# Lecture 14.1

Last time:

- We can do arithmetic with p-adic expansions of integers and rational numbers by treating them as:

  - polynomials in $p$ (nonnegative integers)
  - rational functions in $p$ (rationals)
  - power series in $p$ (negative numbers).

- As a 5-adic number,

$$-1 = \sum_{i=0}^{\infty} 4 \cdot 5^i = \ldots 444.$$

---

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

$\boxed{\text{Ex}}$ 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

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

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

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

$$\vdots$$

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

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

$$\vdots$$

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

<u>and</u> $x_n \equiv x_{n-1} \pmod{p^{n-1}}$.

Working up the chain of congruences, we see that

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

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

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

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

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

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

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

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

etc.

**Exercise 1:** 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 $-1$:

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

$\boxed{\text{Def}}$ 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) $x_n \equiv x_{n-1} \pmod{p^{n-1}}$.

$\boxed{\text{Ex}}$ 1 Let's construct a coherent sequence of solutions to the equation

$$x^2 - 25 = 0$$

using mod $3^n$ arithmetic:

$$x^2 - 25 \equiv 0 \pmod{3}$$

$$x^2 - 25 \equiv 0 \pmod{9}$$

$$\vdots$$

(Pretend you don't know the solutions are $x = \pm 5$.)

The first congruence becomes

$$x - 1 \equiv (x-1)(x-2) \equiv 0 \pmod 3$$

which has solutions $x \equiv 1, 2 \pmod 3$.

Next,

$$x^2 - 25 \equiv (x-5)(x-4) \equiv 0 \pmod 9$$

which has solutions $x \equiv 4, 5 \pmod 9$.

Notice that $5 \equiv 2 \pmod 3$

and $4 \equiv 1 \pmod 3$,

so we should start two separate coherent sequences:

$x_1 = 2, \quad x_2 = 5$

$y_1 = 1, \quad y_2 = 4.$

Next, $x^2 - 25 \equiv (x-5)(x-22) \equiv 0 \pmod{27}$

has solutions $x \equiv 5, 22 \pmod{27}$, which fit into the existing sequences like this:

$$x_1 = 2, \quad x_2 = 5, \quad x_3 = 5$$

$$y_1 = 1, \quad y_2 = 4, \quad y_3 = 22.$$

Here are the fourth terms:

$$x_1 = 2, \quad x_2 = 5, \quad x_3 = 5, \quad x_4 = 5$$

$$y_1 = 1, \quad y_2 = 4, \quad y_3 = 22, \quad y_4 = 76.$$

To see where things are heading, let's reinterpret these 3-adically:

$$x_1 = 2 \cdot 1$$

$$x_2 = 1 \cdot 3 + 2 \cdot 1$$

$$x_3 = 1 \cdot 3 + 2 \cdot 1$$

$$x_4 = 1 \cdot 3 + 2 \cdot 1.$$

This pattern continues indefinitely (can you prove it rigorously?), so the coherent sequence $(x_1, x_2, x_3, x_4, \ldots) = (2, 5, 5, 5, \ldots)$ can be said to "converge" to

$$\ldots + 0 \cdot 27 + 0 \cdot 9 + 1 \cdot 3 + 2 \cdot 1 = 5,$$

one of the actual solutions to $x^2 - 25 = 0$!

What happens with the other sequence?

$$y_1 = 1 \cdot 1$$

$$y_2 = 1 \cdot 3 + 1 \cdot 1$$

$$y_3 = 2 \cdot 9 + 1 \cdot 3 + 1 \cdot 1$$

$$y_4 = 2 \cdot 27 + 2 \cdot 9 + 1 \cdot 3 + 1 \cdot 1.$$

In fact, the 2's repeat indefinitely from here, giving the 5-adic expansion

$$\ldots + 2 \cdot 27 + 2 \cdot 9 + 1 \cdot 3 + 1 \cdot 1 = -5,$$

the <u>other</u> solution to $x^2 - 25 = 0$ !

Exercise 2: Use induction to prove that

$$(x_1, x_2, x_3, x_4, \ldots) = (2, 5, 5, 5, \ldots)$$

and $(y_1, y_2, y_3, y_4, \ldots) = (1, 1, 2, 2, 2, 2, \ldots)$.

Then show that the second sequence determines the 3-adic expansion of $-5$.

Exercise 3: Repeat the process for

(a) $x^2 - 49 = 0$ with $p = 5$

(b) $x^3 - 27 = 0$ with $p = 2$.

There's nothing forcing us to use equations with integer solutions.

$\boxed{\text{Ex}}$ 2 Let's solve $x^2 + 1 = 0$ using 5-adic expansions.

$$x^2 + 1 \equiv (x-2)(x-3) \equiv 0 \pmod{5}$$

$$x^2 + 1 \equiv (x-7)(x-18) \equiv 0 \pmod{25}$$

$$x^2 + 1 \equiv (x-57)(x-68) \equiv 0 \pmod{125}$$

$$x^2 + 1 \equiv (x-182)(x-443) \equiv 0 \pmod{625}$$

etc.

The coherent sequences are

$$(x_1, x_2, x_3, x_4, \ldots) = (2, 7, 57, 182, \ldots)$$

$$(y_1, y_2, y_3, y_4, \ldots) = (3, 18, 68, 443, \ldots)$$

which correspond to the following 5-adic expansions:

$$(x_n) \longrightarrow \quad \ldots + 1 \cdot 125 + 2 \cdot 25 + 1 \cdot 5 + 2 \cdot 1 = \ldots 1212$$

$$(y_n) \longrightarrow \quad \ldots + 3 \cdot 125 + 2 \cdot 25 + 3 \cdot 5 + 3 \cdot 1 = \ldots 3233.$$

We might say $\sqrt{-1} = \ldots 1212$ as a 5-adic number and $-\sqrt{-1} = \ldots 3232$.

In fact, there's no reason we can't switch them and call $\sqrt{-1} = \ldots 3232$

and $-\sqrt{-1} = \ldots 1212$.

In any case, this suggests that there is

a 5-adic solution to

$$x^2+1=0.$$

**Exercise 4:** Why does $x^2+1 \equiv 0 \pmod{5^n}$ have a solution for all $n \geq 1$? Also, show that our two 5-adic solutions above satisfy $x+y=1$.

---

## $\boxed{\text{p-adic Convergence}}$

**Question:** What does it mean that a p-adic expansion $\sum_{i=-N}^{\infty} a_i p^i$ represents a number?

In calculus, we say a power series

$$f(x) = \sum^{\infty}$$

$$F(x) = \sum_{i=0} a_i x^i$$

converges at $x = x_0$ if

$$\lim_{n \to \infty} \sum_{i=0}^{n} a_i x_0^i$$

exists, and we say the limit is $F(x_0)$.

In more detail, this says that for any possible discrepancy $\varepsilon > 0$ between the partial sums and the target $F(x_0)$, there's some $N$ so that for all $n \geq N$,

$$\underbrace{\left| \sum_{i=0}^{n} a_i x_0^i - F(x_0) \right|}_{\text{distance between nth partial sum and target } F(x_0)} < \varepsilon.$$

**Goal:** Make a new definition of $|\cdot|$ to make <u>some</u> p-adic power series $\sum_{i=-N}^{\infty} a_i p^i$ converge.

the ones coming from coherent sequences

We do this in two steps.

$\boxed{\text{Def}}$ Fix a prime $p$. For an integer $a \neq 0$, write $a = p^n b$ where $n \geq 0$ and $p \nmid b$. The p-adic valuation of $a$ is $n$, written

$$v_p(a) = n.$$

For rational numbers $\frac{a}{b} \neq 0$, we extend the definition by

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Also, set $v_p(0) = \infty$.

**Exercise 5:** Prove that if $\frac{a}{b} = \frac{c}{d}$, then $v_p\left(\frac{a}{b}\right) = v_p\left(\frac{c}{d}\right)$. That is, the definition of $v_p$ does not depend on how we write fractions.

**Exercise 6:** Compute each of the following:

(a) $v_5(400)$

(b) $v_7(902)$

(c) $v_2(621)$

(d) $v_3\left(\frac{123}{\ldots}\right)$

(d) $v_3\left(\frac{1}{48}\right)$

(e) $v_5\left(\frac{180}{3}\right)$

$\boxed{\text{Prop}}$ For any rational numbers $x, y$,

(1) If $x$ has $p$-adic expansion

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

with $a_{-N} \neq 0$, then $v_p(x) = -N$.

(2) $v_p(xy) = v_p(x) + v_p(y)$.

(3) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

Exercise 7: Prove the Proposition.

$\boxed{\text{Def}}$ For any rational number $x$, the $p$-adic

absolute value of $x$ is

$$|x|_p := p^{-v_p(x)}$$

where we interpret $|0|_p = p^{-\infty} = 0$.

This allows us to measure distances $p$-adically:

$$\mathrm{dist}_p(x,y) := |x-y|_p .$$

Informally, $x$ and $y$ are $p$-adically "close" if $x-y$ is highly divisible by $p$ (and $x$ is "small" if it is highly divisible by $p$).

Exercise 8: Compute $|x|_p$ for each number

in Exercise 6.

$\boxed{\text{Prop}}$ Fix $p$ and let $x, y$ be rational.

(1) $|x|_p = 0$ if and only if $x = 0$.

(2) $|xy|_p = |x|_p |y|_p$.

(3) $|x+y|_p \leq |x|_p + |y|_p$. In fact,

$|x+y|_p \leq \max\{|x|_p, |y_p|\}$.

This says $|\cdot|_p$ is an absolute value function on the field $\mathbb{Q}$ of rationals.

(4) $|1|_p = 1$ and $|-1|_p = 1$.

(5) $|n|_p \leq 1$ if and only if $n \in \mathbb{Z}$.

Next time: p-adic analysis.