The Law of Quadratic Reciprocity

Theorem 11.7: The Law of Quadratic Reciprocity

Let p and q be distinct odd primes. Then

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

Proof: Exercise

ex: Let $p = 7$ and $q = 17$. Then

$$\left(\frac{7}{17}\right)\left(\frac{17}{7}\right) = (-1)^{\frac{6}{2}\cdot\frac{16}{2}} = 1$$

We can use Euler's criterion or Gauss's lemma to find $\left(\frac{7}{17}\right)$ or $\left(\frac{17}{7}\right)$.
Let's use Gauss's lemma to find $\left(\frac{7}{17}\right)$.

$\frac{17-1}{2} = 8$

Consider 7, 14, 21, 28, 35, 42, 49, 56.
The least positive residues modulo 17 are

7, 14, 4, 11, 1, 8, 15, 5

Only 3 of these are greater than 17/2.
(They are 14, 11 and 15).

$\therefore \left(\frac{7}{17}\right) = (-1)^3 = -1 \quad \therefore \left(\frac{17}{7}\right) = -1$