9. p-ADIC NUMBERS: I

The real numbers $\mathbb{R}$ are an extension of the rational numbers $\mathbb{Q}$. It turns out that for every prime p there is an alternative way to extend the rational numbers.

One way to think of a real number is as a decimal, with a potentially infinite expansion. If you think back, the trickiest part of this whole story is how the rational numbers sit inside the reals. Rationals correspond to reals with a possible infinite, but repeating decimal expansion.

The impetus for p-adic numbers comes from the problem of solving polynomial equations modulo higher and higher powers of p. For example, imagine finding the square root of 2. As in Math 104A one can mimic Newton-Raphson. We start with the function

$$f(x) = x^2 - 2.$$

Over the reals we start with an approximate solution $x_0 = 3/2 = 1.5$. Suppose the actual root is $\xi = x_0 + h$. We have

$$\begin{aligned} 0 &= f(\xi) \\ &= f(x_0) + f'(x_0)h + \dots . \end{aligned}$$

We assume that h is small, so that the higher terms are small. If we ignore the higher terms we get the next approximation:

$$0 = f(x_0) + f'(x_0)h,$$

so that

$$h = \frac{-f(x_0)}{f'(x_0)}.$$

Then

$$x_1 = x_0 + h,$$

and we keep going. Since $f'(x) = 2x$, $f'(x_0) = 3$ and so

$$h = -\frac{1}{12}.$$

Thus

$$x_1 = \frac{17}{12}$$

is a better approximation, and so on.

Now suppose that we wanted to solve this equation modulo higher and higher powers of 7. 2 is a quadratic residue modulo 7. In fact $3^2 = 9 \equiv 2 \mod 7$.

To get an approximation modulo 7^2 we have to solve a linear equation:

$$f(3+7t) = 7 + 7t \cdot 6 \equiv 0 \mod 7^2.$$

Thus $6t \equiv -1 \mod 7$, so that $t = 1$. Thus $3+1\cdot 7$ is a solution modulo 7^2. To get a solution modulo 7^3 we have to solve

$$f(3 + 1 \cdot 7 + t \cdot 7^2) = (3 + 1 \cdot 7)^2 - 2 + 2(3 + 1 \cdot 7) \cdot 7^2 t \equiv 0 \mod 7^3.$$

This reduces to $6t + 2 \equiv 0 \mod 7$, so that $t = 2$. Thus $3 + 1 \cdot 7 + 2 \cdot 7^2$ is a solution modulo 7^3.

To get a solution modulo 7^4 we have to solve

$$f(3+1\cdot 7+2\cdot 7^2+t\cdot 7^3) = (3+1\cdot 7+2\cdot 7^2)^2-2+2(3+1\cdot 7+2\cdot 7^2)\cdot 7^3 t \equiv 0 \mod 7^4.$$

This reduces to $6t + 34 \equiv 0 \mod 7$, so that $t = 6$. Thus $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3$ is a solution modulo 7^4.

We can continue this process indefinitely. It is tempting to try to make sense of an infinite expansion

$$\xi = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \ldots,$$

which is an exact solution to the equation $x^2 - 2 = 0$.

This suggests we make a definition:

Definition 9.1. *Let p be a prime. A **p-adic integer** is a sequence*

$$a_0, a_1, a_2, \ldots$$

of integers from 0 to $p-1$.

It is convenient to denote a p-adic integer as

$$a_0 + a_1 \cdot p + a_2 \cdot p^2 + \ldots.$$

Note that the usual integers all have a representation as a p-adic integer, where all but finitely many terms are zero.

To add two such sequences we add corresponding terms and carry as appropriate. Similarly we multiply two such sequences in the usual way, remembering to carry a term that exceeds $p-1$. It is not hard to see that this extends the usual rules of addition and multiplication of integers. In fact

Proposition 9.2. *The set $\mathcal{O}_p$ of all p-adic integers is a ring. If R_p denotes the set of all rational numbers a/b where p does not divide b, then there is a natural ring homomorphism*

$$R_p \longrightarrow \mathcal{O}_p.$$

Note that if we add and multiply two rational numbers whose denominator is not divisible by p then we get a rational number which is not divisible by p. Thus R_p is indeed a subring of all rational numbers. Not only do we extend the usual rules of addition and multiplication of ordinary integers, we actually extend the usual rules of addition and multiplication of rational numbers of the form a/b, where p does not divide b.

Suppose that we square ξ,

$$\xi = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \dots,$$

If we square the usual way, we get

$$\xi = 9 + 6 \cdot 7 + 13 \cdot 7^2 + 40 \cdot 7^3 + \dots.$$

Now if we subtract 2 and carry then we see that

$$\xi^2 = 2.$$

One can extend the p-adic integers to p-adic numbers $\mathbb{Q}_p$ by formally inverting p. A p-adic number is then of the form

$$\frac{1}{p^N}(a_0 + a_1 \cdot p + a_2 \cdot p^2 + \dots)$$

where the expression in brackets is a p-adic integer. $\mathbb{Q}_p$ is a field, meaning that one can add, multiply, subsract and divide. In practice this means we have show every non-zero p-adic integer has an inverse.