P-adic numbers

Rich Schwartz

October 24, 2014

1 The Arithmetic of Remainders

In class we have talked a fair amount about doing "arithmetic with remainders" and now I'm going to explain what it means in a more formal way. The set $\boldsymbol{Z}/n$ is defined to be $\{0, 1, ..., (n-1)\}$. An element of $\boldsymbol{Z}/n$ is usually writen as $[k]$ to distinguish it from the integer k.

Two elements in $\boldsymbol{Z}/n$ can be added and multiplied like this: First you do the operation, and then you take the remainder upon division by n. For instance, when $n = 7$, we have $5 + 6 = 11 \rightarrow 4$ and $(5)(6) = 30 \rightarrow 2$. So, in $\boldsymbol{Z}/7$, we have $[5] + [6] = [4]$ and $[5][6] = [2]$. (As usual, $[5][6]$ is an abbreviation for $[5] \times [6]$.)

If you forget about multiplication and just use addition, $\boldsymbol{Z}/n$ forms a group. Also, the associative and commutative laws are true for both operations, and the distributive law is true. A set which has two operations that satisfy all these properties is called a *commutative ring*.

Note that the ring $\boldsymbol{Z}/n$ is actually a field when n is prime. That is, you can do division. For instance, in $\boldsymbol{Z}/7$, we have

$$[2][4] = [1], \qquad [3][5] = [1], \qquad [6][6] = [1].$$

So, $[1]/[4]$ is defined by be $[2]$ because $[2][4] = [1]$. Likewise $[1]/[5] = [3]$ and $[1]/[3] = [5]$ and $[1]/[6] = [6]$. Here is a more complicated calculation in $\boldsymbol{Z}/7$:

$$[3]/[4] = [3] \times [1]/[4] = [3] \times [2] = [6].$$

2 The Reduction Maps

Let's consider $\boldsymbol{Z}/6$ and $\boldsymbol{Z}/3$ in detail. There is a map $f : \boldsymbol{Z}/6 \to \boldsymbol{Z}/3$, which considers the remainder of an element of $\boldsymbol{Z}/6$ when you divide by 3. So

$$f([0]) = [0], \qquad f([1]) = [1], \qquad f([2]) = [2],$$

$$f([3]) = [0], \qquad f([4]) = [1], \qquad f([5]) = [2].$$

The map f has two special properties:

- $f([a] + [b]) = f([a]) + f([b])$.
- $f([a][b]) = f([a])f([b])$.

A map with these properties is called a *ring homomorphism*.

Let's try it out for [4] and [5]. We have

$$f([4] + [5]) = f([3]) = [0], \qquad f([4]) + f([5]) = [1] + [2] = [0].$$

$$f([4][5]) = f([2]) = [2], \qquad f([4])f([5]) = [1][2] = [2].$$

So, it works in this one case. The other cases are similar.

What makes this work out is that 3 is a divisor of 6. So, you could say that you are just forgetting some information when you map from $\boldsymbol{Z}/6$ to $\boldsymbol{Z}/3$.

Things don't work out nearly as well when you have two numbers which don't divide each other. For instance, consider the map from $\boldsymbol{Z}/5$ into $\boldsymbol{Z}/3$. In this case $[2][4] = [3]$ and $f[3] = [0]$. On the other hand,

$$f([2])f([4]) = [2][1] = [2].$$

So, $f([2])f([4]) \neq f([2][4])$. Fortunately, we're never going to consider this bad situation in these notes.

3 What is a p-adic Number

The p-adic numbers are defined in terms of a prime number p. For convenience, I'll always take $p = 3$, and (as in class) this case should suffice to explain what you would do in general. The first few powers of 3 are

$$3, \quad 9, \quad 27, \quad 81, \quad 243, \quad 729.$$

We're going to consider the sequence of rings $\boldsymbol{Z}/3$, $\boldsymbol{Z}/9$, $\boldsymbol{Z}/27$, ...

There are maps

- $f : \boldsymbol{Z}/9 \to \boldsymbol{Z}/3$,
- $f : \boldsymbol{Z}/27 \to \boldsymbol{Z}/9$,
- $f : \boldsymbol{Z}/81 \to \boldsymbol{Z}/27$,

and so on. A 3-adic integer is an infinite sequence of the form $[a_1], [a_2], [a_3], ...$ where

- $[a_1] \in \boldsymbol{Z}/3$
- $[z_2] \in \boldsymbol{Z}/9$
- $[z_3] \in \boldsymbol{Z}/27$,

and so on, $\underline{\text{and}}$

- $f([a_2]) = [a_1]$,
- $f([a_3]) = [a_2]$,
- $f([a_4]) = [a_3]$,

and so on. I'll write 3-adic integers like this

$$a_1 \leftarrow a_2 \leftarrow a_3 \leftarrow a_4 \leftarrow ...$$

The set of 3-adic integers is written as $\boldsymbol{Z}_3$.

Here is an example. 17 represents [2] in $\boldsymbol{Z}/3$ and [8] in $\boldsymbol{Z}/9$, and [17] for $\boldsymbol{Z}/27$, $\boldsymbol{Z}/243$, etc. So

$$2 \leftarrow 8 \leftarrow 17 \leftarrow 17 \leftarrow 17 \leftarrow \cdots$$

is the 3-adic integer representing 17. We might abbreviate things and say that $17 \in \boldsymbol{Z}_3$.

4 Addition

3-adic numbers can be added. Here is the rule

$$\Big(a_1 \leftarrow a_2 \leftarrow a_3 \leftarrow a_4 \leftarrow ...\Big) + \Big(b_1 \leftarrow b_2 \leftarrow b_3 \leftarrow b_4 \leftarrow ...\Big) =$$
$$[a_1 + b_1] \leftarrow [a_2 + b_2] \leftarrow [a_3 + b_3] \leftarrow [a_4 + b_4] \leftarrow ....$$

Let's work out some examples. The number

$$0 \leftarrow 0 \leftarrow 0 \leftarrow \cdots$$

behaves just like the ordinary 0. If α is any 3-adic integer, then pretty clearly $0 + \alpha = \alpha + 0 = \alpha$.

Now consider the number

$$\alpha = \Big(2 \leftarrow 8 \leftarrow 26 \leftarrow 80 \leftarrow 242 \leftarrow \cdots\Big)$$

The nth term of α is $3^n - 1$. You can check that α really is a 3-adic integer. Let

$$\beta = \Big(1 \leftarrow 1 \leftarrow 1 \leftarrow \cdots\Big)$$

It is pretty clear that $\alpha + \beta = 0$. We really should write $\alpha = -1$. That is

$$-1 = \Big(2 \leftarrow 8 \leftarrow 26 \leftarrow 80 \leftarrow 242 \leftarrow \cdots\Big)$$

The addition law is both commutative and associative. Does $\boldsymbol{Z}_3$ form a group? We have already have an identity element, namely 0. We also have -1. More generally, if

$$\alpha = \Big(a_1 \leftarrow a_2 \leftarrow a_3 \leftarrow a_4 \leftarrow ...\Big),$$

then

$$-\alpha = \Big([3 - a_1] \leftarrow [9 - a_2] \leftarrow [27 - a_3] \leftarrow [243 - a_4] \cdots\Big).$$

So, yes $\boldsymbol{Z}_3$ forms a group.

At the end of the last section, we saw that $17 \in \boldsymbol{Z}_3$, and the construction there works for any integer. So, in fact $\boldsymbol{N} \subset \boldsymbol{Z}_3$. But then the construction in this section shows that in fact $\boldsymbol{Z} \in \boldsymbol{Z}_3$. So, the 3-adic integers are a group, and they contain the integers as a subgroup.

5 Multiplication

3-adic integers can be multiplied. Here is the rule.

$$\Big(a_1 \leftarrow a_2 \leftarrow a_3 \leftarrow a_4 \leftarrow ...\Big) \times \Big(b_1 \leftarrow b_2 \leftarrow b_3 \leftarrow b_4 \leftarrow ...\Big) =$$

$$[a_1 b_1] \leftarrow [a_2 b_2] \leftarrow [a_3 b_3] \leftarrow [a_4 b_4] \leftarrow ....$$

The multiplication law is commutative and associative, and also the distributive law holds. So, $\boldsymbol{Z}_3$ is a commutative ring.

Let's work out an example. Starting the integer 2, we note that

- $[2][2] = [1]$ in $\boldsymbol{Z}/3$.
- $[2][5] = [1]$ in $\boldsymbol{Z}/9$.
- $[2][14] = [1]$ in $\boldsymbol{Z}/27$.
- $[2][42] = [1]$ in $\boldsymbol{Z}/81$.

and so on. In general, the nth term is $(3^n + 1)/2$. So, if

$$\alpha = 2 \leftarrow 5 \leftarrow 14 \leftarrow 42 \leftarrow \cdots$$

Then $2\alpha = 1$. So, we should write

$$\frac{1}{2} = \Big(2 \leftarrow 5 \leftarrow 14 \leftarrow 42 \leftarrow \cdots\Big)$$

If we want to figure out 1/4, we should compute $(1/2) \times (1/2)$. This gives

$$\frac{1}{4} = \Big(1 \leftarrow 7 \leftarrow 7 \leftarrow 63 \leftarrow \cdots\Big).$$

Where did this come from? Well, for instance

$$42 \times 42 = 1764$$

and 1764 represents [63] mod 243. It is harder to give a formula for the nth term of 1/4, but since the multiplication rule is commutative and associative, we know that

$$(1/4) \times 4 = (1/2) \times (1/2) \times 2 \times 2 = (1/2) \times 2 \times (1/2) \times 2 = 1 \times 1 = 1$$

It might seem that the last calculation is completely obvious, but there is a subtle point. The thing we are calling $1/4$ is the infinite chain above, and we want to prove that it really deserves to be called $1/4$. So, we need to check that *within the* 3*-adic integers* this number really behaves like $1/4$. So, we want to multiply our number by 4 and check that we get 1. Rather than do out the calculation, which would be quite hard without an explicit formula, we are saved by the associative law, which lets us *deduce* that the calculation would work out correctly.

So far we have seen that $\boldsymbol{Z} \subset \boldsymbol{Z}_3$ and also $1/2 \in \boldsymbol{Z}_3$ and $1/4 \in \boldsymbol{Z}_4$. By taking powers of $1/2$, we see more generally that $1/8, 1/16, 1/32, ...$ all belong to $\boldsymbol{Z}_3$. What about $1/3$? Is there a number in $\boldsymbol{Z}_3$ which behaves like $1/3$? The answer is no. Suppose we had

$$1/3 = \Big(a_1 \leftarrow a_2 \leftarrow \cdots\Big).$$

We know that

$$3 = \Big(0 \rightarrow 3 \rightarrow 3 \rightarrow 3 \cdots.\Big).$$

But then we must have $[a_1][0] = [1]$, and this is impossible. So, we can say that $1/3 \not\in \boldsymbol{Z}_3$.

Here is a more general result along these lines.

Lemma 5.1 *If q is divisible by* 3 *then $p/q \not\in \boldsymbol{Z}_3$.*

Proof: Suppose for the sake of contradiction that $p/q \in \boldsymbol{Z}_3$ and q is divisible by 3. We can write

$$p/q = \Big(a_1 \leftarrow a_2 \leftarrow \cdots\Big), \qquad p = \Big(p_1 \leftarrow p_2 \leftarrow \cdots\Big), \qquad q = \Big(q_1 \leftarrow q_2 \leftarrow \cdots\Big).$$

Since q is divisible by 3, we have $q_1 = 0$. Since p/q is in lowest terms, we know that p is not divisible by 3. This means that either $p_1 = 1$ or $p_2 = 2$. But $(p/q) \times (q) = p$. This means that $[a_1][0] = [1]$ or $[a_1][0] = [2]$. Either case is impossible. ♠

The other half of this result is also true:

Theorem 5.2 *If q is not divisible by* 3 *then $p/q \in \boldsymbol{Z}_3$.*

The two results together tell you exactly when $p/q \in \boldsymbol{Z}_3$. These notes contain a proof of Theorem 5.2, as part of a larger result called Hensel's Lemma.

6 Uncountability

You can put the members of $\boldsymbol{Z}_3$ in one-to-one correspondence with the trinary sequences. For instance, the trinary sequence $0, 1, 2, 1, ...$ corresponds to the 3-adic integer

$$0 \leftarrow 0 + 1(3) \leftarrow 0 + 1(3) + 2(9) \leftarrow 0 + 1(3) + 2(9) + 1(27) \leftarrow \cdots$$

Since the set of trinary sequences is uncountable, so is $\boldsymbol{Z}_3$.

Since the integers and the rational numbers are countable sets, $\boldsymbol{Z}_3$ has many elements which are neither integers nor rationals. What are these other numbers like? For the most part, we don't really know. (Same as with the reals.) However, there are some things we can say. The remaining sections of these notes, which are a bit tougher than the sections above, discuss roots of polynomials in $\boldsymbol{Z}_3$.

7 Hensel's Lemma

Consider the number

$$\alpha = \Big(1 \leftarrow 4 \leftarrow 13 \leftarrow 13 \leftarrow 175 \leftarrow \cdots\Big).$$

We compute that

$$\alpha^2 = \Big(1 \leftarrow 7 \leftarrow 7 \leftarrow 7 \leftarrow 7 \leftarrow \cdots\Big)$$

It appears that $\sqrt{7} \in \boldsymbol{Z}_3$. You might be skeptical that the pattern continues, or that there even is a pattern. It turns out that this really does work. Here is one of the great theorems about 3-adic numbers:

Theorem 7.1 *Suppose that $P(x)$ is a polynomial. Let $P'(x)$ denote the derivative of P. Suppose, for one of the three numbers $k = 0, 1, 2$, that $[P(k)] = 0$ in $\boldsymbol{Z}/3$ and $[P'(k)] \neq 0$ in $\boldsymbol{Z}/3$. Then P has a root in $\boldsymbol{Z}_3$.*

This result is often called *Hensel's Lemma.* I'll give a proof of Hensel's Lemma at the end of these notes. As you might guess, there is a version of Hensel's lemma which works for any prime, and not just 3. The formulation is almost exactly the same.

Here are three applications of Hensel's Lemma.

Application 1: Let's use Hensel's lemma so show that $\sqrt{7} \in \boldsymbol{Z}_3$. Consider the polynomial $P(x) = x^2 - 7$. We have $P'(x) = 2x$. So, $P(1) = [-6] = [0]$ in $\boldsymbol{Z}/3$ and also $P'(1) = [2]$ in $\boldsymbol{Z}/3$. So, P does satisfy the hypotheses of Hensel's Lemma. Hensel's Lemma now tells us that P has a root in $\boldsymbol{Z}_3$. This root is what we are calling $\sqrt{7}$.

Application 2: Here is a fancier example. Consider the polynomial

$$P(x) = x^{99} - 7.$$

Taking the derivative, we get $P'(x) = 99x^{98}$. We have $[P(1)] = [0]$ in $\boldsymbol{Z}/3$ and $[P'(1)] = [99] = [1]$ in $\boldsymbol{Z}/3$. So there is a 99th root of 7 in $\boldsymbol{Z}_3$.

Application 3: Let's use Hensel's Lemma to prove Theorem 5.2. So, suppose that q is not divisible by 3. We want to show that $p/q \in \boldsymbol{Z}_3$. Since we already know that $p \in \boldsymbol{Z}_3$, we just have to show that $1/q \in \boldsymbol{Z}_3$. That is, we have to show that the polynomial $P(x) = qx - 1$ has a root in $\boldsymbol{Z}_3$.

Since q is not divisible by 3 and $\boldsymbol{Z}/3$ is a field, the expression $[1]/[q]$ is defined in $\boldsymbol{Z}/3$. There is some $k \in \{0, 1, 2\}$ so that $[k][q] = [1]$ in $\boldsymbol{Z}/3$. But then $P(k) = 0$ in $\boldsymbol{Z}/3$. Also, $P'(x) = q$, so $[P'(k)] = [q] \neq [0]$ in $\boldsymbol{Z}/3$. By Hensel's Lemma, $P(x)$ has a root in $\boldsymbol{Z}_3$. That's what we wanted to prove.

8 Taylor Series

To prove Hensel's Lemma, we need one fact from Taylor series. Suppose that $P(x)$ is a polynomial and a is some number. Then there is always a polynomial $S(x)$ so that

$$P(x) = P(a) + P'(a)(x - a) + (x - a)^2 S(x). \tag{1}$$

To prove this, let

$$Q(x) = P(x) - P(a) - P'(a)(x - a).$$

We have $Q(a) = 0$ and $Q'(a) = 0$. Since a is a root of Q, we can write $Q(x) = (x - a)R(x)$. But $Q'(a) = R(a)$. So $R(a) = 0$. Since a is a root of R, we have $R(x) = (x - a)S(x)$. All in all, $Q(x) = (x - a)^2 S(x)$. This is what we wanted to prove.

9 Proof of Hensel's Lemma

Let's say that we're trying to solve the equation $P(x) = 0$ in $\boldsymbol{Z}/k$. We would write

$$P(x) = 0 \qquad \text{mod } k.$$

This is what the mod k indicates.

Let's remember the setup for Hensel's Lemma. We have a polynomial $P(x)$ and we know that

$$P(k) = 0 \qquad \text{mod } 3.$$

$$P'(k) = 0 \qquad \text{mod } 3.$$

We set $a_1 = k$. We want to show that P has a root in $\boldsymbol{Z}_3$. Let's call our root α and start it out with a_1:

$$\alpha = \Big(a_1 \leftarrow \cdots\Big).$$

The basic idea is to find α term by term, building on what we have so far in order to get the next term.

We're interested in find a sequence $a_1, a_2, a_3, ...$ so that

$$P(a_n) = 0 \qquad \text{mod } 3^n,$$

where $n = 1, 2, 3, ...$, and also $f(a_{n+1}) = a_n$ for $n = 1, 2, 3, ...$ The fact that $P(a_1) = 0$ mod 3 is already given to us, and we want to find the rest of the sequence. The condition that α is a 3-adic sequence says that

$$a_{n+1} = a_n + 3^n \ell \tag{2}$$

for some $l = 0, 1, 2$ whose value probably depends on n. The idea is to find ℓ in each case.

The main idea is that you combine Equations 1 and 2 and just do out the algebra and see that it works. I'll do it in the next section. There is one last thing I want to say before doing out the algebra. Equation 1 works for the integers, so it works "mod anything". That is, when a is an integer, we have

$$P(x) = P(a) + P'(a)(x - a) + (x - a)^2 S(x) \qquad \text{mod } N, \tag{3}$$

for any N we like.

10 The Main Step in the Proof

Let's find the $(n+1)$st term given the first n terms. Equation 3 (using the values $a = a_n$ and $N = 3^{n+1}$) tells us that

$$P(x) = P(a_n) + (x - a_n)P'(a_n) + (x - a_n)^2 S(a_n), \qquad \bmod 3^{n+1}.$$

Now let's plug in $x = a_{n+1}$ and use Equation 2.

$$P(a_{n+1}) = P(a_n) + (3^n \ell)P'(a_n) + (3^{2n}\ell^2)S(a_2) \qquad \bmod 3^{n+1}.$$

Note that $3^{2n}\ell^2 = 0$ in $\boldsymbol{Z}/3^{n+1}$ because $2n \geq n+1$. This gives us

$$P(a_{n+1}) = P(a_n) + (3^n \ell)P'(a_n) \qquad \bmod 3^{n+1}.$$

Since a_n is a root of P in $\boldsymbol{Z}/3^n$, we have $P(a_n) = 3^n b_2$ in $\boldsymbol{Z}/3^{n+1}$. This gives us

$$P(a_{n+1}) = 3^n b_n + (3^n \ell)P'(a_n) \qquad \bmod 3^{n+1}.$$

Dividing by 3^n, we see that $P(a_{n+1}) = 0$ in $\boldsymbol{Z}/3^{n+1}$ provided that

$$b_n + \ell P'(a_n) = 0 \qquad \bmod 3.$$

Since $a_n = a_{n-1} = ... = a_1$ in $\boldsymbol{Z}/3$, we have $P'(a_1) = P'(a_n)$ in $\boldsymbol{Z}/3$. Hence $P'(a_n) \neq 0$ in $\boldsymbol{Z}/3$. This means that we can solve this equation:

$$\ell = \frac{b_n}{P'(a_n)} \qquad \bmod 3.$$

Plugging in this value of ℓ gives us a_{n+1} so that $P(a_{n+1}) = 0$ in $\boldsymbol{Z}/3^{n+1}$.