An effective proof of the p-curvature conjecture for order one linear differential equations

ongoing joint work with Florian Fürnsinn.

Lucas Pannier

Laboratoire de Mathématiques de Versailles, UVSQ
CNRS UMR-8100

June 13th 2025

GADEPs: Differential Equations and Prime Numbers

Power series hierarchy

$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

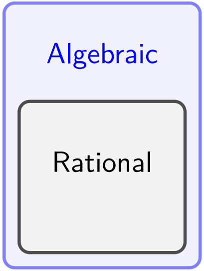
Rational

Power series hierarchy

$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

Algebraic series

y is algebraic if $\exists P \in \mathbb{Z}[x, T],\ P(x, y) = 0.$



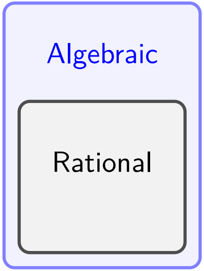
Power series hierarchy

$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

Algebraic series

y is algebraic over $\mathbb{Q}(x)$ if $\exists P \in \mathbb{Z}[x, T]$, $P(x, y) = 0$.

$$\to y = (1-x)^{2/5} = 1 - \tfrac{2}{5}x + \tfrac{6}{50}x^2 + \dots, \quad y^5 - (x-1)^2 = 0.$$



Power series hierarchy

$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

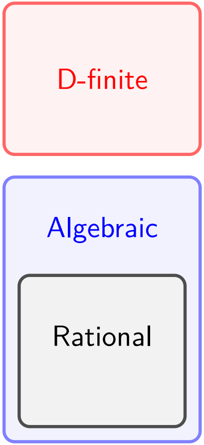
Algebraic series

y is algebraic over $\mathbb{Q}(x)$ if $\exists P \in \mathbb{Z}[x, T]$, $P(x, y) = 0$.

$\rightarrow y = (1-x)^{2/5} = 1 - \frac{2}{5}x + \frac{6}{50}x^2 + \dots, \; y^5 - (x-1)^2 = 0.$

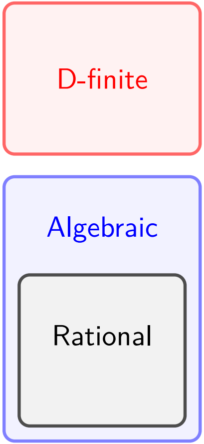
D-finite series

y is D-finite if $\exists a_i \in \mathbb{Z}[x]$ such that $a_r y^{(r)} + \cdots + a_0 y = 0$.



Power series hierarchy

$$y = \sum_{n\geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$



Algebraic series

y is algebraic over $\mathbb{Q}(x)$ if $\exists P \in \mathbb{Z}[x, T]$, $P(x, y) = 0$.

$\rightarrow y = (1-x)^{2/5} = 1 - \frac{2}{5}x + \frac{6}{50}x^2 + \dots,\ y^5 - (x-1)^2 = 0.$

D-finite series

y is D-finite if $\exists a_i \in \mathbb{Z}[x]$ such that $a_r y^{(r)} + \cdots + a_0 y = 0$.

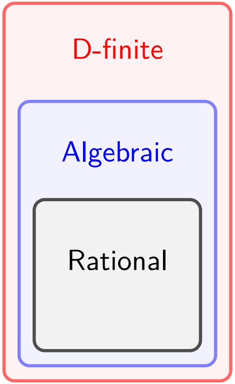
$\rightarrow y = \exp(x^2+1)$ satisfies $y' - 2xy = 0$.

Power series hierarchy

$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

Theorem (Abel, 1827)

Algebraic series are D-finite.



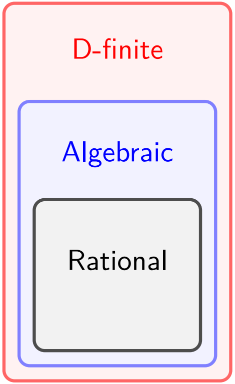
Power series hierarchy

$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

Theorem (Abel, 1827)

Algebraic series are D-finite.

$\rightarrow y = (1-x)^{2/5}$, $5(1-x)y' + 2y = 0$.
$\rightarrow y = \exp(x^2+1)$ is not algebraic.



Power series hierarchy

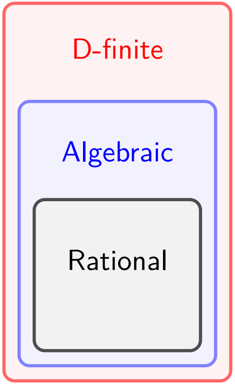
$$y = \sum_{n \geq 0} u_n x^n, \qquad u_n \in \mathbb{Q}$$

Theorem (Abel, 1827)

Algebraic series are D-finite.

$\rightarrow$ $y = (1-x)^{2/5}$, $5(1-x)y' + 2y = 0$.
$\rightarrow$ $y = \exp(x^2+1)$ is not algebraic.

What D-finite power series are algebraic?



Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

- $y := \exp(\int u)$ satisfies $y' = uy$, when is it algebraic?

Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

- $y := \exp(\int u)$ satisfies $y' = uy$, when is it algebraic?

$\rightarrow$ if $u := x^{-1/2}$, then $y = \exp(2\sqrt{x})$ is not algebraic.
$\rightarrow$ if $u := \frac{x}{x^2+1}$, then $y = \sqrt{x^2+1}$ is algebraic.

Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

- $y := \exp(\int u)$ satisfies $y' = uy$, when is it algebraic?

$\rightarrow$ if $u := x^{-1/2}$, then $y = \exp(2\sqrt{x})$ is not algebraic.
$\rightarrow$ if $u := \frac{x}{x^2+1}$, then $y = \sqrt{x^2+1}$ is algebraic.

Fuchs' problem

Let $\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0$, $a_i \in \mathbb{Z}[x]$.
Decide if the differential equation $\mathcal{L}y = 0$ has a basis of algebraic solutions.

Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

- $y := \exp(\int u)$ satisfies $y' = uy$, when is it algebraic?

$\rightarrow$ if $u := x^{-1/2}$, then $y = \exp(2\sqrt{x})$ is not algebraic.
$\rightarrow$ if $u := \frac{x}{x^2+1}$, then $y = \sqrt{x^2+1}$ is algebraic.

Fuchs' problem

Let $\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0$, $a_i \in \mathbb{Z}[x]$.
Decide if the differential equation $\mathcal{L}y = 0$ has a basis of algebraic solutions.

$\rightarrow$ solutions of $xy'' + y' = 0$ are 1 and $\log$ $\rightarrow$ transcendental.
$\rightarrow$ solutions of $2xy'' + y' = 0$ are 1 and $\sqrt{x}$ $\rightarrow$ algebraic.

Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

[Risch, 1971], [Baldassari-Dwork, 1979], [Davenport, 1981], Risch's algorithm.

Fuchs' problem

Let $\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0$, $a_i \in \mathbb{Z}[x]$.
Decide if the differential equation $\mathcal{L}y = 0$ has a basis of algebraic solutions.

$\rightarrow$ solutions of $xy'' + y' = 0$ are 1 and $\log$ $\rightarrow$ transcendental.
$\rightarrow$ solutions of $2xy'' + y' = 0$ are 1 and $\sqrt{x}$ $\rightarrow$ algebraic.

Deciding algebraicity

Abel's problem

Let $u \in \overline{\mathbb{Q}(x)}$, decide if the nonzero solutions of $y' = uy$ are algebraic.

[Risch, 1971], [Baldassari-Dwork, 1979], [Davenport, 1981], Risch's algorithm.

Fuchs' problem

Let $\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0$, $a_i \in \mathbb{Z}[x]$.
Decide if the differential equation $\mathcal{L}y = 0$ has a basis of algebraic solutions.

[Singer, 1980], relying on Risch's algorithm.

A local-global approach

$$\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0 = 0 \quad a_i \in \mathbb{Z}[x].$$

A local-global approach

$$\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0 = 0 \quad a_i \in \mathbb{Z}[x].$$

- For all prime numbers p, consider $\mathcal{L}_p = \mathcal{L} \bmod p$.

A local-global approach

$$\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0 = 0 \quad a_i \in \mathbb{Z}[x].$$

- For all prime numbers p, consider $\mathcal{L}_p = \mathcal{L} \bmod p$.

Grothendieck's conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all prime numbers p, $\mathcal{L}_p y = 0$ has a basis of algebraic solutions over $\mathbb{F}_p(x)$.

A local-global approach

$$\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0 = 0 \quad a_i \in \mathbb{Z}[x].$$

- For all prime numbers p, consider $\mathcal{L}_p = \mathcal{L} \bmod p$.

Grothendieck's conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all prime numbers p, $\mathcal{L}_p y = 0$ has a basis of algebraic solutions over $\mathbb{F}_p(x)$.

Attach to $\mathcal{L}_p$ an $\mathbb{F}_p(x)$-linear map called the p-curvature.

A local-global approach

$$\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0 = 0 \quad a_i \in \mathbb{Z}[x].$$

- For all prime numbers p, consider $\mathcal{L}_p = \mathcal{L} \bmod p$.

Grothendieck's conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all prime numbers p, $\mathcal{L}_p y = 0$ has a basis of algebraic solutions over $\mathbb{F}_p(x)$.

Attach to $\mathcal{L}_p$ an $\mathbb{F}_p(x)$-linear map called the p-curvature.

Theorem (Cartier's Lemma)

The p-curvature is zero if and only if $\mathcal{L}_p y = 0$ has a basis of algebraic solutions.

A local-global approach

$$\mathcal{L} = a_n \left(\frac{d}{dx}\right)^n + \cdots + a_1 \frac{d}{dx} + a_0 = 0 \quad a_i \in \mathbb{Z}[x].$$

- For all prime numbers p, consider $\mathcal{L}_p = \mathcal{L} \bmod p$.

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all prime numbers p, the p-curvature of $\mathcal{L}$ vanishes.

Attach to $\mathcal{L}_p$ an $\mathbb{F}_p(x)$-linear map called the p-curvature.

Theorem (Cartier's Lemma)

The p-curvature is zero if and only if $\mathcal{L}_p y = 0$ has a basis of algebraic solutions.

The p-curvature conjecture

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all primes p, the p-curvature of $\mathcal{L}$ vanishes.

The p-curvature conjecture

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all primes p, the p-curvature of $\mathcal{L}$ vanishes.

- Picard-Fuchs equations [Katz, 1972], order one [Honda, 1974; Chudnovsky^2, 1985], q-difference equations [Di Vizio, 2001],...

The p-curvature conjecture

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all primes p, the p-curvature of $\mathcal{L}$ vanishes.

- Picard-Fuchs equations [Katz, 1972], **order one [Honda, 1974; Chudnovsky[2], 1985]**, q-difference equations [Di Vizio, 2001],...

The p-curvature conjecture

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all primes p, the p-curvature of $\mathcal{L}$ vanishes.

- Picard-Fuchs equations [Katz, 1972], **order one [Honda, 1974; Chudnovsky[2], 1985]**, q-difference equations [Di Vizio, 2001],...

$\to$ Observation: when the solution is not algebraic, p-curvatures are often nonzero.
For $(x^2+1)y' + y = 0$, p-curvatures are $\frac{1}{x^4+1} \in \mathbb{F}_2(x)$, $-\frac{1}{x^6+1} \in \mathbb{F}_3(x)$.

The p-curvature conjecture

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all primes p, the p-curvature of $\mathcal{L}$ vanishes.

- Picard-Fuchs equations [Katz, 1972], **order one [Honda, 1974; Chudnovsky^2, 1985]**, q-difference equations [Di Vizio, 2001],...

$\rightarrow$ Observation: when the solution is not algebraic, p-curvatures are often nonzero.
For $(x^2+1)y' + y = 0$, p-curvatures are $\frac{1}{x^4+1} \in \mathbb{F}_2(x)$, $-\frac{1}{x^6+1} \in \mathbb{F}_3(x)$.

Theorem (Honda, 1974)

The p-curvature conjecture holds for equations $y' = \frac{a}{b}y$ with $a, b \in \mathbb{Q}[x]$.

The p-curvature conjecture

Grothendieck's p-curvature conjecture

All solutions of $\mathcal{L}y = 0$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all primes p, the p-curvature of $\mathcal{L}$ vanishes.

- Picard-Fuchs equations [Katz, 1972], **order one [Honda, 1974; Chudnovsky^2, 1985]**, q-difference equations [Di Vizio, 2001],...

$\rightarrow$ Observation: when the solution is not algebraic, p-curvatures are often nonzero.
For $(x^2+1)y' + y = 0$, p-curvatures are $\frac{1}{x^4+1} \in \mathbb{F}_2(x)$, $-\frac{1}{x^6+1} \in \mathbb{F}_3(x)$.

Theorem (Honda, 1974)

The p-curvature conjecture holds for equations $y' = \frac{a}{b}y$ with $a, b \in \mathbb{Q}[x]$.

- Not a decision procedure: infinitely many conditions to check.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \qquad .$$

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b} y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_{k=0}^{s} c_k x^k + \sum_i \sum_{j \geq 1} \frac{\alpha_{i,j}}{(x - \beta_i)^j}.$$

- $\frac{a}{b} = x, \ y = \exp(\frac{x^2}{2})$

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b} y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_{k=0}^{s} c_k x^k + \sum_i \sum_{j \geq 1} \frac{\alpha_{i,j}}{(x - \beta_i)^j}.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b} y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_{k=0}^{s} c_k x^k + \sum_i \sum_{j \geq 1} \frac{\alpha_{i,j}}{(x - \beta_i)^j}.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$,

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_{k=0}^{s} c_k x^k + \sum_i \sum_{j \geq 1} \frac{\alpha_{i,j}}{(x - \beta_i)^j}.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$, then y is not algebraic.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = 0 + \sum_i \sum_{j \geq 1} \frac{\alpha_{i,j}}{(x-\beta_i)^j}.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$, then y is not algebraic.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_i \sum_{j \geq 1} \frac{\alpha_{i,j}}{(x-\beta_i)^j}.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$, then y is not algebraic.
- $\frac{a}{b} = -\frac{1}{x^2}$, $y = \exp(\frac{1}{x})$ not algebraic

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_i \frac{\alpha_i}{x-\beta_i} + \sum_i \sum_{j \geq 2} \frac{\alpha_{i,j}}{(x-\beta_i)^j}.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$, then y is not algebraic.
- $\frac{a}{b} = -\frac{1}{x^2}$, $y = \exp(\frac{1}{x})$ not algebraic $\rightsquigarrow$ if b has double roots, then y is not algebraic.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_i \frac{\alpha_i}{x - \beta_i} + 0.$$

- $\frac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$, then y is not algebraic.
- $\frac{a}{b} = -\frac{1}{x^2}$, $y = \exp(\frac{1}{x})$ not algebraic $\rightsquigarrow$ if b has double roots, then y is not algebraic.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b} y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_i \frac{\alpha_i}{x - \beta_i}.$$

- $\dfrac{a}{b} = x$, $y = \exp(\frac{x^2}{2})$ not algebraic $\rightsquigarrow$ if $\deg(a) \geq \deg(b)$, then y is not algebraic.
- $\dfrac{a}{b} = -\dfrac{1}{x^2}$, $y = \exp(\frac{1}{x})$ not algebraic $\rightsquigarrow$ if b has double roots, then y is not algebraic.

Fact: If $y' = \frac{a}{b} y$ has algebraic solutions, then $\deg(a) < \deg(b)$ and b is squarefree.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b} y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_i \frac{\alpha_i}{x - \beta_i}.$$

Fact: If $y' = \frac{a}{b} y$ has algebraic solutions, then $\deg(a) < \deg(b)$ and b is squarefree.

$\rightarrow \dfrac{a}{b} = \dfrac{1}{x^2+1} = \dfrac{i}{2(x+i)} - \dfrac{i}{2(x-i)}$, $y = \exp(\arctan(x))$ is not algebraic.

First-order differential equations over $\mathbb{Q}(x)$

$$y' = \frac{a}{b}y, \quad a, b \in \mathbb{Q}[x], \quad \frac{a}{b} = \sum_i \frac{\alpha_i}{x - \beta_i}.$$

Fact: If $y' = \frac{a}{b}y$ has algebraic solutions, then $\deg(a) < \deg(b)$ and b is squarefree.

$\to \dfrac{a}{b} = \dfrac{1}{x^2+1} = \dfrac{i}{2(x+i)} - \dfrac{i}{2(x-i)}$, $y = \exp(\arctan(x))$ is not algebraic.

Fact: $y = \exp\left(\int \sum_i \frac{\alpha_i}{x-\beta_i}\right) = \prod_i (x - \beta_i)^{\alpha_i}$ is algebraic *if and only if* $\forall i, \alpha_i \in \mathbb{Q}$.

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

- No closed formula for higher order.

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

- No closed formula for higher order.
- If the p-curvature vanishes, then u has the form $\sum_i \frac{\alpha_i}{x-\beta_i}$, $\alpha_i, \beta_i \in \overline{\mathbb{F}_p}$.

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

- No closed formula for higher order.
- If the p-curvature vanishes, then u has the form $\sum_i \frac{\alpha_i}{x - \beta_i}$, $\alpha_i, \beta_i \in \overline{\mathbb{F}_p}$.
- Let $u = \sum_i \frac{\alpha_i}{x - \beta_i}$, its p-curvature is $\sum_i \frac{\alpha_i^p - \alpha_i}{(x - \beta_i)^p}$,

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

- No closed formula for higher order.
- If the p-curvature vanishes, then u has the form $\sum_i \frac{\alpha_i}{x - \beta_i}$, $\alpha_i, \beta_i \in \overline{\mathbb{F}_p}$.
- Let $u = \sum_i \frac{\alpha_i}{x - \beta_i}$, its p-curvature is $\sum_i \frac{\alpha_i^p - \alpha_i}{(x - \beta_i)^p}$, vanishes *if and only if* [1] $\alpha_i \in \mathbb{F}_p$.

[1] Except for primes p dividing $\beta_i - \beta_j$, $i \neq j$.

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

- No closed formula for higher order.
- If the p-curvature vanishes, then u has the form $\sum_i \frac{\alpha_i}{x - \beta_i}$, $\alpha_i, \beta_i \in \overline{\mathbb{F}_p}$.
- Let $u = \sum_i \frac{\alpha_i}{x - \beta_i}$, its p-curvature is $\sum_i \frac{\alpha_i^p - \alpha_i}{(x - \beta_i)^p}$, vanishes *if and only if*[1] $\alpha_i \in \mathbb{F}_p$.

The proof of Honda's Theorem is reduced to proving that for a single $\alpha \in \overline{\mathbb{Q}}$, α is rational *if and only if* $\alpha \bmod p \in \mathbb{F}_p$ for almost all primes p.

[1] Except for primes p dividing $\beta_i - \beta_j$, $i \neq j$.

First-order differential equations over $\mathbb{F}_p(x)$

Theorem (Jacobson, 1937)

Let $u \in \mathbb{F}_p(x)$, the p-curvature of equation $y' = uy$ is $u^{(p-1)} + u^p$.

- No closed formula for higher order.
- If the p-curvature vanishes, then u has the form $\sum_i \frac{\alpha_i}{x - \beta_i}$, $\alpha_i, \beta_i \in \overline{\mathbb{F}_p}$.
- Let $u = \sum_i \frac{\alpha_i}{x - \beta_i}$, its p-curvature is $\sum_i \frac{\alpha_i^p - \alpha_i}{(x - \beta_i)^p}$, vanishes *if and only if* [1] $\alpha_i \in \mathbb{F}_p$.

The proof of Honda's Theorem is reduced to proving that for a single $\alpha \in \overline{\mathbb{Q}}$, α is rational *if and only if* α mod $p \in \mathbb{F}_p$ for almost all primes p.

- α mod p is a root of π_α mod p, with $\pi_\alpha \in \mathbb{Z}[x]$ the minimal polynomial of α.

[1] Except for primes p dividing $\beta_i - \beta_j$, $i \neq j$.

Kronecker's theorem

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R \in \mathbb{Q}[x]$ be irreducible. If for almost all prime numbers p the polynomial $R \bmod p$ has a root in $\mathbb{F}_p$, then R has a root in $\mathbb{Q}$, hence is linear.

Kronecker's theorem

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R \in \mathbb{Q}[x]$ be irreducible. If for almost all prime numbers p the polynomial $R \bmod p$ has a root in $\mathbb{F}_p$, then R has a root in $\mathbb{Q}$, hence is linear.

Theorem (Honda, 1974)

The p-curvature conjecture holds for equations $y' = \frac{a}{b}y$ with $a, b \in \mathbb{Q}[x]$.

Kronecker's theorem

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R \in \mathbb{Q}[x]$ be irreducible. If for almost all prime numbers p the polynomial $R \bmod p$ has a root in $\mathbb{F}_p$, then R has a root in $\mathbb{Q}$, hence is linear.

Theorem (Honda, 1974)

The p-curvature conjecture holds for equations $y' = \frac{a}{b}y$ with $a, b \in \mathbb{Q}[x]$.

Proof: Honda's Theorem is equivalent to Kronecker's Theorem.

Kronecker's theorem

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R \in \mathbb{Q}[x]$ be irreducible. If for almost all prime numbers p the polynomial $R \bmod p$ has a root in $\mathbb{F}_p$, then R has a root in $\mathbb{Q}$, hence is linear.

Theorem (Honda, 1974)

The p-curvature conjecture holds for equations $y' = \frac{a}{b} y$ with $a, b \in \mathbb{Q}[x]$.

Proof: Honda's Theorem is equivalent to Kronecker's Theorem.

Theorem (Equivalent statement of Kronecker's Theorem)

Let $R \in \mathbb{Q}[x]$. If for almost all prime numbers p the reduction of R modulo p splits completely over $\mathbb{F}_p$, then R splits completely over $\mathbb{Q}$.

Effective Kronecker

Theorem (Chudnovsky^2, 1985)

Let $R \in \mathbb{Z}[w]$ with leading coefficient $\Delta \in \mathbb{Z}$. There exists $\sigma \in \mathbb{N}$ such that R splits completely over $\mathbb{Q}$ if and only if $R \bmod p$ splits completely over $\mathbb{F}_p$ for all primes p:

- *not dividing Δ,*
- *at most σ.*

Effective Kronecker

Theorem (Chudnovsky[2], 1985; Fürnsinn-P., 2025+)

Let $R \in \mathbb{Z}[w]$ with leading coefficient $\Delta \in \mathbb{Z}$, and let $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$.
Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of R.
Let $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$ and $N := \lceil 10BM \rceil$.
Then R splits completely over $\mathbb{Q}$ if and only if $R \bmod p$ splits completely over $\mathbb{F}_p$ for all primes p:

- *not dividing Δ,*
- *at most $\sigma := (2M+1)N + 2M$.*

Effective Kronecker

Theorem (Chudnovsky^2, 1985; Fürnsinn-P., 2025+)

Let $R \in \mathbb{Z}[w]$ with leading coefficient $\Delta \in \mathbb{Z}$, and let $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$.
Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of R.
Let $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$ and $N := \lceil 10BM \rceil$.
Then R splits completely over $\mathbb{Q}$ if and only if $R \bmod p$ splits completely over $\mathbb{F}_p$ for all primes p:

- *not dividing Δ,*
- *at most $\sigma := (2M+1)N + 2M$.*

Criterion: If $p \le \sigma$, $p \nmid \Delta$ and $R \bmod p$ does not split completely in $\mathbb{F}_p$, then R does not split completely in $\mathbb{Q}$.

Padé approximation

Given power series $f_1, \ldots, f_r \in \mathbb{Q}[[x]]$ and $n, s \in \mathbb{N}$, find polynomials $P_i \in \mathbb{Q}[x]$ such that $\deg(P_i) \leq n$ and

$$P_1 f_1 + \cdots + P_r f_r \in x^s \mathbb{Q}[[x]].$$

Padé approximation

Given power series $f_1, \ldots, f_r \in \mathbb{Q}[[x]]$ and $n, s \in \mathbb{N}$, find polynomials $P_i \in \mathbb{Q}[x]$ such that $\deg(P_i) \leq n$ and

$$P_1 f_1 + \cdots + P_r f_r \in x^s \mathbb{Q}[[x]].$$

- $r(n+1)$ indeterminates, s linear homogeneous equations

Padé approximation

Given power series $f_1, \dots, f_r \in \mathbb{Q}[[x]]$ and $n, s \in \mathbb{N}$, find polynomials $P_i \in \mathbb{Q}[x]$ such that $\deg(P_i) \leq n$ and

$$P_1 f_1 + \cdots + P_r f_r \in x^s \mathbb{Q}[[x]].$$

- $r(n+1)$ indeterminates, s linear homogeneous equations $\Rightarrow s = r(n+1) - 1$.

Padé approximation

Given power series $f_1, \ldots, f_r \in \mathbb{Q}[[x]]$ and $n, s \in \mathbb{N}$, find polynomials $P_i \in \mathbb{Q}[x]$ such that $\deg(P_i) \leq n$ and

$$P_1 f_1 + \cdots + P_r f_r \in x^s \mathbb{Q}[[x]].$$

- $r(n+1)$ indeterminates, s linear homogeneous equations $\Rightarrow s = r(n+1) - 1$.

[Hermite, 1873] e is transcendental, [Padé], [Mahler, 1931].

Padé approximation

Given power series $f_1, \ldots, f_r \in \mathbb{Q}[[x]]$ and $n, s \in \mathbb{N}$, find polynomials $P_i \in \mathbb{Q}[x]$ such that $\deg(P_i) \leq n$ and
$$P_1 f_1 + \cdots + P_r f_r \in x^s \mathbb{Q}[[x]].$$

- $r(n+1)$ indeterminates, s linear homogeneous equations $\Rightarrow s = r(n+1) - 1$.

[Hermite, 1873] e is transcendental, [Padé], [Mahler, 1931].

Algebraicity criterion: With $f_i = f^{i-1}$, f is algebraic *if and only if* the remainder $P_1 + P_2 f + \cdots + P_r f^{r-1}$ vanishes for large n, r.

Chudnovskys' proof

Proof.

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\operatorname{den}(\gamma)^{[L:\mathbb{Q}]} \operatorname{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.
Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, satisfying

- $\left|\operatorname{den}(\gamma_{M,N})^{[L:\mathbb{Q}]} \operatorname{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| \underset{N>>M>>0}{\sim} X(M)^N \cdot Y(M)$;
- $X(M) \underset{M\to\infty}{\to} 0$.

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.
Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, satisfying

- $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| \underset{N>>M>>0}{\sim} X(M)^N \cdot Y(M)$;
- $X(M) \underset{M\to\infty}{\to} 0$.

For $M >> 0$,

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.
Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, satisfying

- $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| \underset{N>>M>>0}{\sim} X(M)^{N} \cdot Y(M)$;
- $X(M) \underset{M\to\infty}{\to} 0$.

For $M >> 0$, $N >> M$,

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.
Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, satisfying

- $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| \underset{N>>M>>0}{\sim} X(M)^N \cdot Y(M)$;
- $X(M) \underset{M\to\infty}{\to} 0$.

For $M >> 0$, $N >> M$, $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| < 1$, hence $\alpha \in \mathbb{Q}$.

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.
Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, satisfying

- $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| \underset{N>>M>>0}{\sim} X(M)^N \cdot Y(M)$;
- $X(M) \underset{M\to\infty}{\to} 0$.

For $M >> 0$, $N >> M$, $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| < 1$, hence $\alpha \in \mathbb{Q}$.
Where do we use the fact that $\alpha \bmod p \in \mathbb{F}_p$?

Chudnovskys' proof

Proof. Assume R has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Padé approximants $P_i(z) \in L[z]$, $\deg(P_i) \leq N$, with $x = 1 - z$

$$P_0(z) + P_1(z)(1-z)^{\alpha} + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = gz^{\sigma} + O(z^{\sigma+1})$$

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$.
For all $\gamma \in L$, $\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right| \geq 1$.
Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, satisfying

- $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| \underset{N>>M>>0}{\sim} X(M)^N \cdot Y(M)$;
- $X(M) \underset{M\to\infty}{\to} 0$.

For $M >> 0$, $N >> M$, $\left|\mathrm{den}(\gamma_{M,N})^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma_{M,N})\right| < 1$, hence $\alpha \in \mathbb{Q}$.
Where do we use the fact that $\alpha \bmod p \in \mathbb{F}_p$?

Effectivity

Lemma

Let $k, \ell, r \in \mathbb{N}$, $p \not| \operatorname{den}(\alpha)$ a rational prime, $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\alpha)$ above p.

i. If $\alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, then p does not divide the denominator of $\binom{k\alpha+\ell}{r}$.

ii. If $\alpha \bmod \mathfrak{p} \notin \mathbb{F}_p$ and p divides the denominator of $\binom{k\alpha+\ell}{r}$, then $p \leq r$.

Effectivity

Lemma

Let $k, \ell, r \in \mathbb{N}$, $p \not| \operatorname{den}(\alpha)$ a rational prime, $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\alpha)$ above p.

i. If $\alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, then p does not divide the denominator of $\binom{k\alpha+\ell}{r}$.

ii. If $\alpha \bmod \mathfrak{p} \notin \mathbb{F}_p$ and p divides the denominator of $\binom{k\alpha+\ell}{r}$, then $p \leq r$.

- Such binomials appear in the Padé approximation with $0 \leq r \leq \sigma$.

Effectivity

Lemma

Let $k, \ell, r \in \mathbb{N}$, $p \nmid \mathrm{den}(\alpha)$ a rational prime, $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\alpha)$ above p.

i. If $\alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, then p does not divide the denominator of $\binom{k\alpha+\ell}{r}$.

ii. If $\alpha \bmod \mathfrak{p} \notin \mathbb{F}_p$ and p divides the denominator of $\binom{k\alpha+\ell}{r}$, then $p \leq r$.

- Such binomials appear in the Padé approximation with $0 \leq r \leq \sigma$.
- Explicit error terms, inequalities instead of asymptotic equivalents.

Effectivity

Lemma

Let $k, \ell, r \in \mathbb{N}$, $p \nmid \mathrm{den}(\alpha)$ a rational prime, $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\alpha)$ above p.

i. If $\alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, then p does not divide the denominator of $\binom{k\alpha+\ell}{r}$.

ii. If $\alpha \bmod \mathfrak{p} \notin \mathbb{F}_p$ and p divides the denominator of $\binom{k\alpha+\ell}{r}$, then $p \leq r$.

- Such binomials appear in the Padé approximation with $0 \leq r \leq \sigma$.
- Explicit error terms, inequalities instead of asymptotic equivalents.

Theorem (Rothstein-Trager, 1976)

Let $a, b \in \mathbb{Q}[x]$ with b squarefree. The roots of the polynomial $\mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$ are exactly the residues of the rational function a/b.

Effectivity

Lemma

Let $k, \ell, r \in \mathbb{N}$, $p \nmid \mathrm{den}(\alpha)$ a rational prime, $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\alpha)$ above p.

i. If $\alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, then p does not divide the denominator of $\binom{k\alpha+\ell}{r}$.

ii. If $\alpha \bmod \mathfrak{p} \notin \mathbb{F}_p$ and p divides the denominator of $\binom{k\alpha+\ell}{r}$, then $p \leq r$.

- Such binomials appear in the Padé approximation with $0 \leq r \leq \sigma$.
- Explicit error terms, inequalities instead of asymptotic equivalents.

Theorem (Rothstein-Trager, 1976)

Let $a, b \in \mathbb{Q}[x]$ with b squarefree. The roots of the polynomial $\mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$ are exactly the residues of the rational function a/b.

- $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$ is called Rothstein-Trager's resultant.

Effective Honda

Corollary [Chudnovsky[2], 1985; Fürnsinn-P., 2025+]

Let $a, b \in \mathbb{Z}[x]$, $\deg(a) < d := \deg(b)$ and $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$, with leading coefficient $\Delta := \mathrm{res}_x(b, -b')$, $t := \prod_{p|\Delta} p^{1/(p-1)}$.
Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of R.
Let $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$ and $N := \lceil 10BM \rceil$.
All solutions of $y' = \frac{a}{b} y$ are algebraic *if and only if* the p-curvatures of the differential equation vanish for all primes p:

- not dividing Δ;
- at most $\sigma := (2M + 1)N + 2M$.

First algorithm and complexity

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

First algorithm and complexity

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$, Δ, t, B;
2. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := 10BM$, $\sigma := (2M+1)N + 2M$, $p \leftarrow 2$;
3. **while** $p \leq \sigma$:
   i. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   ii. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;
4. return algebraic.

First algorithm and complexity

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(d^2)$ bit operations
2. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := 10BM$, $\sigma := (2M+1)N + 2M$, $p \leftarrow 2$;
3. **while** $p \leq \sigma$: $\tilde{O}(d^2\sigma)$ bit operations [Bostan-Schost, 2009]
   i. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   ii. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;
4. return algebraic.

First algorithm and complexity

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(d^2)$ bit operations
2. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := 10BM$, $\sigma := (2M+1)N + 2M$, $p \leftarrow 2$;
3. **while** $p \leq \sigma$: $\tilde{O}(d^2\sigma)$ bit operations [Bostan-Schost, 2009]
   i. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   ii. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;
4. return algebraic.

- $t(\Delta) = O(\log \Delta)$, $\sigma = \tilde{O}(B\Delta^6)$.
- $\tilde{O}$ hides logarithmic factors.

First algorithm and complexity

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(d^2)$ bit operations
2. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := 10BM$, $\sigma := (2M+1)N + 2M$, $p \leftarrow 2$;
3. **while** $p \leq \sigma$: $\tilde{O}(d^2 B \Delta^6)$ bit operations [Bostan-Schost, 2009]
   i. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   ii. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;
4. return algebraic.

- $t(\Delta) = O(\log \Delta)$, $\sigma = \tilde{O}(B\Delta^6)$.
- $\tilde{O}$ hides logarithmic factors.

A second algorithm : polynomial factorization

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

A second algorithm : polynomial factorization

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \operatorname{res}_x(b, a - wb') \in \mathbb{Q}[w]$;
2. factor R in $\mathbb{Q}[w]$;
3. if R splits completely returns algebraic, else return transcendental.

A second algorithm : polynomial factorization

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$; $\tilde{O}(d^2)$ bit operations
2. factor R in $\mathbb{Q}[w]$; $O(?)$
3. if R splits completely returns algebraic, else return transcendental.

A second algorithm : polynomial factorization

Input $a, b \in \mathbb{Z}[x]$ with b squarefree and $\deg(a) < \deg(b)$.

Output The nature (algebraic or transcendental) of $\exp(\int \frac{a}{b})$.

1. $R := \mathrm{res}_x(b, a - wb') \in \mathbb{Q}[w]$; $\tilde{O}(d^2)$ bit operations
2. factor R in $\mathbb{Q}[w]$; $\tilde{O}(d^6)$
3. if R splits completely returns algebraic, else return transcendental.

Theorem (van Hoeij-Novocin, 2012)

Factorization of a monic univariate polynomial $R \in \mathbb{Z}[w]$ of degree d, whose coefficients are bounded by $A \in \mathbb{N}$ can be done in

$$\tilde{O}(d^6 + d^5 \log(A))$$

bit operations where the notation $\tilde{O}$ hides logarithmic factors $\log(d)$ *and* $\log(\log A)$.

Algorithmic

- How to compute p-curvatures?

Algorithmic

- How to compute p-curvatures? [Bostan-Schost, 2009], [Pagès, 2021]

Algorithmic

- How to compute p-curvatures? [Bostan-Schost, 2009], [Pagès, 2021]

a	b	σ	Output	
$2x+1$	x^2+x+1	3126	algebraic	$a = b'$
$3x-4$	$2x^2-6x+4$	344965	algebraic	
x^2+2x-1	x^3+x+1	276012	transcendental	5-curvature $\neq 0$

Effective Chebotarev

Let $R \in \mathbb{Z}[w]$, L be its splitting field with integer ring $\mathcal{O}_L$, $\ell := [L : \mathbb{Q}]$.

Effective Chebotarev

Let $R \in \mathbb{Z}[w]$, L be its splitting field with integer ring $\mathcal{O}_L$, $\ell := [L : \mathbb{Q}]$.

Fact: Let $p \in \mathbb{Z}$, the factorization pattern of R mod p in $\mathbb{F}_p[w]$ is the same as the factorization pattern of p in L.

Effective Chebotarev

Let $R \in \mathbb{Z}[w]$, L be its splitting field with integer ring $\mathcal{O}_L$, $\ell := [L : \mathbb{Q}]$.

Fact: Let $p \in \mathbb{Z}$, the factorization pattern of R mod p in $\mathbb{F}_p[w]$ is the same as the factorization pattern of p in L.

- $R = w^2 + 1$ factors in $\mathbb{F}_p[w]$ *iff* $p \equiv 1[4]$ (or $p = 2$).

Effective Chebotarev

Let $R \in \mathbb{Z}[w]$, L be its splitting field with integer ring $\mathcal{O}_L$, $\ell := [L : \mathbb{Q}]$.

Fact: Let $p \in \mathbb{Z}$, the factorization pattern of R mod p in $\mathbb{F}_p[w]$ is the same as the factorization pattern of p in L.

- $R = w^2 + 1$ factors in $\mathbb{F}_p[w]$ *iff* $p \equiv 1[4]$ (or $p = 2$).

Problem: Obtain an upper bound on the first prime $p \in \mathbb{Z}$ that does not split in L.

Effective Chebotarev

Let $R \in \mathbb{Z}[w]$, L be its splitting field with integer ring $\mathcal{O}_L$, $\ell := [L : \mathbb{Q}]$.

Fact: Let $p \in \mathbb{Z}$, the factorization pattern of R mod p in $\mathbb{F}_p[w]$ is the same as the factorization pattern of p in L.

- $R = w^2 + 1$ factors in $\mathbb{F}_p[w]$ *iff* $p \equiv 1[4]$ (or $p = 2$).

Problem: Obtain an upper bound on the first prime $p \in \mathbb{Z}$ that does not split in L.

Theorem (Vaaler-Voloch, 2000)

Let $L/\mathbb{Q}$ be a Galois extension of degree ℓ and discriminant Δ_L. Assume GRH. If $\Delta_L \geq \frac{1}{8}\exp(2(\ell-1)\max(105, 25\log\ell))$, then there exists a prime $p \in \mathbb{Z}$ such that:

- $p \nmid \Delta_L$;
- *p does not split completely in L;*
- $p \leq 26\ell^2\Delta_L^{\frac{1}{2(\ell-1)}}$.

Perspectives

$\rightsquigarrow$ $y' = uy$ with $u \in \mathbb{Q}(x)$

Perspectives

$\rightsquigarrow$ $y' = uy$ with $u \in \mathbb{Q}(x) \to$ algebraic coefficient $u \in \overline{\mathbb{Q}(x)}$ [Chudnovsky, 1985].

Perspectives

$\rightsquigarrow$ $y' = uy$ with $u \in \mathbb{Q}(x) \to$ algebraic coefficient $u \in \overline{\mathbb{Q}(x)}$ [Chudnovsky, 1985].

$\rightsquigarrow$ Effective versions of all proved cases of the p-curvature conjecture.

Perspectives

$\rightsquigarrow$ $y' = uy$ with $u \in \mathbb{Q}(x) \to$ algebraic coefficient $u \in \overline{\mathbb{Q}(x)}$ [Chudnovsky, 1985].

$\rightsquigarrow$ Effective versions of all proved cases of the p-curvature conjecture.

$\rightsquigarrow$ Link with the smallest prime that does not split.

Perspectives

$\rightsquigarrow$ $y' = uy$ with $u \in \mathbb{Q}(x) \to$ algebraic coefficient $u \in \overline{\mathbb{Q}(x)}$ [Chudnovsky, 1985].

$\rightsquigarrow$ Effective versions of all proved cases of the p-curvature conjecture.

$\rightsquigarrow$ Link with the smallest prime that does not split.

Thank you.