In this lecture, we prove: for $p \neq q$ being odd primes,

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Recall: to find $\left(\frac{2}{p}\right)$, we look at:

$$2 \cdot 1,\ 2 \cdot 2,\ 2 \cdot 3,\ \cdots\ 2 \cdot \frac{p-1}{2}.$$

Now: let p be an odd prime and a an integer satisfying $\gcd(a, p) = 1$.

We study: set $P = \frac{p-1}{2}$

$$a \cdot 1,\ a \cdot 2,\ a \cdot 3,\ \cdots\ a \cdot P.$$

modulo p between $-P$ and P.

Define:

$$\mu(a,p) = \#\left\{\begin{array}{l}\text{integers in the list } a, 2a, 3a, \cdots Pa \\ \text{that become negative when integers} \\ \text{in the list are reduced modulo } p \\ \text{into the interval } [-P, P]\end{array}\right\}$$

Main Steps in the proof:

(1) (Gauss creterion) $\quad \left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$

(2) Let p, q be two primes. Then:

$$\mu(q,p) + \mu(p,q) \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2.$$

If we assume these two steps:

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\mu(q,p)} \cdot (-1)^{\mu(p,q)} = (-1)^{\mu(q,p)+\mu(p,q)}$$

$$= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

This proves Quadratic Reciprocity. □.

We first prove the step I. Let p be an odd prime and $\gcd(a,p)=1$.

Lemma 23.2. When the numbers $a, 2a, 3a, \cdots P a$ are reduced to the range $-P$ to P, the reduced values are $\pm 1, \pm 2, \cdots \pm P$ is some order, with each number appearing once with either a $+$ or $-$ sign.

Proof: For $k = 1, 2, \cdots P$, we write:

$$ka = p \cdot q_k + r_k \quad \text{with} \quad -P \le r_k \le P.$$

Claim: for $i \neq j$, $r_i \neq \pm r_j$

(Proof by contradiction): • Assume that $i \neq j$ but $r_i = r_j$.

Then $ia = p \cdot q_i + r_i$

$ja = p \cdot q_j + r_j = p \cdot q_j + r_i$

$\Rightarrow (i-j)a = p(q_i - q_j)$

Then $p \mid (i-j)a \Rightarrow p \mid i-j$ or $p \mid a$

This is impossible sime $i \neq j \in \{1, 2, \cdots P\}$

and $\gcd(p,a) = 1$.

- Assume that for $i \neq j$, $r_i = -r_j$

Then $ia = p \cdot q_i + r_i$

$ja = p \cdot q_j + r_j = p \cdot q_j - r_i$

$\Rightarrow (i+j)a = p(q_i + q_j)$

Then $p \mid (i+j)a \Rightarrow p \mid i+j$ or $p \mid a$

This is impossible sime $i \neq j \in \{1, 2, \cdots P\}$ $P = \frac{p-1}{2}$.

and $\gcd(p,a) = 1$.

This means: for $i \neq j$, $r_i \neq \pm r_j$.

$\pm 1, \pm 2, \cdots \pm P$ $\qquad$ P - pairs.

$r_1, r_2, \cdots r_P$ $\qquad$ P - numbers.

This shows: when reduced to the range $[-P, P]$,

$a, 2a, 3a, \cdots Pa$ will show up exactly one time

in each pair $\pm 1, \pm 2, \cdots \pm P$. $\square$

Theorem (Gauss's Creterion) Let p be an odd prime and $\gcd(a, p) = 1$. Then:

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$$

Proof: By Euler's creterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

It suffices to show: $a^{\frac{p-1}{2}} \equiv (-1)^{\mu(a,p)} \pmod p$

and use the fact that p is odd.

We multiply all the numbers in the list:

$$a, 2a, 3a, \cdots Pa.$$

- $a \cdot (2a) \cdot (3a) \cdots (Pa) = P! \cdot a^{\frac{p-1}{2}}$
- $a(2a) \cdot (3a) \cdots (Pa) \equiv (-1)^{\mu(a,p)} P! \pmod p$ (Lemma 23.2)

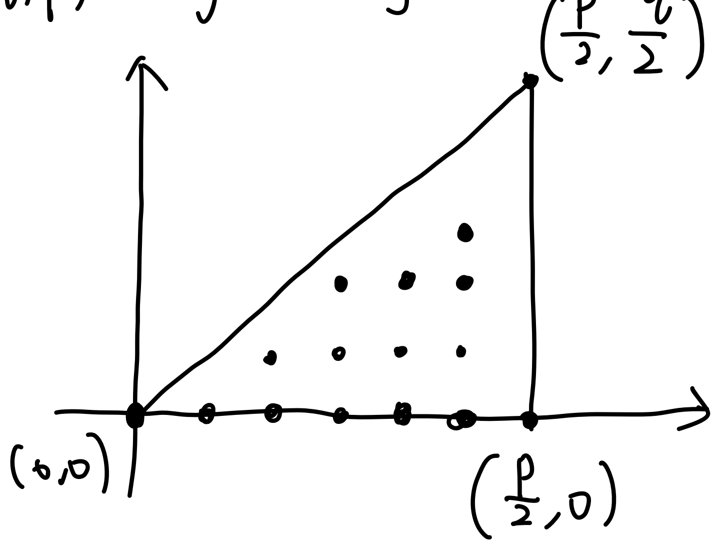
$\Rightarrow a^{\frac{p-1}{2}} \cdot P! \equiv (-1)^{\mu(a,p)} \cdot P! \pmod p$

$\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^{\mu(a,p)} \pmod p$ $(\gcd(P!, p) = 1)$ $\square$

Idea of Step II: let p, q be odd primes

In xy-coordinate, we look at the right triangle

$T(q,p)$ given by:



<u>Question</u>: how many <u>integral points</u> inside the triangle?

Here integral point means: both x and y are integers.

To answer this question, we introduce the floor function:

For $x \in \mathbb{R}$, $\lfloor x \rfloor =$ the largest integer n such $n \leq x$.

Example: $\lfloor 2.1 \rfloor = 2$ $\quad \lfloor -1.3 \rfloor = -2$

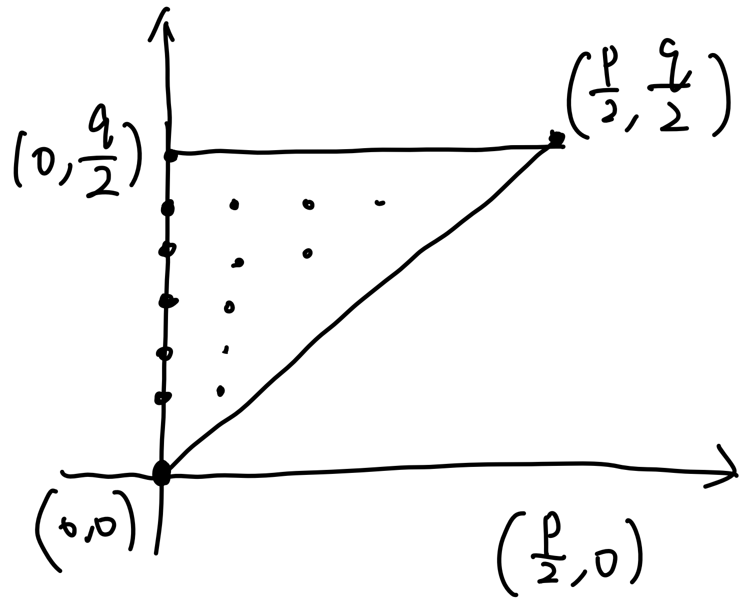
$\lfloor \frac{22}{7} \rfloor = 3$ $\quad \lfloor 4 \rfloor = 4$.

<u>Answer</u>: the number of integral points in $T(q,p)$

is: $\sum_{k=1}^{P} \left\lfloor \frac{kq}{p} \right\rfloor$

On the other hand, we consider another right triangle

$T(p,q)$



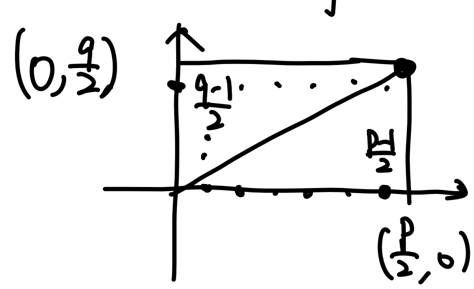
$Q = \frac{q-1}{2}$

Then the number of integral points in $T(p,q)$

is $\sum_{k=1}^{Q} \left\lfloor \frac{kp}{q} \right\rfloor$

Important observation: when we glue two right triangles with the hypotenuse, we get a rectangle

The total number of integral points should be:



$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$

Therefore: $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$

Lemma 23.3 Let p be an odd prime and $P = \frac{p-1}{2}$.

Let a be an odd integer and $\mu(a,p)$ as before.

Then:

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2.$$

If we assume this Lemma,

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \equiv \mu(q,p) + \mu(p,q) \pmod 2$$

This is the result of step II !

Therefore, we only need to prove Lemma 23.2.

Proof of Lemma 23.2: For $1 \le k \le P$,

$$ka = q_k \cdot p + r_k \quad \text{with} \quad -P \le r_k \le P$$

Divide by p, we get

$$\frac{ka}{p} = q_k + \frac{r_k}{p} \quad \text{with} \quad -\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}.$$

This implies: $\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0 \\ q_k - 1 & \text{if } r_k < 0. \end{cases}$

Note: $\mu(a,p) = \# \{ k : r_k < 0 \}$

This gives: $\displaystyle\sum_{k=1}^{p} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{p} q_k - \mu(a,p).$

We want to show: $\displaystyle\sum_{k=1}^{p} q_k \equiv (0 \bmod 2)$ (*)

$$\left(\text{This gives: } \sum_{k=1}^{p} \left\lfloor \frac{ka}{p} \right\rfloor \equiv 0 - \mu(a,p) \pmod 2 \quad \equiv \mu(a,p) \pmod 2 \right)$$

To show (*), we go back to:

$$ka = q_k \cdot p + r_k$$

We consider the equation modulo 2 (a, p are odd)

$$k \equiv q_k + r_k \pmod 2$$

Sum the equations,

$$\sum_{k=1}^{p} k \equiv \sum_{k=1}^{p} q_k + \sum_{k=1}^{p} r_k \pmod 2$$

For $i \in \{1, 2, \cdots p\}$, $i \equiv -i \pmod 2$

Then by Lemma 23.2,

$$\sum_{k=1}^{p} r_k \equiv (\pm)1 + (\pm)2 + \cdots (\pm)p \pmod 2$$
$$\equiv 1 + 2 + \cdots + p \pmod 2$$
$$\equiv \sum_{k=1}^{p} k \pmod 2$$

Therefore, $\sum_{k=1}^{p} q_k \equiv 0 \pmod 2$ and:

$$\sum_{k=1}^{p} \left\lfloor \frac{ka}{p} \right\rfloor \equiv -\mu(a,p) \pmod 2$$
$$\equiv \mu(a,p) \pmod 2$$

$\square$.