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 $\iff \left(\frac{a}{p}\right) = 1$ $\forall$ primes p.

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

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

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

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

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

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

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

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

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.

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

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

$b > 1$

$$v_p(0) = \infty$$

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 $\quad ab' = a'b$

$$\Rightarrow v_p(ab') = v_p(a) + v_p(b')$$
$$= v_p(a') + v_p(b)$$

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

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

$x = a/b \qquad y = c/d \qquad x \neq 0, \; y \neq 0$

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

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

$xy = \frac{ac}{bd} \qquad v_p(xy) = v_p(ac) - v_p(bd)$

$= v_p(a) + v_p(c) - v_p(b) - v_p(d)$

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

If x or $y = 0$, then

$v_p(xy) = \infty$

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

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

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

$\Rightarrow v_p(x) < \infty$ o.w $x=y=0$

If $y=0$, then $v_p(x+y) = v_p(x)$

$\geq \min\{v_p(x), v_p(y)\}$

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

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

$v_p(x) \leq v_p(y)$ 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.

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

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

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

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

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

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

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

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

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

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

$|\ |_p$ satisfies the following properties:

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

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

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

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

(Strong Triangle inequality)

(iv) $\Rightarrow$ (iii)

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

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

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

(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.

$\mathbb{R}$ — Completion of $\mathbb{Q}$ with respect to $|\ |$

$\mathbb{Q}_p$ — Completion of $\mathbb{Q}$ with respect to $|\ |_p$

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

Arithmetic in $\mathbb{Q}_p$

In $\mathbb{Q}_p$ elements look like

$$\sum_{n=n_0}^{\infty} a_n p^n = a_0 + a_1 p + a_2 p^2 + \cdots$$

$n_0 \in \mathbb{Z}$ $\quad a_{n_0} \neq 0$ $\quad 0 \leq a_n \leq p-1$ $\forall$ $n \geq n_0$

Some examples

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

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

$\mod 2$

$\mod 4$

$\mod 8$

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

(Similar to $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$)

$$|2|_2 = \tfrac{1}{2} < 1$$

5 adic expansion of $4/3$

$|4/3|_5 = 1$ If $|x|_p \leq 1$

then p-adic expansion looks like

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

$4/3 \equiv q_0 \pmod 5$

$4 \equiv 3q_0 \pmod 5$

q_0 is 3

$4/3 \equiv 3 + 5q_1 \pmod{25}$

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

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

$q_1 = 3$

Find q_2 & q_3. Do you see a pattern?