p-ADIC INTEGERS

SREEHARI SURESH BABU

The purpose of this note is to give an informal introduction to p-adic integers. Our treatment is inspired by the beginner-friendly book [1], but we will not dwell upon the topological properties here. We will try to understand the algebraic structure of p-adic integers.

Definition 1. Let p be a prime. The ring of p-**adic integers** $\mathbf{Z}_p$ is the set of all infinite sequences

$$x = (x_1 \bmod p, x_2 \bmod p^2, x_3 \bmod p^3, \ldots) \in \prod_{n \geqslant 1} \mathbf{Z}/(p^n)$$

such that

$$x_{n+1} \equiv x_n \bmod p^n$$

for all $n \geqslant 1$. Addition and multiplication are defined componentwise.

In fancy words, $\mathbf{Z}_p$ is the *inverse limit* of the following diagram

$$\cdots \longrightarrow \mathbf{Z}/(p^n) \xrightarrow{\phi_n} \mathbf{Z}/(p^{n-1}) \longrightarrow \cdots \longrightarrow \mathbf{Z}/(p^2) \xrightarrow{\phi_2} \mathbf{Z}/(p),$$

where $\phi_n : \mathbf{Z}/(p^n) \to \mathbf{Z}/(p^{n-1})$ is the canonical map given by $x \bmod p^n \mapsto x \bmod p^{n-1}$. (We will not use the "categorical language" anywhere in this note and the reader who has not seen this notion before may completely ignore it.)

It is clear from the definition that the additive identity is

$$0 = (0 \bmod p, 0 \bmod p^2, 0 \bmod p^3, \ldots)$$

and the multiplicative identity is

$$1 = (1 \bmod p, 1 \bmod p^2, 1 \bmod p^3, \ldots).$$

We will try to understand the basic properties of $\mathbf{Z}_p$ by working with a concrete example. To that end, let $p = 7$. Consider

$$x = (1 \bmod 7, 22 \bmod 7^2, 71 \bmod 7^3, \ldots) \in \mathbf{Z}_7.$$

Notice that the coordinates satisfy the congruence condition. In fact, $22 = 1 + 3p$ and $71 = 22 + p^2 = 1 + 3p + p^2$. Note that this representation of 71 contains information about previous entries. Continuing this way, we can associate to any $z = (z_1 \bmod p, z_2 \bmod p^2, \ldots) \in \mathbf{Z}_7$ a unique infinite formal sum

$$\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 + \cdots,$$

with $0 \leqslant \alpha_i \leqslant 6$ for all i. (The reason we write p instead of 7 is to draw an analogy between the powers of p and the powers of X in a formal power series.) We will call this the p-**adic expansion** of z. For example, the p-adic expansion of x above is

$$1 + 3p + p^2 + \cdots.$$

Notice that the partial sum $S_n = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_{n-1} p^{n-1}$ gives z_n modulo p^n. We may also represent the p-adic expansion as a string of digits in base p that extends indefinitely to left: $\cdots 131$.

Now consider another element

$$y = (5 \bmod 7, 47 \bmod 7^2, 145 \bmod 7^3, \ldots) \in \mathbf{Z}_7.$$

Its p-adic expansion is

$$5 + 6p + 2p^2 + \cdots .$$

If we add x and y, we get

$$\begin{aligned} x + y &= (6 \bmod 7, 69 \bmod 7^2, 216 \bmod 7^3, \ldots) \\ &= (6 \bmod 7, 20 \bmod 7^2, 216 \bmod 7^3, \ldots). \end{aligned}$$

The p-adic expansion of $(6 \bmod 7, 20 \bmod 7^2, 216 \bmod 7^3, \ldots)$ is

$$6 + 2p + 4p^2 + \cdots .$$

Let us now *add* the p-adic expansions of x and y. It is more-or-less like the addition of polynomials or formal power series in X. However, a little more care is needed as the following example illustrates:

$$(1 + 3p + p^2 + \cdots) + (5 + 6p + 2p^2 + \cdots) = 6 + 9p + 3p^2 + \cdots .$$

It doesn't quite look like the p-adic expansion of $x + y$. Where did we go wrong? Well, the catch is that we only allow our α_i to vary between 0 to 6, so 9 in the second sum is an anomaly. To correct it, write $9p = (2+p)p = 2p+p^2$ and add the newly obtained p^2 to $3p^2$ to get $4p^2$. (The reader may recognise this is as the p-adic version of carrying). This should give an idea about how to add p-adic expansions. The reader might find it illuminating to verify that $6 + 6p + 6p^2 + 6p^3 + \cdots$ is the additive inverse of $1 = 1 + 0p + 0p^2 + \cdots$.

Let us now figure out the multiplication of formal sums. First we multiply x and y termwise:

$$\begin{aligned} xy &= (1 \bmod 7, 22 \bmod 7^2, 71 \bmod 7^3, \ldots)(5 \bmod 7, 47 \bmod 7^2, 145 \bmod 7^3, \ldots) \\ &= (5 \bmod 7, 22 \cdot 47 \bmod 7^2, 71 \cdot 145 \bmod 7^3, \ldots) \\ &= (5 \bmod 7, 5 \bmod 7^2, 5 \bmod 7^3, \ldots). \end{aligned}$$

So the p-adic expansion of xy is $5 + 0p + 0p^2 + \cdots$. Do we get the same sum if we *multiply* the p-adic expansions of x and y? Again, multiplication of formal sums is similar to that of polynomials, but we need to add carrys whenever necessary. We demonstrate multiplication below. For simplicity, we discard the cubic and higher degree terms whenever

they appear in the calculation.

$$\begin{aligned}
&(1+3p+p^2+\cdots)\cdot(5+6p+2p^2+\cdots)\\
&=5+6p+2p^2+15p+18p^2+5p^2+\cdots\\
&=5+6p+2p^2+(1+2p)p+(4+2p)p^2+5p^2+\cdots\\
&=5+6p+2p^2+p+2p^2+4p^2+5p^2+\cdots\\
&=5+(p+6p)+(2p^2+2p^2+4p^2+5p^2)+\cdots\\
&=5+0p+p^2+13p^2+\cdots\\
&=5+0p+0p^2+\cdots.
\end{aligned}$$

A careful reader will note that we have not used the primality of 7 anywhere in the above discussions. Of course, everything we have done until now can be done with any other natural number. The importance of being a prime comes from the fact that for a prime p, $\mathbf{Z}_p$ is an *integral domain*, that is, any two nonzero elements have a nonzero product. As a non-example, here are the beginning terms of two elements in the ring of 10-adic integers that give zero as their product:

$$\begin{aligned}
&(5 \bmod 10, 25 \bmod 10^2, 125 \bmod 10^3, \ldots)(2 \bmod 10, 12 \bmod 10^2, 112 \bmod 10^3, \ldots)\\
&=(10 \bmod 10, 300 \bmod 10^2, 14000 \bmod 10^3, \ldots)\\
&=(0 \bmod 10, 0 \bmod 10^2, 0 \bmod 10^3, \ldots).
\end{aligned}$$

Of course, some readers may not find this "example" satisfying. There is another nice way to construct zerodivisors in $\mathbf{Z}_{10}$; find a non-trivial idempotent element. See Richard Borcherds's lecture to find out more: https://youtu.be/VTtBDSWR1Ac.

Now we prove that $\mathbf{Z}_p$ is an integral domain for a prime p. Let x, y be two nonzero elements in $\mathbf{Z}_p$. Suppose their p-adic expansions are given by

$$x = \alpha_n p^n + \alpha_{n+1} p^{n+2} + \alpha_{n+3} p^{n+3} + \cdots$$

and

$$y = \beta_m p^m + \beta_{m+1} p^{m+2} + \beta_{m+3} p^{m+3} + \cdots$$

with $0 < \alpha_n, \beta_m \leqslant p-1$. The first nonzero coefficient of xy is the coefficient of p^{n+m} and it is $\alpha_n\beta_m$ modulo p. Since p doesn't divide α_n or β_m, it doesn't divide $\alpha_n\beta_m$ as well. Thus the product has a nonzero coefficient and hence is not zero.

Notice that we can map any $x \in \mathbf{Z}$ to $(x \bmod p, x \bmod p^2, \ldots) \in \mathbf{Z}_p$. This is an injective map since the only element in $\mathbf{Z}$ that is divisible by all positive powers of p is 0. Through this map, we can think of $\mathbf{Z}$ as a subring of $\mathbf{Z}_p$.

Suppose x is a positive integer and consider its image is $\mathbf{Z}_p$. Its p-adic expansion is a finite series; in fact, it is the base p representation of x. For negative integers, it is not finite. For example, the image of -1 in $\mathbf{Z}_7$ is

$$(-1 \bmod 7, -1 \bmod 7^2, -1 \bmod 7^3, \ldots) = (6 \bmod 7, 48 \bmod 7^2, 342 \bmod 7^3, \ldots).$$

and hence its p-adic expansion is $6 + 6p + 6p^2 + 6p^3 + \cdots$. In fact, this is the worst that can happen. That is, given $x \in \mathbf{Z}$, the p-adic expansion of x is either a finite series or an infinite series with *almost all* coefficients $p-1$.

Let us now describe the invertible elements of $\mathbf{Z}_p$. For a real number x such that $|x| < 1$, we have the geometric series:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots .$$

Notice that the RHS makes sense in $\mathbf{Z}_p$ if we replace x by p. This suggests that the integer $1 - p$ *may be* invertible in $\mathbf{Z}_p$ with inverse

$$1 + p + p^2 + p^3 + \cdots .$$

We might even speculate that $1 - pz$ ($z \in \mathbf{Z}_p$) is invertible with inverse

$$1 + pz + (pz)^2 + (pz)^3 + \cdots .$$

The above expression, as written, is not a p-adic expansion, but maybe we can expand it into a p-adic expansion? Finally, we see that p is not invertible, since

$$p \cdot (\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 + \cdots) = \alpha_0 p + \alpha_1 p^2 + \alpha_2 p^3 + \cdots \neq 1 + 0p + 0p^2 + \cdots .$$

Hence we conjecture that an element z in $\mathbf{Z}_p$ is invertible if and only if it is not divisible by p. Let us prove this formally. Our proof is based on [2, p. 12].

Suppose x is a multiple of p, say $x = pz$. Then

$$\begin{aligned} x &= (p \bmod p, p \bmod p^2, \ldots)(z_1 \bmod p, z_2 \bmod p^2, \ldots) \\ &= (0 \bmod p, pz_2 \bmod p^2, \ldots), \end{aligned}$$

and there is no way we can make the first coordinate 1 by multiplying by some other element in $\mathbf{Z}_p$. (Essentially, this is the same proof as above.)

Now suppose $x = (x_1 \bmod p, x_2 \bmod p^2, \ldots)$ is not a multiple of p. If each x_n is invertible in $\mathbf{Z}/(p^n)$, then $(x_1^{-1} \bmod p, x_2^{-1} \bmod p^2, \ldots)$ is a possible candidate for the inverse of x in $\mathbf{Z}_p$. We need to verify that the entries satisfy

$$x_{n+1}^{-1} \equiv x_n^{-1} \bmod p^n,$$

but that is straightforward. Thus it suffices to prove that if x_n is not a multiple of p in $\mathbf{Z}/(p^n)$, then it is invertible. By hypothesis, $x_n \bmod p$ is a nonzero element of $\mathbf{Z}/(p)$ and hence is invertible in $\mathbf{Z}/(p)$, i.e., there exist integers y, z such that $x_n y = 1 - pz$. So $x_n y \equiv 1 - pz \bmod p^n$ and $1 - pz$ is invertible modulo p^n since

$$(1 - pz)(1 + pz + \cdots + p^{n-1} z^{n-1}) = 1 - p^n z^n \equiv 1 \bmod p^n.$$

Thus $y(1 + pz + \cdots + p^{n-1} z^{n-1})$ is the inverse of x_n in $\mathbf{Z}/(p^n)$.

Notice that the above proposition implies that $\mathbf{Z}_p$ is a *local ring* with $p\mathbf{Z}_p$ as its maximal ideal. In fact, with little work, now one can show that $\mathbf{Z}_p$ is a DVR (a PID with a unique nonzero prime ideal). For details, we refer the reader to [2].

The field of fractions of $\mathbf{Z}_p$ is denoted by $\mathbf{Q}_p$. Topologically, $\mathbf{Q}_p$ is a complete metric space and can be realised as the completion of $\mathbf{Q}$ with respect to a certain metric. Thus they are as important as the real numbers. Moreover, $\mathbf{Z}_p$ is analogous to $[0, 1]$, at least in a topological sense. This kind of analogies leads to a view-point (or a philosophy) in number theory called the local-global principle. It advocates to study a problem over $\mathbf{Q}$ by studying it over various completions of $\mathbf{Q}$, i.e., over $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p. Interested readers may consult any good book on number theory to see it in action.

References

[1] Fernando Q. Gouvêa, "p-adic Numbers: An Introduction," 3rd ed., Springer-Verlag, Berlin, 2020.
[2] J-P. Serre, "A Course in Arithmetic," 1st ed., Springer-Verlag, New York, 1973.