https://arxiv.org/abs/2510.00892

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

joint work with Florian Fürnsinn.

Lucas Pannier

Laboratoire de Mathématiques de Versailles, UVSQ
CNRS UMR-8100

November 19th 2025

Combinatorics and Arithmetic for Physics, IHES

Power series hierarchy

$$y(x) = \sum_{n\geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

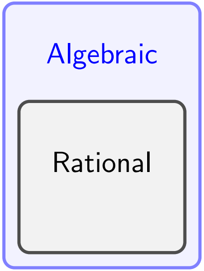
Rational

Power series hierarchy

$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

Algebraic series

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



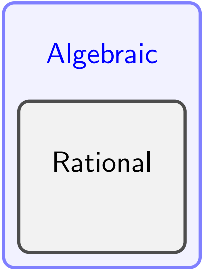
Power series hierarchy

$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

Algebraic series

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

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



Power series hierarchy

$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

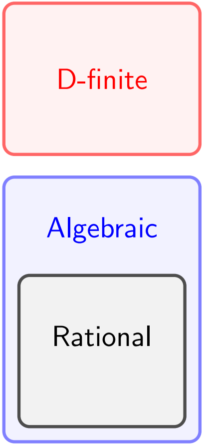
Algebraic series

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

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

D-finite series

$y(x)$ is D-finite if $\exists a_0(x), \dots, a_r(x) \in \mathbb{Z}[x]$ not all zero such that $a_r(x)y^{(r)}(x) + \dots + a_0(x)y(x) = 0$.



Power series hierarchy

$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

Algebraic series

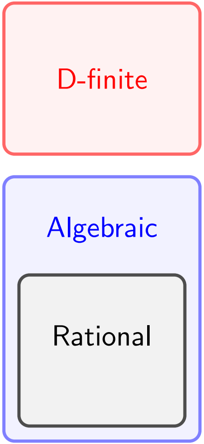
$y(x)$ is algebraic over $\mathbb{Q}(x)$ if $\exists P(x, Y) \in \mathbb{Z}[x, Y]$, $P(x, y(x)) = 0$.

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

D-finite series

$y(x)$ is D-finite if $\exists a_0(x), \dots, a_r(x) \in \mathbb{Z}[x]$ not all zero such that $a_r(x)y^{(r)}(x) + \dots + a_0(x)y(x) = 0$.

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

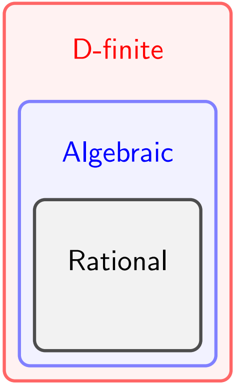


Power series hierarchy

$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[[x]]$$

Theorem (Abel, 1827)

Algebraic series are D-finite.



Power series hierarchy

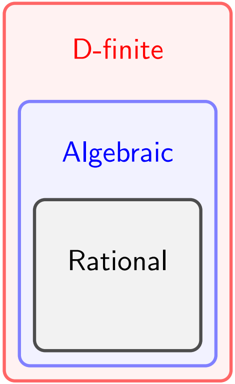
$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

Theorem (Abel, 1827)

Algebraic series are D-finite.

$\to y(x) = (1-x)^{2/5}$, $5(1-x)y' + 2y = 0$.

$\to y(x) = \exp(x^2+1)$ is not algebraic.



Power series hierarchy

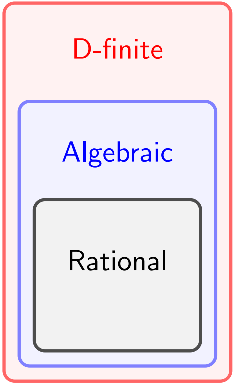
$$y(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{Q}[\![x]\!]$$

Theorem (Abel, 1827)

Algebraic series are D-finite.

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

Given a D-finite power series, decide if it is algebraic.



Deciding algebraicity

Fuchs' problem

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

Deciding algebraicity

Fuchs' problem

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

Abel's problem

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

Deciding algebraicity

Fuchs' problem

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

Abel's problem

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

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

Deciding algebraicity

Fuchs' problem

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

Abel's problem

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

[Risch, 1971], [Baldassari-Dwork, 1979], [Davenport, 1981], Risch's algorithm.
[Singer, 1980], relying on Risch's algorithm.

Differential equations in positive characteristic

$$\mathcal{L} = a_n(x)\left(\frac{d}{dx}\right)^n + \cdots + a_1(x)\frac{d}{dx} + a_0(x), \qquad a_i(x) \in \mathbb{Z}[x], \qquad \mathcal{L}_p := \mathcal{L} \bmod p.$$

Differential equations in positive characteristic

$$\mathcal{L} = a_n(x)\left(\frac{d}{dx}\right)^n + \cdots + a_1(x)\frac{d}{dx} + a_0(x), \qquad a_i(x) \in \mathbb{Z}[x], \qquad \mathcal{L}_p := \mathcal{L} \bmod p.$$

Grothendieck's conjecture

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

Differential equations in positive characteristic

$$\mathcal{L} = a_n(x)\left(\frac{d}{dx}\right)^n + \cdots + a_1(x)\frac{d}{dx} + a_0(x), \qquad a_i(x) \in \mathbb{Z}[x], \qquad \mathcal{L}_p := \mathcal{L} \bmod p.$$

Grothendieck's conjecture

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

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

Differential equations in positive characteristic

$$\mathcal{L} = a_n(x)\left(\frac{d}{dx}\right)^n + \cdots + a_1(x)\frac{d}{dx} + a_0(x), \qquad a_i(x) \in \mathbb{Z}[x], \qquad \mathcal{L}_p := \mathcal{L} \bmod p.$$

Grothendieck's conjecture

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

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

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

Differential equations in positive characteristic

$$\mathcal{L} = a_n(x)\left(\frac{d}{dx}\right)^n + \cdots + a_1(x)\frac{d}{dx} + a_0(x), \qquad a_i(x) \in \mathbb{Z}[x], \qquad \mathcal{L}_p := \mathcal{L} \bmod p.$$

Grothendieck's conjecture

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

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

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

Theorem (Cartier's Lemma)

The p-curvature of $\mathcal{L}_p$ vanishes *iff* $\mathcal{L}_p y(x)$ has a basis of algebraic solutions over $\mathbb{F}_p(x)$.

Differential equations in positive characteristic

$$\mathcal{L} = a_n(x)\left(\frac{d}{dx}\right)^n + \cdots + a_1(x)\frac{d}{dx} + a_0(x), \qquad a_i(x) \in \mathbb{Z}[x], \qquad \mathcal{L}_p := \mathcal{L} \bmod p.$$

Grothendieck's p-curvature conjecture

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

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

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

Theorem (Cartier's Lemma)

The p-curvature of $\mathcal{L}_p$ vanishes *iff* $\mathcal{L}_p y(x)$ has a basis of algebraic solutions over $\mathbb{F}_p(x)$.

Indefinite integration - Inhomogeneous case

Let $u(x) \in \mathbb{Q}(x)$, decide if $y(x) := \int u(x)dx$ is algebraic. $\rightarrow y'(x) = u(x)$

Indefinite integration - Inhomogeneous case

Let $u(x) \in \mathbb{Q}(x)$, decide if $y(x) := \int u(x)dx$ is algebraic. $\rightarrow y'(x) = u(x)$

Proposition

The power series $\int u(x)dx$ is algebraic *if and only if* all residues of $u(x)$ are zero.

Indefinite integration - Inhomogeneous case

Let $u(x) \in \mathbb{Q}(x)$, decide if $y(x) := \int u(x)dx$ is algebraic. $\rightarrow y'(x) = u(x)$

Proposition

The power series $\int u(x)dx$ is algebraic *if and only if* all residues of $u(x)$ are zero.

Theorem (Rothstein, 1976; Trager, 1976)

Let $u(x) \in \mathbb{Q}(x)$ be a rational function of the form

$$u(x) = \frac{a(x)}{b(x)} = F'(x) + \sum_{i=1}^{r} \frac{\alpha_i}{x - \beta_i},$$

with $a(x), b(x) \in \mathbb{Z}[x]$, $F(x) \in \mathbb{Q}(x)$. Then the residues α_i are precisely the roots of

$$R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Z}[w].$$

First-order differential equations

$$y'(x) = u(x)y(x) \quad \text{(Eq)}$$

First-order differential equations

$$y'(x) = u(x)y(x) \quad \textcolor{red}{\text{(Eq)}}$$

with $u(x) = F'(x) + \sum_i \dfrac{\alpha_i}{x - \beta_i} \in \overline{\mathbb{Q}}(x)$, $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$, $F(x) \in \overline{\mathbb{Q}}(x)$.

First-order differential equations

$$y'(x) = u(x)y(x) \quad \text{(Eq)}$$

with $u(x) = F'(x) + \sum_i \dfrac{\alpha_i}{x - \beta_i} \in \overline{\mathbb{Q}}(x)$, $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$, $F(x) \in \overline{\mathbb{Q}}(x)$.

A nonzero solution of (Eq) is $y(x) := \exp(\int u(x)dx) = \exp(F(x)) \cdot \prod_i (x - \beta_i)^{\alpha_i}$.

First-order differential equations

$$y'(x) = u(x)y(x) \quad \text{(Eq)}$$

with $u(x) = \sum_i \dfrac{\alpha_i}{x - \beta_i} \in \overline{\mathbb{Q}}(x)$, $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$.

A nonzero solution of (Eq) is $y(x) := \exp(\int u(x)dx) = \prod_i (x - \beta_i)^{\alpha_i}$.

First-order differential equations

$$y'(x) = u(x)y(x) \quad \text{(Eq)}$$

with $u(x) = \sum_i \frac{\alpha_i}{x - \beta_i} \in \overline{\mathbb{Q}}(x)$, $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$.

A nonzero solution of (Eq) is $y(x) := \exp(\int u(x)dx) = \prod_i (x - \beta_i)^{\alpha_i}$.

Theorem (Jacobson, 1937)

The p-curvature of (Eq) is $u^{(p-1)}(x) + u(x)^p \bmod p \in \mathbb{F}_p(x)$.

First-order differential equations

$$y'(x) = u(x)y(x) \quad \text{(Eq)}$$

with $u(x) = \sum_i \frac{\alpha_i}{x - \beta_i} \in \overline{\mathbb{Q}}(x)$, $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$.
A nonzero solution of (Eq) is $y(x) := \exp(\int u(x)dx) = \prod_i (x - \beta_i)^{\alpha_i}$.

Theorem (Jacobson, 1937)

The p-curvature of (Eq) is $u^{(p-1)}(x) + u(x)^p \bmod p \in \mathbb{F}_p(x)$.

- With $u(x)$ as above the p-curvature is

$$\sum_i \frac{\alpha_i^p - \alpha_i}{(x - \beta_i)^p} \bmod p.$$

First-order differential equations

$$y'(x) = u(x)y(x) \quad \text{(Eq)}$$

with $u(x) = \sum_i \dfrac{\alpha_i}{x - \beta_i} \in \overline{\mathbb{Q}}(x)$, $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$.

A nonzero solution of (Eq) is $y(x) := \exp(\int u(x)dx) = \prod_i (x - \beta_i)^{\alpha_i}$.

Theorem (Jacobson, 1937)

The p-curvature of (Eq) is $u^{(p-1)}(x) + u(x)^p \bmod p \in \mathbb{F}_p(x)$.

- With $u(x)$ as above the p-curvature is

$$\sum_i \frac{\alpha_i^p - \alpha_i}{(x - \beta_i)^p} \bmod p.$$

Kronecker and residues

Theorem (Rothstein, 1976; Trager, 1976)

Let $u(x) \in \mathbb{Q}(x)$ be a rational function of the form

$$u(x) = \frac{a(x)}{b(x)} = \sum_{i=1}^{r} \frac{\alpha_i}{x - \beta_i},$$

with $a(x), b(x) \in \mathbb{Z}[x]$. Then the residues α_i are precisely the roots of

$$R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Z}[w].$$

Kronecker and residues

Theorem (Rothstein, 1976; Trager, 1976)

Let $u(x) \in \mathbb{Q}(x)$ *be a rational function of the form*

$$u(x) = \frac{a(x)}{b(x)} = \sum_{i=1}^{r} \frac{\alpha_i}{x - \beta_i},$$

with $a(x), b(x) \in \mathbb{Z}[x]$. *Then the residues* α_i *are precisely the roots of*

$$R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Z}[w].$$

Theorem (Kronecker, 1880; Chebotarev, 1926)

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

Recap: proof of Honda's Theorem

$$y'(x) = u(x)y(x) \text{ (Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) := \operatorname{res}_x(b(x), a(x) - w \cdot b'(x)).$$

Recap: proof of Honda's Theorem

$$y'(x) = u(x)y(x) \text{ (Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)).$$

Proposition (Folklore; Honda, 1981)

The following are equivalent:

(1) (Eq) *has an algebraic solution.*

(2) We have $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$*.*

Recap: proof of Honda's Theorem

$$y'(x) = u(x)y(x) \text{ (Eq) } \text{ with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)).$$

Proposition (Folklore; Honda, 1981)

The following are equivalent:

(1) (Eq) *has an algebraic solution.*

(2) *We have* $\deg a(x) < \deg b(x)$, *all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$.

Proposition (Honda, 1981)

Let p *be a prime number. TFAE:*

$(1)_p$ $(\mathrm{Eq})_p$ *has an algebraic solution in* $\mathbb{F}_p[\![x]\!]$.

$(2)_p$ *We have* $\deg a(x) < \deg b(x)$, *all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{F}_p[w]$.

$(3)_p$ *We have* $u(x)^p + u^{(p-1)}(x) \bmod p = 0$.

Recap: proof of Honda's Theorem

$$y'(x) = u(x)y(x) \text{ (Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)).$$

Proposition (Folklore; Honda, 1981)

The following are equivalent:

(1) (Eq) *has an algebraic solution.*

(2) We have $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$*.*

Proposition (Honda, 1981)

Let p *be a prime number. TFAE:*

(1)$_p$ (Eq)$_p$ *has an algebraic solution in* $\mathbb{F}_p[[x]]$.

(2)$_p$ *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{F}_p[w]$*.*

(3)$_p$ *We have* $u(x)^p + u^{(p-1)}(x) \bmod p = 0$.

Kronecker's Theorem: $(2)_p$ for almost all prime numbers p implies (2).

Recap: proof of Honda's Theorem

$$y'(x) = u(x)y(x) \text{ (Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)).$$

Proposition (Folklore; Honda, 1981)

The following are equivalent:

(1) (Eq) *has an algebraic solution.*

(2) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$.

Proposition (Honda, 1981)

Let p *be a prime number. TFAE:*

(1)$_p$ (Eq)$_p$ *has an algebraic solution in* $\mathbb{F}_p[[x]]$.

(2)$_p$ *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{F}_p[w]$.

(3)$_p$ *We have* $u(x)^p + u^{(p-1)}(x) \bmod p = 0$.

Kronecker's Theorem: $(2)_p$ for almost all prime numbers p implies (2).

Can we deduce (2) from $(2)_p$ for a *finite* number of primes?

Examples

Example

The equation $y'(x) = y(x)$ has no solution in $\mathbb{F}_p[\![x]\!]$, and $\exp(x)$ is transcendental. Moreover, $1^p + 1^{(p-1)} = 1 \neq 0$ for all primes p.

Examples

Example

The equation $y'(x) = y(x)$ has no solution in $\mathbb{F}_p[\![x]\!]$, and $\exp(x)$ is transcendental. Moreover, $1^p + 1^{(p-1)} = 1 \neq 0$ for all primes p.

Example

Consider $y(x) = \exp(\arctan(x))$ satisfies $y'(x) = \frac{1}{1+x^2} \cdot y(x)$. We have

$$u(x)^p + u^{(p-1)}(x) = \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4 \\ \frac{2}{(x+1)^p} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

So $y(x)$ is not algebraic.

Effective Kronecker

Theorem (Chudnovsky^2, 1985)

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

- *not dividing Δ,*
- *at most σ.*

Effective Kronecker

Theorem (Chudnovsky[2], 1985)

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

- *not dividing Δ,*
- *at most σ.*

Theorem (Fürnsinn-P., 2025+)

In the previous theorem, one can choose $\sigma = (2M+1)N + 2M$ with $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := \lceil 6.076BM \rceil$, where $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$ and $B \in \mathbb{R}$ is an upper bound on the modulus of all complex roots of $R(w)$.

Effective Kronecker

Theorem (Chudnovsky^2, 1985)

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

- *not dividing Δ,*
- *at most σ.*

Theorem (Fürnsinn-P., 2025+)

In the previous theorem, one can choose $\sigma = (2M+1)N + 2M$ with $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := \lceil 6.076BM \rceil$, where $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$ and $B \in \mathbb{R}$ is an upper bound on the modulus of all complex roots of $R(w)$.

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

Hermite-Padé approximation

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

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

Hermite-Padé approximation

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

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

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

Hermite-Padé approximation

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

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

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

Hermite-Padé approximation

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

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

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

[Hermite, 1873] e is transcendental, [Padé, 1894].

Hermite-Padé approximation

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

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

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

[Hermite, 1873] e is transcendental, [Padé, 1894].

Idea to prove algebraicity: With $f_i(x) = f^{i-1}(x)$, $f(x)$ is algebraic *if and only if* for the optimal P_i's, the remainder $P_1(x) + P_2(x) f(x) + \cdots + P_r(x) f^{r-1}(x)$ vanishes for large n, r.

Chudnovskys' proof of Kronecker's Theorem

Proof.

Chudnovskys' proof of Kronecker's Theorem

Proof. By contradiction, assume $R(w)$ has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.

Chudnovskys' proof of Kronecker's Theorem

Proof. By contradiction, assume $R(w)$ has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Hermite-Padé approximants $P_i(z) \in L[z]$, $\deg(P_i(z)) \leq N$ to the powers of $(1-z)^\alpha$

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

Chudnovskys' proof of Kronecker's Theorem

Proof. By contradiction, assume $R(w)$ has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Hermite-Padé approximants $P_i(z) \in L[z]$, $\deg(P_i(z)) \leq N$ to the powers of $(1-z)^\alpha$

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

with $\sigma = (2M+1)N + 2M$, $g = \dfrac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$, $P_0(0) = \left(\prod_{j=1}^{2M} \binom{j\alpha+N-1}{N}\right)^{-1}$.

Chudnovskys' proof of Kronecker's Theorem

Proof. By contradiction, assume $R(w)$ has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$.
We know **explicit** Hermite-Padé approximants $P_i(z) \in L[z]$, $\deg(P_i(z)) \leq N$ to the powers of $(1-z)^\alpha$

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

$$\text{with } \sigma = (2M+1)N + 2M,\ g = \frac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*,\ P_0(0) = \left(\prod_{j=1}^{2M} \binom{j\alpha+N-1}{N}\right)^{-1}.$$

For all $\gamma \in L \setminus \{0\}$, $\underbrace{\left|\operatorname{den}(\gamma)^{[L:\mathbb{Q}]} \operatorname{Norm}_{L/\mathbb{Q}}(\gamma)\right|}_{\in \mathbb{Z}} \geq 1.$

Chudnovskys' proof of Kronecker's Theorem

Proof. By contradiction, assume $R(w)$ has a root $\alpha \notin \mathbb{Q}$. Write $L := \mathbb{Q}(\alpha)$. We know **explicit** Hermite-Padé approximants $P_i(z) \in L[z]$, $\deg(P_i(z)) \leq N$ to the powers of $(1-z)^\alpha$

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

$$\text{with } \sigma = (2M+1)N + 2M,\ g = \frac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*,\ P_0(0) = \left(\prod_{j=1}^{2M} \binom{j\alpha+N-1}{N}\right)^{-1}.$$

For all $\gamma \in L \setminus \{0\}$, $\underbrace{\left|\mathrm{den}(\gamma)^{[L:\mathbb{Q}]}\,\mathrm{Norm}_{L/\mathbb{Q}}(\gamma)\right|}_{\in\mathbb{Z}} \geq 1$.

Construct $\gamma_{M,N} \in L$, $\gamma_{M,N} \neq 0$, such that when $N >> M >> 0$,

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

Effective Honda

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

Let $a(x), b(x) \in \mathbb{Z}[x]$, $\deg(a(x)) < n := \deg(b(x))$ and
$R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$,
with leading coefficient $\Delta := \mathrm{res}_x(b(x), -b'(x))$, $t := \prod_{p|\Delta} p^{1/(p-1)}$.
Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of $R(w)$.
Let $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$ and $N := \lceil 6.076BM \rceil$.

All solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$ are algebraic *if and only if* the p-curvatures of the differential equation vanish for all primes p:

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

The smallest prime that does not split

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R(w) \in \mathbb{Z}[w]$, $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if for almost all prime number p, $R(w) \bmod p$ splits completely in $\mathbb{F}_p[w]$.

The smallest prime that does not split

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R(w) \in \mathbb{Z}[w]$, $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if for almost all prime number p, $R(w) \bmod p$ splits completely in $\mathbb{F}_p[w]$.

Proposition

Let $R(w) \in \mathbb{Z}[w]$, Δ its leading coefficient, and let $L/\mathbb{Q}$ be the splitting field of $R(w)$ and $D = \mathrm{Disc}(L)$, $n = [L : \mathbb{Q}]$.
The smallest prime $p \in \mathbb{Z}$, $p \nmid \Delta D$, such that $R(w) \bmod p$ does not split completely in $\mathbb{F}_p[w]$ is the smallest prime $p \in \mathbb{Z}$, $p \nmid \Delta D$, that does not split completely in L.

The smallest prime that does not split

Theorem (Kronecker, 1880; Chebotarev, 1926)

Let $R(w) \in \mathbb{Z}[w]$, $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if for almost all prime number p, $R(w) \bmod p$ splits completely in $\mathbb{F}_p[w]$.

Proposition

Let $R(w) \in \mathbb{Z}[w]$, Δ its leading coefficient, and let $L/\mathbb{Q}$ be the splitting field of $R(w)$ and $D = \mathrm{Disc}(L)$, $n = [L : \mathbb{Q}]$.
The smallest prime $p \in \mathbb{Z}$, $p \nmid \Delta D$, such that $R(w) \bmod p$ does not split completely in $\mathbb{F}_p[w]$ is the smallest prime $p \in \mathbb{Z}$, $p \nmid \Delta D$, that does not split completely in L.

Theorem (Effective Chebotarev, Vaaler, Voloch, 2000)

If $\exp(\max\{105, 25(\log(n))^2\}) \leq 8D^{\frac{1}{2(n-1)}}$ then there exists a prime p such that p does not split completely in L and $p \leq 26n^2 D^{\frac{1}{2(n-1)}}$.

New algorithm and complexity

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

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

New algorithm and complexity

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

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, Δ, t, B;

New algorithm and complexity

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

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \operatorname{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, Δ, t, B;
2. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta) \rceil$, $N := 10BM$, $\sigma := (2M+1)N + 2M$, $p \leftarrow 2$;

New algorithm and complexity

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

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, 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** $p \leq \sigma$:
   1. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   2. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;

New algorithm and complexity

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

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, 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.

New algorithm and complexity

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$. Coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \text{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(n^2 \log(H))$ 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** $p \leq \sigma$:
   i. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   ii. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \text{nextprime}(p)$;
4. return algebraic.

New algorithm and complexity

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$. Coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(n^2 \log(H))$ 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** $p \leq \sigma$: $\tilde{O}(n^2 \sigma)$ bit operations
   1. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   2. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;
4. return algebraic.

- Computing p-curvatures, [Bostan-Schost, 2009], $\tilde{O}$ hides logarithmic factors.

New algorithm and complexity

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$. Coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(n^2 \log(H))$ 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** $p \leq \sigma$: $\tilde{O}(n^2\sigma)$ bit operations
   1. **if** $p \nmid \Delta$, **then** compute the p-curvature;
   2. **if** p-curvature $\neq 0$, **then** return transcendental, **else** $p \leftarrow \mathrm{nextprime}(p)$;
4. return algebraic.

- Computing p-curvatures, [Bostan-Schost, 2009], $\tilde{O}$ hides logarithmic factors.
- $\sigma = \tilde{O}((Hn)^{12n})$.

New algorithm and complexity

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$. Coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, Δ, t, B; $\tilde{O}(n^2 \log(H))$ 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** $p \leq \sigma$: $\tilde{O}((Hn)^{12n})$ bit operations
   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.

- Computing p-curvatures, [Bostan-Schost, 2009], $\tilde{O}$ hides logarithmic factors.
- $\sigma = \tilde{O}((Hn)^{12n})$.

Other approach: finding rational roots

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$ and coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$; $\tilde{O}(n^2 \log(H))$ bit operations
2. Compute the rational roots of $R(w)$; $\tilde{O}(n^3 \log(H))$ bit operations
3. **If** there are n rational roots, **then** return algebraic, **else** return transcendental.

Other approach: finding rational roots

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$ and coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \operatorname{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$; $\tilde{O}(n^2 \log(H))$ bit operations
2. Compute the rational roots of $R(w)$; $\tilde{O}(n^3 \log(H))$ bit operations
3. **If** there are n rational roots, **then** return algebraic, **else** return transcendental.

- Complexity $\tilde{O}(n^3 \log(H))$ bit operations, polynomial in n and $\log(H)$.

Other approach: finding rational roots

Input $a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$ squarefree, $\deg(a(x)) < \deg(b(x)) = n$ and coefficients bounded by H.

Output The nature (algebraic or transcendental) of the solutions of $y'(x) = \frac{a(x)}{b(x)} y(x)$.

1. $R(w) := \mathrm{res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$; $\tilde{O}(n^2 \log(H))$ bit operations
2. Compute the rational roots of $R(w)$; $\tilde{O}(n^3 \log(H))$ bit operations
3. **If** there are n rational roots, **then** return algebraic, **else** return transcendental.

- Complexity $\tilde{O}(n^3 \log(H))$ bit operations, polynomial in n and $\log(H)$.
- Other approach with indicial equations, polynomial complexity in n and $\log(H)$.

What did we do that for?

$a(x)/b(x)$	σ	Output	p-curv	ist	fact	RR
$\frac{3x-4}{2x^2-6x+4}$	265	algebraic	120 ms	45 ms	<1 ms	25 ms
$\frac{2x+1}{x^2+x+1}$	1926284	algebraic	8 min 9 s	19 ms	<1 ms	24 ms
$\frac{1}{x^2-4}$	$\approx 10^{11}$	algebraic	DNF	15 ms	<1 ms	22 ms
$\frac{7x^2-3x-4}{2x^3+4x^2-6x+4}$	$\approx 6 \cdot 10^{27}$	transcendental	5 ms	38 ms	<1 ms	30 ms

What did we do that for?

$a(x)/b(x)$	σ	Output	p-curv	ist	fact	RR
$\frac{3x-4}{2x^2-6x+4}$	265	algebraic	120 ms	45 ms	<1 ms	25 ms
$\frac{2x+1}{x^2+x+1}$	1926284	algebraic	8 min 9 s	19 ms	<1 ms	24 ms
$\frac{1}{x^2-4}$	$\approx 10^{11}$	algebraic	DNF	15 ms	<1 ms	22 ms
$\frac{7x^2-3x-4}{2x^3+4x^2-6x+4}$	$\approx 6 \cdot 10^{27}$	transcendental	5 ms	38 ms	<1 ms	30 ms

Observation 1: If solutions are not algebraic, a p-curvature is nonzero for a small p.

What did we do that for?

$a(x)/b(x)$	σ	Output	p-curv	ist	fact	RR
$\frac{3x-4}{2x^2-6x+4}$	265	algebraic	120 ms	45 ms	<1 ms	25 ms
$\frac{2x+1}{x^2+x+1}$	1926284	algebraic	8 min 9 s	19 ms	<1 ms	24 ms
$\frac{1}{x^2-4}$	$\approx 10^{11}$	algebraic	DNF	15 ms	<1 ms	22 ms
$\frac{7x^2-3x-4}{2x^3+4x^2-6x+4}$	$\approx 6 \cdot 10^{27}$	transcendental	5 ms	38 ms	<1 ms	30 ms

Observation 1: If solutions are not algebraic, a p-curvature is nonzero for a small p.

Observation 2: Random inputs return transcendental.

Timings on random examples

Degree	Height	p-curv	ist	RT+RR
10	2^{10}	1 ms	12 ms	3 ms
20	2^{10}	2 ms	24 ms	10 ms
20	2^{20}	2 ms	25 ms	21 ms
160	2^{10}	0.4 s	1.8 s	2.4 s
160	2^{20}	0.4 s	1.9 s	4.0 s

Table: Average computation time of algorithms deciding transcendence of solutions on random rational function inputs of prescribed degree and height.

Timings on random examples

Degree	Height	p-curv	ist	RT+RR
10	2^{10}	1 ms	12 ms	3 ms
20	2^{10}	2 ms	24 ms	10 ms
20	2^{20}	2 ms	25 ms	21 ms
160	2^{10}	0.4 s	1.8 s	2.4 s
160	2^{20}	0.4 s	1.9 s	4.0 s

Table: Average computation time of algorithms deciding transcendence of solutions on random rational function inputs of prescribed degree and height.

Takeaway

Proving transcendence is efficient.

Perspectives

Make all proved cases of Grothendieck's p-curvature conjecture effective.

Perspectives

Make all proved cases of Grothendieck's p-curvature conjecture effective.

Thank you for your attention.