P-adic numbers & Hasse-Minkowski Theorem.

D. H. Seo, 2025. 6. 4 and 5.

References) ① J.P. serre
- A course in Arithmetic

② J.W.S. Cassels
— Local Fields

③ 2 Day clean, Siyun Kim

What you have to know) some basic concepts in mathematics.

Contents. 0. Introduction

1. P-adic number ⟶ Day1
2. Hilbert Symbol
3. Quadratic form and H-M thm. ⟶ Day2

Day 1.

0. Introduction.

Q. $f(x) = x^3 - 2x + 17$ in $\mathbb{Z}[x]$ has any solutions in $\mathbb{Z}$?

A. No!

Why?

Then...

Q. If $f(X) \in \mathbb{Z}[X]$ has a solution in all $\mathbb{Z}/p\mathbb{Z}$, f has a integer solution?

A. No! why?

I think most people who read this note can make a counterexample.

From the previous two questions, I can introduce two main questions of this note.

Q1. If we consider the field $\mathbb{Q}$ as the global object, then what are local ones?

Q2. As we have seen that in the case of $\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$, the existence of solutions is not local-global principle.

But, wouldn't L-G principle hold for certain kinds of objects?

1. p-adic Integer.

If you do not know what is a projective limit, consider it is just a good algebraic object and our situations in this note is nice.

Def. [p-adic Integers]

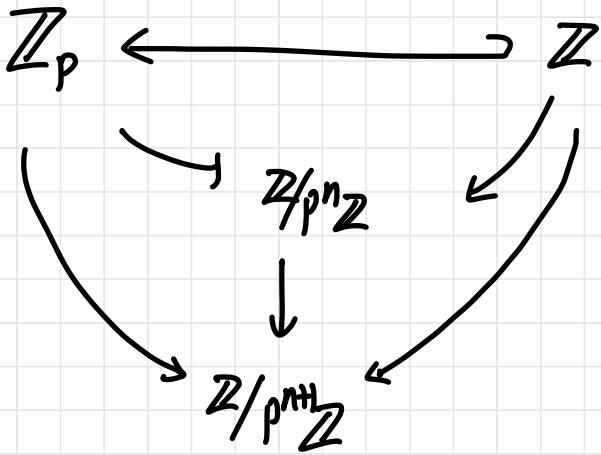
Consider the following (surjective) inverse system. (as a $\mathbb{Z}$-module cat)

$$A_n = \mathbb{Z}/p^n\mathbb{Z}, \quad \underbrace{\phi_n : A_n \longrightarrow A_{n-1}}_{\text{Canonical map}}$$

The p-adic integer, $\mathbb{Z}_p$ is a projective limit of this system.

i.e., $\mathbb{Z}_p := \varprojlim A_n$

*



* Topology on $\mathbb{Z}_p$

① For each A_n, give discrete topology on them.

② By Tychonoff's thm, $\prod A_n$ is compact.

③ Give a subspace topology on $\mathbb{Z}_p \subseteq \prod A_n$.

→ $\mathbb{Z}_p$ is closed ⇒ compact!
(why?)

* Natural valuation of $\mathbb{Z}_p$.

we need following proposition.

Prop. a. $x \in \mathbb{Z}_p$ is invertible
$\Leftrightarrow p \nmid x$.

b. Let U = units in $\mathbb{Z}_p$.
Every nonzero element of $\mathbb{Z}_p$ can be written uniquely in the form

$$p^n u \; ; \begin{cases} u \in U \\ n \geq 0. \end{cases}$$

Pf) omitted here. Calculation + Diagram Chasing.

With the proposition, we can conclude that

$\mathbb{Z}_p$ is DVR with a valuation v_p.

$$v_p : \mathbb{Z}_p \longrightarrow \mathbb{N} \cup \{\infty\}$$
$$0 \longmapsto \infty$$
$$p^n U \longmapsto n$$

Def. [p-adic Number]

Since $\mathbb{Z}_p$ is a domain, we can think its field of fraction; p-adic field.

with the natural valuation, we also have

$\mathbb{Q}_p := Q(\mathbb{Z}_p) = \mathbb{Z}_p[p^{-1}]$.

* Metric in $\mathbb{Q}_p$

* Note that

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x+y) \geq \inf(v_p(x), v_p(y))$.

→ we can define a distance on $\mathbb{Z}_p$.

$d(x,y) :=$

The subspace topology we defined on $\mathbb{Z}_p$.

The topology induced by d.

$\therefore$ $\mathbb{Z}_p$ is closed metric space.

⇓

Examples.

① Choose $a_0 \in \mathbb{Q}_p$ and let $a_n = a_0 \cdot p^n$.

Then $\lim_{n\to\infty} a_n = \lim a_0 \cdot p^n \rightsquigarrow \nearrow$

$= 0.$

Hence, $\sum_0^\infty a_n = \lim \frac{a_0(1-p^n)}{1-p} = \frac{a_0}{1-p}$

Contrast to the situation in $\mathbb{R}$.

$a_n \nearrow \infty$ in $\mathbb{R}$.

If $p=3$, $a_0=1$

$\rightsquigarrow \quad \frac{1}{1-3} = -\frac{1}{2} = \lim \sum 3^n.$

② Again, let $p=3$.

$52 = 1\cdot 3^3 + 2\cdot 3^2 + 2\cdot 3 + 1\cdot 3^0$

$-2 = -1\cdot 3 + 1\cdot 3^0$

$= (-1\cdot 3 + 2)\cdot 3 + 1\cdot 3^0 = -1\cdot 3^2 + 2\cdot 3 + 1\cdot 3^0$

$\rightsquigarrow \quad -2 = 1\cdot 3^0 - (2\cdot 3^1 + 2\cdot 3^2 + \cdots$

$= 1 - 6\cdot\frac{1}{2} = -2.$

③ Again, fix $p=3$.

$25/36 \in \mathbb{Q}_3$.

$25/36 = \underbrace{25/4}_{\mathbb{Z}_3 \ni u} \cdot \underbrace{1/9}_{p^{-2}}$

$\frac{25}{4} = 7 - \frac{3}{4} = 7 - \frac{6}{8}$

$= 7 + \frac{6}{1-9}$

$= 7 + 6 \sum_{0}^{\infty} 1 \cdot 9^n$

$= 13 + 6 \sum_{1}^{\infty} 1 \cdot 9^n$

$= 1 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2$

$+ 6(1 \cdot 3^2 + 1 \cdot 3^4 + \cdots) \in \mathbb{Z}_3$.

☆ Newton's Method in p-adic Numbers & Some Solutions ☆

Return to the introduction, our purpose was

"Find a solution"

Completeness (W.R.T canonical distance)

$\mathbb{Q}$ → $\mathbb{R}$

$\mathbb{Q}$ → alg. $\mathbb{Q}[X]/\langle x^2-2\rangle = \mathbb{Q}(\sqrt{2})$

Note that $\mathbb{Q}_p$ is complete.

Thm. [Newton's Method]

Let $f \in \mathbb{Z}_p[X]$, f' its derivate.

Let $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}$ such that

$$\begin{cases} 0 \le 2k < n, & f(x) \equiv 0 \pmod{p^n} \\ v_p(f'(x)) = k. \end{cases}$$

Then there exists $y \in \mathbb{Z}_p$ such that

$$f(y) \equiv 0 \pmod{p^{n+1}}, \quad v_p(f'(y)) = k$$

and $y \equiv x \pmod{p^{n-k}}$.

↓

Thm. [Hesel's Lemma]

Let $f \in \mathbb{Z}_p[X_1, \cdots, X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ and j an integer such that $0 \le j \le m$. Suppose that $0 < 2k < n$ and that $f(X) \equiv 0 \pmod{p^n}$ and $v_p\left(\frac{\partial f}{\partial x_j}(x)\right) = k$.

Then there exists a zero y of f in $(\mathbb{Z}_p)^m$ which is $y \equiv x \pmod{p^{n-k}}$.

Intuition; Compare to $\mathbb{Q}_\infty$ (= $\mathbb{R}$) - Newton's Method.

Classic (in $\mathbb{R}$)	vs	New (in $\mathbb{Q}_p$)
f is · Conti · diff	⟷	· f is in $\mathbb{Z}_p[x]$
· $f(\alpha)=0$	⟷	
· $f'(\alpha)\neq 0$	⟷	· $v_p(f'(x))=k$.
⇓		⇓
∃ neighborhood U of α such that $\forall\, x_0 \in U$, $(x^i) \to \alpha$.		For large n, ($\approx 2k<n$) (∝ sufficiently small p-adic nbd) $\rightsquigarrow (x^i) \to \alpha$ (zero).

Cor. Every simple zero of the reduction modulo p of a polynomial f lifts to a zero of f with coefficients in $\mathbb{Z}_p$.

Pf) Take $n=1$ and $k=0$ in Hensel's lemma.

Example. Let $p=7$

Consider $f(x) = x^2-2 \in \mathbb{Z}_7[X]$

Then $f(3) = 0$, $f'(3) \neq 0$. (In $\mathbb{Z}/7\mathbb{Z}$)

$\Rightarrow$ There exists $y \in \mathbb{Z}_7$ such that $y^2=2$.

$\therefore$ $\mathbb{Z} \subsetneq \mathbb{Z}_p$ and $\mathbb{Q} \subsetneq \mathbb{Q}_p$.

p-adic number is another way to extend $\mathbb{Q}$ containing roots not contained in $\mathbb{Q}$.

* Structure of $\mathbb{Q}_p$.

- No proof! -

Thm. $\mathbb{Q}_p^* \cong \begin{cases} \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \neq 2. \\ \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & \text{if } p = 2. \end{cases}$

This is because, $\mathbb{Q}_p^* \cong \mathbb{Z} \times U \cong \mathbb{Z} \times (V \times U_1)$

and $U \cong \begin{cases} \underbrace{\mathbb{Z}/(p-1)\mathbb{Z}}_{V} \times \underbrace{\mathbb{Z}_p}_{U_1} & p \neq 2 \\ \text{triv} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & p = 2. \end{cases}$

with this one can show that;

① $p \neq 2$; $x = p^n u \in \mathbb{Q}_p^*$,

x is a square $\Leftrightarrow$ n is even and image of u in $\mathbb{Z}/(p-1)\mathbb{Z}$ is a square.

pf)

② In $p=2$, $x = p^n u \in \mathbb{Q}_2^*$,

x is square $\Leftrightarrow$ n is even and $u \equiv 1 \pmod 8$.

③ $(\mathbb{Q}^*)^2$ is an open subgroup of $\mathbb{Q}^*$.

Note that ① and ② leads us to define Legendre symbol on $\mathbb{Q}_p$.

How?

Day2.

2. Hilbert symbol and its properties.

Today, I will omitt almost proofs.

Def. [Hilbert symbol]

$$(a,b) = \begin{cases} +1 & z^2 - ax^2 - by^2 \text{ has a nontrivial solution in } k^3. \\ -1 & \text{otherwise} \end{cases}$$

($a, b \in k^*$, $k = \underbrace{\mathbb{R}}_{\mathbb{Q}_\infty}$ or $\mathbb{Q}_p$)

Hilbert symbol can be considered as a generalization of Legendre symbol.

It will be an essential tool to prove Hasse-Minkowski theorem.

Notation $v = \{\text{primes}\} \cup \{+\infty\}$.

Easy propositions.

① $a,b \in k^*$. $k_b := k(\sqrt{b})$

Then $(a,b)=1 \Leftrightarrow a \in \underbrace{Nk_b^*}$

group of norms of elements in k_b.

② i) $(a,b)=(b,a)$, $(a,c^2)=1$.

ii) $(a,-a)=1$, $(a,1-a)=1$

iii) $(a,b)=1 \Rightarrow (aa',b)=(a',b)$

iv) $(a,b)=(a,-ab)=(a,(1-a)b)$.

Difficult theorem. [Formula of H.S]

$p \neq 2 \rightsquigarrow (a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}$

$p=2 \rightsquigarrow (a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha w(v)+\beta w(u)}$

where $a = p^{\alpha}u$, $b = p^{\beta}v$.

$p=\infty \rightsquigarrow (a,b)_\infty = \begin{cases} 1 & \text{if } a \text{ or } b > 0 \\ -1 & \text{if } a<0, b<0. \end{cases}$

* Note that, the formulas also show that $(a,b)_v$ is a bilinear map from $k^*/k^{*2} \times k^*/k^{*2}$ to $\{\pm 1\}$.

↳ Although we do not use this in this note, it is important.

These are fundamental theorems about Hilbert symbols.

Thm 1. [Product Formula]

If $a,b \in \mathbb{Q}^*$, we have $(a,b)_v = 1$ for almost all $v \in V$ and $\prod_V (a,b)_v = 1$

Thm 2. [Approximation Theorem]

Let S be a finite subset of V, the image of $\mathbb{Q}$ in $\prod_S \mathbb{Q}_v$ is dense in this product.

Thm3. Let $(a_i)_{i\in I}$ be a finite family of elements in $\mathbb{Q}^*$ and let $(\varepsilon_{i,v})_{i\in I, v\in V}$ be a family of numbers with values ± 1.

Then there exists $x\in\mathbb{Q}^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $(i,v)\in I\times V$.

3. Hasse - Minkowski Theorem and Its Applications.

Before producing H-M thm, go back to the chapter 0.

Q1. What is the local object corresponds to the global one, $\mathbb{Q}$.

A. (Without a doubt) $\mathbb{Q}_p$!

Then... what sense?

★ Example.

Consider the following polynomial.

$f(X,Y) = 11Y^2 - 11^2 + 2^2 11X^2 - 2X^4 \in \mathbb{Q}[X,Y]$.

Q. Is there any rational solution of f?

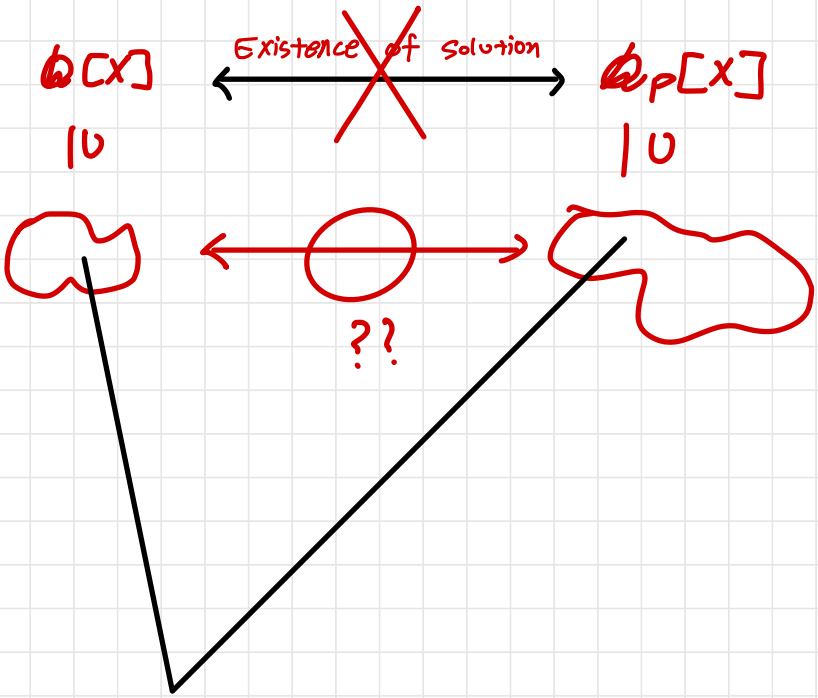
If we don't know p-adic numbers...

→ Can't deduce anything!

But, we know p-adic number now.

→ No solution in $\mathbb{Q}^2$!!!

Back to Ch 0 again, and see the second question.



Quadratic Forms.

Def. [Quadratic Form]

Let k be a field. A quadratic form over k is a polynomial of a form

$$f(X_i) = a_1 X^2 + \cdots + a_n X^2 \in k[x_1, \cdots, x_n].$$

For $a \in k$, we call f represents a if there exists $(a_1, \cdots, a_n) \in k^n$ such that

$$f(a_1, \cdots, a_n) = a.$$

Our Goal. [Hasse-Minkowski]

Let f be a quadratic form over $\mathbb{Q}$.

Then f represents 0 if and only if f_v represents 0 for all $v \in V$.

Example.

Consider the following quadratic form

$$f(X,Y,Z) = 5X^2 + 11Y^2 - 13Z^2.$$

By H-M thm,

Applications. [For details, see ACA].

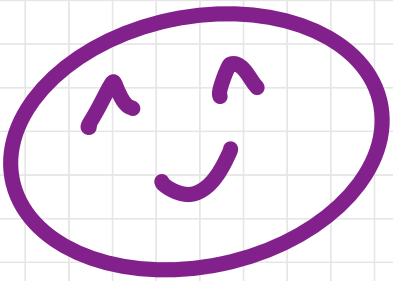
Thm. [Gauss]

In order that a positive integer be a sum of three squares it is equivalent to that it is not of the form $4^a(8b-1)$ with $a,b \in \mathbb{Z}$.

sketch of proof.

Cor. [Gauss]

Every positive integer is a sum of three triangular numbers.



Thank you-!