Local polynomial factorisation

improving the Montes algorithm

Adrien Poteaux* & Martin Weimann♦

*: CFHP - CO2 - CRIStAL - Université de Lille

♦: LMNO - Université de Caen Normandie

February 3rd 2022

Seminari de Teoria de Nombres de Barcelona 2022

Facultad de Matemáticas, Universitat de Barcelona

Université de Lille

CRIStAL Centre de Recherche en Informatique, Signal et Automatique de Lille

cnrs

My background

Singularities of plane algebraic curves

Puiseux series, Newton-Puiseux algorithm

Puiseux series

$\mathrm{Char}(\mathbb{K}) = 0$ or $\mathrm{Char}(\mathbb{K}) > d := deg(F)$

Theorem (Puiseux, 1850)

$F \in \mathbb{K}[[t]][x]$ has d distinct roots in $\overline{\mathbb{K}((t))}$:

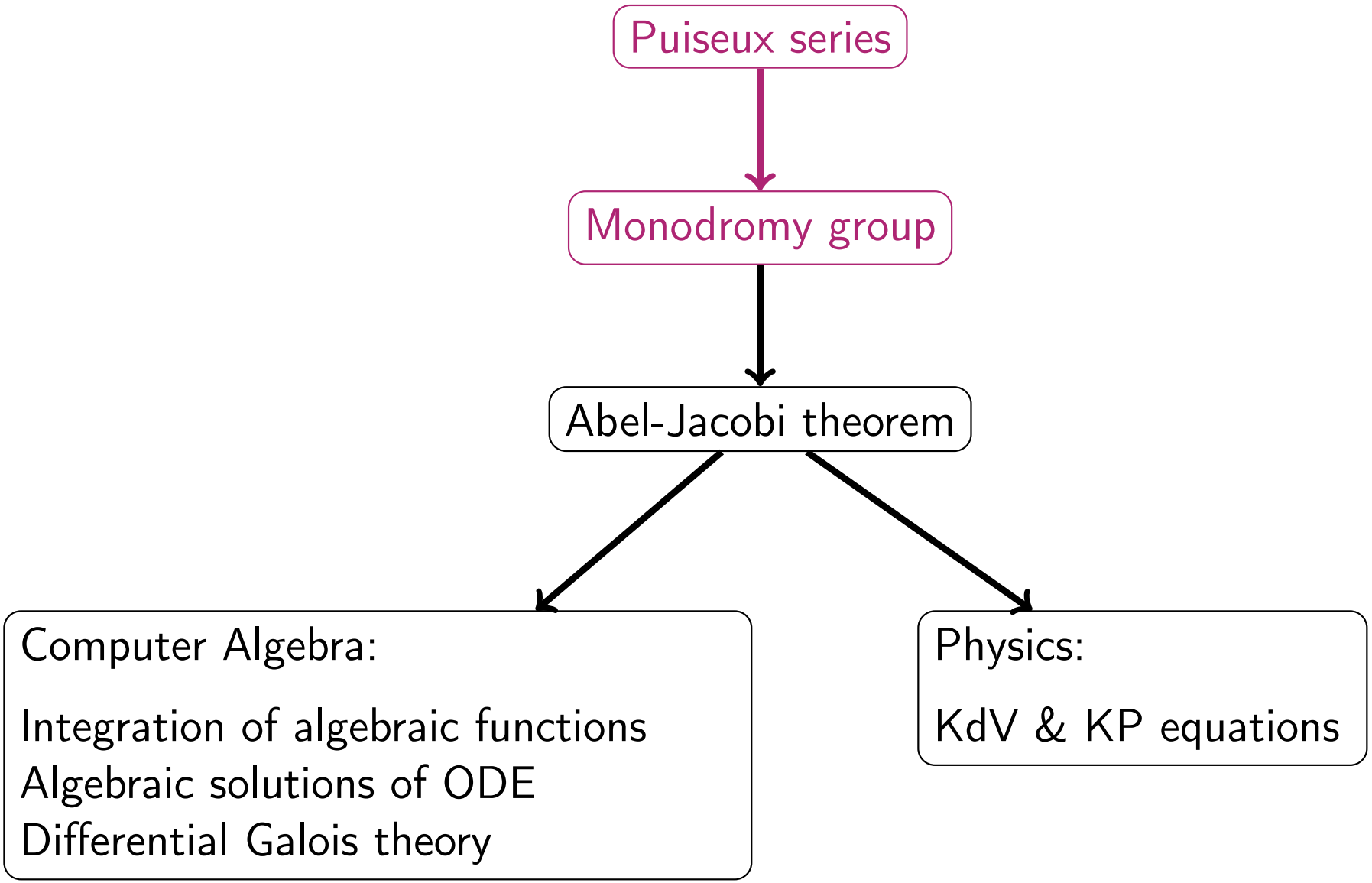
$$S_{ij}(t) = \sum_{k=n_i}^{\infty} \alpha_{i,k}\, \zeta_{e_i}^{jk}\, t^{\frac{k}{e_i}}$$

- $e_1, \cdots, e_s \in \mathbb{N}^\star$ *and* $d = \sum_{i=1}^{s} e_i$
- $0 \leq j \leq e_i - 1$, $1 \leq i \leq s$, $n_i \in \mathbb{Z}$, $\alpha_{i,n_i} \neq 0$
- ζ_{e_i} *primitive e_i-th root of unity.*

Moreover, $\{\alpha_{i,k}\}$ belongs to a finite extension of $\mathbb{K}$.

$$\overline{\mathbb{K}((x))} = \bigcup_{e \in \mathbb{N}^\star} \overline{\mathbb{K}}((x^{\frac{1}{e}}))$$

My initial motivations



Computing Puiseux series: tools and idea

$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

$\Longrightarrow$ We're looking for $S(t) = \alpha\,t^{\frac{m}{q}} + \cdots$ s.t. $F(t, S(t)) = 0$

$$\begin{aligned} F(t, \alpha\,t^{\frac{m}{q}} + \cdots) \quad &= \alpha^6\,t^{\frac{6\,m}{q}} + \alpha^5\,t^{\frac{5\,m}{q}+1} + 5\,\alpha^4\,t^{\frac{4\,m}{q}+3} \\ &\quad -2\,\alpha^4\,t^{\frac{4\,m}{q}+1} + 4\,\alpha^2\,t^{\frac{2\,m}{q}+2} + t^5 - 3\,t^4 + \cdots \end{aligned}$$

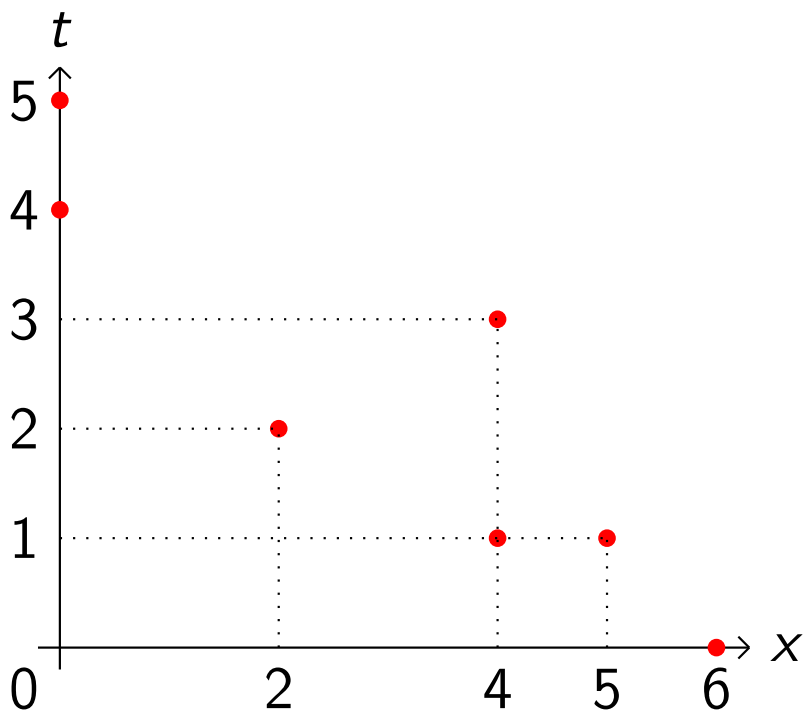
- Some of these terms must cancel !

$\Longrightarrow$ (m, q) s.t. at least two exponents are the same

Support of the polynomial

$$F(t,x) = t^0\,x^6 + t^1\,x^5 + 5\,t^3\,x^4 - 2\,t^1 x^4 + 4\,t^2\,x^2 + t^5\,x^0 - 3\,t^4\,x^0$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$



Choice of (m, q) that increases the t-order ?

$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

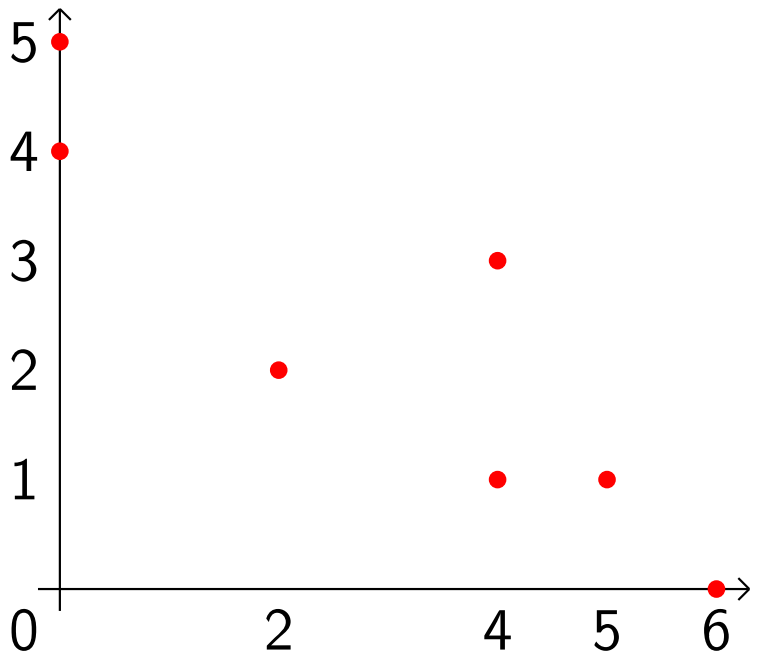
- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

  $*$ (m, q) for cancelling two terms ?

$\rightsquigarrow$ at least two points on $m\,i + q\,j = l$

  $*$ increasing the t-order ?

$\rightsquigarrow$ no other point under the line



Choice of (m, q) that increases the t-order ?

$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) for cancelling two terms ?

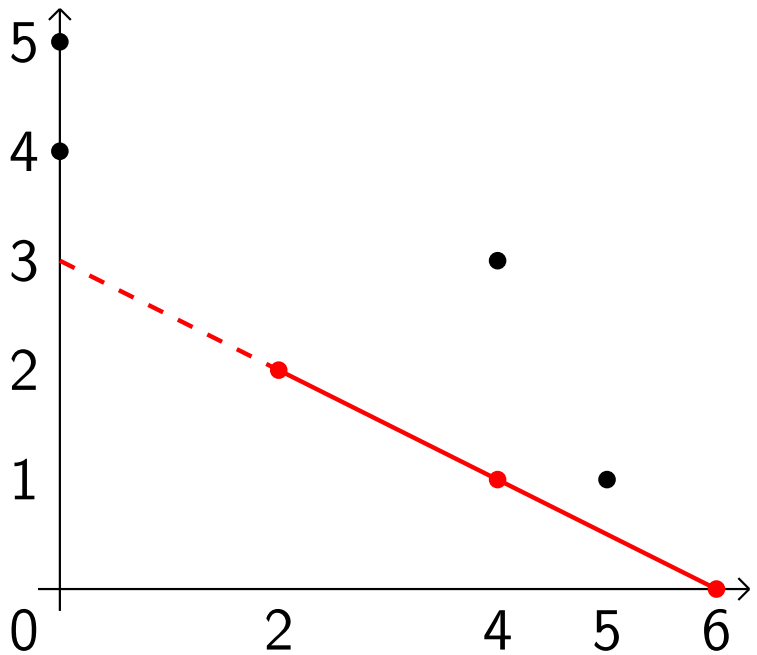
$\rightsquigarrow$ at least two points on $m\,i + q\,j = l$

$*$ increasing the t-order ?

$\rightsquigarrow$ no other point under the line

(Δ_1) $i + 2\,j = 6$ is such a line

$$\rightsquigarrow S(t) = \alpha\,t^{1/2} + \cdots$$



Choice of (m, q) that increases the t-order ?

$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) for cancelling two terms ?

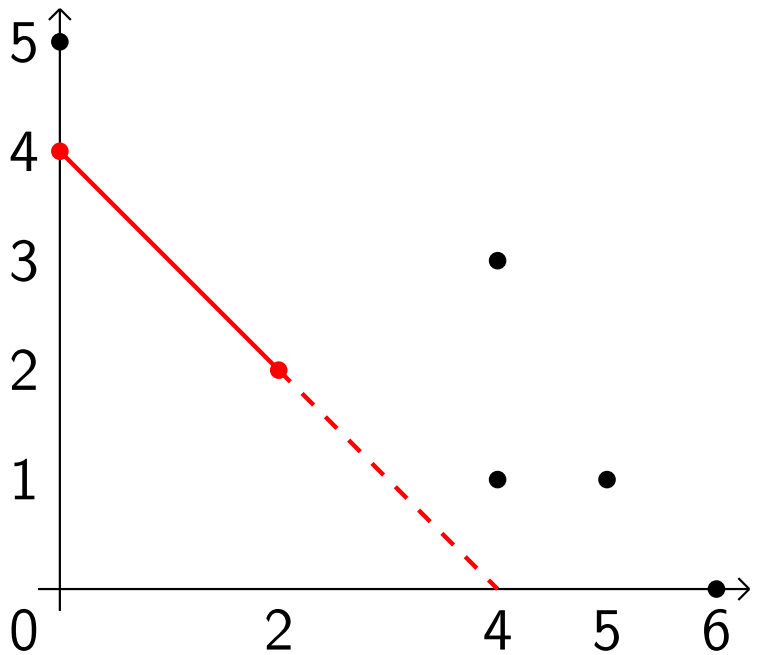
$\rightsquigarrow$ at least two points on $m\,i + q\,j = l$

$*$ increasing the t-order ?

$\rightsquigarrow$ no other point under the line

(Δ_1) $i + 2\,j = 6$ is such a line

(Δ_2) $i + j = 4$ is too

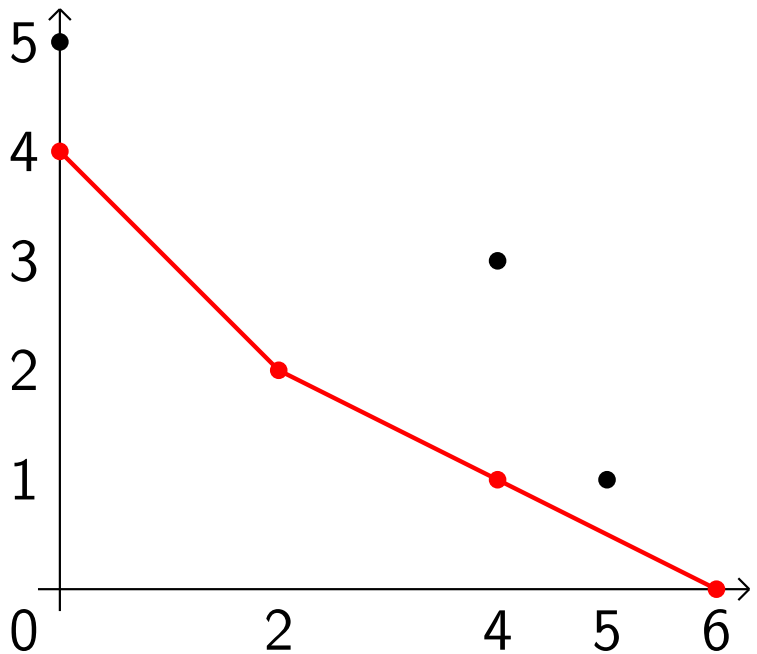


Newton polygon

$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

— $\mathcal{N}(F)$: lower part of convex hull of Supp(F).



Choice of α that increases the t-order ?

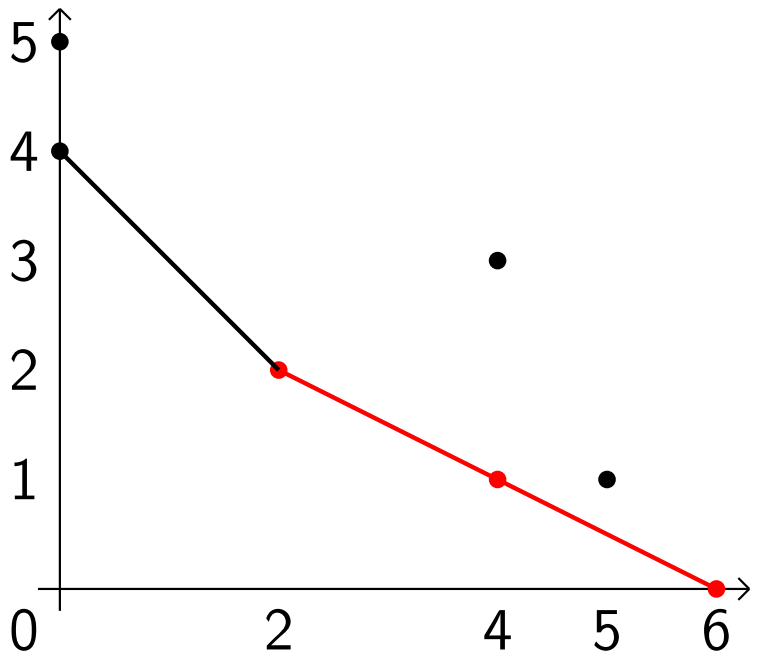
$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

— $\mathcal{N}(F)$: lower part of convex hull of Supp(F).

$$F(T^2, \alpha\,T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\,T^6$$

$$+\alpha^5\,T^7 - 3\,T^8 + (5\alpha^4 + 1)\,T^{10} + \ldots$$



Characteristic polynomial

$$F(t,x) = x^6 + t\,x^5 + 5\,t^3\,x^4 - 2\,t\,x^4 + 4\,t^2\,x^2 + t^5 - 3\,t^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

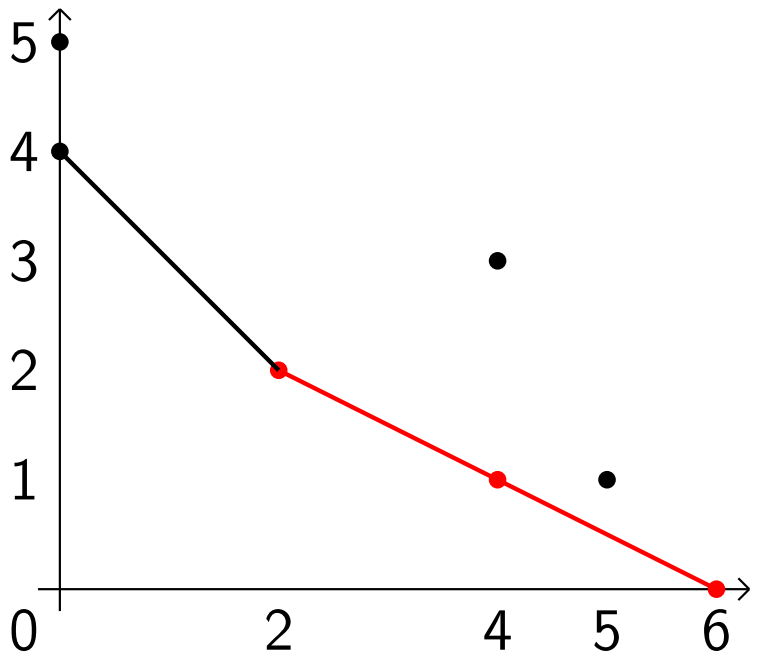
— $\mathcal{N}(F)$: lower part of convex hull of Supp(F).

$$F(T^2, \alpha\,T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\,T^6$$

$$+\alpha^5\,T^7 - 3\,T^8 + (5\alpha^4 + 1)\,T^{10} + \ldots$$

Characteristic polynomial:

$$\phi_{\Delta_1}(\beta) = \beta^2 - 2\,\beta + 4$$



Newton-Puiseux algorithm

For each edge Δ of $\mathcal{N}(F)$

1. Factor $\phi_\Delta = \prod_{k=1}^{s} \phi_k^{M_k}$

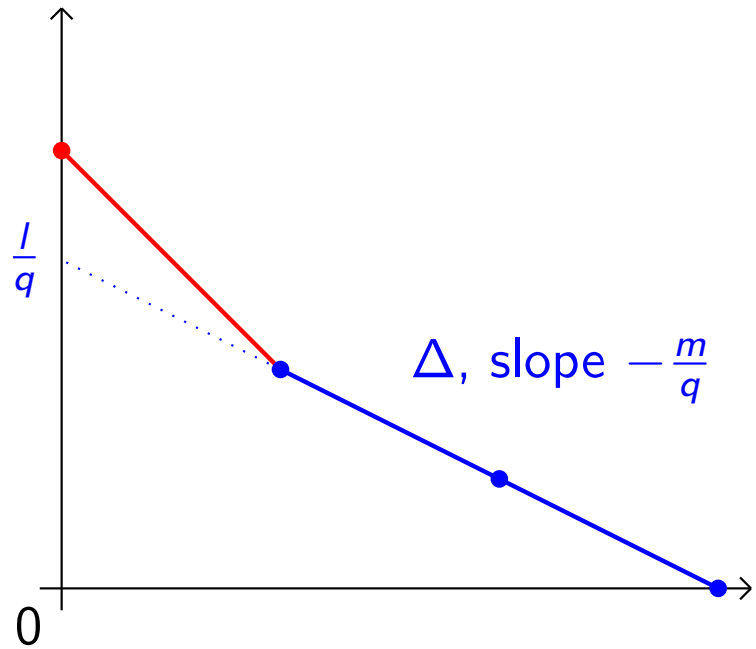
2. For each ϕ_k,

   Puiseux transformation:

   $$F_{\Delta,\xi}(t,x) = \frac{F(t^q, t^m(x+\xi^{\frac{1}{q}}))}{t^l}$$

   with ξ root of ϕ_k.

3. Recursive calls: $\{F_{\Delta,\xi}(t,x)\}_{\Delta,\xi}$



Main results

- [Po08] A modular-numeric strategy.
  1. Compute S modulo a *well chosen* prime $p \rightsquigarrow$ essential terms.
  2. Use this computation to get numerical coefficients of the series.
- Improved arithmetic complexity.
  - [Po08] $\mathcal{O}(D^8) \rightsquigarrow \mathcal{O}^{\sim}(D^5)$.
  - [PoRy15] $\mathcal{O}^{\sim}(D^4)$: *Abhyankhar's trick* (d-th approximate root).
  - [PoWe21] $\mathcal{O}^{\sim}(D^3)$: divide and conquer strategy.

Application: genus in an expected $\mathcal{O}^{\sim}(D^3)$ *binary* operations.

Moving towards generalised Newton polygons

improving the irreducibility test

One example

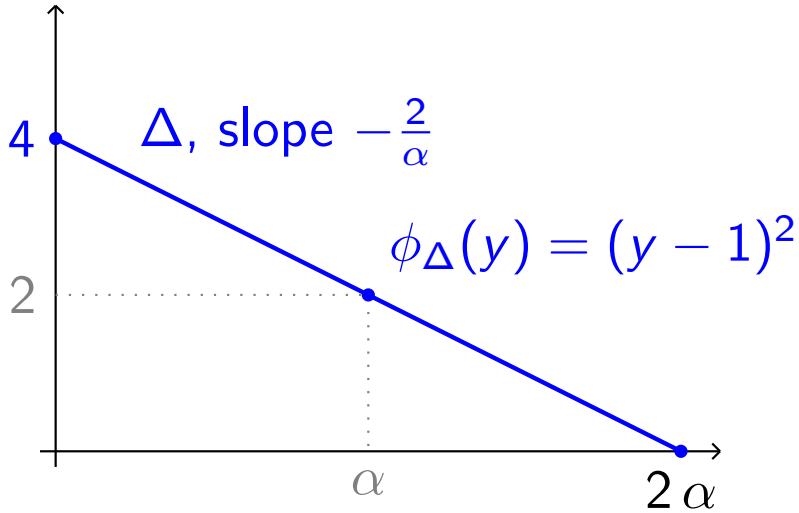
$$F = (x^\alpha - t^2)^2 + t^\alpha \in \mathbb{A}[x] \text{ with } \mathbb{A} = \mathbb{C}[[t]]$$

- $d = \deg(F) = 2\,\alpha$,
- $\delta = v_t(\mathrm{Disc}(F)) = 2\,\alpha^2 - 4\,\alpha + 4$.
- Assume $\alpha > 4$ odd.

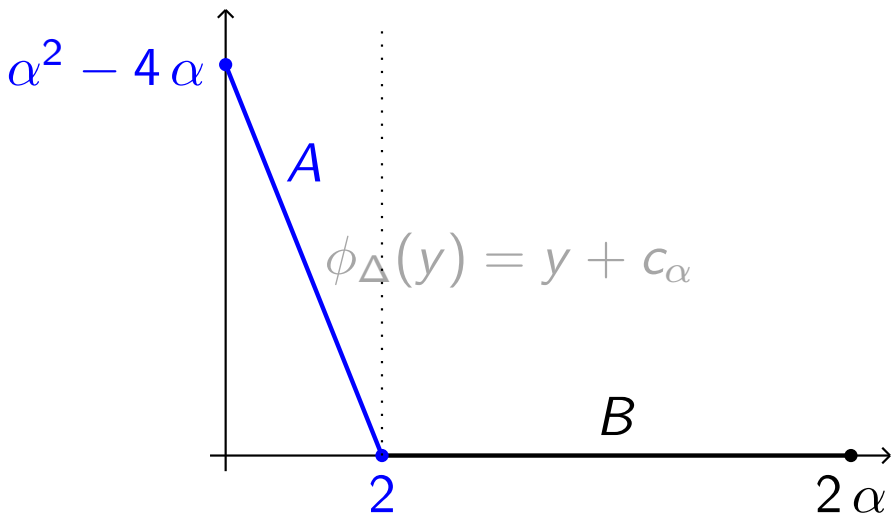
Is F irreducible in $\mathbb{C}[[t]][x]$?

Using the Newton-Puiseux algorithm. [PoWe21]

$$F = y^{2\alpha} - 2x^2 y^\alpha + x^4 + x^\alpha$$



1. $G \leftarrow F(t^\alpha, t^2(x+1))/t^{4\alpha}$,
2. Hensel: $G = A \cdot B$,
3. Recursive call with A

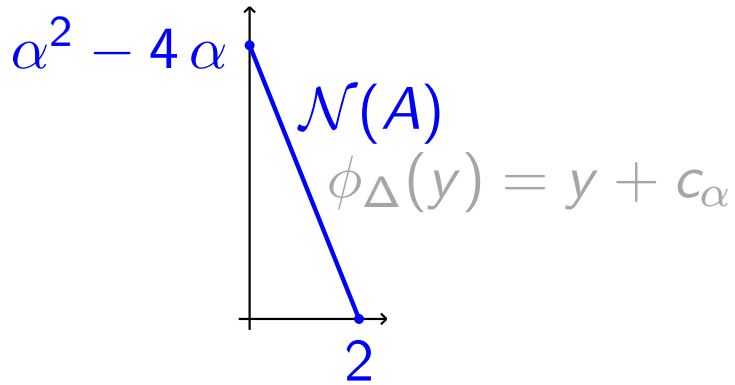


Polynomial	size
F	$\Theta(\alpha^2) = \Theta(\delta)$
G	$\Theta(\alpha^3) = \Theta(d\,\delta)$
A	$\Theta(\alpha^2) = \Theta(\delta)$

Answer: Yes complexity: $\Theta(d\,\delta)$ Answer in $\mathcal{O}(\delta)$?

Avoiding any blow-up ?

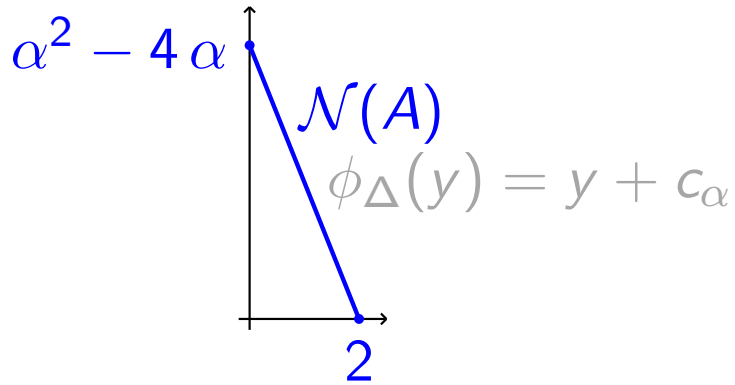
$$F = (x^\alpha - t^2)^2 + t^\alpha$$



- Writing $\psi = x^\alpha - t^2$, we have $F = \psi^2 + t^\alpha$,
  - Can we "guess" the second Newton polygon from $\psi^2 + t^\alpha$?
  - Can we "read" ϕ_Δ ?

Avoiding any blow-up ?

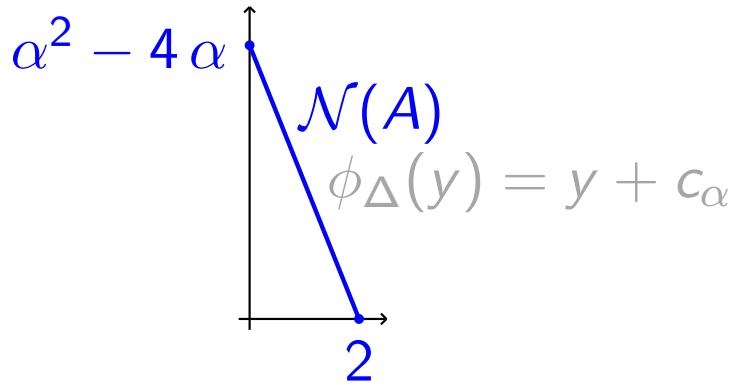
$$F = (x^\alpha - t^2)^2 + t^\alpha$$



- Writing $\psi = x^\alpha - t^2$, we have $F = \psi^2 + t^\alpha$,
  - Can we "guess" the second Newton polygon from $\psi^2 + t^\alpha$?
  - Can we "read" ϕ_Δ ?
- Key ingredients:
  - $\psi = \sqrt[2]{F}$ is an approximate root of F,
  - $F = \psi^2 + t^\alpha$ is the ψ-adic expansion of F.

Avoiding any blow-up ?

$$F = (x^\alpha - t^2)^2 + t^\alpha$$



- Writing $\psi = x^\alpha - t^2$, we have $F = \psi^2 + t^\alpha$,
  - Can we "guess" the second Newton polygon from $\psi^2 + t^\alpha$?
  - Can we "read" ϕ_Δ ?
- Key ingredients:
  - $\psi = \sqrt[2]{F}$ is an approximate root of F,
  - $F = \psi^2 + t^\alpha$ is the ψ-adic expansion of F.
- Questions:
  - Why t^α corresponds to $\alpha^2 - 4\,\alpha$?
  - How to recover the correct characteristic polynomial ?

This talk

Context:

- $\mathbb{A}$ a discrete valuation ring (e.g. $\mathbb{K}[[t]]$, $\mathbb{Z}_p$),
- $v_{\mathbb{A}}$ valuation over $\mathbb{A}$ (e.g. v_t, v_p),
- π an uniformiser (e.g. t, p),
- $\mathbb{F}$ the residue field (e.g. $\mathbb{K}$, $\mathbb{F}_p$).

Objective(s):

1. Irreducibility test in $\mathbb{A}[x]$,
2. Factorisation in $\mathbb{A}[x]$.
3. Case $\mathbb{A} = \mathbb{K}[[t]]$: Puiseux series of F ?

Notations: $F \in \mathbb{A}[x]$ (monic) ; $d = \deg(F)$; $\delta = v_{\mathbb{A}}(\mathrm{Disc}(F))$

Approximate root of $F \in \mathbb{A}[x]$ monic [Ab10]

- Hyp: $\mathrm{char}(\mathbb{A})$ does not divide d,
- Let $N \in \mathbb{N}$ dividing d,

Proposition

There is an unique monic $\psi \in \mathbb{A}[x]$ such that:

- $\deg(\psi) = d/N$,
- $\deg(F - \psi^N) < d - d/N$,

$\rightsquigarrow$ $\psi = \sqrt[N]{F}$ is the N-th approximate root of F.

$$F = \sum_{i=0}^{N} a_i \psi^i \ , \ \deg(a_i) < \deg(\psi) \Longrightarrow a_{N-1} = 0$$

Example: $\psi = \sqrt[d]{F} = x + \dfrac{a_{d-1}}{d}$ is the d-th approximate root of F.

Valuations on $\mathbb{A}[x]$

- Gauss valuation:
  - $F = \sum_i a_i\, x^i$,
  - $\upsilon_0(F) = \min_i \upsilon_{\mathbb{A}}(a_i)$.
- Extended valuation: given $\psi \in \mathbb{A}[x]$ monic, $\frac{m}{q} \in \mathbb{Q}$:
  - $\upsilon_\psi = (\upsilon_0, \psi, \frac{m}{q})$ *extends* υ_0.

    Defined by $\upsilon_\psi(\psi) = m\,q$, $\upsilon_\psi(x) = m$ and $\upsilon_\psi(\pi) = q$,
  - Expand $F = \sum_i a_i(x)\,\psi^i$ with $\deg(a_i) < \deg(\psi)$,
  - Generalised Newton polygon:

    $\mathcal{N}_\psi(F)$ is the lower convex hull of $(i, \upsilon_\psi(a_i\,\psi^i) - \upsilon_\psi(F))_i$.

Improving the irreducibility test

generalisation of the work of Abhyankhar to $\mathbb{A}[x]$.

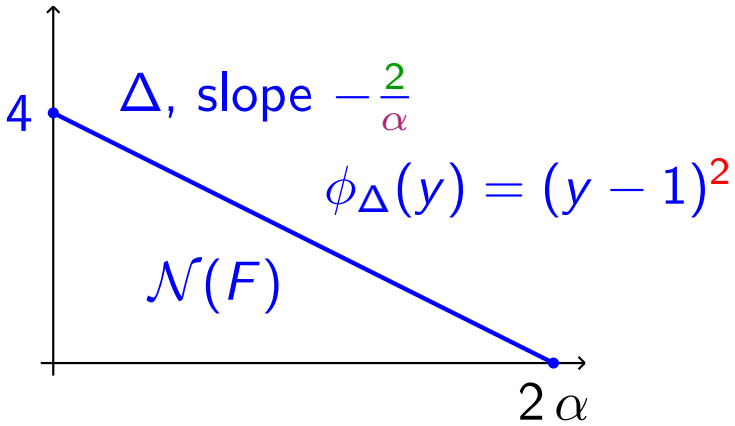
link with the Newton–Puiseux algorithm for $\mathbb{A} = \mathbb{K}[[t]]$

PoWe - Submitted, *A quasi-linear irreduccibility test in* $\mathbb{K}[[x]][y]$

PoWe - Preprint, *Local polynomial factorisation: improving the Montes algorithm*

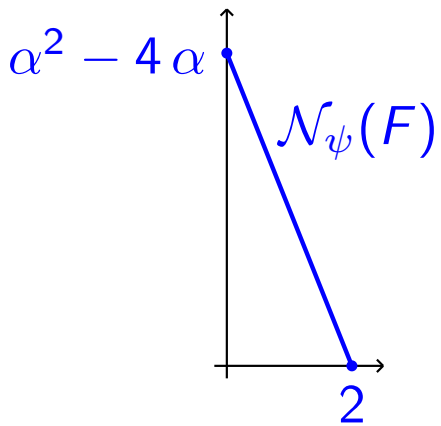
We get the second Newton polygon !

$$F = (x^\alpha - t^2)^2 + t^\alpha$$



With $m = 2$, $q = \alpha$, $\psi = \sqrt[2]{F}$, we get:

- $F = \psi^2 + t^\alpha$.
- $v_\psi(F) = 4\,\alpha$
- $v_\psi(\psi^2) - v_\psi(F) = 0$,
- $v_\psi(t^\alpha) - v_\psi(F) = \alpha^2 - 4\,\alpha$.



Reminder: $v_\psi(t) = \alpha \quad v_\psi(x) = 2 \quad v_\psi(\psi) = 2\,\alpha$

Complexity ?

- Computing $\psi = \sqrt[N]{F}$: $\mathcal{O}(\mathsf{M}(d)) = \mathcal{O}^{\sim}(d)$ op in $\mathbb{A}$.
  - $F_\infty = x^d\, F(1/x)$ the reciprocal polynomial of F,
  - $F_\infty(0) = 1 \rightsquigarrow \exists!\ \phi \in \mathbb{A}[[x]]$ s.t. $\phi(0) = 1$ and $\phi^N = F_\infty$,
  - ϕ is the root of $z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
  - ψ is the reciprocal polynomial of $\lceil \phi \rceil^{\frac{d}{N}}$

Complexity ?

- Computing $\psi = \sqrt[N]{F}$: $\mathcal{O}(\mathsf{M}(d)) = \mathcal{O}^{\sim}(d)$ op in $\mathbb{A}$.
  - $F_\infty = x^d\, F(1/x)$ the reciprocal polynomial of F,
  - $F_\infty(0) = 1 \rightsquigarrow \exists!\ \phi \in \mathbb{A}[[x]]$ s.t. $\phi(0) = 1$ and $\phi^N = F_\infty$,
  - ϕ is the root of $z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
  - ψ is the reciprocal polynomial of $\lceil \phi \rceil^{\frac{d}{N}}$
- ψ-adic expansion: $\mathcal{O}(\mathsf{M}(d)\log(N)) = \mathcal{O}^{\sim}(d)$ op in $\mathbb{A}$.
  - $F = A\,\psi^{\frac{N}{2}} + B \rightsquigarrow \mathcal{O}(\mathsf{M}(d))$
  - Recursive call on A and B.

Complexity ?

- Computing $\psi = \sqrt[N]{F}$: $\mathcal{O}(\mathsf{M}(d)) = \mathcal{O}^{\sim}(d)$ op in $\mathbb{A}$.
  - $F_\infty = x^d\, F(1/x)$ the reciprocal polynomial of F,
  - $F_\infty(0) = 1 \rightsquigarrow \exists!\ \phi \in \mathbb{A}[[x]]$ s.t. $\phi(0) = 1$ and $\phi^N = F_\infty$,
  - ϕ is the root of $z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
  - ψ is the reciprocal polynomial of $\lceil \phi \rceil^{\frac{d}{N}}$
- ψ-adic expansion: $\mathcal{O}(\mathsf{M}(d)\log(N)) = \mathcal{O}^{\sim}(d)$ op in $\mathbb{A}$.
  - $F = A\,\psi^{\frac{N}{2}} + B \rightsquigarrow \mathcal{O}(\mathsf{M}(d))$
  - Recursive call on A and B.
- Truncation: $n = 2\,\delta/d$.

Total cost: $\delta\,\mathrm{plog}(d)$!

Types and operators.

- $\mathbf{t}_0 = [P_0]$, with $P_0 \in \mathbb{F}[y]$ irreducible

  $\rightsquigarrow v_0$ the Gauss valuation, $R_0(G) = \overline{G(y)/\pi^{v_0(G)}}$, $\mathbb{F}_0 = \mathbb{F}$.

Types and operators.

- $\mathbf{t}_0 = [P_0]$, with $P_0 \in \mathbb{F}[y]$ irreducible

  $\rightsquigarrow v_0$ the Gauss valuation, $R_0(G) = \overline{G(y)/\pi^{v_0(G)}}$, $\mathbb{F}_0 = \mathbb{F}$.
- $\mathbf{t}_k = [P_0, (\phi_1, \lambda_1, P_1), \cdots, (\phi_k, \lambda_k, P_k)]$ is a type if:
  - $\mathbf{t}_{k-1}$ is a type.
  - $\phi_k \in \mathbb{A}[x]$ is monic, irreducible and satisfies $R_{k-1}(\phi_k) \sim P_{k-1}$.
  - $\lambda_k = -m_k/q_k \in \mathbb{Q}^-$, with $(q_k, m_k) \in \mathbb{N}^2$ coprime.
  - $P_k \in \mathbb{F}_k[y]$ is monic, irreducible over $\mathbb{F}_k := \mathbb{F}_{k-1}[y]/(P_{k-1})$.

$$\ell_k := \deg(P_k); z_k := y \mod P_k(y) \in \mathbb{F}_{k+1}$$

Types and operators.

- $\mathbf{t}_0 = [P_0]$, with $P_0 \in \mathbb{F}[y]$ irreducible

  $\rightsquigarrow v_0$ the Gauss valuation, $R_0(G) = \overline{G(y)/\pi^{v_0(G)}}$, $\mathbb{F}_0 = \mathbb{F}$.
- $\mathbf{t}_k = [P_0, (\phi_1, \lambda_1, P_1), \cdots, (\phi_k, \lambda_k, P_k)]$ is a type if:
  - $\mathbf{t}_{k-1}$ is a type.
  - $\phi_k \in \mathbb{A}[x]$ is monic, irreducible and satisfies $R_{k-1}(\phi_k) \sim P_{k-1}$.
  - $\lambda_k = -m_k/q_k \in \mathbb{Q}^-$, with $(q_k, m_k) \in \mathbb{N}^2$ coprime.
  - $P_k \in \mathbb{F}_k[y]$ is monic, irreducible over $\mathbb{F}_k := \mathbb{F}_{k-1}[y]/(P_{k-1})$.
- $v_k(G) := \min_i \left(q_{k-1} v_{k-1}(a'_i \phi_{k-1}^i) + m_{k-1} i\right)$

$$\ell_k := \deg(P_k); z_k := y \mod P_k(y) \in \mathbb{F}_{k+1}$$

Types and operators.

- $\mathbf{t}_0 = [P_0]$, with $P_0 \in \mathbb{F}[y]$ irreducible

  $\rightsquigarrow v_0$ the Gauss valuation, $R_0(G) = \overline{G(y)/\pi^{v_0(G)}}$, $\mathbb{F}_0 = \mathbb{F}$.
- $\mathbf{t}_k = [P_0, (\phi_1, \lambda_1, P_1), \cdots, (\phi_k, \lambda_k, P_k)]$ is a type if:
  - $\mathbf{t}_{k-1}$ is a type.
  - $\phi_k \in \mathbb{A}[x]$ is monic, irreducible and satisfies $R_{k-1}(\phi_k) \sim P_{k-1}$.
  - $\lambda_k = -m_k/q_k \in \mathbb{Q}^-$, with $(q_k, m_k) \in \mathbb{N}^2$ coprime.
  - $P_k \in \mathbb{F}_k[y]$ is monic, irreducible over $\mathbb{F}_k := \mathbb{F}_{k-1}[y]/(P_{k-1})$.
- $v_k(G) := \min_i \left(q_{k-1} v_{k-1}(a_i' \phi_{k-1}^i) + m_{k-1} i\right)$
- $R_k(G) = \sum_{i \in \Delta_k} z_{k-1}^{\tau_{k,i}} R_{k-1}(a_i \phi_k^i)(z_{k-1})\, y^{\frac{i - i_k(G)}{q_k}} \in \mathbb{F}_k[y]$

$$\ell_k := \deg(P_k); z_k := y \mod P_k(y) \in \mathbb{F}_{k+1}$$

Types and operators.

- $\mathbf{t}_0 = [P_0]$, with $P_0 \in \mathbb{F}[y]$ irreducible

  $\rightsquigarrow v_0$ the Gauss valuation, $R_0(G) = \overline{G(y)/\pi^{v_0(G)}}$, $\mathbb{F}_0 = \mathbb{F}$.
- $\mathbf{t}_k = [P_0, (\phi_1, \lambda_1, P_1), \cdots, (\phi_k, \lambda_k, P_k)]$ is a type if:
  - $\mathbf{t}_{k-1}$ is a type.
  - $\phi_k \in \mathbb{A}[x]$ is monic, irreducible and satisfies $R_{k-1}(\phi_k) \sim P_{k-1}$.
  - $\lambda_k = -m_k/q_k \in \mathbb{Q}^-$, with $(q_k, m_k) \in \mathbb{N}^2$ coprime.
  - $P_k \in \mathbb{F}_k[y]$ is monic, irreducible over $\mathbb{F}_k := \mathbb{F}_{k-1}[y]/(P_{k-1})$.
- $v_k(G) := \min_i \left(q_{k-1} v_{k-1}(a_i' \phi_{k-1}^i) + m_{k-1} i\right)$
- $R_k(G) = \sum_{i \in \Delta_k} z_{k-1}^{\tau_{k,i}} R_{k-1}(a_i \phi_k^i)(z_{k-1})\, y^{\frac{i - i_k(G)}{q_k}} \in \mathbb{F}_k[y]$

$$\ell_k := \deg(P_k); z_k := y \mod P_k(y) \in \mathbb{F}_{k+1}$$

ϕ_k approximate root $\Longrightarrow \ell_k\, q_k > 1$ (no refinment step !)

General algorithm

Algorithm `FastIrreducible`(F)**:**

Input: $F \in \mathbb{A}[x]$ monic separable s.t. $\mathrm{Char}(\mathbb{F}) \nmid \deg(F)$.
Output: F irreducible ?, a type **t** and a representative ϕ of **t**.

if $R_0(F)$ *is not some* $P_0^{N_0}$ **then return** *False*, [];
$\mathbf{t} \leftarrow [P_0]$, $k \leftarrow 1$, $N \leftarrow N_0$;
while $N > 1$ **do**
  $\phi_k \leftarrow \sqrt[N]{F}$;
  if $\mathcal{N}_k^-(F)$ *is not one sided* **then return** *(False,* **t**, ϕ_k*)*;
  if $R_k(F)$ *is not some* $P_k^{N_k}$ **then return** *(False,* **t**, ϕ_k*)*;
  $\mathbf{t} \leftarrow \mathbf{t} \cup (\phi_k, \lambda_k, P_k)$; // λ_k `the slope of` $\mathcal{N}_k(F)$
  $N \leftarrow N_k$, $k \leftarrow k + 1$;
return *(True,* **t**, F*)*

Factorisation over $\mathbb{A}[x]$

a new divide and conquer strategy

adapt the Hensel–Newton algorithm to extended valuations

Hensel lemma works with extended valuations

- $\phi = \phi_k$ a representative of a type $\mathbf{t}_{k-1}$ (i.e. $R_{k-1}(\phi) \sim P_{k-1}$),
- $v = v_{k+1}$ an augmented valuation (from v_k, ϕ and some λ_k).

Lemma

Assume $B = \phi^b + \cdots$ *and* $v(B) = b\,v(\phi)$. *Then*

- $v(A\%B) \geq v(A)$,
- $v(A /\!\!/ B) \geq v(A) - v(B)$.

Notation:

$$F = \sum_{B=(b_1,\cdots,b_k)} c_B(x)\,\phi_1^{b_1} \cdots \phi_k^{b_k}$$ the multi-adic expansion of F

$\lceil F \rceil^n \rightsquigarrow$ remove from it the terms of valuations $> n$

Adaptation of the Hensel algorithm

In: $v(F - G\,H) \geq v(F) + n$ and $v(S\,G + T\,H - 1) \geq n$.

Algorithm `HenselStep`:

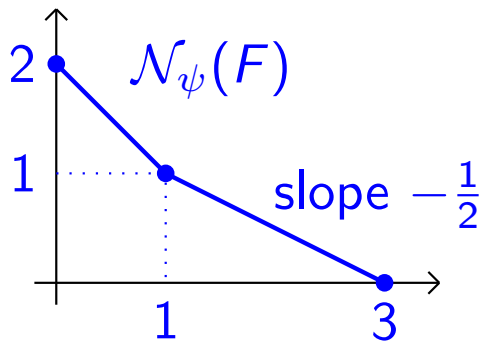
$E \leftarrow \lceil F - G\,H \rceil^{v(F)+2n}$;
$Q, R \leftarrow \lceil \mathtt{QuoRem}(U\,E, H) \rceil^{v(F)+2n}$;
$\tilde{G} \leftarrow \lceil G + E\,V + Q\,G \rceil^{v(G)+2n}$;
$\tilde{H} \leftarrow \lceil H + R \rceil^{v(H)+2n}$;
$B \leftarrow \lceil U\,\tilde{G} + V\,\tilde{H} - 1 \rceil^{2n}$;
$C, D \leftarrow \lceil \mathtt{QuoRem}(U\,B, \tilde{H}) \rceil^{2n}$;
$\tilde{U} \leftarrow \lceil U - D \rceil^{2n-v(G)}$;
$\tilde{V} \leftarrow \lceil V - B\,V - C\,\tilde{G} \rceil^{2n-v(H)}$;
return $\tilde{H}$, $\tilde{G}$, $\tilde{U}$, $\tilde{V}$

Out: $v(F - \tilde{G}\,\tilde{H}) \geq v(F) + 2\,n$ and $v(\tilde{S}\,\tilde{G} + \tilde{T}\,\tilde{H} - 1) \geq 2\,n$.

Good initialisation ?

$$F = \underbrace{\psi^3}_{18} + \underbrace{\pi^3 x^2 \psi}_{19} + \underbrace{\pi^6 x}_{20} \text{ with } \psi = x^3 - \pi^2$$

- $v_\psi(\pi) = 3$, $v_\psi(x) = 2$, $v_\psi(\psi) = 6$.

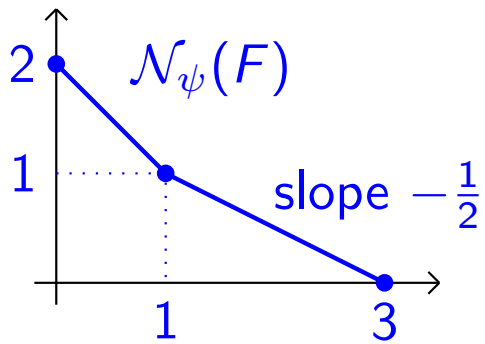


Good initialisation ?

$$F = \underbrace{\psi^3}_{39} + \underbrace{\pi^3 x^2 \psi}_{39} + \underbrace{\pi^6 x}_{40} \text{ with } \psi = x^3 - \pi^2$$

- $v_\psi(\pi) = 3,\ v_\psi(x) = 2,\ v_\psi(\psi) = 6.$
- Extend v_ψ from right hand slope:

$$v(\pi) = 6,\ v(x) = 4,\ v(\psi) = 13$$

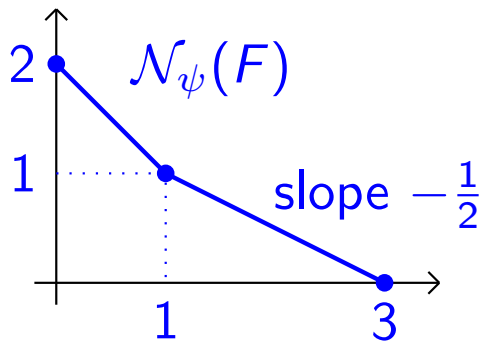


$$v(\pi) = q\, v_\psi(\pi),\ v(x) = q\, v_\psi(x),\ v(\psi) = q\, v_\psi(\psi) + m$$

Good initialisation ?

$$F = \underbrace{\psi^3}_{39} + \underbrace{\pi^3\, x^2\, \psi}_{39} + \underbrace{\pi^6\, x}_{40} \text{ with } \psi = x^3 - \pi^2$$

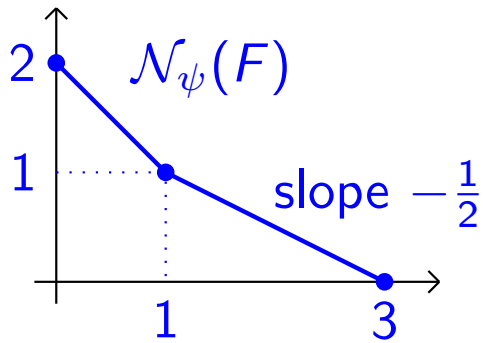
- $v_\psi(\pi) = 3,\ v_\psi(x) = 2,\ v_\psi(\psi) = 6.$
- Extend v_ψ from right hand slope:
$$v(\pi) = 6,\ v(x) = 4,\ v(\psi) = 13$$



- $\tilde{R}(F) = y\,(y^2 + 1)$
- $H_0 = \overbrace{\psi}^{13},\ G_0 = \overbrace{\psi^2 + \pi^3\, x^2}^{26} \Longrightarrow \overbrace{F}^{39} - H_0\, G_0 = \overbrace{\pi^6\, x}^{40}$

Good initialisation ?

$$F = \underbrace{\psi^3}_{39} + \underbrace{\pi^3\, x^2\, \psi}_{39} + \underbrace{\pi^6\, x}_{40} \text{ with } \psi = x^3 - \pi^2$$



- $v_\psi(\pi) = 3,\ v_\psi(x) = 2,\ v_\psi(\psi) = 6.$
- Extend v_ψ from right hand slope:
  $$v(\pi) = 6,\ v(x) = 4,\ v(\psi) = 13$$
- $\tilde{R}(F) = y\,(y^2 + 1)$
- $H_0 = \overbrace{\psi}^{13},\ G_0 = \overbrace{\psi^2 + \pi^3\, x^2}^{26} \Longrightarrow \overbrace{F}^{39} - H_0\, G_0 = \overbrace{\pi^6\, x}^{40}$
- With $s_0 = 1$ and $t_0 = -y$, we have $s_0\,(y^2 + 1) + t_0\, y = 1$,
- $S_0 = \underbrace{\pi^{-5} x}_{-26},\ T_0 = \underbrace{-\pi^{-5} x\, \psi}_{-13} \Longrightarrow S_0\, G_0 + T_0\, H_0 - 1 = \underbrace{\pi^{-2} \psi}_{1}$

Multi-factor Hensel lifting

(modified residual polynomial: $\tilde{R}_k(G)(y) := y^{i_k(G)} R_k(G)(y^{q_k})$)

Main algorithm:

Given
- a factorisation $\tilde{R}(F) = h_0 h_1 \cdots h_r h_\infty$; $h_0 = y^s$, $h_\infty \in \mathbb{F}_k^\times$,
- a precision $n \in \mathbb{N}$.

Compute a factorisation (use a subproduct tree)

$$v(F - F_0 F_1 \cdots F_r F_\infty) > n \quad \text{with} \quad \tilde{R}(F_i) = h_i, \quad i = 0, \ldots, t, \infty.$$

Remark: $F_0, \cdots, F_r$ of type $\mathbf{t}$; $\mathbf{t}$ does not divide F_∞

Complexity: $\mathcal{O}\left(\frac{v(F)+n}{v(\pi)}\, d\right)$

Factorisation with precision σ in $\mathbb{A}[x]$: $\mathcal{O}(\sigma\, d + \delta)$ if $\deg(F_\infty) \leq \frac{d}{2}$.

A factorisation algorithm.

1. Run `FastIrreducible` with precision $2\delta/d$ $\qquad \mathcal{O}(\delta)$

   $\rightsquigarrow$ either F irreducible (return F), either get a type $\mathbf{t}_{k-1}$.

2. Factor $\tilde{R}_k(F) = h_0 h_1 \cdots h_r$ in $\mathbb{F}_k[y]$.

3. Lift $F = F_0 F_1 \cdots F_r$ with precision σ. $\qquad \mathcal{O}(\sigma\, d + \delta)$

4. Go back to Step 1 for each F_i.

Total: $\qquad \mathcal{O}(\rho\,(\sigma\, d + \delta))$.

A divide and conquer algorithm.

1. Find a type $\mathbf{t}$ such that $F_{\mathbf{t}}$ has degree $> d/2$ and that either $F_{\mathbf{t}}$ is irreducible, either any of its proper factor has degree $\leq d/2$.

   Previous algorithm with precision $4\,\delta/d$ $\qquad \mathcal{O}(\rho\,\delta)$

2. Hensel $\rightsquigarrow F = F_0\,F_1 \cdots F_r F_\infty$ $\qquad \mathcal{O}(n\,d + \delta)$

3. Recursive call for each non irreducible factor.

Total: $\qquad \mathcal{O}((n+\delta)\,d)$

State of the art (sketch)

- Abhyankar-Moh [Ab06]: approximate roots,
- Mac Lane, Abhyankar [Ma36^2,Ab90,Ru14]: extended valuations,
- Montes et al [Mo99,GuMoNa11&12,BaNaSt13,GuNaPa12] $\mathcal{O}(d^2 + d\delta^2)$,
- Caruso et al [CaRoVa16]: slope factorisation,

Case $\mathbb{A} = \mathbb{K}[[x]]$:

- Sasaki et al [KaSa99,AlAtMa17]: Extended Hensel Construction at least $\mathcal{O}(d^2(\delta + d^2))$,
- Puiseux [PoRy15,PoWe]: Newton–Puiseux algorithm $\mathcal{O}(d\,\delta)$.

Conclusion

Up to factorisations in $\mathbb{F}_k[y]$:

- Irreducibility test in $\mathbb{A}[x]$ in $\mathcal{O}(\delta)$, $\leftarrow$ improved by a factor d !
- "direct" factorisation in $\mathbb{A}[x]$: $\mathcal{O}(\rho\, n\, d)$, $\leftarrow$ was $\mathcal{O}(n\, d^2)$
- Divide and conquer: $\mathcal{O}((n+\delta)\, d)$.

Application: OM-factorisation for $\mathbb{A} = \mathbb{Z}_p$ when $\mathrm{Char}(\mathbb{F}) \nmid d$:

- $\mathcal{O}(d^2 + \delta\, d\, \log(p))$ $\leftarrow$ was $\mathcal{O}(d^2 + \delta\, d\, \log(p) + d\delta^2)$!

Practical aspects:

- Sage prototype,
- some `C` implementation via Flint (irreducibility for $\mathbb{A} = \mathbb{F}_q[[t]]$).

Bibliography


S. Abhyankar.
Irreducibility criterion for germs of analytic functions of two complex variables.
Adv. Mathematics, 35:190–257, 1989.


S. Abhyankar.
Algebraic Geometry for Scientists and Engineers, volume 35 of *Mathematical surveys and monographs*.
Amer. Math. Soc., 1990.


S. Abhyankar.
Lectures on Algebra.
Number vol. 1 in Lectures on Algebra. World Scientific, 2006.


P. Alvandi, M. Ataei, and M. Moreno Maza.
On the extended hensel construction and its application to the computation of limit points.
In ISSAC '17, pages 13–20.


J.-D. Bauch, E. Nart, and H. Stainsby.

Complexity of the OM factorizations of polynomials over local fields.
LMS Journal of Computation and Mathematics, 16:139–171, 2013.


X. Caruso, D. Roe, and T. Vaccon.
Division and slope factorization of p-adic polynomials.
In ISSAC '16, pages 159–166.


J. v. z. Gathen and J. Gerhard.
Modern Computer Algebra.
Cambridge University Press, New York, NY, USA, 3rd edition, 2013.


J. Guàrdia, J. Montes, and E. Nart.
Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields.
J. Théor. Nombres Bordx., 23(3):667–696, 2011.


J. Guàrdia, J. Montes, and E. Nart.

Newton polygons of higher order in algebraic number theory.
Transsactions of the American Mathematical Society, 364:361–416, 2012.


J. Guàrdia, E. Nart, and S. Pauli.
Single-factor lifting and factorization of polynomials over local fields.
Journal of Symbolic Computation, 47(11):1318 – 1346, 2012.


F. Kako and T. Sasaki.
Solving multivariate algebraic equations by Hensel construction.

Japan J. of Industrial and Applied Math., 16:257–285, 1999.


S. MacLane.
A construction for absolute values in polynomial rings.
Trans. Amer. Math. Soc., 40(3):363–395, 1936.


S. Mac Lane.

A construction for prime ideals as absolute values of an algebraic field.
Duke Math. J., 2(3):492–510, 1936.


J. Montes Peral.
Polígonos de newton de orden superior y aplicaciones aritméticas.
PhD thesis, Universitat de Barcelona, 1999.


A. Poteaux and M. Rybowicz.
Improving complexity bounds for the computation of puiseux series over finite fields.
ISSAC '15, pages 299–306


A. Poteaux and M. Weimann.
Computing Puiseux series: a fast divide and conquer algorithm.
Annales Henri Lebesgue, 4:1061–1102, 2021.


A. Poteaux and M. Weimann.
A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$.

Submitted for publication

A. Poteaux and M. Weimann.
Local polynomial factorisation: improving the Montes algorithm
Preprint

J. Rüth.
Models of curves and valuations.
PhD thesis, Universität Ulm, 2014.