p-adic Numbers

UCLA Math Circle Advanced 1B

by Jack Fasching

Week 6: November 3, 2024

Preface

In this packet, we'll look at an introduction to **p-adic numbers**. These are numeral systems which behave very differently from the ones we traditionally use (like $\mathbb{Q}$), despite having some aspects in common.

But first, let's do a quick lesson on a topic which will be important later:

Prerequisite: Bases

Informally, the **base** of a number system is the number of distinct digits used to represent numbers.

For instance, the standard numeral system we use is in base 10, meaning we only use 10 digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. Moreover, the position of a digit affects its value through powers of ten. For example, the number 523 has the value $5(10)^2 + 2(10)^1 + 3(10)^0 = 523$ in base 10. Here, the digit 2 is in the tens place and has a value of $2(10)^1 = 20$. In the number 42, however, the digit 2 is in the ones place and has a value of $2(10)^0 = 2$.
More formally, in the **positional numeral system** we use (where the position of a digit determines its value), the value of the number

$$x = d_m \cdots d_2 d_1 d_0 . d_{-1} d_{-2} \cdots d_{-n}$$

in base b is

$$d_m \cdot b^m + \cdots + d_2 \cdot b^2 + d_1 \cdot b^1 + d_0 \cdot b^0 + d_{-1} \cdot b^{-1} + d_{-2} \cdot b^{-2} \cdots + d_{-n} \cdot b^{-n}$$

In base 6, for example, the number 523 has the value $5(6)^2 + 2(6) + 3 = 195$ (we always write values in base 10). To prevent any confusion, we will denote the base of our numeral system as the subscript of the number. So for our previous example we could say $523_6 = 195_{10}$.

A numeral system that uses base 10 is called a **decimal** numeral system. We will learn the names of other positional numeral systems in the upcoming problems.

Problem 0.1 *Make the following conversions using the subscript notation we learned:*

- (octal system to decimal system) $47_8 =$ ________$_{10}$
- (senary system to decimal system) $102_6 =$ ________$_{10}$
- (decimal system to octal system) $615_{10} =$ ________$_8$
- (decimal system to senary system) $180_{10} =$ ________$_6$
- (ternary system to quaternary system) $1001_3 =$ ________$_4$
- (binary system to quaternary system) $1001_2 =$ ________$_4$

For numeral systems with bases greater than 10, we will use A, B, C, ... for additional digits, where $A = 11_{10}$, $B = 12_{10}$, $C = 13_{10}$, etc. For bases greater than 36, there are a variety if different methods used, but this packet does not cover any of those scenarios. However, for an arbitrary base b, you can define the digits as $d_1, d_2, ..., d_n$.

Problem 0.2 *Make the following conversions (you may use a calculator):*

- (decimal system to duodecimal system) $99_{10} =$ ________$_{12}$
- (decimal system to duodecimal system) $A1_{12} =$ ________$_{10}$
- (decimal system to hexadecimal system) $125_{10} =$ ________$_{16}$
- (hexadecimal system to decimal system) $ACE_{16} =$ ________$_{10}$

To represent non-integer values, we also have digits to the right of the decimal point. In the base-b numeral system, the digit d_{-n} (the nth digit to the right of the decimal point) has a value of $d_{-n} \cdot b^{-n}$.

Problem 0.3 *Make the following conversions:*

- (octal system to decimal system) $0.33_8 =$ __________$_{10}$
- (decimal system to octal system) $0.5625_{10} =$ __________$_8$

To more clearly state the non-integer values of these numbers, we define a **fraction** as a pair of integers (a, b) in base 10 where $b \neq 0$, notated as $\frac{a}{b}$ and having the value of a divided by b. A value is **rational** if it can be expressed as a fraction.

Problem 0.4 *Convert the decimals from Problem 0.3 to fractions.*

However, the values of some fractions cannot be expressed with a finite amount of decimals (for example, $\frac{1}{3}$ in base 10).

Problem 0.5 *Prove that the value $\frac{1}{3}$ cannot be expressed as a number with a finite amount of decimals in base 10.*

For these cases, we will modify our definition of positional numeral systems to allow an infinite number of digits after the decimal point (expressed using an ellipsis). We will use the vinculum notation $\overline{x}$ for repeating decimal values (for example, $\frac{1}{9} = 0.\overline{1} = 0.111...$ in base 10).

Problem 0.6 *Prove that the number $0.\overline{3}$ in base 10 has the value $\frac{1}{3}$. Hint: Let variable $A = 0.\overline{3}$ and use algebra.*

Problem 0.7 *Make the following conversions, then write the value in fractional notation:*

- (septenary system to decimal system) $0.1_7 =$__________$_{10} =$
- (decimal system to nonary system) $0.875_{10} =$__________$_9 =$
- (decimal system to ternary system) $0.\overline{3}_{10} =$__________$_3 =$

Problem 0.8 *Is it always the case that for any positive $b \in \mathbb{N}$ it is possible to write any rational value in base b?*

Problem 0.9 *Do you think any rational value can be written as a unique number in a positional numeral system? Just say yes or no– we'll cover this problem in the next section.*

*** Challenge Problem 0.1** *Can you think of an important numeral system that isn't positional? Hint: It's used in watches, book chapters, and the Super Bowl.*

*** Challenge Problem 0.2** *Using our formal definition of bases, what would a base -2 numeral system be like? Write the numbers in base -2 with values 1 to 10. Can we do this for any integer value? How about for any rational value?*

1 Interesting Properties in Numeral Systems

(For the next sections, we will only work with base 10 unless we explicitly state so.)

So far, we've looked at how values in positional numeral systems work. However, we haven't addressed the implications of allowing infinitely many digits to the right of the decimal point. Looking back at Problem 0.7 for instance, it would make sense to think that every value can be uniquely expressed as a number in this system.

Problem 1.1 *In a decimal numeral system, prove that there cannot be two distinct numbers with finite decimal representations that have the same value. Extend this proof to include any positional numeral system.*

However, this proof can't be applied when we include infinite decimal representations. For instance, let's look at one proposed equality between two different numbers:

$$0.\overline{9} = 0.999... = 1$$

Problem 1.2 *Prove that this equality is true. Hint: Let variable $B = 0.\overline{9}$ and use algebra.*

*** Challenge Problem 1.1** *We can also use calculus to prove this equality is true:*

*Given a sequence $\{x_i\} = x_1, x_2, x_3, ... \in \mathbb{R}$, we say $\{x_i\}$ **converges** to $l \in \mathbb{R}$ if for every $\varepsilon > 0$ there exists some N such that $n > N \Rightarrow |x_n - l| < \varepsilon$. If a sequence doesn't converge, we say it **diverges**.*
*We define the sequence's **nth partial sum** as*

$$S_n = x_1 + x_2 + \cdots + x_n = \sum_{k=1}^{n} x_k$$

and we define the sequence's ***series*** *(if it exists) as*

$$S = x_1 + x_2 + \cdots = \sum_{k=1}^{\infty} x_k$$

S exists only when the sequence $S_1, S_2, S_3, ...$ converges.
Using this definition of the limit of a series, show that $0.9 + 0.09 + 0.009 + ... = 0.999... = 1$.

Problem 1.3 *Why can't we use a proof similar to that of Problem 1.1 to show* $0.999... \neq 1$*?*

We used an algebraic proof in Problem 1.2 to show $0.\overline{9} = 1$, which we also backed using the definition of limits from calculus. However, we must be careful making such proofs involving infinity, as it may be different from our intuition.

Let's look at the concept of infinity from another angle. Previously, we allowed an infinite number of digits to the *right* of the decimal point. But what if we allowed an infinite number of digits to the *left* of the decimal point? For example, take the number

$$...999$$

If we assume that this is a meaningful number and not just "infinity"), how do we find its value? We could do the following:

Problem 1.4 *Let* $C = ...999$. *Use algebra to find the value of* C. *Then fill the blanks in the following paragraphs.*

However, this doesn't make sense in our traditional decimal numeral system. If ...999 = 9 + 90 + 900 + ... has a value, it should be _______, but our result of _____ is a _______ value. Therefore, we cannot make this proof in our traditional numeral system.

Problem 1.5 *Using our traditional numeral system, why is the proof in Problem 1.2 valid, but not the one in Problem 1.4?*

*** Challenge Problem 1.2** *Using our definition of the limit of a sequence from Challenge Problem 1.1, show that* $9 + 90 + 900 + ... = ...999$ *has no value.*

Despite allowing numbers with infinitely many digits to the left of the decimal point, we can clearly see that such numbers don't follow the basic laws of our numeral system (such as arithmetic and distances between numbers). In this case, we have to create a new numeral system.

2 Creating the p-adic Numeral System

For our traditional numeral system, the **distance** between two numbers a and b is $|b - a|$. In a special case, the distance of a from 0 is $|a|$. This involves the **absolute value** function $|x| : \mathbb{Q} \to \mathbb{R}$.

If we try to allow infinitely many digits to the left of the decimal point, like with ...999, the definition of limits from calculus shows us we cannot assign this number a value (see Challenge Problem 1.2). However, this definition relies on our concept of distance (look back at our definition from Challenge Problem 1.1). So to create this new numeral system, we have to redefine distance between numbers. But while our traditional definition of distance is defined similar to addition and subtraction, our new definition is more similar to multiplication and division.

Problem 2.1 *Prove that, for any $0 \neq x \in \mathbb{Q}$, we can write $x = 10^v \frac{a}{b}$ for $a, b, v \in \mathbb{Z}, a \neq 0, b \neq 0, 10 \nmid a, 10 \nmid b$.*

We denote this value v by $v_{10}(x)$.

Then we can define the **10-adic absolute value** function $|x|_{10} : \mathbb{Q} \to \mathbb{R}$ as:

$$|x|_{10} = \begin{cases} \frac{1}{10}^{v_{10}(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

For our new numeral system, the **distance** between two numbers a and b is $|b - a|_{10}$. In a special case, the distance of a from 0 is $|a|_{10}$.

Problem 2.2 *Find the following values:*

- $|1700|_{10} =$_____
- $|40|_{10} =$_____
- $|10^{25}|_{10} =$_____
- $|1|_{10} =$_____
- $|2|_{10} =$_____
- $|5/2|_{10} =$_____
- $|30/13|_{10} =$_____
- $|2^3 \cdot 5^{14} \cdot 11^2|_{10} =$_____

*** Challenge Problem 2.1** *Using our 10-adic absolute value in our definition of limit convergence, show that* $...999999 = -1$.

Now we see that $...999999 = -1$ with our new p-adic definition of distance. But we can also make some other conclusions:

Problem 2.3 *For each of the following values, find the equivalent finite number:*

- $...999998 =$_____
- $...999997 =$_____
- $...999953 =$_____

Problem 2.4 *Prove that every negative integer has a 10-adic equivalent.*

For these problems onward, we will use the vinculum notation for repeating decimal values fo the left of the decimal point (for example, $\overline{123}4 = ...1231234$).

Problem 2.5 *What is the equivalent finite number of* $\overline{6} = ...666$*?*

Problem 2.6 *What is the equivalent finite number of* $\overline{6}7 = ...6667$*?*

Problem 2.7 *What are the equivalent 10-adic numbers of* $-\frac{1}{3}$, $-\frac{3}{7}$, *and* $-\frac{11}{13}$*?*
What about $\frac{2}{3}$, $\frac{4}{7}$, *and* $\frac{2}{13}$*?*

Problem 2.8 *What are the repeated decimal notations of* $\frac{2}{3}$, $\frac{4}{7}$, *and* $\frac{2}{13}$*?*

Problem 2.9 *Do you see anything in common with these representations?*

Problem 2.10 *For any fraction* $0 < \frac{a}{b} < 1$ *that can be expressed as a repeated decimal*

$$0.\overline{d_1 ... d_n}$$

prove that the equivalent 10-adic number of $-\frac{a}{b}$ *is*

$$\overline{d_1 ... d_n}$$

Problem 2.11 *Can any fraction be represented as an infinite string of digits in our 10-adic numeral system?*

Notice that we can still represent fractions using decimal notation.

However, we soon encounter a serious flaw with our 10-adic numeral system. To see why that's the case, we need to look at the powers of 2 and 5:

$2^1 = 2$	$5^1 = 5$
$2^2 = 4$	$5^2 = 25$
$2^3 = 8$	$5^3 = 125$
$2^4 = 16$	$5^4 = 625$
$2^5 = 32$	$5^5 = 3125$
$2^6 = 64$	$5^6 = 15625$
$2^7 = 128$	$5^6 = 78125$

Problem 2.12 *Prove that every power of 5 ends in 25.*

Problem 2.13 *Prove that every power of 5 ends in ether 125 or 625.*

We notice how powers of 5 always end in other smaller powers of 5. The same is true for powers of 2. It turns out we can create two infinite, 10-adic numbers that always end in power of 2 or 5 respectively:

$$M = ...33554432 \qquad N = ...1953125$$

(The proof for this is complicated, so we won't go through it.)

Problem 2.14 *That happens when we try to multiply* M *by* N*?*

This means that it is impossible to divide by M or N, creating a serious flaw in our numeral system, however, we can bypass this by using some number p other than 10 in a new **p-adic numeral system** (replacing 10 with p for our definitions of $v_p(x)$ and $|x|_p$.

*** Challenge Problem 2.2** *For what values of p do we not encounter the same problem we did for 10-adic numbers? What do you think the "p" stands for in "p-adic numbers"?*

3 Extra Challenge Problems

Previously, we talked about the basic concept of the absolute value $|x| : \mathbb{Q} \to \mathbb{R}$. But actually, any mapping $|x| : D \to \mathbb{R}$ for any integral domain D can be called an **absolute value** if it satisfies these four conditions:

- Non-negativity: $|x| \geq 0$ for all $x \in D$
- Positive definiteness: $|x| = 0$ if and only if $x = 0$
- Multiplicativity: $|xy| = |x||y|$
- Triangle inequality: $|x + y| \leq |x| + |y|$

*** Challenge Problem 3.1** *Prove that $|x|_p : \mathbb{Q} \to \mathbb{R}$ is an absolute value (you do not need to show $\mathbb{Q}$ is an integral domain).*

Formally, given a prime number p, a p-adic number can be defined as the series

$$s = \sum_{i=k}^{\infty} a_i p^i = a_k p^k + a_{k+1} p^{k+1} + a_{k+2} p^{k+2} + ...$$

where k is an integer (possibly negative) and each a_i is an integer such that $0 \leq a_i < p$. A **p-adic** integer is a p-adic number such that $k \geq 0$. The set of p-adic integers is $\mathbb{Z}_p$.

*** Challenge Problem 3.2** *Say that a p-adic integer m is **invertible** in $\mathbb{Z}_p$ if there exists a number $n \in \mathbb{Z}_p$ such that $mn = 1$. Determine the criterion for a p-adic integer m to be invertible in $\mathbb{Z}_p$.*

Here's a problem unrelated to the contents of this packet, but nevertheless challenging:

*** Challenge Problem 3.3** *Jane, Jack, and Tom are playing ping pong where the loser of every game swaps out with the person sitting out. Jane played 17 games. Jack played 15 games. Tom played 10 games. Who lost the second game?*