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 sol'n with $x_i \in \mathbb{Z}$?

Weaker Q: Does $f \equiv 0 \bmod m$ have a sol'n for all $m \in \mathbb{Z}$?

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

Fix a rat'l prime p. The p-adic integers are

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z} = \left\{ (a_1, a_2, a_3, \ldots) \;\middle|\; \begin{array}{l} a_k \in \mathbb{Z}/_{k}\mathbb{Z} \\ a_{k+1} \equiv a_k \bmod p^k \end{array} \right\}$$

inverse or projective limit.

which we can think of in terms of

$$\begin{array}{ccccccccc} \mathbb{Z}/p\mathbb{Z} & \leftarrow & \mathbb{Z}/p^2\mathbb{Z} & \leftarrow & \mathbb{Z}/p^3\mathbb{Z} & \leftarrow & \mathbb{Z}/p^4\mathbb{Z} & \leftarrow & \cdots \\ a_1 & \leftarrow & a_2 & \leftarrow & a_3 & \leftarrow & a_4 & \leftarrow & \cdots \end{array}$$

Note: ① $\mathbb{Z}_p$ are a ring (add + mult the coor)

② $\mathbb{Z} \subseteq \mathbb{Z}_p$ via $a \mapsto (a \bmod p,\ a \bmod p^2,\ a \bmod p^3, \ldots)$

However, $\mathbb{Z}_p$ is <u>much</u> larger that $\mathbb{Z}$ — it's uncountable as we'll see shortly. Concretely, $\mathbb{Z}_5$ contains $\frac{1}{2}, \frac{1}{3}, i, \sqrt{6}, \sqrt{11}, \sqrt[3]{3}, \ldots$

<u>Ex</u>: $i = (3, 18, 68, 443, 1068, 1068, 32318, \ldots$
mod $5 \quad 25 \quad 125 \quad 625 \quad 5^5 \quad 5^6 \quad 5^7$

$2 = (2, 2, 2, 2, 2, \ldots)$

Since $a_{n+1} \equiv a_n \bmod p^n$, have $a_{n+1} = a_n + b_n p^n$ where b in $0, 1, \ldots, p-1$. Thus

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

Purely formally (for now!) we write

$$(a_n) = \sum_{k=0}^{\infty} b_k p^k$$

<u>Ex</u>: In $\mathbb{Z}_5$, $i = 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 2 \cdot 5^6 + 5^7 + \ldots$

$$= \underbrace{3.3231021412243\ldots}_{\text{5-adic expansion}}$$

$158 = 3 + 5 + 5^2 + 5^3 = 3.111$

Alternate point of view

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

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.

Ex: $|20|_3 = 1$, $|21|_3 = 1/3$, $|81|_3 = \frac{1}{81}$, $|0|_3 = 0$ by def

Extend $|\cdot|_p$ to $\mathbb{Q}$ by $|r|_p = p^{-k}$ where $r = p^k \frac{a}{b}$ with $a+b$ coprime to p. Equivalently, $\left|\frac{x}{y}\right|_p = \frac{|x|_p}{|y|_p}$

Ex: $\left|\frac{19}{21}\right|_3 = 3$, $\left|\frac{1181}{81}\right|_3 = \frac{1}{81}$

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

$|r|_p = 0 \iff r = 0$

$|rs|_p = |r|_p |s|_p$

$|r+s|_p \le \max\{|r|_p, |s_p|\} \le |r|_p + |s|_p$

non-Archimedean prop

Pf of the last one: $r = p^k \frac{a}{b}$ $\quad s = p^j \frac{c}{d}$ $\quad$ a, b, c, d coprime to p.

W.L.O.G assume $k \ge j$

$r+s = p^j\left(\frac{p^{k-j}ad + bc}{bd}\right)$ and so

$$|r+s|_p = |s|_p \cdot |p^{k-j} ad - bc|_p \leq |s_p|$$

$\boxed{}$

The completion of $\mathbb{Q}$ w.r.t $|\,|_p$ 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.

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

$$|S_n - S_m|_p \leq \max_{n<k\leq m} \{\underbrace{|b_k p^k|_p}_{=p^{-k}}\} = p^{-n}$$

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

<u>To be continued.</u>