

Quadratic reciprocity

Introducing quadratic reciprocity.

We are going to explore the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$. Let's look at an example:

Question 1 We want to know if 3 is a quadratic residue modulo 107. It would be a lot easier to check if 107 is a quadratic residue modulo 3. We know that $107 \equiv \boxed{2} \pmod{3}$, so $\left(\frac{107}{3}\right) = \boxed{-1}$. It would be nice if this also gave us $\left(\frac{3}{107}\right)$.

Question 2 Another example: Find $\left(\frac{p}{5}\right)$ and $\left(\frac{5}{p}\right)$.

| p | 3 | 5 | 7 | 11 | 13 |
|----------------------------|--------------|-------------|--------------|-------------|--------------|
| $\left(\frac{p}{5}\right)$ | $\boxed{-1}$ | $\boxed{0}$ | $\boxed{-1}$ | $\boxed{1}$ | $\boxed{-1}$ |
| $\left(\frac{5}{p}\right)$ | -1 | 0 | -1 | 1 | -1 |

Question 3 Another example: Find $\left(\frac{p}{7}\right)$ and $\left(\frac{7}{p}\right)$.

| p | 3 | 5 | 7 | 11 | 13 |
|----------------------------|--------------|--------------|---|-------------|--------------|
| $\left(\frac{p}{7}\right)$ | $\boxed{-1}$ | $\boxed{-1}$ | 0 | $\boxed{1}$ | $\boxed{-1}$ |
| $\left(\frac{7}{p}\right)$ | $\boxed{1}$ | $\boxed{-1}$ | 0 | -1 | -1 |

This gives some evidence for our theorem:

Theorem 1. Let p and q be odd primes with $p \neq q$.

- if $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

Learning outcomes:
Author(s):

Quadratic reciprocity

- if $p \equiv q \equiv 3 \pmod{4}$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Our goal for Friday is to prove this.