An Introduction to p-adic Numbers, Part 1 of 2

Abstract

In this session, we explore algebraic and number theoretic concepts relevant to the p-adic integers, $\mathbb{Z}_p$, and the field of p-adic numbers, $\mathbb{Q}_p$. Introduction will begin by experimenting with the 10-adic numbers, $\mathbb{Z}_{10}$, and contrasting its properties with those of $\mathbb{Z}_p$, where p is a positive prime.
Background needed: We assume familiarity with basic principles from number theory, especially properties of primes with respect to divisibility. Other results, perhaps unfamiliar, will be presented in this worksheet.

0 Warmup

Exercises:

0.1 Let n be an integer, and $m > 1$ a positive integer. What is the *base-m representation* of n? In particular, which digits can appear in base-m representations?

For example, what is the base-2 representation of 43? What about the base-7 representation of 43?

0.2 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?

0.3 Consider the "number"

$$\ldots 1111111,$$

where there are infinitely many 1's repeating to the left. Assuming this "number" makes sense, what would you say its value is? (It may help to consider

$$\ldots 9999999,$$

first, especially after adding $1 = \ldots 0001$ to this value.)

Note: A binary/base-two result analogous to this exercise appears at the beginning of [1].

1 Introduction: A New Kind of Number

A nonnegative integer can be viewed as a concatenation of *at most finitely many* nonzero digits. What happens if we consider a new type of number, allowing (countably) infinitely many nonzero digits? As we saw in the warmup, these new numbers behave counterintuitively.

Over the next two sessions, we shall explore the properties of different families of such infinite integers. Today's session will take a primarily *algebraic* and number theoretic perspective. In two weeks, we'll consider the *metric space* structure.

Let's begin with some very basic notation:

Notation. The sets below are denoted as follows:

1.1 The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\{1,2,3,...\}$ of all positive integers.

1.2 The set of all *integers*, denoted $\mathbb{Z}$, is the set $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$.

1.3 The set of all *rational numbers*, denoted $\mathbb{Q}$, is the set

$$\mathbb{Q} := \left\{\frac{r}{s} : r,s \in \mathbb{Z}, s \neq 0\right\}$$

consisting of all quotients of integers with nonzero denominator.

1.4 The set of all *real numbers* is denoted $\mathbb{R}$.

1.5 The set of all *complex numbers*, denoted $\mathbb{C}$, is the set

$$\mathbb{C} := \{a + bi : a,b \in \mathbb{R}\},$$

where i is the imaginary unit satisfying $i^2 = -1$.

1.6 The set of all "infinite integers" described in Exercise #0.3 is the set of 10-*adic integers*, denoted $\mathbb{Z}_{10}$.

That is, an element $x \in \mathbb{Z}_{10}$—i.e., a 10-adic integer—can be denoted in the form

$$x := \ldots x_4 x_3 x_2 x_1 x_0,$$

where x_j denotes the jth digit of x. Further, we assume each x_j is one of the digits in $\{0, 1, 2, \ldots, 8, 9\}$.

1.7 More generally, if $m > 1$ is a positive integer, then we can generalize the 10-adic integers from Notation 1.6 above to the m-adic integers. In particular, if p is a positive prime, then we can consider the p-adic integers, Z_p.

Regarding Notation 1.7, for those unfamiliar with base-m representations of integers, see Section 2 below.

Exercises:

1.1 Let $x, y \in \mathbb{Z}_{10}$ be 10-adic integers as denoted above. How would you define $x + y$? For example, how would you compute the sum $\ldots 342901 + \ldots 552301$?

1.2 How would you define multiplication in $\mathbb{Z}_{10}$? For example, how would you compute the product $\ldots 342901 \times \ldots 552301$?

1.3 Let $x := \ldots 9999 \in \mathbb{Z}_{10}$. What is $x + 1$? What can we conclude about -1 in Z_{10}?

1.4 If $x \in \mathbb{Z}_{10}$, how would you compute $-x$?

Note: It may help to note that $-x = (-1-x)+1$, then use results from the warmup question.

1.5 Let $x := \ldots x_4x_3x_2x_1x_0 \in \mathbb{Z}_{10}$ as in Notation 1.6. Can you solve the equation

$$3x = 1 \tag{1.1}$$

in $\mathbb{Z}_{10}$? What about the equation

$$6x = 1 \tag{1.2}$$

in $\mathbb{Z}_{10}$?

Hint: Assuming there is a solution to (1.1), can you first compute the rightmost digit X_0? If so, can you then recursively compute the other digits x_j for $j \geq 1$? Alternatively, consider (1.1), in particular, in light of previous exercises.

1.6 If $n \in \mathbb{N}$, then we can view n as lying in $\mathbb{Z}_{10}$ in the natural way. For which n can you find $1/n = n^{-1}$ in $\mathbb{Z}_{10}$? That is, for which $n \in \mathbb{N}$ can we find a 10-adic integer x such that $nx = 1$ in $\mathbb{Z}_{10}$? For those n for which such a *multiplicative inverse* exists, how can you compute it?

Followup: If $x := \ldots x_4x_3x_2x_1x_0 \in \mathbb{Z}_{10}$, when does x have a 10-adic multiplicative inverse? For such x, how can we compute x^{-1}? For example, does $\ldots 4386$ have a multiplicative inverse in $\mathbb{Z}_{10}$? What about $\ldots 3273$ and $\ldots 7065$?

1.7 Can you solve the equation $x^2 = 1$ in $\mathbb{Z}_{10}$? There are two obvious solutions. Are there any others?

Hint: First, try to determine whether the equation $y^2 = y$ has any solutions in $\mathbb{Z}_{10}$ other than $y = 0$ and $y = 1$. If so, then what can we say about $(2y-1)^2$? For computations here, the numbers get large quickly, so I strongly recommend using a calculator or computer.

Note: One approach to solving $y^2 = y$ in $\mathbb{Z}_{10}$ is given by observations in [4].

1.8 Can you produce *nonzero* 10-adic numbers x and y such that $xy = 0$? The hint of Exercise #1.7 may prove useful.

2 Base-m Representations, Congruence mod m^k, and m-adic Integers

Let's begin with some basic definitions and terminology:

Definition 2.1. Let $a, b \in \mathbb{Z}$. We say *a divides b*, denoted $a \mid b$, if and only if there exists some $n \in \mathbb{Z}$ such that $an = b$. (Equivalently: a is a *divisor* of b, and b is a *multiple* of a.)

Example 2.2. Some examples of divisibility:

(a) $2 \mid 6$ since $2 \cdot 3 = 6$ and $3 \in \mathbb{Z}$.

(b) $3 \nmid 5$, since there is no *integer* n such that $3n = 5$.

(c) For every integer a, $a \mid 0$, since $a \cdot 0 = 0$.

Definition 2.3. Let $a, b, m \in \mathbb{Z}$. Then a is *congruent to b modulo m*, denoted $a \equiv b \pmod{m}$, if and only if $m \mid a - b$.

Example 2.4. Some examples of congruence:

(a) $17 \equiv 3 \pmod 7$, since $7 \mid 17-3$.

(b) $9 \not\equiv 4 \pmod 6$, since $6 \nmid 9-4$.

(c) For all $m \in \mathbb{Z}$, $m-1 \equiv -1 \pmod m$. This is because for all m, $m \mid [(m-1)-(-1)]$.

Remark. Intuitively, $a \equiv b \pmod m$ if and only if a and b have the same remainder upon being divided by m. Congruence modulo m is also an *equivalence relation*. Further, in practice we are typically interested only in the case where $m \geq 2$, even though this definition makes sense for all integers m.

Definition 2.5. Irreducibles and primes in $\mathbb{Z}$:

(a) An element $p \in \mathbb{Z}$ is *irreducible* if and only if whenever $a, b \in \mathbb{Z}$ and $p = ab$, either a is a unit or b is a unit. That is, there is no nontrivial factorization of an irreducible p.

(b) An element $p \in \mathbb{Z}$ is *prime* if and only if $p \neq 0$, and whenever $m, n \in \mathbb{Z}$ and $p \mid mn$, either $p \mid m$ or $p \mid n$.

Remark. One can show that in $\mathbb{Z}$, $p \in \mathbb{Z}$ is irreducible if and only if p is prime. Separately, note that under this definition, p need not be *positive* in order to be prime.

Definition 2.6. Fix a positive integer m, with $m \geq 2$. Consider $D_m := \{0, 1, \ldots, m-1\}$, the set 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

$$x = a_k m^k + a_{k-1} m^{k-1} + \cdots + a_2 m^2 + a_1 m + a_0, \tag{2.1}$$

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

That is, the base-m representation of an integer n expresses using the digits $\{0, 1, 2, \ldots, m-2, m-1\}$, writing n as a sum of powers of m.

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

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

Remark. It is true, but a digression for our purposes, that for every fixed positive integer $m \geq 2$, any nonnegative integer $x \in \mathbb{Z}$ has a unique base-m representation.

Our usual way of denoting integers is base-ten. *If m is not explicitly given, nor unambiguously clear from context, then assume that $m = 10$ as usual.*

You may already be familiar with binary (base-two) and hexadecimal (base-sixteen) representation. Note that if $m > 10$, we need to include new "digits" in D_m. For example, if m is sixteen, then the standard convention is to take $D_m := \{0, 1, 2, \ldots, 8, 9, A, B, C, D, E, F\}$, where $A := 10_{10}$, $B := 11_{10}$, and so on, up to $F := 15_{10}$.

Example 2.7. Some examples of base-m representations:

(a) $1A2_{16} = 1\cdot 16^2 + 10\cdot 16 + 1 = 256_{10} + 160_{10} + 2_{10} = 418_{10}$

(b) $72_{10} = 1\cdot 7^2 + 3\cdot 7 + 2 = 132_7$.

(c) With $A_{12} := 10_{10}$ and $B_{12} := 11_{10}$, we have $A4_{12} = 10\cdot 12 + 2 = 1\cdot 6^2 + 2\cdot 6 + 4 = 124_6$.

Exercises:

2.1 Compute the following:

(a) Compute $23_5 + 12_5$.

(b) Compute $2A_{16}\cdot F3_{16}$.
(Recall from the Remark following Definition 2.6 that in base-sixteen, $A := 10_{10}$ and $B := 11_{10}$.)

(c) Compute $12_7\cdot 21_8$, and express it in base-9.

2.2 Let x be a nonnegative integer with base-m representation $x = (a_k a_{k-1}\cdots a_2 a_1 a_0)_m$. What is the smallest nonnegative integer x_1 such that $x \equiv x_1 \pmod{m}$? What is the smallest nonnegative integer x_2 such that $x \equiv x_2 \pmod{m}$? Generalize this to find the smallest nonnegative integer x_j so that $x \equiv x_j \pmod{m^j}$.

2.3 Fix distinct positive integers $m, n \geq 2$. Given an arbitrary nonnegative integer x, explain a procedure for how to translate between the base-m and base-n representations of x. Ideally, do so without having to use an intermediate representation, such as base-ten.

2.4 Consider the 10-adic integers, $\mathbb{Z}_{10}$. How can we characterize an element $x \in \mathbb{Z}_{10}$ in terms of congruences mod 10^k for each positive integer k?

2.5 We implicitaly defined $\mathbb{Z}_{10}$ back in Section 1. Given a positive integer $m > 1$, how might you define $\mathbb{Z}_m$, the m-adic integers?

2.6 **Very challenging:** Consider *distinct* positive integers $m, n > 1$. In the context of Exercises #2.4 and #2.5, what might it mean to say that $\mathbb{Z}_m$ is "equivalent to" $\mathbb{Z}_n$, even though $m \neq n$ by hypothesis?

3 Properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ when p a Prime

Because primes have valuable number theoretic properties, we are typically most interested in the p-adic integers when p is a prime, as well as the field $\mathbb{Q}_p$, also when p is prime. In this section, we consider some of these useful properties, and we use the 3-adics to find a solution to a particular *Diophantine equation*.

Exercises:

Throughout the exercises in this section, p shall denote a fixed positive prime.

3.1 In Exercise #1.8, we saw that $\mathbb{Z}_{10}$ has *zero divisors*: there exist nonzero elements $x, y \in \mathbb{Z}_{10}$ such that $xy = 0$. Can this happen in $\mathbb{Z}_p$ when p is prime?

3.2 Let $x \in \mathbb{Z}_p$, with $x := (\ldots x_3 x_2 x_1 x_0)_p$. When is x a *unit* in $\mathbb{Z}_p$? That is, when can we find some $y \in \mathbb{Z}_p$ such that $xy = 1$ in $\mathbb{Z}_p$? If they exists, how might you compute multiplicative inverses of p-adic integers?

3.3 Consider the set

$$\mathbb{Q}_p := \left\{ xp^{-k} : x \in \mathbb{Z}_p, k \in \mathbb{N} \right\}; \tag{3.1}$$

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

$$(\ldots x_3 x_2 x_1 x_0 . x_{-1} x_{-2} \cdots x_{-k} \tag{3.2}$$

for some nonnegative integer k. That is, an element of $\mathbb{Q}_p$ is some nonpositive integer power of p times an element of $\mathbb{Z}_p$, itself a (potentially infinite) sequence of digits expressed in base-p.

3.4 Prove that for all $x \in \mathbb{Q}_p$ such that $x \neq 0$, there exists some $y \in \mathbb{Q}_p$ such that $xy = 1$. That is, $\mathbb{Q}_p$ is a *field*: not only can we add and multiply in $\mathbb{Q}_p$ such that these operations are well-behaved, but we can also take multiplicative inverses of nonzero elements.

3.5 Let $x \in \mathbb{Z}_p$. Further, assume (for reasons that may become clear) that $p \neq 2$. When does there exist some $y \in \mathbb{Z}_p$ such that $y^2 = x$? That is, when do we have that x has a p-adic square root in $\mathbb{Z}_p$?

3.6 An important subject in number theory is the study of *Diophantine equations*. These are algebraic equations where we want to find solutions—or prove none exist—that are either integers or rational numbers. The following Diophantine equation and its solution are provided in [4]:

> Find three squares whose areas add to create a bigger square, and the area of the first square is the side length of the second square, and area of the second square is the side length of the third square.

This exercise, taken from *Arithmetica* by Diophantus of Alexandria, asks us to find *rational*[1] numbers x and y such that

$$x^2 + x^4 + x^8 = y^2. \tag{3.3}$$

Clearly $(x, y) = (0, 0)$ is one such rational solution. Use the algebra of $\mathbb{Z}_3$, the 3-adic integers, to try to find another rational solution to (3.3).

Hint: Assume there are rational solutions which arise as 3-adic integers of the forms

$$x := (\ldots x_4 x_3 x_2 x_1 x_0)_3$$
$$y := (\ldots y_4 y_3 y_2 y_1 y_0)_3.$$

[1] We can find *real* solutions immediately: for any real number x, simply set $y := \pm\sqrt{x^2 + x^4 + x^8}$. Ensuring that x and y satisfy (3.3) *and* are simultaneously rational numbers is much more challenging.

First try to find *nonzero* terminal digits x_0, y_0 that satisfy (3.3) after reducing it modulo 3. Using those choices, then determine viable digits x_1, y_1 by reducing (3.3) modulo 3^2, or mod 9. Can you continue this process indefinitely? Finally, use techniques similar to those in Exercises #1.3 and #1.1 to interpret your 3-adic integers $x := (\ldots x_4 x_3 x_2 x_1 x_0)_3$ and $y := (\ldots y_4 y_3 y_2 y_1 y_0)_3$ as rational numbers.

References

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

[2] 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.

[3] 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.

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