

Chapter 4 - Quadratic Residues

(p.1)

4.1 Quadratic Residues

Definition: Let $m \geq 1$ and suppose $a \in \mathbb{Z}$ and
if a is a quadratic residue mod m

(*)

has \dots . Otherwise a is a

quadratic nonresidue mod m .

Example Find all quadratic residues & non residues
mod 13. We consider \mathbb{Z}_m congruence

NOTE:

$$\frac{x}{x^2 \pmod{13}}$$

Let a be incongruent quadratic residues mod 13

are $a =$

and the quadratic nonresidues mod 13 are

$a =$

(p.2)

Proposition Let p be an odd prime, $a \in \mathbb{Z}$ and

square free. The congruence

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

has

Proof:

(p.3)

Proposition Let p be an odd prime.

There are exactly $\frac{p-1}{2}$ incongruent g.r. mod p .
" " " " " g.n.r. mod p .

PROOF:

Consider each of the congruences

$$\begin{aligned} &\equiv \\ &\equiv \\ &\dots \\ &\dots \\ &\dots \\ &\equiv \end{aligned}$$

Each congruence has

Each of numbers (incongruent mod p)

(**)

occurs as

Conversely a solution

Each congruence

Hence =

and # of incongruent g.r. mod p =

as $\frac{p-1}{2}$ are

Hence,

(p-1)

#6. Let p be an odd prime. Prove that the $\frac{1}{2}(p-1)$

quadratic residues mod p are congruent to

$$1^2, 2^2, 3^2, \dots, \left(\frac{1}{2}(p-1)\right)^2$$

mod p .

4.2 The Legendre Symbol

Definition Let p be an odd prime, $a \in \mathbb{Z}$ and suppose $a \not\equiv 0 \pmod{p}$. The Legendre symbol of a mod p

denoted by $\left(\frac{a}{p}\right)$ is defined by

$$= \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}$$

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 g.c.f. of a and p mod 13.

(6)

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

$1, 2, \dots, p-1$

into pairs such that the product

of each pair is congruent to $\underline{\hspace{2cm}}$ \pmod{p} .

(7)

It follows that

$$(p-1)! \equiv \equiv \pmod{p}$$

$$\text{But } (p-1)! \equiv \text{ad} \pmod{p}$$

□

An Example of Case 2 $a=2, p=13$ $x=2 \pmod{13}$

$$x=2$$

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

$$\equiv 2 \pmod{13}$$

$$\equiv 2 \pmod{13}$$

$$\equiv 2 \pmod{13}$$

$$\equiv 2 \pmod{13}$$

$$\equiv 2 \pmod{13}$$

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

By Wilson

$$12! \equiv \equiv$$

$$\equiv$$

$$\equiv$$

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

$$\text{We want } 5^{\dots} \pmod{17}$$

$$5^2 \equiv$$

$$5^4 \equiv$$

$$5^8 \equiv$$

(p.8)

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

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

non

).

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

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

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

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

Proof:

(i)

(ii)

(iii) By Euler's Criterion,

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

(9)

$a \mid b$

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

a

Since

□

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

$$\left(\frac{3}{17}\right) = \left(\frac{-1}{17}\right) \quad (\text{since } 3 \equiv -1 \pmod{17})$$

Theorem Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

(10)

Proof By Euler's Criterion,

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

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

it follows by a previous argument that

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

$$\text{Since } p \text{ is odd } p \equiv \pmod{4}.$$

$$\text{If } p \equiv \pmod{4} \text{ then}$$

$$\text{If } p \equiv \pmod{4} \text{ then}$$

□

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

(11)

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

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

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

$$p = 13 \quad \& \quad \frac{p-1}{2} = 6 \quad \cdot \quad \frac{p}{2} = 6.5$$

Consider

(*)

$$\text{Hence } n = 6 \quad \& \quad \left(\frac{3}{13}\right) =$$

Idea of Proof of Gauss' Lemma

Proof of Gauss' Lemma

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

$$a, \quad (\text{mod } p)$$

that are a, \dots, a

a_1, a_2, \dots, a_m be the least positive residues of mod p of these integers that are

$$(\text{mod } p).$$

Clearly each r_i, s_j

Now give form the sequence

(*)

We will show that (*) consists of the numbers

in some order.

Claim 1.

(13)

Claim 2

It follows that

$$\begin{aligned} & \binom{p-1}{2}! \equiv \\ & \equiv \\ & \equiv \\ & \equiv \end{aligned}$$

Note that

Hence

≡

≡

≡

≡

and it follows that

Theorem Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

PROOF By Gauss Lemma we have

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

where

(15)

Hence $n =$

We need to show that

$$(*) \quad \equiv \equiv \pmod{.}$$

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

$$= \equiv$$

$$= .$$

$$r \pmod{.} \pmod{.}$$

17

The image shows a grid of 17 vertical columns. A red horizontal line is drawn across the middle of the grid, and a black horizontal line is drawn at the bottom. The grid is otherwise empty.

(18)

4.3 The Law of Quadratic Reciprocity

Theorem (Law of Quadratic Reciprocity)

Let p, q be primes.
Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\dots}$$
$$= \left\{ \begin{array}{l} \dots \end{array} \right.$$

NOTE: In the theorem if -----

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

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

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

(19)

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

Eisenstein's Lemma

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

and $p \nmid a^2 + 3a$. Then

$$\left(\frac{a}{p}\right) = \left(\frac{a^2 + 3a}{p}\right)$$

where

(20)

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

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

$$a = qb + r$$

where

$$0 \leq r < b$$

(See proof of the Division Algorithm, Chap 6.1).

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

(*)

(21)

Let r_1, r_2, \dots, r_n be the
of the numbers in (x) that are \dots . Let

s_1, s_2, \dots, s_m

be the remaining residues.

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

$$ka = p + \dots,$$

all $\frac{1}{2}(p-1)$

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

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

are the numbers

in some order. Therefore,

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

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

(2) - (1) gives

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

(22)

Since a is odd we have

$$\equiv \pmod{2},$$

$$n \equiv \pmod{2}.$$

By Gauss' Lemma we have

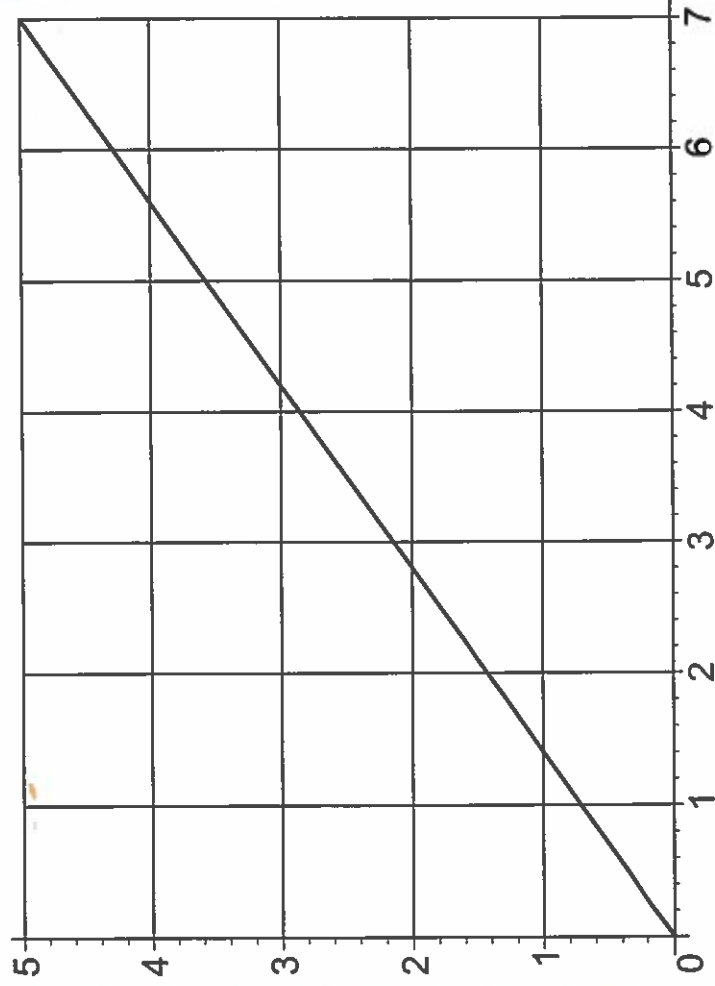
$$\left(\frac{a}{p}\right) = =$$

above

□

Proof of the Law of Quadratic Reciprocity

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



(23)

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

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

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

$$= \dots < \dots < \dots < \dots < \dots$$

So the y -coordinate of M lies between two

namely and
 Similarly the x -coord of the point P is

$$x =$$

$$=$$

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

Note if $p < 3q$ then

$<$ $<$

So the analog for P does not hold.
 But, there are in ΔPMB

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

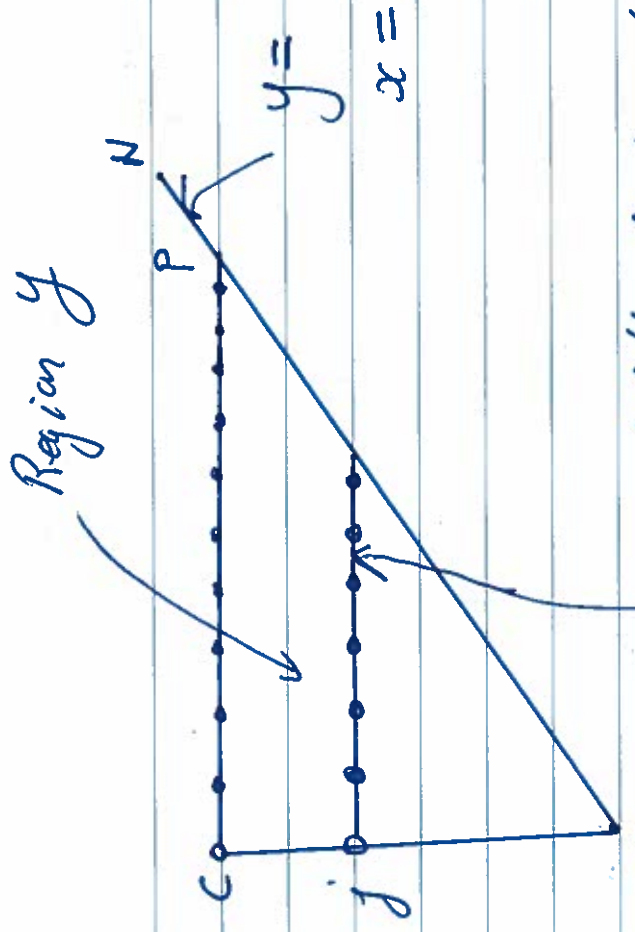
is

where

$$N_1 :=$$

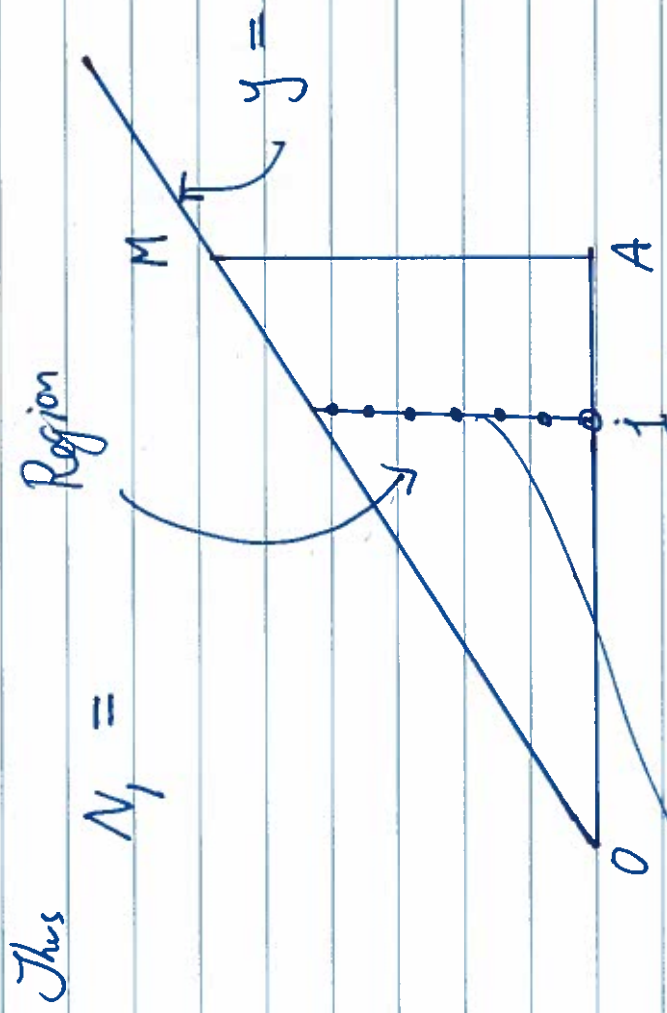
$$N_2 :=$$

(25)



of lattice points on this horizontal line (inside ΔOPC)

=



Lattice point on this vertical line have $y =$

$N_2 =$

(29)

Hence

$$N_1 + N_2 =$$

↳ by Eisenstein's Lemma

$$\binom{p}{q} \binom{q}{p} =$$

□

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

(2)

(28)

Problem Assume $p \nmid 11$ is an odd prime.

Find when $\left(\frac{11}{p}\right) = +1$.

(22)

The image shows a blank ledger page with 20 vertical blue lines and a horizontal red line near the bottom. The lines are evenly spaced and extend across the width of the page. The red line is positioned approximately one-fifth of the way up from the bottom edge. The page is otherwise empty of any text or markings.