Informal Talk Notes for the P-Adic People Seminar

Stephanie A.

February 2026

Contents

1 2/2/26: The Algebra and Arithmetic of $\mathbb{Q}_p$ and $\mathbb{Z}_p$

Goal(s):

1. Review canonical forms of p-adics and prove periodicity of the canonical form of a rational number
2. Introduce arithmetic with p-adics using their canonical forms
3. Describe and prove some algebraic properties of the ring of p-adic integers $\mathbb{Z}_p$, including existence of the **Teichmuller character** ω

Given a level of comfort with canonical p-adic expansions is required in order to perform p-adic arithmetic, we begin with relevant review.

1. Recall that a p-adic number x can be defined by a **formal Laurent series** $a = \sum_{i=k}^{\infty} a_i p^i$.
2. We follow an algorithm dependent on modular arithmetic in order to determine the coefficients of our series and write out the base p expansion of a.
3. We can now write a in its **canonical form**.

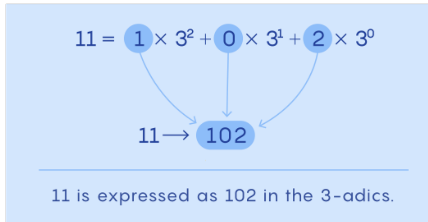

Figure 1: Recall in comparison the **base p expansion** of a number.

Definition 1. Canonical form of a p-integer
Let $a \in \mathbb{Z}_p$ be an equivalence class of **Cauchy sequences** in $\mathbb{Q}$ w.r.t. to the extension of the **p-adic norm**. We can write

$$a = ...d_n...d_2d_1d_0,$$

with d_i extending infinitely to the left.

Example 1. 5-adic Integers

- $15 = 3 \times 5^1 + 0 \times 5^0$, so $15 = ...0030_5$. *Note the 5-adic base expansion of a positive integer is identical to its base 5 expansion.*
- -1 = $\overline{.4}_5$, verifiable by th geo series formula $\sum_{i=0}^{\infty} = \frac{a}{1-r} = \frac{4}{1-5} = -1$.
- $-3 = \overline{.4}2$

Not all rational numbers can be written as p-integers, so we have the p-numbers of form $\frac{x}{p^k}$.

Example 2. $\frac{1}{p} = .1_p$, similar to how $\frac{1}{10} = .1_{10}$.

Recall the p-adic valuation of a number, denoted $|x|_p$, measures its "size" in the p-adic world. For a prime p, $|p|_p = 1/p$, and $|1/p|_p = p$. The p-adic integers $\mathbb{Z}_p$ have a p-adic valuation of 1 or less by definition. Since $|1/p|_p = p > 1$, $1/p$ cannot bee a p-adic integer, but it is a p-adic number.

Definition 2. Canonical form of a p-number
Let $a \in \mathbb{Q}_p$ be an equivalence class of **Cauchy sequences** in $\mathbb{Q}$ w.r.t. to the extension of the **p-adic norm**. We can write

$$a = ...d_n...d_2d_1d_0d_{-1}...d_{-m},$$

with infinitely many p-adic digits d before a radix point and finitely many digits after a radix point.

Remark. If two p-adic expansions converge to the same p-adic number, *all their p-adic digits are identical.* We emphasize the uniqueness of such representations.

Theorem 1.1. [Kat07] The canonical p-adic expansion (see Definition 2) represents a rational number if and only if it is eventually periodic to the left.

(WTS: Rationality $\implies$ Periodicity and Periodicity $\implies$ Rationality)

Proof: [1]

$\Longrightarrow$

1. Assume the canonical p-adic expansion of x is eventually periodic. **A useful tool in p-adic analysis is to reduce the scope of analysis to the ring $\mathbb{Z}_p$,** which we can achieve by multiplying x by a suitable power of p (if necessary). Now let us subtract a rational to give $x \in \mathbb{Z}_p$ a periodic expansion of form

$$x = x_0 + x_1p^1 + x_2p^2 + ... + x_{k-1}^p k - 1 + x_0p^k + x_1p^{k+1}.$$

2. The number $a = x_0 + x_1p^1 + x_2p^2 + ... + x_{k-1}^p k - 1$ is a rational by existence of negative powers and we can express x in form

$$x = a(1 + p^k + p^{2k} + ...) = a\frac{1}{1 - p^k},$$

which is a rational number.

$\Longleftarrow$

1. Suppose a, b rel. prime and b, p rel. prime for

$$\frac{a}{b} = \sum_{i \geq 0} x_i p^i \in \mathbb{Z}_p.$$

2. Since $\gcd(b, p^n) = 1$, there exists c_n, d_n st $1 = c_nb + d_np^n$, which we **multiply by** a to obtain $a = ac_nb + ad_np^n$.

3. Add $ac_n + p^n$ and set $A_n = ac_n + p^n \leq p^n - 1$ considering the above equation. Also set $r_n = ad_n$ so that we have

$$a = A_nb + r_np^n$$

4. **Divide by** b to obtain

$$\frac{a}{b} = A_n + p^n\frac{r_n}{b}.$$

So

$$r_n = \frac{a - A_nb}{p^n},$$

which we will use to **form an inequality**:

$$\frac{a - (p^n - 1)b}{p^n} \leq r_n \leq \frac{a}{p^n}.$$

[1] As a convention, we intend to keep most proofs terribly informal throughout, but refer one to the bibliography for appropriate constructions and details.

5. For sufficiently large n,
$$-b \leq r_n \leq 0,$$
r_n **only takes finite many values, bounding** A_n. We can write
$$\frac{a}{b} = A_n + p^n \frac{r_n}{b} = A_{n+1} + p^{n+1} \frac{r_{n+1}}{b},$$
which implies
$$A_{n+1} - A_n = p^n \left(\frac{r_n}{b} - p \frac{r_{n+1}}{b} \right).$$
Since $A_{n+1} - A_n$ is an integer, $\frac{r_n - p r_{n+1}}{b}$ must also be an integer. Crucially, as $A_{n+1} \equiv A_n \pmod{p^n}$, so we have $A_{n+1} = A_n + x_n p^n$, where $\{A_n\}$ **is the sequence of partial sums of the** p**-adic expansion of** $\frac{a}{b}$.

6. Since r_n **takes only finite many values, there exists an index and positive integer** P st $r_m = r_m + P$, hence
$$x_m b + p r_{m+1} = x_{m+P} b + p r_{m+P+1},$$
so that
$$(x_m - x_{m+P}) b = p(r_{m+P+1} - r_{m+1}).$$

7. Since $(b, p) = 1$, it follows $p \mid (x_m - x_{m+P})$ and given x_m, x_{m+P} are both digits in $\{0, 1, 2, ...p-1\}$, we must have $x_m = x_{m+1}$. Subbing back into
$$x_m b + p r_{m+1} = x_{m+P} b + p r_{m+P+1},$$
also gives $r_m = m + 1 = r_{m+P+1}$.

8. Repeating the above argument,
$$r_n = r_{n+P}, \quad x_n = x_{n+P}, \quad n \geq m,$$
which shows that **the digits** x_n **and numerators** r_n **have period length** P **for** $n \geq m$.

∎

1.1 Arithmetic

The reduction to canonical form leads to an addition/subtraction system of carries similar to $\mathbb{R}$ but starting from right to left (see Figure 2).

We must recall the concept of a multiplicative inverse in order to retain some notion of division with p-adics.

Definition 3. Multiplicative Inverse

We say a^{-1} is the inverse of a if $aa^{-1} = e$, where e is the multiplicative identity. If the multiplicative inverse a^{-1} exists, it is *unique*.

Proposition 1.1. [Kat07] A p-adic integer $a = ...a_1 a_0 \in \mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.

$$
\begin{array}{cccccccc}
 & & & 1 & 1 & & 1 & \\
 & \cdots & 0 & 1 & 2 & 1 & 0 & 2_3 \\
+ & \cdots & 1 & 0 & 1 & 2 & 1 & 1_3 \\
\hline
 & \cdots & 1 & 2 & 1 & 0 & 2 & 0_3
\end{array}
$$

Figure 2: $146 + 292 = 438$ in the 3-adics [Image Source: Wikipedia]

Proof: We will leave the details of this proof as a straightforward exercise, but **one should show**: Existence of unit $u \in \mathbb{Z}_p^\times \implies a_0 \neq 0$ and $a_0 \neq 0 \implies$ Existence of unit $u \in \mathbb{Z}_p^\times$. ∎

Example 3. Inverses[2] in $\mathbb{Z}_5$ and their 5-adic expansions

- The inverse of 2 is 3 in $\mathbb{Z}_5$, with 5-adic expansion $\ldots 0003_5$.
- The inverse of 3 is 2 in $\mathbb{Z}_5$, with 5-adic expansion $\ldots 0002_5$.
- The inverse of 4 is 4 in $\mathbb{Z}_5$, with 5-adic expansion. $\ldots 0004_5$

Proposition 1.2. [Kat07] Let x be a p-adic number of norm p^{-n}. Then p can be written as the product $p^n u$, where $u \in \mathbb{Z}_p^\times$.

Recall the below basic definitions:

Definition 4. p-adic valuation

The valuation $v_p(x)$ is an integer representing the exponent of p in the prime factorization of x (in the field of p-adic numbers $\mathbb{Q}_p$).

Definition 5. p-adic norm

The p-adic norm of a non-zero p-adic number x, denoted by $|x|_p$, is defined as $p^{-v_p(x)}$, where $v_p(x)$ is the p-adic valuation of x.

Proof: We will also leave this proof as an exercise. ∎

1.2 Algebra

1.2.1 Review of Ring Theory

Given we perform addition and multiplication in $\mathbb{Z}_p$, it forms a **ring**. Let us review some basic definitions from ring theory.

Definition 6. Commutative Ring

A ring R is a set equipped with two binary operations $(+, \times)$ in which multiplication is commutative. As a ring, R must also satisfy the following ring axioms:

1. R is abelian under addition

[2] We omit the invertible element 1 in this example

2. R is a monoid under multiplication (i.e. we require a **unity** element)

3. Multiplication is distributive w.r.t. addition

Example 4. $\mathbb{Z}/4\mathbb{Z}$
Consider cosets

- $0 + 4\mathbb{Z}$
- $1 + 4\mathbb{Z}$
- $2 + 4\mathbb{Z}$
- $3 + 4\mathbb{Z}$

with additive identity $0 + 4\mathbb{Z}$ and unity $1 + 4\mathbb{Z}$.

Non-Example 5. (Not a ring)
The even integers $2\mathbb{Z}$ is not a ring because it lacks a mutliplicative identity.

Non-Example 6. (Non-commutative Ring)
The set of 2×2 real matrices $M_2(\mathbb{R})$ form a **non-commutative ring**.

Definition 7. Integral Domain
A commutative ring that has no zero divisors; that is, the product of any two nonzero elements is nonzero.

Example 7. The integers $\mathbb{Z}$ under multiplication and addition form an integral domain.

Example 8. Every field is an integral domain, following from existence of an inverse for every element of the field.

Non-Example 9. $\mathbb{Z}/4\mathbb{Z}$: $2 \times 2 \equiv 0$ modulo 4, but $2 \neq 0$, so $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, nor a field.

The fields $\mathbb{Q}_p$ and $\mathbb{R}$ are both what are known as **local fields**, yet they are not isomorphic. It is a major result of **Local Class Field Theory** that every local field is isomorphic to one of the below possibilities:

1. $\mathbb{R}$ (Archimedean, char $= 0$)

2. $\mathbb{C}$ (Archimedean, char $= 0$)

3. $\mathbb{Q}_p$ and its finite extensions (Non-Archimedean, char $= 0$)

4. The field $\mathbb{F}_q(T)$ of **formal Laurent power series** in the variable T over a **finite field** $\mathbb{F}_q$, where q is a power of p. (Non-Archimedean, char $= p$)

.

Proposition 1.3. The fields $\mathbb{Q}_p$ and $\mathbb{R}$ are not isomorphic.

(WTS: It suffices to show $\mathbb{Q}_p$ and $\mathbb{R}$ is not a ring homomorphism, which we will do by counterexample/contradiction with $\mathbb{Q}_5$.)

Proof:

1. **In $\mathbb{R}$, the equation $x^2 = -1$ has no solution**. For any real number x, $x^2 \geq 0$, so $x^2 \neq -1$.

2. **Compare with $\mathbb{Q}_p$, for certain primes p, the equation $x^2 = -1$ DOES have a solution**. For example, in $\mathbb{Q}_5$, there exists an element x such that $x^2 = -1$. This is because the group of units in $\mathbb{Q}_p$ has torsion elements, unlike $\mathbb{R}$.

3. ("Forward Iso") Supposing $\phi : \mathbb{R} \to \mathbb{Q}_p$ is a ring iso, then $\phi(1) = 1$ in order to preserve structure. Then im(-1) would be $\phi(-1) = -1$. If an element $i \in \mathbb{R}$ satisfied $i^2 = -1$, then $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$. If $p = 5$, this is possible in $\mathbb{Q}_5$.

4. ("Backward Iso": **Contradiction**:) $\mathbb{Q}_5$ contains an element u such that $u^2 = -1$. A hypothetical isomorphism ϕ would map u to $\phi(u) \in \mathbb{R}$, which would satisfy $\phi(u)^2 = \phi(u^2) = \phi(-1) = -1$, which is impossible in $\mathbb{R}$.

∎

Next week's talk should introduce **Hensel's Lemma** [Cona], a handy "algebraic lifting tool" which allows us to verify local existence of roots. In conjuction with Hasse's **Local-Global Principle** [Conb], one can study problems over the global field $\mathbb{Q}$ by studying it in $\mathbb{R}$ and all of $\mathbb{Q}_p$. While beyond the intended scope of this seminar, the local-global principle captures much of the essence of **Class Field Theory**, with Milne's CFT [Mil20] as a popular graduate-level reference.

For now, we continue with a review of ring theory so that we may understand the algebraic structure of p-adic fields.

Definition 8. Ideal of a Ring
An ideal $I \subseteq R$ satisfies:

- As an Additive Subgroup
- Closure
- Absorption

Remark. Ideals are often used to construct **quotient rings**, which can show up quite a bit in algebraic NT.

Non-Example 10. Note that $\mathbb{Z}$ is not an ideal of $\mathbb{R}$ nor $\mathbb{Q}$, even though it is a subring of both.

Definition 9. Principal Ideal
We call an ideal I of R *principal* if there is an element a of R such that

$$I = aR = \{ar \mid r \in R\}.$$

In other words, the ideal is **generated by a single element** a of R through multiplication by every element of R.

Example 11. The even integers $2\mathbb{Z}$ of $\mathbb{Z}$ is a principal ideal.

Example 12. More generally, the set of all integers divisible by a fixed integer n, denoted $n\mathbb{Z}$, is a principal ideal in $\mathbb{Z}$.

Example 13. "To divide is to contain" for Dedekind domains, a "prime factorizable" integral domain (see Definition 7). All PIDs (see Definition 10) are Dedekind domains.

Definition 10. Principal Ideal Domain (PID)
A PID is an integral domain (see Definition 7) in which every ideal is principal.

Example 14. $\mathbb{Z}$

Definition 11. Maximal Ideal of a Ring
A maximal ideal of a ring R is a proper ideal I such that there are no ideals "in between" I and R. In other words, if J is an ideal which contains I, then either $J = I$ or $J = R$.

Example 15. In the ring $\mathbb{Z}$ of integers, the maximal ideals are the principal ideals generated by a prime number.

1.2.2 The ring $\mathbb{Z}_p$

Proposition 1.4. [Kat07] The ring $\mathbb{Z}_p$ is an integral domain (see Definition 7).

Proof: Follows from $\mathbb{Z}_p \subset \mathbb{Q}_p$ which is a field and has no zero divisors. ∎

Corrollary. The ring $\mathbb{Z}_p$ has a unique maximal ideal (see Definition 11), namely

$$p\mathbb{Z}_p = \mathbb{Z}_p/\mathbb{Z}_p^\times.$$

Proof: Suppose I is another max ideal. Since $p\mathbb{Z}_p$ is max in $\mathbb{Z}_p$, I must contain element from its complement $a \in \mathbb{Z}_p^\times$. As an ideal, $1 = a \cdot a^{-1} \in I$, but then $I = \mathbb{Z}_p$. ∎

Remark. We call $\mathbb{Z}_p$ a local ring.

Proposition 1.5. [Kat07] The ring $\mathbb{Z}_p$ is a PID (see Definition 10). More precisely, its ideals are the principal ideals (see Definition 9) $\{0\}$ and $p^k\mathbb{Z}_p$ for all $k \in \mathbb{N}$.

Proof: $\boxed{p^k\mathbb{Z}_p \subset I}$
Let I be a nonzero ideal in $\mathbb{Z}_p$ and $0 \neq a \in I$ be an element of max norm. Assume $|a|_p = p^{-k}$ for some $k \in \mathbb{N}$. Then $a = \varepsilon p^k$, where ε is a unit, by

$$|a|_p = |\epsilon p^k|_p = |\epsilon|_p |p^k|_p = 1 \cdot p^{-k} = p^{-k}$$

using $v_p(p^k) = k$. Then $p^k = \varepsilon^{-1} a \subset I$. Hence $p^k\mathbb{Z}_p \subset I$.

$\boxed{I \subset p^k\mathbb{Z}_p}$

Conversely for any $b \in I$, $|b|_p = p^{-w} \leq p^{-k}$ and we can write

$$b = p^w \varepsilon' = p^k p^{w-k} \varepsilon' \in p^k\mathbb{Z}_p.$$

Therefore $I \subset p^k\mathbb{Z}_p$.

∎

Theorem 1.2. For any $x \in \mathbb{Z}_p$, the Teichmuller character [3] $\omega(x) = \lim_{n\to\infty} x^{p^n}$ exists. This limit is denoted by $\omega(x)$ and has properties

1. **Dependence on Residue Class:** $\omega(x)$ depends only on x_0 of x in the p-adic expansion
$$x = x_0 + x_1 p + x_2 p^2 ...$$
2. **Multiplicativity:** $\omega(xy) = \omega(x) \cdot \omega(y)$
3. **Root of Unity:** $\omega(x) = 0$ if $x_0 = 0$, and it is a $(p-1)$th root of 1 if $x_0 \neq 0$

(WTS: The sequence $\{x_0^{p^n}\}$ is Cauchy and converges to the desired limit in $\mathbb{Z}_p$. We use Lemma 1.1 to show that the limit exists for all $x \in \mathbb{Z}_p$ and is defined by x_0 to prove 1) and swiftly proceed to prove 2) and 3).)

Proof:

1. We will use **Euler's Totient Function** $\varphi(n)$ which counts the rel. prime integers up to n and **Euler's Theorem** $x^{\varphi(n)} \equiv 1 \pmod n$ if $\gcd(x, n) = 1$. Applying to our case, $x_0^{\varphi(p^n)} \equiv 1 \pmod{p^n}$.
2. Since p is prime, the totient function $\varphi(p^n) = p^n - p^{n-1}$.
3. Sub
$$x_0^{p^n - p^{n-1}} \equiv 1 \pmod{p^n}$$
$$x_0^{p^n} \equiv x_0^{p^{n-1}} \pmod{p^n},$$
which means that the difference between consecutive terms becomes divisible by increasingly higher powers p, so
$$|x_0^{p^n} - x_0^{p^{n-1}}|_p$$
tends to zero as $n \to \infty$ and $\{x_0^{p^n}\}$ is Cauchy. By **completeness of $\mathbb{Z}_p$, $\{x_0^{p^n}\}$ converges** to $\omega(x_0) = \lim_{n\to\infty} x_0^{p^n}$.

[3] By Remark 3.1.8 of [Ked21], some may prefer the non-eponymous (yet non-standardized) terminology and notation for what is historically known as the Teichmuller character. We thank Gabriel Ong for pointing out the discrepancy to us.

We use Lemma 1.1 to prove existence of a limit for all $x \in \mathbb{Z}_p$, **defined by digit x_0 of x.**

Lemma 1.1. [Kat07] Suppose $x \in \mathbb{Z}_p$ with first digit x_0. Then we have $|x^p - x_0^p|_p \leq p^{-1}|x - x_0|_p$.

Proof: Let $x = x_0 + \alpha$ with $|\alpha|_p \leq p^{-1}$. We **expand $x^p - x_0^p$ using the binomial theorem**:

$$\binom{p}{1}x_0^{p-1}\alpha + \binom{p}{2}x_0^{p-2}\alpha^2 + \binom{p}{p}\alpha^p$$

$$= x - x_0\left(\binom{p}{1}x_0^{p-1} + \binom{p}{2}x_0^{p-2}\alpha + \binom{p}{p}\alpha^{p-1}\right)$$

Since $|\binom{p}{j}x_0^{p-j}\alpha^{j-1}|_p \leq p^{-1}|$ for $j \geq 1$, by **strong tri inequality** we obtain

$$|x^p - x_0^p|_p \leq p^{-1}|x - x_0|_p.$$

∎

Applying 1.1, we obtain

$$|x^{p^n} - x_0^{p^n}|_p \leq p^{-1}|x^{p^{n-1}} - x_0^{p^{n-1}}|_p \leq ... \leq p^{-n}|x - x_0|_p,$$

implying existence of $\lim_{n\to\infty} x^{p^n} = \lim_{n\to\infty} x_0^{p^n}$. **Thus we have proved Property 1).**

- Property 2) follows from the product law for limits.
- Applying property 2 and FLT, obtain

  $$\omega_p^{p-1}(x_0) = \omega(x_0^{p-1}) = \omega(1) = 1.$$

  Thus the values of $\omega(x)$ are solutions to $y^p - y = 0$. Since $\mathbb{Q}_p$ is a field, this equation cannot have more than p solutions in $\mathbb{Q}_p$, nor in $\mathbb{Z}_p$. Consequently, the only solutions are values of ω, verifying Property 3).

∎

While also beyond the intended scope of this seminar, we find it worthwhile to note that the Teichmuller character plays a necessary role in the construction and theory of **Witt vectors** [Rab07]. By their "lifting" ability, the commutative ring (see Definition 6) of Witt vectors $W(\mathbb{F}_p) \cong \mathbb{Z}_p$.

Warning: Avoid char $= p$ at all costs :)

JK, it has it *p*ros and cons [Conc, BHK+19], promise there are lots of successful mathematicians working in characteristic p!

References

[BHK$^+$19] Renee Bell, Julia Hartmann, Valentijn Karemaker, Padmavathi Srinivasan, and Isabel Vogt. Thinking postiive: Arithmetic in characteristic p. *Notices of the American Mathematical Society*, 2019. https://padmask.github.io/thinkingpositive.pdf.

[Cona] Keith Conrad. Hensel's lemma. https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

[Conb] Keith Conrad. The local global principle. https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf.

[Conc] Keith Conrad. Perfect fields. https://kconrad.math.uconn.edu/blurbs/galoistheory/perfect.pdf.

[Kat07] Svetlana Katok. *P-adic Analysis Compared with Real*. AMS, 2007.

[Ked21] Kieran S. Kedlaya. *Notes on Prismatic Cohomology*. Topics in Algebraic Geometry Course Notes, 2021. https://kskedlaya.org/prismatic/prismatic.html.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Rab07] Joseph Rabinoff. The theory of witt vectors. *arxiv*, 2007. https://arxiv.org/abs/1409.7445.