Lecture 1.

1) Diophantine equations:

$\mathbb{Z}[x_1 \dots x_n]$

$$* \quad \begin{cases} f_1(x_1 \dots x_n) = 0 \\ \vdots \\ f_n(x_1 \dots x_n) = 0 \end{cases}$$

Lemma: TFAE

1) $*$ has $\mathbb{Z}^n$ solutn.
2) $*$ has solutions in $(\mathbb{Z}/m\mathbb{Z})^n$ $\forall m \in \mathbb{Z}_{>0}$
3) $*$ has solutions in $(\mathbb{Z}/p^m\mathbb{Z})^n$ $\forall p, m$.

Proof:

$1 \Leftrightarrow 2$ easy (linear algebra).

$2 \Leftrightarrow 3$ Chinese Remainder Theorem.

2) Q: Higher degrees? Q. Rational solutions?

Ex: $3x^3 + 4y^3 + 5z^3 = 0$ (Selmer)

Remark: Real solutions

3) Conclusion: $\mathbb{R} \oplus (\mathbb{Z}/p^m\mathbb{Z})^n$

4) Taylor expansion

$\mathbb{C}(z)$ (or $\mathbb{R}(x)$)

$$f(z) = f(0) + f'(0)z + \frac{f''}{2}(0)z^2 + \dots$$

- f → Rational functions
- $f(0)$ → poly
- $f'(0)z$ → formal
- $\frac{f''}{2}(0)z^2$ → convergn

5) $f = \sum_{i \geq -n} a_i z^i$ Laurent series.

Ex: $\frac{1}{1+z-z^2} = 1 + a_1 z + a_2 z^2 + \dots \pmod{z^4}$

6) $\frac{1}{3} = a_0 + a_1 5 + a_2 5^2 + a_3 5^3 + \dots$

$a_0 \in \{0, 1, 2, 3, 4, 5\}$

$* \quad \frac{1}{1-5} = a_0 + a_1 \cdot 5 + \dots$

check:

$2 + \left(\frac{1}{1-5^2} - 1\right) + 3 \cdot 5 \left(\frac{1}{1-5^2}\right) = \frac{1}{3}$

$1 = 3a_0 + 3a_1 \cdot 5 + 3a_2 \cdot 5^2 + \dots$

$a_0 = 2 \qquad -5 = 3a_1 \cdot 5 + 3a_2 \cdot 5^2 \dots$

$-1 = 3a_1 + 3a_2 \cdot 5 + \dots$

$a_1 = 3 \qquad -2 = 3a_2 + 3a_3 \cdot 5 + \dots$

$2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 3 \cdot 5^5 \dots$

$a_2 = 1 \qquad -1 = 3a_3 + 3a_4 \cdot 5 + \dots$

7) Fix $p > 0$ prime.

$f \in \mathbb{N}_{\geq 0}$

$$f = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n$$

$$a_0, a_1, \ldots a_n \in \{0, \ldots p-1\}.$$

$\Downarrow$

inductive

$$* \quad \begin{cases} f = a_0 + p \cdot f_1 \\ f_1 = a_1 + p f_2 \\ f_2 = a_2 + p f_3 \\ \vdots \\ f_n = a_n + 0. \end{cases}$$

8) Ex: $p = 5$ $\quad f = -1$

$$-1 = 4 + p \cdot (-1) \quad \Rightarrow \quad -1 \Rightarrow 4 + 4p + 4p^2 + \cdots$$

$$\frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 3 \cdot 5^5 \cdots$$

Fix p.

Lecture 1

9) Def: A p-adic integer is a formal infinite series

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

$$\forall a_i \in \{0, \ldots p-1\}$$

$\mathbb{Z}_p$ = the set of all p-adic integers.

10) Take any $q \in \mathbb{Q}$ s.t. $q = \frac{a}{b}$ $(a,b) = 1$

$p \nmid b$ $(\mathbb{Z}_{(p)})$

Then we can consider p-adic expon.

(similar to $q = 1/3$ $p = 5$)

Lemma: Take $a \in \mathbb{Z}/p^n\mathbb{Z}$. Then

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}$$

$$\forall a_i \in \{0, \ldots p-1\}$$

& they are unique.

Proof: induction on n.

11) Take $f \in \mathbb{Z}_{(p)}$ $f = \frac{a}{b}$ p ∤ b

$\Rightarrow \exists\, s_n = f \bmod p^n$ in $\mathbb{Z}/p^n\mathbb{Z}$

$s_1 = a_0 \bmod p$

$s_2 = a_0 + a_1 p \bmod p^2$

$\vdots$

$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}$ $\forall n \geq 1$

This defines $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$.

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

$\uparrow \quad \nearrow$

$\mathbb{Z}_{(p)}$

Claim: injective.

So we can identify $\mathbb{Z}$ with a subset of $\mathbb{Z}_p$.

Ex: $\frac{1}{1-p} = 1 + p + p^2 + \cdots$

Proof: $1 = (1 + p + \cdots + p^{n-1})(1-p) + p^n$

So $\frac{1}{1-p} \equiv 1 + p + \cdots + p^{n-1} \bmod p^n$

$\forall n$.

12) $\mathbb{Q}_p$

Def: A p-adic number is a formal infinite series

$$a_{-n}p^{-n} + a_{-(n-1)}p^{-(n-1)} \cdots + a_0 + a_1 p + \cdots$$

$n > 0$

$$\left(\sum_{i \geq -n} a_i p^i \right)$$

Similarly we can define a map:

$\mathbb{Q} \longrightarrow \mathbb{Q}_p$

compatible with "other" maps above

$\frac{a}{b} \rightsquigarrow \frac{1}{p^n}(a_0 + a_1 p + \cdots)$

expansion for $\frac{a}{b}$

$(a,b) = 1$

$(a,p) = 1$

$(b,p) = 1$

Claim: injective

So we can identify $\mathbb{Q}$ with a subset of $\mathbb{Q}_p$.

13) $\mathbb{Q}_p$ is a field, $\mathbb{Z}_p$ is a ring } natural compatible structures.

Try examples.

$$f = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$$

$$s_n = \sum_{i=0}^{n-1} a_i p^i \longrightarrow \bar{s}_n \in \mathbb{Z}/p^n\mathbb{Z}$$

$\bar{s}_1, \bar{s}_2, \bar{s}_3 \cdots$

$\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \cdots$

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$$

natural maps (projections)

$$\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} = \{ (x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z} \}$$

$\cup$

all elements $(x_n)_{n\in\mathbb{N}}$ s.t. $\lambda_n(x_{n+1}) = x_n$ $\forall\, n = 1, \cdots$

$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ projective limit

14) Proposition. $\exists$ natural map:

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

that is a bijection.

We can use this to equip $\mathbb{Z}_p$ with $+, -, \times$. So it is a Ring.

Then $\mathbb{Q}_p$ as its field of fractions:

$\forall f \in \mathbb{Q}_p$ we have. $f = g \cdot p^{-m}$

$g \in \mathbb{Z}_p$.

Note: $a \in \mathbb{Z} \rightsquigarrow$ $a \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \mod p^n$

$\downarrow$

$(a \bmod p,\ a \bmod p^2,\ a \bmod p^3 \ldots)$

15) Back to Diophantine eq.

$F \in \mathbb{Z}[x_1, \dots x_n]$

TFAE:

Th: $F(x_1, \dots x_n) \equiv 0 \bmod p^r \ \forall n$

* $\exists$ solution

** $F(x_1, \dots x_n) = 0$ is solvable in $\mathbb{Z}_p$.

Proof: $\Leftarrow$ by definition.

$\Rightarrow$ $n = 1$.

(x_r) a solution mod p^r

$\cup$

$(x_r^{(1)})$ s.t. all of them $\equiv y_1 \bmod p$.

$\cup$

$(x_r^{(2)})$ s.t. all of th $\equiv y_2 \bmod p^2$.

$\vdots$

$(y_1, y_2, y_3 \dots) \in \mathbb{Z}_p$. (projective lim)

16) Alternative approach

Fix p.

p-adic absolute value

$a \in \mathbb{Q} \Rightarrow a = \frac{b}{c} = p^m \frac{b'}{c'}$ b', c' are coprime top.

Put $|a|_p = \frac{1}{p^m}$.

Put $m = \nu_p(a)$. Put $\nu_p(0) = \infty$

$\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$

1) $\nu_p(a) = \infty \iff a = 0$

2) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

3) $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$

$x + \infty = \infty$

$x < \infty$

$\infty + \infty = \infty$

p-adic exponential valuation of $\mathbb{Q}$.

$|\ |_p : \mathbb{Q} \to \mathbb{R} \quad a \to |a|_p = p^{-\nu_p(a)}$

p-adic absolute value.

17) $|\ |_p$ satisfies

1) $|a|_p = 0 \iff a = 0$

2) $|ab|_p = |a|_p |b|_p$

3) $|a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$.

Rem: usual norm $|a| := |a|_\infty$

$\mathbb{Q}$ → Cauchy sequences → R/m (null seq)

$\mathbb{Z}_p \subset \mathbb{Q}_p$

$|x|_p \leq 1$.