
MATH 4573: Elementary Number Theory March 30

Claire Merriman

March 30, 2020

Contents

Quadratic reciprocity	3
---------------------------------	---

Quadratic reciprocity

We finally prove quadratic reciprocity!

Theorem 1 (Restatement of quadratic reciprocity). *Let p and q be odd primes with $p \neq q$. Then*

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

Definition 1. A lattice point is a point $(x, y) \in \mathbb{R}^2$ where $x, y \in \mathbb{Z}$. We can write this as $(x, y) \in \mathbb{Z}^2$.

Proof Without loss of generality, assume that $p > q$. We draw the rectangle $O = (0, 0), A = \left(\frac{p-1}{2}, 0\right), B = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, and $C = \left(0, \frac{q-1}{2}\right)$, like in the graphic below:



The participation assignment is to count the lattice points in the rectangle $OABC$ outlined in grey, including those on the lines AB and BC , but not those on OA or OC .

In order to count these lattice points another way, we are going to show that there are N_1 lattice points in the triangle OPC not including OC (pink) and N_2

Learning outcomes:
Author(s): Claire Merriman

lattice points in in OAM not including OA (yellow), thus the total number of lattice points is $N_1 + N_2$. We will find that $N_1 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$ and $N_2 = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$. Thus, by the previous lemma, $\left\lfloor \frac{p}{q} \right\rfloor = (-1)^{N_1}$ and $\left\lfloor \frac{q}{p} \right\rfloor = (-1)^{N_2}$, which will let us finish the proof.

We will do an examples first:

Example 1. We look at the example above with $p = 7$ and $q = 5$.

- a) The line ON has slope $\left\lfloor \frac{5}{7} \right\rfloor$. Since p and q are distinct primes, there are no lattice points on ON except the endpoints.
- b) The x -coordinate of M is $\left\lfloor 3 \right\rfloor$, y -coordinate of M is $\left\lfloor \frac{15}{7} \right\rfloor$.
- c) The y -coordinate of M lies between two consecutive integers $\left\lfloor 2 \right\rfloor$ and $\left\lfloor 3 \right\rfloor$.

Thus, the triangle PMB has no lattice points except possibly those on PB . We can then count the number of lattice points in $OABC$ by adding the number of lattice points in OCP to those in OAM .

To find N_1 , the number of lattice points in OPC , not including those on OC , we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \dots, \frac{q-1}{2}$ (in our case, this is only $j = 1, 2$.) Another way of saying this is for each j , we want the number of nonnegative integers less than

Multiple Choice:

- (a) $\frac{7j}{5}$ ✓
- (b) $\frac{5j}{7}$

Thus, we have for each j , there are

Multiple Choice:

- (a) $\left\lfloor \frac{7j}{5} \right\rfloor$ ✓
- (b) $\left\lfloor \frac{5j}{7} \right\rfloor$

lattice points in OPC. Then $N_1 =$

Multiple Choice:

(a) $\sum_{j=1}^2 \left\lfloor \frac{7j}{5} \right\rfloor \quad \checkmark$

(b) $\sum_{j=1}^2 \left\lfloor \frac{5j}{7} \right\rfloor$

To find N_2 , we use a similar counting method on OAM. Now, we count the lattice points on $x = j$ for $j = 1, 2, \dots, \frac{p-1}{2}$. Thus, for each j , we want the number of nonnegative integers less than

Multiple Choice:

(a) $\frac{7j}{5}$

(b) $\frac{5j}{7} \quad \checkmark$

Thus, we have for each j , there are

Multiple Choice:

(a) $\left\lfloor \frac{7j}{5} \right\rfloor$

(b) $\left\lfloor \frac{5j}{7} \right\rfloor \quad \checkmark$

l lattice points in OPC. Then $N_2 =$

Multiple Choice:

(a) $\sum_{j=1}^3 \left\lfloor \frac{7j}{5} \right\rfloor \quad \checkmark$

(b) $\sum_{j=1}^3 \left\lfloor \frac{5j}{7} \right\rfloor$

Now we generalize this idea to any odd primes p and q with $p > q$.

- a) The line ON has slope $\frac{q}{p}$. Since p and q are distinct primes, there are no lattice points on ON except the endpoints.
- b) The x -coordinate of M is $\frac{p-1}{2}$, y -coordinate of M is $\frac{(p-1)q}{2p} = \frac{q}{2} - \frac{q}{2p}$.
- c) The y -coordinate of M lies between two consecutive integers $\frac{q-1}{2}$ and $\frac{q+1}{2}$, since

$$\frac{q-1}{2} = \frac{q}{2} - \frac{1}{2} < \frac{q}{2} - \frac{q}{2p} < \frac{q}{2} < \frac{q+1}{2}$$

Thus, the triangle PMB has no lattice points except possibly those on PB . We can then count the number of lattice points in $OABC$ by adding the number of lattice points in OC to those in OAM .

To find N_1 , the number of lattice points in OPC , not including those on OC , we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \dots, \frac{q-1}{2}$. Another way of saying this is for each j , we want the number of nonnegative integers less than

Multiple Choice:

- (a) $\frac{jp}{q}$ ✓
- (b) $\frac{jq}{p}$

Thus, we have for each j , there are

Multiple Choice:

- (a) $\left\lfloor \frac{jp}{q} \right\rfloor$ ✓
- (b) $\left\lfloor \frac{jq}{p} \right\rfloor$

lattice points in OPC . Then $N_1 =$

Multiple Choice:

- (a) $\sum_{j=1}^2 \left\lfloor \frac{jp}{q} \right\rfloor$ ✓

$$(b) \sum_{j=1}^2 \left\lfloor \frac{jq}{p} \right\rfloor$$

To find N_2 , we use a similar counting method on OAM . Now, we count the lattice points on $x = j$ for $j = 1, 2, \dots, \frac{p-1}{2}$. Thus, for each j , we want the number of nonnegative integers less than

Multiple Choice:

$$(a) \frac{jp}{q}$$

$$(b) \frac{jq}{p} \quad \checkmark$$

Thus, we have for each j , there are

Multiple Choice:

$$(a) \left\lfloor \frac{jp}{q} \right\rfloor$$

$$(b) \left\lfloor \frac{jq}{p} \right\rfloor \quad \checkmark$$

lattice points in OPC . Then $N_2 =$

Multiple Choice:

$$(a) \sum_{j=1}^2 \left\lfloor \frac{jp}{q} \right\rfloor$$

$$(b) \sum_{j=1}^2 \left\lfloor \frac{jq}{p} \right\rfloor \quad \checkmark$$

From the previous Lemma, $\left(\frac{p}{q}\right) = (-1)^{N_1}$ and $\left(\frac{q}{p}\right) = (-1)^{N_2}$. Thus,

$$\begin{aligned} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) &= (-1)^{N_1} (-1)^{N_2} \\ &= (-1)^{N_1 + N_2} \\ &= (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \end{aligned}$$

with the result from the participation assignment. ■

Quadratic reciprocity

Quadratic reciprocity means that determining all quadratic residues (perfect squares) modulo an odd prime is a finite problem. In terms of Legendre symbol, this is finding all a where $\left(\frac{a}{p}\right) = 1$ for a given p . For example, when $p = 11$, we can check all positive integers a . However, what about the reverse? Quadratic reciprocity allows us to find all odd primes p where $\left(\frac{11}{p}\right) = 1$, even though there are infinitely many odd primes. This idea is the last homework problem.