Lecture 4

Recap: In Lecture 3, we proved

$(a,b)_F$ splits over $F \iff C(a,b): ax^2+by^2=1$ has soln $(x,y)\in F^2$.

$F=\mathbb{Q}$: hard to determine!

$F=\mathbb{R}$: just need $a>0$ or $b>0$

Today: $F=\mathbb{Q}_p$ (p-adics): reduces to congruence checks modulo a prime p and powers p^n.

We'll show $\mathbb{Q}\subseteq\mathbb{R}$ and $\mathbb{Q}\subseteq\mathbb{Q}_p$ for each prime p, so a soln to an eqn over $\mathbb{Q}$ $\Rightarrow$ soln over $\mathbb{R}$ & $\mathbb{Q}_p$.

Def: Let p be a prime number. The ring of p-adic integers is

$$\mathbb{Z}_p := \left\{ (a_n)_{n\geq 1} \in \prod_{n\in\mathbb{Z}^+} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; a_{n+1} \equiv a_n \bmod p^n \right\}$$

Addition and multiplication are defined component-wise.

Note: $1_{\mathbb{Z}_p} = (\bar{1},\bar{1},\bar{1},\dots)$ where $\bar{1}$ denotes residue class of 1 in $\mathbb{Z}/p^n\mathbb{Z}$.

The integers form a subring of $\mathbb{Z}_p$ via

$$\begin{aligned} \mathbb{Z} &\hookrightarrow \mathbb{Z}_p \\ x &\longmapsto (x \bmod p,\ x \bmod p^2,\ x \bmod p^3,\ \dots) \end{aligned}$$

Made with Goodnotes

Extended example : $\mathbb{Z}_5$

"$\frac{1}{2}$" in a ring means a solution to linear equation $2x = 1$.

What does this look like in $\mathbb{Z}_5$?

unique soln at each step.

$n=1$: $2a_1 \equiv 1 \bmod 5 \implies a_1 = 3$

$n=2$: $2a_2 \equiv 1 \bmod 5^2$ and $a_2 \equiv a_1 \bmod 5$ (or $a_2 = a_1 + 5k$)

So $2(3+5k) \equiv 1 \bmod 5^2 \implies k = 2 \implies a_2 = 13$

$n=3$: $2a_3 \equiv 1 \bmod 5^3$ and $a_3 \equiv a_2 \bmod 5^2$ $(a_3 = a_2 + 5^2 \ell)$

So $2(13+5^2\ell) \equiv 1 \bmod 5^2 \implies \ell = 2 \implies a_3 = 63$

$\vdots$

In $\mathbb{Z}_5$, $\frac{1}{2} = (3, 13, 63, \ldots)$

What about quadratic equations? Let's look at $x^2 = -1$ in $\mathbb{Z}_p$.

- Just like in other rings, things can go wrong.
  $x^2 = -1$ has no soln in $\mathbb{Z}_3$ since $x^2 \equiv -1 \bmod 3$ has no soln.

- There are solutions in $\mathbb{Z}_5$ however:

$n=1$: $a_1^2 \equiv -1 \bmod 5 \implies a_1 = 2$ (or $a_1 = 3$)

$n=2$: $a_2^2 \equiv -1 \bmod 5^2$ and $a_2 \equiv a_1 \bmod 5$
$(a_2 = a_1 + 5k)$

So $(a_1+5k)^2 \equiv -1 \bmod 5^2 \implies k = 1$ and $a_2 = 7$

in Lecture 5 we'll see more about when/why this works. Nontrivial!

$n=3$: $a_3^2 \equiv -1 \bmod 5^3$ and $a_3 \equiv a_2 \bmod 5^2$...

$\implies \ell = 2$ and $a_3 = 57$ $(a_3 = a_2 + 5^2\ell)$

So $\alpha = (2, 7, 57, \ldots) \in \mathbb{Z}_5$ is one solution to $x^2 = -1$ in $\mathbb{Z}_5$.

Made with Goodnotes

To better understand the elements of $\mathbb{Z}_p$ and when polynomial eqns w/ integer coeffs have solns in $\mathbb{Z}_p$, observe that while natural, our defn of a compatible sequence has some redundancy.

Another way to view elements of $\mathbb{Z}_p$:

If $a=(a_n)\in\mathbb{Z}_p$ and we represent each a_n as an integer in the set $\{0,1,\dots,p^n-1\}$ then $a_{n+1}\equiv a_n \bmod p^n$ means we can always write $a_{n+1}=a_n+p^n\cdot b_n$ w/ $b_n\in\{0,1,\dots,p-1\}$

Def: Let $a=(a_n)\in\mathbb{Z}_p$ w/ $a_n\in\{0,1,\dots,p^n-1\}$. Let $b_0=a_1$ and $b_n=(a_{n+1}-a_n)/p^n$. The sequence $(b_0,b_1,b_2,\dots)$ is called the p-adic expansion of a.

We can represent elts of $\mathbb{Z}_p$ as formal power series in powers of p, ie., $(b_0,b_1,b_2,\dots)$ as $\sum_{n\geq 0} b_n p^n$. Here, $a_n\equiv\sum_{i=0}^{n-1} b_i p^i \bmod p^n$.

Ex from before:

$\frac{1}{2}$ in $\mathbb{Z}_5$: had $a_1=3$, $a_2=13$, $a_3=63$, ...

5-adic expn has $b_0=3$, $b_1=\frac{13-3}{5}=2$, $b_2=\frac{63-13}{5^2}=2$

and $\frac{1}{2}=3+2\cdot 5+2\cdot 5^2+\dots$ in $\mathbb{Z}_5$

Elts of $\mathbb{Z}_p$ are in bijection w/ formal power series $\sum_{n\geq 0} b_n p^n$ w/ $b_n\in\{0,\dots,p-1\}$

Made with Goodnotes

Via this perspective, you can verify that $\mathbb{Z}_p$ is an integral domain. Let $\mathbb{Q}_p$ be its field of fractions. Note that since $\mathbb{Z} \subseteq \mathbb{Z}_p$ we get $\mathbb{Q} \subseteq \mathbb{Q}_p$.

Goal: Understand isoms and splitting of quaternion algebras over $\mathbb{Q}$.

Turns out we can get a lot of insight by studying this question over $\mathbb{Q}_p$. (Lecture 5).

Example: Consider $A = (-1,-1)_{\mathbb{Q}_5}$. Does this algebra split over $\mathbb{Q}_5$? Have several ways to check now!

We saw that $\exists\, \alpha \in \mathbb{Z}_5$ with $\alpha^2 = -1$. Note that this gives us an elt $\alpha i + j \in A$ w/ $N(\alpha) = \alpha^2 + 1^2 = -1+1 = 0$. So A is not a division algebra, i.e., A splits!

Solving equations in $\mathbb{Z}_p$ or $\mathbb{Q}_p$ (mostly) reduces to solving congruences mod powers of p :)

Made with Goodnotes

Further properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$

- (Exercise): A p-adic integer $x = \sum_{n \geq 0} b_n p^n$ is invertible iff $b_0 \neq 0$ iff x is not divisible by p

- Every $x \neq 0 \in \mathbb{Z}$ can be written uniquely as

$$x = p^{v_p(x)} u \quad \text{w/ } p \nmid u.$$

Define $v_p(0) = \infty$ and $v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$.

This gives a function $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ called the p-adic valuation.

- Can extend defn of v_p to $\mathbb{Z}_p$: gives the smallest power of p in the p-adic expansion of an elt., i.e.

If $x = \sum_{i \geq k} b_i p^i = b_k p^k + b_{k+1} p^{k+1} + \dots = p^k \sum_{n \geq 0} b_{n+k} p^n$

then $v_p(x) = k$.

- Invertible elts in $\mathbb{Z}_p$ are then

$$\mathbb{Z}_p^\times = \{ x \in \mathbb{Z}_p \mid v_p(x) = 0 \}$$ (Exercise)

- Finally, elts of $\mathbb{Q}_p$ can be written as formal Laurent series in p: $x \in \mathbb{Q}_p \Rightarrow x = \sum_{n \geq k} b_n p^n$ for some integer $k \in \mathbb{Z}$.

Made with Goodnotes