

Review Problems

(1) Lagrange's four-square theorem

(2) Let m, n be odd coprime numbers.

Show that

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{\left(\frac{m-1}{2}\right) \left(\frac{n-1}{2}\right)}$$

(3) Show that an integer $a \in \mathbb{Z}$ is a square $\iff \left(\frac{a}{p}\right) = 1 \quad \forall p$ primes

Problem 1: a) Let p be a prime. We want to show that there exists two integers r, s such that $r^2 + s^2 \equiv -1 \pmod{p}$.

Let's show a more general version of this.

For any prime p, r there exists r, s such that $r^2 + s^2 \equiv r \pmod{p}$

r^2 takes $\left(\frac{p+1}{2}\right)$ values (0 included)

$R-s^2$ also takes $\left(\frac{p+1}{2}\right)$ values

but they must intersect b/c there are
only p values from $\{0, 1, \dots, p-1\}$.

b) This is straight forward, just compute
Squares and add them up mod p .

c) The lattice in part b) has covolume p^2 .

$$\frac{n^2 \pi r^4}{2} = 2^4 \cdot p^2$$

$$r^2 = \frac{2^2 \sqrt{2} P}{\pi} = \frac{4\sqrt{2}}{\pi} P < 2P$$

So, if (a, b, c, d) is a point in the interior
of this circle not equal to origin and
lies on the lattice then

$$a^2 + b^2 + c^2 + d^2 = P$$

d) The general result now follows from
an observation that

$$(a^2 + b^2 + c^2 + d^2) (A^2 + B^2 + C^2 + D^2) \\ = E^2 + F^2 + G^2 + H^2$$

where $E = aA - bB - cC - dD$

$$F = aB + bA + cD - dC$$

$$G = aC - bD + cA + dB$$

$$H = aD + bC - cB + dA$$

Introduction to p-adic numbers

Let p be a prime.

Define v_p on \mathbb{Q} as follows.

$$\text{If } a \in \mathbb{Z} \quad a = p^{v_p(a)} a' \quad p \nmid a$$

$$\text{If } \frac{a}{b} \in \mathbb{Q}, \quad v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

$b > 1$

$$v_p(0) = \infty$$

Observe that if $\frac{a}{b} = \frac{a'}{b'}$, then

$$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{a'}{b'}\right)$$

$$b/c \quad ab' = a'b$$

$$\begin{aligned} \Rightarrow v_p(ab') &= v_p(a) + v_p(b') \\ &= v_p(a') + v_p(b) \end{aligned}$$

The following properties hold for all $x, y \in Q$

i) $v_p(xy) = v_p(x) + v_p(y)$

$$x = a/b \quad y = c/d \quad x \neq 0 \quad y \neq 0$$

$$v_p(x) = v_p(a) - v_p(b)$$

$$v_p(y) = v_p(c) - v_p(d)$$

$$\begin{aligned} xy &= \frac{ac}{bd} & v_p(xy) &= v_p(ac) - v_p(bd) \\ &&&= v_p(a) + v_p(c) \\ &&&- v_p(b) - v_p(d) \\ &&&= v_p(x) + v_p(y) \end{aligned}$$

If x or $y = 0$, then

$$v_p(xy) = \infty$$

$$v_p(x) + v_p(y) = \infty$$

$$\text{ii}) \quad v_p(x+ty) \geq \min \{v_p(x), v_p(y)\}$$

Assume $x+ty \neq 0$ & $v_p(x) \leq v_p(y)$

$$\Rightarrow v_p(x) < \infty \text{ or } x=y=0$$

If $y=0$, then $v_p(x+ty) = v_p(x)$
 $\geq \min \{v_p(x), v_p(y)\}$

$y \neq 0$ $x = ay_b$ $v_p(x) = v_p(a) - v_p(b)$

$y = cy_d$ $v_p(y) = v_p(c) - v_p(d)$

$$v_p(x) \leq v_p(y) \text{ so}$$

$$v_p(a) - v_p(b) \leq v_p(c) - v_p(d)$$

$$\Rightarrow v_p(a) + v_p(d) \leq v_p(c) + v_p(b)$$

$$v_p(ad) \leq v_p(bc)$$

$$v_p(ad+bc) \geq v_p(ad)$$

We will manipulate this inequality.

$$v_p(ad+bc) \geq v_p(ad)$$

$$\Rightarrow v_p(ad+bc) \geq v_p(a) + v_p(d)$$

$$\Rightarrow v_p(ad+bc) - v_p(d) \geq v_p(a)$$

$$\Rightarrow v_p(ad+bc) - v_p(a) - v_p(b) \geq v_p(a) - v_p(b)$$

$$\Rightarrow v_p(ad+bc) - v_p(ba) \geq v_p(a) - v_p(b)$$

$$x+_{\bar{y}} = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$v_p(x+_{\bar{y}}) \geq v_p(x) = \min \{ v_p(x), v_p(y) \}$$

We are now ready to define p-adic absolute value on \mathbb{Q}_p .

$$||_p: \mathbb{Q} \rightarrow \mathbb{R}$$

$$|x|_p = \begin{cases} p^{-v_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

$| \cdot |_p$ satisfies the following properties:

i) $|x|_p = 0 \Leftrightarrow x = 0$

ii) $|xy|_p = |x|_p |y|_p$

iii) $|x+y|_p \leq |x|_p + |y|_p$ (Triangle inequality)

iv) $|x+y|_p \leq \max \{ |x|_p, |y|_p \}$

(Strong Triangle inequality)

(iv) \Rightarrow (iii)

Examples:

$$\left| \frac{8}{13} \right|_2, \quad \left| \frac{13}{8} \right|_2$$

$$v_2\left(\frac{8}{13}\right) = 3 \quad v_2\left(\frac{13}{8}\right) = -3$$

$$\left| \frac{8}{13} \right|_2 = 2^{-3} = \frac{1}{8} \quad \left| \frac{13}{8} \right|_2 = 2^3 = 8$$

(Ostrowski's Thm) Every non-trivial
absolute value on \mathbb{Q} is equivalent to
either standard absolute value or to
P-adic absolute value for some
prime p .

\mathbb{R}

\mathbb{Q}_p

Completion of \mathbb{Q}

Completion of \mathbb{Q}

with respect to

with respect to

$|$ $|$

$|$ $|_p$

Completion : taking limits of sequences
and including those limits in your
set.

Arithmetic in \mathbb{Q}_p

For \mathbb{Q}_p elements look like

$$\sum_{n=n_0}^{\infty} q_n p^n = q_0 + q_1 p + q_2 p^2 + \dots$$

$$\underline{n_0 \in \mathbb{Z}} \quad q_{n_0} \neq 0 \quad 0 \leq q_n \leq p-1 \quad \begin{matrix} \nearrow \\ n \geq n_0 \end{matrix}$$

Some examples

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

$$-1 = \underbrace{1 + 1 \cdot 2}_{\text{mod } 2} + \underbrace{1 \cdot 2^2 + 1 \cdot 2^3}_{\text{mod } 4} + \dots$$

$$\qquad \qquad \qquad \text{mod } 8$$

$$-1 = \frac{1}{1-2} = 1 + 2 + 2^2 + 2^3 + \dots$$

$$\left(\text{Similar to } \frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots \right)$$

$$|2|_2 = 1 < 1$$

5-adic expansion of $\sqrt{3}$

$$\left\lfloor \frac{\sqrt{3}}{5} \right\rfloor_5 = 1 \quad \text{if } |x|_p \leq 1$$

then p-adic expansion looks like

$$\sum_{n=0}^{\infty} q_n p^n \quad 1 \leq q_n \leq p-1$$

$$\frac{\sqrt{3}}{5} \equiv q_0 \pmod{5}$$

$$4 \equiv 3q_0 \pmod{5}$$

q_0 is 3

$$\frac{\sqrt{3}}{5} \equiv 3 + 5q_1 \pmod{25}$$

$$4 \equiv 9 + 15q_1 \pmod{25}$$

$$20 \equiv 15q_1 \pmod{25}$$

$$q_1 = 3$$

Find q_2 & q_3 . Do you see a pattern?

SOME GEOMETRY IN \mathbb{Q}_p

We define a ball centered at x and of radius R as follows:

$$B(x, R) = \{ y \in \mathbb{Q}_p \mid |x - y|_p \leq R \}$$

Pick any other point $z \neq x$ in $B(x, R)$.

$$B(x, R) = B(z, R)$$

Say $y \in B(x, R)$

$$|x - y|_p \leq R$$

$$\begin{aligned} |z - y|_p &= |z - x + x - y|_p \\ &\leq \max \{ |z - x|_p, |x - y|_p \} \\ &\leq R \end{aligned}$$

$$\Rightarrow y \in B(z, R) \Rightarrow B(x, R) \subseteq B(z, R)$$

Say $y \in B(z, R)$

$$|x-y|_P \leq \max \{ |x-z|_P, |z-y|_P \} \\ \leq R$$

$y \in B(x, R)$

$$B(z, R) \subseteq B(x, R)$$

$$\text{So, } B(x, R) = B(z, R)$$

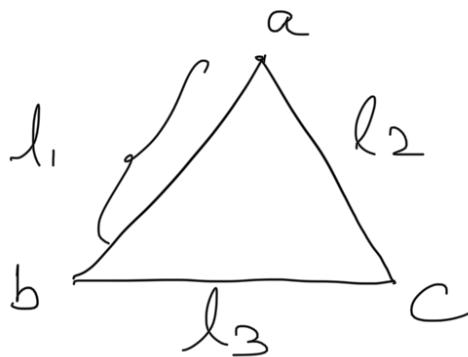
Every point is the center!

Triangles

→ In \mathbb{Q}_p , all triangles are isosceles.

Proof:

Say



is our triangle.

$$l_1 = |a - b|_p$$

$$l_2 = |a - c|_p$$

$$l_3 = |b - c|_p$$

Say $l_1 \neq l_2$ and $l_1 > l_2$

$$|b - c|_p = |b - a + a - c|_p$$

$$\leq \max \{ |b - a|_p, |a - c|_p \}$$

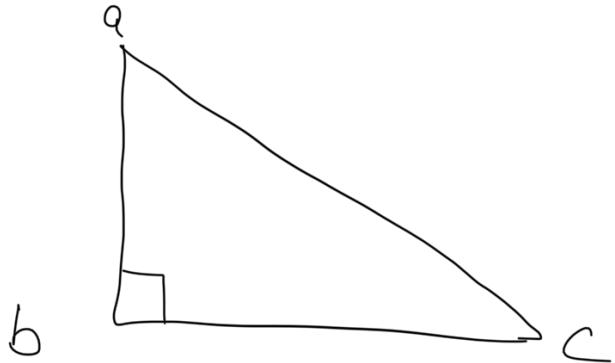
Suppose $l_3 \leq |b - a|_p$

$$|b - a|_p \leq \max \{ |b - c|_p, |c - a|_p \}$$

$$|b - a|_p < l_3 \quad \text{or} \quad |b - a|_p < l_2 \rightarrow$$

→ There are no right triangles
in \triangle_{P} .

Assume there is.



$$\text{So, } |\alpha - c|_P^2 = |\alpha - b|_P^2 + |b - c|_P^2$$

$$\Rightarrow |\alpha - b|_P = |b - c|_P$$

$$\begin{aligned} \text{So, } |\alpha - c|_P &= |\alpha - b + b - c|_P \\ &\leq \max \{ |\alpha - b|_P, |b - c|_P \} \end{aligned}$$

$$\Rightarrow |\alpha - c|_P \leq |\alpha - b|_P$$

$$\text{or } |\alpha - c|_P \leq |b - c|_P$$

→ ← .

→ Find 2-adic expansion of $\frac{2}{3}$.