BUIUM'S LEIDEN LECTURES ON ARITHMETIC DIFFERENTIAL EQUATIONS

ALEXANDRU BUIUM

Abstract. These notes develop the comparison between ordinary differential algebra and arithmetic differential algebra presented in Alexandru Buium's Leiden lectures. They begin with p-derivations and arithmetic jet spaces, then describe arithmetic differential characters, modular forms, special points, and two kinds of arithmetic partial differential equations. The account is based on Taylor Dupuy's initial conference notes and Buium's lecture handout [Bui09, §§1–5]. Results quoted from the lectures are attributed; the short calculations included here are given explicitly.

Contents

1. The analogy between functions and numbers 1
1.1. Derivations and Frobenius lifts 2
2. Differential functions and arithmetic jets 3
2.1. Characters and curves 4
3. Differential modular forms and special points 4
3.1. A Diophantine application 5
4. Partial differential equations with a prime and a variable 6
5. Partial differential equations at two primes 6
AI usage statement 7
References 7

1. The analogy between functions and numbers

The starting point of the lectures is the familiar dictionary

functions	numbers
$\mathbb{C}[x]$	$\mathbb{Z}$
finite extensions of $\mathbb{C}(x)$	finite extensions of $\mathbb{Q}$
points of a compact Riemann surface	places of a number field
Jacobian and its divisor classes	ideal class group

The question is what should fill the arithmetic side of the additional rows "differential calculus" and "differential equations." Fixing a prime p and replacing a derivation by a p-derivation provides Buium's answer [Bui09, §§1–2]. Here an arithmetic differential equation is an equation satisfied by numbers or points over a p-adic ring. This is distinct from a p-adic differential equation whose unknown is a function of a p-adic variable.

Date: Lorentz Center, Leiden, 5–9 October 2009.

Lectures delivered at the Lorentz Center, Leiden, 5–9 October 2009. Transcribed by Taylor Dupuy from his initial conference notes, with Buium's lecture handout as an additional source.

1.1. **Derivations and Frobenius lifts.** For a prime p, put

$$C_p(X,Y) = \frac{X^p + Y^p - (X+Y)^p}{p} \in \mathbb{Z}[X,Y]. \tag{1}$$

The integrality follows because p divides the intermediate binomial coefficients of $(X+Y)^p$.

Definition 1.1. Let R be a commutative ring.

(1) A *derivation* is a map $d : R \to R$ satisfying $d(x+y) = d(x) + d(y)$ and $d(xy) = xd(y) + yd(x)$.
(2) A *p-derivation* is a map $\delta : R \to R$ satisfying $\delta(1) = 0$ and

$$\delta(x+y) = \delta(x) + \delta(y) + C_p(x,y), \tag{2}$$

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y). \tag{3}$$

The powers in (3) matter: replacing x^p, y^p by x, y does not give the arithmetic product rule.

Proposition 1.2. *For every p-derivation δ on R, the map*

$$\phi(x) = x^p + p\delta(x) \tag{4}$$

is a ring endomorphism whose reduction modulo p is Frobenius. If R is p-torsion free, this construction is a bijection between p-derivations on R and ring endomorphisms $\phi : R \to R$ reducing to Frobenius modulo p.

Proof. Equation (2), together with the definition of C_p, gives $\phi(x+y) = \phi(x)+\phi(y)$. Expanding $(x^p + p\delta(x))(y^p + p\delta(y))$ and using (3) gives $\phi(xy) = \phi(x)\phi(y)$; also $\phi(1) = 1$. The reduction of (4) is $x \mapsto x^p$. Conversely, if R has no p-torsion, then $(\phi(x) - x^p)/p$ is uniquely defined in R and the same identities, read backwards, give (2)–(3). □

The comparison with dual numbers is equally concrete. The first dual number ring is $D_2(R) = R[\epsilon]/(\epsilon^2)$, with elements written $(a_0, a_1) = a_0 + a_1\epsilon$. The length-two p-typical Witt ring $W_2(R)$ has the same underlying set R^2, but its laws are

$$(a_0,a_1) +_W (b_0,b_1) = \big(a_0 + b_0,\, a_1 + b_1 + C_p(a_0,b_0)\big),$$
$$(a_0,a_1) \cdot_W (b_0,b_1) = \big(a_0b_0,\, a_0^p b_1 + b_0^p a_1 + pa_1b_1\big).$$

Thus d is a derivation exactly when $x \mapsto (x, d(x))$ is a ring map $R \to D_2(R)$, and δ is a p-derivation exactly when $x \mapsto (x, \delta(x))$ is a ring map $R \to W_2(R)$.

Example 1.3. The identity is the only Frobenius lift on $\mathbb{Z}$, and hence $\delta(a) = (a - a^p)/p$ is its unique p-derivation. For odd p its constants $\{a : \delta(a) = 0\}$ are $\{-1, 0, 1\}$; for $p = 2$ they are $\{0, 1\}$. More generally let

$$R = W(\overline{\mathbb{F}}_p) = \widehat{\mathbb{Z}_p^{\mathrm{ur}}}.$$

Its Witt Frobenius gives the canonical p-derivation $\delta(a) = (\phi(a) - a^p)/p$. Its δ-constants are zero and the Teichmüller representatives of $\overline{\mathbb{F}}_p^{\times}$, equivalently the roots of unity of order prime to p [Bui09, §2, examples].

The δ-constants form a multiplicative monoid by (3); they need not form an additive subgroup. This is an early warning that arithmetic differential algebra imitates, but does not copy, ordinary differential algebra.

2. Differential functions and arithmetic jets

For the rest of the one-prime discussion, take $R = W(\overline{\mathbb{F}}_p)$ with its canonical p-derivation, unless a different base is specified. All completions in this section are p-adic.

Definition 2.1. For a p-adically complete R-algebra with p-derivation and a smooth R-scheme X, a *δ-function of order at most n* on $X(R)$ is a function which, on an affine chart, can be written as a restricted power series in the coordinates $x, \delta x, \dots, \delta^n x$. Their ring is denoted $\mathcal{O}^n(X)$.

For an ordinary differential ring, one instead uses polynomials in $x, dx, \dots, d^n x$. The restricted power series are needed in the arithmetic case because the coefficient ring is complete and the relevant functions are p-adic limits of differential polynomials. One example on $\mathbb{A}^1(R)$ is

$$f(u) = \sum_{m \geq 0} p^m (\delta^3 u)^{8m^2} (\delta^2 u)^m u^{7m}.$$

Definition 2.2. Let $X = \operatorname{Spec} R[T_1, \dots, T_d]/(F_1, \dots, F_s)$ be affine. Extend δ to the polynomial ring in the formal variables $T, T', \dots, T^{(n)}$ by $\delta(T^{(i)}) = T^{(i+1)}$. The *nth arithmetic jet space* is

$$J^n(X) = \operatorname{Spf}\left(R[T, T', \dots, T^{(n)}]^{\wedge_p}/(F, \delta F, \dots, \delta^n F)\right). \tag{5}$$

For nonaffine X these local constructions glue. The truncation maps $J^n(X) \to J^{n-1}(X)$ and $J^0(X) = \widehat{X}$ form the jet tower.

The classical jet space is obtained from the same displayed presentation using an ordinary derivation, polynomial rings without completion, and Spec in place of Spf. The section of the arithmetic jet tower on R-points sends x to $(x, \delta x, \dots, \delta^n x)$. Evaluating functions along it gives a map

$$\mathcal{O}(J^n(X)) \longrightarrow \operatorname{Map}(X(R), R) \tag{6}$$

whose image is $\mathcal{O}^n(X)$. In the smooth case over the chosen R, Buium's handout identifies the source with this image [Bui09, §2, after the jet-space construction].

Proposition 2.3 (A limit of the classical analogy)**.** *Over a differential base, $J^1(X)$ is generally a torsor under the relative tangent bundle, rather than the tangent bundle itself; likewise higher differential jets are generally distinct from ordinary arc spaces. The familiar identifications apply when X descends to the ring of constants.*

This is the comparison made in the jet-space table [Bui09, §2, jet-space table]. The derivation of the base changes the gluing of the fibers even though those fibers look like affine spaces.

For a group scheme G, write $N^n(G) = \ker(J^n(G) \to \widehat{G})$.

Proposition 2.4 (Structure of the jet tower)**.** *If X/R is smooth of relative dimension d, each truncation $J^n(X) \to J^{n-1}(X)$ is Zariski locally a formal affine-space fibration with fiber $\widehat{\mathbb{A}}^d$. If G/R is a smooth group scheme, each $J^n(G)$ is a group object. For commutative G, the kernel $N^n(G)$ is a formal affine space of dimension nd as a formal scheme, but is generally not an additive formal vector group.*

This is the structural comparison in Buium's handout [Bui09, §2, jet-space table]. In particular, the underlying formal affine-space description does not determine the group law on the kernel.

2.1. **Characters and curves.** An arithmetic differential character of a commutative group scheme G is a group homomorphism $G(R) \to R$ represented by a δ-function. It is an arithmetic analogue of an ordinary differential character. For an abelian group H, write $p^\infty H = \bigcap_{m\geq 0} p^m H$. An elliptic curve over R is a *canonical lift* if its reduction is ordinary and it is the distinguished Serre–Tate lift of that reduction (the split deformation of its ordinary p-divisible group).

Theorem 2.5 (Buium: elliptic differential character)**.** *Let E/R be an elliptic curve. There is a nonzero arithmetic differential character $\psi : E(R) \to R$ of order at most two, and $[\ker \psi : p^\infty E(R)]$ is finite.*

This is the arithmetic half of Theorem 2 of the lecture handout [Bui09, §2, Thm. 2]. Its construction uses the extension $0 \to N^2 \to J^2(E) \to \widehat{E} \to 0$ and the connecting map from characters of N^2 to $H^1(E, \mathcal{O}_E)$. The handout only sketches that argument; the theorem is used here as an imported result.

Theorem 2.6 (Buium: the order-one obstruction)**.** *For E/R as in Theorem 2.5, a nonzero arithmetic differential character of order one exists if and only if E is a canonical lift.*

This is Theorem 3 of the lecture handout [Bui09, §2, Thm. 3]. Thus the natural expectation that every elliptic curve should have an order-one arithmetic Manin map fails for elliptic curves that are not canonical lifts.

Theorem 2.7 (Buium: projective space)**.** *For every $n \geq 0$ and $N \geq 1$, one has $\mathcal{O}^n(\mathbb{P}^N_R) = R$.*

This is Theorem 1 of the handout [Bui09, §2, Thm. 1].

Theorem 2.8 (Buium: higher-genus curves)**.** *If X/R is a smooth projective curve of genus at least two, then $J^n(X)$ is affine for $n \geq 1$ and $\mathcal{O}^1(X)$ separates the points of $X(R)$.*

This is Theorem 4 of the handout [Bui09, §2, Thm. 4]. The contrast is useful: ordinary regular functions on a projective curve cannot separate its points, while arithmetic differential functions can.

The handout also gives an effective Manin–Mumford bound for a genus-g curve X embedded in its Jacobian: the cardinality of $X \cap \mathrm{Jac}(X)_{\mathrm{tors}}$ is bounded by a quantity $C(g, p)$, where p is chosen as the smallest prime of good reduction [Bui09, §2, Thm. 5]. The draft of these notes asserted a stronger genus-only bound without a supporting argument. The bound stated here retains the dependence on p present in the lecture.

Question 2.9 (The 2009 handout's arithmetic analogue)**.** *For a smooth projective curve X/R of genus at least two, to what extent do arithmetic differential characters of its Jacobian, restricted to $X(R)$, generate the fraction field of $\mathcal{O}^1(X)$ over R?*

The handout lists a geometric generation theorem but marks its arithmetic counterpart open [Bui09, §2, Thm. 6 row]. Question 2.9 records the lecture's 2009 boundary; it does not assert that the question remains open today.

3. Differential modular forms and special points

Let $N \geq 4$ with $p \nmid N$, and let X be an open part of the ordinary locus of the modular curve $X_1(N)$, disjoint from its cusps. Write $\pi : \mathcal{E} \to X$ for the universal elliptic curve and $L = \pi_* \Omega^1_{\mathcal{E}/X}$. Let $V^\times$ be the torsor of nonzero invariant differentials. Its R-points are represented

by triples (E, α, ω): an elliptic curve, a level structure, and a nonzero invariant differential. A differential modular function of order at most n is an element of

$$M^n = \mathcal{O}^n(V^\times), \qquad M^\infty = \bigcup_{n \geq 0} M^n.$$

Definition 3.1. (1) The *weight ring* is $W = \mathbb{Z}[\phi]$. If $w = \sum_i a_i \phi^i \in W$, set $\deg(w) = \sum_i a_i$ and, for a unit $\lambda \in R^\times$, set $\lambda^w = \prod_i \phi^i(\lambda)^{a_i}$.

(2) A function $f \in M^n$ has *weight* w if $f(\lambda \cdot P) = \lambda^w f(P)$ for all λ and P. The module of such forms is $M^n(w)$.

Definition 3.2. Suppose $\deg(w)$ is even. A form $f \in M^n(w)$ is *isogeny covariant* if, whenever $u : E_1 \to E_2$ is an isogeny of degree *prime to* p and $u^*\omega_2 = \omega_1$, its values on the corresponding triples satisfy

$$f(E_1, \alpha_1, \omega_1) = \deg(u)^{-\deg(w)/2} f(E_2, \alpha_2, \omega_2).$$

The module of these forms is denoted $I^n(w)$.

The prime-to-p condition is essential in the lecture's definition [Bui09, §3, isogeny-covariance table]. The initial conference draft had $p \mid \deg(u)$ at this point.

On the ordinary locus the lecture states that the ring of isogeny covariant differential modular forms is δ-generated by two order-one forms

$$f^1 \in M^1(-1 - \phi), \qquad f^\partial \in M^1(\phi - 1).$$

It also identifies the δ-ideal kernel of the Fourier expansion map by f^1 and $f^\partial - 1$, and identifies the p-adic closure of its image with Katz's ring of generalized p-adic modular forms [Bui09, §3, Thm. 7]. These are imported assertions; the lecture gives constructions and a table of formulas, not full proofs. The same table notes that the classical theory has no counterpart of f^∂.

The geometric meaning of f^1 is especially striking. Local sections of $J^1(\mathcal{E}) \to \widehat{\mathcal{E}}$ differ on overlaps by elements of the kernel N^1, yielding a class in $H^1(\mathcal{E}, \mathcal{O}_\mathcal{E})$. Serre duality turns this class into f^1. For a point of the modular space, its vanishing characterizes a canonical lift [Bui09, §3, construction of f^1].

3.1. **A Diophantine application.** For a modular curve $S = X_1(N)$ and an elliptic curve A, a *modular–elliptic correspondence* consists of nonconstant maps $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ of smooth projective curves, with the marked points specified in [BP07, Def. 1.1]. Let $\mathrm{CM} \subset S(\overline{\mathbb{Q}})$ be the complex multiplication locus. A group Γ has finite rank if $\dim_{\mathbb{Q}}(\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}) < \infty$.

Theorem 3.3 (Buium–Poonen)**.** *For a modular–elliptic correspondence as above and a subgroup $\Gamma \leq A(\overline{\mathbb{Q}})$ of finite rank, $\Phi(\Pi^{-1}(\mathrm{CM})) \cap \Gamma$ is finite.*

This is [BP07, Cor. 2.3]; it is the global special-points result highlighted as Theorem 8 of the lecture handout [Bui09, §3, Thm. 8]. The local version replaces the CM locus by canonical-lift points and gives effective bounds under its local hypotheses [Bui09, §3, Thm. 9]. In that local argument a differential character on A is composed with Φ and paired with a differential modular function vanishing at canonical lifts. Eliminating the differential coordinates gives an order-zero equation; the finiteness step then uses a p-adic zero estimate. The incomplete placeholder calculation in the initial draft is not needed for this statement.

4. Partial differential equations with a prime and a variable

Buium's fourth handout section compares classical PDEs in variables (x,t) with arithmetic differential equations in (p,q) [Bui09, §4]. Keep $R = W(\overline{\mathbb{F}}_p)$ and set $A = R[[q]]$. Two operations on A are

$$\delta_p f(q) = \frac{\phi_R(f)(q^p) - f(q)^p}{p}, \qquad \delta_q f(q) = q\frac{df}{dq}, \tag{7}$$

where $\phi_R(f)$ applies Witt Frobenius to the coefficients. The first is a p-derivation and the second is an ordinary derivation. Arithmetic PDEs are restricted power series in iterates of these operations. For a group scheme G, the analogue of a linear differential operator is a group homomorphism $G(A) \to A$ represented by such a function.

Example 4.1. For $G = \mathbb{G}_m$, the first-order q-character is the logarithmic derivative $\psi_q^1(u) = \delta_q(u)/u$. Its arithmetic partner is obtained by applying the p-adic logarithm to $\phi(u)/u^p = 1 + p\delta_p(u)/u^p$; the initial terms are

$$\psi_p^1(u) = \frac{\delta_p u}{u^p} - \frac{p}{2}\left(\frac{\delta_p u}{u^p}\right)^2 + \cdots .$$

The logarithm converts multiplication in $\mathbb{G}_m(A)$ into addition in A. The series is interpreted p-adically on the indicated formal neighborhood [Bui09, §4, Thm. 10].

The lecture's classification compares convection, heat, and wave equations with arithmetic characters of $\mathbb{G}_a$, $\mathbb{G}_m$, and elliptic curves. For $\mathbb{G}_a$ the operators are built from the identity using ϕ_p and δ_q; for $\mathbb{G}_m$ they are built from the characters in Example 4.1. For a general elliptic curve in the lecture's (p,q) setup, the first-order pure p and pure q characters have no analogues, yet a mixed first-order character exists, along with second-order characters and a relation resembling a wave equation [Bui09, §4, Thm. 10]. This failure of the obvious first-order analogues is part of the result, not a missing construction.

The solution set of a character ψ is $\mathcal{U} = \{u \in G(A) : \psi(u) = 0\}$. If $\mu(R)$ denotes the roots of unity in R, the group ring $\mathbb{Z}[\mu(R)]$ acts on suitable solution sets by the substitutions $q \mapsto \zeta q$. Buium and Simanca describe nonstationary solutions and, under a nondegeneracy condition on the operator's symbol, obtain a finite free module of fundamental solutions [Bui09, §4, Thms. 11–12]. The handout states that condition only schematically, so no stronger unconditional classification is asserted here. The classical Laplace equation is listed there with no direct arithmetic analogue in this (p,q) comparison.

5. Partial differential equations at two primes

The fifth section of the handout starts with distinct primes p_1, p_2 and a smooth group scheme G over a ring of S-integers [Bui09, §5]. A p_i-derivation yields a local arithmetic differential character after p_i-adic completion. The two local characters live in different completed rings; one cannot simply equate their coefficients as global regular functions.

Definition 5.1. (1) Let $A_0 = \mathbb{Z}_{(p_1)} \cap \mathbb{Z}_{(p_2)}$, let B_0 be the coordinate ring after base change to A_0, and let $I \subset B_0$ be the ideal of a chosen section. Local elements ψ_{p_1} and ψ_{p_2} are *analytically continued along the section* if there is an element $\psi_0 \in \widehat{B_0}^{,I}$ whose images in the respective (I,p_1)- and (I,p_2)-adic completions equal the given local elements.

(2) A *linear arithmetic partial differential operator* on G is a pair of local linear characters admitting this continuation along the identity section.

Locally at the identity this asks whether two power series over $\mathbb{Z}_{p_1}$ and $\mathbb{Z}_{p_2}$ arise from one series over A_0. For $G = \mathbb{G}_m$, put

$$\chi_{p_i}(u) = \log\left(1 + p_i \frac{\delta_{p_i} u}{u^{p_i}}\right)$$

as a formal series near the identity. The handout constructs the order-two pair

$$\Psi_{p_1} = \left(1 - \frac{\phi_{p_2}}{p_2}\right)\chi_{p_1}, \qquad \Psi_{p_2} = \left(1 - \frac{\phi_{p_1}}{p_1}\right)\chi_{p_2}. \tag{8}$$

Their expansions at the identity come from the same A_0-series. This is the arithmetic counterpart of factoring $\partial_z \partial_{\bar{z}} \log u$ in two orders [Bui09, §5, example preceding Thm. 13].

For an elliptic curve E with ordinary reduction at both primes, let a_{p_i} be the corresponding Frobenius traces and let $\psi^2_{p_i}$ denote its one-prime order-two character. The handout forms a pair of order-four operators by

$$\Psi^4_{p_i} = \left(1 - a_{p_j}\frac{\phi_{p_j}}{p_j} + p_j\left(\frac{\phi_{p_j}}{p_j}\right)^2\right)\psi^2_{p_i}, \qquad \{i,j\} = \{1,2\}. \tag{9}$$

These formulas denote local components; their common expansion at the identity is what makes them a two-prime operator.

Theorem 5.2 (Buium–Simanca: the multiplicative case)**.** *Every linear arithmetic partial differential operator on $\mathbb{G}_m$ in the lecture's category is generated by the pair* (8)*.*

This is the attributed classification statement [Bui09, §5, Thm. 13].

Theorem 5.3 (Buium–Simanca: the elliptic case)**.** *If E has ordinary reduction at both p_1 and p_2, every linear arithmetic partial differential operator on E in the lecture's category is generated by the pair* (9)*.*

This is the attributed classification statement [Bui09, §5, Thm. 14]. The two-prime construction illustrates why analytic continuation is part of the definition: local differential equations at distinct primes need a common expansion before they form one arithmetic PDE.

AI usage statement

The starting materials for this transcription were Taylor Dupuy's initial notes from the 2009 Leiden conference and Alexandru Buium's lecture handout. OpenAI Codex (GPT-6, October 2026) assisted with completing the transcription, editing the exposition, checking notation and citations, and compiling the LaTeX. Codex also drafted this AI usage statement. The mathematical claims are attributed to the lecture handout or the cited literature; Codex is not an independent mathematical source or an author. Taylor Dupuy is responsible for the transcription and editorial choices in this edition.

References

[BP07] Alexandru Buium and Bjorn Poonen, *Relations among modular points on elliptic curves*, Preprint, arXiv:0706.0566, 2007, Corollary 2.3 gives the finite-rank intersection statement.

[Bui09] Alexandru Buium, *Lectures on arithmetic differential equations*, Lecture handout, Lorentz Center conference on lifts of Frobenius, Leiden, 5–9 October 2009, 2009, Source copy: official/lectures.tex in the Buium lifts-of-Frobenius archive.