The Diophantine Problem

Given a polynomial $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, does there exist $\underline{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ s.t. $F(\underline{a}) = 0$?

(one can ask the same question for other rings, e.g. $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{F}_p$)

if $F(\underline{a}) = 0$ then

$$F(\underline{a}) \equiv 0 \pmod N \qquad (*)$$

for every integer N is a necessary condition for integer solutions.

Ex.: 1. $x^2 - 3y^2 = 2$

mod 3, $x^2 \equiv 2 \pmod 3$, which is impossible.

2. $x^2 - 3y^2 = 7$

mod 4, no solutions.

3. $x^3 + y^3 + z^3 = 0 \Rightarrow 3 \mid xyz$

considering modulo 9

Chinese Remainder Theorem

$N = N_1 \cdot \dots \cdot N_r$, pairwise coprime

$$\mathbb{Z}/_N \simeq \mathbb{Z}/_{N_1} \times \mathbb{Z}/_{N_2} \times \dots \times \mathbb{Z}/_{N_r}$$

$a \bmod N \quad (a \bmod N_1, a \bmod N_2, \dots, a \bmod N_r)$

by the CRT, to have a solution to $(*)$ modulo every N, it is enough to have a solution modulo all powers of primes, p^k.

Congruences mod p (p prime)

$\mathbb{Z}/p$ is a field (the finite field with p elements).

sketch of proof:
for $x \neq 0 \in \mathbb{Z}/p$, consider $\phi: \mathbb{Z}/p \longrightarrow \mathbb{Z}/p$, $a \longmapsto ax$

we want to show that $\exists a: ax \equiv 1$. this will be true if ϕ is injective (since $\mathbb{Z}/p$ is finite).

if $ax \equiv 0 \pmod p$, i.e. $p \mid ax$ then either $p \mid a$ or $p \mid x$. but $x \neq 0$ so $a \equiv 0$ and ϕ is injective.

Prop.: Let $\mathbb{K}$ be a field. a polynomial $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $a_i \in \mathbb{K}$, has at most n roots.

(proof by induction in n)

$(\mathbb{Z}/p)^\times$ – units in $\mathbb{Z}/p$ (p prime, everything $\neq 0$)

↳ group under multiplication

in fact, it is a cyclic group:

proof: as an abstract group,

$$(\mathbb{Z}/p)^\times \simeq \mathbb{Z}/q_1^{a_1} \times \mathbb{Z}/q_2^{a_2} \times \dots \times \mathbb{Z}/q_r^{a_r} \overset{\text{CRT}}{\simeq} \mathbb{Z}/\prod_i q_i^{a_i},$$

q_i primes (not a priori distinct), $a_i \geq 1$.

if $q_1 = q_2 \equiv q$ then there are at least q^2 elements of order q in $(\mathbb{Z}/p)^\times$, i.e. q^2 solutions to $x^q \equiv 1 \pmod p$

↳ contradiction ∎

$(\mathbb{Z}/p)^\times$ is a cyclic group of order $p-1$. any generator g is called a primitive root mod p.

$$(\mathbb{Z}/p)^\times = \{g, g^2, \dots, g^{p-1} = 1\}$$

suppose a is a solution of $x^2 \equiv -1 \pmod p$. then $a^2 \neq 1$ in $(\mathbb{Z}/p)^\times$ but $a^4 = 1$ in $(\mathbb{Z}/p)^\times$ $(p \neq 2)$

this means a has order 4 in $(\mathbb{Z}/p)^\times$. this happens iff $4 \mid p-1$.
($a = g^{p-1/4}$, g primitive root).

Theorem: (Chevalley – Warning):
let $F(x_1, \dots, x_s) \in \mathbb{Z}/p[x_1, \dots, x_s]$. if $s > \deg F$ then

$$p \mid \#\{\underline{a} = (a_1, \dots, a_s) \in \mathbb{Z}/p^s : F(\underline{a}) = 0\}$$

(p divides # of solns.)

Key lemma: let $r \geq 0$ be an integer. then:

$$\sum_{x \in \mathbb{Z}/p} x^r = \begin{cases} p-1 & \text{if } p-1 \mid r \\ 0 & \text{otherwise} \end{cases}$$

proof: let g be a primitive root in $(\mathbb{Z}/p)^\times$. then

$$\sum_{x \in \mathbb{Z}/p} x^r = \sum_{x \in (\mathbb{Z}/p)^\times} x^r = \sum_{i=0}^{p-2} g^{ir} \underset{\substack{\uparrow \\ p-1 \nmid r}}{=} \frac{g^{r(p-1)} - 1}{g^r - 1} = 0$$

$$\underset{\substack{\uparrow \\ p-1 \mid r}}{=} \sum_{i=0}^{p-2} 1 = p-1$$

proof of Theorem:

$$F(\underline{a})^{p-1} = \begin{cases} 0 & \text{if } F(\underline{a}) \equiv 0 \\ 1 & \text{if } F(\underline{a}) \not\equiv 0 \end{cases}$$

$$\sum_{\underline{a} \in (\mathbb{Z}/p)^s} 1 - F(\underline{a})^{p-1} \equiv \#\{\underline{a} \in (\mathbb{Z}/p)^s : F(\underline{a}) \equiv 0\}$$

$$\|$$

$$\sum_{\underline{a} \in \mathbb{Z}/p^s} G(\underline{a}) \quad , \quad G(x_1, \dots, x_s) = 1 - F(x_1, \dots, x_s)^{p-1}$$

$$\deg G = (p-1) \deg F$$

G is a sum of monomials of the form:

$I \subseteq \{1, \dots, s\}$

$$\prod_{i \in I} x_i^{d_i} \quad , \quad \sum_{i \in I} d_i \leq \deg G$$
$$\leq (p-1) \deg F$$
$$< (p-1) s$$

$$\sum_{\underline{a}} \prod_{i \in I} a_i^{d_i}$$

2 cases: $I = \{1, \dots, s\}$: some $d_i < p-1 \to$ key lemma

$I \neq \{1, \dots, s\}$: $\sum_{a \in \mathbb{Z}/p} 1 = p$.

Corollary: if the constant term of F is zero, then there's a solution $0 \neq \underline{a}$ to $F(\underline{x}) = 0$ ($s > \deg F$).

Proof: $F(\underline{0}) = 0$, but $p \geq 2$ and $p \mid \#$solns. hence $\#$solns ≥ 2.

Powers of p

$\mathbb{Z}/p^k$ ring, not field if $k > 1$ (p is not invertible)

$(\mathbb{Z}/p^k)^\times$ — residue classes of integers not divisible by p

$$\#(\mathbb{Z}/p^k)^\times = \varphi(p^k) = (p-1)p^{k-1}$$

if $F[x_1, \dots, x_s] \in \mathbb{Z}[x_1, \dots, x_s]$ then any $\underline{a} = (a_1, \dots, a_s) \in \mathbb{Z}^s$ s.t. $F(\underline{a}) = 0$ gives a solution $\underline{a}^{(k)} \in (\mathbb{Z}/p^k)^s$ to $F(\underline{x}) \equiv 0 \pmod{p^k}$

Note: $\underline{a}^{(k)} \equiv \underline{a}^{(k-1)} \pmod{p^{k-1}}$, since they are reductions of the same solution $\underline{a} \in \mathbb{Z}^s$.

Lemma (Hensel): Let $F(x) \in \mathbb{Z}[x]$. Suppose $a_0 \in \mathbb{Z}$ s.t. $F(a_0) \equiv 0 \pmod{p^{k-1}}$, then there's $a \in \mathbb{Z}$ s.t. $F(a) \equiv 0 \pmod{p^k}$ and $a \equiv a_0 \pmod{p^{k-1}}$, provided

$$F'(a_0) \not\equiv 0 \pmod{p} \quad (\text{i.e. } F'(a_0) \in (\mathbb{Z}/p^{k-1})^\times)$$

moreover, a is uniquely determined mod p^k and $F'(a) \equiv F'(a_0) \pmod{p}$

notice how the Lemma allows us to go from a solution mod p^{k-1} to a soln mod p^k to a soln mod p^{k+1} to ...

Proof: key observation:

$$(a_0 + p^{k-1}b)^n = a_0^n + n a_0^{n-1} p^{k-1} b + \underbrace{\sum_{i=2}^{n} \binom{n}{i} a_0^{n-i} (p^{k-1}b)^i}_{\substack{= \\ p^{2(k-1)} g_n(b), \\ g_n \in \mathbb{Z}[x]}}$$

This means

$$F(a_0 + p^{k-1}b) = F(a_0) + F'(a_0) p^{k-1} b + p^{2(k-1)} G(b),$$
$$G(x) \in \mathbb{Z}[x]$$

so,

$$F(a_0 + p^{k-1}b) \equiv F(a_0) + F'(a_0) p^{k-1} b \pmod{p^k}$$

since, by hypothesis, $p^{k-1} \mid F(a_0)$, we have

$$b \equiv - \frac{F(a_0)}{F'(a_0)} \frac{1}{p^{k-1}} \pmod p$$

inverse in $\mathbb{Z}/p$

then $a = a_0 + p^{k-1} b$ satisfies $F(a) \equiv 0 \pmod{p^k}$ and $a \equiv a_0 \pmod{p^{k-1}}$.

we can apply Hensel's Lemma to equations with more than one variable.

e.g. $x^2 + y^2 + 3 \equiv 0 \pmod{5^k}$

first solve mod 5: $(x,y) = (1,1)$. fix $y \equiv 1 \pmod 5$ and consider $x^2 + 1^2 + 3 \equiv 0 \pmod{5^k}$. Hensel's produces a solution to $x^2 + 4 \equiv 0 \pmod{5^k}$ s.t. $x_0 \equiv 1 \pmod 5$.

then $(x_0, 1)$ will be a solution to $x^2 + y^2 + 3 \equiv 0 \pmod{5^k}$.

Application: let $F(x_1, \dots, x_s) = a_1 x_1^n + \dots + a_n x_s^n$ s.t. $p \nmid a_i$, $s > n$. then there exists $\underline{c} = (c_1, \dots, c_s)$ s.t. $F(\underline{c}) \equiv 0 \ (p^k)$ and some c_i is not divisible by p.

Why?

Chevalley-Warning gives a soln. mod p:

$$0 \neq \underline{c}^{(0)} = (c_1^{(0)}, \dots, c_s^{(0)})$$

after optional relabeling, we can assume $c_1^{(0)} \not\equiv 0 \pmod p$. to apply Hensel's we need to know that $f'(c_1^{(0)}) \not\equiv 0 \ (p)$.

$$f'(x) = \underbrace{a_1 n}_{\text{not divisible by } p} x^{n-1}$$

what we have now is a way to go down the chain of $\mathbb{Z}/p^n$ by Hensel's lemma:

$$\begin{array}{ccccccccccc} \mathbb{Z}/p & \twoheadleftarrow & \mathbb{Z}/p^2 & \twoheadleftarrow & \mathbb{Z}/p^3 & \twoheadleftarrow & \cdots & \twoheadleftarrow & \mathbb{Z}/p^n & \twoheadleftarrow & \cdots \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \\ a_1 & \leftarrow\!\shortmid & a_2 & \leftarrow\!\shortmid & a_3 & \leftarrow\!\shortmid & \cdots & \leftarrow\!\shortmid & a_n & \leftarrow\!\shortmid & \cdots \end{array}$$

where all the a_i's are "compatible" in the sense that $a_k \equiv a_{k-1} \ (p^{k-1})$

P-adic numbers

we use the p-adic numbers to conveniently "package" this process:

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

$\hookrightarrow$ p-adic integers

e.g.: $p=2$: $(1, 3, 5, 7, 15, \dots, 2^n - 1, \dots) \in \mathbb{Z}_2$

Properties of $\mathbb{Z}_p$:

- $\mathbb{Z}_p$ is a ring

  $+$: add "coordinate-wise"

  $$(a_n) + (b_n) = (a_n + b_n)$$

  $\times$: multiply "coordinate-wise"

- there exists an injective ring homomorphism:

  $$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$$
  $$m \mapsto (a_n)$$

  $a_n = m \bmod p^n$ $\quad [(a_n) = (m)]$

  injective: $0 \in \mathbb{Z}_p$ is (0)

  $(m) = 0$ in $\mathbb{Z}_p \Leftrightarrow m = 0$ in $\mathbb{Z}/p^n$, $\forall n$
  $\Rightarrow m = 0$

- $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n$ $\leftarrow$ homomorphism of rings
  $(a_n) \mapsto a_n$

  surjective: $\mathbb{Z}/p^{r+n} \xrightarrow{\bmod p^n} \mathbb{Z}/p^n$ is always surjective

  the kernel of this map is $p^n \mathbb{Z}_p$

if we have a polynomial $F \in \mathbb{Z}[x]$, we can evaluate it on $x \in \mathbb{Z}_p$.
Suppose $(a_n) \in \mathbb{Z}_p$.

$$F((a_n)) = (F(a_n))$$

e.g.: $p = 2$, $F(x) = x^2 - 1$

$$\alpha = (1, 3, 7, 15, \dots) = -1$$
$$\alpha^2 = (1, 1, 1, 1, \dots) = 1$$
$$\downarrow$$
$$F(\alpha) = (0, 0, 0, \dots)$$

what are the units in $\mathbb{Z}_p$?

$$\mathbb{Z}_p^\times = \{(a_n) \in \mathbb{Z}_p : a_n \in (\mathbb{Z}/p^n)^\times\}$$

$(a_n b_n) = (a_n)(b_n) = 1 = (1)$ ← def. of unit

so $a_n b_n = 1$ in $\mathbb{Z}/p^n$.
let $b_n \in \mathbb{Z}/p^n$ be a solution of $a_n x \equiv 1 \ (p^n)$

$\downarrow$ unique soln. in $\mathbb{Z}/p^n$

we need to check that $b_{n+1} \equiv b_n \ (p^n)$ (exercise) ✓

every $0 \neq x \in \mathbb{Z}_p$ can be expressed uniquely as $x = p^k u$, $u \in \mathbb{Z}_p^\times$, $k \geq 0$.

Some x_{n_0} is not zero in $\mathbb{Z}/p^{n_0}$. So $x_n \neq 0$ in $\mathbb{Z}/p^n$, $\forall n \geq n_0$

x_{n_0} is the first non-zero x_n.

(if $x_{n_0+1} = 0$ then $x_{n_0} \equiv x_{n_0+1} \equiv 0 \ (p^{n_0})$)

each x_n, $n \geq n_0$, can be written as $x_n = p^{k_n} v_n$, $k_n \geq 0$ unique, $v_n \in (\mathbb{Z}/p^n)^\times$.

$k_n = k_{n_0}$ because $x_{n_0} \equiv x_n \ (p^{n_0})$

$x_n \in \mathbb{Z}/p^n$
$\Downarrow$

we define $u = (u_n) \in \mathbb{Z}_p^\times$ as

$p^{k_{n_0}}$ superdivides x_n

$$\left.\begin{array}{l} v_n \in \mathbb{Z}/p^{n-k_n} \\ u_n \in \mathbb{Z}/p^n \end{array}\right\} \quad u_n = \begin{cases} v_{n+k_0}, & n \geq n_0 \\ v_{n_0+k_0} \bmod p^n, & n < n_0 \end{cases}$$

$x_n = \phi$, no unit

$u_{n+1} \equiv u_n \pmod{p^n}$ true if $n < n_0$, $u_n \equiv v_{n_0+k_0} \pmod{p^n}$

$$\underset{\substack{\parallel \\ x_{n+1+k_0}}}{p^{k_0} v_{n+1+k_0}} \equiv \underset{\substack{\parallel \\ x_{n+k_0}}}{p^{k_0} v_{n+k_0}} \pmod{p^{n+k_0}}$$

$$\hookrightarrow v_{n+1+k_0} \equiv v_{n+k_0} \pmod{p^n}$$

$$p^{k_0} u = (\underset{\substack{\parallel \\ x_{n+k_0}}}{p^{k_0} v_{n+k_0}} \bmod p^n)$$

$$x_{n+k_0} \bmod p^n \equiv x_n$$

uniqueness of u:

$$x = p^k u = p^{k'} u', \quad u u' \in \mathbb{Z}_p^\times$$

suppose $k' > k$:

$$p^k u - p^{k'} u' = 0$$

$$= p^k \underbrace{(u - p^{k'-k} u')}_{w = (w_n)}$$

$$w_1 \equiv u_1 \ (p) \Rightarrow w_1 \in \mathbb{Z}_p^\times$$

so $0 = p^k \cdot$ unit, contradiction and $k = k'$.

$$p^k u_n \equiv p^k u_n' \mod p^n, \quad \forall n > k$$

$$\Downarrow$$

$$\begin{array}{ccc} u_n & \equiv & u_n' \\ \shortparallel & & \shortparallel \\ u_{n-k} & & u_{n-k}' \end{array} \quad \mod p^{n-k}$$

rewrite as $u_m \equiv u_m' \mod p^m$, $\forall m$, so $u = (u_n) = (u_n') = u'$.

$\mathbb{Z}_p$ is a domain:

$$p^k u \cdot p^{k'} u' = 0$$

$$= p^{k+k'} u u' = 0 \Rightarrow p^{k+k'} = 0$$ but this is impossible ($\mathbb{Z} \hookrightarrow \mathbb{Z}_p$)

the nonzero ideals of $\mathbb{Z}_p$ are the ideals $p^k \mathbb{Z}_p$, $k \geq 0$.

we can define the p-adic numbers, $\mathbb{Q}_p$:

$$\mathbb{Q}_p = \mathbb{Z}_p[1/p] = \{p^k u, \ u \in \mathbb{Z}_p^\times, \ k \in \mathbb{Z}\}$$

$\hookrightarrow$ <u>field</u>

let's reformulate Hensel's Lemma I:

Hensel's Lemma II:
Let $F \in \mathbb{Z}_p[x]$. Suppose $a_1 \in \mathbb{Z}_p$ s.t.

$$F(a_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$
$$F'(a_1) \in \mathbb{Z}_p^\times$$

then $\exists$ unique $a \in \mathbb{Z}_p$ s.t.

$$a \equiv a_1 \pmod p$$
$$F(a) = 0$$
$$F'(a) \equiv F'(a_1) \pmod p$$

Alternative construction

$R_1 = \{0, 1, 2, \dots, p-1\}$ complete set of representatives of residue classes mod p.

$R_n = \{ \sum_i^{n-1} r_i p^i : r_i \in R_1 \}$ " mod p^n

↳ representation base p.

using R_n, we construct $a \in \mathbb{Z}_p$, $a = (a_n)$ s.t. $a_n \in R_n$, obeying:

$$a_{n+1} = \sum_{i=0}^{n} r_i p^i \quad , \quad r_i \in R_i$$

$$\Downarrow$$

$$a_n = \sum_{i=0}^{n-1} r_i p^i \quad , \quad r_i \in R_i$$

just drop the p^n term

$$a \longrightarrow \sum_{i=0}^{\infty} r_i p^i \quad , \quad r_i \in R_i$$

we can now think of the p-adic integers as

$$\mathbb{Z}_p \longleftrightarrow \left\{ \sum_{i=0}^{\infty} r_i p^i \ : \ r_i \in R_i \right\}$$

(a_n) where $a_n = \sum_{i=0}^{n-1} r_i p^i$

this has obvious multiplication and addition (base p) $\Leftrightarrow$ those in $\mathbb{Z}_p$.

e.g. $p = 2$ $\quad -1 \in \mathbb{Z}_2$

$R_1 = \{0, 1\}$

$$-1 \longleftrightarrow 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + \dots + 1 \cdot 2^n + \dots$$

notice the sum of this series is indeed -1, which suggests a strong connection between the series and the number it represents.

we define a map $\mathrm{ord}_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{+\infty\}$ as:

$$\mathrm{ord}_p(x) = \begin{cases} +\infty, & \text{if } x = 0 \\ k, & \text{if } x = p^k u, \ u \in \mathbb{Z}_p^\times, \ k \in \mathbb{Z} \end{cases}$$

ord_p has similar properties to a logarithm:

- $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$
- $\mathrm{ord}_p(x) = 0 \Leftrightarrow x \in \mathbb{Z}_p^\times$
- $\mathrm{ord}_p(x^{-1}) = -\mathrm{ord}_p(x)$

therefore it's a homomorphism.

- $\mathrm{ord}_p(x) \geq n \Leftrightarrow x \in p^n \mathbb{Z}_p$, $n \geq 0$
- $\mathrm{ord}_p(x+y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$
  $=$ if $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$

using the order, we can define a multiplicative measure (useful for analysis):

$$|\cdot|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}_{\geq 0}$$
$$x \longmapsto p^{-\mathrm{ord}_p(x)} \qquad (|0|_p = 0)$$

p-adic absolute value

$$x = p^k u \Rightarrow |x|_p = p^{-k}$$

- $|x|_p = 0 \Leftrightarrow x = 0$
- $|xy|_p = |x|_p |y|_p$
- $|x+y|_p \leq p^{-\min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}} = \max\{|x|_p, |y|_p\}$

  this is stronger than the typical triangle inequality for norms.

Ostrowski's theorem:
if $f : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ s.t.

(i) $f(x) = 0 \Leftrightarrow x = 0$
(ii) $f(xy) = f(x) f(y)$
(iii) $f(x+y) \leq f(x) + f(y)$

then either:

(a) $f(x) = 1, \quad \forall x \neq 0$

(b) $f(x) = |x|^\alpha, \quad 0 < \alpha \leq 1$

(c) $f(x) = |x|_p^\beta, \quad 1 \leq \beta$

we can now replace the usual absolute value $|\cdot|$ with the p-adic absolute value $|\cdot|_p$ in order to get "p-adically convergent" series:

for $x, y \in \mathbb{Z}_p$, they are "p-adically close" if $|x-y|_p$ is "small":

$$|x-y|_p \leq p^{-m} \Leftrightarrow \mathrm{ord}_p(x-y) \geq m$$
$$\Leftrightarrow x-y \in p^m \mathbb{Z}_p \quad (p^m \mid x-y)$$

going back to the p-adic representation for -1 $(p=2)$:

$$\sigma_n = 1 + 2 + \dots + 2^n = \frac{2^{n+1}-1}{2-1} = 2^{n+1} - 1$$

$$|-1-\sigma_n|_2 = |2^{+n+1}|_2 = 2^{-n-1} \xrightarrow{n} 0$$

in general, we say a sequence $\{a_n\}$, $a_n \in \mathbb{Q}_p$ converges to a when

$$\forall \varepsilon > 0, \ \exists N_\varepsilon > 0 : |a - a_n|_p < \varepsilon \text{ if } n > N_\varepsilon$$

in addition, we define Cauchy sequences:

$\{a_n\}$ s.t. $\forall \varepsilon > 0, \ \exists N_\varepsilon > 0 : |a_n - a_m|_p < \varepsilon, \ \forall n, m > N_\varepsilon$

in $\mathbb{Q}_p$, every Cauchy sequence converges:

$a_n = p^{k_n} u_n$, $k_n \in \mathbb{Z}$, $u_n \in \mathbb{Z}_p^\times$

if k_n is unbounded: $\{a_n\} \to 0$ p-adically

bounded: $|p^{k_n} u_n - p^{k_m} u_m|_p < p^{-j}$, large j

$$\underset{\parallel}{} \quad |p|_p^{k_n} |u_n - p^{k_m - k_n} u_m|_p$$

$$\Downarrow$$

$$k_m = k_n$$

$$\Rightarrow \quad |u_n - u_m|_p < p^{k-j}$$

$$u_n \equiv u_m \quad (p^{k-j}), \quad \forall n,m \text{ large}$$

every element of $\mathbb{Q}_p$ is the limit of a Cauchy sequence of rational numbers:

$x \in \mathbb{Q}_p$, $\exists \{r_n\}$ conv. series s.t. $\{r_n\} \to x$, $r_k \in \mathbb{Q}$

$x = p^k u$, $u = \{u_n\}$, $u_n \in \mathbb{Z}/p^n$
$u_{n+1} \equiv u_n \quad (p^n)$

we can assume $u_n \equiv r_n \mod p^n$, $r_n \in R_n$. then $\{r_n\}$ is a sequence of rational numbers

$$r_n = \sum_{i=0}^{n-1} c_i p^i, \quad c_i \in R_1$$

$$|r_n - r_m|_p = \left|\sum_{i=n}^{m-1} c_i p^i\right|_p = |p^n|_p \cdot |c_n + c_{n+1} p + \dots + c_{m-1} p^{m-1-n}|_p \leq p^{-n}$$
$(n \leq m)$

$$u = \{u_n\} = \{r_n \mod p^n\}$$

$$u - r_m = \{r_n - r_m \mod p^n\}$$

$$\underset{\parallel}{} \quad 0 \text{ if } m \geq n \Rightarrow p^m \mid u - r_m$$

this means $|u - r_m|_p \leq p^{-m} \Rightarrow \{r_m\} \to u$.

$$\sum_{i=0}^{\infty} c_i p^i = u \quad \text{in } \mathbb{Q}_p$$

we denote by $\mathcal{C}_p$ as the set of p-adic Cauchy sequences $\{r_n\}$, $r_n \in \mathbb{Q}$ w.r.t. $|\cdot|_p$. this is a ring under mult. and addition of seqns.

$$\mathcal{C}_p \twoheadrightarrow \mathbb{Q}_p$$
$$\{r_n\} \longmapsto \text{its limit } (p\text{-adically})$$

the kernel is the set of Cauchy seqns. that converge to 0. thus:

$$\mathcal{C}_p / \mathcal{N}_p \simeq \mathbb{Q}_p$$