An Introduction to p-adic Numbers, Part 2 of 2

Abstract

In this session, we continue exploring the p-adic numbers. Whereas the previous session introduced the p-adic numbers via algebra and number theory, this session will consider the p-adics from the perspective of the p-adic metric. That is, we shall fix a prime p, then define a distance d_p on $\mathbb{Z}$ (and $\mathbb{Q}$) relative to p. This p-adic distance has a number of interesting—and counterintuitive—properties.

Background needed: We assume familiarity with basic principles from number theory, especially properties of primes and prime factorization of integers. Other results, perhaps unfamiliar, will be presented in this worksheet.

0 Warmup: Unique Factorization

Exercises:

0.1 Let n be a postive integer with $n > 1$. What is the *prime factorization* of n? What do you know about prime factorizations?

0.2 Let (a, b) be some fixed point in the plane $\mathbb{R}^2$. Assume that we measure distance in the plane in the usual way. What is the set of all points in the plane whose distance to (a, b) is less than 1? What does this set look like when you draw it?

Note: A general description will suffice here. This example appears again as Example 4.4(b), too.

0.3 What is a *geometric series*? In particular, what is an *infinite geometric series*? What is the formula for computing such an infinite series, and when does it apply?

1 Review of Session 1

In our first session on this topic, we introduced the m-adic numbers as generalized, possibly infinitely long base-m representations. This will not be the focus of this particular session, but we restate these definitions in the interest of thoroughness.

Definition 1.1. Fix a positive integer m, with $m \geq 2$. Consider the set $D_m := \{0, 1, \ldots, m-1\}$ of all nonnegative integers strictly less than m. Then for any nonnegative integer x, if $a_0, a_1, \ldots, a_k \in D_m$ are such that

$$x = a_k m^k + a_{k_1} m^{k-1} + \cdots + a_2 m^2 + a_1 m + a_0, \tag{1.1}$$

then the above is the *base-m representation* of x.

Notation: We shall denote base-m representations by concatenation and a subscript denoting our base, where

$$x = (a_k a_{k-1} \cdots a_2 a_1 a_0)_m \text{ or } a_k a_{k-1} \cdots a_1 a_0 \ {}_m$$

represents the integer x given in (1.1).

Though m-adic representations are interesting in general, these systems are most useful when m is a positive prime, p.

Definition 1.2. Let p be a fixed, positive prime. The set of *p-adic integers*, denoted $\mathbb{Z}_p$, is the set of infinite strings

$$x := (\ldots x_3 x_2 x_1 x_0)_p, \tag{1.2}$$

where for each j, $x_j \in \{0, 1, 2, \ldots, p-1\}$.

The set

$$\mathbb{Q}_p := \left\{ x p^{-k} : x \in \mathbb{Z}_p, k \in \mathbb{N} \right\}; \tag{1.3}$$

is the set of *p-adic numbers*. that is, $\mathbb{Q}_p$ is the set of all p-adic integers, together with fractions that include denominators divisible by p. We can view $\mathbb{Q}_p$ as the set of elements of the form

$$(\ldots x_3 x_2 x_1 x_0 . x_{-1} x_{-2} \cdots x_{-k} \tag{1.4}$$

for some nonnegative integer k

Example 1.3. We do not, in general, need to use negative signs to obtain additive inverses in $\mathbb{Z}_p$ or $\mathbb{Q}_p$. In $\mathbb{Z}_5$, we have

$$-1 = \ldots 444444_5,$$

since $\ldots 444444_5 + 1 = 0$ in $\mathbb{Z}_5$.

Remark. Recall that in both $\mathbb{Z}_p$ and $\mathbb{Q}_p$, one can add, subtract, and multiply elements, and the results remain in the respective sets. In $\mathbb{Q}_p$, we also have that every element has a *multiplicative inverse*. That is, for all $x \in \mathbb{Q}_p$, there exists some $y \in \mathbb{Q}_p$ such that $xy = 1$.

This is not, in general, true for $\mathbb{Z}_p$. For example, for each positive prime p, p has the multiplicative inverse p^{-1} lying in $\mathbb{Q}_p$, but p^{-1} does not lie in $\mathbb{Z}_p$.

In both $\mathbb{Z}_p$ and $\mathbb{Q}_p$, there are no *zero divisors*. That is, there are no *nonzero* elements $x, y \in \mathbb{Q}_p$ such that $xy = 0$. (This is *not* true in general when p is not a prime. For example, in our last session, we showed there are nonzero $x, y \in \mathbb{Z}_{10}$ such that $xy = 0$.)

2 p-adic Valuations and Metrics on $\mathbb{Z}$ and $\mathbb{Q}$

We have considered the p-adic numbers in the context of algebra and number theory. For example, $\mathbb{Z}_p$ is a generalization of the idea of base-p representations of nonnegative integers, and $\mathbb{Q}_p$ extends $\mathbb{Z}_p$ by allowing quotients of p-adic integers. In this session, we shall explore the *metric space*[1] properties of $\mathbb{Z}$ and $\mathbb{Q}$ relative to new distances defined with respect to primes.

Definition 2.1. Fix a prime p, and let q be a nonzero rational number. If

$$q = p^k \cdot \frac{r}{s},$$

where $k \in \mathbb{Z}$, $r, s \in \mathbb{Z}$, $\gcd(r, s) = 1$, and $p \nmid rs$, then we say the *multiplicity of p in q* (or *order of p in q*), denoted $\operatorname{ord}_p q$, is defined by $\operatorname{ord}_p q := k$.

If $q := 0$, we use the convention $\operatorname{ord}_p 0 := +\infty$.

Remark. Note that in the above definition, we do *not* assume $r, s > 0$. (Compare to Exercise 3.3(b) below.)

Definition 2.2. Fix a prime p, and let q be a rational number such that $\operatorname{ord}_p = k \in \mathbb{Z} \cup \{+\infty\}$. We define the *$p$-adic absolute value of q* (also called the *p-adic norm* or *p-adic valuation of q*), denoted $\left|q\right|_p$, to be

$$\left|q\right|_p := \begin{cases} +\infty, & \text{if } q = 0 \\ \dfrac{1}{p^k}, & \text{otherwise.} \end{cases} \tag{2.1}$$

Definition 2.2 means, roughly, that a rational number q is p-adically "small" if it is divisible by a large power of p. Conversely, q is p-adically "large" if, written in lowest terms, it has a high power of p in the denominator.

Definition 2.3. Fix a prime p, and let $q, q' \in \mathbb{Q}$. We define the *p-adic distance between q and q'*, denoted $d_p(q, q')$, to be

$$d_p(q, q') := \left|q - q'\right|_p, \tag{2.2}$$

where $\left|q - q'\right|_p$ is the p-adic valuation of $q - q'$ as defined in Definition 2.2. The resulting function $d_p \colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$ is called the *p-adic metric on $\mathbb{Q}$*.

[1] Metric spaces are generalizations of the notion of distance. Chapel Hill Math Circle has explored metric spaces before, especially in the problem sets for June 16, 2018 and for September 8, 2018.

Remark. In Definition 2.3, the intuition is that two numbers q and q' are *near* each other in the p-adic metric if their distance is is divisible by a *large* power of p.

For example, in the 3-adic metric, 1 and 82 are much closer to each other than 81 and 82 are. This is because $|1-82| = 81 = 3^4$ is divisible by a higher power of 3 that $|81-82| = 1 = 3^0$ is.

3 Exercises: p-adic Valuations and Metrics

Throughout, unless indicated otherwise, p is a fixed prime.
Exercises:

3.1 Compute the following:

(a) $\operatorname{ord}_3 45$, $\operatorname{ord}_5 45$, and $\operatorname{ord}_7 45$

(b) $|45|_3$, $|45|_5$, and $|45|_7$

(c) $d_p(12/7, 4/5)$ for every prime p.

3.2 Fix a prime p. Prove that for all $a, b \in \mathbb{Q}$,

$$|ab|_p = |a|_p \cdot |b|_p . \tag{3.1}$$

Important: Explain why your proof uses that p is a *prime* integer. (An analogous result breaks down when m is composite.)

3.3 In the following, we prove that $|\cdot|_p$ is a specific example of an *absolute value* on $\mathbb{Q}$:

(a) Prove that for all $a \in \mathbb{Q}$, $|a|_p \geq 0$. Further, $|a|_p = 0$ if and only if $a = 0$.

(b) For all $a \in \mathbb{Q}$, $|-a|_p = |a|_p$.

(c) For all $a, b \in \mathbb{Q}$, $|a+b|_p \leq \max\{|a|_p, |b|_p\}$. In particular, $|a+b|_p \leq |a|_p + |b|_p$.

3.4 In the following, we prove that d_p is not just a *metric* on $\mathbb{Q}$, but it satisfies the stronger conditions of being an *ultrametric* on $\mathbb{Q}$:

(a) Prove that for all $a, b \in \mathbb{Q}$, $d_p(a,b) \geq 0$. Further, $d_p(a,b) = 0$ if and only if $a = b$. This is sometimes expressed as saying that d_p is *positive definite*.

(b) For all $a, b \in \mathbb{Q}$, $d_p(a,b) = d_p(b,a)$. That is, d_p is *symmetric*.

(c) For all $a, b, c \in \mathbb{Q}$, we have

$$d_p(a,c) \leq \max\{d_p(a,b), d_p(b,c)\}. \tag{3.2}$$

the *ultrametric triangle inequality* (or *strong triangle inequality*).
In particular, $d_p(a,c) \leq d_p(a,b) + d_p(b,c)$, meaning d_p satisfies the usual *triangle inequality*, too.

3.5 Recall that in Definition 2.3, we have defined a metric on $\mathbb{Q}$, the set of all rational numbers. From our previous session, though, we have built the p-adic integers, $\mathbb{Z}_p$, and the field of p-adic numbers, $\mathbb{Q}_p$. How would you extend the definition of $\operatorname{ord}_p x$, $|x|_p$, and $d_p(x,y)$ from $\mathbb{Q}$ to $\mathbb{Z}_p$ and $\mathbb{Q}_p$?

4 An Informal Introduction to p-adic Limits

One of the most fundamental concepts in calculus, if not all of mathematics, is that of a *limit*. The rigorous definition of the limit of a sequence is a bit technical for our purposes, so let's consider a more intuitive, less rigorous approach.

Definition 4.1. Let (x_n) be a sequence in a metric space X with metric d. (I.e., X is a set, and $d(x,y)$ denotes the distance between the points $x, y \in X$.) Further, assume $x \in X$.

(a) We say (x_n) *converges to* x or that x *is the limit of* (x_n) if and only if $d(x_n, x)$ gets very small (as a usual real number) as n gets large. Further, we denote this by writing

$$\lim_{n\to\infty} x_n = x \tag{4.1}$$

or

$$x_n \to x. \tag{4.2}$$

(b) We say (x_n) *converges* or *is convergent* if and only if there exists some $x \in X$ such that $x_n \to x$.

That is, a sequence converges if and only if it has a limit.

(c) We say (x_n) *diverges* or *is divergent* if and only if (x_n) does not converge.

Example 4.2. Consider the following examples:

(a) Using the usual distance on $\mathbb{R}$, given by $d(x,y) := |x-y|$, we have

$$\lim_{n\to\infty} \frac{1}{n} = 0.$$

That is, $(1/n)$ converges relative to the usual metric, and its limit is 0.

(b) Using the usual distance on $\mathbb{R}$, the sequence $((-1)^n)$ diverges. This is because the sequence $-1, 1, -1, 1, -1, 1, \ldots$ keeps oscillating between -1 and 1, preventing it from approaching any specific limit.

(c) Let d_2 denote the 2-adic metric, as in Definition 2.3. Then *relative to this metric*,

$$\lim_{n\to\infty} 2^n = 0.$$

Relative to the standard metric on $\mathbb{R}$, though, (2^n) diverges.

(d) Let p be *any* prime. Then relative to the p-adic metric d_p, we have

$$\lim_{n\to\infty} n! = 0,$$

where $n! = n(n-1)(n-2)\cdots 1$ is n factorial. (See Exercise 5.2(b) below for more.)

(e) Fix a positive prime p, and let (x_n) be the sequence defined by

$$x_n := \frac{p^n}{p^n+1}.$$

Then relative to the standard metric on $\mathbb{R}$, we have $x_n \to 1$. However, relative to the p-adic metric d_p on $\mathbb{Q}$, we have $x_n \to 0$.

Moral: Not only does *whether* a sequence converges depend upon the metric, but *its limit* likewise depends upon the metric.

Definition 4.3. Let (X,d) be a metric space, with $a \in X$ and $r > 0$. We define the *open ball centered at a with radius r*, denoted $B(a,r)$ to be the set

$$B(a,r) := \{x \in X : d(x,a) < r\}. \tag{4.3}$$

That is, $B(a,r)$ is the set of all $x \in X$ whose distance from a is less than r.

If our set X has multiple metrics, we shall use the notation $B_d(a,r)$ to emphasize that our open ball is relative to the metric d.

Example 4.4. Consider the following examples:

(a) If $X := \mathbb{R}$, $a \in X$, $r > 0$, and d is the standard metric, then $B(a,r)$ is the open interval $(a-r, a+r)$.

(b) If $X := \mathbb{R}^2$, $(a,b) \in X$, $r > 0$, and d is the standard Euclidean metric in the plane, then $B((a,b),r)$ is the open disc centered at (a,b) of radius r.

(c) If $X := \mathbb{Z}$ and d is the standard metric on $\mathbb{Z}$, then the unit ball $B(0,1)$ is the singleton set $\{0\}$.

(d) Fix a prime p. If $X := \mathbb{Z}$ and d_p is the p-adic metric, then the unit ball $B(0,1)$ is $p\mathbb{Z}$, the set of all integers divisible by p. (Explain, and compare to Example 4.4(c).)

5 Exercises: Properties of the p-adic Metric

Exercises:

5.1 Consider the following images in Figures 5.1 and 5.2. Explain how these images represent the 3-adic metric on $\mathbb{Z}$. Can you explain how to continue?

Hint: Think of each yellow circle in Figure 5.1a in terms of the open 3-adic balls of radius 1 centered at 0, 1, and 2, respectively. What do the green circles in Figure 5.1b then represent?

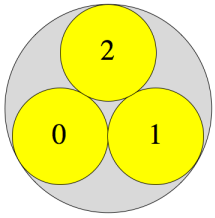
Followup: For those of you who were here for our previous session, What can you say about the images in Figures 5.1 and 5.2 in the context of the base three representation of the integers $0, 1_{10}, 2_{10}, \ldots, 242_{10} = 3^5 - 1$? What about considering these visual representations in terms of congruence modulo 3^k?

5.2 Determine whether the following sequences converge, relative to the indicated metrics. If a sequence converges, explain why, and find its limit. If a sequence diverges, explain why.

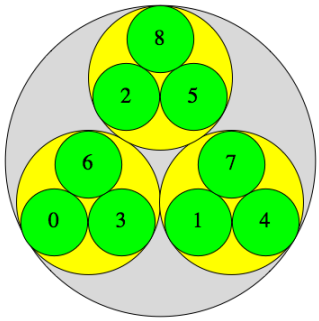
(a) Let (x_n) be the sequence defined by

$$x_n := (p-1) + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^{n-2} + (p-1)p^{n-1}.$$

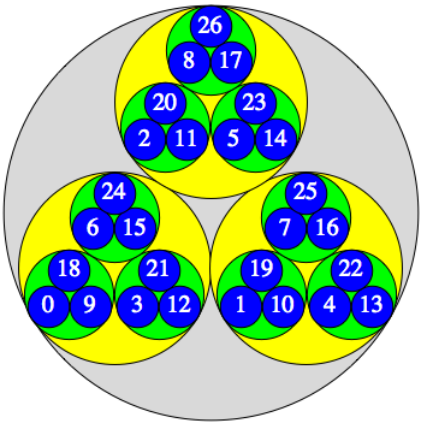
Determine whether (x_n) converges with respect to d_p. If so, what is its limit?



(a) A geometric representation of 0, 1, and 2 in the 3-adic metric. from Heiko Knopse.



(b) A refined geometric representation of 0, 1, …, 8 in the 3-adic metric. from Heiko Knopse.



(c) A further refined geometric representation of 0, 1, …, 26 in the 3-adic metric. from Heiko Knopse.

Figure 5.1: Examples of 3-adic distances taken from "The p-adic integers and their topology", Heiko Knopse, August 3, 2019.

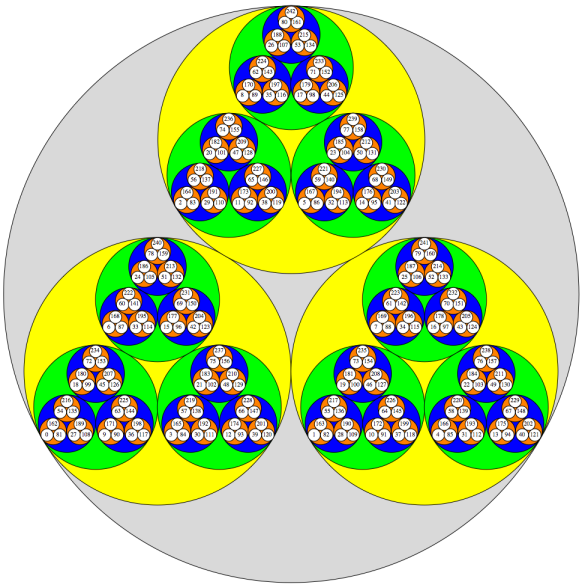


Figure 5.2: A geometric representation of 0, 1, …, 242 in the 3-adic metric taken from "The p-adic integers and their topology", Heiko Knopse, August 3, 2019.

Simplified example: Consider computing the limit of the sequence given by

$$x_n := 1 + 2 + 4 + \cdots + 2^{n-1}$$

relative to the 2-adic metric for a more concrete instance of the above.

(b) $(n!)$ with respect to d_p

(c) Let $a_0, a_1, a_2, \ldots$ each be base-p digits, meaning $a_j \in \{0, 1, 2, \ldots, p-2, p-1\}$ for each j. Consider the sequence (x_n) defined by

$$x_n := a_{n-1}p^{n-1} + a_{n-2}p^{n-2} + \cdots + a_2 p^2 + a_1 p + a_0.$$

Does the sequence (x_n) converge p-adically? Explain.

5.3 Consider the open ball $B(1, 1/3)$ relative to the 3-adic metric d_3. Describe this open ball, and give some example elements of the set.

Note: Recall Exercise 5.1.

5.4 Throughout, fix a prime p.

(a) Let $x, y, z \in \mathbb{Q}$ be rational numbers. Prove that at least two of the distances $d_p(x,y)$, $d_p(y,z)$, and $d_p(x,z)$ are equal. More specifically, prove that the two longest of these three values are equal.

This is typically expressed as saying that in an ultrametric space like $(\mathbb{Q}, d_p)$, "every triangle is isosceles", even though we're not considering typical triangles in a plane.

(b) Let $B(a,r)$ be a nonempty open ball in the metric space $(\mathbb{Q}, d_p)$. If $b \in B(a,r)$, then $B(a,r) = B(b,r)$.

That is, in an ultrametric space, "every point inside an open ball is its center".

5.5 **Challenging:** Let n be a positive integer with $n > 1$. Prove that

$$H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

is never an integer.

Generalization: Prove, more generally, that $H_n \notin \mathbb{Z}_2$, the 2-adic integers. (Recall that some noninteger rational numbers lie in $\mathbb{Z}_p$, so this is indeed a stronger claim than simply not being an ordinary integer.)

5.6 **Very Challenging:** Fix a positive prime p, and let r, s be arbitrary rational numbers. Can you find a sequence (x_n) in $\mathbb{Q}$ such that $x_n \to r$ relative to d_p, but $x_n \to s$ relative to the standard metric?

Further, if q is another positive prime distinct from p, can we have $x_n \to r$ relative to d_p, but $x_n \to s$ relative to d_q?

References

[1] 3Blue1Brown. What does it feel like to invent math? https://www.youtube.com/watch?v=XFDM1ip5HdU, August 13, 2015.

[2] Hans-Dieter Ebbinghaus et al. *Numbers*, volume 123 of *Graduate Texts in Mathematics*. Springer-Verlag New York Inc., New York, English transation of second German edition edition, 1991.

[3] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Walton Street, Oxford OX2 6DP, fifth edition, 1979.

[4] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[5] Jean-Pierre Serre. *Numbers*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag New York Inc., New York, 1973.

[6] Veritasium. Mathematicians use numbers differently from the rest of us. https://www.youtube.com/watch?v=tRaq4aYPzCc, June 6, 2023.