is the residual polynomial of $\Phi(x)$ with respect to $\varphi_2(x)$.

The 2nd Iteration – Residual Polynomial

Let $\overline{A}_2(z)$ be the residual polynomial of $\Phi(x)$ with respect to $\varphi_2(x)$.

If $\overline{A}_2(z)$ splits into coprime factors then $\varphi_2(x)\psi_2(x)^{-1}$ fails the Hensel test and we can derive a proper factorization of $\Phi(x)$.

Otherwise there is $\overline{\rho}_2(z) \in \overline{K_1}[z]$ irreducible such that $\overline{\rho}_2(z)^{r_2} = \overline{A}_2(z)$.
We set $F_2^+ = \deg \overline{\rho}_2$, $F_2 = F_1 F_2^+$.

The 2nd Iteration – Residual Polynomial

Let $\overline{A}_2(z)$ be the residual polynomial of $\Phi(x)$ with respect to $\varphi_2(x)$.

If $\overline{A}_2(z)$ splits into coprime factors then $\varphi_2(x)\psi_2(x)^{-1}$ fails the Hensel test and we can derive a proper factorization of $\Phi(x)$.

Otherwise there is $\overline{\rho}_2(z) \in \overline{K}_1[z]$ irreducible such that $\overline{\rho}_2(z)^{r_2} = \overline{A}_2(z)$. We set $F_2^+ = \deg \overline{\rho}_2$, $F_2 = F_1 F_2^+$.

If $E_2 F_2 = N = \deg \Phi$ then $\Phi(x)$ is irreducible.

The 2nd Iteration – Next $\varphi(x)$

From

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

we construct $\varphi_3(x) \in \mathcal{O}_K[x]$ such that

- $v_\Phi^*(\varphi_3^* - \varphi_3) > v_\Phi^*(\varphi_3^*)$ and
- $\deg \varphi_3 = E_2 F_2 = E_2^+ F_2^+ E_1 F_1$.

using that

- r_{ij} is congruent to a linear combination of x^{E_1}/π^{h_1},
- $v_\Phi^*(\rho_1(x^{E_1}/\pi^{h_1})) > 0$, and
- $\deg(\rho_1(x^{E_1}/\pi^{h_1})) = E_1 F_1$

The 2nd Iteration – Next $\varphi(x)$

From

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

we construct $\varphi_3(x) \in \mathcal{O}_K[x]$ such that

- $v_\Phi^*(\varphi_3^* - \varphi_3) > v_\Phi^*(\varphi_3^*)$ and
- $\deg \varphi_3 = E_2 F_2 = E_2^+ F_2^+ E_1 F_1$.

using that

- r_{ij} is congruent to a linear combination of x^{E_1}/π^{h_1},
- $v_\Phi^*(\rho_1(x^{E_1}/\pi^{h_1})) > 0$, and
- $\deg(\rho_1(x^{E_1}/\pi^{h_1})) = E_1 F_1$

Remark

$\varphi_3(x)$ is irreducible.

The $(t-1)$-st Iteration – Data

$\varphi_{t-1}(x) \in \mathcal{O}_K[x]$	an approximation to an irreducible factor of $\Phi(x)$ with $\deg \varphi_{t-1} = E_{t-2}F_{t-2}$
$h_{t-1}/e_{t-1} = v_\Phi^*(\varphi_{t-1})$	with $\gcd(h_{t-1}, e_{t-1}) = 1$
$E_{t-1}^+ = \frac{e_{t-1}}{\gcd(E_{t-2}, e_{t-1})}$	the increase of known ramification index
$E_{t-1} = E_{t-2} \cdot E_{t-1}^+$	the maximal known ramification index
$\vdots$	$\vdots$

The t-th Iteration – Newton Polygon

Find $\nu\big(\varphi_t(\alpha)\big)$ for all roots α of $\Phi(x)$.

φ_t-expansion

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_t = n_t = E_{t-1}F_{t-1}$ such that

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

The t-th Iteration – Newton Polygon

Find $\nu\big(\varphi_t(\alpha)\big)$ for all roots α of $\Phi(x)$.

φ_t-expansion

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_t = n_t = E_{t-1}F_{t-1}$ such that

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

The $(\varphi_1, \ldots, \varphi_{t-1})$-expansion of the coefficients of the expansion yields the valuations of the coefficients a_i.

$(\varphi_1, \ldots, \varphi_{t-1})$-expansion of $a_i(x)$

$$a_i(x) = \sum_{j_{t-1}=0}^{E_{t-1}^+ F_{t-1}^+ - 1} \varphi_{t-1}^{j_{t-1}}(x) \;\cdots \sum_{j_{t-2}=0}^{E_{t-2}^+ F_{t-2}^+ - 1} \varphi_2^{j_2}(x) \sum_{j_1=0}^{E_1^+ F_1^+ - 1} x^{j_1} \cdot a_{j_1 \ldots j_{t-1}}$$

The t-th Iteration – Newton Polygon

Find $\nu\big(\varphi_t(\alpha)\big)$ for all roots α of $\Phi(x)$.

φ_t-expansion

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_t = n_t = E_{t-1}F_{t-1}$ such that

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

The $(\varphi_1, \dots, \varphi_{t-1})$-expansion of the coefficients of the expansion yields the valuations of the coefficients a_i.

$(\varphi_1, \dots, \varphi_{t-1})$-expansion of $a_i(x)$

$$a_i(x) = \sum_{j_{t-1}=0}^{E_{t-1}^{+}F_{t-1}^{+}-1} \varphi_{t-1}^{j_{t-1}}(x) \;\cdots \sum_{j_{t-2}=0}^{E_{t-2}^{+}F_{t-2}^{+}-1} \varphi_2^{j_2}(x) \sum_{j_1=0}^{E_1^{+}F_1^{+}-1} x^{j_1} \cdot a_{j_1 \dots j_{t-1}}$$

Lemma

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

Complexity

Theorem

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.

Complexity

Theorem

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.

Thank You