Hensel's Lemma

Question: can one "improve" a solution of $f(x) \equiv 0 \pmod{b^n}$ to ——" —— $f(x) \equiv 0 \pmod{b^{n+1}}$?

Notation: $b \in \mathbb{Z}$, $b \geq 2$, $n \geq 1$, $f \in \mathbb{Z}[X_1, \dots, X_N]$

$$Z_f(\mathbb{Z}/b^n\mathbb{Z}) = \{\text{solutions of } f(x_1,\dots,x_N) \equiv 0 \pmod{b^n}\} = \{x=(x_1,\dots,x_N) \in (\mathbb{Z}/b^n\mathbb{Z})^N,\ f(x)=0\}$$

$$\begin{array}{ccc} Z_f(\mathbb{Z}/b^{n+1}\mathbb{Z}) & \subset & (\mathbb{Z}/b^{n+1}\mathbb{Z})^N \\ \downarrow & & \downarrow \text{pr} \\ Z_f(\mathbb{Z}/b^n\mathbb{Z}) & \subset & (\mathbb{Z}/b^n\mathbb{Z})^N \end{array} \qquad \begin{array}{c} x \pmod{b^{n+1}} \\ \downarrow \\ x \pmod{b^n} \end{array} \qquad (*)$$

Questions: what is $\text{pr}^{-1}(x) = ?$, for $x \in Z_f(\mathbb{Z}/b^n\mathbb{Z})$? Is $\text{pr}^{-1}(x) \neq \emptyset$?

Ex: $b=p$ prime, $f = Y^2 - X^3 - p$ $\quad (X=X_1, Y=X_2)$

$f(0,0) \equiv 0 \pmod{p}$, there is no solution of $f(x,y) \equiv 0 \pmod{p^2}$ with $(x,y) \equiv (0,0) \pmod{p}$

$(\Rightarrow p \mid x,\ p \mid y \Rightarrow y^2 - x^3 - p \equiv -p \not\equiv 0 \pmod{p^2})$.

$\overline{f} = f \pmod{p} = Y^2 - X^3$, $\quad \frac{\partial \overline{f}}{\partial X}(0,0) = \frac{\partial \overline{f}}{\partial Y}(0,0) = 0 \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

$Y^2 - X^3 = 0$

$(0,0)$ singular point

So the singular point $(0,0) \in Z_f(\mathbb{Z}/p\mathbb{Z})$ cannot be lifted to a point of $Z_f(\mathbb{Z}/p^2\mathbb{Z})$.

Hensel's Lemma (1st version) — Non-singular points lift

In the situation of $(*)$, let $x=(x_1,\dots,x_N) \in \mathbb{Z}^N$ such that $x \pmod{b^n} \in Z_f(\mathbb{Z}/b^n\mathbb{Z})$.

Let $a_i = \frac{\partial f}{\partial X_i}(x_1,\dots,x_N) \in \mathbb{Z}$ $\quad (1 \leq i \leq N)$.

If $\exists\, i_0$ $\quad a_{i_0} \pmod{b} \in (\mathbb{Z}/b\mathbb{Z})^*$ $\Longrightarrow$ $\left|\text{pr}^{-1}(x \pmod{b^n})\right| = b^{N-1}$

Pf: Let $y=(y_1,\dots,y_N)$, $y_i = x_i + b^n t_i$, $t_i \in \mathbb{Z}$ (so $\text{pr}(\underbrace{y \pmod{b^{n+1}}}_{\text{depends only on } t \pmod{p}}) = x \pmod{b^n}$)

When is $f(y) \equiv 0 \pmod{b^{n+1}}$?

$$f(y) = \underbrace{\frac{f(x)}{b^n}}_{a,\ a \in \mathbb{Z}} + \sum_{i=1}^{N} a_i b^n t_i + \underbrace{(b^n t_i)^2 c}_{\equiv 0 \pmod{b^{n+1}}} \qquad c \in \mathbb{Z}$$

So $f(y) \equiv 0 \pmod{b^{n+1}} \iff \underbrace{\sum_{i=1}^{N} a_i t_i \equiv -a \pmod{b}}$

solutions: $t_i \pmod{b} \in \mathbb{Z}/b\mathbb{Z}$ arbitrary if $i \neq i_0$

$$t_{i_0} \pmod{b} = (a_{i_0} \pmod{b})^{-1} \left(-a - \sum_{i \neq i_0} a_i t_i \pmod{b}\right)$$

There are b possible values for each $t_i \pmod{b}$ $(i \neq i_0)$

$\Rightarrow$ b^{N-1} ——" —— $y \pmod{b^{n+1}}$.

Cor: If $N=1$ and $f'(x) \pmod{b} \in (\mathbb{Z}/b\mathbb{Z})^*$ $\Rightarrow$ $\text{pr}^{-1}(x)$ has 1 element

Hensel's lemma (1st version, one variable) $b \in \mathbb{Z}, b \geq 2, n \geq 1, f(X) \in \mathbb{Z}[X]$

If $x_n \in \mathbb{Z}$, $f(x_n) \equiv 0 \pmod{b^n}$, $f'(x_n) \pmod b \in (\mathbb{Z}/b\mathbb{Z})^\times$ $\Rightarrow$ $\exists\, x_{n+1} \in \mathbb{Z}$, $x_{n+1} \equiv x_n \pmod{b^n}$, $f(x_{n+1}) \equiv 0 \pmod{b^{n+1}}$

$x_{n+1} \pmod{b^{n+1}}$ is unique

Pf: If $x_{n+1} = x_n + b^n t$ $(t \in \mathbb{Z}) \Rightarrow f(x_{n+1}) = \underbrace{f(x_n)}_{b^n a} + \underbrace{f'(x_n)}_{a'} b^n t + \underbrace{(b^n t)^2 c}_{\equiv 0 \pmod{b^{n+1}}}$ $a, a', c \in \mathbb{Z}$, $p \nmid a'$

So $f(x_{n+1}) \equiv 0 \pmod{b^{n+1}} \iff 0 \equiv a + a't \pmod b \iff t \pmod b = -(a' \pmod b)^{-1} a \pmod b$

unique value in $\mathbb{Z}/b\mathbb{Z}$

Ex: $b = 10$, $f(X) = X^2 - X$, $x_1 = 5$ $\quad 5^2 = 25 \equiv 5 \pmod{10}$

$x_2 = 10t + 5$, $x_2^2 \equiv 25 \equiv 10t + 5 \pmod{10^2} \iff t \equiv 2 \pmod{10} \iff x_2 \equiv 25 \pmod{10^2}$

$x_3 = 100t + 25 \equiv x_3^2 \equiv 25^2 \equiv 625 \pmod{1000} \iff t \equiv 6 \pmod{10} \iff x_3 \equiv 625 \pmod{10^3}$

$x_4 = 1000t + 625 \equiv x_4^2 \equiv 625^2 \equiv 0625 \pmod{10^4}$ etc., $\boxed{x_n^2 \equiv x_n \pmod{10^n}}$

$y_n = 1 - x_n$ also satisfies $y_n^2 = 1 - 2x_n + x_n^2 \equiv 1 - x_n \equiv y_n \pmod{10^n}$

n	$x_n \pmod{10^n}$	$y_n \pmod{10^n}$
1	5	6
2	25	76
3	625	376
4	0625	9376

Morally, $x_n \equiv \alpha \pmod{b^n}$ is an <u>approximative equality</u>

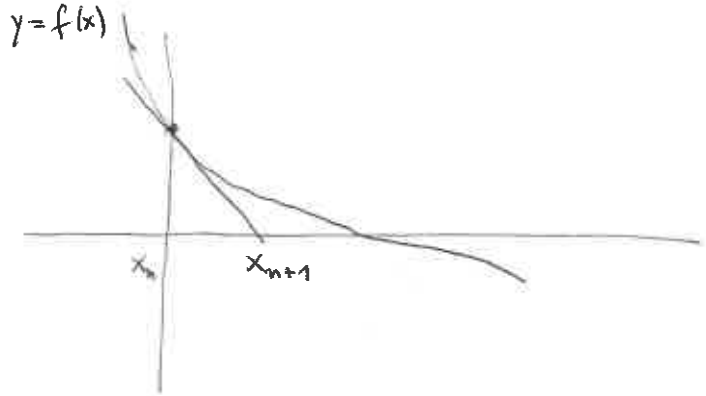
$x_{n+1} \equiv \alpha \pmod{b^{n+1}}$ is a <u>better approximation</u>

equality $x = \alpha$ is a congruence $x \equiv \alpha \pmod{b^\infty}$

Exercise: generalise to a system of congruences $f_1 \equiv \cdots \equiv f_M (x_1, \ldots, x_N) \equiv 0$

Hensel's lemma = Newton's method

In $\mathbb{R}$: ($N=1$)



approximative solution $f(x_n) \doteq 0$

$\rightsquigarrow$ better (?) approximation $x_{n+1} = x_n + t$

$$f(x_{n+1}) = \underbrace{f(x_n) + t f'(x_n)}_{0} + o(t^2) \iff t = -\frac{f(x_n)}{f'(x_n)} \qquad (\text{need } f'(x_n) \neq 0)$$

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Ex: $b = p$ prime, $m \geq 1$, $a \in \mathbb{Z}$, $x^m \equiv a \pmod{p^n}$, $f(X) = X^m - a$, $f'(X) = m X^{m-1}$

If $p \nmid am \Longrightarrow$ (Hensel) every solution of $x^m \equiv a \pmod{p^n}$ $(n \geq 1)$ lifts to a unique solution of $x^m \equiv a \pmod{p^{n+1}}$

Ex: $p \neq 2$ prime, $m = 2$, $a, b \in \mathbb{Z}$, $p \nmid ab$, $n \geq 1$:

(1) $\exists\, x \in \mathbb{Z}$ $x^2 \equiv a \pmod{p^n} \iff \exists\, x_1 \in \mathbb{Z}$ $x_1^2 \equiv a \pmod{p}$ $\left(\iff \left(\frac{a}{p}\right) = 1\right)$.

(2) $\forall\, n \geq 1$ $\exists\, x, y \in \mathbb{Z}$ $ax^2 + by^2 \equiv 1 \pmod{p^n}$

(we have proved this for $n=1 \overset{\text{Hensel}}{\Longrightarrow}$ every $n \geq 1$).

Exercise: $p > 5$ prime, $n \geq 1 \Rightarrow \exists$ solution of $3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod{p^n}$ with $\gcd(x, y, z, p) = 1$.

Question: what if $b = p$ prime, $\frac{\partial f}{\partial X_i}(a) \equiv 0 \pmod{p}$ for all i?

Ex: Can one lift $1^7 + 2^7 \equiv 3^7 \pmod{7^2}$ to a solution $\pmod{7^n}$, $n > 2$?

Hensel's Lemma (2^{nd} version) p = prime, $f \in \mathbb{Z}[X]$, $x_0 \in \mathbb{Z}$, $e \geq 0$

If $f(x_0) \equiv 0 \pmod{p^{2e+1}}$, $f'(x_0) \equiv 0 \pmod{p^e}$, $f'(x_0) \not\equiv 0 \pmod{p^{e+1}}$ ($e=0 \iff$ 1st version)

$\Rightarrow \forall n \geq 1 \ \exists x_n \in \mathbb{Z}$ $f(x_n) \equiv 0 \pmod{p^{2e+1+n}}$, $x_n \equiv x_{n-1} \pmod{p^{e+n}}$; $x_n \pmod{p^{e+n+1}}$ is unique

---

Pf: morally, "$x_n = x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})} \pmod{p^{e+n+1}}$"

Step 1: if $y \in \mathbb{Z}$, $y \equiv x_0 \pmod{p^{e+1}} \Rightarrow f'(y) \equiv f'(x_0) \pmod{p^{e+1}} \Rightarrow$ $f'(y) \equiv 0 \pmod{p^e}$, $f'(y) \not\equiv 0 \pmod{p^{e+1}}$

Step 2: assume $x_0, \dots, x_{n-1}$ exist. Then $f'(x_{n-1}) \equiv 0 \pmod{p^e}$, $\not\equiv 0 \pmod{p^{e+1}}$ (by Step 1)

Let $x_n = x_{n-1} + p^{e+n}t$, $t \in \mathbb{Z}$

$f(x_n) = \underbrace{f(x_{n-1})}_{p^{2e+n}a,\ a \in \mathbb{Z}} + p^{e+n}t\,\underbrace{f'(x_{n-1})}_{p^e a',\ a' \in \mathbb{Z},\ p \nmid a'} + \underbrace{(p^{e+n}t)^2 c}_{\equiv 0 \pmod{p^{2e+1+n}}}$ $c \in \mathbb{Z}$

So $f(x_n) \equiv p^{2e+n}(a + a't) \pmod{p^{2e+1+n}}$, hence

$f(x_n) \equiv 0 \pmod{p^{2e+1+n}} \iff a + a't \equiv 0 \pmod{p} \iff t \equiv -(a' \pmod{p})^{-1} a \pmod{p}$.

unique $t \in \mathbb{Z}/p\mathbb{Z}$

Ex: $p=2$, $a \in \mathbb{Z}$, $2 \nmid a$, $f(X) = X^2 - a$, $f'(X) = 2X$, $e=1$

$\exists x \in \mathbb{Z}$ $x^2 \equiv a \pmod{8}$ $\iff \forall n \geq 4 \ \exists x_n \in \mathbb{Z}$ $x_n^2 \equiv a \pmod{2^n}$

$\iff a \equiv 1 \pmod{8}$ there is unique such x_n satisfying $x_n \equiv x_1 \pmod{2^2}$ ($e+1=2$)

Ex: $p=3$, $a \in \mathbb{Z}$, $3 \nmid a$, $f(X) = X^3 - a$, $f'(X) = 3X^2$, $e=1$

$\forall n \geq 3 \ \exists x_n \in \mathbb{Z}$ $x_n^3 \equiv a \pmod{3^n} \iff \exists x \in \mathbb{Z}$ $x^3 \equiv a \pmod{3^3}$

$\Updownarrow$

$a \equiv \pm 1 \pmod{9} \iff a \equiv (\pm 1)^3, (\pm 2)^3, (\pm 4)^3 \equiv \pm 1, \pm 10, \pm 19 \pmod{3^3}$

Exercise: $p \neq 2$ prime, $a \in \mathbb{Z}$, $p \nmid a$

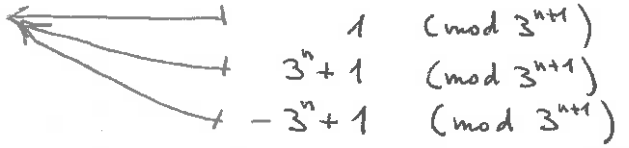
$\forall n \geq 3 \ \exists x_n \in \mathbb{Z}$ $x_n^p \equiv a \pmod{p^n} \iff \exists x \in \mathbb{Z}$ $x^p \equiv 1 \pmod{p^2}$

Cor: $\forall n \geq 3 \ \exists z_n \in \mathbb{Z}$, $z_n \equiv 3 \pmod{7}$

$1^7 + 2^7 \equiv z_n^7 \pmod{7^n}$

Ex: $(n \geq 2)$

$\{x \pmod{3^n} \mid x^3 \equiv 1 \pmod{3^n}\} \xleftarrow{pr} \{x \pmod{3^{n+1}} \mid x^3 \equiv 1 \pmod{3^{n+1}}\}$



Exercise: $\forall$ prime p $\forall n \geq 1$ $3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod{p^n}$ has a solution with $\gcd(x, y, z, p) = 1$.

Taking $\lim_{n\to\infty}$ $\mathbb{Z}/b^n\mathbb{Z}$

Ex: $x_n^2 \equiv x_n \pmod{10^n}$, $y_n = 1 - x_n \equiv y_n^2 \pmod{10^n}$

n	$x_n \pmod{10^n}$	$y_n \pmod{10^n}$
1	5	6
2	25	76
3	625	376
4	0625	9376

The table continues. In the limit we obtain two numbers with infinitely many digits:

$x = \cdots 0625 = x^2$

$y = \cdots 9376 = y^2$

$x+y = \cdots 0001 = 1$

$xy = x(1-x) = x - x^2 = 0$

Where do x, y live? They are 10-adic integers, $x, y \in \mathbb{Z}_{10}$

1st definition: $\mathbb{Z}_{10} = \left\{ \cdots a_2 a_1 a_0 = \sum_{i=0}^{\infty} a_i 10^i \;\middle|\; a_i \in \{0,1,\dots,9\} \right\}$ 10-adic integers

$\cap$

$\mathbb{Q}_{10} = \left\{ \cdots a_2 a_1 a_0, a_{-1} \cdots a_{-m} = \sum_{i=-m}^{\infty} a_i 10^i \;\middle|\; a_i \in \{0,1,\dots,9\},\ m \geq 0 \right\}$ 10-adic numbers

these are (commutative) rings, with obvious operations.

Ex: $z = \cdots 1111 = \sum_{i=0}^{\infty} 10^i \in \mathbb{Z}_{10}$

$9z = \cdots 9999$

$1 = \cdots 0001$

$9z+1 = \cdots 0000 = 0$

$\Rightarrow z = -\frac{1}{9} = \frac{1}{1-10}$

"10^5 is small in $\mathbb{Z}_{10}$"

"10^{10} is even smaller"

Two elements of $\mathbb{Q}_{10}$ are close to each other if they have a long common tail:

$x = \cdots 9712133$

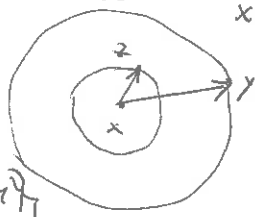
$y = \cdots 5412133$

$z = \cdots 5712133$

$\Rightarrow x - y = \cdots 4300000$ divisible by 10^5 ($x \equiv y \pmod{10^5}$)

$x - z = \cdots 4000000$ — " — 10^6 ($x \not\equiv y \pmod{10^6}$, $x \equiv z \pmod{10^6}$)

z is closer to x than y is



1st Def: $\{b\text{-adic numbers}\} = \mathbb{Q}_b \supset \mathbb{Z}_b = \{b\text{-adic integers}\}$

$b \in \mathbb{Z}$, $b \geq 2$

$\left\{ \sum_{i=-m}^{\infty} a_i b^i \;\middle|\; a_i \in \{0,1,\dots,b-1\},\ m \geq 0 \right\} = \left\{ \sum_{i=0}^{\infty} a_i b^i \;\middle|\; a_i \in \{0,1,\dots,b-1\} \right\}$

$\mathbb{Q}_b = \bigcup_{m \geq 0} b^{-m} \mathbb{Z}_b$

b^5 is small in $\mathbb{Z}_b$

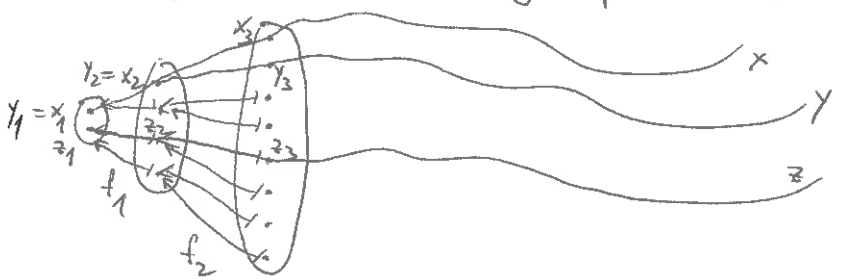
2nd Def: $\mathbb{Z}_b = \varprojlim_n \mathbb{Z}/b^n\mathbb{Z}$ the projective limit

Def: Given sets $A_1, A_2, A_3, \dots$ and maps $A_n \xleftarrow{f_n} A_{n+1}$ (a "projective system of sets"), its projective limit is $A = \varprojlim_n A_n = \{ x = (x_n)_{n \geq 1} \mid \forall n \geq 1,\ x_n \in A_n,\ f_n(x_{n+1}) = x_n \}$ compatible systems of elements

If each A_n is a ring and f_n is a ring morphism $\Rightarrow A$ is a ring: $(x_n) + (y_n) = (x_n + y_n)$

$(x_n)(y_n) = (x_n y_n)$

$0 = (0)$, $1 = (1)$



Ex: $\mathbb{Z}_b = \varprojlim_n \mathbb{Z}/b^n\mathbb{Z} = \{x=(x_n)_{n\geq 1} \mid x_n \in \mathbb{Z}/b^n\mathbb{Z},\ x_{n+1} \equiv x_n \pmod{b^n}\ \forall n\geq 1\}$

$$\sum_{i=0}^{\infty} a_i b^i \longmapsto x=(x_n)_{n\geq 1}, \quad x_n = \sum_{i=0}^{n-1} a_i b^i \pmod{b^n}$$

Basic properties: (0) $\mathbb{Z}_{100} = \varprojlim_n \underbrace{\mathbb{Z}/10^{2n}\mathbb{Z}}_{A_{2n}} = \varprojlim_n \underbrace{\mathbb{Z}/10^n\mathbb{Z}}_{A_n} = \mathbb{Z}_{10}$ (and $\mathbb{Z}_{b^m} = \mathbb{Z}_b$, $\forall m\geq 1$)

(if $x = (\cdots \xleftarrow{f_{2n}\circ f_{2n+1}} x_{2n} \xleftarrow{} x_{2n+2} \cdots) \in \varprojlim_n A_{2n}$, take $x_{2n+1} = f_{2n+1}(x_{2n+2}) \Rightarrow (x_n) \in \varprojlim A_n$)

---

(1) $(j\geq 1)$ $x = \sum_{i=0}^{\infty} a_i b^i \in \mathbb{Z}_b$ satisfies $x \in b^j\mathbb{Z}_b \iff x = \cdots a_j \underbrace{0\cdots 0}_{j} \iff x \in \ker\left(\mathbb{Z}_b \xrightarrow{pr_j} \mathbb{Z}/b^j\mathbb{Z}\right)$, $(x_n) \longmapsto x_j$

So $\overline{pr_j}: \mathbb{Z}_b/b^j\mathbb{Z}_b \xrightarrow{\sim} \mathbb{Z}/b^j\mathbb{Z}$

Def: $x,y \in \mathbb{Z}_b$ $\quad x \equiv y \pmod{b^j} \iff x-y \in b^j\mathbb{Z}_b$ ($\iff x,y$ have the same last j digits)

---

(2) $x=(x_n)_{n\geq 1} \in \mathbb{Z}_b$ satisfies: $x \in \mathbb{Z}_b^* \iff \exists y=(y_n)\in\mathbb{Z}_b$ $xy=1$ $\iff x_n y_n = 1 \in \mathbb{Z}/b^n\mathbb{Z}$

$\sum_{i=0}^{\infty} a_i b^i$ $\quad a_0 \pmod b = pr_1(x) = x_1 \in (\mathbb{Z}/b\mathbb{Z})^* \iff \forall n\geq 1 \quad x_n \in (\mathbb{Z}/b^n\mathbb{Z})^*$

Special case: if $b=p$ prime, $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, so $x \in \mathbb{Z}_p^* \iff a_0 \neq 0 \iff x \notin p\mathbb{Z}_p$

(3) **the chinese remainder thm:** If $b = \prod_i p_i^{r_i}$, p_i distinct primes, $r_i \geq 1$

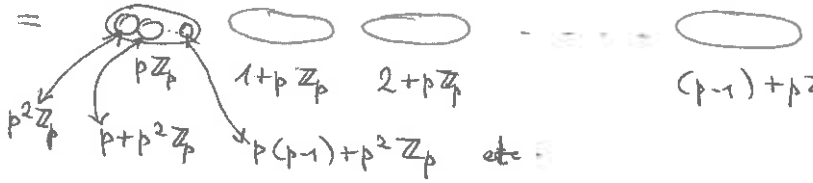
$$\mathbb{Z}/10^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/5^n\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$$
$$x_n \longmapsto (0,1), \quad y_n \longmapsto (1,0) \Rightarrow \mathbb{Z}_{10} \xrightarrow{\sim} \mathbb{Z}_5 \times \mathbb{Z}_2, \quad x \longmapsto (0,1), \ y \longmapsto (1,0)$$

$\Downarrow$

$$\mathbb{Z}_b \xrightarrow{\sim} \prod_i \mathbb{Z}_{p_i^{r_i}} = \prod_i \mathbb{Z}_{p_i}$$

$\{p\text{-adic numbers}\} = \mathbb{Q}_p \supset \mathbb{Z}_p = \{p\text{-adic integers}\}$ (p = prime)

Recall: $\mathbb{Z}_p = \{\underbrace{\cdots a_2 a_1 a_0}_{\sum_{i\geq 0} a_i p^i} \mid a_i \in \{0,1,\dots,p-1\}\} \supset \mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{\cdots a_2 a_1 a_0 \mid a_0 \neq 0\}$

$\mathbb{Z}_p =$ 

disjoint union

$\forall n\geq 1$ $\quad \mathbb{Z}_p = \coprod_{u=0}^{p^n-1} (u + p^n\mathbb{Z}_p)$, $\quad u+p^n\mathbb{Z}_p = \{x\in\mathbb{Z}_p \mid x \equiv u \pmod{p^n}\}$

p-adic valuation: if $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ and $x\neq 0$, let $v(x) = v_p(x) = \min\{n\geq 0 \mid a_n \neq 0\}$

$v(0) := +\infty$

$v(x) \geq n \iff x = \cdots \underbrace{0\cdots 0}_{n} \in p^n\mathbb{Z}_p$

$v(x) = n \iff x \in p^n\mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p = p^n\mathbb{Z}_p^*$

$v(x-y) \geq n \iff x \equiv y \pmod{p^n}$

Properties of $v: \mathbb{Z}_p \longrightarrow \mathbb{N} \cup \{+\infty\}$

(1) $x, y \in \mathbb{Z}_p \setminus \{0\}$, $x = p^m u$, $y = p^n u'$, $u, u' \in \mathbb{Z}_p^*$ $(\Rightarrow \underline{m = v(x),\ n = v(y)})$

$\Rightarrow xy = p^{m+n} uu' \Rightarrow \underline{v(xy) = v(x) + v(y)}$ $(\neq 0)$ $(\Rightarrow \mathbb{Z}_p$ is an integral domain$)$

(2) If $m \le n \Rightarrow x + y = p^m (u + p^{n-m} u') \Rightarrow \underline{v(x+y) \ge m = \min(v(x), v(y))}$

(2') If $\underline{m < n} \Rightarrow x + y = p^m (u + p^{n-m} u') \in p^m (\mathbb{Z}_p \setminus p\mathbb{Z}_p) = p^m \mathbb{Z}_p^* \Rightarrow v(x+y) = m = \min(v(x), v(y))$

$\mathbb{Q}_p = \bigcup_{m \ge 0} p^{-m} \mathbb{Z}_p = \left\{ \frac{x}{y} \mid x, y \in \mathbb{Z}_p,\ y \neq 0 \right\}$ $\quad y = p^m u,\ u \in \mathbb{Z}_p^* \Rightarrow \frac{x}{y} = \frac{x u^{-1}}{p^m},\ u^{-1} \in \mathbb{Z}_p$

$\mathbb{Q}_p$ is a field (= the field of fractions of $\mathbb{Z}_p$): if $x \neq 0 \Rightarrow \left(\frac{x}{y}\right)^{-1} = \frac{y}{x}$. So $\mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$.

Def: $v: \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{+\infty\}$, $v\left(\frac{x}{y}\right) = v(x) - v(y)$ (well-defined, by (1))

Prop: $v: \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{+\infty\}$ is surjective,

(0) $v(x) = +\infty \iff x = 0$

(1) $v(xy) = v(x) + v(y)$

(2) $v(x+y) \ge \min(v(x), v(y))$ $(\Rightarrow$ equality if $v(x) \neq v(y))$

} "v is a discrete valuation of the field $\mathbb{Q}_p$"

Note: (a) $v(x) = n \iff x \in p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p = p^n \mathbb{Z}_p^*$ $(n \in \mathbb{Z})$

(b) $x, y \in \mathbb{Q}_p$ are close to each other if $v(x-y) \gg 0$

(c) $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v(x) \ge 0\}$

$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v(x) > 0\}$

Prop: If $x_1, \dots, x_n \in \mathbb{Q}_p^*$ $(n \ge 2)$, $v(x_1) \le v(x_2) \le \dots \le v(x_n)$, $x_1 + \dots + x_n = 0 \Rightarrow \underline{v(x_1) = v(x_2)}$

If: If $v(x_1) < v(x_2) \Rightarrow -x_1 = x_2 + \dots + x_n \in p^{v(x_2)} \mathbb{Z}_p \subset p^{v(x_1)+1} \mathbb{Z}_p$ – contradiction.

Norm, distance on $\mathbb{Q}_p$

Def. For $x, y \in \mathbb{Q}_p$ let $\|x\| = \|x\|_p = \begin{cases} 0 & x = 0 \\ \frac{1}{p^{v(x)}} & x \neq 0 \end{cases}$ $\left(\|p^n u\| = \frac{1}{p^n},\ u \in \mathbb{Z}_p^* \right)$

$d(x, y) = \|x - y\|$ = distance between x, y $\quad \|\cdot\|: \mathbb{Q}_p \longrightarrow \mathbb{R}_{\ge 0}$

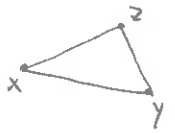
Properties: (0) $\|x\| = 0 \iff x = 0$

(1) $\|xy\| = \|x\| \cdot \|y\|$

(2) $\|x+y\| \le \max(\|x\|, \|y\|)$

$(\Rightarrow$ equality if $\|x\| \neq \|y\|)$

$d(x, y) \ge 0$, $d(x, y) = 0 \iff x = y$



$d(x, z) \le \max(d(x, y), d(y, z))$

(equality if $d(x, y) \neq d(y, z)$)

$d(x, y) \le \frac{1}{p^n} \iff x - y \in p^n \mathbb{Z}_p \iff x \equiv y \pmod{p^n}$

Note: (a) $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \|x\| \le 1\}$, $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \|x\| < 1\}$

(b) $\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b \right\}$ is a subring of $\mathbb{Z}_p$: $\forall n \ge 1\ \exists\ c_n$ $bc_n \equiv 1 \pmod{p^n}$

$\Rightarrow c = (c_n) \in \mathbb{Z}_p$, $bc = 1 \Rightarrow \frac{a}{b} = ac \in \mathbb{Z}_p$

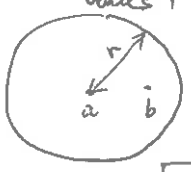
$\Rightarrow \mathbb{Q} = \bigcup_{m \ge 0} p^{-m} \mathbb{Z}_{(p)}$ is a subfield of $\mathbb{Q}_p$

and $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.

---

p-adic discs (balls): $r \in \mathbb{R}_{>0}$, $a \in \mathbb{Q}_p$ $\quad D(a, r] = \{x \in \mathbb{Q}_p \mid \|x - a\| \le r\}$

$D(a, <r] = \{x \in \mathbb{Q}_p \mid \|x - a\| < r\}$



Every point is a centre: $b \in D(a, r] \Rightarrow D(a, r] = D(b, r]$

$b \in D(a, <r] \Rightarrow D(a, <r] = D(b, <r]$

$\boxed{a + p^n \mathbb{Z}_p = D\left(a, \frac{1}{p^n}\right)}$

Convergence in $\mathbb{Q}_p$

Recall: (a) $U \subset \mathbb{Q}_p$ is *open* if $\forall a \in U \ \exists\ D(a, <r) \subset U$

(b) $V \subset \mathbb{Q}_p$ is *closed* if $\mathbb{Q}_p \setminus V$ is open

Note: each $a + p^n \mathbb{Z}_p = D(a, \frac{1}{p^n})$ is *open and closed*.

(c) $X \subset \mathbb{Q}_p$, $f: X \longrightarrow Y$ (Y = topological or metric space) is *continuous* if f^{-1}(open subset of Y) = $X \cap$ (open subset of $\mathbb{Q}_p$).

Ex: (1) $\|\cdot\|: \mathbb{Q}_p \longrightarrow \mathbb{R}_{\geq 0}$ is continuous

(2) $\mathbb{Q}_p \times \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$, $x, y \longmapsto x \pm y$; $x, y \longmapsto xy$; $\mathbb{Q}_p^* \longrightarrow \mathbb{Q}_p^*$, $x \longmapsto \frac{1}{x}$ are continuous ($\mathbb{Q}_p$ is a *topological field*)

$\Downarrow$

$\forall$ polynomials $g, h \in \mathbb{Q}_p[X_1, \dots, X_n] \setminus \{0\}$

$f = \frac{g}{h}$: $\underbrace{\{ a \in \mathbb{Q}_p^n \mid h(a) \neq 0 \}}_{\text{open subset of } \mathbb{Q}_p^n} \longrightarrow \mathbb{Q}_p$ is continuous

---

Def: (1) A sequence $\{a(n)\}$ in $\mathbb{Q}_p$ converges to $a \in \mathbb{Q}_p$ if $\lim_{n\to\infty} \|a(n) - a\| = 0$ in $\mathbb{R}$ ($\Rightarrow$ a is unique).

(2) $\{a(n)\}$ is a *Cauchy sequence* if $\forall \varepsilon > 0 \ \exists\, c(\varepsilon) \ \forall m, n > c(\varepsilon) \quad \|a(m) - a(n)\| < \varepsilon$

(3) $X \subset \mathbb{Q}_p$ is *dense* in $\mathbb{Q}_p$ if $\forall a \in \mathbb{Q}_p \ \forall \varepsilon > 0 \ \exists x \in X \quad \|x - a\| < \varepsilon$

Prop. (1) $\mathbb{Q}$ (resp. $\mathbb{Z}$) is dense in $\mathbb{Q}_p$ (resp. in $\mathbb{Z}_p$).

(2) Every Cauchy sequence $\{a(n)\}$ in $\mathbb{Q}_p$ converges ("$\mathbb{Q}_p$ is complete")

} $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ for $d(x,y) = \|x - y\|_p$

(3) Every sequence $A = \{a(n)\}$ in $\mathbb{Z}_p$ contains a convergent subsequence.

(4) A sequence $\{a(n)\}$ in $\mathbb{Q}_p$ converges $\Longleftrightarrow$ $\lim_{n\to\infty} \|a(n+1) - a(n)\| = 0$ in $\mathbb{R}$.

Cor. $\sum_{n=1}^{\infty} b(n)$ converges in $\mathbb{Q}_p \Longleftrightarrow \lim_{n\to\infty} \|b(n)\| = 0$ in $\mathbb{R}$.

Pf. (1) $\forall\ a = \sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}_p$ $\forall \varepsilon > 0$, let $n \gg 0$, $\frac{1}{p^n} < \varepsilon$, $x = \sum_{i=-m}^{n-1} a_i p^i \Rightarrow$ $x - a \in p^n \mathbb{Z}_p$, $\|x - a\| \leq \frac{1}{p^n} < \varepsilon$.

(2) For (big) $m_0 \gg 0$ the modified sequence $b(n) = a(n + m_0) - a(m_0)$ lies in $\mathbb{Z}_p$ and is Cauchy $\Rightarrow$

$\Rightarrow \forall j \geq 1 \ \exists\, n_j \ \forall n \geq n_j \quad pr_j(b(n)) = pr_j(b(n_j)) = c_j \in \mathbb{Z}/p^j\mathbb{Z}$

$b(n_{j+1}) \equiv b(n_j) \pmod{p^j} \Rightarrow$ $c = (c_j) \in \mathbb{Z}_p$ and $c = \lim_{n\to\infty} b(n)$.

(3) $\forall j \geq 1 \ \exists\, d_j \in \mathbb{Z}/p^j\mathbb{Z}$ ($\uparrow pr_j$, $\mathbb{Z}_p$) $\quad \underbrace{|pr_j^{-1}(d_j) \cap A|}_{A_j} = \infty$. We can choose inductively $d_1, d_2, \dots$ so that, in addition, $d_{j+1} \equiv d_j \pmod{p^j}$.

Then $d = (d_j) \in \mathbb{Z}_p$ and $A_1 \supset A_2 \supset A_3 \supset \dots$. Choose any $a'(j) \in A_j$. Then $\{a'(n)\} \subset A$ and $\forall m \geq n \ pr_n(a'(m)) = d_n \Rightarrow \lim_{n\to\infty} a'(n) = d$.

(4) ($\Rightarrow$) If $a(n) \longrightarrow a$, then $\|a(n) - a\| < \frac{\varepsilon}{2}$ for $n > c(\varepsilon) \Rightarrow \|a(n+1) - a(n)\| \leq \max(\|a(n+1) - a\|, \|a(n) - a\|) < \varepsilon$

($\Leftarrow$) $\forall \varepsilon > 0 \ \exists\, c'(\varepsilon) \ \forall n > c'(\varepsilon) \quad \|a(n+1) - a(n)\| < \varepsilon$. If $m > n > c'(\varepsilon) \Rightarrow \|a(m) - a(n)\| \leq \max_{n \leq k < m} \|a(k+1) - a(k)\| < \varepsilon$

$\Rightarrow \{a(n)\}$ is a Cauchy sequence $\overset{(2)}{\Longrightarrow}$ $a(n)$ converges.

Exercise: $\mathbb{Z}_p$ is compact (every open covering has a finite subcovering)

($\Rightarrow$ $a + p^n \mathbb{Z}_p$ is compact).

Prop. Let $f \in \mathbb{Z}_p[X]$. It is equivalent:

$\exists x \in \mathbb{Z}_p \quad f(x)=0 \iff \forall n \geq 1 \quad \exists a(n) \in \mathbb{Z}_p \quad f(a(n)) \equiv 0 \pmod{p^n}$.

Pf: $\Rightarrow$ take $a(n)=x$ | $\Leftarrow$ $\|f(a(n))\| \leq \frac{1}{p^n} \Rightarrow \lim_{n\to\infty} \|f(a(n))\| = 0$.

$\exists$ convergent subsequence $\{a'(n)\} \subset \{a(n)\}$ $\quad a'(n) \longrightarrow x \in \mathbb{Z}_p$. Then $\lim_{n\to\infty} \|f(a'(n))\| = \|f(x)\|$ ($\to 0$, $f(x)=0$).

Rmks. (1) Idem for several polynomials in several variables.

(2) In fact, we only require $f: \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ to be a continuous function.

Hensel's lemma (3^{rd} version) Let $f \in \mathbb{Z}_p[X]$, $x_0 \in \mathbb{Z}_p$, $\|f(x_0)\| < \|f'(x_0)\|^2$.

Then $\exists$ unique $x \in \mathbb{Z}_p$ such that $f(x)=0$, $\|x-x_0\| < \|f'(x_0)\|$.

Rks: (1) This also works if $f(X)=\sum_{n=0}^{\infty} a_n X^n$, $a_n \in \mathbb{Z}_p$, $\lim_{n\to\infty} \|a_n\| = 0$.

(2) Explicitly: $r(f'(x_0)) = e \in \mathbb{Z}$, $e \geq 0$, $f'(x_0) \equiv 0 \pmod{p^e}$, $f'(x_0) \not\equiv 0 \pmod{p^{e+1}}$, $f(x_0) \equiv 0 \pmod{p^{2e+1}}$

$\Rightarrow \exists!\, x \in \mathbb{Z}_p \quad f(x)=0, \quad x \equiv x_0 \pmod{p^{e+1}}$.

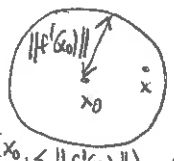
Ex: $p=2$, $a \in \mathbb{Z}_2^*$, $f(X)=X^2-a$, $f'(X)=2X$, $e=1$

- If $\exists x_0 \in \mathbb{Z}_2$, $f(x_0) \equiv 0 \pmod{2^3} \Rightarrow 2 \nmid x_0 \Rightarrow a \equiv x_0^2 \equiv 1 \pmod 8$.
- If $a \equiv 1 \pmod 8$ and $f(x_0)=x_0^2-a \equiv 0 \pmod 8 \Rightarrow f'(x_0)=2x_0 \equiv 0 \pmod 2$, $\not\equiv 0 \pmod 4$

$\overset{\text{Hensel}}{\Longrightarrow} \exists!\, x \in \mathbb{Z}_2$, $x^2=a$, $x \equiv x_0 \pmod 4$.

Cor: $\mathbb{Z}_2^{*2} = 1+8\mathbb{Z}_2 = \operatorname{Ker}(pr_3: \mathbb{Z}_2^* \longrightarrow (\mathbb{Z}/8\mathbb{Z})^*) \Rightarrow \overline{pr_3}: \mathbb{Z}_2^*/\mathbb{Z}_2^{*2} \xrightarrow{\sim} (\mathbb{Z}/8\mathbb{Z})^* = \{\bar 1, \bar 5, \overline{-1}, \overline{-5}\}$

Pf.



$D(x_0, <\|f'(x_0)\|)$

(1) If $\|x-x_0\| < \|f'(x_0)\|$ $(\leq 1) \Rightarrow \|x\| \leq \max(\|x_0\|, \|x-x_0\|) \leq 1 \Rightarrow x \in \mathbb{Z}_p$

Taylor expansion: $f'(x) = f'(x_0) + (x-x_0)a$, $\quad a \in \mathbb{Z}_p \Rightarrow \|a\| \leq 1$

$\|(x-x_0)a\| \leq \|x-x_0\| < \|f'(x_0)\| \Rightarrow \|f'(x)\| = \max(\|f'(x_0)\|, \|(x-x_0)a\|) = \|f'(x_0)\|$

(2) Uniqueness of x: let $\|x-x_0\|, \|y-x_0\| < \|f'(x_0)\|$, $f(x)=f(y)$

Taylor expansion: $0 = f(y)-f(x) = f'(x)(y-x) + b(y-x)^2$, $b \in \mathbb{Z}_p \Rightarrow \|b\| \leq 1$

If $x \neq y \Rightarrow f'(x) = b(x-y) \Rightarrow \|f'(x)\| \leq \|x-y\| \leq \max(\|x-x_0\|, \|y-x_0\|) < \|f'(x_0)\| \overset{(1)}{=} \|f'(x)\|$

contradiction $\Rightarrow x=y$.

(3) Existence of x: Newton's method $\quad 0 < r = \|f(x_0)\| / \|f'(x_0)\|^2 < 1$

(assume $f(x_0) \neq 0$) Define $\forall n \geq 0 \quad x_{n+1} = x_n + t_n$, $\quad t_n = -\frac{f(x_n)}{f'(x_n)}$

Properties: (A_n) $\|f'(x_n)\| = \|f'(x_0)\|$

(B_n) $\|f(x_n)\| / \|f'(x_0)\| \leq r^{2^n} \|f'(x_0)\|$

(C_n) $\|x_n - x_0\| < \|f'(x_0)\|$

Induction: $n=0$ ok.

$(A_n)+(B_n) \Rightarrow \|t_n\| \leq r^{2^n} \|f'(x_0)\| < \|f'(x_0)\| \Rightarrow \|x_{n+1}-x_0\| \leq \max(\|t_n\|, \|x_n-x_0\|) < \|f'(x_0)\|$ (C_{n+1})

$(C_{n+1}) \overset{(1)}{\Longrightarrow} (A_{n+1})$

Taylor expansion: $f(x_{n+1}) = \underbrace{f(x_n) + t_n f'(x_n)}_{0} + c t_n^2$, $\quad c \in \mathbb{Z}_p \Rightarrow \|c\| \leq 1$

$\Rightarrow \|f(x_{n+1})\| / \|f'(x_0)\| \leq \|f(x_n)\|^2 / \|f'(x_0)\| \overset{(B_n)}{\leq} r^{2^{n+1}} \|f'(x_0)\|$ (B_{n+1})

So $\lim_{n\to\infty} \underbrace{\|x_{n+1}-x_n\|}_{\|t_n\|} = 0 \Rightarrow x = \lim_{n\to\infty} x_n \in \mathbb{Z}_p$ exists, $\|f(x)\| = \lim_{n\to\infty} \|f(x_n)\| = 0$

$\Rightarrow f(x)=0$.

Analogies

Arithmetic		Geometry
$\mathbb{Z}$	ring	$\mathbb{C}[X]$ regular functions on a complex (affine) line
$\mathbb{Z}^* = \{\pm 1\}$	units	$\mathbb{C}[X]^* = \mathbb{C}^*$
$\mathbb{Q} = \left\{ f = \frac{a}{b} \mid \substack{a,b \in \mathbb{Z} \\ b \neq 0} \right\}$	field	$\mathbb{C}(X) = \left\{ f = \frac{g}{h} \mid \substack{g,h \in \mathbb{C}[X] \\ h \neq 0} \right\}$ rational functions — " —
p = prime	normalised irreducible elements	$X - a$ $(a \in \mathbb{C})$ local coordinate at a
$0 \neq f = \pm \prod_p p^{v_p(f)}$	unique factorisation	$0 \neq f = c \prod_{a \in \mathbb{C}} (X-a)^{v_a(f)}$, $c \in \mathbb{C}^*$
$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\pm\infty\}$	discrete valuations	$v_a : \mathbb{C}(X) \longrightarrow \mathbb{Z} \cup \{+\infty\}$ $v_a(f)$ = order of zero of f at a
$v_p^{-1}(\mathbb{N} \cup \{+\infty\})$ = $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid p \nmid b \right\}$	valuation rings	$v_a^{-1}(\mathbb{N} \cup \{+\infty\})$ = $\mathbb{C}[X]_{(X-a)} = \left\{ \frac{g}{h} \mid h(a) \neq 0 \right\}$ rational functions defined at a
$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$	completions	$\varprojlim_n \mathbb{C}[X]/(X-a)^n = \mathbb{C}[[X-a]] = \left\{ \sum_{j=0}^{\infty} c_j (X-a)^j \mid c_j \in \mathbb{C} \right\}$ formal power series $\mathbb{C}((X-a)) = \mathbb{C}[[X-a]]\left[\frac{1}{X-a}\right] = \left\{ \sum_{j=-m}^{\infty} c_j (X-a)^j \mid c_j \in \mathbb{C},\ m \geq 0 \right\}$
$\sum_p \overbrace{v_p(f)\log(p)}^{-\log \|f\|_p} = \log\lvert f \rvert$		$\sum_{a \in \mathbb{C}} v_a(f) = \deg(f)$ $(= \deg(g) - \deg(h))$
$\|f\|_\infty = \lvert f \rvert$	valuation at ∞	$v_\infty(f) = -\deg(f)$ $f = \left(\frac{1}{X}\right)^{v_\infty(f)} \cdot c \prod_{a \in \mathbb{C}} \left(1 - \frac{a}{X}\right)^{v_a(f)}$, $\frac{1}{X}$ local coordinate at ∞
$\|f\|_\infty \prod_p \|f\|_p = 1$	product/sum formula for valuations	$\sum_{a \in \mathbb{P}^1(\mathbb{C})} v_a(f) = 0$
	points	$a \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ projective line point at infinity
(2) (3) (5) (p) primes; (∞) infinite prime		usual points $a \in \mathbb{C}$; ∞
$\mathbb{Q}_\infty = \mathbb{R}$	completions at ∞	$\mathbb{C}[[\frac{1}{X}]] = \left\{ \sum_{j=0}^{\infty} c_j \left(\frac{1}{X}\right)^j \mid c_j \in \mathbb{C} \right\}$ $\cap$ $\mathbb{C}((\frac{1}{X})) = \left\{ \sum_{j=-m}^{\infty} c_j \left(\frac{1}{X}\right)^j \mid c_j \in \mathbb{C},\ m \geq 0 \right\}$

$\mathbb{Q}$ = global field

$\mathbb{Q}_p$, $\mathbb{R}$ = local fields (easier)