Lecture 13.2

The p-adic numbers

Motivations:

- For a prime p, solutions to

$$f(x) \equiv 0 \pmod{p}$$

$$f(x) \equiv 0 \pmod{p^2}$$

$$f(x) \equiv 0 \pmod{p^3}$$

etc.

can often be packaged together into coherent sequences

$$(x_n) = (x_1, x_2, x_3, \ldots)$$

where $f(x_n) \equiv 0 \pmod{p^n}$.

- Sequences like

$$(x_n) = (2, 17, 42, 417, 1042, \ldots)$$

which appear to diverge can be made to converge, with a different notion of distance.

(The above sequence converges to $\frac{1}{3}$ in the 5-adic number system.)

- Writing numbers in their base p expansion,

$$27 = 1 \cdot 25 + 0 \cdot 5 + 2 \cdot 1,$$

lets us treat them like polynomials

$$a = a_n p^n + \ldots + a_1 p + a_0.$$

Then fractions are like rational functions

$$\frac{a}{b} = \frac{a_n p^n + \ldots + a_1 p + a_0}{b_m p^m + \ldots + b_1 p + b_0}.$$

The p-adic numbers play the role of power series in this analogy:

$$\ldots + a_2 p^2 + a_1 p + a_0 = \sum_{i=0}^{\infty} a_i p^i.$$

Numbers	Functions
natural number $a = \sum_{i=0}^{n} a_i p^i$	polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$
rational number $\frac{a}{b} = \frac{\sum_{i=0}^{n} a_i p^i}{\sum_{i=0}^{m} b_i p^i}$	rational function $\frac{f(x)}{g(x)} = \frac{\sum_{i=0}^{n} a_i x_i}{\sum_{i=0}^{m} b_i x_i}$
p-adic integer $\sum_{i=0}^{\infty} a_i p^i$	power series $\sum_{i=0}^{\infty} a_i x^i$

p-adic number

$$\sum_{i=-n}^{\infty} a_i p^i$$

Laurent series

$$\sum_{i=-n}^{\infty} a_i x^i$$

With this analogy, we can already construct a p-adic representation for any $n \in \mathbb{Z}$:

$$n = a_n p^n + a_{n-1} p^{n-1} + \dots + a_1 p + a_0$$

for <u>unique</u> integers $a_0, a_1, \dots, a_n$ satisfying

$$0 \le a_i \le p-1 \quad \text{for each } i.$$

Ex 1 For $p = 5$, we have

$5 = 1 \cdot 5 + 0 \cdot 1 \longleftrightarrow \dots 00010$

$7 = 1 \cdot 5 + 2 \cdot 1 \longleftrightarrow \dots 00012$

$70 = 2 \cdot 25 + 4 \cdot 5 + 0 \cdot 1 \longleftrightarrow \dots 00240$

We can add and multiply in base 5:

$$5 + 7 = (1 \cdot 5 + 0 \cdot 1) + (1 \cdot 5 + 2 \cdot 1)$$

$$= 2 \cdot 5 + 2 \cdot 1$$

$$7 + 70 = (1 \cdot 5 + 2 \cdot 1) + (2 \cdot 25 + 4 \cdot 5 + 0 \cdot 1)$$

$$= 2 \cdot 25 + 5 \cdot 5 + 2 \cdot 1$$

$$= 3 \cdot 25 + 2 \cdot 1.$$

Subtraction and division are more subtle, e.g.

-1 is the unique solution to

$$x + 1 = 0.$$

If $x = \ldots + a_2 \cdot 25 + a_1 \cdot 5 + a_0 \cdot 1$ then

$$x + 1 = (\ldots + a_2 \cdot 25 + a_1 \cdot 5 + a_0 \cdot 1) + (1 \cdot 1)$$

$$= \ldots + a_2 \cdot 25 + a_1 \cdot 5 + (a_0 + 1) \cdot 1$$

so $a_0 + 1 = 0$ OR $a_0 + 1 = 5$, in which case

not possible for $0 \le a_0 \le 4$

$a_0 = 4$ and we can carry the power of 5:

$$x + 1 = \ldots + a_2 \cdot 25 + a_1 \cdot 5 + 5 \cdot 1$$

$$= \ldots + a_2 \cdot 25 + (a_1 + 1) \cdot 5.$$

This is still equal to 0, so $a_1 + 1 = 0$

OR $a_1 + 1 = 5$. Repeating the same steps gives us the base 5 expansion of -1:

$$-1 = \ldots + 4 \cdot 125 + 4 \cdot 25 + 4 \cdot 5 + 4 \cdot 1$$

$$= \ldots 4444.$$

Remark: This is analogous to the identity

$$0.999\ldots = 1$$

which we can verify using power series:

$$0.999\ldots = 9\cdot 10^{-1} + 9\cdot 10^{-2} + 9\cdot 10^{-3} + \ldots$$

$$= \sum_{i=1}^{\infty} 9\cdot 10^{-i} = \frac{9/10}{1 - 1/10}$$ by geometric series

$$= \frac{9/10}{9/10} = 1.$$

Technically, we should say the sequence

$$0.9,\ 0.99,\ 0.999,\ \ldots$$

converges to 1.

What we're building towards is a way of

saying $4, 44, 444, \ldots$ converges to -1.

To make this rigorous, we will need to define a new notion of "distance".

Similarly, we can express fractions in base 5,

e.g. $\frac{1}{2}$ is the unique solution to

$$2x = 1.$$

If $x = \ldots + a_2 \cdot 25 + a_1 \cdot 5 + a_0 \cdot 1$ then

$$2x = \ldots + 2a_2 \cdot 25 + 2a_1 \cdot 5 + 2a_0 \cdot 1$$

so ~~$2a_0 = 1$~~ OR $2a_0 \geq 5$.

not possible for $0 \leq a_0 \leq 4$

Write $2a_0 = 5 + r_0$, $1 \le r_0 \le 3$. Then

$$2x = \ldots + 2a_2 \cdot 25 + 2a_1 \cdot 5 + 2a_0 \cdot 1$$

$$= \ldots + 2a_2 \cdot 25 + (2a_1 + 1) \cdot 5 + r_0 \cdot 1.$$

From this, we learn two things:

- $r_0 = 1 \Longrightarrow 2a_0 = 6 \Rightarrow a_0 = 3$
- ~~$2a_1 + 1 = 0$~~ OR $2a_1 + 1 \ge 5$.

Write $2a_1 + 1 = 5 + r_1$, $0 \le r_1 \le 4$.

Then $2x = \ldots + 2a_2 \cdot 25 + (2a_1 + 1) \cdot 5 + 3 \cdot 1$

$$= \ldots + 2a_2 \cdot 25 + (5 + r_1) \cdot 5 + 3 \cdot 1$$

$$= \ldots + (2a_2 + 1) \cdot 25 + r_1 \cdot 5 + 3 \cdot 1.$$

This implies $r_1 = 0$, so $2a_1 + 1 = 5$ and

we deduce $a_4 = 2$. The full base 5 expansion of $1/2$ is:

$$\frac{1}{2} = \ldots 2 \cdot 125 + 2 \cdot 25 + 2 \cdot 5 + 3 \cdot 1$$

$$= \ldots 2223.$$

Exercise 1: For each prime p and number a, find the p-adic expansion of a.

(a) $p = 3$, $a = 72$

(b) $p = 7$, $a = 320$

(c) $p = 7$, $a = 321$

(d) $p = 7$, $a = \frac{320}{49}$

(e) $p = 7$, $a = -1$

(f) $p = 11, \quad a = -1$

(g) $p = 11, \quad a = \frac{1}{2}$

(h) $p = 3, \quad a = \frac{24}{17}$

Exercise 2: Do you see a pattern so far for the p-adic expansion of -1? Try to prove it if so.

The examples so far indicate the following patterns:

Prop Fix a prime p. Then any rational number $\frac{a}{b}$ has a unique p-adic expansion

$$\frac{a}{b} = \dots + c_2 p^2 + c_1 p + c_0 + c_{-1} p^{-1} + \dots + c_{-n} p^{-n}$$

where:

(a) Each c_i is an integer $0 \leq c_i \leq p-1$.

(b) $c_{-1} = \dots = c_{-n} = 0$ if and only if $p \nmid b$.

(c) $c_0 = c_{-1} = \dots = c_{-n} = 0$ if and only if $p \nmid b$ and $p \mid a$.

Let's reinterpret these p-adic expansions using modular arithmetic.

Ex Recall that the 5-adic expansion of -1 was obtained by solving

$$x + 1 = 0$$

p-adically, i.e. by comparing p-adic expansions and solving for the coefficients of x. Let's instead consider the system of congruences

$$x+1 \equiv 0 \pmod 5$$

$$x+1 \equiv 0 \pmod{25}$$

$$x+1 \equiv 0 \pmod{125}$$

$$\vdots$$

$$x+1 \equiv 0 \pmod{5^n}$$

$$\vdots$$

If $x = \sum_{i=0}^{\infty} a_i 5^i$ is a 5-adic expansion satisfying $x+1=0$, then

$$x+1 \equiv a_0 + 1 \equiv 0 \pmod 5$$

$$x+1 \equiv 5a_1 + a_0 + 1 \equiv 0 \pmod{25}$$

$$\vdots$$

$$x+1 \equiv \left(\sum_{i=0}^{n-1} a_i 5^i\right) + 1 \equiv 0 \pmod{5^n}$$

$$\vdots$$

Set $x_n = \sum_{i=0}^{n-1} a_i 5^i$. Then each x_n is a solution to $x+1 \equiv 0 \pmod{p^n}$ and $x_n \equiv x_{n-1} \pmod{p^{n-1}}$.

Working up the chain of congruences, we see that

$$x+1 \equiv a_0 + 1 \equiv 0 \pmod 5$$

$$\Longrightarrow a_0 \equiv 4 \pmod 5$$

$$x + 1 \equiv 5a_1 + 5 \equiv 0 \pmod{25}$$

$$\Rightarrow a_1 \equiv 4, 9, 14, 19, 24 \pmod{25}$$

$$\Rightarrow a_1 \equiv 4 \pmod{5}$$

$$x + 1 \equiv 25a_2 + 25 \equiv 0 \pmod{125}$$

$$\Rightarrow a_2 \equiv 4, 9, \ldots, 119, 124 \pmod{125}$$

$$\Rightarrow a_2 \equiv 4 \pmod{25}$$

etc.

Exercise 3: Use induction to confirm that $a_i \equiv 4 \pmod{5^{i-1}}$ for each $i \geq 2$.

This allows us to "lift" the sequence of residue classes $(4 \bmod 5^i)$ to

the coefficients of -1:

$$-1 = \ldots + 4 \cdot 125 + 4 \cdot 25 + 4 \cdot 5 + 4 \cdot 1.$$

Def For a prime p, a *coherent sequence* is a sequence of integers $(x_n)_{n \geq 1}$ such that for each $n \geq 1$,

(1) $0 \leq x_n \leq p^n - 1$

(2) $x_n \equiv x_{n-1} \pmod{p^{n-1}}$.

Next time: more examples, definition of p-adic numbers, convergence.