Introduction to p-adic Integers

Molly Bradley

University of Pennsylvania Directed Reading Program

May 2, 2024

Modular Arithmetic

Surjective Map

$$\mathbb{Z} \to \mathbb{Z}/p^n, z \mapsto z \bmod p^n.$$

Example

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/5 & 156 &\mapsto 1 \\ \mathbb{Z} &\to \mathbb{Z}/25 & 156 &\mapsto 6 \\ \mathbb{Z} &\to \mathbb{Z}/125 & 156 &\mapsto 31 \\ \mathbb{Z} &\to \mathbb{Z}/625 & 156 &\mapsto 156 \end{aligned}$$

$$\ldots$$

p-adic Integers

Another Surjective Map

There is also a natural surjective map from any $\mathbb{Z}/p^n$ to $\mathbb{Z}/p^{n-1}$.

Sequence of Projections

$$... \to \mathbb{Z}/p^4 \to \mathbb{Z}/p^3 \to \mathbb{Z}/p^2 \to \mathbb{Z}/p$$

Example

$$... \to \mathbb{Z}/625 \to \mathbb{Z}/125 \to \mathbb{Z}/25 \to \mathbb{Z}/5$$

Definition

We define the p-adic integers to be the *inverse limit* of this system, and write $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n = \{(....b_3, b_2, b_1) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n \mid b_{i+1} \mapsto b_i \forall i \in \mathbb{N}\}$

Integers $\rightarrow$ p-adic Integers

Surjective Map

We use the surjective maps $\mathbb{Z} \to \mathbb{Z}/p^n$ to write any integer as a p-adic integer.

Example

$$156 \mapsto (...156, 156, 156, 31, 6, 1)$$

$$5 \mapsto (...5, 5, 5, 5, 5, 0)$$

$$-1 \mapsto (...3124, 624, 124, 24, 4)$$

Question

Are there elements of $\mathbb{Z}_p$ that aren't integers?

$$(...3906, 781, 156, 31, 6, 1)$$

Solving Equations

Example

We consider the equation $x^2 + 1 = 0$.

$$(x^2 + 1 = 0) \in \mathbb{Z}/5 \implies \mathbf{b_1 = 2} \implies b_2 = 2 + 5x$$

$$((2+5x)^2 + 1 = 0) \in \mathbb{Z}/25 \implies 4 + 20x + 25x^2 + 1 = 0 \implies 5 + 20x = 0$$

$$\implies 5(1 + 4x) = 0 \implies x = 1 \implies \mathbf{b_2 = 7}$$

$$(\ldots\mathbf{7}, \mathbf{2}) \cdot (\ldots\mathbf{7}, \mathbf{2}) + \mathbf{1} = (\ldots., \mathbf{0}, \mathbf{0})$$

Solving More Equations

Question

Will this continuous computation process always give us a valid solution?

Hensel's Lemma

Given $f(x)$, if there exists r such that $f(r) = 0 \mod p^k$ and $f'(r) \neq 0 \mod p$, then for any $m \leq k$, there exists s such that $f(s) = 0 \mod p^{k+m}$, and $s = r \mod p^k$.

Analytic Perspective on the p-adic Integers

Localization of $\mathbb{Z}$ at (p)

$$\mathbb{Z}_{(p)} = \left\{ \frac{n}{d} \mid n, d \in \mathbb{Z}, d \nmid p \right\}$$

p-adic Norm

$$||x - y|| = \left(\frac{1}{p} \right)^{v(x-y)}$$

We define $v(x - y)$ by decomposing $x - y = p^a \cdot \frac{m}{d}$ with m, d coprime to p and setting $v(x - y) = a$.

Analytic Completion

We can equivalently define $\mathbb{Z}_p$ as the completion of $\mathbb{Z}_{(p)}$ with regards to the p-adic norm.

Applications of p-adic Integers

Hasse-Minkowski Theorem

1. Fundamental result in Number Theory.
2. States that a quadratic form has a solution over $\mathbb{Q}$ iff it has a solution over $\mathbb{Q}_p$ for all primes p and over $\mathbb{R}$.
3. This is very helpful! Tools like Hensel's lemma allow us to find solutions more easily in these fields.

Acknowledgements

Thank you so much to my mentor, Deependra Singh!

Sources: A Course in Arithmetic, Jean-Pierre Serre.