Lecture 26: p-adic numbers.

Mention resources. [Many ways to motivate...]

**Diophantine Equations:** Given $f \in \mathbb{Z}[x_1, \ldots, x_k]$ does $f = 0$ have a solution with $x_i \in \mathbb{Z}$?

**Weaker Q:** Does $f \equiv 0 \pmod{m}$ have a solution for all $m \in \mathbb{Z}$?

By the Chinese Remainder Theorem, solving $f \equiv 0 \pmod{m}$ for all $m$ is again to solving $f \equiv 0 \pmod{p}$ for all prime powers. [For fixed $p$, is equivalent to solving over $\mathbb{Z}_p$, the $p$-adic integers.]

Fix a natural prime $p$. The $p$-adic integers are

$$
\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^k \mathbb{Z} = \left\{ (a_1, a_2, a_3, \ldots) \mid a_k \in \mathbb{Z}/p^k \mathbb{Z}, a_{k+1} \equiv a_k \pmod{p^k} \right\}
$$

which we can think of in terms of

$$
\mathbb{Z}/p \mathbb{Z} \leftarrow \mathbb{Z}/p^2 \mathbb{Z} \leftarrow \mathbb{Z}/p^3 \mathbb{Z} \leftarrow \mathbb{Z}/p^4 \mathbb{Z} \leftarrow \cdots
$$

$$a_1 \leftarrow a_2 \leftarrow a_3 \leftarrow a_4 \leftarrow \cdots
$$

**Note:**

1. $\mathbb{Z}_p$ are a ring (add + mult the corner)
2. $\mathbb{Z} \cong \mathbb{Z}_p$ via $a \mapsto (a \pmod{p}, a \pmod{p^2}, a \pmod{p^3}, \ldots)$
However, \( \mathbb{Z}_p \) is much larger than \( \mathbb{Z} \) — it is uncountable as we'll see shortly. Concretely,

\[ \mathbb{Z}_5 \text{ contains } \frac{1}{2}, \frac{1}{3}, i, \sqrt{6}, \sqrt{11}, \sqrt{3}, \ldots \]

\[ \text{Ex: } i = (3, 18, 68, 443, 1068, 1068, 32318, \ldots) \mod 5 \]
\[ z = (2, 2, 2, 2, 2, 2, \ldots) \]

Since \( a_{n+1} \equiv a_n \mod p^n \), have \( a_{n+1} = a_n + b_n \cdot p^n \)

where \( b_n \in 0, 1, \ldots, p-1 \). Thus

\[ a_1 = b_0, \quad a_2 = a_1 + b_1 \cdot p = b_0 + b_1 \cdot p \]
\[ a_3 = b_0 + b_1 \cdot p + b_2 \cdot p^2, \ldots, \quad a_n = \sum_{k=0}^{n-1} b_k \cdot p^k \]

Purely formally (for now!) we write

\[ (a_n) = \sum_{k=0}^{\infty} b_k \cdot p^k \]

\[ \text{Ex: } \text{in } \mathbb{Z}_5, \quad i = 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 2 \cdot 5^6 + 5^7 + \ldots \]
\[ = 3, 3231021412243143, \ldots \]
\[ 5\text{-adic expansion} \]

\[ 158 = 3 + 5 + 5^2 + 5^3 = 3, 111 \]
Alternate point of view.

Recall: constructed \( R \) from \( \mathbb{Q} \) by completing it w.r.t. the metric \( d(x,y) = |x - y|_p \).

\( p \)-adic Absolute Value:

Fix a prime \( p \). For \( a \in \mathbb{Z} \) define \( |a|_p = p^{-k} \) where \( p^k \) is the largest power of \( p \) dividing \( a \).

Example: \( |20|_3 = 1, \ 121/3 = \frac{1}{3}, \ 181/3 = \frac{1}{81}, \ 101/3 = 0 \).

Extend \( |r|_p \) to \( \mathbb{Q} \) by \( |r|_p = p^{-k} \) where \( r = p^k \frac{a}{b} \) with \( a, b \) coprime to \( p \). Equivalently, \( \frac{|x|_p}{|y|_p} = \frac{|x|_p}{|y|_p} \).

Example: \( |19/21|_3 = 3, \ |118/81|_3 = \frac{1}{81} \).

Properties: for \( r,s \in \mathbb{Q} \)

\[ |r|_p = 0 \iff r = 0 \]

\[ |rs|_p = |r|_p |s|_p \]

\[ |r+s|_p \leq \max \{ |r|_p , |s|_p \} \leq |r|_p + |s|_p \]

\( \uparrow \) non-Archimedean prop

\( \iff \) of the last one:

\[ r = p^k \frac{a}{b}, \quad s = p^j \frac{c}{d}, \quad a,b,c,d \text{ coprime to } p. \]

WLOG assume \( k \geq j \)

\[ r+s = p^i \left( \frac{p^{k-j} ad + bc}{bd} \right) \] and so
\[ |r + s|_p = |s|_p \cdot |p^{k-1} a d - b c|_p \leq |s|_p \]

The completion of \( \mathbb{Q} \) with \( \| \cdot \|_p \) is the field of \( p \)-adic numbers \( \mathbb{Q}_p \). The closure of \( \mathbb{Z} \) in \( \mathbb{Q}_p \) is the \( \mathbb{Z}_p \) we discussed before.

Consider: \( p^n \to 0 \) in \((\mathbb{Z}, \| \cdot \|_p)\). Moreover, for a seq \( \{ b_k \}_{k=0}^{\infty} \) of elts of \( \{ 0, 1, 2, \ldots, p-1 \} \), the partial sums \( S_n = \sum_{k=0}^{n} b_k p^k \) form a Cauchy sequence:

\[ |S_n - S_m|_p \leq \max_{0 \leq k \leq m} \{ |b_k p^k|_p \} \leq p^{-n} \]

Thus, \( \sum_{k=0}^{\infty} b_k p^k \) exists in the completed space \( \mathbb{Z}_p \)...

To be continued.