BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 61, Number 4, October 2024, Pages 609–658
https://doi.org/10.1090/bull/1835
Article electronically published on August 15, 2024

ALGEBRAIC SOLUTIONS OF LINEAR DIFFERENTIAL EQUATIONS: AN ARITHMETIC APPROACH

ALIN BOSTAN, XAVIER CARUSO, AND JULIEN ROQUES

ABSTRACT. Given a linear differential equation with coefficients in $\mathbb{Q}(x)$, an important question is to know whether its full space of solutions consists of algebraic functions, or at least if one of its specific solutions is algebraic. After presenting motivating examples coming from various branches of mathematics, we advertise in an elementary way a beautiful local-global arithmetic approach to these questions, initiated by Grothendieck in the late sixties. This approach has deep ramifications and leads to the still unsolved Grothendieck–Katz p-curvature conjecture.

CONTENTS

1. CONTEXT, MOTIVATION, AND BASIC EXAMPLES

In this text we consider linear differential equations (LDEs) of order r

$$a_r(x)y^{(r)}(x) + a_{r-1}(x)y^{(r-1)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0, \tag{1}$$

where the a_i are known rational functions in $\mathbb{Q}(x)$, with a_r not identically zero and $y(x)$ is an unknown "function". In many applications, the desired solution $y(x)$ is a formal power series with coefficients in $\mathbb{Q}$. Therefore, in what follows, when we write "function" we actually mean an element of $\mathbb{Q}[[x]]$ unless otherwise specified. We will say that a function $y \in \mathbb{Q}[[x]]$ is *differentially finite* (in short, *D-finite*) if it satisfies a linear differential equation like (1).

2020 *Mathematics Subject Classification.* Primary 11-02; Secondary 12H05, 33C20, 12H25, 34A30, 34M15, 05A15, 68W30.

This work was partially supported by the French grants CLap-CLap (ANR-18-CE40-0026) and DeRerumNatura (ANR-19-CE40-0018), and by the French–Austrian project EAGLES (ANR-22-CE91-0007 & FWF I6130-N). The authors were supported by the Austrian Science Fund FWF, project P-34765.

©2024 by the authors

A function $y \in \mathbb{Q}[[x]]$ is called *algebraic* if it is algebraic over $\mathbb{Q}(x)$, that is, if $y(x)$ satisfies a polynomial equation of the form $P(x, y(x)) = 0$, for some $P \in \mathbb{Q}[x,y] \setminus \{0\}$. Otherwise, $y(x)$ is called *transcendental*. The simplest algebraic functions are polynomials in $\mathbb{Q}[x]$, closely followed by rational power series: these are rational functions in $\mathbb{Q}(x)$ that have no pole at $x = 0$ and therefore admit a Taylor expansion around the origin. A little more general are Nth roots of rational power series, such as $y(x) = 1/\sqrt[N]{1-x}$. In all these three cases, $y(x)$ is clearly D-finite and satisfies a linear differential equation of order $r = 1$.

Many other examples of interesting functions that might or might not be solutions of linear differential equations arise from combinatorics. A basic example is given by the Catalan numbers.

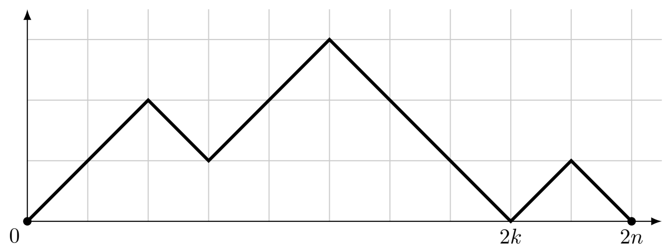

FIGURE 1. A Dyck path

Example 1.1 (Catalan numbers)**.** By definition, a *Dyck path* is a path drawn in the quarter plane $\mathbb{N}^2$ that starts at $(0,0)$, consists of steps $\nearrow$ (directed by the vector $(1,1)$) or $\searrow$ (directed by the vector $(1,-1)$) and finally ends on the x-axis (see Figure 1).

Let C_n be the number of Dyck paths ending at $(2n, 0)$; we say that such paths have length n. For instance, $C_1 = 1$ since there is a single Dyck path ending at $(2,0)$, namely $\nearrow\!-\!\searrow$, while $C_2 = 2$ since there are two Dyck paths ending at $(4,0)$, namely $\nearrow\!-\!\nearrow\!-\!\searrow\!-\!\searrow$ and $\nearrow\!-\!\searrow\!-\!\nearrow\!-\!\searrow$. We use the convention that $C_0 = 1$. We notice that any Dyck path of length $n+1$ can be written uniquely as the concatenation of

(1) a step $\nearrow$,
(2) a Dyck path of length $k-1$ (translated by $(1,1)$),
(3) a step $\searrow$ and
(4) a Dyck path of length $n-k$.

It follows that the sequence $(C_n)_{n\geq 0}$ satisfies the following nonlinear recurrence relation:

$$C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k}, \qquad \text{for all } n \geq 1.$$

If $y(x)$ denotes the generating function of the C_n, i.e., $y(x) = \sum_{n=0}^{\infty} C_n x^n$, the previous relation translates to the algebraic identity

$$y(x) = 1 + x \cdot y(x)^2 \tag{2}$$

(the summand 1 comes from the fact that $C_0 = 1$). Therefore, $y(x)$ is algebraic and one can even solve equation (2) and get the closed formula $y(x) = \frac{1-\sqrt{1-4x}}{2x}$. It is worth noting that, starting from the algebraic relation (2), one can also derive a linear differential equation satisfied by $y(x)$. Indeed, differentiating (2), one gets $y'(x) = y(x)^2 + 2x\,y(x)\,y'(x)$. Therefore,

$$y'(x) = \frac{y(x)^2}{1 - 2x\,y(x)}.$$

The right-hand side in the latter expression can be further simplified using equation (2) again. Notice that

$$\big(1 - 2x\,y(x)\big)^2 = 1 - 4x\,y(x) + 4x^2\,y(x)^2 = 1 - 4x$$

and, consequently,

$$\begin{aligned}\frac{y(x)^2}{1 - 2x\,y(x)} &= \frac{y(x)^2 \cdot \big(1 - 2x\,y(x)\big)}{1 - 4x}\\ &= \frac{\big(y(x) - 1\big)\big(1 - 2x\,y(x)\big)}{x(1 - 4x)}\\ &= \frac{2x\,y(x) - y(x) + 1}{x(1 - 4x)}\end{aligned}$$

after replacing two times $y(x)^2$ by $\frac{y(x)-1}{x}$.

Finally, one obtains the inhomogeneous differential equation

$$(4x^2 - x)y'(x) + (2x - 1)y(x) + 1 = 0.$$

From this, we can derive new interesting information about the sequence $(C_n)_{n\geq 0}$. For instance, it easily implies the simpler recurrence relation $C_n = \frac{4n-2}{n+1} \cdot C_{n-1}$ for all $n \geq 1$, from which we further derive the closed formula $C_n = \frac{1}{n+1}\binom{2n}{n}$. Using Stirling's formula, we also deduce the asymptotic estimate $C_n \sim 4^n/\sqrt{\pi n^3}$.

The previous example shows that being able to write down an equation (either algebraic or differential) for a generating series can help a lot in studying its coefficients. Of course, obtaining explicit closed formulas (as we did for the Catalan numbers) will not be possible in general; however, meaningful information (such as the asymptotic growth of the coefficients) can often be extracted from the equation. Besides, in many cases it turns out that the algebraicity of a generating series is the mirror of a (sometimes hidden) "algebraic" structure on the combinatorial side, which often takes the form of a recursive tree structure: in Example 1.1, for instance, a Dyck path can be decomposed as a concatenation of smaller Dyck paths, which themselves can be decomposed similarly, etc. We refer to [25] for a much more detailed discussion on this topic (including many more examples).

In Example 1.1, we transformed an algebraic equation into a differential equation. It is actually a general fact and an old result, already known by Abel, that *any algebraic function is D-finite*. Precisely if $y(x)$ satisfies an algebraic equation $P(x, y(x)) = 0$ with P of degree n in y, then $y(x)$ also satisfies a differential equation like (1) of order r bounded from above by n. This follows easily from the following reasoning. By differentiating $P(x, y(x)) = 0$ with respect to x and by using the chain rule, we obtain the equality

$$P_x(x, y(x)) + y'(x)P_y(x, y(x)) = 0.$$

Here and in what follows, we denote by P_x the derivative $\partial P/\partial x$ of P with respect to x. Therefore, if P is assumed to be a polynomial of minimal degree in y satisfied by $y(x)$, then $P_y(x, y(x))$ is a nonzero function in $\mathbb{Q}[[x]]$, and hence

$y'(x) = -P_x(x, y(x))/P_y(x, y(x))$ is a rational function in $y(x)$. By using the equation $P(x, y(x)) = 0$ again, it is easy to see that any rational function in $y(x)$ can be re-written as a polynomial of degree at most $n-1$ in $y(x)$. In other terms, the derivative $y'(x)$ lives in the $\mathbb{Q}(x)$-vector space generated by $1, y(x), \ldots, y(x)^{n-1}$. Similarly, the same holds for all derivatives $y(x), y'(x), y''(x), \ldots, y^{(n)}(x)$, and hence these elements must satisfy a nontrivial linear relation over $\mathbb{Q}(x)$; any such relation yields a linear differential equation (1) of order at most n. Observe that the same reasoning also proves the existence of an inhomogeneous linear differential equation of order at most $n-1$ for $y(x)$.

A naive though very natural question is whether the converse of Abel's result holds: *is every D-finite function algebraic?* The answer is negative, already for differential equations of order $r = 1$, as the following example shows.

Example 1.2. The function $\exp(x) := \sum_{n \geq 0} x^n/n!$, solution of $y' = y$, is transcendental. Here is a purely algebraic proof. Let us assume by contradiction that $\exp(x)$ satisfies a polynomial equation, of minimal degree $d \geq 1$, of the form $e^{dx} + \sum_{k=0}^{d-1} r_k(x) e^{kx} = 0$ for some rational functions $r_k(x) \in \mathbb{Q}(x)$. By differentiating this equality with respect to x and using $\exp'(x) = \exp(x)$, we get a new degree-d equation $de^{dx} + \sum_{k=0}^{d-1} (r_k'(x) + k r_k(x)) e^{kx} = 0$, which, by minimality, is equal the former up to a factor d. In other words, $r_k'(x) + k r_k(x) = d r_k(x)$ for all $k < d$. In particular, $r_0'(x) = d r_0(x)$, which implies that $r_0 = 0$. (Indeed, if $r_0(x) = A/B$ for two coprime polynomials $A, B \in \mathbb{Q}[x]$ with $A'B - AB' = dAB$, then B divides AB', hence B divides B' and $B' = 0$. Thus $A' = dA$, which implies $A = 0$ and $r_0(x) = 0$.) The nullity of r_0 now implies that $\exp(x)$ satisfies a polynomial equation of degree $d-1$, which contradicts the minimality of d.

The reader could object that in Example 1.2 we were probably lucky, because the differential equation of $\exp(x)$ is so simple, being of order 1 with constant coefficients. Indeed, in the particular case of the exponential function, there are many other ad hoc transcendence proofs, based on various branches of mathematics. For instance, a direct analytic argument is that, viewed as a complex analytic function, any nonpolynomial algebraic function needs to have a finite (and positive) radius of convergence, while $\exp(x)$ is entire (that is, analytic in the whole complex plane). Another proof is that $\exp(x)$ cannot satisfy a nontrivial algebraic equation, since by otherwise specializing that equation at $x = 1$ we would find that the number $e = \exp(1)$ is an algebraic number, a statement known be to false since Hermite (1873). One could qualify this last proof as "cheating", since it is intuitively clear that proving transcendence of functions should be easier than proving transcendence of numbers.

A systematic and very useful analytic way to establish functional transcendence is *Flajolet's criterion* [46, Criterion D] (see also [47, Theorem VII.8] and [67, §2.3]). It is a consequence of the classical Newton–Puiseux theorem on fractional (Puiseux) series expansion of algebraic functions and on Darboux's transfer results from the local behavior of $f(x) = \sum_{n \geq 0} a_n x^n$ around its singularities to the asymptotic behavior of its coefficient sequence $(a_n)_{n \geq 0}$. Before stating it, we recall the definition of the gamma function

$$\Gamma(s) := \int_0^{+\infty} t^{s-1} e^t dt,$$

where the variable s is a complex number with positive real part. The gamma function interpolates the factorial in the sense that $\Gamma(n) = (n-1)!$ for any positive integer n.

Proposition 1.3 ([46, Theorems A and D]). *Let $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]] \setminus \mathbb{Q}[x]$ be an algebraic nonpolynomial function. Then $f(x)$ has a finite number of singularities, a finite nonzero radius of convergence, and its coefficient sequence $(a_n)_{n\geq 0}$ is such that*

$$a_n = \frac{\beta^n n^r}{\Gamma(r+1)} \sum_{i=0}^{m} C_i \omega_i^n + O(\beta^n n^q), \tag{3}$$

where $m \in \mathbb{Z}_{\geq 0}$, $r \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$, $q < r$, $\beta \in \overline{\mathbb{Q}}_{>0}$, and $C_i, \omega_i \in \overline{\mathbb{Q}} \setminus \{0\}$ with $|\omega_i| = 1$.

The most useful form of the criterion is Corollary 1.4.

Corollary 1.4 ("Flajolet's criterion"). *If $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]$ and $a_n \sim \gamma\, \beta^n\, n^r$ with either $r \notin \mathbb{Q} \setminus \mathbb{Z}_{<0}$, or $\beta \notin \overline{\mathbb{Q}}_{>0}$, or $\gamma \cdot \Gamma(r+1) \notin \overline{\mathbb{Q}}$, then $f(x)$ is transcendental.*

As an example of application, Proposition 1.3 immediately implies that $\exp(x) = \sum_{n\geq 0} x^n/n!$ is transcendental, since the sequence $1/n!$ is not of the form (3) (or, since the radius of convergence of $\exp(x)$ is infinite).

At this point, we can ask ourselves: *is there a purely arithmetic proof of the transcendence of* $\exp(x)$*?* This question can be seen as the starting point of the present article, whose main aim is precisely to advertise a very beautiful number-theoretic approach to algebraicity of solutions of linear differential equations. More generally, we can raise the following question.

Question 1.5. Is there any number-theoretic way to recognize whether the differential equation (1) admits only algebraic solutions in its solution space?

Nicely enough, the answer to this question is positive, for two distinct but related reasons. Let us first explain them a bit in the case of the exponential function $\exp(x) = \sum_{k\geq 0} x^k/k!$. The first arithmetic proof of the transcendence of $\exp(x)$ is based on the following result, which, in rough terms, asserts that the coefficients of algebraic functions are "almost integral".

Proposition 1.6 ("Eisenstein's criterion" (1852)). *If the function*

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

is algebraic, then there exists $N \in \mathbb{N} \setminus \{0\}$ such that $y(Nx) - y(0) \in \mathbb{Z}[[x]]$. In particular, only a finite number of prime numbers can divide the denominators of the coefficients a_k.

Since in the factorial sequence $(k!)_{k\geq 0}$, obviously, all prime numbers appear as divisors, and Proposition 1.6 immediately implies that $\exp(x)$ is transcendental.

To formulate the second arithmetic proof of the transcendence of $\exp(x)$, we will need a little bit of additional vocabulary. The differential equation (1) can be rewritten in the compact form $\mathscr{L}(y) = 0$, where $\mathscr{L}$ is the linear differential operator

$$\mathscr{L} = a_r(x)\cdot\partial_x^r + a_{r-1}(x)\cdot\partial_x^{r-1} + \cdots + a_1(x)\cdot\partial_x + a_0(x). \tag{4}$$

We denote by $\mathbb{Q}(x)\langle\partial_x\rangle$ the set of such linear differential operators. For convenience, we also allow the trivial operator, in which all coefficients $a_i(x)$ are zero. The elements of $\mathbb{Q}(x)\langle\partial_x\rangle$ act on functions in x by letting the variable ∂_x act through the differentiation $\frac{d}{dx}$. The set $\mathbb{Q}(x)\langle\partial_x\rangle$ is then endowed with a structure of *noncommutative* ring where the addition is the usual one but the multiplication is twisted according to the following rule, reminiscent of Leibniz's differentiation rule:

$$\forall r \in \mathbb{Q}(x), \quad \partial_x r(x) = r(x)\partial_x + r'(x).$$

Although the ring $\mathbb{Q}(x)\langle\partial_x\rangle$ is noncommutative, it shares many properties with the classical commutative ring of polynomials $\mathbb{Q}(x)[y]$. First, one has a well-defined notion of degree: the *degree* of the nonzero operator $\mathscr{L}$ in (4) is the order r of the corresponding differential equation (1), that is, the largest integer r such that $a_r(x) \neq 0$. We will denote it by $\operatorname{ord}(\mathscr{L})$ in what follows. Second, the ring $\mathbb{Q}(x)\langle\partial_x\rangle$ admits an Euclidean division.

Proposition 1.7. *The ring $\mathbb{Q}(x)\langle\partial_x\rangle$ is right Euclidean, i.e., for all $A, B \in \mathbb{Q}(x)\langle\partial_x\rangle$ with $B \neq 0$, there exist Q and R in $\mathbb{Q}(x)\langle\partial_x\rangle$ such that $A = QB + R$ and $\operatorname{ord} R < \operatorname{ord} B$. Moreover, the pair (Q, R) is unique with these properties.*

Using these notions, we can now formulate a very basic but important arithmetic result.

Proposition 1.8. *If all solutions of* (1) *are algebraic functions, then for all but a finite number of prime numbers p, the remainder of the right Euclidean division of ∂_x^p by $\mathscr{L}$ has all its coefficients divisible by p.*

Proof. By Eisenstein's criterion (Proposition 1.6), there exists a basis of algebraic solutions $y_1, \dots, y_r$ of $\mathscr{L}$ and an integer $N \in \mathbb{N}\backslash\{0\}$ such that $y_i(x)$ is in $\mathbb{Q}+x\mathbb{Z}[[\frac{x}{N}]]$ for all i. This implies that for all but a finite number of prime numbers p (namely, the ones dividing N and the denominators of $y_i(0)$) the power series $y_i^{(p)}(x)$ are in $p\mathbb{Z}[[x]]$, i.e., zero modulo p. Thus, writing $\partial_x^p = Q\mathscr{L} + R$ with R of order at most $r-1$, we have $R(y_i) = 0 \bmod p$ for all i. Writing $R = c_0(x) + \cdots + c_{r-1}(x)\partial_x^{r-1}$, we deduce that the vector $(c_0, \dots, c_{r-1})$ times the Wronskian matrix of the y_i is zero modulo p. Since the Wronskian matrix is invertible (because the y_i form a basis of solutions of $\mathscr{L}$), it is also invertible modulo p for all but a finite number of prime numbers p, and thus the c_i are all 0 modulo p for any such prime p. □

Example 1.9. The generating function of the Catalan numbers $y(x) = \sum_{k\geq 0} C_k x^k$ satisfies the differential equation $(4x^2 - x)y''(x) + (10x - 2)y'(x) + 2y(x) = 0$, which is easily deduced, either from the inhomogeneous differential equation of order 1 in Example 1.1, or directly from the recurrence $(k+2)C_{k+1} - (4k+2)C_k = 0$. The associated differential operator is $\mathscr{L} = \left(4x^2 - x\right)\partial_x^2 + (10x - 2)\,\partial_x + 2$, and the remainders of the right Euclidean divisions of ∂_x^p by $\mathscr{L}$ for $p \in \{2,3,5\}$ are

$$\partial_x^2 \bmod \mathscr{L} = -\frac{2\,(5x-1)}{x\,(4x-1)}\partial_x - \frac{2}{x\,(4x-1)},$$

$$\partial_x^3 \bmod \mathscr{L} = \frac{6\left(22x^2-9x+1\right)}{x^2\,(4x-1)^2}\partial_x + \frac{6(6x-1)}{x^2\,(4x-1)^2},$$

$$\partial_x^5 \bmod \mathscr{L} = \frac{120\left(386x^4-325x^3+110x^2-17x+1\right)}{x^4\,(4x-1)^4}\partial_x + \frac{120(130x^3-69x^2+14x-1)}{x^4\,(4x-1)^4}.$$

Note that we have $\partial_x^p \bmod \mathscr{L} = 0$ modulo p in the three cases.

Proposition 1.8 will be discussed in more detail in §3.2. For now, let us simply observe how it implies the transcendence of $\exp(x)$. In this case $\mathscr{L} = \partial_x - 1$. Hence $\partial_x^p \bmod \mathscr{L}$ is equal to 1 for all p. Indeed, in this case, $\mathscr{L}$ and ∂_x commute, hence the computation of the remainder is the same as the computation in $\mathbb{Q}[x]$ of the remainder of x^p by $x-1$, that is, the evaluation of x^p at $x=1$.

Example 1.10. Let us consider the logarithmic function $y(x) = \log(1-x)$. Of course, since $\log(\exp(x)) = x$ and $\exp(\log(1-x)) = 1-x$, the transcendence of the logarithm function follows from that of the exponential function. However, the two arithmetic criteria can be used directly. First, Eisenstein's criterion (Proposition 1.6) can be applied since $\log(1-x) = -\sum_{k\geq 1} x^k/k$. Second, we have that a full basis of solutions of $\mathscr{L} = (1-x)\partial_x^2 - \partial_x$ is $\{1, \log(1-x)\}$, and it holds by induction that

$$\partial_x^n \bmod \mathscr{L} = \frac{(n-1)!}{(1-x)^{n-1}}\partial_x \qquad \text{for all } n \geq 1.$$

Therefore, Wilson's theorem implies that modulo any prime number p, the remainder $\partial_x^p \bmod \mathscr{L}$ is equal to $-\frac{1}{(1-x)^{p-1}}\partial_x$, hence it is never 0. Then, Proposition 1.8 implies that $\log(1-x)$ is transcendental.

A natural question is whether the converses of Proposition 1.6 and Proposition 1.8 have any chance to hold true. Concerning Proposition 1.6, it is not difficult to exhibit a transcendental D-finite power series with integer coefficients, showing that its converse is false. A natural example that comes to mind is $y(x) = \sum_{k\geq 0} k!x^k$, which satisfies $x^2y''(x) + (3x-1)y'(x) + y(x) = 0$. One can prove that $y(x)$ is not algebraic in various ways. One of them is again analytic, by observing that $y(x)$ has radius of convergence 0 and by applying Proposition 1.3. A purely algebraic proof also exists, but it is less immediate: it relies on the combination of the following facts: (i) $y(x)$ does not satisfy any first-order differential equation, hence the second-order differential equation above is the minimal-order LDE satisfied by $y(x)$; (ii) this second-order differential equation admits in its solution space the transcendental solution $e^{-1/x}/x$; (iii) if $y(x)$ were algebraic, then its minimal-order LDE would have only algebraic solutions [80, Proposition 2.5].

However, the reader may object that this counterexample is "degenerate" since the coefficient sequence $(k!)_{k\geq 0}$ grows too fast, which is not compatible with the growth of the coefficient sequence of an algebraic function. A better converse of Proposition 1.6 would be: *is there any example of a D-finite but transcendental* *function $y \in \mathbb{Z}[[x]]$, whose coefficient sequence grows at most geometrically?* The answer is, again, positive.

Example 1.11. Again, let (C_k) be the sequence of Catalan numbers, and consider the function $y(x) = \sum_{k\geq 0} C_k \binom{2k}{k} x^k$. One easily checks that it is D-finite and it satisfies the second-order equation $x(16x-1)y''(x) + 2(16x-1)y'(x) + 4y(x) = 0$. From there, it follows that $y(x)$ is the Gauss hypergeometric function ${}_2F_1([1/2, 1/2], [2]; 16x)$ and classical results (that we shall recall in Section 2.1.3) imply that $y(x)$ is transcendental.

Thus, even the stronger converse of Proposition 1.6 appears to be false. One may wonder if there is any way to further reinforce the conclusion of Proposition 1.6, such that its converse becomes true. As of today, this is still an open problem, although there exist conjectural statements in this spirit. One of them is the following.

Conjecture 1.12 (Christol–André conjecture)**.** *Assume that $y(x) = \sum_{k\geq 0} a_k x^k \in \mathbb{Q}[[x]]$ is D-finite. Let $\mathscr{L}$ be the minimal-order monic linear differential equation satisfied by $y(x)$. We assume that:*

(1) *the sequence $(a_k)_{k\geq 0}$ has at most geometric growth;*
(2) *there exists $N \in \mathbb{N}$ such that $y(Nx) - y(0) \in \mathbb{Z}[[x]]$;*
(3) *the point $x = 0$ is not a pole of any of the coefficients of $\mathscr{L}$.*

Then, $y(x)$ is algebraic over $\mathbb{Q}(x)$.

If r denotes the order of $\mathscr{L}$, it is also conjectured that condition (3) can be replaced by

(3b) *$\mathscr{L}$ has r linearly independent solutions in $\mathbb{C}((x^{1/D}))$ for some positive integer D.*

Now, what about the converse of Proposition 1.8? It turns out that this converse is one of the simplest formulations of what is usually called the *Grothendieck conjecture*. This conjecture was formulated in the late 1960s and it has a rich history. It was proved for some important classes of differential equations (1), which will be discussed in Section 3.

Conjecture 1.13 (Grothendieck's conjecture, version 1)**.** *Let $\mathscr{L} \in \mathbb{Q}(x)\langle\partial_x\rangle$ be the differential operator attached to* (1)*. If for all but a finite number of prime numbers p, the remainder of the right Euclidean division of ∂_x^p by $\mathscr{L}$ has all its coefficients divisible by p, then all solutions of* (1) *are algebraic functions over $\mathbb{Q}(x)$.*

Example 1.14. Consider the operator

$$\mathscr{L} = 2x\,(x-1)\,\partial_x^2 + (4x-1)\,\partial_x + 1.$$

Then, for any prime number $p > 2$, the reduction modulo p of $\partial_x^p \bmod \mathscr{L}$ is equal to 0 if $p \equiv 1 \bmod 4$; otherwise it is equal to

$$-\frac{2}{(x(x-1))^{\frac{p-1}{2}}}\partial_x - \frac{1}{(x-1)^{\frac{p+1}{2}}x^{\frac{p-1}{2}}}.$$

Therefore, for half of the primes p, the remainder is nonzero, hence Proposition 1.8 implies that $\mathscr{L}$ does not admit only algebraic solutions.

Example 1.15. Consider now the operator

$$\mathscr{L}_r = 2x\,(x-1)\,\partial_x^2 + (4x-1)\,\partial_x + 2r(1-r), \quad \text{with } r \in \mathbb{Q} \setminus \{1/2\},$$

which is a tiny modification of the operator in Example 1.14: only the constant term has changed. Then, for any prime $p \neq 2$ not dividing the denominator of r, the reduction modulo p of $\partial_x^p \bmod \mathscr{L}_r$ is equal to

$$\frac{r(r+1)\cdots\widehat{(r+\frac{p-1}{2})}\cdots(r+p-1)}{(x(x-1))^{\frac{p-1}{2}}}\partial_x + \frac{r(r+1)\cdots\widehat{(r+\frac{p-1}{2})}\cdots(r+p-1)}{2(x-1)^{\frac{p+1}{2}}x^{\frac{p-1}{2}}},$$

where the notation $\widehat{(r+\frac{p-1}{2})}$ indicates that $r+\frac{p-1}{2}$ is missing in the above products. For any prime number $p > 2$ not dividing the denominator of r nor the numerator of $2r-1$, the previous remainder is zero modulo p. Therefore, for all but finitely many primes p, the remainder is zero modulo p. Can we conclude that the operator $\mathscr{L}_r$ admits only algebraic solutions? Conjecture 1.13 predicts that the answer is positive and, indeed, one easily checks that $\mathscr{L}_r$ admits the algebraic solutions $f_1 = \left(\sqrt{x}+\sqrt{x-1}\right)^{2r-1}/\sqrt{x-1}$ and $f_2 = \left(\sqrt{x}+\sqrt{x-1}\right)^{1-2r}/\sqrt{x-1}$, which are linearly independent for $r \neq \frac{1}{2}$ since $f_1 f_2' - f_2 f_1' = (1-2r)/(\sqrt{x}\,(x-1)^{3/2})$.

2. Several natural differential equations have algebraic solutions

As we have just seen in Section 1, although in general the solutions $y(x)$ of (1) are transcendental functions (e.g., $y(x) = \exp(x)$ and $y(x) = \log(1-x)$), they may sometimes be algebraic. Most of the examples given in Section 1 were "academic examples", in the sense that they were simple and constructed to illustrate the exposition.

The aim of this section is to give evidence showing that linear differential equations naturally appear in many areas of mathematics, including algebra, combinatorics, and number theory. In all these settings, we shall see examples of differential equations that admit algebraic solutions and others that do not, demonstrating that both behaviors are common and deserve our attention. Hence, besides its beauty and intrinsic fundamental nature, being able to recognize whether a given D-finite function is algebraic or not appears as an important question, likely to have profound applications.

For instance, in number theory one often wants to understand the (algebraic or transcendental) nature of a complex number given as the value $f(\alpha)$ of a function $f \in \mathbb{Q}[[x]]$ at an algebraic point $\alpha \in \overline{\mathbb{Q}}$; understanding the algebraic nature of the corresponding function $f(x)$ is a first important step in this process. In the theory of the *E-functions* (an important class of D-finite functions generalizing the exponential function), the methods of Siegel and Shidlovskii, revisited recently in [1] and [21], are used to show that a number (such as $e = \exp(1)$) is transcendental by checking, among other things, that it is the value of a transcendental E-function. Another motivation comes from combinatorics, where predicting the nature of the generating function of some class of combinatorial objects is a central task, as it may reveal strong underlying structures. Indeed, knowing that a class of objects is counted by an algebraic function suggests that it should be possible to construct these objects recursively by concatenation of objects of the same type [25].

2.1. **Examples from special functions: Hypergeometric functions.**

2.1.1. *Elliptic integrals: Euler's differential equation.* Perhaps one of the oldest special functions distinct from the classical algebraic, exponential, logarithmic, or trigonometric functions, is the one arising from the question: *what is the perimeter $p(x)$ of an ellipse with semi-major axis* 1*, as a function of its eccentricity x?* (Recall that the eccentricity is the quotient between the focal distance and the semi-major axis.)

This question, which was solved by Euler [43, §7] in 1733, is more challenging than the analogous one with "perimeter" replaced by "area", since the area is expressible algebraically as $\pi\sqrt{1-x^2}$. First, we express the arc length using a real integral and the parametrization of the ellipse:

$$(5)\qquad p(x) = 4\int_0^1 \sqrt{\frac{1-x^2u^2}{1-u^2}}\,\mathrm{d}u = 2\pi - \frac{\pi}{2}x^2 - \frac{3\pi}{32}x^4 - \frac{5\pi}{128}x^6 - \frac{175\pi}{8192}x^8 - \cdots.$$

Up to the factor of 4, the function $p(x)$ is called the *complete elliptic integral of the second kind.* The second equality above is obtained by expanding the integrand in power series with respect to x, and integrating between 0 and 1. It is a fact familiar to algebraic geometers that this function $p(x)$ satisfies a linear differential equation: $p(x)$ is what we call a *period function* and, as such, it satisfies a linear differential equation called Picard–Fuchs differential equation (or Gauss–Manin connection). An alternative way to establish this fact and to find a differential equation satisfied by $p(x)$ is to use the "method of creative telescoping" [2]. The "magic" of creative telescoping is that it constructs the equality below, which expresses a linear combination of the integrand and of its first and second derivative with respect to x as a pure derivative with respect to u of another algebraic function (a rational multiple of the integrand):

$$(6)\qquad \left((x-x^3)\partial_x^2 + (1-x^2)\partial_x + x\right)\left(\sqrt{\frac{1-x^2u^2}{1-u^2}}\right) = \partial_u\left(\frac{xu\sqrt{1-u^2}}{\sqrt{1-x^2u^2}}\right).$$

Now, integrating both sides of equation (6) with respect to u, it follows that $p(x)$ is a D-finite function with respect to x, and that it satisfies the linear differential equation

$$(7)\qquad (x-x^3)p''(x) + (1-x^2)p'(x) + xp(x) = 0.$$

Writing $p(x) = \sum_{k\ge 0} a_k x^k$, we deduce from equation (7) the recursion $(k-1)(k+1)a_k = (k+2)^2 a_{k+2}$ for all $k \ge 0$. From $a_0 = 2\pi$ and $a_1 = 0$, it follows that

$$a_{2k} = \frac{2\pi\binom{2k}{k}^2}{(1-2k)16^k} \quad \text{and} \quad a_{2k+1} = 0 \quad \text{for all } k \ge 0.$$

Stirling's formula then implies that $a_{2k} \sim -1/k^2$, and hence transcendence of $p(x)$. Indeed, the presence of the factor k^{-2} is incompatible with algebraicity by Flajolet's criterion (Corollary 1.4).

2.1.2. *Elliptic integrals: Legendre's differential equation.* A special function similar to $p(x)$ is obtained by a different construction. Consider the family of elliptic curves (with $x \in \mathbb{C}$) given by the *Legendre equation*

$$E_x\colon y^2 = u(u-1)(u-x).$$

On E_x, there exists a unique (up to a constant multiple) holomorphic 1-form, given by

$$\omega_x = \frac{\mathrm{d}u}{y} = \frac{\mathrm{d}u}{\sqrt{u(u-1)(u-x)}}.$$

This form is necessarily closed since it is a holomorphic 1-form on a variety of complex dimension 1. The method of creative telescoping finds an exact form that is a linear combination of ω_x and of its first and second derivatives with respect to x, namely

$$\big((4x^2-4x)\partial_x^2 + (8x-4)\partial_x + 1\big)\,\omega_x = -\mathrm{d}\left(\frac{2\sqrt{u(u-1)}}{(u-x)^{3/2}}\right). \tag{8}$$

From equation (8) it follows that the integral $y(x) = \int_\gamma \omega_x$ over any closed curve γ on E_x satisfies the *Legendre differential equation*

$$(4x^2-4x)y''(x) + (8x-4)y'(x) + y(x) = 0. \tag{9}$$

This is the most basic case of the *Picard–Fuchs differential equation* of a period function. For instance, by taking C to be the curve on E_x given by the double cover $y = \pm\sqrt{u(u-1)(u-x)}$ of $[1,\infty)$, the corresponding period is the *complete elliptic integral of the first kind*,

$$\int_C \omega_x = 2\int_1^\infty \frac{\mathrm{d}u}{\sqrt{u(u-1)(u-x)}} = \sum_{k\geq 0} b_k x^k,$$

where $b_0 = 2\int_1^\infty \frac{\mathrm{d}u}{u\sqrt{u-1}} = 2\pi$ and $(2k+1)^2\,b_k = 4\,(k+1)^2\,b_{k+1}$ for all $k \geq 0$, this recurrence relation being a consequence of the fact that $y(x) = \int_C \omega_x$ satisfies equation (9). Thus,

$$\int_C \omega_x = 2\pi \sum_{k\geq 0} \binom{2k}{k}^2 \left(\frac{x}{16}\right)^k. \tag{10}$$

Once again, Stirling's formula gives $b_k \sim 2/k$, which excludes algebraicity of $y(x) = \int_C \omega_x$ by Flajolet's criterion (Corollary 1.4).

2.1.3. *Gauss's hypergeometric functions.* The D-finite functions considered in Sections 2.1.1 and 2.1.2 are special cases of the *Gauss hypergeometric function* with parameters $a, b, c \in \mathbb{Q}$, $c \notin \mathbb{Z}_{\leq 0}$, defined by

$${}_2F_1([a,b],[c];x) := \sum_{k\geq 0} \frac{(a)_k (b)_k}{(c)_k k!} x^k, \tag{11}$$

where $(a)_k = a(a+1)\cdots(a+k-1)$ denotes the rising factorial. Indeed, $p(x)$ in equation (5) is equal to $2\pi \cdot {}_2F_1([-1/2,1/2],[1];x^2)$, while $\int_C \omega_x$ in equation (10) is equal to $2\pi \cdot {}_2F_1([1/2,1/2],[1];x)$. We have seen that, in both cases, these functions are transcendental.

In general, $y(x) = {}_2F_1([a,b],[c];x)$ satisfies the second-order differential equation

$$x(x-1)y''(x) + ((a+b+1)x - c)y'(x) + aby(x) = 0 \tag{12}$$

and the name *hypergeometric* comes from the fact that the coefficient sequence $(u_k)_{k\geq 0}$ of ${}_2F_1([a,b],[c];x) = \sum_{k\geq 0} u_k x^k$ satisfies a linear recurrence of order 1, namely

$$(a+k)(b+k)u_k = (k+1)(k+c)u_{k+1}, \qquad (k \geq 0).$$

For other choices of parameters we recover the functions

$$(1-x)^\alpha = {}_2F_1([-\alpha, 1], [1]; x), \quad \text{for all } \alpha \in \mathbb{Q},$$
$$\sum_{k\geq 0} C_k x^k = {}_2F_1([1, 1/2], [2]; 4x),$$
$$\log(1-x) = -x \cdot {}_2F_1([1, 1], [2]; x),$$
$$\arcsin(x) = x \cdot {}_2F_1([1/2, 1/2], [3/2]; x^2),$$

the first two of which are algebraic, the last two of which are transcendental. In some cases, the Gauss's hypergeometric function even becomes a polynomial: this is so for

$$P_n(x) = {}_2F_1([-n, n+1], [1]; (1-x)/2),$$

the *Legendre polynomial* given by $P_n(x) := \frac{1}{2^n \cdot n!} \cdot \frac{\partial^n}{\partial x^n}(x^2-1)^n$, as well as for

$$T_n(x) = (-1)^n \cdot {}_2F_1([-n, n], [1/2]; (x+1)/2),$$

the *Chebyshev polynomial of the first kind* given by $T_n(\cos x) = \cos(nx)$.

Deciding the algebraicity of ${}_2F_1$ hypergeometric functions is an old problem, solved by Schwarz [76] using geometric tools (Riemann mappings, Schwarzian derivatives and sphere tilings by spherical triangles) and by Landau [64, 65] and Errera [42] using arithmetic tools (Eisenstein's criterion for algebraic power series, and Dirichlet's theorem on prime numbers in arithmetic progressions). Both approaches are algorithmic: Schwarz's criterion reduces the problem to a table look-up after some preprocessing on the parameters a, b, c; the Landau–Errera criterion amounts to checking a finite number of inequalities.

More precisely, let us assume that none of a, b, $c-a$ and $c-b$ is an integer (equivalently, the operator $H(a, b; c) := x(1-x)\partial_x^2 + (c-(a+b+1)x)\partial_x - ab$ is irreducible) and let D be the common denominator of a, b and c. Then, the Landau–Errera criterion says that the following assertions are equivalent:

(1) The hypergeometric function ${}_2F_1([a, b], [c]; x)$ is algebraic;
(2) The operator $H(a, b; c)$ admits only algebraic solutions;
(3) For every $\ell < D$ coprime with D, either $\{\ell a\} < \{\ell c\} < \{\ell b\}$ or $\{\ell b\} < \{\ell c\} < \{\ell a\}$. (Here $\{x\}$ denotes the fractional part $x - \lfloor x \rfloor$ of x.)

The last condition is equivalent to the fact that, for every $\ell < D$ coprime with D, the two sets $\{e^{2\pi i \ell a}, e^{2\pi i \ell b}\}$ and $\{e^{2\pi i \ell c}, 1\}$ are interlaced on the unit circle. This "interlacing condition" was first proved by Landau [64, 65] to be necessary for the algebraicity of ${}_2F_1([a, b], [c]; x)$ and then also proved to be sufficient by Errera [42]; see also Stridsberg's intermediate contribution [82], which relates the conditions in Eisenstein's criterion to the ones in the Landau–Errera condition. In Section 3.3 we will see that Theorem 3.23 provides an extension of the Landau–Errera "interlacing criterion" to the generalized hypergeometric function ${}_{s+1}F_s$ defined by

$$(13) \qquad {}_{s+1}F_s([a_1, \ldots, a_{s+1}], [b_1, \ldots, b_s]; x) = \sum_{k\geq 0} \frac{(a_1)_k \cdots (a_{s+1})_k}{(b_1)_k \cdots (b_s)_k k!} x^k.$$

2.2. **Examples from Algebra: Diagonals.** As proved in Section 1, algebraic functions are D-finite. A larger, yet very important, class of D-finite functions is formed by the *diagonals of rational functions*. By definition, the *diagonal* of a multivariate power series

$$F = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n} x_1^{i_1}\cdots x_n^{i_n} \ \in \mathbb{Q}[[x_1,\dots,x_n]]$$

is the univariate power series

$$\mathrm{Diag}(F) = \sum_{i\in\mathbb{N}} a_{i,\dots,i} t^i \ \in \mathbb{Q}[[t]].$$

Example 2.1 (Dyck bridges)**.** Let B_n be the number of $\{\uparrow,\rightarrow\}$-walks in $\mathbb{Z}^2$ from $(0,0)$ to (n,n) (i.e., there are exactly B_n ways of going from the origin to (n,n) using only North and East steps; see Section 2.3 for a more general context) and let $B(t)$ be its generating function $\sum_{n\geq 0} B_n t^n$. Then,

$$B(t) = \mathrm{Diag}\left(\frac{1}{1-x-y}\right) = \sum_{n\geq 0}\binom{2n}{n} t^n.$$

This is perhaps the simplest example of a diagonal. By the binomial theorem, it comes that $B(t) = 1/\sqrt{1-4t}$, hence this diagonal is even an algebraic function. This is not an accident. Indeed, a century ago Pólya [73] proved that diagonals of bivariate rational functions are algebraic. (Later, Furstenberg [52] showed that the converse also holds true.) Pólya's result can be proved as follows. First, using the simple observation[1] $\mathsf{Diag}(F)(t) = [x^0]\, F(x,t/x)$, the diagonal of the rational function $F(x,y)\in\mathbb{Q}(x,y)$ is encoded as a complex integral using Cauchy's integral theorem (for some $\epsilon > 0$)

$$\mathrm{Diag}\,(F)\,(t) = [x^{-1}]\frac{1}{x}F\left(x,\frac{t}{x}\right) = \frac{1}{2\pi i}\oint_{|x|=\epsilon} F\left(x,\frac{t}{x}\right)\frac{dx}{x},$$

which, in a second step can be evaluated using the residues theorem as a sum of residues (precisely: the residues of $F(x,t/x)/x$ at its "small poles", having limit 0 at $t=0$). Each of these residues are algebraic functions, and so is their sum $\mathsf{Diag}(F)$.

Example 2.2 (Dyck bridges, continued)**.** The proof sketched above directly concludes that

$$\mathrm{Diag}\left(\frac{1}{1-x-y}\right) = \frac{1}{2\pi i}\oint_{|x|=\epsilon}\frac{dx}{x-x^2-t} = \left.\frac{1}{1-2x}\right|_{x=\frac{1-\sqrt{1-4t}}{2}} = \frac{1}{\sqrt{1-4t}}.$$

Example 2.3. Interestingly, Pólya's result becomes false for more than two variables. A simple example is provided by the rational function $1/(1-x-y-z) = \sum_{i,j,k}\frac{(i+j+k)!}{i!j!k!}x^iy^jz^k$, whose diagonal is

$$\mathrm{Diag}\left(\frac{1}{1-x-y-z}\right) = \sum_{n\geq 0}\frac{(3n)!}{n!^3}t^n.$$

The transcendence of this function can be proved in various ways, for instance, by using asymptotics: Stirling's formula implies that $\frac{(3n)!}{n!^3}\sim\frac{\sqrt{3}}{2\pi}\frac{27^n}{n}$ and the presence of the factor n^{-1} is incompatible with algebraicity by Corollary 1.4. Another proof is based on rewriting

$$\mathrm{Diag}\left(\frac{1}{1-x-y-z}\right) = {}_2F_1\left(\left[\frac{1}{3},\frac{2}{3}\right],[1];27t\right), \tag{14}$$

[1]Here, and in all the text, $[x^n]$ denotes coefficient extraction of x^n.

and by using the Schwarz or the Landau–Errera criteria mentioned above.

The diagonal in equation (14) is hypergeometric, hence D-finite. In general, there is no reason that the diagonal of a multivariate rational function be hypergeometric. However, that all such diagonals are D-finite functions is a general fact. In fact, much more holds: a theorem by Lipshitz [66] states that if $F(x_1, \ldots, x_n)$ is a multivariate D-finite function,[2] then $\mathrm{Diag}(F)$ is D-finite.

The particular case where F is rational is already interesting and nontrivial to prove. In this case, the argument is the following. First, as in the bivariate case, if $F = P/Q \in \mathbb{Q}(x_1, \ldots, x_n) \cap \mathbb{Q}[[x_1, \ldots, x_n]]$, then the residue theorem allows one to write (for some $\epsilon > 0$)

$$\mathrm{Diag}(F)(t) = \frac{1}{(2\pi i)^{n-1}} \oint_{|x_1|=\cdots=|x_{n-1}|=\epsilon} F\left(x_1, \ldots, x_{n-1}, \frac{t}{x_1 \cdots x_{n-1}}\right) \frac{dx_1 \cdots dx_{n-1}}{x_1 \cdots x_{n-1}},$$

so that $\mathrm{Diag}(F)(t)$ is the period function of a (family of) rational functions. Its D-finiteness is then a consequence of the finite-dimensionality over $\mathbb{C}(t)$ of the de Rham cohomology for the complement of the variety in $\mathbb{A}^n_{\mathbb{C}(t)}$ defined by the equations $Q(x_1, \ldots, x_n) = 0$ and $x_1 \cdots x_n = t$. (This finiteness proof usually relies on a geometric argument in the smooth case, and on Hironaka's resolution of singularities in the general case.) In more down-to-earth terms this proof guarantees, in a noneffective way, that repeated differentiation under the integral sign eventually produces a finite sequence of rational integrands that admit a linear combination with coefficients in $\mathbb{Q}(t)$ that becomes an exact differential.

If $f(t)$ is the diagonal of a rational function, then not only is $f(t)$ D-finite, but in addition $f(t)$ is *globally bounded*—that is, $f(t)$ has a nonzero radius of convergence in $\mathbb{C}$ and $\beta \cdot f(\alpha \cdot t) \in \mathbb{Z}[[t]]$ for some $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$. (Note that this second property is equivalent to the existence of an $N \in \mathbb{N} \setminus \{0\}$ such that $f(Nt) - f(0) \in \mathbb{Z}[[t]]$, as in Proposition 1.6.) The following beautiful conjecture predicts that the converse is also true; it was formulated by Christol in the late 1980s, see, e.g., [30] and [32, Conjecture 4].

Conjecture 2.4 (Christol's conjecture)**.** *For $f(t) \in \mathbb{Q}[[t]]$, the following properties are equivalent:*

1. $f(t) = \mathrm{Diag}(F)$ *for some* $F \in \mathbb{Q}(x_1, \ldots, x_n) \cap \mathbb{Q}[[x_1, \ldots, x_n]]$*;*
2. $f \in \mathbb{Q}[[t]]$ *is D-finite and globally bounded.*

Christol's conjecture is far from being proved; the following explicit problem, also due to Christol [32, p. 51], is a very particular case of Conjecture 2.4 and it is still open as of today.

Question 2.5. Is

$$f(t) = {}_3F_2\left(\left[\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right], \left[1, \frac{1}{3}\right]; 3^6\, t\right) = 1 + 60\,t + 20475\,t^2 + 9373650\,t^3 + 4881796920\,t^4 + \cdots$$

the diagonal of a rational power series?

[2] This means that F satisfies a system of n linear partial differential equations, the i-th one being an ordinary linear differential equation with respect to $\frac{\partial}{\partial x_i}$ and with polynomial coefficients in $x_1, \ldots, x_n$.

Therefore, even understanding diagonals which are hypergeometric functions is a very difficult problem; for some recent progress see [24].

Another natural and difficult question is whether a given diagonal of a rational function is algebraic or transcendental. This question is directly connected to the main aim of this article. One may wonder whether it is possible to detect transcendence of a given diagonal $f(t) = \mathrm{Diag}(F)$ by reducing it modulo a prime p, and proving the transcendence of $f(t) \bmod p$ over $\mathbb{F}_p(t)$. Unfortunately, this strategy is systematically doomed to failure: indeed, even if the diagonal $f(t)$ is transcendental, its reduction modulo p is necessarily algebraic! This was proved by Furstenberg in [52, Theorem 1]. For instance, the transcendental diagonal in (14) is equal to

$$(1+t)^{-1/4} \bmod 5,$$
$$(1+6t+6t^2)^{-1/6} \bmod 7,$$
$$(1+6t+2t^2+8t^3)^{-1/10} \bmod 11.$$

On the other hand, the Christol–André conjecture (Conjecture 1.12) implies that if $f(t)$ is the diagonal of a rational function, then $f(t)$ is algebraic if and only if the condition (3b) is fulfilled. The direct implication is true without the Christol–André conjecture; it relies on three nontrivial facts: (i) the minimal-order LDE for a diagonal has only regular singularities with rational exponents [31]; (ii) the classification of local solutions of Fuchsian linear differential equations [74, Section 19]; (iii) if $f(t)$ is algebraic, then its minimal-order LDE has only algebraic solutions [36, Section 2]. If condition (3b) fails, then by (i) and (ii) at least one local solution $g(t)$ around $t = 0$ of the minimal-order LDE for $f(t)$ involves logarithms, hence $g(t)$ is transcendental; then (iii) implies that $f(t)$ must be transcendental as well.

For instance, the diagonal in (14) admits $t\,(27t-1)\,\partial_t^2 + (54t-1)\,\partial_t + 6$ as minimal-order differential equation, with local basis

$$1 + 6t + 90t^2 + \cdots \quad \text{and} \quad \log(t) + (6\log(t) + 15)\,t + \cdots .$$

Hence it is transcendental.

As a final remark, note that [87, Theorem 1.1] implies that for any prime $p \neq 3$, the reduction modulo p of the ${}_3F_2$ (transcendental) function from Question 2.5 is algebraic (of degree at most p^{54}). Hence, even if this ${}_3F_2$ function is not known to be a diagonal of a rational function, its reductions modulo p are known to behave as reductions modulo p of diagonals of rational functions.

2.3. **Examples from combinatorics: Walks in the quarter plane.** In combinatorics, studying the nature of generating functions is of primary importance; for instance, algebraicity may reveal essential (but potentially hidden) recursive structures of the combinatorial classes under consideration. In particular, many examples have been studied over the past decades in *lattice path combinatorics*, a subfield of enumerative combinatorics. A plethora of interesting mathematical phenomena occur even when restricting to the *walks with small steps in the quarter plane* $\mathbb{N}^2$. These are walks in the lattice $\mathbb{Z}^2$, confined to the cone $\mathbb{R}_+^2$ that start at the origin $(0,0)$ and use steps in a model (or stepset) $\mathscr{S}$ which is a fixed subset of the set of nearest-neighbor steps $\{\swarrow, \leftarrow, \nwarrow, \uparrow, \nearrow, \rightarrow, \searrow, \downarrow\}$. The systematic study of small step walks in $\mathbb{N}^2$ has been initiated by Bousquet-Mélou and Mishna in their germinal article [27]. An earlier reference on the topic, in a probabilistic context, is the book [45]. The study of generating functions of walks with small steps in the quarter plane now spans several decades and dozens of articles. For instance, in [38], the differential-algebraic nature of these generating functions is completely elucidated using tools from differential Galois theory. A survey with many references can be found in the recent article [13].

Given a model $\mathscr{S} \subseteq \{\swarrow, \leftarrow, \nwarrow, \uparrow, \nearrow, \rightarrow, \searrow, \downarrow\}$, we denote by $q_{i,j,n}$ the number of $\mathscr{S}$-walks of length n ending at (i, j). The *full counting sequence* $(q_{i,j,n})_{(i,j,n)\in\mathbb{N}^3}$ admits several interesting specializations, for instance, $e_n := q_{0,0,n}$, the number of $\mathscr{S}$-walks of length n returning to $(0, 0)$ ("excursions") and $q_n := \sum_{i,j\geq 0} q_{i,j,n}$, the number of $\mathscr{S}$-walks with prescribed length n.

To these sequences one attaches various functions, namely the *full generating function*

$$Q_{\mathscr{S}}(x, y, t) = \sum_{n=0}^{\infty}\Bigg(\sum_{i,j=0}^{\infty} q_{i,j,n}x^i y^j\Bigg)t^n \ \in \mathbb{Q}[x, y][[t]],$$

and its corresponding univariate specializations $Q_{\mathscr{S}}(0, 0, t) = \sum_{n\geq 0} e_n t^n$ ("excursions generating function"), $Q_{\mathscr{S}}(1, 1, t) = \sum_{n\geq 0} q_n t^n$ ("length generating function"); $Q_{\mathscr{S}}(1, 0, t)$ and $Q_{\mathscr{S}}(0, 1, t)$ ("boundary returns"); and $[x^0]\, Q_{\mathscr{S}}(x, 1/x, t)$ ("diagonal returns").

The general question in this setting is: given a model $\mathscr{S}$, what can be said about the generating function $Q_{\mathscr{S}}(x, y, t)$, and its specializations? In particular, is $Q_{\mathscr{S}}(x, y, t)$ algebraic? Is it at least D-finite? Does $Q_{\mathscr{S}}(x, y, t)$ (or at least some of its specializations) admit closed-form expressions?

The model $\mathscr{S} = \{\uparrow, \rightarrow\}$ in Example 2.1 (Dyck bridges) is one of the simplest possible models. In that case, the generating function $Q_{\mathscr{S}}(x, y, t)$ is algebraic. This is actually a particular case of a classical result stating that whenever $\mathscr{S}$ is included in $\{\uparrow, \nearrow, \rightarrow, \searrow, \downarrow\}$ or in $\{\leftarrow, \nwarrow, \uparrow, \nearrow, \rightarrow\}$, that is, if the walks are essentially 1-dimensional, then $Q_{\mathscr{S}}(x, y, t)$ is algebraic.

For this reason, most studies in the area focus on the truly 2-dimensional cases, that is, on models $\mathscr{S}$ that contain both a step oriented towards the horizontal and the vertical axes (see [13, Figure 1]). A full classification is now available, according to the algebro-differential properties of $Q_{\mathscr{S}}(x, y, t)$, but here we restrict to two examples.

2.3.1. *Trident walks.* Up to some canonical reductions, there are exactly 23 models of walks with small steps in the quarter plane whose full generating function $Q(x, y, t)$ is D-finite (with respect to x, y and t). They are displayed in [13, Figure 4].

One of these models is that of the "trident walks", with $\mathscr{S} = \{\nwarrow, \uparrow, \nearrow, \downarrow\}$. This is entry 7 in [13, Figure 4] and in [18, Table 6]. There exist 1 trident walk of length 0 (the empty walk), 2 trident walks of length 1 ($\{\uparrow\}, \{\nearrow\}$) and 7 trident walks of length 2 ($\{\uparrow - \uparrow\}, \{\uparrow - \downarrow\}, \{\uparrow - \nearrow\}, \{\nearrow - \nwarrow\}, \{\nearrow - \uparrow\}, \{\nearrow - \nearrow\}, \{\nearrow - \downarrow\}$). It was proved in [18] that the length generating function of trident walks

$$Q(t) = \sum_{n\geq 0} q_n t^n = 1 + 2\,t + 7\,t^2 + 23\,t^3 + 84\,t^4 + 301\,t^5 + 1127\,t^6 + \cdots$$

is D-finite and satisfies $L_5(Q(t)) = 0$, where L_5 is the following differential equation of order 5 with polynomial coefficients of degree at most 15:

$$t^2\,(t-1)\,(4t-1)\left(12t^2-1\right)\left(5184t^7-4128t^6+4416t^5+400t^4+252t^3-90t^2-42t\right.$$
$$\left.+3\right)\left(4t^2+1\right)\partial_t^5+t\left(21399552t^{13}-38486016t^{12}+43416576t^{11}-125803264t^{10}+7762176t^9\right.$$
$$\left.-3848960t^8+337088t^7+143168t^6-7128t^5+45328t^4-11304\,t^3-1854t^2+540t-27\right)\partial_t^4$$
$$+\left(143327232t^{13}-222621696t^{12}+257753088t^{11}-122575104t^{10}+36213888t^9-19897728t^8\right.$$
$$\left.+1942656t^7+70768t^6-100456t^5+254712t^4-35124t^3-7404\,t^2+1116t-48\right)\partial_t^3$$
$$+\left(346374144t^{12}-454643712t^{11}+545398272t^{10}-166067712t^9+59053824t^8\right.$$
$$\left.-32668800t^7+2167392t^6+54912t^5-687744t^4+500616t^3-31176t^2-5004t+288\right)\partial_t^2$$
$$+\left(262766592t^{11}-284000256t^{10}+358041600\,t^9-21846528t^8+33115392t^7-13748736t^6\right.$$
$$\left.-1184640t^5+651744t^4-894672t^3+278496t^2-7272t+2880\right)\partial_t+35831808t^{10}$$
$$-31186944t^9+42163200t^8+11639808t^7+4981248t^6-981504t^5-809280t^4+72576t^3$$
$$-177408t^2+8064t-3168.$$

The length generating function $Q(t)$ is completely and uniquely defined by L_5 and by the first coefficients $[t^k]Q(t)$ for $k = 0, \ldots, 14$. The question is how to determine the algebraic or transcendental nature of $Q(t)$.

Note that the asymptotic estimate $q_n \sim \gamma\beta^n n^r$ in [13, Fig. 4], with $\gamma = 4/(3\sqrt{\pi})$, $\beta = 4$, $r = -1/2$, is compatible with algebraicity, since $r \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$, $\beta \in \overline{\mathbb{Q}}$ and $\gamma\Gamma(r+1) = 4/3 \in \overline{\mathbb{Q}}$. Hence we cannot conclude the transcendence using asymptotic arguments, as in Example 2.3.

An interesting feature is that L_5 admits a factorization $L_2 \cdot L_{1,a} \cdot L_{1,b} \cdot L_{1,c}$, where the three operators $L_{1,\star}$ have order 1, and L_2 has order 2. This type of factorization $2/1/\cdots/1$ actually holds in cases 1–19 in [13, Fig. 4]. On the other hand, the algorithmic method (a variant of the *creative telescoping* mentioned in Section 2.1.1) that produces the differential equation L_5 does not guarantee that it is the least-order one satisfied by $Q(t)$. In [18], the above factorization was algorithmically computed and exploited (together with some other computer algebra algorithms) in order to produce the following expression for $Q(t)$ (and similar expressions for all cases 1–19 in [13, Fig. 4]):

$$Q(t) = \frac{1}{t(t-1)} \int_0^t \frac{u}{(1-4u)^{3/2}}$$
$$\left\{ 4 + \int_0^u \frac{(1-4v)^{1/2}(\frac{1}{2}+v)}{v^2} \left[1 + \frac{1}{2v(1+2v)(1+4v^2)^{1/2}} \right.\right.$$
$$\times \left((1-v)\,{}_2F_1\left(\left[\frac{1}{2}, \frac{3}{2}\right], [1]; \frac{16t^2}{4t^2+1} \right) \right.$$
$$\left.\left.\left. -(1+v)(1-4v+8v^2)\,{}_2F_1\left(\left[\frac{1}{2}, \frac{1}{2}\right], [1]; \frac{16t^2}{4t^2+1} \right) \right) \right] dv \right\} du.$$

From such an expression it is not difficult to prove that $Q(t)$ is transcendental using the fact that the ${}_2F_1$ occurring in the complete elliptic integral of the first kind, ${}_2F_1([1/2, 1/2], [1]; t)$, is transcendental. In [18, Section 4.2] it was shown that $Q(t)$ is transcendental by exploiting the explicit factorization of L_5, and by applying to L_2 a specific algorithm that decides algebraicity of solutions for operators of order 2, namely Kovacic's algorithm [62]. The same approach works uniformly on models 1–19 and allows one to prove the transcendence of the corresponding $Q(t)$ except in case 17 for the model $\mathscr{S} = \{\uparrow, \leftarrow, \searrow\}$, and in case 18 for the model $\mathscr{S} = \{\uparrow, \leftarrow, \searrow, \downarrow, \rightarrow, \nwarrow\}$ (in these two cases the algorithm proves algebraicity of all solutions of the corresponding L_2). Very interestingly, the full generating function $Q(x, y, t)$ is proved to be transcendental in all cases 1–19, and cases 17 and 18 are the only ones with algebraic specialization $Q(1, 1, t)$.

An alternative proof of the transcendence of the length generating function $Q(t)$ for trident walks is based on the fact that L_5 is indeed the minimal-order differential equation for $Q(t)$; this implies that if $Q(t)$ were algebraic, then L_5 would only have algebraic solutions, a situation discarded by exhibiting logarithms in the local solutions of L_5 at $t = 0$. This approach to the proof of transcendence of solutions of linear differential equations is used in [22]; its heart is the "minimization" algorithm from [21].

2.3.2. *Gessel walks.* The most difficult model of small-step walks in the quarter plane is Gessel's model, for which $\mathscr{S} = \{\nearrow, \swarrow, \leftarrow, \rightarrow\}$. For notational simplicity we will write $G(x, y, t)$ for the full generating function in this case, and $G(t)$ for the length generating function for Gessel walks $G(1, 1, t)$.

Around 2000, Ira Gessel formulated two conjectures equivalent to the following statements:

Conjecture 2.6. *The generating function*

$$G(0, 0, t) = 1 + 2t^2 + 11t^4 + 85t^6 + 782t^7 + \cdots$$

of Gessel excursions is equal to ${}_3F_2\left([5/6, 1/2, 1], [5/3, 2]; 16t^2\right)$.

Conjecture 2.7. *The generating function $G(x, y, t)$ is not D-finite.*

Gessel's first conjecture was first solved in 2009 by Kauers, Koutschan and Zeilberger in [58] using a computerized guess-and-prove approach. Unfortunately, solving Conjecture 2.6 had no implication concerning Conjecture 2.7, and in particular on the D-finiteness of the length generating function $G(t)$. It came as a total surprise when Bostan and Kauers [19] proved that Gessel's second conjecture was false.

Theorem 2.8 ([19])**.** *The generating function $G(x, y, t)$ for Gessel walks is algebraic.*

Moreover, the coefficients (g_n) of $G(t) = 1 + 2t + 7t^2 + 21t^3 + 78t^4 + 260t^5 + \cdots$ *satisfy* $(3n+1)\, g_{2n} = (12n+2)\, g_{2n-1}$ *and* $(n+1)\, g_{2n+1} = (4n+2)\, g_{2n}$ *for all* $n \geq 0$.

In addition, $G(t) = (H(t)-1)/(2t)$ *where* $H(t) = 1+2t+4t^2+14t^3+42t^4+\cdots$ *is a root of* $27\,(4t-1)^2\, H(t)^8 - 18\,(4t-1)^2\, H(t)^4 - 8\left(16t^2 + 24t + 1\right) H(t)^2 - (4t-1)^2 = 0$*, and*

$$H(t) = {}_2F_1\left(\left[-\frac{1}{12}, \frac{1}{4}\right], \left[\frac{2}{3}\right]; -\frac{64t\,(4t+1)^2}{(4t-1)^4}\right).$$

The original discovery and proof of Theorem 2.8 was computer-driven, and used a guess-and-prove approach, based on *Hermite–Padé approximants.* As a byproduct of this proof, the minimal polynomial of $G(x, y, t)$ has been estimated to have more than 10^{11} terms when written in expanded form, for a total size of ≈ 30 Gb! The guess-and-prove method is a 3-step process: (i) compute $G(x,y,t)$ to precision t^{1200} ($\approx$ 1.5 billion coefficients!); (ii) conjecture polynomial equations for $G(x,0,t)$ and $G(0,y,t)$; (iii) conclude the proof by computing multivariate resultants of (very big) polynomials (30 pages each).

As a matter of fact, the discovery of algebraicity was initially performed in a different way: the expansion of the generating function $G(x,y,t)$ modulo t^{1000} was sufficient to guess (by using *differential* Hermite–Padé approximants) two differential operators

- $\mathscr{L}_{x,0} \in \mathbb{Q}(x,t)\langle\partial_t\rangle$, of order 11 in ∂_t, bidegree $(96,78)$ in (t,x), and integer coefficients of at most 61 digits; and
- $\mathscr{L}_{0,y} \in \mathbb{Q}(y,t)\langle\partial_t\rangle$, of order 11 in ∂_t, bidegree $(68,28)$ in (t,y), and integer coefficients of at most 51 digits,

such that $\mathscr{L}_{x,0}(G(x,0,t)) = 0 \bmod t^{1000}$ and $\mathscr{L}_{0,y}(G(0,y,t)) = 0 \bmod t^{1000}$.

After this guessing step of plausible differential equations for $Q(x,0,t)$ and for $Q(0,y,t)$, an important step in the discovery process was to apply Conjecture 1.13 with several primes p. More precisely, for randomly chosen prime numbers p, and $a,b \in \mathbb{F}_p$, both $\mathscr{L}_{a,0}$ and $\mathscr{L}_{0,b}$ right-divide the pure power ∂_t^p in $\mathbb{F}_p(x)\langle\partial_t\rangle$; in other words, they have zero p-curvature for all the tested primes p (see Definition 3.18). This was the key observation in the discovery [19] that the trivariate generating function for Gessel walks is algebraic.

Several *human proofs* of Conjecture 2.6 and Theorem 2.8 have been discovered since the publication of [19]: the first one used complex analysis [20], the second one is purely algebraic [26], the third one is both combinatorial and analytic [28], while the more recent one is probably the most elementary [8].

2.4. **Examples from number theory.** In his ICM 2018 paper [89, p. 768], Zagier introduced a recurrent sequence of rational numbers $(c_n)_{n\geq 0}$ defined by initial terms $c_0 = 1, c_1 = -161/(2^{10}\cdot 3^5)$ and $c_2 = 26605753/(2^{23}\cdot 3^{12}\cdot 5^2)$, and by the following linear recursion with polynomial coefficients:

$$c_{n-3}+20\left(4500n^2-18900n+19739\right)c_{n-2}+80352000n(5n-1)(5n-2)(5n-4)c_n$$
$$+25\left(2592000n^4-16588800n^3+39118320n^2-39189168n+14092603\right)c_{n-1}=0.$$

This mysterious-looking sequence arises from a topological differential equation in the work of Bertola, Dubrovin, and Yang [9], each coefficient c_n being defined by an integral over the Deligne–Mumford moduli spaces of stable curves of genus g with n marked points. It is not difficult to prove that c_n behaves asymptotically like $1/n!^2$. Inspired by an analogy with the behavior of the *quantum periods* in mirror symmetry, Zagier asked whether it is possible that all the c_n become integers after multiplication by $n!^2$, or more generally by the product of two rising factorials. Zagier mentions the following highly nontrivial two results:

- [Yang & Zagier]: $a_n := (2^{10}\cdot 3^5\cdot 5^4)^n\cdot (3/5)_n\cdot (4/5)_n\cdot c_n \in \mathbb{Z}$ for all integers $n\geq 0$;
- [Dubrovin & Yang]: $b_n := (2^{12}\cdot 3^5\cdot 5^4)^n\cdot (2/5)_n\cdot (9/10)_n\cdot c_n \in \mathbb{Z}$ for all integers $n\geq 0$.

Both sequences are integer sequences of exponential growth, and hence can be expected to have a generating series that is (the Taylor expansion at 0 of) a period function in the sense of algebraic geometry. For the sequence (b_n), Zagier mentions that its generating function is even algebraic, but that the sequence (a_n) seems to be

TABLE 1. Pairs (u, v) for which the sequence $(u)_n \cdot (v)_n \cdot c_n$ is (conjecturally) almost integral. In all cases, the generating functions are (conjecturally) algebraic. Algebraicity degrees are "guessed" by numerical monodromy computations.

#	u	v	order	alg. degree	#	u	v	order	alg. degree
1	1/5	4/5	2	120	6	19/60	49/60	4	155520
2	3/5	4/5	2	120	7	19/60	59/60	4	46080
3	2/5	9/10	4	120	8	29/60	49/60	4	46080
4	7/30	9/10	4	155520	9	29/60	59/60	4	155520
5	9/10	17/30	4	155520					

more challenging. Yurkevich [88, Theorem 2] proved that the generating function of the sequence (a_n) is also algebraic. (See [40, Theorem 2] for a closely related result.) Inspired by these results, it is natural to look at the following question.

Question 2.9. Find $(u, v) \in \mathbb{Q}$ such that $\widetilde{c}_n := w^n \cdot (u)_n \cdot (v)_n \cdot c_n \in \mathbb{Z}$ for all $n \geq 0$, for some $w \in \mathbb{Z}$.

A natural related question is the following.

Question 2.10. Is it true that for these $(u, v) \in \mathbb{Q}$, the generating function $\sum_{n \geq 0} \widetilde{c}_n x^n$ is algebraic?

In a work (in progress) by Bostan, Weil, and Yurkevich, the following result is conjectured:

Conjecture 2.11. *The only pairs $(u, v) \in \mathbb{Q}^2 \cap (0, 1)^2$ such that there exists $w \in \mathbb{Z}$ such that $\widetilde{c}_n := w^n \cdot (u)_n \cdot (v)_n \cdot c_n \in \mathbb{Z}$ for all $n \geq 0$ are the ones listed in Table 1. Moreover, for each of these pairs, the corresponding generating function $\sum_{n \geq 0} \widetilde{c}_n x^n$ is algebraic, of algebraicity degree as in Table 1.*

For instance, in case 4 of Table 1, Conjecture 2.11 states that the generating function of the sequence $\widetilde{c}_n := (2^{14} \cdot 3^7 \cdot 5^4)^n \cdot (7/30)_n \cdot (9/10)_n \cdot c_n$,

$$\sum_{n \geq 0} \widetilde{c}_n x^n = 1 - 3042900x + 58917109730850x^2 - 1389307608898903890000x^3 + \cdots$$

is an algebraic solution of degree 155520 of the following order-4 (irreducible) operator

$$\begin{aligned} \mathscr{L}_4 = {} & 125x^3 (88335360x+1) (7739670528000x^2+31104000x+1)\, \partial_x^4 \\ & +25x^2 (3509591122844319744000 0x^3+95685546737664000x^2+2823828480x+23)\, \partial_x^3 \\ & +60x (368969189384886681600 00x^3+56436938459136000x^2+1177963920x+7)\, \partial_x^2 \\ & +(125498268712012087296 0000x^3+654118326337536000x^2+16648081920x+12)\, \partial_x \\ & +42055270898174263296000x^2 - 134823448166400x+36514800. \end{aligned}$$

In particular, this operator admits (conjecturally) only algebraic solutions. To our knowledge, this is an open problem. A heuristic check is based on Conjecture 1.13: it is not difficult to check (using a computer-algebra system) that the remainder of the right Euclidean division of ∂_x^p by $\mathscr{L}_4$ is zero for all primes $5 < p < 100$ except for $p \in \{7, 31\}$. Conjecture 1.13 then suggests that indeed $\mathscr{L}_4$ possesses algebraic solutions only.

3. Grothendieck's conjecture

The examples presented in Section 2 motivate the following question: given the linear differential equation (1) with coefficients in $\mathbb{Q}(x)$, can we give necessary and/or sufficient conditions for admitting algebraic solutions (either one, or all of them)?

As already mentioned earlier, Grothendieck's conjecture (Conjecture 1.13) provides such a criterion: in its enhanced version (Conjecture 3.17) it relates the existence of a "full basis of algebraic solutions" of the differential equation (1) to the existence of a "full basis of rational solutions" of its reductions modulo almost all prime numbers p.

The aim of this section is, first of all, to introduce the notion of p-curvature and to state a precise version of Grothendieck's conjecture. We first examine in detail the case of first order equations in Section 3.1 and come to the general case in Section 3.2. The next sections are more focused on the p-curvature itself: in Section 4, we describe efficient methods for computing it in practice, while in Section 5, we examine how it controls the growth of denominators and, in particular, the integrality of the solutions of the starting differential equation.

3.1. **The case of equations of order 1.**

Consider a linear differential operator of order 1

$$\mathscr{L} = \partial_x + a(x) \tag{15}$$

with $a(x) \in \mathbb{Q}(x)$. It makes sense to consider the reduction $a(x) \bmod p \in \mathbb{F}_p(x)$ of (the coefficients of) $a(x)$ modulo p for almost all prime numbers p. Thus, one can consider the reduction

$$\mathscr{L}_p = \partial_x + a(x) \bmod p \tag{16}$$

of $\mathscr{L}$ modulo p for almost all primes p. This is a linear differential operator of order 1 with coefficients in $\mathbb{F}_p(x)$. Our aim is to relate the existence of a nonzero algebraic solution of (15) to the existence of nonzero rational solutions of the reduced equations (16).

In what follows, we say that a function f is a solution of $\mathscr{L}$ (resp. of $\mathscr{L}_p$) when it is a solution of the corresponding differential equation, i.e., when $\mathscr{L}(f) = 0$ (resp. $\mathscr{L}_p(f) = 0$).

3.1.1. *Rational and algebraic solutions in characteristic* 0*: A criterion.* What makes the case of first order equations tractable is the fact that there is an explicit criterion for the existence of a nonzero algebraic (or rational) solution.

Proposition 3.1. *The monic first order differential operator* (15) *has a nonzero rational (resp., algebraic) solution if and only if its constant coefficient $a(x)$ has at most a simple pole with integral (resp., rational) residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞.*

Proof. We first consider the "rational case." Let us first assume that $a(x)$ has at most a simple pole with integral residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞. We thus have

$$a(x) = \sum_{i=1}^{m} \frac{n_i}{x - a_i} \tag{17}$$

for some $a_i \in \overline{\mathbb{Q}}$ and some $n_i \in \mathbb{Z}$. A straightforward calculation shows that

$$f(x) = \prod_{i=1}^{m} (x - a_i)^{n_i} \tag{18}$$

is a nonzero rational solution of (15).

Conversely, assume that (15) has a nonzero rational solution $f(x)$. This $f(x)$ can be factored as a product of linear factors $f(x) = c\prod_{i=1}^{m}(x - a_i)^{n_i}$ with $c \in \overline{\mathbb{Q}}^{\times}$, $a_i \in \overline{\mathbb{Q}}$ and $n_i \in \mathbb{Z}$. A straightforward calculation yields

$$a(x) = \frac{f'(x)}{f(x)} = \sum_{i=1}^{m} \frac{n_i}{x - a_i}.$$

This shows that $a(x)$ has at most a simple pole with integral residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞, as expected.

We now consider the "algebraic case." Let us first assume that $a(x)$ has at most a simple pole with rational residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞. Then, we can argue as we did above in the rational case, the only differences being that the n_i involved in (17) are no longer in $\mathbb{Z}$ but in $\mathbb{Q}$ and that (18) is no longer rational but algebraic.

Conversely, assume that (15) has a nonzero algebraic solution $f(x)$. Let $M(Y) = Y^N + \sum_{i=0}^{N-1} m_i(x)Y^i \in \mathbb{Q}(x)[Y]$ be the minimal polynomial of $f(x)$ over $\mathbb{Q}(x)$. By differentiating the equality $M(f) = 0$ with respect to x and by using $f'(x) = a(x)f(x)$, we get

$$\begin{aligned} 0 = M(f)' &= Nf^{N-1}f' + \sum_{i=0}^{N-1} m_i'(x)f^i + \sum_{i=0}^{N-1} m_i(x)if^{i-1}f' \\ &= Nf^{N-1}a(x)f + \sum_{i=0}^{N-1} m_i'(x)f^i + \sum_{i=0}^{N-1} m_i(x)if^{i-1}a(x)f \\ &= Na(x)f^N + \sum_{i=0}^{N-1} (m_i'(x) + m_i(x)ia(x))f^i. \end{aligned}$$

Hence, the polynomial $P(Y) = Na(x)Y^N + \sum_{i=0}^{N-1}(m_i'(x) + m_i(x)ia(x))Y^i$ satisfies $P(f) = 0$. By minimality of $M(Y)$, we get $P(Y) = Na(x)M(Y)$. Equating the constant terms in this equality, we get that $m_0(x)$ is a nonzero solution in $\mathbb{Q}(x)$ of $y'(x) = Na(x)y(x)$. Using the "rational case" treated above, we get that $Na(x)$ has at most a simple pole with integral residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞. Hence, $a(x)$ has at most a simple pole with rational residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞, as expected. □

Note that the proof above is very similar (in fact, generalizes) the one used in Example 1.2 to prove that the exponential function is transcendental.

3.1.2. *Algebraic solutions: From characteristic* 0 *to characteristic* p. We shall now consider the following question: assuming that (15) has a nonzero algebraic solution, what can be said about the reduced equation (16)? It is natural to expect that the latter has a nonzero algebraic solution for almost all primes p as well. Actually, something even better happens.

Example 3.2. Consider the differential equation

$$y' = \frac{1}{2(x-1)}y. \tag{19}$$

It has a nonzero algebraic solution, namely $f(x) = (1-x)^{1/2}$. For any prime $p \neq 2$, one can consider the reduction of (19) modulo p. Any such reduced equation has a nonzero algebraic solution, namely $f_p(x) = (1-x)^{1/2}$. Let us clarify our notations: $f_p(x)$ is a root of the polynomial $Y^2 - (1-x) \in \mathbb{F}_p(x)[Y]$, whereas $f(x)$ is a root of the polynomial $Y^2 - (1-x) \in \mathbb{Q}(x)[Y]$. However, the reduction of (19) modulo p can also be written as $y' = \frac{n_p}{x-1}y$ where $n_p \in \mathbb{Z}$ is such that $n_p \equiv \frac{1}{2} \bmod p$ and, hence $\widetilde{f_p}(x) = (1-x)^{n_p}$ is a nonzero solution of the reduction modulo p of (19). The interesting point is that $\widetilde{f_p}(x)$ is not only algebraic but rational, contrary to $f_p(x)$!

The conclusion of Example 3.2 is a general fact as shown by Theorem 3.5. Let us first give an analogue in positive characteristic of the "rational case" of Proposition 3.1.

Proposition 3.3. *Consider $b(x) \in \mathbb{F}_p(x)$. The differential equation*

$$y' + b(x)y = 0$$

has a nonzero rational solution if and only if $b(x)$ has at most a simple pole with residue in $\mathbb{F}_p$ at each point of $\overline{\mathbb{F}_p}$ and vanishes at ∞.

Proof. The proof is entirely similar to the proof of the rational case of Proposition 3.1; it is sufficient to replace $\overline{\mathbb{Q}}$ by $\overline{\mathbb{F}_p}$ and $\mathbb{Z}$ by $\mathbb{F}_p$ everywhere. □

Example 3.4. Consider the differential equation

$$y' = \frac{1}{x^2+1}y, \tag{20}$$

whose general solution in characteristic zero is $c \cdot \exp(\arctan(x))$ where c is a constant. We are interested in determining whether or not this equation has a rational solution in characteristic $p > 0$. Modulo $p = 2$, the rational function $b(x) = 1/(x^2+1)$ writes $1/(x+1)^2$; thus it has a pole of order 2 and hence the differential equation (20) has no nonzero rational solutions by Proposition 3.3. For $p \neq 2$, the partial fraction decomposition of $b(x)$ reads

$$b(x) = \frac{i}{2} \cdot \left(\frac{1}{x+i} - \frac{1}{x-i} \right),$$

where i denotes a square root of -1 in $\overline{\mathbb{F}_p}$. We now need to distinguish between two cases depending on the congruence class of p modulo 4. Indeed, when $p \equiv 1 \pmod 4$, we have $i \in \mathbb{F}_p$ and so the residues belong to $\mathbb{F}_p$ as well. In this case, equation (20) has then a nonzero rational solution, namely

$$y(x) = \left(\frac{x+i}{x-i} \right)^{i/2},$$

where the exponent $i/2$ is a lift in $\mathbb{Z}$ of $i/2 \in \mathbb{F}_p$. On the contrary, when $p \equiv 3 \pmod 4$, we know that -1 is not a square in $\mathbb{F}_p$, showing that the residues are not in $\mathbb{F}_p$ either. Therefore, in this case, equation (20) has no nonzero rational solution.

Theorem 3.5. *If* (15) *has a nonzero algebraic solution, then, for almost all primes* p*,* (16) *has a nonzero rational solution.*

Proof. Proposition 3.1 (and its proof) ensures that

$$a(x) = \sum_{i=1}^{m} \frac{e_i}{x - a_i} \tag{21}$$

for some $a_i \in \overline{\mathbb{Q}}$ and some $e_i \in \mathbb{Q}$.

Let us first assume that the a_i belong to $\mathbb{Q}$. For any prime p, we let $\mathbb{Z}_{(p)}$ be the ring of rational numbers with denominator relatively prime to p. We denote by $\pi_p : \mathbb{Z}_{(p)} \to \mathbb{F}_p$ the "reduction modulo p" map. For almost all primes p, the a_i and the e_i belong to $\mathbb{Z}_{(p)}$. For any such p, we have

$$a(x) \bmod p = \sum_{i=1}^{m} \frac{\pi_p(e_i)}{x - \pi_p(a_i)}$$

and the result follows from Proposition 3.3.

The proof in the general case is similar but requires basic notions from algebraic number theory. Let K be a number field containing the a_i and the e_i. Let $\mathcal{O}_K$ be the ring of integers of K. For any prime $\mathfrak{P}$ of K (which is, by definition, a prime ideal of $\mathcal{O}_K$), we let $\mathcal{O}_{\mathfrak{P}}$ be the valuation ring of K at $\mathfrak{P}$. We denote by $\kappa_{\mathfrak{P}}$ the corresponding residue field, and by $\pi_{\mathfrak{P}} : \mathcal{O}_{\mathfrak{P}} \to \kappa_{\mathfrak{P}}$ the quotient map. The residue field $\kappa_{\mathfrak{P}}$ is a finite field of characteristic p such that $\mathfrak{P} \cap \mathbb{Z} = (p)$. We say that $\mathfrak{P}$ is above p. For almost all primes p, and for all primes $\mathfrak{P}$ of K above p, the a_i and the e_i belong to $\mathcal{O}_{\mathfrak{P}}$. For such p and $\mathfrak{P}$, we have

$$a(x) \bmod p = a(x) \bmod \mathfrak{P} = \sum_{i=1}^{m} \frac{\pi_{\mathfrak{P}}(e_i)}{x - \pi_{\mathfrak{P}}(a_i)}.$$

Since e_i is rational, $\pi_{\mathfrak{P}}(e_i)$ belongs to the prime subfield $\mathbb{F}_p$ of $\kappa_{\mathfrak{P}}$. The result follows from Proposition 3.3. □

3.1.3. *From characteristic* p *to characteristic* 0. It is now tempting to ask if (16) has a nonzero rational solution for almost all primes p, does (15) have a nonzero algebraic solution. The (positive) answer is given by the following result.

Theorem 3.6 (Honda [53])**.** *The converse of Theorem* 3.5 *holds true, i.e., if, for almost all primes* p*,* (16) *has a nonzero rational solution, then* (15) *has a nonzero algebraic solution.*

Proof. Consider the partial fraction decomposition of $a(x)$:

$$a(x) = P(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\alpha_{i,j}}{(x - a_i)^j}$$

with $P(x) \in \overline{\mathbb{Q}}[x]$, $a_i \in \overline{\mathbb{Q}}$, $\alpha_{i,j} \in \overline{\mathbb{Q}}$, and $r_j \in \mathbb{Z}_{\geq 1}$. According to Proposition 3.1, we have to prove that $P(x)$ and all the $\alpha_{i,j}$ for $j \geq 2$ are 0 and that all the $\alpha_{i,1}$ belong to $\mathbb{Q}$.

Let K be a number field containing the a_i, all the $\alpha_{i,j}$ and the coefficients of $P(x)$. We will use the notation and terminology (prime $\mathfrak{P}$ of K, valuation ring $\mathcal{O}_{\mathfrak{P}}$, quotient map $\pi_{\mathfrak{P}}$, etc.) introduced in the proof of Theorem 3.5. For almost all primes p, for all primes $\mathfrak{P}$ of K above p, all the a_i, all the $\alpha_{i,j}$ and the coefficients of $P(x)$ belong to $\mathcal{O}_{\mathfrak{P}}$. For such p and $\mathfrak{P}$, we have:

$$a(x) \bmod p = a(x) \bmod \mathfrak{P} = P^{\pi_{\mathfrak{P}}}(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\pi_{\mathfrak{P}}(\alpha_{i,j})}{(x - \pi_{\mathfrak{P}}(a_i))^j},$$

where $P^{\pi_{\mathfrak{P}}}(x)$ denotes the polynomial obtained from $P(x)$ by applying $\pi_{\mathfrak{P}}$ coefficientwise.

Proposition 3.3 ensures that, for almost all primes p, $a(x) \bmod p$ has at most simple poles, so, for almost all primes p, for all primes $\mathfrak{P}$ of K above p, for all $j \in \{2, \ldots, r_i\}$, we have $\pi_{\mathfrak{P}}(\alpha_{i,j}) = 0$, i.e., $\alpha_{i,j} \in \mathfrak{P}$. This implies that, for all $j \in \{2, \ldots, r_i\}$, we have $\alpha_{i,j} = 0$. Similarly, Proposition 3.3 also ensures that, for almost all primes p, $a(x) \bmod p$ vanishes at ∞, so, for almost all primes p, and for all primes $\mathfrak{P}$ of K above p, $P^{\pi_{\mathfrak{P}}}(x) = 0$. This implies that $P(x) = 0$. Last, Proposition 3.3 ensures that, for almost all primes p, and for all primes $\mathfrak{P}$ above p, we have $\pi_{\mathfrak{P}}(\alpha_{i,1}) \in \mathbb{F}_p$. Using Kronecker's theorem recalled below, we get that $\alpha_{i,1}$ belongs to $\mathbb{Q}$ and Proposition 3.1 yields the desired result: (15) has a nonzero algebraic solution. □

The Kronecker theorem mentioned above (which is usually seen as a consequence of Chebotarev's density theorem) reads as follows.

Theorem 3.7 (Kronecker)**.** *An irreducible element $P(x)$ of $\mathbb{Q}[x]$ such that, for almost all primes p, $P(x) \bmod p$ has a zero in $\mathbb{F}_p$ is linear.*

3.1.4. *Rational solutions in characteristic p and p-curvature.* Consider a differential equation

$$y' + b(x)y = 0 \tag{22}$$

with $b(x) \in \mathbb{F}_p(x)$. We will give an alternative criterion (an alternative to Proposition 3.3) for determining whether (22) has a nonzero rational solution based on the notion of p-curvature that we shall now introduce.

Consider the $\mathbb{F}_p(x^p)$-linear map

$$\begin{aligned} \Delta : \mathbb{F}_p(x) &\to \mathbb{F}_p(x) \\ f &\mapsto f' + b(x)f. \end{aligned}$$

The additivity is clear; the homogeneity follows from the fact that the elements of $\mathbb{F}_p(x^p)$ are constants of (the differential field) $\mathbb{F}_p(x)$ in the sense that their derivative is 0 (more precisely, $\mathbb{F}_p(x^p) = \{f(x) \in \mathbb{F}_p(x) \mid f'(x) = 0\}$) implying that $(\alpha f)' = \alpha f'$ for all $\alpha \in \mathbb{F}_p(x^p)$ and $f \in \mathbb{F}_p(x)$.

Definition 3.8. The map

$$\Delta^p : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$$

is called the p-curvature of (22).

A remarkable and fundamental fact is that the p-curvature is not only $\mathbb{F}_p(x^p)$-linear but it is also $\mathbb{F}_p(x)$-linear. Indeed, a simple induction along with the Leibniz rule show that, for all $k \geq 0$, for all $\alpha, f \in \mathbb{F}_p(x)$, we have

$$\Delta^k(\alpha f) = \sum_{i=0}^{k} \binom{k}{i} \alpha^{(i)} \Delta^{k-i}(f).$$

Taking $k = p$ and using the fact that $\binom{p}{i} \equiv 0 \bmod p$ for all $1 < i < p$, we get

$$\Delta^p(\alpha f) = \alpha^{(p)} + \alpha \Delta^p(f),$$

and therefore the $\mathbb{F}_p(x)$-homogeneity follows from the fact that $\alpha^{(p)} = 0$.

Proposition 3.9. *The differential equation* (22) *has a nonzero rational solution if and only if* $\Delta^p = 0$.

Proof. If (22) has a nonzero rational solution f, then $\Delta(f)$=0 and, hence, $\Delta^p(f)$=0. As Δ^p is $\mathbb{F}_p(x)$-linear, we get $\Delta^p = 0$. Conversely, if $\Delta^p = 0$, then Δ has a nonzero kernel and, hence, (22) has a nonzero rational solution. □

Remark 3.10. An easy calculation shows that, if (22) has p-curvature 0, then an explicit nonzero rational solution is given by

$$\sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} \Delta^k(1).$$

We conclude this section by giving inductive and closed formulae for the p-curvature. As it is $\mathbb{F}_p(x)$-linear, the p-curvature is entirely determined by its value at 1:

$$\forall f \in \mathbb{F}_p(x), \ \Delta^p(f) = \Delta^p(1) f.$$

For this reason, we often say that the p-curvature of (22) is $\Delta^p(1)$. It turns out that the p-curvature $\Delta^p(1)$ can be calculated inductively. Indeed, for all $k \geq 0$, we denote by $b_k(x) \in \mathbb{F}_p(x)$ the constant term of the differential operator $\big(\partial_x + b(x)\big)^k$, so that

$$\big(\partial_x + b(x)\big)^k = \partial_x^k + \star \partial_x^{k-1} + \cdots + \star \partial_x + b_k(x), \tag{23}$$

where $\star$ are some unspecified elements of $\mathbb{F}_p(x)$. Equating the terms of degree 0 (with respect to ∂_x) in the equality $(\partial_x + b(x))^{k+1} = (\partial_x + b(x)) \cdot (\partial_x + b(x))^k$, we get the following inductive formula for computing the $b_k(x)$:

$$\forall k \geq 0, \ b_{k+1}(x) = b_k'(x) + b(x) b_k(x). \tag{24}$$

This gives the expected inductive formula for the p-curvature of (22), since this is equal to

$$\Delta^p(1) = b_p(x).$$

Remark 3.11. When $k = p$, it is actually possible to determine the coefficients $\star$ in Equation (23). Indeed, we observe that $(\partial_x + b(x))^p$ is a central element in $\mathbb{F}_p(x)\langle \partial_x \rangle$. This shows that the right-hand side of equation (23) must be central as well, implying that all terms in ∂_x^i with $0 \leq i < p$ have to vanish eventually, and that $b_p(x)$ belongs to $\mathbb{F}_p(x^p)$.

In conclusion, we have the relation

$$\big(\partial_x + b(x)\big)^p = \partial_x^p + b_p(x).$$

From this, we deduce that $b_p(x)$ is also the opposite of the remainder in the right Euclidean division of ∂_x^p by $\mathscr{L} = \partial_x + b(x)$. In particular, the p-curvature vanishes if and only if $\mathscr{L}$ divides ∂_x^p in $\mathbb{F}_p(x)\langle \partial_x \rangle$.

Last, one can deduce from (24) the following remarkable closed formula (that does not extend to higher-order equations).

Theorem 3.12. *We have* $b_p(x) = b^{(p-1)}(x) + b(x)^p$.

Proof (after Jacobson [54]*).* For a positive integer k, let I_k be the set of all tuples $\underline{\alpha} = (\alpha_1, \ldots, \alpha_k)$ of nonnegative integers such that $\sum_{i=1}^k i\alpha_i = k$. A calculation shows that $b_k(x)$ is explicitly given by

$$b_k(x) = \sum_{\underline{\alpha} \in I_k} \lambda_{\underline{\alpha}} \cdot b(x)^{\alpha_1} \cdot b^{(1)}(x)^{\alpha_2} \cdots b^{(k-1)}(x)^{\alpha_k},$$

where $\lambda_{\underline{\alpha}}$ is a coefficient in $\mathbb{Z}$ determined by the following rule

$$\lambda_{\underline{\alpha}} = \sum_{i=1}^{k} (\alpha_{i-1} + 1) \cdot \lambda_{\tau_i(\underline{\alpha})} \qquad (\text{for } \underline{\alpha} \in I_k),$$

where τ_i denotes the function from I_k to I_{k-1} defined by

$$\tau_i(\underline{\alpha}) = (\alpha_1,\ \ldots,\ \alpha_{i-2},\ \alpha_{i-1}{-}1,\ \alpha_i{+}1,\ \alpha_{i+1},\ \ldots,\ \alpha_{k-1})$$

and where we agree that $\lambda_{\underline{\beta}} = 0$ if $\underline{\beta}$ has one negative coordinate. From this relation, one can check by induction on k that $\lambda_{\underline{\alpha}}$ (with $\underline{\alpha} = (\alpha_1, \ldots, \alpha_k) \in I_k$) is given by the closed formula

$$\lambda_{\underline{\alpha}} = \frac{k!}{(\alpha_1)! \cdots (\alpha_k)! \cdot (2!)^{\alpha_2} \cdot (3!)^{\alpha_3} \cdots (k!)^{\alpha_k}}.$$

In particular, when $k = p$, we find that the $\lambda_{\underline{\alpha}}$ vanish modulo p for all $\underline{\alpha} \in I_p$ (thanks to the numerator $p!$) except when $\underline{\alpha} = (p, 0, \ldots, 0)$ or $\underline{\alpha} = (0, \ldots, 0, 1)$ (because, in those cases, the numerator cancels with a factor $p!$ in the denominator). Besides, in both cases, one finds $\lambda_{\underline{\alpha}} = 1$. This concludes the proof. ☐

Remark 3.13. Remarkably, the explicit formula of Theorem 3.12 provides a second proof of Proposition 3.3. Indeed, consider a rational function $b(x) \in \mathbb{F}_p(x)$ and write its partial fraction decomposition

$$b(x) = P(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\beta_{i,j}}{(x - b_i)^j}$$

where $P(x)$ is a polynomial, the b_i are pairwise distinct elements of $\overline{\mathbb{F}_p}$ and $\beta_{i,j} \in \overline{\mathbb{F}_p}$ with $\beta_{i,r_i} \neq 0$. Each b_i is a pole of $b(x)$ of multiplicity r_i and residue $\beta_{i,1}$. Moreover, $b(x)$ has an extra pole at infinity when the degree of $P(x)$ is positive. A direct computation now gives

$$b_p(x) = P^{(p-1)}(x) + P(x)^p - \sum_{i=1}^{m} \sum_{\substack{1 \le j \le r_i \\ j \equiv 1 \bmod p}} \frac{\beta_{i,j}}{(x - b_i)^{j+p-1}} + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\beta_{i,j}^p}{(x - b_i)^{pj}}$$

and we see that the latter is zero if and only if $P(x)$ vanishes and, for all $i \in \{1, \ldots, m\}$, we have $r_i = 1$ and $\beta_{i,1}^p = \beta_{i,1}$, i.e., $\beta_{i,1} \in \mathbb{F}_p$. After Proposition 3.9, we then recover by different means the result of Proposition 3.3.

Example 3.14. Applying the above recipe with the differential operator

$$\mathscr{L}_p = \partial_x - \frac{1}{x^2 + 1}$$

of Example 3.4, we find that its p-curvature is explicitly given by

$$b_p(x) = -\frac{c_p}{(x^2 + 1)^p}$$

where $c_p = 1$ if $p = 2$, $c_p = 0$ for $p \equiv 1 \pmod 4$ and $c_p = 2$ for $p \equiv 3 \pmod 4$. In particular, we retrieve by different means the dichotomy that we had already observed in Example 3.4.

The situation can be more complex if we change the coefficient $b(x)$ slightly. For instance, consider the first-order differential operator

$$\mathscr{L}_p = \partial_x - \frac{1}{x^3 - x - 1}.$$

Its p-curvature is zero if and only if the polynomial $x^3 - x - 1$ splits in $\mathbb{F}_p[x]$ and $p \neq 23$. By [78, Section 5.3], this happens only for the primes

$$p \in \{59, 101, 167, 173, 211, 223, 271, 307, 317, \ldots\}$$

that have the property that $p \neq 23$ and they can be written as $p = m^2 + mn + 6n^2$ with $m, n \in \mathbb{Z}$, or equivalently, if and only if the coefficient of x^{p-1} in

$$\prod_{n=1}^{\infty} (1 - x^n)(1 - x^{23n})$$

is equal to 2. (See [84, Proposition 3.3].)

Remark 3.15. There is a link between the p-curvature of first-order linear differential operators and a fairly famous algorithm for factoring polynomials in $\mathbb{F}_p[x]$, designed by Niederreiter in [68]. This connection seems to have been unnoticed until now. To factor a separable polynomial $f = \prod_i g_i$ of $\mathbb{F}_p[x]$, with irreducible g_i, Niederreiter considers the space of rational functions $y = h/f$ solutions of the equation $y^{(p-1)} + y^p = 0$, and shows that as a vector space over $\mathbb{F}_p$ it is generated by the logarithmic derivatives g_i'/g_i. As a result, factoring boils down to a linear algebra problem over $\mathbb{F}_p$. This algorithm created a lot of excitement as a promising alternative to the much more classical one due to Berlekamp [7].

Putting together Theorem 3.5, Theorem 3.6, Proposition 3.9, and Remark 3.11, we obtain the following result.

Theorem 3.16. *Let $\mathscr{L} = \partial_x + a(x)$ as in equation* (15) *and, for almost all prime numbers p, denote by $\mathscr{L}_p$ its reduction modulo p as in equation* (16). *The following properties are equivalent:*

(1) *$\mathscr{L}$ has a nonzero algebraic solution;*
(2) *For almost all primes p, $\mathscr{L}_p$ has a nonzero rational solution;*
(3) *For almost all primes p, the p-curvature of $\mathscr{L}_p$ vanishes;*
(4) *For almost all primes p, the operator $\mathscr{L}_p$ divides ∂_x^p in $\mathbb{F}_p(x)\langle\partial_x\rangle$.*

Grothendieck's p-curvature conjecture is a far-reaching conjectural generalization of these equivalences for higher-order equations.

3.2. **The general case.** Let us now consider a linear differential operator of arbitrary order:

$$\mathscr{L} = \partial_x^n + a_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + a_1(x)\cdot\partial_x + a_0(x) \tag{25}$$

with $a_i(x) \in \mathbb{Q}(x)$. As in the first-order case, one can consider the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p for almost all primes p. This is a differential operator of order n with coefficients in $\mathbb{F}_p(x)$. Grothendieck's conjecture relates the algebraicity of the solutions of $\mathscr{L}$ to the rationality of the solutions of $\mathscr{L}_p$ for almost all primes p.

First of all, we notice that the straightforward generalization of Theorem 3.16 cannot be true for higher-order differential operators; indeed, we have seen in Section 2 many examples of differential equations that do not admit algebraic solutions and whose reductions modulo p have nonzero rational solutions for almost all p; this is the case, for instance, of most of hypergeometric functions and diagonals. The main new insight behind Grothendieck's conjecture is the brilliant idea to replace the existence of a unique nonzero solution by the existence of a *full basis* of solutions.

We recall that the set of solutions of $\mathscr{L}$ in $\overline{\mathbb{Q}(x)}$ is a $\overline{\mathbb{Q}}$-vector space of dimension at most n. When this dimension is maximal, that is, equal to n, we say that $\mathscr{L}$ has a full basis of algebraic solutions. Similarly, it is tempting to look at the set of solutions of $\mathscr{L}_p$ in $\mathbb{F}_p(x)$ as an $\mathbb{F}_p$-vector space. However, the example given by the differential equation $y^{(p)} = 0$ shows that this vector space may be infinite dimensional (any element of $\mathbb{F}_p(x)$ is a solution of $y^{(p)} = 0$). The point is that $\overline{\mathbb{Q}}$ is the relevant base field in characteristic 0 because it is the field of differential constants of $\overline{\mathbb{Q}(x)}$. In characteristic p, the field of differential constants of $\mathbb{F}_p(x)$ is not $\mathbb{F}_p$ but $\mathbb{F}_p(x^p)$; thus, a differential constant may depend on x in characteristic p (!). Now, one can prove that the set of solutions of $\mathscr{L}_p$ in $\mathbb{F}_p(x)$ is an $\mathbb{F}_p(x^p)$-vector space of dimension at most n. When this dimension is maximal, that is, equal to n, we say that $\mathscr{L}_p$ has a full basis of rational solutions.

We are now ready to state Grothendieck's conjecture.

Conjecture 3.17 (Grothendieck's conjecture)**.** *For a differential operator $\mathscr{L} \in \mathbb{Q}(x)\langle\partial_x\rangle$ as in equation* (25)*, the following properties are equivalent:*

(1) *$\mathscr{L}$ has a full basis of algebraic solutions;*
(2) *For almost all primes p, $\mathscr{L}_p$ has a full basis of rational solutions.*

Consider the linear differential operator

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x) \tag{26}$$

with $b_i(x) \in \mathbb{F}_p(x)$. There is no straightforward generalization of Proposition 3.3 for determining whether (26) has a full basis of rational solutions but the criterion given by Proposition 3.9 via the p-curvature does extend to higher-order equations. Let us briefly explain this.

Let $Y' + B(x)Y = 0$ be the differential system associated to (26), where

$$B = \begin{pmatrix} 0 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 \\ b_0 & b_1 & b_2 & \cdots & b_{n-2} & b_{n-1} \end{pmatrix} \in M_n(\mathbb{F}_p(x)). \tag{27}$$

Mimicking what has been done in Section 3.1.4 in the first-order case, we consider the $\mathbb{F}_p(x^p)$-linear map

$$\begin{aligned} \Delta : \mathbb{F}_p(x)^n &\to \mathbb{F}_p(x)^n \\ F &\mapsto F' + B(x)F. \end{aligned}$$

Definition 3.18. The map

$$\Delta^p : \mathbb{F}_p(x)^n \to \mathbb{F}_p(x)^n$$

is called the p-curvature of (26).

As in the first-order case, one can easily prove that the p-curvature is not only $\mathbb{F}_p(x^p)$-linear, but also $\mathbb{F}_p(x)$-linear. Moreover, the inductive formula (24) for computing the p-curvature of equations of order 1 can be extended as follows: the matrix $B_p(x)$ of the p-curvature with respect to the canonical basis is given by the recurrence

$$B_{k+1}(x) = B_k'(x) + B(x)B_k(x) \tag{28}$$

starting with $B_0(x) = B(x)$.

The following fundamental result is a generalization of Proposition 3.9 to higher-order differential equations. We recall the fact, already mentioned at the very beginning of Section 3.2, that the set of solutions of a given $\mathscr{L} \in \mathbb{F}_p(x)\langle\partial_x\rangle$ in $\mathbb{F}_p(x)$ of order n is an $\mathbb{F}_p(x^p)$-vector space of dimension at most n and that, when this dimension is maximal, that is, equal to n, we say that $\mathscr{L}$ has a full basis of rational solutions.

Theorem 3.19 (Cartier's lemma). *Let $\mathscr{L} \in \mathbb{F}_p(x)\langle\partial_x\rangle$ be a differential operator as in equation* (26)*. The following properties are equivalent:*

(1) *$\mathscr{L}$ has a full basis of rational solutions;*
(2) *The p-curvature of $\mathscr{L}$ (that is Δ^p) vanishes;*
(3) *$\mathscr{L}$ divides ∂_x^p in $\mathbb{F}_p(x)\langle\partial_x\rangle$.*

Proof. Let us first note that the following properties, relative to the $\mathbb{F}_p(x^p)$-vector space $S := \ker(\Delta)$, are equivalent:

(i) The differential equation (26) has a full basis of rational solutions;
(ii) The $\mathbb{F}_p(x^p)$-vector space S has dimension n;
(iii) The $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S.

The equivalence between (i) and (ii) follows immediately from the easily verifiable fact that the map

$$f(x) \mapsto (f(x), f'(x), \dots, f^{(n-1)}(x))$$

induces an $\mathbb{F}_p(x^p)$-linear isomorphism from the $\mathbb{F}_p(x^p)$-vector space of solutions of $\mathscr{L}$ in $\mathbb{F}_p(x)$ to the $\mathbb{F}_p(x^p)$-vector space S. The equivalence between (ii) and (iii) follows from the "Wronskian lemma" [86, Lemma 1.12]. Indeed, the Wronskian lemma ensures that any family of elements of S is linearly dependent over $\mathbb{F}_p(x^p)$ if and only if it is linearly dependent over $\mathbb{F}_p(x)$. Therefore, the dimension of the $\mathbb{F}_p(x^p)$-vector space S and the dimension of the $\mathbb{F}_p(x)$-vector space spanned by S are equal. Considering the case where one or the other of these dimensions is n, we obtain the equivalence between (ii) and (iii).

We are now ready to prove the theorem.

Let us first prove (1)$\Longrightarrow$(2). If $\mathscr{L}$ has a full basis of rational solutions, then the implication (i)$\Longrightarrow$(iii) ensures that the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S. Since Δ^p is $\mathbb{F}_p(x)$-linear and vanishes on S, we have $\Delta^p = 0$.

Let us now prove (2)$\Longrightarrow$(1). We assume that $\Delta^p = 0$. We claim that the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S. Consider the map

$$\begin{aligned} P : \mathbb{F}_p(x)^n &\to \mathbb{F}_p(x)^n \\ F &\mapsto \sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} \Delta^k(F). \end{aligned}$$

A simple calculation shows that

$$\Delta(P(F)) = -(-x)^{p-1}\Delta^p(F) = 0$$

and, hence, P has values in S. But another simple calculation shows that, for all $F \in \mathbb{F}_p(x)^n$, we have

$$F = \sum_{k=0}^{p-1} \frac{x^k}{k!} P(\Delta^k(F)).$$

This shows that the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S as claimed. Now, using the implication (iii)$\Longrightarrow$(i), we get that $\mathscr{L}$ has a full basis of rational solutions.

It remains to prove that (2)$\Longleftrightarrow$(3). In order to do so, we first notice that, given rational functions $f_0(x), \ldots, f_{n-1}(x), g_0(x), \ldots, g_{n-1}(x)$, the equality

$$\Delta\big(f_0(x), \ldots, f_{n-1}(x)\big) = \big(g_0(x), \ldots, g_{n-1}(x)\big)$$

is equivalent to the following congruence in $\mathbb{F}_p(x)\langle\partial_x\rangle$:

$$\big(f_0(x) + \cdots + f_{n-1}(x)\partial_x^{n-1}\big) \cdot \partial_x \equiv g_0(x) + \cdots + g_{n-1}(x)\partial_x^{n-1} \pmod{\mathscr{L}}.$$

It follows from this observation that, writing $E_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with the coordinate 1 in ith position, the coordinates of $\Delta^p(E_i)$ are exactly the coefficients of the remainder in the division of ∂_x^{p+i} by $\mathscr{L}$. Hence $\Delta^p(E_i)$ vanishes if and only if $\mathscr{L}$ divides ∂_x^{p+i}. The equivalence (2)$\Longleftrightarrow$(3) follows immediately. □

Remark 3.20. The three assertions of Theorem 3.19 are also equivalent to

(4) $\mathscr{L}$ admits n power series solutions in $\mathbb{F}_p[[x]]$, linearly independent over $\mathbb{F}_p((x^p))$;

(5) $\mathscr{L}$ admits n polynomial solutions in $\mathbb{F}_p[x]$, linearly independent over $\mathbb{F}_p((x^p))$.

The implication (4) $\Longrightarrow$ (5) is proved in [53, Lemma 1], while (5) $\Longrightarrow$ (1) and (1) $\Longrightarrow$ (4) are trivial. Moreover, under the equivalent assertions (1)–(5), [23, Proposition 1] shows that there exists a full basis of polynomial solutions in $\mathbb{F}_p[x]$, each of them having degree less than pd, where d is the maximal degree of the numerators/denominators of the coefficients $b_i(x)$ of $\mathscr{L}$ in (26).

Remark 3.21. Assume that $\mathscr{L}$ has p-curvature zero. An easy calculation shows that

$$U_0(x) = \sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} B_k(x) \in M_n(\mathbb{F}_p(x))$$

is a solution of $Y' + B(x)Y = 0$. If, moreover, $B(x)$ has no pole at 0, then $U_0(x)$ has no pole at 0 as well and we have $U_0(0) = I_n$, so $U_0(x)$ is a fundamental matrix of rational solutions of $Y' + B(x)Y = 0$. If $B(x)$ has a pole at 0, then $U_0(x)$ is not necessarily invertible. Note that, more generally, if $a \in \mathbb{F}_p$ is not a pole of $B(x)$, then

$$U_a(x) = \sum_{k=0}^{p-1} (-1)^k \frac{(x-a)^k}{k!} B_k(x-a)$$

is a fundamental matrix of rational solutions of $Y' + B(x)Y = 0$.

Putting together all that precedes, we obtain a simple algorithm to determine whether (26) has a full basis of rational solutions: compute inductively $B_p(x)$ and then check whether $B_p(x)$ vanishes. Note, however, that no extension of the simple formula of Theorem 3.12 is known for higher-order differential equations. Roughly speaking, this is due to the fact that, contrarily to $\mathbb{F}_p(x)$, the ring of $n \times n$ matrices over $\mathbb{F}_p(x)$ is noncommutative as soon as $n \geq 2$. Computing the p-curvature is then much more complicated in this case, but rather efficient algorithms for this task are nevertheless available; we will discuss them in Section 4.

Using Theorem 3.19 (Cartier's lemma), we get the following reformulation of Grothendieck's conjecture.

Conjecture 3.22 (Grothendieck's conjecture in terms of p-curvature)**.** *For a differential operator $\mathscr{L}$ as in equation* (25)*, the following properties are equivalent:*

(1) *$\mathscr{L}$ has a full basis of algebraic solutions;*
(2) *For almost all primes p, the p-curvature of $\mathscr{L}_p$ vanishes;*
(3) *For almost all primes p, $\mathscr{L}_p$ divides ∂_x^p in the ring of differential operators $\mathbb{F}_p(x)\langle\partial_x\rangle$.*

3.3. Progresses toward Grothendieck's conjecture.

3.3.1. *A known case: The generalized hypergeometric equations.* It is in general very difficult to determine whether a given differential equation has a full basis of algebraic solutions. In their celebrated work [10], Beukers and Heckman managed to do this for an important class of differential equations, omnipresent in the mathematical and physical literature, namely the *generalized hypergeometric equations*. In fact, Beukers and Heckman extended the Landau–Errera criterion mentioned in Section 2.1.3. Let $\mathbf{a} = (a_1, \dots, a_{s+1})$ and $\mathbf{b} = (b_1, \dots, b_s, b_{s+1} = 1)$ be two $(s+1)$-tuples of rational parameters, assumed disjoint modulo $\mathbb{Z}$. This assumption is equivalent to the irreducibility in $\mathbb{Q}(x)\langle\partial\rangle$ of the "generalized hypergeometric operator" defined by

$$\mathscr{H}(\mathbf{a}, \mathbf{b}) := (x\partial_x + b_1 - 1) \cdots (x\partial_x + b_s - 1)x\partial_x - x(x\partial_x + a_1) \cdots (x\partial_x + a_{s+1}).$$

It is easy to check that $\mathscr{H}(\mathbf{a}, \mathbf{b})$ admits in its solution space the generalized hypergeometric function ${}_{s+1}F_s([a_1, \dots, a_{s+1}], [b_1, \dots, b_s]; x)$ defined in (13). The Beukers–Heckman result then reads as follows.

Theorem 3.23 ("interlacing criterion", Beukers–Heckman, [10])**.** *Given two $(s+1)$-tuples of rational numbers $\mathbf{a} = (a_1, \dots, a_{s+1})$ and $\mathbf{b} = (b_1, \dots, b_s, b_{s+1} = 1)$, assumed to be disjoint modulo $\mathbb{Z}$, let D be the common denominator of their elements. Then, the following assertions are equivalent:*

(1) *The hypergeometric function ${}_{s+1}F_s([a_1, \dots, a_{s+1}], [b_1, \dots, b_s]; x)$ is algebraic;*
(2) *The operator $\mathscr{H}(\mathbf{a}, \mathbf{b})$ admits a full basis of algebraic solutions;*
(3) *For all $1 \leq \ell < D$ with $\gcd(\ell, D) = 1$ the $(s+1)$-tuples $(e^{2\pi i \ell a_j})_{1 \leq j \leq s+1}$ and $(e^{2\pi i \ell b_j})_{1 \leq j \leq s+1}$ interlace on the unit circle.*

The interlacing condition mentioned in the latter result is defined as follows. We say that two $(s+1)$-tuples $(u_j)_{1 \leq j \leq s+1}$ and $(v_j)_{1 \leq j \leq s+1}$ of elements of the unit circle interlace if, up to renumbering the u_j and the v_j, we have $u_1 = e^{2\pi i \alpha_1}, \dots, u_{s+1} = e^{2\pi i \alpha_{s+1}}$ and $v_1 = e^{2\pi i \beta_1}, \dots, v_{s+1} = e^{2\pi i \beta_{s+1}}$ with either

$$0 \leq \alpha_1 < \beta_1 < \alpha_2 < \beta_2 \leq \cdots < \alpha_{s+1} < \beta_{s+1} < 1$$

or

$$0 \leq \beta_1 < \alpha_1 < \beta_2 < \alpha_2 \leq \cdots < \beta_{s+1} < \alpha_{s+1} < 1.$$

Example 3.24. The Beukers–Heckman criterion immediately implies that the operator $\mathscr{H}(\mathbf{a},\mathbf{b})$ admits a full basis of algebraic solutions for the choice

$$\mathbf{a} = \left\{\frac{1}{30}, \frac{7}{30}, \frac{11}{30}, \frac{13}{30}, \frac{17}{30}, \frac{19}{30}, \frac{23}{30}, \frac{29}{30}\right\}, \quad \mathbf{b} = \left\{\frac{1}{5}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{4}{5}, 1\right\}.$$

This proves in particular a beautiful observation due to Fernando Rodriguez-Villegas, namely that the generating function $\sum_{n\geq 0} u_n x^n$ of the sequence

$$u_n := \frac{(30n)!n!}{(15n)!(10n)!(6n)!}$$

(used by Chebyshev in his work on estimates for the prime counting function) is algebraic.

Note that without the irreducibility assumption on $\mathscr{H}(\mathbf{a},\mathbf{b})$, the situation is much more subtle. For instance, ${}_2F_1([1/2,1/3],[3/2];x)$ is transcendental, while ${}_2F_1([3/2,1/3],[1/2];x)$ is algebraic. In a recent work by Fürnsinn and Yurkevich [51], a generalization of Theorem 3.23 is given, which allows us to decide algebraicity/transcendence of arbitrary generalized hypergeometric functions (with potentially irrational parameters).

In addition to Theorem 3.23, Beukers and Heckman also drew up in [10] the list of generalized hypergeometric equations having a full basis of algebraic solutions, thus extending Schwarz's classification of algebraic ${}_2F_1$ [76].

On the other hand, a calculation due to Katz in [57, Section 5.5] (also in [56, Section 6] for the specific case of ${}_2F_1$) shows that this list coincides with the list of generalized hypergeometric equations whose reductions modulo p have a full basis of rational solutions for almost all primes p, in accordance with Grothendieck's conjecture.

3.3.2. *State of the art on Grothendieck's conjecture.* Besides for first-order equations and for generalized hypergeometric equations, Grothendieck's conjecture has been proved in several particular cases.

On the one hand, for Picard–Fuchs differential equations (satisfied by periods of a family of smooth algebraic varieties), and more generally for certain direct factors, Grothendieck's conjecture was established by Katz [56]. As an application, Katz gave in [57, Theorem 5.5.3] a new proof of the aforementioned results of Beukers and Heckman [10] about the generalized hypergeometric equations. Katz [56, Section 1], and later André [5, Section III], related the p-curvatures to the reduction modulo p of the *Kodaira–Spencer map.* (See also Foucault [48] and Foucault and Toffin [49] for explicit computations for families of curves of genus 2 and 3.) As explained in [5, p. 108], this approach has a potential for delivering effective versions of Grothendieck's conjecture, similar to effective versions of Chebotarev's density theorem [63, 77]: the hope is to obtain, for instance, for any Picard–Fuchs operator $\mathscr{L}$, an integer $N(\mathscr{L})$ such that the fact that $\mathscr{L}$ has a full basis of algebraic solutions can be read on the p-curvatures of $\mathscr{L}$ for the primes $p < N(\mathscr{L})$.

On the other hand, an arithmetic approach to Grothendieck's conjecture was introduced by the Chudnovsky brothers [35] who proved Grothendieck's conjecture for any rank one linear homogeneous differential equation over an algebraic curve [35, Theorem 8.1] (the case of first order equations over $\mathbb{P}^1$ had been proved by Honda in [53, Section 1, see Theorem 3.6]). They also proved Grothendieck's conjecture for the class of Lamé equations [35, Theorem 7.2], of the form

$$p(x)y''(x) + \frac{1}{2}p'(x)y'(x) - \big(n(n+1)x + B\big)\cdot y(x) = 0$$

where $n \in \mathbb{N}$, $B \in \mathbb{Q}$ and $p(x) \in \mathbb{Q}[x]$ has degree 3. The arithmetic approach was extended by André to the case when the differential Galois group has a solvable neutral component [5] (see also [3], [4, Chapter VIII], [12, Theorem 2.9] and [29, Theorem 3.5]).

Katz [55] proposed a conjectural description of the differential Galois group in terms of p-curvatures and he proved that his conjecture is equivalent to the initial conjecture by Grothendieck.

Using the language of schemes and sheaves, Grothendieck's conjecture can be formulated more generally for differential equations over any algebraic smooth curve defined over a number field. In [5, Remark 7.1.4], André noticed that, using Belyi maps, one can reduce the general case to that of the curve $X = \mathbb{P}^1 \backslash \{0, 1, \infty\}$. In our setting, this means that one can safely assume that the differential operator $\mathscr{L}$ has only singularities at 0, 1, and ∞. Under this additional assumption, Tang [83] proves that if *all*[3] the p-curvatures of $\mathscr{L}$ vanish, then $\mathscr{L}$ has a full basis of *rational* solutions. Although this latter result differs from Grothendieck's in the hypotheses (which are stronger) and the conclusion (which is also stronger), it is closely related.

We also point out the work of Bost in [12] giving an algebraicity criterion for leaves of algebraic foliations defined over number fields. For additional details, we refer to [29]. We mention the work of van der Put in [85] concerned with inhomogeneous equations of order 1. Other special cases of the conjecture have been proven recently, see [44, 71, 79]. Last but not least, an analogue of Grothendieck's conjecture for q-difference equations was conjectured by Bézivin [11, Section 5] and proved by Di Vizio in [37].

3.4. **A formal parallel with Kronecker's theorem.** It is instructive to observe that Grothendieck's conjecture appears to be, in some sense, a differential version of Kronecker's theorem we have already encountered earlier (see Theorem 3.7). Indeed, Kronecker's theorem can be reformulated as follows.

Theorem 3.25. *For a separable polynomial $L \in \mathbb{Q}[x]$, the following conditions are equivalent:*

(1) *All the roots of L are in $\mathbb{Q}$;*
(2) *For almost all primes p, all the roots of L mod p are in $\mathbb{F}_p$;*
(3) *For almost all primes p, we have $X^p \equiv X \pmod{L, p}$.*

It is striking that the three conditions of Theorem 3.25 are formal analogues of the conditions of Conjecture 3.17, at least if we admit that algebraic solutions in the differential case correspond to rational solutions in the algebraic case. Besides, the fact that the condition $X^p \equiv X \pmod{L, p}$ translates to $\partial_x^p \equiv 0 \pmod{\mathscr{L}, p}$, i.e., that the right-hand side shifts from X to 0 is explained by the fact that the classical Frobenius map behaves "multiplicatively" (it belongs naturally to some Galois group) while the p-curvature behaves "additively" (it belongs naturally to some Lie algebra).

[3] When $\mathscr{L}$ does not reduce properly at a prime p, the p-curvature of $\mathscr{L}_p$ is *a priori* not defined; however Tang manages to give an alternative definition of the vanishing of the p-curvature, see [83, Definition 2.1.7].

In the classical setting, Kronecker's theorem is obtained as a corollary of Chebotarev's density theorem, which is itself proved by means of Artin's L-functions. Unfortunately, similar tools do not seem to be available so far in the differential context; developing them might then sound like an exciting project.

As mentioned above, Honda proved that the Grothendieck conjecture for first-order differential equations is equivalent to Kronecker's theorem. In [35, Section 4], the Chudnovsky brothers gave an elementary (although "extravagant") proof of these equivalent statements; their approach is based on Hermite's explicit Hermite–Padé approximants to binomial functions. More precisely, they proved that if $y'(x) = \frac{x}{\alpha} y(x)$ has zero p-curvature for almost all primes p, then for all primes ideals $\mathfrak{P}$ of $\mathbb{Q}(\alpha)$ all the binomial coefficients $\binom{\alpha}{n}$ are $\mathfrak{P}$-integral for all n. From there, it is shown that Hermite–Padé approximants to $1, x^\alpha, \dots, x^{(m-1)\alpha}$ at $x = 1$ with weights $(N, \dots, N)$ are trivial for large m and N. This in turn implies that $1, x^\alpha, \dots, x^{(m-1)\alpha}$ are linearly dependent over $\mathbb{Q}(x)$, that is, x^α is an algebraic function, which is equivalent to $\alpha \in \mathbb{Q}$.

4. About the computation of the p-curvature

After Cartier's lemma (Theorem 3.19) and Grothendieck's conjecture (Conjecture 3.17), it is clear that the p-curvature is an invariant of primary importance of linear differential equations in characteristic p. In this section, we outline some algorithms for computing it (or other quantities associated to it) efficiently.

4.1. **Operators of order 1.**

In the case of differential equations of order 1 of the form (22)

$$y' + b(x)y = 0$$

we have seen in Theorem 3.12 that the p-curvature is explicitly given by the formula

$$b_p(x) = b^{(p-1)}(x) + b(x)^p.$$

Furthermore, explicitly computing the latter is quite an easy task which directly reduces to writing down the partial fraction decomposition of $b(x)$. Indeed, we have seen that if $b(x)$ decomposes as

$$b(x) = P(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\alpha_{i,j}}{(x-a_i)^j}$$

then

$$b_p(x) = P^{(p-1)}(x) + P(x)^p - \sum_{i=1}^{m} \sum_{\substack{1 \le j \le r_i \\ j \equiv 1 \bmod p}} \frac{\alpha_{i,j}}{(x-a_i)^{j+p-1}} + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\alpha_{i,j}^p}{(x-a_i)^{pj}}.$$

Importantly for algorithmic purposes, we observe that the size of $b_p(x)$ is roughly the same as the size of the input $b(x)$, although the degree of (the numerator and the denominator of) the former is p times larger the degree of the latter. This apparent contradiction is explained by the fact that $b_p(x)$ is actually a function of x^p; it is then a sparse rational function, in the sense that a large proportion of its coefficients vanish.

Remark 4.1. Another option for explicitly computing the p-curvature of differential operators of order 1 is presented in [23, Theorem 2]; it avoids the computation of partial fraction decomposition and the factorization of the denominator of $b(x)$. Let us briefly sketch it with the differential operator

$$\partial_x - \frac{1}{x^2+1}$$

of Example 3.4. We write $b(x) = -1/(x^2+1)$ and assume $p > 2$ for simplicity. In order to compute $b_p(x)$, we expand $b(x)$ in power series:

$$b(x) = -\sum_{n=0}^{\infty} (-1)^n x^{2n}.$$

The $(p-1)$-st derivative of x^{2n} is 0 when $2n \not\equiv -1 \pmod p$, and it is $-x^{2n-p+2}$ otherwise thanks to Wilson's theorem. Writing $2n = p-1+pk$ and noticing that k has to be even, $k = 2\ell$, we end up with

$$b^{(p-1)}(x) = -\sum_{\ell=0}^{\infty} (-1)^{\ell - \frac{p-1}{2}} x^{2\ell p}.$$

On the other hand, it is clear that $b(x)^p = -\sum_{n=0}^{\infty} (-1)^n x^{2np}$. Adding both sums, we find

$$b_p(x) = -\sum_{n=0}^{\infty} (-1)^n \cdot \left(1 - (-1)^{\frac{p-1}{2}}\right) \cdot x^{2np}.$$

When $p \equiv 1 \pmod 4$, the exponent $\frac{p-1}{2}$ is even and the term in the parenthesis vanishes. Therefore $b_p(x) = 0$ in this case. On the contrary, when $p \equiv 3 \pmod 4$, we have

$$b_p(x) = -2 \cdot \sum_{n=0}^{\infty} (-1)^n \cdot x^{2np} = -\frac{2}{1+x^{2p}} = -\frac{2}{(1+x^2)^p},$$

and we recover the result of Example 3.14.

The same idea applies to any differential operator $\mathscr{L} = \partial_x - b(x)$. Indeed, as we already noticed, its p-curvature is a rational function in x^p. Besides, it is of the form $f(x^p)/\mathrm{denom}(b(x))^p$, where $f(x)$ is a polynomial of degree at most $d = \deg(b(x))$. Hence, it is enough to determine the power series expansion of $(b(x)^{(p-1)})^{1/p}$ at precision x^d, starting from the power series expansion of $b(x)$ at the same precision d. If $b(x) = \sum_{n\geq 0} u_n x^n$, then by Wilson's theorem we have $(b(x)^{(p-1)})^{1/p} = -\sum_{n\geq 1} u_{np-1} x^{n-1}$, and hence it is enough to be able to compute the terms $u_{p-1}, \dots, u_{dp-1}$. Since $b(x)$ is a rational function, the sequence $(u_n)_{n\geq 0}$ satisfies a linear recursion of order at most d, with coefficients in $\mathbb{F}_p$ (given by the coefficients of $\mathrm{denom}(b)$). As the Nth term of such a linear recurrence with *constant* coefficients can be computed using $O(d \log(d) \log(N))$ operations in $\mathbb{F}_p$ using the technique of *binary powering* combined with fast polynomial multiplication in $\mathbb{F}_p[x]$, we conclude that the p-curvature $b_p(x)$ can be computed by an algorithm that uses $O(d^2 \log(d) \log(p))$ operations in $\mathbb{F}_p$.

Note that the reasoning above shows that the p-curvature $b_p(x)$ of $\mathscr{L} = \partial_x - b(x)$ is zero if and only if the following infinite systems of congruences hold

$$u_n \equiv u_{(n+1)p-1} \pmod p \quad \text{for all } n \geq 0.$$

4.2. **Reading the p-curvature on the solutions.** For differential equations of higher orders, the sparsity of the p-curvature no longer holds in general. However, we have the following result.

Proposition 4.2. *Let*

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

with $b_i(x) \in \mathbb{F}_p(x)$ and let $B(x)$ be the associated companion matrix (see equation (27)). Let $f(x) \in \mathbb{F}_p[x]$ be a common denominator of the $b_i(x)$ and

$$d = \max\big(\deg f(x),\, \deg(f(x)b_0(x)),\, \ldots,\, \deg(f(x)b_{n-1}(x))\big).$$

Let $B_p(x)$ be the matrix of the p-curvature of $\mathscr{L}$ defined by the recurrence (28). *Then, the following holds.*

(i) *The matrix $B_p(x)$ has the form $\frac{1}{f(x)^p}C_p(x)$ where the entries of $C_p(x)$ are all polynomials of degree at most dp.*
(ii) *The matrix $B_p(x)$ is similar to a matrix with coefficients in $\mathbb{F}_p(x^p)$.*

The first assertion of the proposition follows easily from the induction formula (28) (see [23, Lemma 1]). Assertion (ii) is more subtle and requires the construction of a differential extension of $\mathbb{F}_p(x)$ over which $\mathscr{L}$ has a full basis of solutions. We refer to [41, Proposition 2.1.2] for a detailed proof.

Besides, we notice that (ii) implies that the trace, the determinant of $B_p(x)$ and, more generally, all the coefficients of its characteristic polynomial lie in $\mathbb{F}_p(x^p)$. This latter statement can be also seen as a consequence of the following easy lemma: the determinant of a linear mapping $\mathbb{F}_p(x)^n \to \mathbb{F}_p(x)^n$ commuting with

$$\nabla : F \mapsto F' + B(x)F$$

has zero derivative. This alternative proof has the advantage to avoid going to an extension. We derive from what precedes that the sizes of the coefficients of the characteristic polynomial of $B_p(x)$ are comparable to the sizes of the $b_i(x)$, although the size of the p-curvature itself is, in general, p times larger.

In order to design fast algorithms for computing the p-curvature, it is useful to go beyond Cartier's lemma (see Theorem 3.19) and relate the p-curvature to the shape of solutions. Let

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

be a differential operator as before. In Section 3.2, we have seen that, when the p-curvature of $\mathscr{L}$ vanishes and the $b_i(x)$ have no pole at 0, a fundamental system of solutions of $\mathscr{L}$ is explicitly given by

$$\sum_{k=0}^{p-1}(-1)^k B_k(x)\frac{x^k}{k!}$$

where the $B_k(x)$ are the matrices defined by the recurrence (28). In full generality, i.e., without assuming the vanishing of B_p, the idea is to consider the formal expansion

$$\sum_{k=0}^{\infty}(-1)^k B_k(x)\frac{x^k}{k!}.$$

Of course, this does not make sense in $\mathbb{F}_p(x)$ because of the division by $k!$, but we shall see that it does make sense in a suitable ring. A natural idea to achieve this goal is to introduce divided powers, i.e., to consider the ring of *Hurwitz series*, denoted by $\mathbb{F}_p[[x]]^{\mathrm{dp}}$, whose elements are formal series of the form

$$a_0 + a_1\gamma_1(x) + a_2\gamma_2(x) + \cdots + a_k\gamma_k(x) + \cdots .$$

In the above expression, the $\gamma_k(x)$ are formal names without further additional meaning. Of course, they should be thought of as $\frac{x^k}{k!}$ but we cannot write this division because the denominator may vanish. The multiplication on $\mathbb{F}_p[[x]]^{\mathrm{dp}}$ is governed by the rule

$$\gamma_m(x) \cdot \gamma_n(x) = \binom{m+n}{m} \cdot \gamma_{n+m}(x)$$

for any nonnegative integers m and n. Besides, $\mathbb{F}_p[[x]]^{\mathrm{dp}}$ is equipped with a natural derivation that takes $\sum_k a_k\gamma_k(x)$ to $\sum_k a_{k+1}\gamma_k(x)$. We have to be careful, however, that $\mathbb{F}_p[[x]]^{\mathrm{dp}}$ is not a domain (e.g., $\gamma_1(x)^p = 0$) and, because of that, we cannot consider its ring of fractions. But still, if the matrix $B(x)$ has polynomial coefficients, all the $B_k(x)$ have the same property and we can consider their image $B_k^{\mathrm{dp}}(x)$ is the ring $M_n\big(\mathbb{F}_p[[x]]^{\mathrm{dp}}\big)$. We then can form

$$S^{\mathrm{dp}}(x) = \sum_{k=0}^{\infty} (-1)^k B_k^{\mathrm{dp}}(x) \cdot \gamma_k(x), \tag{29}$$

obtaining this way a fundamental matrix of solutions of $\mathscr{L}$ over $\mathbb{F}_p[[x]]^{\mathrm{dp}}$. This construction works more generally as soon as the entries of $B(x)$ have no pole at 0: in this case, we can expand them as series in x in order to view them in $\mathbb{F}_p[[x]]^{\mathrm{dp}}$. The precise relation between $S^{\mathrm{dp}}(x)$ and the p-curvature is given by Lemma 4.3.

Lemma 4.3 (Bostan, Caruso, and Schost [15])**.** *We have the matrix relation:*

$$\frac{d^p S^{\mathrm{dp}}(x)}{dx^p} = -B_p^{\mathrm{dp}}(x) \cdot S^{\mathrm{dp}}(x).$$

Proof. Set $M = \mathbb{F}_p[x]$ and let $\Delta : M^n \to M^n, Y \mapsto \frac{dY}{dx} + B(x)Y$. By definition of the p-curvature, Δ^p is the multiplication by $B_p(x)$.

Now consider the endomorphism Δ^{dp} of $M^{\mathrm{dp}} = \mathbb{F}_p[[x]]^{\mathrm{dp}} \otimes_{\mathbb{F}_p[x]} M$ defined by

$$\Delta^{\mathrm{dp}} = \frac{d}{dx} \otimes \mathrm{id}_M + 1 \otimes \Delta_M.$$

One checks that it satisfies the Leibniz rule: for $f \in \mathbb{F}_p[[x]]^{\mathrm{dp}}$ and $m \in M$, we have

$$\Delta^{\mathrm{dp}}(f \otimes m) = \frac{df}{dx} \otimes m + f \otimes \Delta(m).$$

Hence, raising it to the pth power, we obtain

$$(\Delta^{\mathrm{dp}})^p(Y^{\mathrm{dp}}) = \frac{d^p Y^{\mathrm{dp}}}{dx^p} + B_p^{\mathrm{dp}}(x) \cdot Y^{\mathrm{dp}}$$

for all vectors $Y^{\mathrm{dp}} \in M^{\mathrm{dp}}$. The equality of the lemma follows given that the columns of $S^{\mathrm{dp}}(x)$ map to 0 under Δ^{dp}. ☐

Remark 4.4. Hurwitz series provide a framework in which the Picard–Lindelöf (or, Cauchy–Lipschitz) theorem holds for linear differential equations in characteristic p. The recent article [50] provides another construction allowing this theorem, which has the advantage of yielding an integral domain but which, in return, does not seem so directly linked to the p-curvature.

4.3. **Application to algorithmics.** Given that the matrix $S^{\mathrm{dp}}(x)$ is invertible, it follows from Lemma 4.3 that one can deduce the value of $B_p^{\mathrm{dp}}(x)$ from that of $S^{\mathrm{dp}}(x)$ which, in turn, can be computed using the techniques of [17]. However, at this point, we have not solved the question of the computation of the p-curvature entirely for two reasons. Firstly, the previous reasoning assumes implicitly that the coefficients $b_i(x)$ have no pole at 0. Secondly, and more importantly, the knowledge of $B_p^{\mathrm{dp}}(x)$ is not enough to recover B_p. Precisely by letting $\mathbb{F}_p(x)_0$ denote the subring of $\mathbb{F}_p(x)$ consisting of functions with no pole at 0, the natural map $\delta_0 : \mathbb{F}_p(x)_0 \to \mathbb{F}_p[[x]]^{\mathrm{dp}}$ is not injective; its kernel is the ideal generated by x^p.

To tackle these issues, the idea is to shift around any other base point $a \in \mathbb{F}_p$. Doing so, we get a new differential ring homomorphism $\delta_a : \mathbb{F}_p(x)_a \to \mathbb{F}_p[[x-a]]^{\mathrm{dp}}$ and, reusing the same techniques, we end up with a fast algorithm that computes the p-curvature B_p modulo $(x-a)^p$. Since we have at our disposal *a priori* bounds on the size of the p-curvature (see Proposition 4.2), one can pick enough elements a in $\mathbb{F}_p$ (or in a finite extension of $\mathbb{F}_p$, if needed), to compute the p-curvature modulo $(x-a)^p$ for all those points a and reconstruct the complete matrix $B_p(x)$ using the Chinese remainder theorem. Implementing this strategy, we end up with the following theorem.

Theorem 4.5 (Bostan, Caruso, and Schost [15]). *There exists an algorithm that takes as input a differential operator*

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

over $\mathbb{F}_p(x)$ and outputs its p-curvature for a cost of $O^{\sim}(dn^\omega p)$ operations in $\mathbb{F}_p$ with

$$d = \max\big(\deg f(x),\, \deg(f(x)b_0(x)),\, \ldots,\, \deg(f(x)b_{n-1}(x))\big)$$

where $f(x)$ is a common denominator of the $b_i(x)$.

Before commenting on the above result, we need to explain some notation. Firstly, the notation $O^{\sim}(-)$ means that we are hiding logarithmic factors. Secondly, the exponent ω refers to what we usually call a *feasible* exponent for the matrix multiplication. It simply means that we suppose that we are given an algorithm that computes the product of two square matrices of size n using at most $O(n^\omega)$ operations in the base field. The naive method for multiplying matrices (the one we have all learned in our first course of linear algebra) indicates that we can take $\omega = 3$. However, it turns out that better algorithms exist. For example, Strassen's algorithm [81] results in $\omega = \log_2 7 \approx 2.8$. Nowadays, the best known value for ω is about 2.37188 and the corresponding algorithm is due to Duan, Wu, and Zhou [39]. It is a widely open conjecture if one can take $\omega = 2+\varepsilon$ for all $\varepsilon > 0$.

The announced complexity $O^{\sim}(dn^\omega p)$ should be compared to the size of the output, i.e., the number of scalars in $\mathbb{F}_p$ needed to write down completely the p-curvature. By Proposition 4.2, B_p if an $n \times n$ matrix whose entries are rational functions with numerators and denominators of degree at most dp; in practice, this bound is, in general, sharp. Therefore, the size of the output is about dn^2p. As a consequence, the algorithm behind Theorem 4.5 would be quasi-optimal (i.e., optimal up to constant and logarithmic factors) if ω were equal to 2. Even if this limit cannot be attained, this comparison underlines the good performances of the algorithm. In practice, using it makes it possible to compute p-curvatures of operators of order and degree 20 in a few seconds when $p < 100$ and in about half an hour when $p = 12007$.

4.4. **Similarity class and characteristic polynomial.** We have seen previously (after Proposition 4.2) that, although the size of the p-curvature grows linearly with respect to p, its characteristic polynomial has roughly the same size as the input operator $\mathscr{L}$ even when p gets large. For this reason, one might hope to be able to compute the characteristic polynomial faster than the p-curvature itself.

The main observation for achieving this is a refinement of Lemma 4.3 which asserts that $B_p^{\mathrm{dp}}(x) = B_p(x) \bmod x^p$ is not only equal to

$$-(S^{\mathrm{dp}}(x))^{-1} \cdot \frac{d^p S^{\mathrm{dp}}(x)}{dx^p}$$

but it is further *similar* to the value at $x = 0$ (i.e., the reduction modulo x) of the latter product. On the other hand, evaluating this reduction can be done with standard algorithmic techniques (based on a "baby step/giant step" approach) in time proportional to $\sqrt{p}$. Based on this, we obtain the next theorem.

Theorem 4.6 (Bostan, Caruso, and Schost [16])**.** *There exists an algorithm that takes as input a differential operator*

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

over $\mathbb{F}_p(x)$ and outputs the invariant factors of its p-curvature for a cost of

$$O^{\sim}\big(d^{\omega+\frac{3}{2}} n^{\omega+1} \sqrt{p}\big)$$

operations in $\mathbb{F}_p$ where d is defined as in Theorem 4.5*.*

We notice that the knowledge of the invariant factors is finer than that of the characteristic polynomial since the latter is the product of the former. Furthermore, knowing the invariant factors, one can decide whether the p-curvature vanishes or not, whereas the characteristic polynomial only gives information about its nilpotency.

On the complexity side, we notice that the cost of the algorithm of Theorem 4.6 is worse with respect to the parameters d and n but better with respect to p. It is then interesting for small operators but large characteristic.

Finally, we mention that, if we are only interested by the characteristic polynomial of the p-curvature, faster algorithms (based on different techniques) exist.

Theorem 4.7 (Bostan, Caruso, and Schost [14])**.** *There exists an algorithm that takes as input a differential operator*

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

over $\mathbb{F}_p(x)$ and outputs the characteristic polynomial of its p-curvature for a cost of

$$O^{\sim}\big((d{+}n)^{\omega} \min(d,n)\sqrt{p} + (d{+}n)^{\omega+1} \min(d,n)\big)$$

operations in $\mathbb{F}_p$ where d is defined as in Theorem 4.5*.*

In practice, this algorithm performs quite well and allows for computing the characteristic polynomial in less than one hour for the parameters $d = n = 20$ and $p = 120\,011$.

Recently, Pagès proved an "average version" of this theorem which, roughly speaking, states that, starting with a differential operator over $\mathbb{Q}(x)$, one can compute all its p-curvatures (up to some given bound) in average time proportional to $\log p$.

Theorem 4.8 (Pagès [70]). *There exists an algorithm that takes as input a differential operator*

$$\mathscr{L} = b_n(x)\cdot\partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

with $b_i(x) \in \mathbb{Z}[x]$ and outputs the characteristic polynomial of all the p-curvatures of $\mathscr{L}$ mod p for $p \leq N$ for a cost of

$$O^{\sim}\big(\big((d+n)^{\omega}(d+m) + (d+n)^3\big) \cdot Nd\big)$$

operations on bits, where d is the maximal degree of the $b_i(x)$ and m is the maximal bitsize of an integer appearing as the coefficient of one of the $b_i(x)$.

5. Algebraicity and integrality

The theoretical developments we carried out in Section 4.2 also have interesting consequences in characteristic 0, as they allow us to relate algebraicity of solutions with the growth of denominators of the coefficients in their Taylor expansions. The aim of this section is to appetize the reader with some charming results and perspectives in this direction.

Throughout this section, we let

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

be a differential operator over $\mathbb{Q}(x)$ and assume that $b_i(x)$ has no pole at 0 for all i. We set:

$$S(x) = \sum_{k=0}^{\infty} (-1)^k B_k(x) \cdot \frac{x^k}{k!} \tag{30}$$

where the $B_k(x)$ are defined by equation (28). The matrix $S(x)$ has entries in $\mathbb{Q}[[x]]$ and we write $S(x) = \sum_{i=0}^{\infty} S_i x^i$ where the S_i are matrices over $\mathbb{Q}$. We emphasize that S_i is *not* equal to $\frac{(-1)^i}{i!} B_i(x)$ because the latter has in general coefficients in $\mathbb{Q}(x)$.

5.1. Growth of denominators and p-curvatures.

We would like to compare $S(x)$ with the matrix $S^{\mathrm{dp}}(x)$ introduced in equation (29) and, for this, to reduce everything ($\mathscr{L}$, $S(x)$, etc.) modulo a prime number p. However, this operation requires some care because the $B_k(x)$ may exhibit denominators. In order to do it properly, we introduce new rings. For any subring $R \subset \mathbb{Q}$, we set:

$$R(x) = \left\{ \frac{P}{Q} \quad \text{with} \quad P, Q \in R[x] \text{ and } Q \text{ monic} \right\},$$

$$R(x)_0 = \left\{ \frac{P}{Q} \quad \text{with} \quad P, Q \in R[x],\, Q \text{ monic and } Q(0) \neq 0 \right\},$$

$$R[[x]]^{\mathrm{dp}} = \left\{ \sum_{i=0}^{\infty} a_i \frac{x^i}{i!} \quad \text{with} \quad a_i \in R \text{ for all } i \right\}.$$

One has the following chain of inclusions $R[x] \subset R(x)_0 \subset R(x)$ together with an injective morphism of rings $R(x)_0 \hookrightarrow R[[x]]$. All these maps commute with the derivation $\frac{d}{dx}$ and, if p is a prime number which is noninvertible in R, they are compatible with the reduction modulo p; in particular, we have the following commutative diagram

$$\begin{array}{ccccc} R(x)_0 & \longrightarrow & R[[x]] & \longrightarrow & R[[x]]^{\mathrm{dp}} \\ \big\downarrow{\scriptstyle \bmod p} & & \big\downarrow{\scriptstyle \bmod p} & & \big\downarrow{\scriptstyle \bmod p} \\ \mathbb{F}_p(x)_0 & \longrightarrow & \mathbb{F}_p[[x]] & \longrightarrow & \mathbb{F}_p[[x]]^{\mathrm{dp}} \end{array}$$

where all the arrows are homomorphisms of rings and commute with the derivation. We now assume that the entries of $B(x)$ have no pole at 0 and choose R in such a way that they all belong to $R(x)_0$ (one can always take $R = \mathbb{Z}[\frac{1}{D}]$ for D large enough). All the $B_m(x)$ then take coefficients in $R(x)_0$ as well and the matrix $S(x)$ is defined over $R[[x]]^{\mathrm{dp}}$. The image of $S(x)$ modulo p is the matrix $S^{\mathrm{dp}}(x)$ modulo p associated to the differential system $Y' + (B(x) \bmod p) \cdot Y = 0$ in characteristic p. Lemma 4.3 then leaves us with the congruence:

$$S_p \equiv \frac{B_p(x)}{p!} \pmod{x}, \quad \text{i.e.} \quad S_p = \frac{B_p(0)}{p!}. \tag{31}$$

Hence the p-curvatures (which, we recall, are the matrices $B_p(x) \bmod p$) are directly related to the coefficients appearing in a fundamental system of solutions. In particular, the vanishing of $B_p(0)$ modulo p is equivalent to the fact that the denominator of S_p is coprime with p. Many variations on this theme are possible; a beautiful example is given by the following theorem.

Theorem 5.1 ([5, Proposition 5.3.3])**.** *Let*

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

be a differential operator over $\mathbb{Q}(x)$ and D be a positive integer. We assume that $\mathscr{L}$ admits n solutions $Y_1, \ldots, Y_n$ which have coordinates in $\mathbb{Z}[\frac{1}{D}][[x]]$ and are linearly independent over $\mathbb{Q}$. Then almost all the p-curvatures of $\mathscr{L}$ vanish.

Remark 5.2. Under Grothendieck's conjecture, Theorem 5.1 can be elegantly rephrased as follows: if a differential system admits a basis of solutions in $\mathbb{Z}[\frac{1}{D}][[x]]$ for some positive integer D (i.e., a basis of *globally bounded* solutions), then it also admits a basis of algebraic solutions. This is known as *Bézivin's conjecture*; it was formulated by Bézivin in [11, p. 299] and proved by him for q-differential equations [11, Theorem 7.1]; see also [34, Conjecture 6.3]. It is widely open whether Bézivin's conjecture is more difficult than Grothendieck's conjecture; at any rate, it appears that for the time being the only cases for which Bézivin's conjecture is proven are those for which Grothendieck's conjecture is known to be true.

Example 5.3. We illustrate Theorem 5.1 with the differential equation

$$y' = \frac{1}{x^2+1} y$$

already considered in Example 3.4. Over the rationals, the solutions are all proportional to the fundamental solution

$$y_0(x) = \exp(\arctan(x)) = \sum_{n=0}^{\infty} c_n x^n$$

where the c_n are rational numbers. We would like to find bounds on denominators of the c_n. More precisely, we fix a prime number $p \neq 2$ (for simplicity) and ask whether the denominators of the c_n are all coprime with p. For this, we use the following important result due to Dwork.

Theorem 5.4 (Dwork's criterion, [75, p. 409]). *Given a prime p and $f(x) \in x\mathbb{Q}[[x]]$, we have $\exp(f(x)) \in 1+x\mathbb{Z}_{(p)}[[x]]$ if and only if $f(x^p)-pf(x) \in px\mathbb{Z}_{(p)}[[x]]$, where $\mathbb{Z}_{(p)}$ is the subring of $\mathbb{Q}$ consisting of fractions $\frac{a}{b}$ with b coprime with p.*

According to Dwork's criterion, the denominators of the c_n are all coprime with p if and only if

$$\arctan(x^p) - p \cdot \arctan(x) \in p\mathbb{Z}_{(p)}[[x]].$$

We have:

$$\arctan(x^p) - p \cdot \arctan(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{(2n+1)p} - p \cdot \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{(2n+1)}. \tag{32}$$

Clearly, when $2n+1$ is coprime with p, the coefficient $p \cdot \frac{(-1)^n}{2n+1}$ is divisible by p. Therefore, we can only retain in the second sum of equation (32) the terms for which $2n \equiv -1 \pmod{p}$, i.e., $2n = p - 1 + 2\ell p$ with $\ell \in \mathbb{N}$. We thus get:

$$\begin{aligned} &\arctan(x^p) - p \cdot \arctan(x) \\ &\quad \equiv \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{(2n+1)p} - \sum_{\ell=0}^{\infty} \frac{(-1)^{\ell - \frac{p-1}{2}}}{2\ell+1} x^{(2\ell+1)p} \\ &\quad = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} \cdot \left(1 - (-1)^{\frac{p-1}{2}}\right) \cdot x^{(2n+1)p} \pmod{p\mathbb{Z}_{(p)}[[x]]}, \end{aligned}$$

hence $\arctan(x^p) - p \cdot \arctan(x)$ is divisible by p when $p \equiv 1 \bmod 4$ and is not otherwise. In conclusion, the denominators of the c_n are all coprime with p (that is, $\exp(\arctan(x))$ can be reduced modulo p) if and only if $p \equiv 1 \bmod 4$.

Remark 5.5. Note that the sequence $(T_n)_{n\geq 0}$ defined by $T_n = n! \cdot c_n$, satisfies the linear recurrence $T_{n+2} = T_{n+1} - n(n+1)T_n$ with $T_0 = T_1 = 1$, hence its terms are all integer numbers. Kelinsky proved in [61, Theorem 3] that for any prime $p \neq 2$, the term T_p is congruent to 0 modulo p if $p \equiv 1 \bmod 4$ (and to 2 if $p \equiv 3 \bmod 4$). The computation in Example 5.3 provides a new proof of this statement: if $p \equiv 1 \bmod 4$, then T_n is congruent to 0 modulo p for all $n \geq p$, in other terms the generating function $\sum_{n\geq 0} T_n x^n$ is a *polynomial* modulo p.

In the same orbit, we mention two other theorems which are not directly related to our discussion but highlight other intricate relations between algebraicity and integrality.

Theorem 5.6 (Conjectured by Ogus [69], proved by André [4]). *Let $f(x) \in \mathbb{Z}[[x]]$ such that $f'(x)$ is algebraic over $\mathbb{Q}(x)$. Then $f(x)$ is algebraic over $\mathbb{Q}(x)$.*

Theorem 5.7 (Conjectured by Katz [56], proved by the Chudnovsky–Chudnovsky [35]). *Let $f(x) \in \mathbb{Z}[[x]]$ such that $f'(x)/f(x)$ is algebraic over $\mathbb{Q}(x)$. Then $f(x)$ is algebraic over $\mathbb{Q}(x)$.*

5.2. **An analytic perspective on the p-curvature.** All that precedes indicates that the vanishing properties of the p-curvatures tend to control the growth of the denominators of the coefficients of the fundamental system of solutions $S(x)$. Typically, after equation (31), we have seen that $B_p(0) \equiv 0 \pmod{p}$ is equivalent to the fact that p does not divide the smallest common denominator of the entries of S_p.

It is convenient to reformulate this class of properties in terms of p-adic valuation and p-adic numbers. We recall that the p-adic valuation of an integer n, denoted by $v_p(n)$, is the greatest integer v such that p^v divides n. We then define the p-adic valuation of a rational number $x = \frac{a}{b}$ by setting $v_p(x) = v_p(a) - v_p(b)$. Having a denominator coprime with p is then equivalent to having nonnegative p-adic valuation. If M is a matrix over $\mathbb{Q}$, we define $v_p(M)$ as the minimum of the p-valuations of its entries.

Recall that, for all nonnegative integer i, we have

$$v_p(i!) = \sum_{n=1}^{\infty} \left\lfloor \frac{i}{p^n} \right\rfloor \leq \frac{i}{p-1}$$

(where $\lfloor \cdot \rfloor$ is the floor function). Hence, if $S(x)$ is defined over $\mathbb{Z}[\frac{1}{D}][[x]]$ and p is a prime number which does not divide N, we deduce from the very first definition of $S(x)$ (see equation (30)) that $v_p(S_i) \geq -v_p(i!) \geq \frac{-i}{p-1}$ for all i. On the other hand, the property we have recalled above indicates that $B_p(0) \equiv 0 \pmod p$ if and only if $v_p(S_p) \geq 0$. It turns out actually that the vanishing of the p-curvature implies a general lower bound on the p-adic valuation of the S_i.

Proposition 5.8. *Let*

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x)$$

be a differential operator over $\mathbb{Q}(x)$ *and let* S *be the matrix defined by equation* (30)*. If the reduction of* $\mathscr{L}$ *modulo* p *is well defined and if the* p*-curvature of* $\mathscr{L}$ mod p *vanishes, then for all* $i \geq 0$*:*

$$v_p(S_i) \geq -v_p\big(\lfloor i/p \rfloor !\big) \geq \frac{-i}{p(p-1)}. \tag{33}$$

Proposition 5.8 can be further rephrased in more analytic terms using p-adic numbers. We recall briefly that the field of p-adic numbers is the completion of $\mathbb{Q}$ for the p-adic norm $\|\cdot\|_p$ defined by $\|x\|_p = p^{-v_p(x)}$. Set $\omega = p^{-1/(p-1)}$. Without any assumption on the p-curvature, we have seen that $v_p(S_i) \geq \frac{-i}{p-1}$, that is $\|S_i\|_p \leq \omega^{-i}$. This upper bound indicates that the (p-adic) radius of convergence of the series $S(x) = \sum_{i=0}^{\infty} S_i x^i$ is at least ω. On the contrary, when the p-curvature vanishes, Proposition 5.8 tells us that $\|S_i\|_p \leq \omega^{-i/p}$ for all i. Hence, the radius of convergence of S is now at least $\omega^{1/p} > \omega$. The p-curvature then measures some analytic properties of the solutions of our differential system in the p-adic world. A classical result in the theory of p-adic differential equations [60, Theorem 10.4.2], refining the *Frobenius antecedent theorem* of Christol and Dwork [33, Theorem 5.4] (see also [59, Theorem 6.15]), asserts that when the radius of convergence of a fundamental system of solutions is strictly greater than ω, the corresponding differential system $Y'(x) + B(x)Y(x) = 0$ is equivalent, up to a base change, to a system of the form $Y'(x^p) + C(x^p)Y(x^p) = 0$ where the entries of $C(x)$ are p-adic analytic functions converging on the closed unit disk. The differential system

$$(\Sigma_1) : Y' + C(x)Y = 0$$

is called a *Frobenius antecedent* of (Σ). The aforementioned convergence conditions allow for reducing (Σ_1) modulo p, thus obtaining a new differential system on $\mathbb{F}_p(x)$.

The latter has a well-defined p-curvature and if this second p-curvature persists to vanish, one eventually deduces that the radius of convergence of S is at least ω^{1/p^2}. When this occurs, one can continue this process and find a second Frobenius antecedent (Σ_2) of (Σ). If its p-curvature vanishes, the radius of convergence of S will be at least ω^{1/p^3} and so on and so forth.

In the perspective of the Grothendieck conjecture, we would like to let p vary and understand how the aforementioned convergence properties interact. A promising object, which looks capable of reflecting these interactions is the *Berkovich line over* $\mathbb{Z}$, which was anticipated by Berkovich himself in [6] and then developed by Poineau [72]. By definition, it is the space $\mathcal{M}(\mathbb{Z}[x])$ consisting of all *bounded multiplicative semi-norms* $\|\cdot\| : \mathbb{Z}[x] \to \mathbb{R}$. A semi-norm is a norm except that we authorize nonzero elements to have norm zero. It is said multiplicative if $\|fg\| = \|f\| \cdot \|g\|$ for all $f, g \in \mathbb{Z}[x]$ and bounded when

$$\|a_0 + a_1 x + \cdots + a_n x^n\| \leq \max\left(|a_0|, |a_1|, \ldots, |a_n|\right),$$

where $|a_i|$ denotes the usual absolute value of a_i. Of course, the Berkovich line $\mathcal{M}(\mathbb{Z}[x])$ is not only a set but is endowed with a rich additional geometrical structure: a topology, a structural sheaf, etc. After Poineau's work, we have at our disposal a whole panel of powerful tools (inspired by modern algebraic geometry) to work with.

Describing the space $\mathcal{M}(\mathbb{Z}[x])$ is not obvious, but it is not difficult to exhibit elements in it. Take $K = \mathbb{R}$ or $\mathbb{Q}_p$ (the field of p-adic numbers) for some prime number p and write $\|\cdot\|_K$ for the standard absolute value of K. Additionally, pick an element $a \in K$ of norm at most 1 and a nonnegative real number r. Polynomials in $\mathbb{Z}[x]$ then define (real or p-adic) analytic functions on the closed ball $B(a, r)$ of center a and radius r. For $f \in \mathbb{Z}[x]$, we can then consider the sup norm on this domain:

$$\|f\|_{a,r} = \sup_{x \in B(a,r)} \|f(x)\|_K.$$

One checks that it is an element of $\mathcal{M}(\mathbb{Z}[x])$. Moreover, at least in the p-adic case, the completion of $\mathbb{Z}[x]$ with respect to this norm is the ring of p-adic analytic functions on $B(a, r)$; we shall denote it by $\mathcal{A}_{a,r}$ in what follows. Another nice observation is that the notion of "ball of center a and radius r" has a well-defined meaning in the Berkovich geometry. Indeed, let $\mathcal{M}(\mathcal{A}_{a,r})$ be the Berkovich space associated to the ring $\mathcal{A}_{a,r}$, i.e., the set of bounded multiplicative semi-norms on $\mathcal{A}_{a,r}$. Restricting a semi-norm from $\mathcal{A}_{a,r}$ to $\mathbb{Z}[x]$ leaves us with an injective map

$$\mathcal{M}(\mathcal{A}_{a,r}) \hookrightarrow \mathcal{M}(\mathbb{Z}[x])$$

whose image, denoted by $U_{a,r}$, is an open subset (for the Berkovich topology) in $\mathcal{M}(\mathbb{Z}[x])$. In addition, we observe that any analytic function f on $B(a, r)$, that is any element $f \in \mathcal{A}_{a,r}$, induces a function on $U_{a,r}$: to each semi-norm $\|\cdot\| \in \mathcal{M}(\mathcal{A}_{a,r})$, we associate $\|f\|$. For this reason, it is natural to think at $U_{a,r}$ as the Berkovich incarnation of the ball of center a and radius r.

Coming back to our topic, let us consider a differential system $(\Sigma) : Y' + A(x)Y = 0$ over $\mathbb{Z}[x]$. By what we have seen previously, for almost all prime numbers p and all $a \in \mathbb{Z}_p$, the system (Σ) admits a full basis of solutions in $\mathcal{A}_{a,\omega}$ where we recall that we have set $\omega = p^{-1/(p-1)}$. In the Berkovich language, these functions give rise to new functions defined on $U_{a,\omega}$. Putting them together, we conclude that (Σ) always admits a basis of solutions on a certain open subspace $U_0 \subset \mathcal{M}(\mathbb{Z}[x])$. Now, the assumption that almost all the p-curvatures vanish shows that those solutions extend automatically to a larger subspace $U_1 \subset \mathcal{M}(\mathbb{Z}[x])$. On the other hand, in the Berkovich language, proving the Grothendieck conjecture amounts to showing that there exist a full basis of solution on an étale covering of $\mathcal{M}(\mathbb{Z}[x])$. Of course, these remarks do not give any proof of the Grothendieck conjecture because U_1 itself is certainly *not* an étale covering of $\mathcal{M}(\mathbb{Z}[x])$. However, we think that this point of view has the potential to lead to new interesting developments towards the Grothendieck conjecture in the future.

Acknowledgments

We are very grateful to Herwig Hauser for the initial idea of this survey, for his constant support along the various phases of the project, and for the marvelous workshops he organized in Lisbon these last years, from which the three authors benefited a lot. Our warm thanks go to Florian Fürnsinn, Mark van Hoeij and Sergey Yurkevich for their careful reading and helpful comments.

References

[1] B. Adamczewski and T. Rivoal, *Exceptional values of E-functions at algebraic points*, Bull. Lond. Math. Soc. **50** (2018), no. 4, 697–708, DOI 10.1112/blms.12168. MR3870952

[2] G. Almkvist and D. Zeilberger, *The method of differentiating under the integral sign*, J. Symbolic Comput. **10** (1990), no. 6, 571–591, DOI 10.1016/S0747-7171(08)80159-9. MR1087980

[3] Y. André, *Quatre descriptions des groupes de Galois différentiels* (French), Séminaire d'algèbre Paul Dubreil et Marie-Paule Malliavin (Paris, 1986), Lecture Notes in Math., vol. 1296, Springer, Berlin, 1987, pp. 28–41, DOI 10.1007/BFb0078522. MR932051

[4] Y. André, *G-functions and geometry*, Aspects of Mathematics, E13, Friedr. Vieweg & Sohn, Braunschweig, 1989, DOI 10.1007/978-3-663-14108-2. MR990016

[5] Y. André. Sur la conjecture des p-courbures de Grothendieck-Katz et un problème de Dwork. In *Geometric aspects of Dwork theory. Vol. I, II*, pages 55–112. Walter de Gruyter, Berlin, 2004.

[6] V. G. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs, vol. 33, American Mathematical Society, Providence, RI, 1990, DOI 10.1090/surv/033. MR1070709

[7] E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859, DOI 10.1002/j.1538-7305.1967.tb03174.x. MR219231

[8] O. Bernardi, M. Bousquet-Mélou, and K. Raschel, *Counting quadrant walks via Tutte's invariant method*, Comb. Theory **1** (2021), Paper No. 3, 77, DOI 10.5070/C61055360. MR4396208

[9] M. Bertola, B. Dubrovin, and D. Yang, *Simple Lie algebras and topological ODEs*, Int. Math. Res. Not. IMRN **5** (2018), 1368–1410, DOI 10.1093/imrn/rnw285. MR3801466

[10] F. Beukers and G. Heckman, *Monodromy for the hypergeometric function* ${}_nF_{n-1}$, Invent. Math. **95** (1989), no. 2, 325–354, DOI 10.1007/BF01393900. MR974906

[11] J.-P. Bézivin, *Les suites q-récurrentes linéaires* (French), Compositio Math. **80** (1991), no. 3, 285–307. MR1134257

[12] J.-B. Bost, *Algebraic leaves of algebraic foliations over number fields* (English, with English and French summaries), Publ. Math. Inst. Hautes Études Sci. **93** (2001), 161–221, DOI 10.1007/s10240-001-8191-3. MR1863738

[13] A. Bostan, *Computer algebra in the service of enumerative combinatorics*, ISSAC '21—Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation, ACM, New York, [2021] ©2021, pp. 1–8, DOI 10.1145/3452143.3465507. MR4398758

[14] A. Bostan, X. Caruso, and É. Schost, *A fast algorithm for computing the characteristic polynomial of the p-curvature*, ISSAC 2014—Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2014, pp. 59–66, DOI 10.1145/2608628.2608650. MR3239909

[15] A. Bostan, X. Caruso, and É. Schost, *A fast algorithm for computing the p-curvature*, ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2015, pp. 69–76. MR3388284

[16] A. Bostan, X. Caruso, and É. Schost, *Computation of the similarity class of the p-curvature*, Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2016, pp. 111–118, DOI 10.1145/2930889.2930897. MR3565704

[17] A. Bostan, F. Chyzak, F. Ollivier, B. Salvy, É. Schost, and A. Sedoglavic, *Fast computation of power series solutions of systems of differential equations*, Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, ACM, New York, 2007, pp. 1012–1021. MR2485252

[18] A. Bostan, F. Chyzak, M. van Hoeij, M. Kauers, and L. Pech, *Hypergeometric expressions for generating functions of walks with small steps in the quarter plane*, European J. Combin. **61** (2017), 242–275, DOI 10.1016/j.ejc.2016.10.010. MR3588720

[19] A. Bostan and M. Kauers, *The complete generating function for Gessel walks is algebraic*, Proc. Amer. Math. Soc. **138** (2010), no. 9, 3063–3078, DOI 10.1090/S0002-9939-2010-10398-2. With an appendix by Mark van Hoeij. MR2653931

[20] A. Bostan, I. Kurkova, and K. Raschel, *A human proof of Gessel's lattice path conjecture*, Trans. Amer. Math. Soc. **369** (2017), no. 2, 1365–1393, DOI 10.1090/tran/6804. MR3572277

[21] A. Bostan, T. Rivoal, and B. Salvy, *Minimization of differential equations and algebraic values of E-functions*, Math. Comp. **93** (2024), no. 347, 1427–1472, DOI 10.1090/mcom/3912. MR4709207

[22] A. Bostan, B. Salvy, and M. Singer, *On deciding transcendence of power series*, In preparation.

[23] A. Bostan and É. Schost, *Fast algorithms for differential equations in positive characteristic*, ISSAC 2009—Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2009, pp. 47–54, DOI 10.1145/1576702.1576712. MR2742690

[24] A. Bostan and S. Yurkevich, *On a class of hypergeometric diagonals*, Proc. Amer. Math. Soc. **150** (2022), no. 3, 1071–1087, DOI 10.1090/proc/15693. MR4375704

[25] M. Bousquet-Mélou, *Rational and algebraic series in combinatorial enumeration*, International Congress of Mathematicians. Vol. III, Eur. Math. Soc., Zürich, 2006, pp. 789–826. MR2275707

[26] M. Bousquet-Mélou, *An elementary solution of Gessel's walks in the quadrant*, Adv. Math. **303** (2016), 1171–1189, DOI 10.1016/j.aim.2016.08.038. MR3552547

[27] M. Bousquet-Mélou and M. Mishna, *Walks with small steps in the quarter plane*, Algorithmic probability and combinatorics, Contemp. Math., vol. 520, Amer. Math. Soc., Providence, RI, 2010, pp. 1–39, DOI 10.1090/conm/520/10252. MR2681853

[28] T. Budd, *Winding of simple walks on the square lattice*, J. Combin. Theory Ser. A **172** (2020), 105191, 59, DOI 10.1016/j.jcta.2019.105191. MR4046317

[29] A. Chambert-Loir, *Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. & G. Chudnovsky)* (French, with French summary), Astérisque **282** (2002), Exp. No. 886, viii, 175–209. Séminaire Bourbaki, Vol. 2000/2001. MR1975179

[30] G. Christol. Fonctions hypergéométriques bornées. *Groupe de travail d'analyse ultramétrique*, 14, 1986-1987. Talk:8.

[31] G. Christol, *Diagonales de fractions rationnelles* (French), Séminaire de Théorie des Nombres, Paris 1986–87, Progr. Math., vol. 75, Birkhäuser Boston, Boston, MA, 1988, pp. 65–90. MR990506

[32] G. Christol, *Globally bounded solutions of differential equations*, Analytic number theory (Tokyo, 1988), Lecture Notes in Math., vol. 1434, Springer, Berlin, 1990, pp. 45–64, DOI 10.1007/BFb0097124. MR1071744

[33] G. Christol and B. Dwork, *Modules différentiels sur des couronnes* (French, with English and French summaries), Ann. Inst. Fourier (Grenoble) **44** (1994), no. 3, 663–701. MR1303881

[34] G. Christol, *Solutions algébriques des équations différentielles p-adiques* (French), Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Progr. Math., vol. 38, Birkhäuser Boston, Boston, MA, 1983, pp. 51–58. MR0729159

[35] D. V. Chudnovsky and G. V. Chudnovsky, *Applications of Padé approximations to the Grothendieck conjecture on linear differential equations*, Number theory (New York, 1983), Lecture Notes in Math., vol. 1135, Springer, Berlin, 1985, pp. 52–100, DOI 10.1007/BFb0074601. MR803350

[36] O. Cormier, M. F. Singer, B. M. Trager, and F. Ulmer, *Linear differential operators for polynomial equations*, J. Symbolic Comput. **34** (2002), no. 5, 355–398, DOI 10.1006/jsco.2002.0564. MR1937466

[37] L. Di Vizio, *Arithmetic theory of q-difference equations: the q-analogue of Grothendieck-Katz's conjecture on p-curvatures*, Invent. Math. **150** (2002), no. 3, 517–578, DOI 10.1007/s00222-002-0241-z. MR1946552

[38] T. Dreyfus, C. Hardouin, J. Roques, and M. F. Singer, *On the nature of the generating series of walks in the quarter plane*, Invent. Math. **213** (2018), no. 1, 139–203, DOI 10.1007/s00222-018-0787-z. MR3815564

[39] R. Duan, H. Wu, and R. Zhou, *Faster matrix multiplication via asymmetric hashing*, 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS), IEEE Computer Soc., Los Alamitos, CA, [2023] ©2023, pp. 2129–2138, DOI 10.1109/FOCS57990.2023.00130. MR4720372

[40] B. Dubrovin, D. Yang, and D. Zagier, *Geometry and arithmetic of integrable hierarchies of KdV type. I. Integrality*, Adv. Math. **433** (2023), Paper No. 109311, 73, DOI 10.1016/j.aim.2023.109311. MR4650621

[41] B. Dwork, *Differential operators with nilpotent p-curvature*, Amer. J. Math. **112** (1990), no. 5, 749–786, DOI 10.2307/2374806. MR1073008

[42] A. Errera. Zahlentheoretische Lösung einer functionentheoretischen Frage. *Rend. Circ. Mat. Palermo*, **35**:107–144, 1913.

[43] L. Euler, *Specimen de constructione aequationum differentialium sime indeterminatarum separatione*, Commentarii academiae scientiarum Petropolitanae, **6**:168–174. 1733.

[44] B. Farb and M. Kisin, *Rigidity, locally symmetric varieties, and the Grothendieck-Katz conjecture*, Int. Math. Res. Not. IMRN **22** (2009), 4159–4167, DOI 10.1093/imrn/rnp082. MR2552299

[45] G. Fayolle, R. Iasnogorodski, and V. Malyshev, *Random walks in the quarter-plane*, Applications of Mathematics (New York), vol. 40, Springer-Verlag, Berlin, 1999. Algebraic methods, boundary value problems and applications, DOI 10.1007/978-3-642-60001-2. MR1691900

[46] P. Flajolet, *Analytic models and ambiguity of context-free languages*, Theoret. Comput. Sci. **49** (1987), no. 2-3, 283–309, DOI 10.1016/0304-3975(87)90011-9. Twelfth international colloquium on automata, languages and programming (Nafplion, 1985). MR909335

[47] P. Flajolet and R. Sedgewick, *Analytic combinatorics*, Cambridge University Press, Cambridge, 2009, DOI 10.1017/CBO9780511801655. MR2483235

[48] F. Foucault, *Équations de Picard-Fuchs et invariants des courbes de genre* 2 (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 8, 617–619. MR1158748

[49] F. Foucault and P. Toffin, *Courbes hyperelliptiques de genre trois et application de Kodaira-Spencer* (French, with English and French summaries), C. R. Math. Acad. Sci. Paris **345** (2007), no. 12, 685–687, DOI 10.1016/j.crma.2007.10.030. MR2376639

[50] F. Fürnsinn and H. Hauser, *Fuchs' theorem on linear differential equations in arbitrary characteristic*, Preprint, `arXiv:2307.01712`, (2023).

[51] F. Fürnsinn and S. Yurkevich, *Algebraicity of hypergeometric functions with arbitrary parameters*, Bull. Lond. Math. Soc., 23 pages, in print, `https://doi.org/10.1112/blms.13103` (2024).

[52] H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra **7** (1967), 271–277, DOI 10.1016/0021-8693(67)90061-0. MR215820

[53] T. Honda, *Algebraic differential equations*, Symposia Mathematica, Vol. XXIV (Sympos., INDAM, Rome, 1979), Academic Press, London-New York, 1981, pp. 169–204. MR619247

[54] N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), no. 2, 206–224, DOI 10.2307/1989656. MR1501922

[55] N. M. Katz, *A conjecture in the arithmetic theory of differential equations* (English, with French summary), Bull. Soc. Math. France **110** (1982), no. 2, 203–239. MR0667751

[56] N. M. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Invent. Math. **18** (1972), 1–118, DOI 10.1007/BF01389714. MR337959

[57] N. M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, Princeton, NJ, 1990, DOI 10.1515/9781400882434. MR1081536

[58] M. Kauers, C. Koutschan, and D. Zeilberger, *Proof of Ira Gessel's lattice path conjecture*, Proc. Natl. Acad. Sci. USA **106** (2009), no. 28, 11502–11505, DOI 10.1073/pnas.0901678106. MR2538821

[59] K. S. Kedlaya, *Local monodromy of p-adic differential equations: an overview*, Int. J. Number Theory **1** (2005), no. 1, 109–154, DOI 10.1142/S179304210500008X. MR2172335

[60] K. S. Kedlaya, *p-adic differential equations*, Cambridge Studies in Advanced Mathematics, vol. 125, Cambridge University Press, Cambridge, 2010, DOI 10.1017/CBO9780511750922. MR2663480

[61] R. Kelisky, *The numbers generated by* exp(arctan x), Duke Math. J. **26** (1959), 569–581. MR109229

[62] J. J. Kovacic, *An algorithm for solving second order linear homogeneous differential equations*, J. Symbolic Comput. **2** (1986), no. 1, 3–43, DOI 10.1016/S0747-7171(86)80010-4. MR839134

[63] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London-New York, 1977, pp. 409–464. MR447191

[64] E. Landau, *Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gaussschen Differentialgleichung* (German), J. Reine Angew. Math. **127** (1904), 92–102, DOI 10.1515/crll.1904.127.92. MR1580634

[65] E. Landau. Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe. *Sitzungsber. Heidelb. Akad. Wiss. Math.-Natur. Kl.*, 18:3–38, 1911.

[66] L. Lipshitz, *The diagonal of a D-finite power series is D-finite*, J. Algebra **113** (1988), no. 2, 373–378, DOI 10.1016/0021-8693(88)90166-4. MR929767

[67] S. Melczer, *Algorithmic and symbolic combinatorics—an invitation to analytic combinatorics in several variables*, Texts and Monographs in Symbolic Computation, Springer, Cham, [2021] ©2021. With a foreword by Robin Pemantle and Mark Wilson, DOI 10.1007/978-3-030-67080-1. MR4241372

[68] H. Niederreiter, *A new efficient factorization algorithm for polynomials over small finite fields*, Appl. Algebra Engrg. Comm. Comput. **4** (1993), no. 2, 81–87, DOI 10.1007/BF01386831. MR1223850

[69] P. Deligne, J. S. Milne, A. Ogus, and K.-y. Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982. MR654325

[70] R. Pagès, *Computing characteristic polynomials of p-curvatures in average polynomial time*, ISSAC '21—Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation, ACM, New York, [2021] ©2021, pp. 329–336, DOI 10.1145/3452143.3465524. MR4398801

[71] A. Patel, A. N. Shankar, and J. P. Whang, *The rank two p-curvature conjecture on generic curves*, Adv. Math. **386** (2021), Paper No. 107800, 33, DOI 10.1016/j.aim.2021.107800. MR4270046

[72] J. Poineau, *La droite de Berkovich sur* $\mathbf{Z}$ (French, with English and French summaries), Astérisque **334** (2010), viii+xii+284. MR2759805

[73] G. Pólya, *Sur les séries entières, dont la somme est une fonction algébrique*, Enseign. Math., **22**:38–47, 1921/1922.

[74] E. G. C. Poole, *Introduction to the theory of linear differential equations*, Dover Publications, Inc., New York, 1960. MR111886

[75] A. M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000, DOI 10.1007/978-1-4757-3254-2. MR1760253

[76] H. A. Schwarz, *Ueber diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt* (German), J. Reine Angew. Math. **75** (1873), 292–335, DOI 10.1515/crll.1873.75.292. MR1579568

[77] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev* (French), Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR644559

[78] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440, DOI 10.1090/S0273-0979-03-00992-3. MR1997347

[79] A. N. Shankar, *The p-curvature conjecture and monodromy around simple closed loops*, Duke Math. J. **167** (2018), no. 10, 1951–1980, DOI 10.1215/00127094-2018-0008. MR3827814

[80] M. F. Singer, *Algebraic solutions of nth order linear differential equations*, Proceedings of the Queen's Number Theory Conference, 1979 (Kingston, Ont., 1979), Queen's Papers in Pure and Appl. Math., vol. 54, Queen's Univ., Kingston, ON, 1980, pp. 379–420. MR634699

[81] V. Strassen, *Gaussian elimination is not optimal*, Numer. Math. **13** (1969), 354–356, DOI 10.1007/BF02165411. MR248973

[82] E. Stridsberg. Sur le théorème d'Eisenstein et l'équation différentielle de Gauss. *Ark. Mat. Astron. Fys.*, 6(35):1–17, 1911.

[83] Y. Tang, *Algebraic solutions of differential equations over* $\mathbb{P}^1 - \{0, 1, \infty\}$, Int. J. Number Theory **14** (2018), no. 5, 1427–1457, DOI 10.1142/S1793042118500884. MR3806314

[84] M. van der Put, *Reduction modulo p of differential equations*, Indag. Math. (N.S.) **7** (1996), no. 3, 367–387, DOI 10.1016/0019-3577(96)83726-8. MR1621401

[85] M. van der Put, *Grothendieck's conjecture for the Risch equation* $y' = ay + b$, Indag. Math. (N.S.) **12** (2001), no. 1, 113–124, DOI 10.1016/S0019-3577(01)80009-4. MR1908143

[86] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 328, Springer-Verlag, Berlin, 2003, DOI 10.1007/978-3-642-55750-7. MR1960772

[87] D. Vargas-Montoya, *Algébricité modulo p, séries hypergéométriques et structures de Frobenius fortes* (French, with English and French summaries), Bull. Soc. Math. France **149** (2021), no. 3, 439–477, DOI 10.24033/bsmf.2834. MR4349570

[88] S. Yurkevich. The art of algorithmic guessing in gfun. *Maple Trans.*, 2(1):14421:1–14421:19, 2022.

[89] D. Zagier, *The arithmetic and topology of differential equations*, European Congress of Mathematics, Eur. Math. Soc., Zürich, 2018, pp. 717–776. MR3890449

Inria, Université Paris-Saclay, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France

URL: https://mathexp.eu/bostan/

CNRS; Université de Bordeaux, IMB; Inria Bordeaux Sud-Ouest, CANARI, 351 cours de la Libération, 33405 Talence, France

URL: https://xavier.caruso.ovh

Universite Claude Bernard Lyon 1, CNRS, Ecole Centrale de Lyon, INSA Lyon, Université Jean Monnet, ICJ UMR5208, 69622 Villeurbanne, France

URL: http://math.univ-lyon1.fr/~roques/