



ANNALES

DE

L'INSTITUT FOURIER

Alexandru BUIUM & Santiago R. SIMANCA

Arithmetic differential equations in several variables

Tome 59, n° 7 (2009), p. 2685-2708.

http://aif.cedram.org/item?id=AIF_2009__59_7_2685_0

© Association des Annales de l'institut Fourier, 2009, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

ARITHMETIC DIFFERENTIAL EQUATIONS IN SEVERAL VARIABLES

by Alexandru BUIUM & Santiago R. SIMANCA (*)

ABSTRACT. — We survey recent work on arithmetic analogues of ordinary and partial differential equations.

RÉSUMÉ. — On présente des résultats récents sur les analogues arithmétiques des équations différentielles ordinaires et aux dérivées partielles.

1. Introduction

In this paper, we survey some of the basic ideas, results, and applications of the theory of *arithmetic ordinary differential equations* [6, 7, 8, 9, 11], and we explain how some of these ideas can be extended to the case of *arithmetic partial differential equations* [13, 14, 15, 12].

1.1. Classical analogies between functions and numbers

The analogies between functions and numbers played a key role in the development of modern number theory. The most elementary example of such an analogy is that between the ring $\mathbb{C}[x]$ of polynomial functions with complex coefficients and the ring \mathbb{Z} of integers. In $\mathbb{C}[x]$, any non-constant polynomial is, in a unique way, a product of linear factors (the fundamental theorem of algebra), whereas in \mathbb{Z} , any number different from $-1, 0, 1$ is, in a unique way and up to a sign, a product of prime numbers (the

Keywords: Differential equations, elliptic curves, p -adic numbers, modular forms.

Math. classification: 11G07, 35G20, 11F03.

(*) During the preparation of this work, the first author was partially supported by NSF grant DMS 0552314.

fundamental theorem of arithmetic). This makes the primes in \mathbb{Z} the analogues of the linear polynomials in $\mathbb{C}[x]$, and the set $\{-1, 0, 1\}$ in \mathbb{Z} the analogue of the field \mathbb{C} of constant polynomials in $\mathbb{C}[x]$. This analogy runs deeper. Indeed the finite extensions of the field $\mathbb{C}(x)$ of rational functions, called function fields, correspond to complex algebraic curves and should be viewed as analogues of number fields, which are the finite extensions of the field \mathbb{Q} of rational numbers. The fundamental groups $\pi_1(X)$ of complex algebraic curves X have, as arithmetic analogues, the absolute Galois groups $G(F^a/F)$ of number fields F . The divisor class groups $Cl(X)$ of complex algebraic curves have, as arithmetic analogues, the divisor class groups $Cl(F)$ of the rings of integers in number fields. The intersection theory on complex algebraic surfaces fibered over curves has, as an arithmetic analogue, the Arakelov intersection theory on curves over number fields. Cohomology of foliated spaces has a conjectural arithmetic analogue proposed by Deninger [16]. All of these examples of analogies are in some sense at the level of algebraic topology. But we could ask if the analogies between functions and numbers manifest themselves at other levels as well, such as that of differential calculus and differential equations, for instance.

1.2. Arithmetic analogue of differential equations

Going back to the analogy between the polynomial ring $\mathbb{C}[x]$ and the integers \mathbb{Z} , we may ask for an analogue of differential calculus and ordinary differential equations in which the derivative operator $\partial_x := \frac{d}{dx} : \mathbb{C}[x] \rightarrow \mathbb{C}[x]$ with respect to x is replaced by an appropriate operator $\delta_p : \mathbb{Z} \rightarrow \mathbb{Z}$ playing the role of “derivative with respect to (a fixed prime) p .” Such a theory was proposed by the first author in [6], where δ_p was taken to be the *Fermat quotient operator*

$$(1.1) \quad \begin{array}{ccc} \mathbb{Z} & \xrightarrow{\delta_p} & \mathbb{Z} \\ n & \longmapsto & \delta_p n := \frac{n - n^p}{p} . \end{array}$$

Notice that for p odd, we have that $\delta_p n = 0$ if, and only if, $n \in \{-1, 0, 1\}$; this is consistent with the idea that $\{-1, 0, 1\}$ plays the role of “set of constants” in \mathbb{Z} .

The theory in [6] was further developed by the first author in a series of papers (*cf.* the monograph [9] for an account of this). Several purely number theoretic applications of this theory have been found, such as

- (1) an effective uniform bound for the number of torsion points on curves over number fields [7],
- (2) results on congruences of classical modular forms [8, 1, 20, 12],
- (3) finiteness results for points on elliptic curves arising from special points on modular and Shimura curves [10, 11].

With this theory in place, we could ask for a generalization to the partial differential case. Starting all over again with our prototypical analogy between $\mathbb{C}[x]$ and \mathbb{Z} , we could ask for the arithmetic analogue of the ring of polynomials $\mathbb{C}[x_1, x_2] \simeq \mathbb{C}[x] \otimes_{\mathbb{C}} \mathbb{C}[x]$ in two variables. According to the “myth of the field \mathbb{F}_1 with one element” (cf. [28, 24, 2, 16] and the bibliographies therein), the analogue of $\mathbb{C}[x_1, x_2]$ should be a ring of the form “ $\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$.” The question of considering the latter is very worthwhile. Indeed, one possible approach to the proof of the Riemann hypothesis could be to imitate Weil’s proof of its analogue for curves X over finite fields, such as \mathbb{F}_p ; Weil’s proof is based on the analysis of the two-fold product $X \times_{\mathbb{F}_p} X$ and hence has in its background the ring $\mathbb{F}_p[x_1, x_2]$. This would make the search for “ $\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$ ” significant.

A different viewpoint on the two variable theory was suggested in [15]. Instead of viewing the elusive “ $\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$ ” as an analogue of $\mathbb{C}[x_1, x_2]$, the authors proposed to look at the triple $(\mathbb{Z}, \delta_{p_1}, \delta_{p_2})$ as an analogue of $(\mathbb{C}[x_1, x_2], \partial_{x_1}, \partial_{x_2})$, where $\partial_{x_i} := \frac{\partial}{\partial x_i}$, $i = 1, 2$, and

$$(1.2) \quad \begin{array}{ccc} \mathbb{Z} & \xrightarrow{\delta_{p_1}, \delta_{p_2}} & \mathbb{Z} \\ n & \longmapsto & \begin{array}{l} \delta_{p_1} n := \frac{n - n^{p_1}}{p_1}, \\ \delta_{p_2} n := \frac{n - n^{p_2}}{p_2}. \end{array} \end{array}$$

This is consistent with a suggestion of J. Borger to see geometry over lambda rings as the possible incarnation of the geometry over \mathbb{F}_1 ; cf. also the first author’s suggestion, in the “one prime case,” in the Introduction of [9]. For the theory of lambda rings and the related theory of Witt rings we refer to [19, 21, 30, 2, 3].

There is yet another way of extending the ordinary theory to the partial differential case; cf. [13, 14]. In this approach, the analogue of $(\mathbb{C}[x_1, x_2], \partial_{x_1},$

∂_{x_2}) is the triple $(\mathbb{Z}[q], \delta_p, \delta_q)$, where $\mathbb{Z}[q]$ is a polynomial ring in the indeterminate q , and

$$(1.3) \quad \begin{array}{ccc} \mathbb{Z}[q] & \xrightarrow{\delta_p, \delta_q} & \mathbb{Z}[q] \\ \sum a_n q^n & \longmapsto & \begin{aligned} \delta_p(\sum a_n q^n) &:= \frac{(\sum a_n q^{pn}) - (\sum a_n q^n)^p}{p}, \\ \delta_q(\sum a_n q^n) &:= q \frac{d}{dq} \left(\sum a_n q^n \right) = \sum n a_n q^n. \end{aligned} \end{array}$$

We shall refer to the cases (1.1), (1.2), (1.3) above as the cases of $0 + 1$, $0 + 2$, and $1 + 1$ variables, respectively. More generally, all of these cases are subsumed by the case of $d_1 + d_2$ variables, where d_1 is the number of arithmetic variables and d_2 is the number of geometric variables; cf. section 2.2. Here, the variables we refer to are the independent variables; in our discussion below, besides these, there will be yet another dimensional parameter, the number of dependent variables appearing in our differential equations.

Before going any further, it is worth stressing the important point that the paradigm of arithmetic differential equations that we are going to explain here is quite different from the paradigm of Dwork’s theory of differential equations over p -adic fields [17]. The easiest way to understand the difference between the two theories is to look at the ordinary case. In Dwork’s theory of ordinary differential equations, the solutions to the equations are functions $u = u(x)$ (usually p -adic analytic functions $u : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ or, more generally, $u : \mathbb{C}_p \rightarrow \mathbb{C}_p$), and the operator applied to them is the usual derivation operator $u \mapsto \partial_x u = \frac{du}{dx}$. In the theory of arithmetic differential equations (which we are explaining here), the solutions to the equations are numbers (typically p -adic numbers $a \in \mathbb{Z}_p$ or, more generally, $a \in \widehat{\mathbb{Z}}_p^{ur}$, cf. our discussion later in the paper), and the operator applied to them is a Fermat quotient operator $a \mapsto \delta_p a$. In spite of this fundamental difference between these two paradigms, some crystalline aspects of Dwork’s theory do play a role in our theory, as tools in some of our proofs.

1.3. Plan of the paper

In §2, we start by reviewing the framework of jet spaces in differential, analytic, and algebraic geometry. We then proceed to define the arithmetic analogues of these spaces; cf. [6, 9] for the ordinary case. In §3, 4, and 5, we examine the main results in the case of $0 + 1$ variables [6, 9], $0 + 2$ variables [15], and $1 + 1$ variables [13]. In §6, we explain some difficulties in extending the theory to the case of $1 + 2$ variables.

2. Main concepts

2.1. Classical differential equations

For a (smooth, analytic, or algebraic) manifold M , we denote by $\mathcal{O}(M)$ the ring of complex valued (smooth, analytic, or algebraic) functions on M . Here, smooth manifolds are assumed to be real, while analytic and algebraic manifolds are assumed to be complex. Given a submersion $M \rightarrow N$ of (smooth, analytic, or algebraic) manifolds with $\dim N = d$, $\dim M = d + d'$, let us assume, for simplicity, that we have global (smooth, analytic, or étale) coordinates x on N and (x, y) on M , such that the submersion mapping $M \rightarrow N$ is given by $(x, y) \mapsto x$. Here $x = (x_1, \dots, x_d)$, $y = (y_1, \dots, y_{d'})$, where we view d as the number of *independent* variables, and we view d' as the number of *dependent* variables. We can consider jet spaces $J^r(M/N)$ of various orders $r = (r_1, \dots, r_d) \in \mathbb{Z}_{\geq 0}^d$, with local coordinates

$$\{x, \partial^s y : s \leq r\},$$

where $\partial^s := \partial_{x_1}^{s_1} \dots \partial_{x_d}^{s_d}$, $s = (s_1, \dots, s_d)$, and $s \leq r$ means that $s_i \leq r_i$ for all i . A classical differential equation on M of order r is, by definition, a (smooth, analytic, or algebraic) function on $J^r(M/N)$, that is to say, an element of $\mathcal{O}(J^r(M/N))$. In the smooth or analytic case, and in the coordinates above, a differential equation is simply a (smooth or analytic) function

$$f(x, \partial^s y).$$

For each i , $1 \leq i \leq d$, we have an operator

$$(2.1) \quad \delta_{x_i} : \mathcal{O}(J^r(M/N)) \rightarrow \mathcal{O}(J^{r+e_i}(M/N)),$$

where $e_i = (0, \dots, 1, \dots, 0)$ with the 1 on the i -th component; by definition, in coordinates,

$$\delta_{x_i} := \frac{\partial}{\partial x_i} + \sum_{s,j} (\partial^{s+e_i} y_j) \frac{\partial}{\partial (\partial^s y_j)}.$$

Let $M(N)$ denote the set of all (smooth, analytic, or algebraic) sections of $M \rightarrow N$. Any differential equation $f \in \mathcal{O}(J^r(M/N))$ induces a map of sets, still denoted by f ,

$$f : M(N) \rightarrow \mathcal{O}(N),$$

which can be referred to as the (nonlinear) *partial differential operator* attached to f . The sections in $M(N)$ sent by f to 0 are interpreted as the

“solutions of $f = 0$.” In the smooth or analytic case, sections are given by functions $x \mapsto (x, u(x))$, and the map $M(N) \rightarrow \mathcal{O}(N)$ is given by

$$u = u(x) \mapsto fu = f(x, \partial^s(u(x))).$$

There is a less refined, more familiar version of the above formalism in which, for $n \in \mathbb{Z}_{\geq 0}$, we consider the jet spaces $J^n(M/N)$ of order n , with local coordinates

$$\{x, \partial^s y : |s| \leq n\},$$

where $|s| := s_1 + \cdots + s_d$.

The constructions above can be globalized appropriately. Then the main problems that arise in the theory are

- (1) the classification of all differential equations (possibly invariant under various group actions on M “over N ”), and
- (2) the description, for any such an equation f , of the space of solutions of $f = 0$.

For the latter problem, we may hope to parameterize solutions by Cauchy data along a given non-characteristic submanifold. But of course, even if we start with smooth initial data, the solutions could develop singularities, and the theory is soon pushed into the non-smooth realm of distributions.

If $M \rightarrow N$ is a group in the category of manifolds over N (that is to say, there exists a multiplication $\mu : M \times_N M \rightarrow M$ with the expected properties) then, in the smooth or analytic case, the differential equation f will be called *linear* if for any open set $N' \subset N$, the induced nonlinear differential operator $f : M(N') \rightarrow \mathcal{O}(N')$ is a group homomorphism. (Here, $M(N')$ is the set of sections of $M \rightarrow N$ above N' and $\mathcal{O}(N')$ is viewed as a group with the usual addition of functions.) There is a corresponding definition in the algebraic case. In all cases, the solutions of $f = 0$ form a subgroup of $M(N)$. The most familiar case of this paradigm is that where M is a vector bundle over N ; in this case the linear differential equations in the sense above coincide with what is classically understood by *linear partial differential operators*. A subclass of these is constituted by the class of operators $u \mapsto Pu$ with constant coefficients. Among these, the standard examples are (in the case of $d = 2$ variables and order $n \leq 2$):

$$\begin{aligned}
 Pu &= \partial_{x_1} u - \partial_{x_2} u, & \text{the convection operator,} \\
 Pu &= \partial_{x_1} u - \partial_{x_2}^2 u, & \text{the heat operator,} \\
 Pu &= \partial_{x_1}^2 u - \partial_{x_2}^2 u, & \text{the wave operator,} \\
 Pu &= \partial_{x_1}^2 u + \partial_{x_2}^2 u, & \text{the Laplace operator.}
 \end{aligned}
 \tag{2.2}$$

Besides vector bundles, we can consider other groups M over N , such as multiplicative tori $M = N \times T \rightarrow N$ (where $T = \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times$), or families of compact complex tori $M \rightarrow N$ (for example, abelian varieties). In the case of families of abelian varieties, for instance, there is a fundamental construction of differential equations due to Manin [25], which played a key role in his proof of the function field analogue of the Mordell's conjecture. The case $d = d' = 1$ of this construction (which Manin attributes to Fuchs) says that if N is an affine algebraic curve (equipped with an étale coordinate x , to simplify), and $M \rightarrow N$ is a smooth projective morphism with a section whose fibers are elliptic curves, then there is a non-zero order 2 differential equation $\psi^2 \in \mathcal{O}(J^2(M/N))$ that is linear in the sense of our definition above. Here and below, an upper index in a differential equation, like the 2 in ψ^2 , indicates the order of the corresponding equation. (N.B. The expression for ψ^2 in the affine coordinates of the cubic defining the family of elliptic curves is far from being "linear" in the naive sense!) This differential equation ψ^2 is usually referred to as the *Manin map*. A different construction of such maps (including the higher dimensional case) was given in [4]. By the way, in the "degenerate" situation where $M = N \times E$ for E an elliptic curve, there is a natural order 1 differential equation $\psi^1 \in \mathcal{O}(J^1(M/N))$ given by the "logarithmic derivative." Of course, an analogue of the latter exists also in the case $M = N \times \mathbb{C}^\times$, where the corresponding differential equation $\psi^1 \in \mathcal{O}(J^1(M/N))$ induces the differential operator $\psi^1 : M(N) = \mathcal{O}(N)^\times \rightarrow \mathcal{O}(N)$ defined by $\psi^1 u = \partial_x u / u$. There are analogues of Manin maps (and of logarithmic derivatives) in the case of several (independent and dependent) variables. These can be used to construct analogues of the operators (2.2) for the corresponding groups $M \rightarrow N$.

Let us mention that there is a notion of linearity that is related to groups in a less obvious way; indeed, we can talk about linear partial differential operators on $M = N \times S$, where S is a modular curve or a Shimura curve (or, more generally, a moduli space of appropriate abelian varieties). Cf. [14]. We will not discuss this in the present paper.

In what follows, we would like to consider an arithmetic analogue of the theory above.

2.2. Arithmetic differential equations

Let $\mathcal{Q} = \{q_1, \dots, q_{d_1}\}$ be a set of indeterminates and $\mathcal{P} = \{p_1, \dots, p_{d_2}\}$ be a set of primes in \mathbb{Z} . The analogue of the manifold N in the previous section

is the scheme $\text{Spec } A$, where $A = \mathbb{Z}[q_1, \dots, q_{d_1}]$. Consider the operators $\delta_{\mathcal{P}} = \{\delta_{p_1}, \dots, \delta_{p_{d_2}}\}$ and $\delta_{\Omega} = \{\delta_{q_1}, \dots, \delta_{q_{d_1}}\}$ given by

(2.3)

$$\begin{aligned} \mathbb{Z}[q_1, \dots, q_{d_1}] &\xrightarrow{\delta_{p_i}, \delta_{q_j}} \mathbb{Z}[q_1, \dots, q_{d_1}] \\ \sum a_n q^n &\longmapsto \begin{aligned} \delta_{p_i}(\sum a_n q^n) &:= \frac{(\sum a_n q^{p_i n}) - (\sum a_n q^n)^{p_i}}{p_i}, \\ \delta_{q_j}(\sum a_n q^n) &:= q_j \frac{\partial}{\partial q_j} \left(\sum a_n q^n \right), \end{aligned} \end{aligned}$$

where d_1 is the number of *geometric variables* q_1, \dots, q_{d_1} , d_2 is the number of *arithmetic variables* p_1, \dots, p_{d_2} , and for a multi-index $n = (n_1, \dots, n_{d_1})$, we set $q^n := q_1^{n_1} \dots q_{d_1}^{n_{d_1}}$. We shall refer to the situation above as the case of $d_1 + d_2$ variables. From this perspective, the case of $d + 0$ variables can be referred to as the *purely geometric* case, and corresponds to the *classical* case of differential calculus in d variables. By the same token, the case of $0 + d$ variables can be referred to as the *purely arithmetic* case.

The analogue of the manifold M is any scheme of finite type X over A . The analogue of the set $M(N)$ of sections of $M \rightarrow N$ is the set $X(A)$ of A -points of the scheme X . Let us assume firstly that $X = \text{Spec } B$ is affine, with $B = A[y]/(f)$, y a tuple of variables and f a tuple of polynomials in $A[y]$. For multi-indices $\alpha \in \mathbb{Z}_{\geq 0}^{d_2}$, $\beta \in \mathbb{Z}_{\geq 0}^{d_1}$, we set $\delta_{\mathcal{P}}^\alpha = \delta_{p_1}^{\alpha_1} \dots \delta_{p_{d_2}}^{\alpha_{d_2}}$, $\delta_{\Omega}^\beta = \delta_{q_1}^{\beta_1} \dots \delta_{q_{d_1}}^{\beta_{d_1}}$, and consider the indeterminates $\delta_{\mathcal{P}}^\alpha \delta_{\Omega}^\beta y$. The operators (2.3) can be extended naturally to operators $\delta_{p_i}, \delta_{q_j}$ on the polynomial ring $A[\delta_{\mathcal{P}}^\alpha \delta_{\Omega}^\beta y : \alpha, \beta \geq 0]$; to do so, we need to use the natural commutation relations among these operators on A . Then, we define the jet space of X of order $(a, b) \in \mathbb{Z}_{\geq 0}^{d_2} \times \mathbb{Z}_{\geq 0}^{d_1}$ by

$$\mathcal{J}_{\mathcal{P}, \Omega}^{a, b}(X) = \mathcal{J}_{\mathcal{P}, \Omega}^{a, b}(X/A) = \text{Spec} \frac{A[\delta_{\mathcal{P}}^\alpha \delta_{\Omega}^\beta y : \alpha \leq a, \beta \leq b]}{(\delta_{\mathcal{P}}^\alpha \delta_{\Omega}^\beta f : \alpha \leq a, \beta \leq b)}.$$

There are induced operators

$$\delta_{p_i} : \mathcal{O}(\mathcal{J}_{\mathcal{P}, \Omega}^{a, b}(X)) \rightarrow \mathcal{O}(\mathcal{J}_{\mathcal{P}, \Omega}^{a+e_i, b}(X)),$$

and

$$\delta_{q_j} : \mathcal{O}(\mathcal{J}_{\mathcal{P}, \Omega}^{a, b}(X)) \rightarrow \mathcal{O}(\mathcal{J}_{\mathcal{P}, \Omega}^{a, b+e_j}(X)),$$

which are analogous to (2.1). In the purely geometric case of $d+0$ variables, this construction goes back to Ritt and Kolchin [23], and was the basis for the first author’s work in [4, 5] in Diophantine geometry over function fields. The purely arithmetic case of $0 + 1$ variables was introduced in [6]. The cases of $1 + 1$ and $0 + d$ variables ($d \geq 2$) were introduced in [13] and [15, 2], respectively. We refer to these papers for details of the construction above.

There are various variants of these definitions.

For instance, for $n \in \mathbb{Z}_{\geq 0}$, we define the jet space of order n by

$$\mathcal{J}_{\mathcal{P}, \Omega}^n(X) = \mathcal{J}_{\mathcal{P}, \Omega}^n(X/A) = \text{Spec} \frac{A[\delta_{\mathcal{P}}^{\alpha} \delta_{\Omega}^{\beta} y : |\alpha| + |\beta| \leq n]}{(\delta_{\mathcal{P}}^{\alpha} \delta_{\Omega}^{\beta} f : |\alpha| + |\beta| \leq n)}.$$

Next, we can take (and later on will) other rings A in all of the definitions above; for instance, we can replace the ring of polynomials by rings obtained from it by taking étale extensions and/or completing with respect to various ideals.

In the purely geometric case ($d + 0$ variables), there is a variant of the construction above due to Vojta [29], in which the derivations δ_{q_j} are replaced by *Hasse-Schmidt derivations* $\{\delta_{q_j}^n/n!; n \geq 0\}$. Notice that the Hasse-Schmidt derivations are still, morally, “differentiations in geometric directions,” so Vojta’s jet spaces do not involve “differentiations in arithmetic directions.” In particular, they do not involve operations that play the role of our δ_{p_i} s.

Going back to our jet spaces $\mathcal{J}_{\mathcal{P}, \Omega}^{a,b}(X)$, at this point we can attempt to define differential equations on X as elements of the rings of global functions $\mathcal{O}(\mathcal{J}_{\mathcal{P}, \Omega}^{a,b}(X))$. Such a definition works well in the purely geometric case of $d + 0$ variables, where it can be generalized to nonaffine X s and leads to an interesting theory with applications to diophantine results over function fields [4, 5]. In particular, in the case of $1 + 0$ variables, we have the natural Manin maps $\psi^2 \in \mathcal{O}^2(J_q^2(X))$ for any elliptic curve X over A . For the multiplicative group \mathbb{G}_m , or for elliptic curves X over A , there are also analogues ψ^1 of logarithmic derivatives that are defined over the ring of δ_q -constants of A . But the definition of differential equations suggested above is too naive to work in the case of $d_1 + d_2$ variables where $d_2 \geq 1$. Indeed, with this definition, if $d_2 \geq 1$, in most cases there are no “interesting” differential equations (in particular, for instance, there are no non-trivial arithmetic analogues of linear differential operators!) Later on, however, we shall be able to introduce a less naive definition of differential equations. This will allow us to pass to the case where X is not necessarily affine and then to introduce, for X equal to a group scheme, the notion of linear differential equation on X , in which case the solutions form a group. There is also a notion of linearity of differential equations in the case where X is a modular or a Shimura curve (which we are not going to review in this paper). Up to a point, we can consider these matters in general, but it will be much more convenient to examine these issues separately in the cases of $0 + 1$, $0 + 2$, and $1 + 1$ variables. In the case of $0 + 2$ variables, we will encounter analogues of the Laplace operator, while in the case of $1 + 1$

variables, we will encounter analogues of the convection, heat, and wave equations. The cases of $0 + 2$ and $1 + 1$ variables can be easily generalized to the cases of $0 + d$ and $d + 1$ variables respectively. However, even in the case of $1 + 2$ variables, new ideas seem to be required to make the theory work.

3. $0 + 1$ variables

This theory was introduced in [6]. We assume that $\mathcal{P} = \{p\}$ consists of one prime $p \geq 5$, and that $\mathcal{Q} = \emptyset$. In this setting, the most natural variant of the theory is that in which we take A to be the ring $R := \widehat{\mathbb{Z}}_p^{ur}$ obtained by p -adically completing the maximum unramified extension of the ring of p -adic integers. (Here and below, for a fixed prime p , we denote by $\widehat{}$ the p -adic completion of a ring or a scheme.) The elements of R can be uniquely represented as power series $\sum_{n \geq 0} \xi_n p^n$, where the ξ_n s are either zero or roots of unity of order prime to p . The collection consisting of zero and the roots of unity of order prime to p will be called the *monoid of constants* of R . The ring R has a well-known automorphism, referred to as the *lift of Frobenius*, defined by

$$\begin{aligned} R & \xrightarrow{\phi} R \\ \sum \xi_n p^n & \longmapsto \phi(\sum \xi_n p^n) = \sum \xi_n^p p^n. \end{aligned}$$

We consider the “Fermat quotient operator” $\delta = \delta_p : R \rightarrow R$ defined by

$$\delta a = \frac{\phi(a) - a^p}{p}.$$

Note that $\delta a = 0$ if, and only if, a is in the monoid of constants.

For any affine scheme of finite type X over R , we consider the jet spaces $\mathcal{J}_p^n(X)$, $n \in \mathbb{Z}_{\geq 0}$ and we consider the formal schemes $J^n(X) = J_p^n(X) = \mathcal{J}_p^n(X)^\wedge$, the p -adic completions of the jet spaces. It is then a fact that, if X is a scheme of finite type over R , and if $X = \bigcup X_i$ is an affine open cover, then the formal schemes $J^n(X_i)$ naturally glue together to give a formal scheme $J^n(X)$, the p -jet space of X of order n [6, 7]. The reduction mod p , $J^n(X) \otimes R/pR$, of these p -jet spaces coincide with the Greenberg transforms of X [18]. But notice that the Fermat quotient operators $\delta : \mathcal{O}(J^n(X)) \rightarrow \mathcal{O}(J^{n+1}(X))$, which are the most salient feature of our theory, do not survive after reduction mod p , that is, they do not survive on the Greenberg transforms. We define a *differential equation* on X to be a formal function $f \in \mathcal{O}(J^n(X))$. Any such equation defines a map of sets, referred

to as the associated (nonlinear) *differential operator*, $f : X(R) \rightarrow R$. The set $f^{-1}(0) \subset X(R)$ is the *set of solutions* of f (or of $f = 0$). If X is a group scheme over R , and f is a differential equation such that the operator $f : X(R) \rightarrow R$ is a homomorphism, we say that f is *linear*, or that f is a δ -character.

There is also a natural concept of *linear differential equation (operator)* in the context of modular and Shimura curves [8, 9]. This leads to a theory of what we call *differential modular forms*. We will not touch this subject in this paper, although Theorem 3.3 below is an example of what this theory can produce.

We now discuss some results about δ -characters. We start by noticing that the logarithmic derivatives in the purely geometric case have an arithmetic analogue:

THEOREM 3.1. — [6]

- (1) *On the multiplicative group \mathbb{G}_m over R there is a non-zero δ -character $\psi^1 : \mathbb{G}_m(R) = R^\times \rightarrow R$ of order 1, unique up to multiplication by an element of R ; it is given by*

$$\psi^1 u = \sum_{n \geq 1} (-1)^{n-1} \frac{p^{n-1}}{n} \left(\frac{\delta u}{u^p} \right)^n .$$

- (2) *If E is an elliptic curve over R that has ordinary reduction and is a canonical lift of its reduction, then there is a non-zero δ -character $\psi^1 : E(R) \rightarrow R$ of order 1, unique up to multiplication by an element of R .*

More remarkably, there is an arithmetic analogue of the Manin map:

THEOREM 3.2. — [6] *If E is any elliptic curve over R , then there is a non-zero δ -character $\psi^2 : E(R) \rightarrow R$ of order 2 whose group of solutions contains $\cap_n p^n E(R)$ as a subgroup of finite index.*

There is a modular analogue of this that can be roughly stated as follows:

THEOREM 3.3. — [8] *If S is a modular or a Shimura curve over R , then there exists a Zariski open set $S^\dagger \subset S$ and a differential operator $f^\dagger : S^\dagger(R) \rightarrow R$ of order 1, whose set of solutions is exactly the set of CL (canonical lift) points.*

Theorems 3.2 and 3.3 were recently applied to prove a finiteness result in diophantine geometry over local fields:

THEOREM 3.4. — [11] *Let E be an elliptic curve and S a modular curve over \mathbb{Q} . Let $\Phi : X \rightarrow E$ and $\Pi : X \rightarrow S$ be non-constant morphisms from*

a curve X over $\overline{\mathbb{Q}}$. Let p be a sufficiently large prime, let $R = \widehat{\mathbb{Z}}_p^{ur}$, and consider the induced maps $\Phi : X(R) \rightarrow E(R)$ and $\Pi : X(R) \rightarrow S(R)$. Let $CL \subset S(R)$ be the set of CL (canonical lift) points. Then there exists a constant c_p depending on p such that for any subgroup $\Gamma \leq E(R)$ with $r := \text{rank } \Gamma := \dim_{\mathbb{Q}}(\Gamma \otimes \mathbb{Q}) < \infty$, the set $\Phi^{-1}(\Gamma) \cap \Pi^{-1}(CL)$ is finite of cardinality at most $c_p p^r$.

The constant c_p can be made entirely explicit if Π is the identity and Φ is a modular parametrization. A stronger result is actually true, in which $r = \text{rank } \Gamma$ is replaced by

$$r := \dim_{\mathbb{F}_p} \left(\frac{\Gamma}{\Gamma \cap (E(R)_{\text{tors}} + pE(R))} \right).$$

Theorem 3.4 has an analogue over number fields:

THEOREM 3.5. — [10] *Let E be an elliptic curve and S a modular curve over $\overline{\mathbb{Q}}$. Let $\Phi : X \rightarrow E$ and $\Pi : X \rightarrow S$ be non-constant morphisms from a curve X over $\overline{\mathbb{Q}}$. Let $\Gamma \leq E(\overline{\mathbb{Q}})$ be a finite rank subgroup, and let $CM \subset S(\overline{\mathbb{Q}})$ be the set of CM (complex multiplication) points. Then the set $\Phi^{-1}(\Gamma) \cap \Pi^{-1}(CM)$ is finite.*

The proof of Theorem 3.5 uses equidistribution arguments. In the special case where $\Gamma = E(\overline{\mathbb{Q}})_{\text{tors}}$, restricting the attention to Heegner points (when, in particular, Π is the identity and Φ is a modular parametrization), Theorem 3.5 was proved using a different method in [26].

It is instructive to sketch the proof of Theorem 3.4 in the simple situation when $\Gamma = E(\overline{\mathbb{Q}})_{\text{tors}}$ and Π is the identity. Let us recall the differential operators ψ^2 and f^b in Theorems 3.2 and 3.3, respectively. We consider the differential operator $f^\sharp : S^\dagger(R) \rightarrow R$, defined by the composition

$$S^\dagger(R) \subset S(R) \xrightarrow{\Phi} E(R) \xrightarrow{\psi^2} R.$$

Then the set $\Phi^{-1}(\Gamma) \cap CL$ is contained in the set of solutions of the system of differential equations

$$\begin{cases} f^b = 0, \\ f^\sharp = 0. \end{cases}$$

The main idea of the proof is to show that the derivatives of the unknowns in this system can be eliminated, in other words, that there exist nonlinear differential operators $h_0, h_1 : S^\dagger(R) \rightarrow R$ such that the operator

$$f^\sharp - h_0 \cdot f^b - h_1 \cdot \delta \circ f^b$$

has order 0, i.e., it is a formal function in usual (formal) algebraic geometry. Such functions (on curves) have only finitely many zeroes, and the number

of zeroes can be estimated. This leads to the finiteness and the estimate in Theorem 3.4.

We can ask what differential operators we may obtain on projective curves of genus $\neq 1$. The pictures for genus 0 and genus ≥ 2 are entirely different. Indeed we have the following results.

THEOREM 3.6. — [7] *Any differential operator $\mathbb{P}^1(R) \rightarrow R$ of any order is a constant map.*

THEOREM 3.7. — [7] *If X is a smooth projective curve of genus ≥ 2 , then for any $n \geq 1$ the formal scheme $J^n(X)$ is affine. In particular there exist differential operators $f_1, \dots, f_N : X(R) \rightarrow R$ of order 1 such that the map $(f_1, \dots, f_N) : X(R) \rightarrow R^N$ is injective.*

Incidentally, Theorem 3.7 has a purely number theoretic application, which is the following effective bound for the Manin-Mumford conjecture. Manin and Mumford conjectured that the intersection of a smooth projective curve of genus ≥ 2 with the torsion subgroup of its Jacobian is finite. This was proved by Raynaud [27]. A different proof, plus an effective bound on the cardinality of this intersection, was provided in [7]; this was done via an argument involving Theorem 3.7. Here is the result:

THEOREM 3.8. — [7] *If X is a smooth projective curve of genus $g \geq 2$ defined over a number field K , and if $X \subset A$ is the Abeli-Jacobi embedding of X into its Jacobian A (corresponding to a given point on X), then the set $X(\mathbb{C}) \cap A(\mathbb{C})_{\text{tors}}$ has cardinality $\leq c(g, p)$, where $c(g, p)$ is an explicit constant that depends only on the genus g and on the smallest prime p that is unramified in K , and for which there is a place of K over p where X has good reduction.*

Roughly speaking, the idea of the proof of Theorem 3.8 is as follows. By a result of Coleman, the problem can be reduced to a problem over $R = \widehat{\mathbb{Z}}_p^{ur}$. Then, taking “jets of points,” we can show that the intersection $X(R) \cap A(R)_{\text{tors}}$ can be embedded into an intersection of the form $J^1(X)(R/pR) \cap B(R/pR)$, where B is an abelian subvariety of $J^1(A) \otimes R/pR$. Now $J^1(X) \otimes R/pR$ is affine (by Theorem 3.7) while B is projective. So the intersection $J^1(X)(R/pR) \cap B(R/pR)$ is finite, with cardinality easily estimated by Bézout’s theorem. This ends the proof of Theorem 3.8.

For more applications of the $0 + 1$ variable theory, we refer the reader to [9]. In that monograph, a systematic study was made of differential operators $f : X(R) \rightarrow R$ on curves X with the property that f is “invariant” under the action of various “arithmetically flavored” correspondences

$Y \subset X \times X$. The problem of determining all such f s should be viewed as an arithmetic analogue of the problem in geometry and/or theoretical physics of determining all Lagrangians (functions on jet spaces $J^n(M/N)$) that are invariant under a group of symmetries acting on M “over N .”

Other applications of the $0 + 1$ variable theory involve congruences between classical modular forms [8, 1, 12]. We shall not discuss these applications here.

4. $0 + 2$ variables

In this section we follow [15]. Passing from the case of one prime to the case of several primes (in particular, the 2 we consider here) requires new ideas. We let $\mathcal{P} = \{p_1, p_2\}$, $\mathcal{Q} = \emptyset$. The natural choice for A in this section is the semi-local ring $A = \mathbb{Z}_{(p_1)} \cap \mathbb{Z}_{(p_2)} \subset \mathbb{Q}$. The first difficulty we encounter now is that the jet spaces $\mathcal{J}_{\mathcal{P}}^r(X)$ above were only defined for A -schemes X that are affine, and the gluing procedure which would extend this definition to the nonaffine case is not straightforward. The problem of defining the jet spaces for nonaffine X s was solved independently in [15] and [2]. In [2], the approach is via algebraic spaces and works in full generality. In [15], a more naive approach is taken which nevertheless suffices for the applications we have in mind here; in the discussion below we follow [15].

Let X be any quasiprojective scheme over A , and let $X = \cup X_i$ be an affine cover. Then the schemes $\mathcal{J}_{\mathcal{P}}^r(X_i)$ can be glued together to give a scheme $\mathcal{J}_{\mathcal{P}}^r(X)$. The trouble here is that the latter genuinely depends on the covering we started with, and in particular, the construction is not functorial in X . What turns out to be true, however, is that for each $k = 1, 2$, the ring of global functions $\mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X)^{\widehat{p}_k})$ on the p_k -adic completion $\mathcal{J}_{\mathcal{P}}^r(X)^{\widehat{p}_k}$ of $\mathcal{J}_{\mathcal{P}}^r(X)$ does not depend on the covering, and is functorial in X .

Now the single prime theory provides, in interesting situations, interesting formal functions $f_k \in \mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X)^{\widehat{p}_k})$, $k = 1, 2$. Obviously, the next puzzle comes then from the fact that we would like to “glue together” pairs of these elements f_1, f_2 . This cannot be done directly since, for instance, in the case where X is affine, each f_k is a function on the “tubular neighborhood” $\mathrm{Spf} \mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X))^{\widehat{p}_k}$ of $\mathrm{Spec} \mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X)) \otimes \mathbb{F}_{p_k}$ in $\mathrm{Spec} \mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X))$, and these tubular neighborhoods are disjoint. This puzzle was solved in [15]. What we proposed there was to declare that f_1 and f_2 can be “analytically continued” along a section $P : \mathrm{Spec} A \rightarrow X$ of $X \rightarrow \mathrm{Spec} A$ if there is an element f_0 in the P^r -adic completion of $\mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X))$ (where $P^r \in \mathcal{J}_{\mathcal{P}}^r(X)(A)$) is the natural prolongation of $P \in X(A)$) such that, for each $k = 1, 2$, f_k

and f_0 coincide in the (p_k, P^r) -adic completion of $\mathcal{O}(\mathcal{J}_{\mathcal{P}}^r(X))$. (As is, such a definition makes sense only in the affine case, but can be easily extended to the quasiprojective case.) Then we declare that a *differential equation* on X (of order r) is a pair (f_1, f_2) , $f_k \in \mathcal{O}(\widehat{\mathcal{J}_{\mathcal{P}}^r(X)^{p_k}})$, that can be analytically continued along a given section. The section is kept fixed throughout, but in most cases there is a preferred section anyway: for instance if X is a group scheme over A , then the section should be taken to be the identity section. In the group scheme situation, there is a natural notion of *linear differential equation* also called $\delta_{\mathcal{P}}$ -character: we simply ask that f_1 and f_2 be linear.

Again, there is a concept of *linear differential equation (operator)* in the context of modular and Shimura curves [12]. This leads to a theory of what we call *Igusa differential modular forms*. We will not touch this subject in this paper.

Here are our main results about $\delta_{\mathcal{P}}$ -characters.

THEOREM 4.1. — [15] *Let $X = \mathbb{G}_m := \text{Spec } A[x, x^{-1}]$ be the multiplicative group scheme over A . There exists, up to a unit in A , a unique $\delta_{\mathcal{P}}$ -character $\psi^{(1,1)}$ of order $(1, 1)$ on X . Every other $\delta_{\mathcal{P}}$ -character is obtained (in an appropriate sense) from $\psi^{(1,1)}$.*

THEOREM 4.2. — [15] *Let X be an elliptic curve over A with ordinary reduction at p_1 and p_2 . There exists, up to a unit in A , a unique $\delta_{\mathcal{P}}$ -character $\psi^{(2,2)}$ of order $(2, 2)$ on X . Every other $\delta_{\mathcal{P}}$ -character on X is obtained (in an appropriate sense) from $\psi^{(2,2)}$.*

The $\delta_{\mathcal{P}}$ -character $\psi^{(1,1)}$ can be explicitly described as follows. First, let us observe that

$$(4.1) \quad \mathcal{O}(\mathcal{J}_{\mathcal{P}}^{(1,1)}(\mathbb{G}_m)) = A[x, x^{-1}, \phi_{p_1}(x^{-1}), \phi_{p_2}(x^{-1}), \phi_{p_1}\phi_{p_2}(x^{-1}), \delta_{p_1}x, \delta_{p_2}x, \delta_{p_1}\delta_{p_2}x],$$

where $\phi_{p_k}u := u^{p_k} + p_k\delta_{p_k}u$. Then, let us consider the series

$$(4.2) \quad \begin{aligned} f_1 &:= \left(1 - \frac{\phi_{p_2}}{p_2}\right) \psi_{p_1}^1 \in \mathcal{O}(\widehat{\mathcal{J}_{\mathcal{P}}^{(1,1)}(\mathbb{G}_m)})^{p_1}, \\ f_2 &:= \left(1 - \frac{\phi_{p_1}}{p_1}\right) \psi_{p_2}^1 \in \mathcal{O}(\widehat{\mathcal{J}_{\mathcal{P}}^{(1,1)}(\mathbb{G}_m)})^{p_2}, \end{aligned}$$

where

$$\psi_{p_k}^1 := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p_k^{n-1}}{n} \left(\frac{\delta_{p_k}x}{x^{p_k}}\right)^n, \quad k = 1, 2.$$

It is an easy exercise to see that f_1, f_2 can be analytically continued along the identity, thus giving rise to our equation $\psi^{(1,1)}$; essentially this amounts

to noticing that after substituting $T + 1$ for x in the series f_k , $k = 1, 2$, we obtain series in

$$\mathbb{Q}_{p_k} [[T, \delta_{p_1} T, \delta_{p_2} T, \delta_{p_1} \delta_{p_2} T]]$$

coming from one and the same series

$$-\left(1 - \frac{\phi_{p_1}}{p_1}\right) \left(1 - \frac{\phi_{p_2}}{p_2}\right) \sum (-1)^{n-1} \frac{T^n}{n} \in \mathbb{Q} [[T, \delta_{p_1} T, \delta_{p_2} T, \delta_{p_1} \delta_{p_2} T]].$$

By the way, this $\psi^{(1,1)}$ should be viewed as an arithmetic analogue of a partial differential operator in analysis, which we now describe. Let $N \subset \mathbb{C}$ be a disk, viewed as a (real) smooth manifold, and let $M = N \times \mathbb{C}^\times$ (viewed again as a real smooth manifold). Then our $\psi^{(1,1)}$ should be viewed as the arithmetic analogue of the partial differential operator

$$\psi_{z\bar{z}}^{(1,1)} : M(N) = C^\infty(N, \mathbb{C}^\times) \rightarrow \mathcal{O}(N) = C^\infty(N, \mathbb{C}),$$

defined by

$$\psi_{z\bar{z}}^{(1,1)}(u) := \frac{1}{4} \Delta \log u = \partial_z \partial_{\bar{z}} \log u,$$

where $z = x + iy$ is the complex coordinate in N , and $\Delta = \partial_x^2 + \partial_y^2$ is the Euclidean Laplacian. (Here, $\partial_x, \partial_y, \partial_z, \partial_{\bar{z}}$ are the corresponding partial derivative operators.) Like our arithmetic $\psi^{(1,1)}$, the operator $\psi_{z\bar{z}}^{(1,1)}$ is a group homomorphism, and has the “Dirac decomposition”

$$\psi_{z\bar{z}}^{(1,1)}(u) = \partial_z \left(\frac{\partial_{\bar{z}} u}{u} \right) = \partial_{\bar{z}} \left(\frac{\partial_z u}{u} \right),$$

which is analogous to the decompositions of f_1 and f_2 in (4.2) into products of equations of lower order. In what follows, such a decomposition will be loosely referred to as a *Dirac decomposition*

The equation $\psi^{(2,2)}$ for elliptic curves can be constructed similarly (although not explicitly). The factors $\left(1 - \frac{\phi_{p_k}}{p_k}\right)$ in the \mathbb{G}_m case have to be replaced by the corresponding Euler factors in the L -series of the elliptic curve. As in the case of \mathbb{G}_m , there is a partial differential operator in analysis (a “double Laplacian” applied to the logarithm of a family of elliptic curves $M \rightarrow N$) that renders $\psi^{(2,2)}$ as its analogue; cf. the Introduction of [15] for details.

5. 1 + 1 variables

In this section we follow [13, 14]. We let $\mathcal{P} = \{p\}$ consist of one prime $p \geq 5$, and we let $\mathcal{Q} = \{q\}$ consist of one variable q . Then we let $A := R[[q]]$,

where $R = \widehat{\mathbb{Z}}_p^{ur}$, and we consider the operators

$$\begin{aligned}
 R[[q]] &\xrightarrow{\delta_p, \delta_q} R[[q]] \\
 \sum a_n q^n &\longmapsto \delta_p(\sum a_n q^n) := \frac{(\sum \phi_p(a_n) q^{pn}) - (\sum a_n q^n)^p}{p}, \\
 &\delta_q(\sum a_n q^n) := q \frac{d}{dq} \left(\sum a_n q^n \right) = \sum n a_n q^n.
 \end{aligned}$$

where $\phi_p = \phi : R \rightarrow R$ is the lift of Frobenius. As in the case of $0 + 1$ variables, for any affine scheme of finite type X over A we consider the jet spaces $\mathcal{J}_{pq}^n(X)$, $n \in \mathbb{Z}_{\geq 0}$. Consider the formal schemes $J_{pq}^n(X) = \mathcal{J}_{pq}^n(X)^\wedge$, the p -adic completions of the jet spaces. If X is a scheme that is not necessarily affine, and if $X = \bigcup X_i$ is an affine open cover, then the formal schemes $J_{pq}^n(X_i)$ naturally glue together to give a formal scheme $J_{pq}^n(X)$. We define a *differential equation* on X to be a formal function $f \in \mathcal{O}(J_{pq}^n(X))$. Any such equation defines a map of sets, referred to as the associated (nonlinear) *differential operator*, $f : X(A) \rightarrow A$. The set $f^{-1}(0) \subset X(A)$ is the *set of solutions* of f (or of $f = 0$). If X is a group scheme over A , we say that a differential equation f is *linear*, or that f is a $\{\delta_p, \delta_q\}$ -*character*, if f defines a homomorphism (of group objects in the category of formal p -adic schemes) from $J_{pq}^n(X)$ to the additive group; if this is the case, then the induced map $X(A) \rightarrow A$ is a homomorphism, and the solution set $f^{-1}(0)$ is a group.

And once again, there is a concept of *linear differential equation (operator)* in the context of modular curves [14]. We will not touch upon this subject in this paper.

Going back to $\{\delta_p, \delta_q\}$ -characters, the first task we face is the classification of all such objects on a given group scheme. This was done in [13] for the groups \mathbb{G}_a , \mathbb{G}_m , and any elliptic curve E over A . The salient features of this classification are roughly stated in the Theorems below; for further details and more precise statements, we refer the reader to [13].

THEOREM 5.1. — [13]

- (1) For \mathbb{G}_a , all $\{\delta_p, \delta_q\}$ -characters are given by polynomials in ϕ_p and δ_q .
- (2) For \mathbb{G}_m , all $\{\delta_p, \delta_q\}$ -characters are obtained (in an appropriate sense) from the differential equations ψ_p^1 and ψ_q^1 , where ψ_p^1 is the δ_p -character described in (1) of Theorem 3.1, and ψ_q^1 is the logarithmic derivative $\psi_q^1 u = \delta_q u / u$.

THEOREM 5.2. — [13] For a “sufficiently general” elliptic curve E over A , the following hold:

- (1) There are no non-zero δ_p -characters ψ_p^1 of order 1, and no non-zero δ_q -characters ψ_q^1 of order 1.
- (2) There is a non-zero $\{\delta_p, \delta_q\}$ -character ψ_{pq}^1 of order 1. This character is essentially unique.
- (3) All $\{\delta_p, \delta_q\}$ -characters on E can be obtained (in an appropriate sense) from ψ_{pq}^1 , ψ_p^2 , and ψ_q^2 , where ψ_{pq}^1 is the character in (2) above, ψ_p^2 is the arithmetic analogue of the Manin map in Theorem 3.2, and ψ_q^2 is the classical Manin map. Also, there exists a relation of the form

$$\psi_q^2 + \lambda \psi_p^2 = \psi_{pq,a}^1 \circ \psi_p^1$$

where $\lambda \in A$, and $\psi_{pq,a}^1$ is a linear polynomial in ϕ_p and δ_q .

The character ψ_{pq}^1 can be viewed as an analogue of a convection equation on E , and its existence is sort of a surprise. The character $\psi_q^2 + \lambda \psi_p^2$ can be viewed as an analogue of a wave equation on E . In a suitable sense, both of these objects are canonical.

THEOREM 5.3. — [13] Assume that E is a sufficiently general elliptic curve over R . Then all the $\{\delta_p, \delta_q\}$ -characters on E are obtained (in an appropriate sense) from ψ_q^1 and ψ_p^2 , where ψ_q^1 is the logarithmic derivative with respect to δ_q , and ψ_p^2 is the arithmetic analogue of the Manin map.

The linear combinations $\psi = \psi_q^1 + \lambda \psi_p^2$ can then be viewed as arithmetic analogues of the heat equation on E .

Let us now assume, for simplicity, that our groups X/A are actually defined over R (this is automatic, of course, for $\mathbb{G}_a, \mathbb{G}_m$). Let $\psi : X(A) \rightarrow A$ be a linear differential operator. A solution $u \in \psi^{-1}(0)$ will be called *stationary* if $u \in X(R)$. (The terminology comes from viewing q as an exponential of “time.”) Then the next question addressed in [13] is the characterization of all $\{\delta_p, \delta_q\}$ -characters on $\mathbb{G}_a, \mathbb{G}_m, E$ that admit *nonstationary solutions*. For the results, we refer the reader to [13]. Let us just note here that what we encounter is a “quantization phenomenon” that can be nicely illustrated in the case of the heat equations referred to after Theorem 5.3. Indeed, we can prove that the $\psi = \psi_q^1 + \lambda \psi_p^2$ above has nonstationary solutions if, and only if, λ is a \mathbb{Z} -multiple of a certain invariant of E (which we refer to as an *arithmetic Kodaira-Spencer class*). As we shall explain presently, a similar phenomenon occurs for \mathbb{G}_m and the “convection equation” $\psi = \psi_q^1 + \lambda \psi_p^1$.

Finally, there is an intriguing analogy between the theory of fundamental solutions in the classical theory of linear partial differential operators, and the arithmetic counterpart that we are discussing here. Indeed, let us assume we are in the framework of the classical theory, and that we are

given a linear partial differential operator in 2 variables,

$$u = u(x_1, x_2) \mapsto Pu = \sum c_{i_1 i_2} \partial_{x_1}^{i_1} \partial_{x_2}^{i_2} u$$

with constant coefficients. Then, given a “well-posed” boundary value problem for P , there is a way to describe the space of solutions $\{u : Pu = 0\}$ as a “free module of finite rank” over the “ring” of functions of x ; here, the ring multiplication and module structure are given by convolution. (The quotation marks above indicate the fact that the ring and the module structures are not “everywhere defined,” as convolution is only defined under some restrictions.) The rank of this module is closely related to the symbol of P , which is the polynomial

$$\sigma(\xi_1, \xi_2) = \sum (\sqrt{-1})^{i_1+i_2} c_{i_1 i_2} \xi_1^{i_1} \xi_2^{i_2} \in \mathbb{C}[\xi_1, \xi_2].$$

An analogue of this description can be given in the arithmetic case. Roughly speaking, the result is the following:

THEOREM 5.4. — *Let $\psi : X(A) \rightarrow A$ be the operator associated to a “non-degenerate” $\{\delta_p, \delta_q\}$ -character on $X = \mathbb{G}_a, \mathbb{G}_m, E$. (Here “non-degeneracy” is a condition defined in terms of a well-defined “symbol” $\mu(\xi_p, \xi_q) \in A[\xi_p, \xi_q]$ of ψ , where ξ_p, ξ_q are 2 variables.) Let $\psi^{-1}(0)_1$ be the group of solutions in $\psi^{-1}(0)$ that vanish at $q = 0$. Then there is a natural R -module structure on $\psi^{-1}(0)_1$ (given by a “convolution” operation) such that $\psi^{-1}(0)_1$ is a finitely generated free R -module. The rank of this module is the number of positive integers that are roots of the polynomial $\mu(0, \xi_q)$.*

It is instructive to give an explicit example of this theory; we choose the simplest of the non-trivial ones, that of the multiplicative group \mathbb{G}_m . In this case, any $\{\delta_p, \delta_q\}$ -character of order 1 is, up to multiplication by an element of A , an A -linear combination of ψ_p^1 and ψ_q^1 , and any such linear combination can be viewed as an arithmetic analogue of a convection equation. Let us restrict attention to linear combinations of the form $\psi = \psi_q^1 + \lambda\psi_p^1$, $\lambda \in R^\times$. Then the symbol of ψ turns out to be the linear polynomial

$$\mu(\xi_p, \xi_q) = \xi_q + \lambda\xi_p - \lambda.$$

So the set of positive integers that are roots of $\mu(0, \xi_q)$ is either $\{\kappa\}$, if $\lambda = \kappa \in \mathbb{Z}_{\geq 0}$, or \emptyset , if $\lambda \notin \mathbb{Z}_{\geq 0}$. In the second case, the space $\psi^{-1}(0)_1$ vanishes. In the first case, the space of solutions $\psi^{-1}(0)_1$ is a free R -module

(under a certain convolution operation) of rank 1, with basis

$$u_\kappa := \exp \left(\frac{q^\kappa}{\kappa} + \sum_{n \geq 1} (-1)^n \frac{q^{\kappa p^n}}{\kappa p^n (p-1)(p^2-1) \cdots (p^n-1)} \right).$$

Notice that this series is a sort of hybrid between the Artin-Hasse exponential and the quantum exponential in [22], p. 30; the integrality of this series is a consequence of the Dwork-Dieudonné lemma.

The example above illustrates the quantization phenomenon alluded to above: the space $\psi^{-1}(0)_1$ is non-zero if, and only if, $\lambda \in \mathbb{Z}_{\geq 0}$.

6. 1 + 2 variables

As of now, there is no theory available for the case of 1 + 2 variables. We could hope to tackle such a case by combining the ideas used in the cases of 0 + 2 and 1 + 1 variables, respectively. However, the natural attempts to proceed in this manner lead to difficulties that we explain next.

Indeed, we may attempt to construct linear differential equations on \mathbb{G}_m in 1 + 2 variables by using the idea of “Dirac decompositions” from the case of 0 + 2 variables, but replacing the 0 + 1 variable equations $\psi_{p_k}^1$ there by appropriate 1 + 1 variable equations. This fails in order 2. If the order is increased (or if the “Dirac decomposition” assumption is dropped), then analytic continuation can be achieved; but in the examples we can construct, there seem to be no nonstationary solutions.

For let $\mathcal{P} = \{p_1, p_2\}$, $\mathcal{Q} = \{q\}$, $A_0 = \mathbb{Z}_{(p_1)} \cap \mathbb{Z}_{(p_2)}$, and $A = A_0[[q]]$. We consider $\mathbb{G}_m := \text{Spec } A[x, x^{-1}]$. Then the ring $\mathcal{O}(\mathcal{J}_{\mathcal{P}, \mathcal{Q}}^n(\mathbb{G}_m))$ identifies with the ring

$$A[x, x^{-1}, \phi_{p_1}(x^{-1}), \phi_{p_2}(x^{-1}), \phi_{p_1} \phi_{p_2}(x^{-1}), \delta_{p_1}^{i_1} \delta_{p_2}^{i_2} \delta_q^j x : i_1 + i_2 + j \leq n].$$

Consider the two elements

$$\begin{aligned} f_1 &\in \mathcal{O}(\mathcal{J}_{\mathcal{P}, \mathcal{Q}}^n(\mathbb{G}_m))^{\widehat{p}_1}, \\ f_2 &\in \mathcal{O}(\mathcal{J}_{\mathcal{P}, \mathcal{Q}}^n(\mathbb{G}_m))^{\widehat{p}_2}. \end{aligned}$$

Let us say that f_1 and f_2 can be *analytically continued* (along the identity) if, after replacing x by $T + 1$, we get 2 series coming from the same series in

$$\mathbb{Q}[[\delta_{p_1}^{i_1} \delta_{p_2}^{i_2} \delta_q^j T : i_1 + i_2 + j \leq n]].$$

This is a natural generalization of the construction in the case of 0 + 2 variables.

We can derive then the following result, showing that if the order n is 2, and if f_1, f_2 have “Dirac decompositions,” then the only instances where analytic continuation holds are those coming from the cases of $1 + 0, 0 + 2,$ and $1 + 1$ variables, respectively. So morally speaking, there is no analytic continuation in the genuine $1 + 2$ variable case.

The “most general” form of $f_1, f_2,$ of order 2, with “Dirac decomposition” is

$$(6.1) \quad \begin{aligned} f_1 &= (\alpha_2 \delta_q + \beta_2 \phi_{p_2} + \gamma_2)(\mu_1 \psi_q^1 + \lambda_1 \psi_{p_1}^1), \\ f_2 &= (\alpha_1 \delta_q + \beta_1 \phi_{p_1} + \gamma_1)(\mu_2 \psi_q^1 + \lambda_2 \psi_{p_2}^1), \end{aligned}$$

where, for $k = 1, 2, \alpha_k, \beta_k, \gamma_k, \mu_k, \lambda_k \in A_0,$ and

$$\begin{aligned} \psi_{p_k}^1 &:= \sum_{n \geq 1} (-1)^{n-1} \frac{p_k^{n-1}}{n} \left(\frac{\delta_{p_k} x}{x^{p_k}} \right)^n \\ \psi_q^1 &:= \frac{\delta_q x}{x}. \end{aligned}$$

In order to state our result, let us assume that f_1, f_2 are non-zero, and let us denote by $U_k \in \mathbb{Q}^3, V_k \in \mathbb{Q}^2, (k = 1, 2),$ the unique vectors belonging to the \mathbb{Q} -linear spaces spanned by $(\alpha_k, \beta_k, \gamma_k)$ and $(\mu_k, \lambda_k),$ respectively, having their first non-zero component equal to 1.

PROPOSITION 6.1. — Assume that f_1 and f_2 are as in (6.1), and that they can be analytically continued along the identity. Then one of the following holds:

- | | | | | | |
|----|-------------------------------|-------------------------------|-----------------------|----------------------|---------------|
| 1) | $U_1 = (1, 0, \gamma),$ | $U_2 = (1, 0, \gamma),$ | $V_1 = (1, 0),$ | $V_2 = (1, 0)$ | (1 + 0 case); |
| 2) | $U_1 = (1, 0, 0),$ | $U_2 = (1, -\gamma, \gamma),$ | $V_1 = (1, 0),$ | $V_2 = (1, -\gamma)$ | (1 + 1 case); |
| 3) | $U_1 = (1, -\gamma, \gamma),$ | $U_2 = (1, 0, 0),$ | $V_1 = (1, -\gamma),$ | $V_2 = (1, 0)$ | (1 + 1 case); |
| 4) | $U_1 = (0, 0, 1),$ | $U_2 = (0, 0, 1),$ | $V_1 = (1, 0),$ | $V_2 = (1, 0)$ | (1 + 0 case); |
| 5) | $U_1 = (0, 1, -1),$ | $U_2 = (1, 0, 0),$ | $V_1 = (0, 1),$ | $V_2 = (1, 0)$ | (1 + 1 case); |
| 6) | $U_1 = (1, 0, 0),$ | $U_2 = (0, 1, -1),$ | $V_1 = (1, 0),$ | $V_2 = (0, 1)$ | (1 + 1 case); |
| 7) | $U_1 = (0, 1, -p_1),$ | $U_2 = (0, 1, -p_2),$ | $V_1 = (0, 1),$ | $V_2 = (0, 1)$ | (0 + 2 case). |

Proof. — The image of f_1 in

$$\mathbb{Q}_{p_1} [[q]] [[\delta_{p_1}^{i_1} \delta_{p_2}^{i_2} \delta_q^j T : i_1 \leq 1, i_2 \leq 1, j \leq 2]]$$

equals

$$(\alpha_2 \delta_q + \beta_2 \phi_{p_2} + \gamma_2)(\mu_1 \delta_q + \lambda_1 \frac{\phi_{p_1}}{p_1} - \lambda_1) \left(\sum_{n \geq 1} (-1)^{n-1} \frac{T^n}{n} \right),$$

and a similar assertion holds for $f_2.$ So if f_1 and f_2 can be analytically continued, we must have an equality

$$(\alpha_2 \delta_q + \beta_2 \phi_{p_2} + \gamma_2)(\mu_1 \delta_q + \lambda_1 \frac{\phi_{p_1}}{p_1} - \lambda_1) = (\alpha_1 \delta_q + \beta_1 \phi_{p_1} + \gamma_1)(\mu_2 \delta_q + \lambda_2 \frac{\phi_{p_2}}{p_2} - \lambda_2).$$

Using the commutation relations $\delta_q \phi_{p_k} = p_k \phi_{p_k} \delta_q$, we derive the following system of equations:

$$\left\{ \begin{array}{l} \gamma_2 \mu_1 - \alpha_2 \lambda_1 = \gamma_1 \mu_2 - \alpha_1 \lambda_2, \\ \alpha_1 \mu_2 = \alpha_2 \mu_1, \\ \beta_1 \mu_2 = \alpha_2 \lambda_1, \\ \beta_2 \mu_1 = \alpha_1 \lambda_2, \\ \beta_2 \lambda_1 / p_1 = \beta_1 \lambda_2 / p_2, \\ \beta_2 \lambda_1 = -\gamma_1 \lambda_2 / p_2, \\ \beta_1 \lambda_2 = -\gamma_2 \lambda_1 / p_1, \\ \gamma_2 \lambda_1 = \gamma_1 \lambda_2. \end{array} \right.$$

It is now an elementary task to show that the only solutions to this system are of the form stated. □

The result above shows that there is no analytic continuation in $1 + 2$ variables (that does not arise from fewer variables) if we insist that the order n be 2 and that we have “Dirac decomposition.” However, we give easy examples below showing that as soon as we relax either of these two conditions, we can achieve analytic continuation.

Indeed, if $n = 3$, we can take

$$(6.2) \quad \begin{aligned} f_1 &= (\phi_{p_2} - p_2)[(\phi_{p_1} - p_1)\psi_q^1 + \lambda\psi_{p_1}^1] \in \mathcal{O}(\mathcal{J}_{p,\Omega}^3(\mathbb{G}_m))^{\widehat{p}_1}, \\ f_2 &= (\phi_{p_1} - p_1)[(\phi_{p_2} - p_2)\psi_q^1 + \lambda\psi_{p_2}^1] \in \mathcal{O}(\mathcal{J}_{p,\Omega}^3(\mathbb{G}_m))^{\widehat{p}_2}, \end{aligned}$$

where $\lambda \in A_0^\times$. These f_1, f_2 have “Dirac decompositions,” and can be analytically continued.

Alternatively, if $n = 2$, and

$$(6.3) \quad \begin{aligned} f_1 &= \psi_q^1 + \lambda(\phi_{p_2} - p_2)\psi_{p_1}^1 \in \mathcal{O}(\mathcal{J}_{p,\Omega}^2(\mathbb{G}_m))^{\widehat{p}_1}, \\ f_2 &= \psi_q^1 + \lambda(\phi_{p_1} - p_1)\psi_{p_2}^1 \in \mathcal{O}(\mathcal{J}_{p,\Omega}^2(\mathbb{G}_m))^{\widehat{p}_2}, \end{aligned}$$

with $\lambda \in A_0^\times$, then f_1, f_2 can be analytically continued. Of course, in this case, f_1 and f_2 do not have “Dirac decompositions.”

We can raise the question of whether there exist values of λ such that the f_1, f_2 in these two examples possess nonstationary solutions (*i.e.*, solutions that effectively depend on q). The answer is *no* for the f_1, f_2 in (6.2), *cf.* Theorem 7.10 in [13]. We expect the answer to be *no* also in the case given by the f_1, f_2 in (6.3). The question then arises as to whether there actually exist equations f_1, f_2 in $1 + 2$ variables (not coming from fewer variables) that can be analytically continued and possess “nonstationary solutions.”

If the answer to this question were to be yes, an interesting theory could emerge. If the answer were to be *no*, we could be led to a generalization of the notion of solution. Both prospects seem quite intriguing at this point.

BIBLIOGRAPHY

- [1] M. BARCAU, “Isogeny covariant differential modular forms and the space of elliptic curves up to isogeny”, *Compositio Math.* **137** (2003), p. 237-273.
- [2] J. BORGER, “The basic geometry of Witt vectors”, arXiv:math/0801.1691.
- [3] J. BORGER & B. WIELAND, “Plethystic algebra”, *Adv. Math.* **194** (2005), no. 2, p. 246-283.
- [4] A. BUIUM, “Intersections in jet spaces and a conjecture of S. Lang”, *Ann. of Math.* **136** (1992), p. 583-593.
- [5] ———, *Differential Algebra and Diophantine Geometry*, Hermann, Paris, 1994.
- [6] ———, “Differential characters of Abelian varieties over p -adic fields”, *Invent. Math.* **122** (1995), p. 309-340.
- [7] ———, “Geometry of p -jets”, *Duke J. Math.* **82** (1996), no. 2, p. 349-367.
- [8] ———, “Differential modular forms”, *J. reine angew. Math.* **520** (2000), p. 95-167.
- [9] ———, “Arithmetic Differential Equations”, in *Math. Surveys and Monographs*, vol. 118, American Mathematical Society, Providence, RI, 2005, p. xxxii+310.
- [10] A. BUIUM & B. POONEN, “Independence of points on elliptic curves arising from special points on modular and Shimura curves, I: global results”, *Duke Math. J.*, to appear.
- [11] ———, “Independence of points on elliptic curves arising from special points on modular and Shimura curves, II: local results”, *Compositio Math.*, to appear.
- [12] A. BUIUM & A. SAHA, “Igusa differential modular forms”, preprint.
- [13] A. BUIUM & S. R. SIMANCA, “Arithmetic partial differential equations”, arXiv:math/0605107.
- [14] ———, “Arithmetic partial differential equations II: modular curves”, arXiv:0804.4856.
- [15] ———, “Arithmetic Laplacians”, *Adv. Math.* **220** (2009), p. 246-277.
- [16] C. DENINGER, “Local L -factors of motives and regularized determinants”, *Invent. Math.* **107** (1992), no. 1, p. 135-150.
- [17] B. DWORK, G. GEROTTO & F. J. SULLIVAN, “An introduction to G -functions”, in *Annals of Mathematics Studies*, vol. 133, Princeton University Press, Princeton, NJ, 1994, p. xxii+323.
- [18] M. GREENBERG, “Schemata over local rings”, *Ann. of Math.* **73** (1961), p. 624-648.
- [19] A. GROTHENDIECK, “La théorie des classes de Chern”, *Bull. Soc. Math. France* **86** (1958), p. 137-154.
- [20] C. HURLBURT, “Isogeny covariant differential modular forms modulo p ”, *Compositio Math.* **128** (2001), no. 1, p. 17-34.
- [21] A. JOYAL, “ δ -anneaux et λ -anneaux”, *C.R. Math. Rep. Acad. Sci. Canada* **4** (1985), p. 227-232.
- [22] V. KAC & P. CHEUNG, “Quantum calculus”, Universitext, Springer-Verlag, New York, 2002, x+112 pp.
- [23] E. R. KOLCHIN, “Differential algebra and algebraic groups”, in *Pure and Applied Mathematics*, vol. 54, Academic Press, New York-London, 1973, p. xviii+446.
- [24] Y. I. MANIN, “Cyclotomy and analytic geometry over \mathbb{F}_1 ”, arXiv:0809.1564.

- [25] ———, “Algebraic curves over fields with differentiation”, in *Ser. Mat.*, vol. 22, Izv. Akad. Nauk SSSR, 1958, AMS translations Series 2, 37 (1964), pp. 59-78, p. 737-756.
- [26] J. NEKOVÁR & N. SCHAPPACHER, “On the asymptotic behaviour of Heegner points”, *Turkish J. Math.* **23** (1999), p. 549-556.
- [27] M. RAYNAUD, “Courbes sur une variété abélienne et points de torsion”, *Invent. Math.* **71** (1983), p. 207-235.
- [28] SOULÉ, “Les variétés sur le corps à un élément”, *Moscow Math. J.* **4** (2004), no. 1, p. 217-244.
- [29] P. VOJTA, “Jets via Hasse-Schmidt derivations”, in *Diophantine geometry* (U. Zanier, ed.), CRM Series, vol. 4, Sc. Norm., Pisa, 2007, p. 335-361.
- [30] C. WILKERSON, “Lambda-rings, binomial domains, and vector bundles over $\mathbb{C}\mathbb{P}(\infty)$ ”, *Comm. Algebra* **10** (1982), no. 3, p. 311-328.

Manuscrit reçu le 11 décembre 2008,
accepté le 30 janvier 2009.

Alexandru BUIUM & Santiago R. SIMANCA
University of New Mexico
Department of Mathematics and Statistics
Albuquerque, NM 87131 (USA)
buium@math.unm.edu
santiago@math.unm.edu