Chapter 4 – Quadratic Residues

4.1 Quadratic Residues

Definition: Let $m \geq 1$ and suppose $a \in \mathbb{Z}$ and $\gcd(a, m) = 1$. a is a *quadratic residue mod m* if

(*) $x^2 \equiv a \pmod{m}$

has a solution. Otherwise a is a *quadratic nonresidue mod m*.

Example Find all quadratic residues & nonresidues mod 13. We consider the congruence

NOTE:

x	$x^2 \pmod{13}$

The incongruent quadratic residues mod 13 are $a =$

and the quadratic nonresidues mod 13 are

$a =$

Proposition Let p be an odd prime, $a \in \mathbb{Z}$ al suppose $p \nmid a$. The congruence

(*) $$x^2 \equiv a \pmod{p}$$

has

PROOF:

Proposition Let p be an odd prime.
There are exactly _____ incongruent q.r. mod p, &
" " " _____ " q.n.r. mod p.

PROOF:
Consider each of the congruences

$\equiv$
$\equiv$
$\vdots$
$\equiv$

Each congruence has
Each of number (incongruent mod p)
(**)
occurs as
Corresponding a solution

Each congruence

Hence $=$
and # of incongruent q.r. mod p $=$

and Jere are

Hence,

#6. Let p be an odd prime. Prove that the $\frac{1}{2}(p-1)$ quadratic residues mod p are congruent to

$$1^2, 2^2, 3^2, \ldots, \left(\tfrac{1}{2}(p-1)\right)^2$$

mod p.

4.2 The Legendre Symbol

Definition Let p be an ___ prime, $a \in \mathbb{Z}$ and suppose ____. The **Legendre symbol** of a mod p denoted by $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} \\ \\ \end{cases}$$

Example $p = 13$

$$\left(\frac{a}{p}\right) = \left(\frac{a}{13}\right)$$

a
1
2
3
4
5
6
7
8
9
10
11
12

Note In Section 4.1 we found the q.r. & q.n.r. mod 13.

Euler's Criterion Let p be an odd prime, $a \in \mathbb{Z}$ & suppose $p \nmid a$. Then

$$\left(\frac{a}{p}\right)$$

Proof:

Case 1 $\left(\frac{a}{p}\right) = 1$.

Case 2 $\left(\frac{a}{p}\right) = -1$. For each $1 \leq i \leq p-1$

$$xi \equiv a \pmod{p}$$

has a

Thus we can pair the integers

$$1, 2, \ldots, p-1$$

into pairs such that the product of each pair is congruent to ___ (mod p).

It follows that

$(p-1)! \equiv$

$\equiv$ $\pmod p$

But $(p-1)! \equiv$ $a \neq 1$

□

An Example of Case 2 $a=2$, $p=13$ $x \equiv 2 \pmod 3$

$x = 2$

$1 \cdot 2 \equiv 2 \pmod{13}$ 15

$\equiv 2 \pmod{13}$ 28

$\equiv 2 \pmod{13}$

$\equiv 2 \pmod{13}$

$\equiv 2 \pmod{13}$

$\equiv 2 \pmod{13}$

$x^2 \equiv 2 \pmod{13}$ has ____, $\text{ord}\left(\frac{2}{13}\right) =$

By Wilson

$12! \equiv \equiv$

$\equiv$

$\equiv$

Example Find $\left(\frac{5}{17}\right)$ by Euler's Criterion.

We want $5^{--} \pmod{17}$.

$5^2 \equiv$

$5^4 \equiv$

$5^8 \equiv$

$\left(\frac{5}{17}\right) \equiv$

Hence $\left(\frac{5}{17}\right) =$ (since if $\left(\frac{5}{17}\right) =$

Then).

Proposition Let p be a odd prime, $a, b \in \mathbb{Z}$ & suppose $p \nmid a$ & $p \nmid b$. Then

(i) $\left(\frac{a^2}{p}\right) =$

(ii) If $a \equiv b \pmod{p}$ Then

(iii) $\left(\frac{ab}{p}\right) =$

Proof:

(i)

(ii)

(iii) By Euler's Criterion,

$\left(\frac{ab}{p}\right) \equiv$

$\not{a}$ $\not{p}$ |

But $\left(\frac{ab}{p}\right), \left(\frac{a}{p}\right), \left(\frac{b}{p}\right) =$

$\not{a}$

Since

□

<u>Example</u> Find $\left(\frac{3}{17}\right)$ using the fact that $\left(\frac{5}{17}\right) = 1$.

$\left(\frac{3}{17}\right) = \left(\frac{\quad}{17}\right)$ (since $3 \equiv$ (mod A))

<u>Theorem</u> Let p be an odd prime. Then

$\left(\frac{-1}{p}\right) =$ $=$ $\begin{cases} \end{cases}$

Proof By Euler's Criterion,

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

Since $\left(\frac{-1}{p}\right) =$ &

it follows by a previous argument that

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

Since p is odd $p \equiv$ (mod 4).

If $p \equiv$ (mod 4) then

If $p \equiv$ (mod 4) then

□

Example Find $\left(\frac{14}{17}\right)$ using the fact that $\left(\frac{3}{17}\right) = -1$.

Gauss' Lemma Let p be an odd prime, $a \in \mathbb{Z}$ & suppose $p \nmid a$. Let n be the number of _____ of the integers

(*)

that are _____ Then

$$\left(\frac{a}{p}\right) = \quad .$$

Example Find $\left(\frac{3}{13}\right)$ using Gauss' Lemma.

$p =$ & $\frac{p-1}{2} =$. $\frac{p}{2} =$

Consider

(*)

Hence $n =$ & $\left(\frac{3}{13}\right) =$

Idea of Proof of Gauss's Lemma

Proof of Gauss' Lemma

Let $r_1, r_2, \ldots, r_n$ be the least positive residues of the numbers

$a,$ $\qquad\qquad$ $(\mathrm{mod}\ p)$

that are $\qquad\qquad$, al

$s_1, s_2, \ldots, s_m$ be the least positive residues (mod p) of these integers that are

Clearly each r_i, s_j $\qquad$ $(\mathrm{mod}\ p)$.

Now we form the sequence

$(*)$

We will show that $(*)$ consists of the numbers

in some order.

Claim 1.

Claim 2

It follows that

$$\left(\frac{p-1}{2}\right)_0! \equiv$$

$$\equiv$$

$$\equiv$$

$$\equiv$$

Note that

Hence

$$\equiv$$

$$\equiv$$

$$\equiv$$

$$\equiv$$

and it follows that

Theorem Let p be a odd prime. Then

$$\left(\frac{2}{p}\right) = \qquad = \begin{cases} \\ \\ \end{cases}$$

PROOF By Gauss' Lemma we have

$$\left(\frac{2}{p}\right)$$

where

Hence $n =$

We need to show that

$(*)$ $\equiv$ (mod).

Let $p = 8k + r$ where $r =$.
Then

$=$ $\equiv$

$=$

r (mod) (mod)

Here we have

$$\left(\frac{2}{p}\right) = \quad = \quad = \begin{cases} \\ \\ \end{cases}$$

and

Example $\left(\frac{2}{13}\right) =$

Recall If p is an odd prime then

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

Problem #26 Prove that there are infinitely many primes of the form $4n+1$ (where n is a positive integer)

4.3 The Law of Quadratic Reciprocity

Theorem (Law of Quadratic Reciprocity)
Let p, q be _____ _____ primes.
Then

$$\left(\frac{\quad}{\quad}\right)\left(\frac{\quad}{\quad}\right) = (-1)^{\cdots\cdots}$$

$$= \begin{cases} \\ \\ \end{cases}$$

NOTE: In the theorem if _____
Then $\left(\frac{\quad}{\quad}\right) = \left(\frac{\quad}{\quad}\right)$.

In the theorem if _____
Then $\left(\frac{\quad}{\quad}\right) = -\left(\frac{\quad}{\quad}\right)$.

Example (1) Find $\left(\frac{11}{101}\right)$ (11, 101 are odd primes)

(2) Find $\left(\frac{14}{101}\right)$

Eisenstein's Lemma

Let p be an odd prime, $a \in \mathbb{Z}$, $p \nmid a$ and _____. Then

$$\left(\frac{a}{p}\right) =$$

where

Example Find $\left(\frac{5}{13}\right)$ using Eisenstein's Lemma

NOTE Let $a, b > 0$ be integers. Then

$$a = q \cdot b + r$$

where

$q =$, and r .

(See proof of the Division Algorithm, Chapter 1).

Proof of Eisenstein's Lemma As in the proof of Gauss's Lemma we consider the integers

(*)

Let $r_1, r_2, \ldots, r_n$ be the ---------- of the numbers in (*) that are ---- Let

$s_1, s_2, \ldots, s_m$

be the remaining residues.

Then for $1 \leq k \leq \frac{1}{2}(p-1)$

$$ka = \qquad p + \qquad ,$$

$$(1) \quad \sum_{k=1}^{\frac{1}{2}(p-1)} ka =$$

We know from the proof of Gauss' Lemma that the numbers

are the numbers

in some order. Therefore,

$$\sum \quad + \sum \quad = \sum$$

$$(2) \quad \sum_{k=1}^{\frac{1}{2}(p-1)} k =$$

(2) − (1) gives

$$\sum_{k=1}^{\frac{1}{2}(p-1)} k =$$

Since a is odd we have

$\equiv$ (mod 2),

$n \equiv$ (mod 2).

By Gauss' Lemma we have

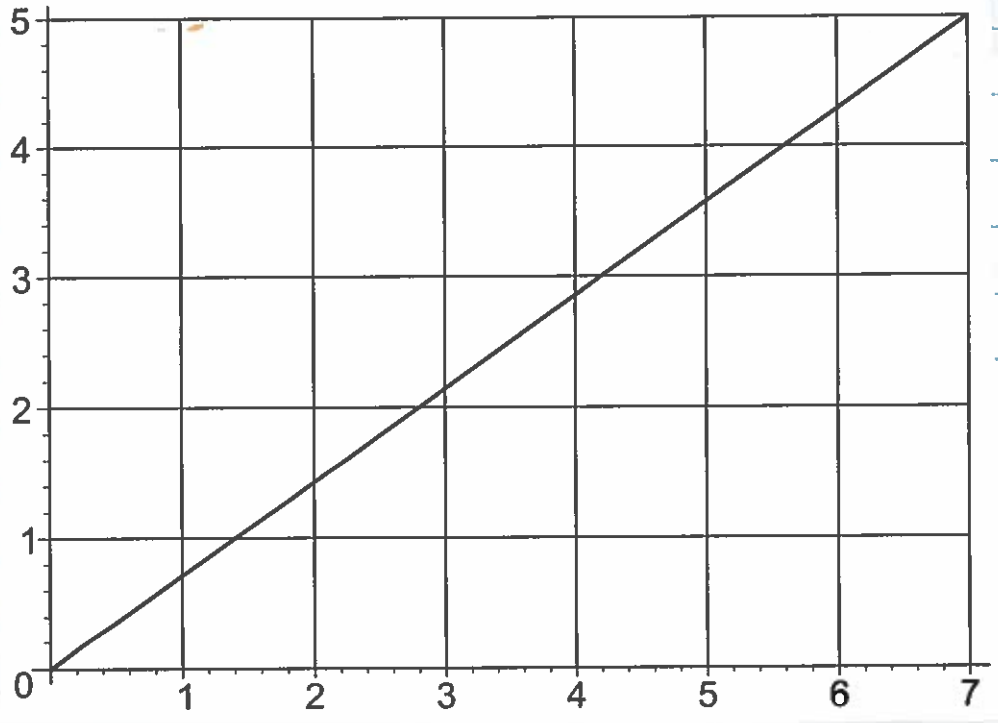
$\left(\frac{a}{p}\right) =$ $=$

where

□

Proof of The Law of Quadratic Reciprocity

Let p, q be odd primes with $q < p$.



We count the number of lattice points in the rectangle OABC (excluding
i.e. the set

$$\{(x,y) : \qquad \}$$

The number of points in this set is

The line ON has equation

$$y =$$

If x, y are integers, $1 \leq x \leq p$ and $1 \leq y \leq q$ and (x,y) is on this line then

and since p, q are distinct primes.

Hence

is the ____ lattice point on ON.

The y-coord of the point M is

$$y =$$

Note $q < p$ so

$$= \quad < \quad < \quad < \quad <$$

So the y-co-ordinate of M lies between two _____.

namely and .

Similarly the x-coord of the point P is

$x =$

$=$

Now $\frac{p}{q} >$ and $<$

Note if $p < 3q$ then

$<$ $<$

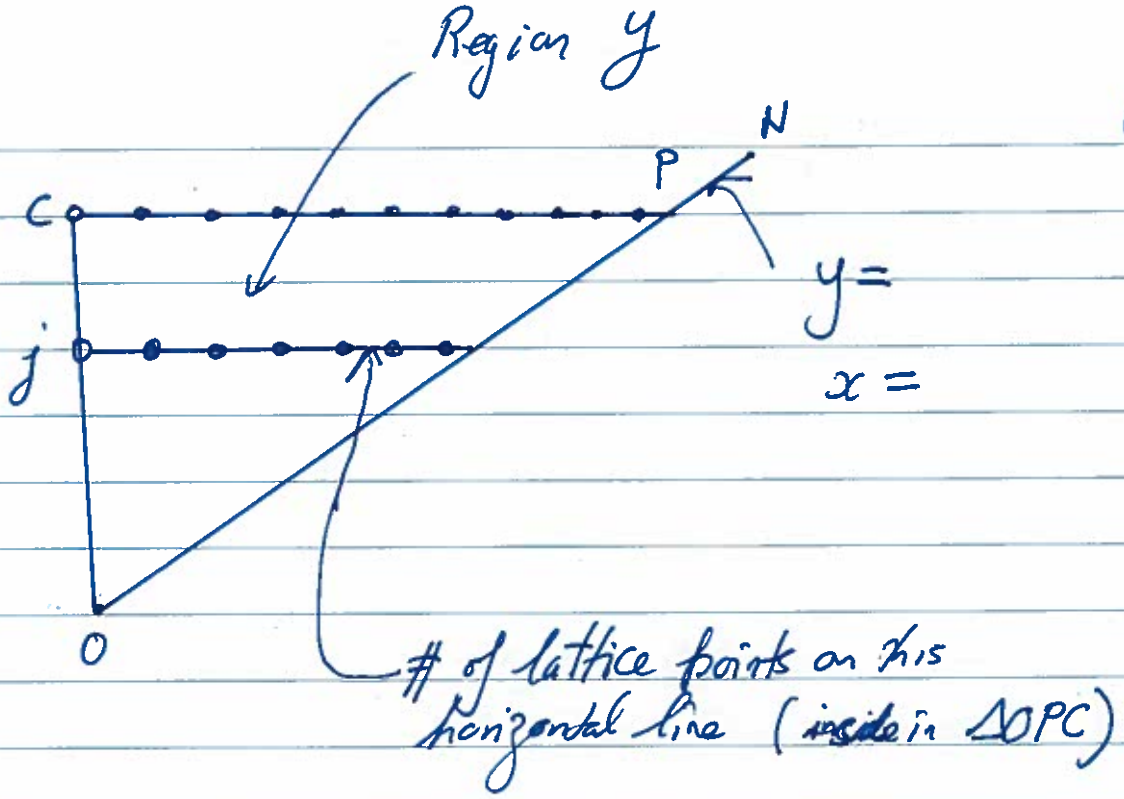
So the analog for P does not hold.
But, there are _____ in Δ PMB
_____.

So the number of lattice points in the rectangle OABC (excluding) is $N_1 + N_2$

where

$N_1 :=$,

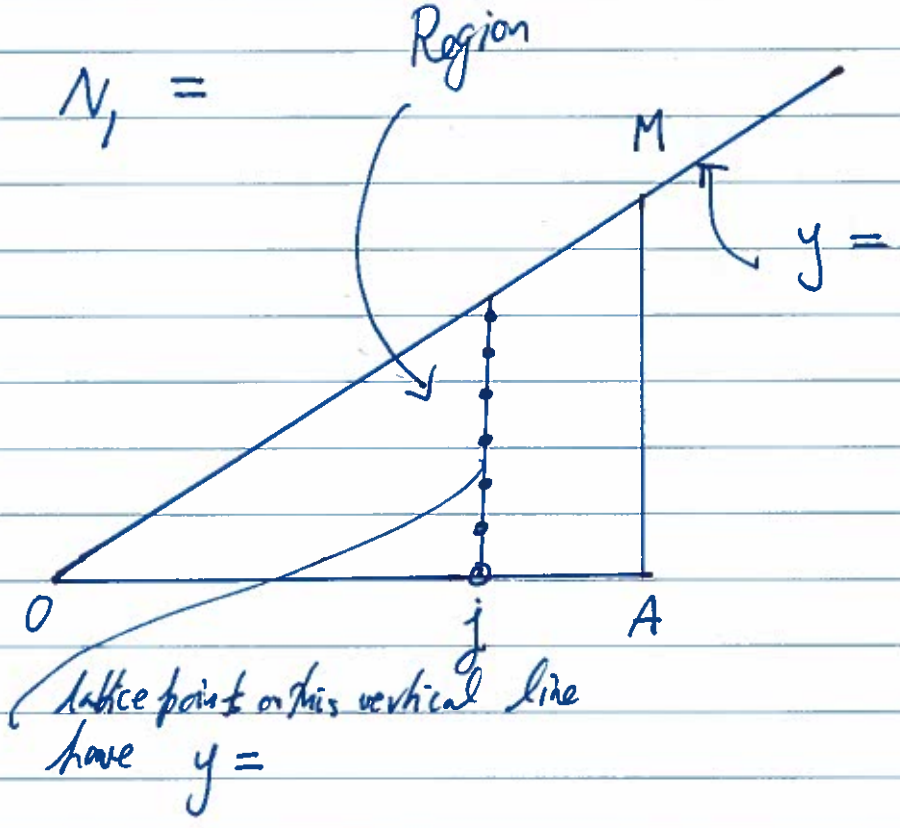
$N_2 :=$


Region y
N
P
C
y =
j
x =
O
# of lattice points on this horizontal line (inside in ΔOPC)

=

Thus

N_1 =


Region
M
y =
O
j
A
lattice points on this vertical line have y =

N_2 =

Hence

$N_1 + N_2 =$

by Eisenstein's Lemma

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) =$$

□

Problem Assume $p > 3$ is prime.
Find when $\left(\frac{3}{p}\right) = +1$.

Problem Assume $p \neq 11$ is an odd prime.
Find when $\left(\frac{11}{p}\right) = +1$.