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

October 6th 2025
EThéN school in number theory.

UFR des Sciences
CAMPUS DE VERSAILLES

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

Algebraic

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

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

Algebraic

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

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

D-finite series

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

D-finite

Algebraic

Rational

Power series hierarchy

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

Algebraic series

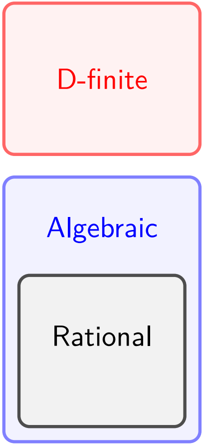
$y(x)$ is algebraic over $\mathbb{Q}(x)$ if $\exists P(x, Y) \in \mathbb{Z}[x, Y]$, $P(x, y(x)) = 0$.

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

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

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

Algebraic series

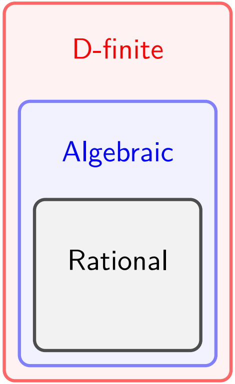
$y(x)$ is algebraic over $\mathbb{Q}(x)$ if $\exists P(x, Y) \in \mathbb{Z}[x, Y]$, $P(x, y(x)) = 0$.

D-finite series

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

Theorem (Abel, 1827)

Algebraic series are D-finite.



Deciding algebraicity

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

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

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.

Special case of Grothendieck's conjecture, [Chudnovsky^2, 1985]

All solutions of $y'(x) = u(x)y(x)$ are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all prime numbers p, all solutions of $y'(x) = (u(x) \bmod p)y(x)$ are algebraic over $\mathbb{F}_p(x)$.

The p-curvature conjecture

$$\begin{cases} y'(x) &= u(x)y(x) \qquad \color{red}{(\mathrm{Eq})} \\ y'(x) &= (u(x) \bmod p)y(x) \qquad \color{red}{(\mathrm{Eq})_p} \end{cases} \quad \text{with } u(x) = \frac{a(x)}{b(x)} \in \mathbb{Q}(x).$$

The p-curvature conjecture

$$\begin{cases} y'(x) &= u(x)y(x) \qquad \text{(Eq)} \\ y'(x) &= (u(x) \bmod p)y(x) \qquad \text{(Eq)}_p \end{cases} \quad \text{with } u(x) = \frac{a(x)}{b(x)} \in \mathbb{Q}(x).$$

To (Eq)$_p$, attach the p-curvature $u^{(p-1)}(x) + u(x)^p \bmod p \in \mathbb{F}_p(x)$ [Jacobson, 1937].

The p-curvature conjecture

$$\begin{cases} y'(x) = u(x)y(x) & \text{(Eq)} \\ y'(x) = (u(x) \bmod p)y(x) & \text{(Eq)}_p \end{cases} \quad \text{with } u(x) = \frac{a(x)}{b(x)} \in \mathbb{Q}(x).$$

To $(\mathrm{Eq})_p$, attach the p-curvature $u^{(p-1)}(x) + u(x)^p \bmod p \in \mathbb{F}_p(x)$ [Jacobson, 1937].

Special case of Cartier's Lemma

The p-curvature is zero if and only if $(\mathrm{Eq})_p$ has a basis of algebraic solutions.

The p-curvature conjecture

$$\begin{cases} y'(x) &= u(x)y(x) & \text{(Eq)} \\ y'(x) &= (u(x) \bmod p)y(x) & \text{(Eq)}_p \end{cases} \quad \text{with } u(x) = \frac{a(x)}{b(x)} \in \mathbb{Q}(x).$$

To $(\mathrm{Eq})_p$, attach the p-curvature $u^{(p-1)}(x) + u(x)^p \bmod p \in \mathbb{F}_p(x)$ [Jacobson, 1937].

Special case of Cartier's Lemma

The p-curvature is zero if and only if $(\mathrm{Eq})_p$ has a basis of algebraic solutions.

Special case of Grothendieck's p-curvature conjecture, [Chudnovsky^2, 1985; Honda, 1974]

All solutions of (Eq) are algebraic over $\mathbb{Q}(x)$ *if and only if* for almost all prime numbers p, the p-curvature of $(\mathrm{Eq})_p$ vanishes.

From p-curvatures to polynomials

Theorem (Honda, 1974)

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

From p-curvatures to polynomials

Theorem (Honda, 1974)

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

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* $\mathbb{Q}$*, and hence it is linear.*

From p-curvatures to polynomials

Theorem (Honda, 1974)

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

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* $\mathbb{Q}$, *and hence it is linear.*

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

Towards effectivity

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

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

Proof of Honda's Theorem

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

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* $\mathbb{Q}[w]$*.*

Proof of Honda's Theorem

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

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

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:*

$(1)_p$ $(\mathrm{Eq})_p$ *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* $u(x)^p + u^{(p-1)}(x) \bmod p = 0$*.*

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

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:*

$(1)_p$ $(\mathrm{Eq})_p$ *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* $u(x)^p + u^{(p-1)}(x) \bmod p = 0$.

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?

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 (Chudnovsky², 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 $t(\Delta) := \prod_{p \mid \Delta} p^{1/(p-1)}$ 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 $f_1(x), \ldots, f_r(x) \in \mathbb{Q}[\![x]\!]$ 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, 1873] e is transcendental, [Padé, 1894], [Mahler, 1931].

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], [Mahler, 1931].

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

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

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 $(1-z)^\alpha$

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

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

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

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

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

Effective Honda

Corollary [Chudnovsky², 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 $N := \lceil 6.076 BM \rceil$.

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 $\sigma := (2M+1)N + 2M$.

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;
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** $p \leftarrow \mathrm{nextprime}(p)$;
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
   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]

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
   i. **if** $p \not| \Delta$, **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]
- $\sigma = \tilde{O}((Hn)^{12n})$.

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** $p \not| \Delta$, **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]
- $\sigma = \tilde{O}((Hn)^{12n})$.

Comparison

Alternative approaches: Given $a(x), b(x) \in \mathbb{Z}[x]$ of degree at most n and coefficients at most H, one can either compute $R(w) = \mathrm{res}_x(b(x), a(x) - w \cdot b'(x))$ and find its rational roots, or compute the indicial equations to decide transcendence.

Comparison

Alternative approaches: Given $a(x), b(x) \in \mathbb{Z}[x]$ of degree at most n and coefficients at most H, one can either compute $R(w) = \mathrm{res}_x(b(x), a(x) - w \cdot b'(x))$ and find its rational roots, or compute the indicial equations to decide transcendence.

- Polynomial in n and $\log(H)$.

Comparison

Alternative approaches: Given $a(x), b(x) \in \mathbb{Z}[x]$ of degree at most n and coefficients at most H, one can either compute $R(w) = \mathrm{res}_x(b(x), a(x) - w \cdot b'(x))$ and find its rational roots, or compute the indicial equations to decide transcendence.

- Polynomial in n and $\log(H)$.
- For $u(x) = \frac{2x+1}{x^2+x+1}$, $\sigma = 1926284$.

Comparison

Alternative approaches: Given $a(x), b(x) \in \mathbb{Z}[x]$ of degree at most n and coefficients at most H, one can either compute $R(w) = \mathrm{res}_x(b(x), a(x) - w \cdot b'(x))$ and find its rational roots, or compute the indicial equations to decide transcendence.

- Polynomial in n and $\log(H)$.
- For $u(x) = \frac{2x+1}{x^2+x+1}$, $\sigma = 1926284$. Runtime: ≈ 8 min for p-curvatures vs < 1 ms.

Comparison

Alternative approaches: Given $a(x), b(x) \in \mathbb{Z}[x]$ of degree at most n and coefficients at most H, one can either compute $R(w) = \mathrm{res}_x(b(x), a(x) - w \cdot b'(x))$ and find its rational roots, or compute the indicial equations to decide transcendence.

- Polynomial in n and $\log(H)$.
- For $u(x) = \frac{2x+1}{x^2+x+1}$, $\sigma = 1926284$. Runtime: ≈ 8 min for p-curvatures vs < 1 ms.

$\rightarrow$ Try on random examples that will return transcendental.

Comparison

- Polynomial in n and $\log(H)$.
- For $u(x) = \frac{2x+1}{x^2+x+1}$, $\sigma = 1926284$. Runtime: ≈ 8 min for p-curvatures vs < 1 ms.

$\rightarrow$ Try on random examples that will return transcendental.

Degree	Height	p-curv	IE	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.

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.