Recall: let p be an odd prime. Then

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

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Question: let p, q be odd primes, what is $\left(\frac{p}{q}\right)$?

Theorem 22.1. (Quadratic Reciprocity) Let p, q be distinct odd primes, then

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

Remark: (1) If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then

$\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even.

Therefore, $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

(2) If $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, then

$\frac{p-1}{2} \cdot \frac{q-1}{2}$ is odd

Therefore, $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = -1 \Rightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

Example: Find $\left(\frac{7}{137}\right)$

Solution: $7 \equiv 3 \pmod 4$, $\quad 137 \equiv 1 \pmod 4$

By quadratic reciprocity, $\left(\frac{7}{137}\right) = \left(\frac{137}{7}\right)$

$$137 = 7 \cdot 19 + 4 \Rightarrow \left(\frac{137}{7}\right) = \left(\frac{4}{7}\right)$$

Notice that $4 = 2^2 \equiv 2^2 \pmod 7 \Rightarrow \left(\frac{4}{7}\right) = 1$

Therefore $\left(\frac{7}{137}\right) = 1$. $\square$

Next, we define the following symbol: let a be an integer

Then by the primary factorization,

$$a = p_1 p_2 \cdots p_r \quad (p_i \text{ might be same})$$

Then we define (let p be an odd prime)

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right) \cdots \left(\frac{p_r}{p}\right).$$

Example: Find $\left(\frac{55}{179}\right)$

$$\left(\frac{55}{179}\right) = \left(\frac{5}{179}\right) \cdot \left(\frac{11}{179}\right)$$

$5 \equiv 1 \pmod 4$
$11 \equiv 3 \pmod 4$
$179 \equiv 3 \pmod 4$

$$= \left(\frac{179}{5}\right) \cdot (-1) \cdot \left(\frac{179}{11}\right)$$

$179 = 5 \cdot 35 + 4 \qquad \left(\frac{179}{5}\right) = \left(\frac{4}{5}\right) = 1.$

$179 = 11 \cdot 16 + 3 \qquad \left(\frac{179}{11}\right) = \left(\frac{3}{11}\right)$

$3 \equiv 3 \pmod 4$
$11 \equiv 3 \pmod 4$

$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1 \qquad 11 = 3 \cdot 3 + 2)$

$$\Rightarrow \left(\frac{55}{179}\right) = \left(\frac{179}{5}\right) \cdot (-1) \cdot \left(\frac{179}{11}\right)$$

$$= 1 \cdot (-1) \cdot 1 = -1. \qquad \square.$$

Moreover, let a, b be odd positive integers.

We can write $a = p_1 p_2 \cdots p_r$

$b = q_1 q_2 \cdots q_s$

$\boxed{\text{Indeed, } a \text{ can take value } -1 \text{ or } 2}$

We define the Jacobi symbol:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right) \cdots \left(\frac{a}{q_s}\right)$$

$$= \left(\frac{p_1}{q_1}\right)\left(\frac{p_2}{q_1}\right) \cdots \left(\frac{p_r}{q_1}\right) \cdots \left(\frac{p_r}{q_s}\right)$$

$$= \prod_{\substack{1 \le i \le r \\ 1 \le j \le s}} \left(\frac{p_i}{q_j}\right)$$

Theorem 22.2 (Generalized Law of Quadratic reciprocity)

Let a, b be <u>odd</u> <u>positive</u> integers,

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

$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1, 7 \pmod 8 \\ -1 & \text{if } b \equiv 3, 5 \pmod 8 \end{cases}$$

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

Remark: the proof is an application of the original version.

Here we only do one simple example:

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

Proof: We write b as its primary deconposition

Furthermore, we rearrange the primes of b such that:

$$b = \underbrace{p_1 p_2 \cdots p_r}_{p_i \equiv 1 \pmod 4} \underbrace{q_1 \cdots q_s}_{q_i \equiv 3 \pmod 4}$$

Exercise: if s is even, then $b \equiv 1 \pmod 4$

if s is odd, then $b \equiv 3 \pmod 4$.

Case I: s is even $\Rightarrow b \equiv 1 \pmod 4$

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) \cdot \left(\frac{-1}{q_1}\right) \cdots \left(\frac{-1}{q_s}\right)$$

$$= (1)^r \cdot (-1)^s = 1 \qquad (s \text{ even})$$

$$= (-1)^{\frac{b-1}{2}} \qquad (b \equiv 1 \pmod 4)$$

Case II: s is odd $\Rightarrow b \equiv 3 \pmod 4$

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) \cdot \left(\frac{-1}{q_1}\right) \cdots \left(\frac{-1}{q_s}\right)$$

$$= (1)^r \cdot (-1)^s = -1 \qquad (s \text{ odd})$$

$$= (-1)^{\frac{b-1}{2}} \qquad (b \equiv 3 \pmod 4) \qquad \square.$$

History: (1) Euler and Lagrange were the first to formulate the Law of Quadratic Reciprocity.

(2) Gauss gave the first proof in 1801.

During his life, he found 7 different proofs.

(3) We will give a proof due to Eisenstein.

(4) The quadratic reciprocity was subsumed into

the Class Field Theory developed by Hilbert, Artin and others from 1890s through 1920s and 1930s.

(5) During 1960s and 1970s, a number of mathematicians formulated a series of conjectures that vastly generaliz Class Field Theory and that today go by the name of the Langlands Program.

- The fundamental theorem proved by Wiles in 1995 is a small piece of the Langlands Program, yet it sufficed to solve Fermat's 350-year-old "Last Theorem."