

1

Introduction

Our purpose in this monograph is to provide a concise and complete introduction to the study of arithmetic differential operators over the p -adic integers \mathbb{Z}_p . These are the analogues of the usual differential operators over say, the ring $\mathbb{C}[x]$, but where the role of the variable x is replaced by a prime p , and the roles of a function $f(x)$ and its derivative df/dx are now played by an integer $a \in \mathbb{Z}$ and its Fermat quotient $\delta_p a = (a - a^p)/p$.

In making our presentation of these type of operators, we find no better way than discussing the p -adic numbers in detail also, and some of the classical differential analysis on the field of p -adic numbers, emphasizing the aspects that give rise to the philosophy behind the arithmetic differential operators. The reader is urged to contrast these ideas at will, while keeping in mind that our study is neither exhaustive nor intended to be so, and most of the time we shall content ourselves by explaining the *differential* aspect of an arithmetic operator by way of analogy, rather than appealing to the language of jet spaces. But even then, the importance of these operators will be justified by their significant appearance in number theoretic considerations. One of our goals will be to illustrate how different these operators are when the ground field where they are defined is rather coarse, as are the p -adic integers \mathbb{Z}_p that we use.

In order to put our work in proper perspective, it is convenient to introduce some basic facts first, and recall a bit of history. Given a prime p , we may define the p -adic norm $\|\cdot\|_p$ over the field of rational numbers \mathbb{Q} . The completion of the rationals in the metric that this norm induces is the field \mathbb{Q}_p of p -adic numbers, and this field carries a non-Archimedean p -adic norm extending the original p -adic norm on \mathbb{Q} . This is the description of \mathbb{Q}_p as given by K. Hensel circa 1897 (see, for instance,

[28]). Two decades later, A. Ostrovski [39] proved that any nontrivial norm on \mathbb{Q} is equivalent to either the Euclidean norm or to a p -adic norm for some prime p . In this way, there arose the philosophical principle that treats the real numbers and all of the p -adic numbers on equal footing.

In the twentieth century, the p -adic numbers had a rich history. We briefly mention some major results.

The idea that studying a question about the field \mathbb{Q} can be answered by putting together the answers to the same question over the fields \mathbb{R} and \mathbb{Q}_p for all p s was born with the Hasse–Minkowski’s theorem. This states that a quadratic form over \mathbb{Q} has a nontrivial zero in \mathbb{Q}^n if, and only if, it has a nontrivial zero in \mathbb{R}^n and a nontrivial zero in \mathbb{Q}_p^n for each prime p . This theorem was proven by Hasse in his thesis around 1921 [27], the problem having been proposed to him by Hensel who had proven the $n = 2$ case a few years earlier. Such a principle fails for cubics.

The development above came after several interesting results that preceded the introduction of the p -adic numbers. The local-to-global principle embodied in the Hasse–Minkowski theorem had a precedent in Riemannian geometric, since as recently as 1855, Bonnet had proved that if the curvature of a compact surface was bounded below by a positive constant, then its diameter was bounded above by a quantity depending only on the said constant. Strictly on the arithmetic side of things, in the seventeenth century J. Bernoulli defined the Bernoulli numbers B_k , the coefficients in the expansion $e^t/(e^t - 1) = \sum_k B_k t^k/k!$, used them to compute closed-form expressions for the sums $\sum_{j=0}^m j^n$, and developed several identities that these numbers satisfy. A century later, the Bernoulli numbers were used by Euler to show heuristically that if ζ is the Riemann zeta function, then $\zeta(1 - k) = \sum_{n=1}^{\infty} 1/n^{1-k} = -B_k/k$ for any integer $k \geq 2$. In the mid nineteenth century, Riemann proved that $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ is a meromorphic function on the complex plane \mathbb{C} , giving Euler’s argument complete sense. Further, he used the Gamma function to define $\Lambda(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$ and proved the functional equation $\Lambda(s) = \Lambda(1 - s)$. The intimate relationship between the Bernoulli numbers and the values of $\zeta(s)$ at negative integers led to the idea that these numbers have profound arithmetical properties, a fact discovered by Kummer in his work on Fermat’s last theorem circa 1847. The ideal class group of $\mathbb{Q}(\zeta_N)$, ζ_N a primitive N -th root of unity, is the quotient of the fractional ideals of $\mathbb{Q}(\zeta_N)$ by the set of principal ideals, and it turns out to be a group of finite order h_N with respect to ideal multiplication. A prime p is said to be regular if $p \nmid h_p$, and irregular otherwise. Kummer proved that p is regular if, and only if, p does not divide the

numerator of B_2, B_3, \dots, B_{p-3} and that Fermat last theorem holds for all regular primes. He also proved that, if $m \equiv n \not\equiv 0 \pmod{p-1}$, then $B_m/m \equiv B_n/n \pmod{p}$, the congruences that are nowadays named after him. They led to the proof that there are infinitely many irregular primes. Since heuristically it can be proven that there is a large percentile of regular primes, Kummer's ideas had remarkable implications in the study of Fermat's last theorem. Thus, algebraic number theory and the theory of L -functions were born and replaced the elementary methods used before him in the analysis of this problem.

C. Chevalley defined the *adèle* ring and *idèle* group [20], and used them to reformulate class field theory [21] around 1932. For convenience, if we denote by $\|\cdot\|_\infty$ the Euclidean norm in \mathbb{R} , which we think of as \mathbb{Q}_∞ , the field of p -adic numbers corresponding to $p = \infty$, we take the Cartesian product $\mathbb{Q}_\infty \times \prod_p \mathbb{Q}_p$, and define the adèle ring $\mathbb{A}_\mathbb{Q}$ to be

$$\mathbb{A}_\mathbb{Q} = \left\{ (a_\infty, a_2, a_3, a_5, \dots) \in \mathbb{Q}_\infty \times \prod_p \mathbb{Q}_p : \|a_p\|_p \leq 1 \text{ for almost all } ps \right\}.$$

Its ring structure is obtained by defining addition and multiplication component-wise; it contains an isomorphic image of \mathbb{Q} via the mapping

$$\mathbb{Q} \ni q \xrightarrow{a_\mathbb{Q}} (q, q, \dots) \in \mathbb{A}_\mathbb{Q}.$$

For $a \in \mathbb{Q}_\infty \times \prod_p \mathbb{Q}_p$, we define $\|a\|_p = \|a_p\|_p$. Then $a \in \mathbb{A}_\mathbb{Q}$ if, and only if, $\|a\|_p \leq 1$ for all but finitely many ps . The subset $I_\mathbb{Q}$ of $\mathbb{A}_\mathbb{Q}$ consisting of all a s such $\|a\|_p \neq 0$ for all ps , and $\|a\|_p = 1$ for all but finitely many of them, is the idèle multiplicative group. It contains an isomorphic image of \mathbb{Q}^\times by restriction of the mapping $a_\mathbb{Q}$ above. If F is an extension of \mathbb{Q} , the norms on \mathbb{Q} can be extended to norms on F , and we naturally define I_F also. There is a norm homomorphism $I_F \rightarrow I_\mathbb{Q}$, and its image $N(I_F/I_\mathbb{Q})$ is a group. The Galois group of F/\mathbb{Q} is naturally isomorphic to $I_\mathbb{Q}/\mathbb{Q}^\times N(I_F/I_\mathbb{Q})$. Chevalley proved this fact using the local theory, avoiding the use of tools from analytic number theory. He generalized it also for number fields, fields that are extensions of \mathbb{Q} of infinite degree.

In his thesis, J. Tate used real harmonic analysis on the adèles to prove functional equations for the Riemann zeta function. T. Kubota and H.W. Leopoldt [32] introduced a p -adic version of the Riemann zeta function, and used it to interpret Kummer's congruences for Bernoulli numbers mentioned above, which date back to 1851. Y.I. Manin and B. Mazur [38] interpreted the result of Kubota and Leopoldt in terms of a p -adic Mellin transform, and found p -adic interpretations of L -

functions of elliptic curves. The p -adic integers \mathbb{Z}_p were known to appear as Galois groups of some infinite cyclotomic extensions. K. Iwasawa considered the completed group algebras of these Galois groups, which act on class groups and make them modules over the completed groups. These modules have some invariants. Iwasawa conjectured that these invariants could be read off from classical Dirichlet L -functions after a p -adic interpolation, using the p -adic Mellin transform. This conjecture was proved by B. Mazur and A. Wiles [33]. Triggered by the work of Tate, B. Dwork studied p -adic differential equations, and gave a p -adic proof of the rationality of Weil's zeta function [23], taking then a major step in the settling of all of the Weil conjectures about this function [48], work that was completed by P. Deligne [22]. J.-P. Serre and N. Katz studied several other p -adic functions of arithmetic interest, and A. Grothendieck studied p -adic cohomology and crystalline cohomology.

The list of problems in the field is outstanding, and the list of contributors to their understanding and resolution is important. We have not come even close to exhausting either one. But we can now retake the main theme of our work in this introduction with a better perspective in mind.

In the course of modern mathematical history, analogies between functions and numbers have played an important role in the development of number theory. The fundamental theorems of algebra and arithmetic can be seen as counterparts to each other, with the integers -1 , 0 and 1 playing the role of the constant polynomials in $\mathbb{C}[x]$. This point of view is once again motivational to the philosophy of arithmetic differential operators, the idea at the level of the integers \mathbb{Z} being to find an appropriate substitute $\delta_p : \mathbb{Z} \rightarrow \mathbb{Z}$ for the derivative operator

$$\partial_x = \frac{d}{dx} : \mathbb{C}[x] \rightarrow \mathbb{C}[x].$$

Indeed, given a “number” x , lets us think of it as a “function,” and consider the expression $x - x^p$, one that makes frequent appearances in number theoretic considerations. For \mathbb{F}_p , the finite field of p elements, the identity $x - x^p = 0$ holds for all elements. In the more general situation, we can restrict our attention to numbers such that $x - x^p \equiv 0 \pmod{p}$. We think of x as a function of p , and interpret the difference $x - x^p$ as the variation of x as its argument changes to p . We then use the Fermat quotient

$$\delta_p x = \frac{x - x^p}{p} \tag{\dagger}$$

to define the notion of arithmetic derivative of x in the direction of p . This is the notion that we shall be studying here, most of the time restricting our attention to x s that are taken from the ring of p -adic integers \mathbb{Z}_p . At this point, though, this quotient is just a heuristic statement.

The theory of arithmetic differential operators that ensues from the idea outlined above was proposed by A. Buium [6, 8], with δ_p serving in the role of the arithmetic analogue of the operator ∂_x on the polynomial ring $\mathbb{C}[x]$. At the purely arithmetic level, it serves also as a substitute for Dwork's operator

$$\frac{d}{dx} : \overline{\mathbb{F}}_p[x] \rightarrow \overline{\mathbb{F}}_p[x]$$

in his theory of p -adic differential equations over the differential field $\overline{\mathbb{F}}_p[x]$, $\overline{\mathbb{F}}_p$ the algebraic closure of the field \mathbb{F}_p with p -elements. In Dwork's theory [25], the x s are still being viewed as an "argument to the functions" rather than as functions themselves. But the arithmetic differential operator δ_p exhibits an additional fundamental difference with the Dwork's operator that is worth pointing out now: δ_p is highly nonlinear, with additivity holding only modulo a lower order term measured by a polynomial with integer coefficients, and a Leibniz rule that holds but only highly intertwined with the p -th power homomorphism, and modulo terms that are p -adically smaller.

In fact, more can be said at this point. If we were to develop a differential theory with operators of the type

$$u \mapsto P\left(u, \frac{du}{dx}, \dots, \frac{d^r u}{dx^r}\right)$$

where $P(x_0, \dots, x_r)$ is a polynomial function, we would obtain the Ritt–Kolchin theory of "ordinary differential equations" with respect to $\frac{d}{dx}$, cf. [41, 30, 19]. This would lead to the notion of the $\frac{d}{dx}$ -character of an algebraic group, which should be viewed as the analogue of a linear ordinary differential operator on an algebraic group (cf. to the Kolchin logarithmic derivative of algebraic groups defined over $\widehat{\mathbb{Z}}_p^{ur}$, [30, 19], and the Manin maps of Abelian varieties defined over $\widehat{\mathbb{Z}}_p^{ur}[[q]]$ [38, 12], $\widehat{\mathbb{Z}}_p^{ur}$ the unramified completion of the ring of p -adic integers).

If instead we were to develop a theory with operators that are the p -adic limits of $P(u, \delta_p u, \dots, \delta_p^r u)$, $P(x_0, \dots, x_r)$ a polynomial, we would then obtain the arithmetic analogue of the ordinary differential equations of Buium, as found in [8, 9, 6]. In particular, we would then arrive at

the notion of a δ_p -character of a group scheme, the arithmetic “version” of a linear ordinary differential equation on a group scheme.

In this monograph, we apply and study Buium’s idea over the rather coarse ring of p -adic integers \mathbb{Z}_p . We think of the elements in this ring as functions over a space of dimension zero that vary *infinitesimally* according to the heuristic equation (\dagger) at the prime p . The ensuing notion of derivative is the one alluded to in the title, and on which we shall elaborate extensively in what follows. We will pause at some point to define these arithmetic operators with the generality given in Buium’s work. This will benefit the interested reader while allowing us to contrast the behaviour of these operators when defined over \mathbb{Z}_p or $\widehat{\mathbb{Z}}_p^{ur}$. Ultimately, it is the fact that we can cast these operators as global functions on a suitable arithmetic jet space, for any smooth scheme of finite type, which allows for their interpretation as differential operators of sorts, the way the usual differential operators on a manifold are sections of its jet bundles.

Given such a notion of arithmetic derivative, we then may define in the obvious manner an arithmetic differential operator of order n , where n is an arbitrary positive integer. Over the ring of p -adic integers \mathbb{Z}_p , we have also the classical notion of an analytic function. We shall show that all arithmetic differential operators turn out to be analytic functions. Quite remarkably in fact, characteristic functions of p -adic discs are shown to be equal to arithmetic operators of an order that depends upon the radius of the disc, generalizing a result that we first prove via an explicit construction, namely that the characteristic function of a disc of radius $1/2$ over the 2-adic integers is an arithmetic differential operator of order one. The extended result for a general prime is a bit surprising, point upon which we will elaborate in due course.

We organize our work as follows: in Chapter 2, we summarize the construction of the p -adic numbers and the p -adic integers, describe its topology as a metric space, its analytic and algebraic properties, and study the $(p-1)$ -roots of unity in it. In Chapter 3 we study some results from classical analysis on \mathbb{Q}_p , including Mahler’s theorem that establishes a bijection between the sets of restricted sequences and that of continuous functions on \mathbb{Z}_p , we present basic properties of the Artin–Hasse function, and study the analytic completion of the algebraic closure of \mathbb{Q}_p , the p -adic alter ego of the complex numbers that result when we complete \mathbb{Q} in the Euclidean metric instead. In Chapter 4 we introduce the set of analytic functions as a required preliminary to our discussion later on. The arithmetic differential operators make their

first appearance in Chapter 5, where we tie them to their associated homomorphisms. This in turn allows us to prove that equation (\dagger) defines the only arithmetic differential operator over \mathbb{Z}_p since this ring carries just one automorphism. Using it as a building block, we define an arithmetic differential operator of any order. We discuss also the basic rings that must be used in the theory when we have multiple primes, essentially to indicate the additional difficulties that arise then. In Chapter 6 we pause to define arithmetic operators in general, developing succinctly the theory of arithmetic jet spaces of Buium. In order to make things easier for analysts not accustomed to algebraic concepts, we present a list of the concepts from commutative algebra and schemes that are needed in the development of the general theory. In the case of group schemes, we discuss the characters that have been alluded to earlier, the analogs in the theory of the *linear* differential operators. And we outline the theory for multiple primes also, in a succinct manner. In Chapter 7 we prove that all arithmetic differential operators over \mathbb{Z}_p are analytic functions. In Chapter 8 we study characteristic functions of p -adic discs from the point of view of the theory of arithmetic differential operators, and prove that they are indeed differential operators of an order depending upon the radii of the discs. The prime $p = 2$ manifests itself in a rather special manner here, as we are able to prove by way of a direct argument that the characteristic function of a discs of radius $1/2$ over the 2-adic integers is an arithmetic differential operator of order one. This work is carried out in *standard coordinates*, and leads to some formal power series representations of the characteristic functions when the prime in question is singular, a concept that we define then. In Chapter 9 we work with *harmonic coordinates*, and improve significantly upon the result in the previous chapter, showing that all analytic functions on \mathbb{Z}_p are arithmetic differential operators, with the order being equal to the level of analyticity. This last concept had made its first appearance earlier, in the context of Chapter 4. Finally, in Chapter 10, we exhibit some fundamental differences in the behavior of arithmetic differential operators that manifest when we work over the ring $\widehat{\mathbb{Z}}_p^{ur}$ instead of \mathbb{Z}_p . In particular, we indicate how to show that as soon as we adjoin one unramified root of unity to \mathbb{Z}_p , the counterpart of the theorem above on the characteristic function of discs no longer holds.

2

The p -adic numbers \mathbb{Q}_p

The field \mathbb{Q}_p of p -adic numbers is the completion of the field \mathbb{Q} of rational numbers with respect to the p -adic norm. In this chapter, we explain their construction from various points of view, all, of course, equivalent to each other.

Let $p \in \mathbb{Z}$ be a prime that we fix hereafter. For $a \in \mathbb{Z}$, we let $\text{ord}_p a$ be the exponent of p in the prime factorization of a , that is to say, the integer l such that $a = p^l r$, where $r \in \mathbb{Z}$ is not divisible by p . This notion is extended to a rational number $q = a/b$ by setting $\text{ord}_p q = \text{ord}_p a - \text{ord}_p b$, and the resulting function is multiplicative, that is to say, it has the property that $\text{ord}_p q_1 q_2 = \text{ord}_p q_1 + \text{ord}_p q_2$. We then define the p -adic norm function on \mathbb{Q} by

$$\|q\|_p = \frac{1}{p^{\text{ord}_p q}}. \quad (2.1)$$

We shall denote by d_p the metric on \mathbb{Q} that this norm induces.

In the resulting norm on \mathbb{Q} , a rational q has $\|q\|_p \leq 1$ if, and only if, the denominator b of its reduced rational form a/b is not divisible by p . Integers are closer to each other in the metric d_p on \mathbb{Q} the higher the power of p that divides their difference. So, for instance,

$$d_5(2, 1) = \|1 - 2\|_5 = 1, \text{ while } d_5(2, 127) = \|2 - 127\|_5 = \frac{1}{5^3}.$$

The p -adic norm satisfies a condition stronger than the triangle inequality. Indeed, if $q = a/b$ and $r = c/d$, since the biggest power of p that divides $ad+bc$ is at least the minimum of the biggest power dividing

ad and the biggest power dividing bc , we have that

$$\begin{aligned} \text{ord}_p(q+r) &= \text{ord}_p\left(\frac{ad+bc}{bd}\right) \\ &\geq \min\{\text{ord}_p ad, \text{ord}_p bc\} - \text{ord}_p b - \text{ord}_p d \\ &= \min\{\text{ord}_p a + \text{ord}_p d, \text{ord}_p b + \text{ord}_p c\} - \text{ord}_p b - \text{ord}_p d \\ &= \min\{\text{ord}_p a - \text{ord}_p b, \text{ord}_p c - \text{ord}_p d\} \\ &= \min\{\text{ord}_p q, \text{ord}_p r\}, \end{aligned}$$

and therefore,

$$\|q+r\|_p = \frac{1}{p^{\text{ord}_p(q+r)}} \leq \max\{p^{-\text{ord}_p q}, p^{-\text{ord}_p r}\} = \max\{\|q\|_p, \|r\|_p\}. \tag{2.2}$$

The triangle inequality now follows readily. This stronger inequality (2.2), referred to as the “non-Archimedean property” of $\|\cdot\|_p$, produces some geometric results that contrast a bit with those from our more traditional point of view in Euclidean geometry. Triangles, for instance, are all isosceles.

For let us assume that we have a “triangle with vertices at $0, q$ and r ,” respectively. We then know that $\|q-r\|_p \leq \max\{\|q\|_p, \|r\|_p\}$. If $\|q\|_p < \|r\|_p$, the non-Archimedean property of the norm implies that

$$\|q-r\|_p \leq \|r\|_p.$$

Since $\|r\|_p = \|q-(q-r)\|_p \leq \max\{\|q\|_p, \|q-r\|_p\}$, it follows that

$$\|r\|_p \leq \|q-r\|_p$$

also. Thus, $\|r\|_p = \|q-r\|_p$ and so, in the geometry generated by $\|\cdot\|_p$, all triangles are isosceles, with the two largest sides equal to each other in length. Sometimes we shall refer to this as the “isosceles triangle property” of $\|\cdot\|_p$.

Now we describe briefly the general process that defines \mathbb{Q}_p as the metric completion of \mathbb{Q} in the distance defined by the p -adic norm. This yields \mathbb{Q}_p as the unique complete field, up to isometric isomorphism, that contains a $\|\cdot\|_p$ -isometric dense copy of the field \mathbb{Q} .

We say that a sequence $\{q_n\}$ of rational numbers is Cauchy with respect to the norm $\|\cdot\|_p$, if for any real number $\varepsilon > 0$ there exists N such that $\|q_n - q_m\|_p < \varepsilon$ for all $n, m \geq N$. We say that the sequence $\{q_n\}$ is null if for any $\varepsilon > 0$ there exists N such that $\|q_n\|_p < \varepsilon$ for all $n \geq N$.

Given rational Cauchy sequences $\{q_n\}$ and $\{r_n\}$, we define their addition and multiplication by

$$\{q_n\} + \{r_n\} = \{q_n + r_n\}, \quad \{q_n\}\{r_n\} = \{q_n r_n\}.$$

Let R be the set of all rational Cauchy sequences, and let M be the subset of all null sequences. The operations above provide R with a ring structure, and M becomes an ideal in R . In fact, M is a maximal ideal. For if $\{q_n\} \in R$ is not null, there exists an $\varepsilon > 0$ and an integer N such that $\|q_n\|_p > \varepsilon$ for any $n > N$, and we may set

$$r_n = \begin{cases} 0 & \text{for } n \leq N, \\ \frac{1}{q_n} & \text{for } n > N. \end{cases}$$

This is a Cauchy sequence also, and we have

$$\{q_n\}\{r_n\} = \{0, \dots, 0, 1, 1, \dots\} = \{1, 1, \dots\} - \{1, \dots, 1, 0, 0, \dots\}.$$

If I were an ideal with $M \subset I$ properly, then I would contain a non-null sequence $\{q_n\}$. Since the sequence $\{1, \dots, 1, 0, 0, \dots\}$ is null, the argument above with r_n would imply that the constant sequence $\{1, 1, \dots\}$ must be contained in I , and so I would have to be equal to R . Thus, M is a maximal ideal. The quotient field R/M is, by definition, the field of p -adic numbers \mathbb{Q}_p .

An additional detail exhibits a fundamental difference between this construction of \mathbb{Q}_p and the analogous construction of \mathbb{R} as the completion of \mathbb{Q} in the Euclidean norm. Given a p -adic number $\alpha = \{q_n\} + M$, if the Cauchy sequence $\{q_n\}$ is null, we set $\|\alpha\|_p = 0$. Otherwise, there exist a positive real number ε and an integer N such that $\|q_n\|_p > \varepsilon$ for any $n > N$. We may choose N sufficiently large so that $\|q_n - q_m\|_p < \varepsilon$ for $n, m > N$ also. Then, by the isosceles triangle property, we have that $\|q_n\|_p$ is constant for all $n > N$, and so we may define

$$\|\alpha\|_p = \lim_{n \rightarrow \infty} \|q_n\|_p,$$

extending in this manner the p -adic norm on \mathbb{Q} to a p -adic norm on \mathbb{Q}_p . Using this extension, we may also extend the notion of p -adic order.

In the construction of \mathbb{R} as the completion of \mathbb{Q} in the Euclidean norm, this said norm admits an extension to a norm on \mathbb{R} as well. However, in spite of the fact that their constructions derive from exactly the same procedure, this and the p -adic norm above exhibit a substantial difference. For unlike the case of the Euclidean norm on \mathbb{R} , the extended $\|\cdot\|_p$ -norm on \mathbb{Q}_p still ranges over the set $\{0\} \cup \{p^n\}_{n \in \mathbb{Z}}$, the same range this norm function has over \mathbb{Q} , whereas, for \mathbb{R} , the range of the Euclidean norm is \mathbb{R} itself.