The Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR mod } p \\ -1 & \text{if } a \text{ is a QNR mod } p \end{cases}$$

QR = non-zero square
QNR = non-zero non-square

Properties

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

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$ "Euler's Criterion"

Reciprocity

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

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

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

Example.

$$\left(\frac{55}{103}\right) = \left(\frac{5}{103}\right)\cdot\left(\frac{11}{103}\right) \quad \text{multiplicativity}$$

$$= \left(\frac{103}{5}\right)\cdot\left(\frac{103}{11}\right)\cdot(-1) \quad \text{Q. Recip.}$$

$103 \equiv 3 \pmod 4$
$5 \equiv 1 \pmod 4$
$11 \equiv 3 \pmod 4$

$$= \left(\frac{3}{5}\right)\cdot\left(\frac{4}{11}\right)\cdot(-1) \quad \text{reduce mod bottom}$$

$$= \left(\frac{-2}{5}\right)\cdot 1\cdot(-1) \quad \begin{array}{l}4 \text{ is a square} \\ 3 \equiv -2 \bmod 5\end{array}$$

$$= \left(\frac{-1}{5}\right)\cdot\left(\frac{2}{5}\right)\cdot(-1) \quad \text{multiplicativity}$$

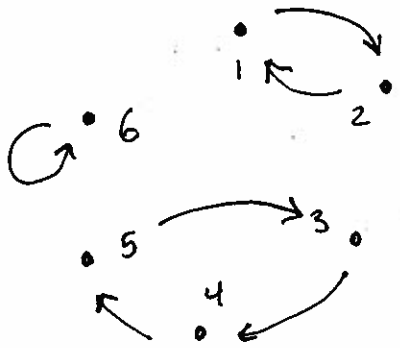
$$= 1\cdot(-1)\cdot(-1) \quad \text{recip. for } -1 \text{ and } 2$$

$$= 1$$

Check: $40^2 \equiv 55 \pmod{103}$

The sign of a permutation

x	1	2	3	4	5	6
$f(x)$	2	1	4	5	3	6



Braid Representation:

1 2 3 4 5 6

2 1 3 4 5 6

2 1 4 3 5 6

2 1 4 5 3 6

Inversions:

(s,t)	$(f(s), f(t))$
$(1,2)$	$(2,1)$
$(3,5)$	$(4,3)$
$(4,5)$	$(5,3)$

$$Sgn(f) = (+1)(-1)(+1) = -1$$

$$sgn(f) = (-1)^{\#\text{ of transpositions}} = (-1)^3 = -1$$

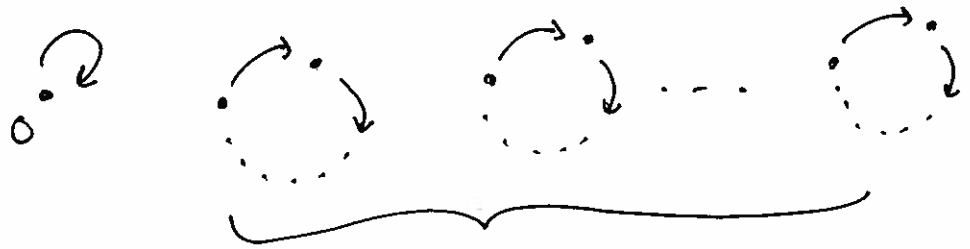
$$sgn(f) = (-1)^{\#\text{ of inversions}} = (-1)^3 = -1$$

Zolotarev's Lemma

Let p be an odd prime.
Let a be coprime to p.

Then $\left(\frac{a}{p}\right) = \operatorname{sgn}\left(x \mapsto ax \bmod p\right)$

Pf



c cycles of length ℓ ; $\ell \cdot c = p-1$

Case 1: c is even

① $\operatorname{sgn}(x \mapsto ax) = \left((-1)^{\ell+1}\right)^c = 1$

② $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (a^\ell)^{c/2} \equiv 1^{c/2} \equiv 1$

$\Rightarrow \left(\frac{a}{p}\right) = \operatorname{sgn}(x \mapsto ax)$

Case 2: c is odd $\Rightarrow \ell$ is even

① $\operatorname{sgn}(x \mapsto ax) = \left((-1)^{\ell+1}\right)^c = -1$

② Let $b \equiv a^{\ell/2} \pmod{p}$

$\Rightarrow b^2 \equiv 1, \; b \not\equiv 1.$

$\Rightarrow b \equiv -1.$

So

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (a^{\ell/2})^c \equiv b^c \equiv (-1)^c \equiv -1.$$

$$\Rightarrow \left(\frac{a}{p}\right) = \operatorname{sgn}(x \mapsto ax)$$

□

Theorem. Let p, q be odd primes, distinct.

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

Pf. $S = \{1, 2, \ldots, pq-1\}$.

Notation: For $0 \le a \le p-1$, $0 \le b \le q-1$

① $[a,b] = s \in S$ s.t. $\begin{cases} s \equiv a \pmod p \\ s \equiv b \pmod q \end{cases}$

② $\langle a,b] = aq + b \in S$

③ $[a,b\rangle = a + bp \in S$

[a,b] → ↓	0	1	2	3	4
0	⟨0,0] [0,0⟩ 0	⟨2,0] [1,1⟩ 6	⟨4,0] [2,2⟩ 12	⟨1,0] [3,0⟩ 3	⟨3,0] [4,1⟩ 9
1	⟨3,1] [0,2⟩ 10	⟨0,1] [1,0⟩ 1	⟨2,1] [2,1⟩ 7	⟨4,1] [3,2⟩ 13	⟨1,1] [4,0⟩ 4
2	⟨1,2] [0,1⟩ 5	⟨3,2] [1,2⟩ 11	⟨0,2] [2,0⟩ 2	⟨2,2] [3,1⟩ 8	⟨4,2] [4,2⟩ 14

$p = 5$

$1 \cdot 3 + 1 = 4$

$4 \cdot 3 + 2 = 14$

$q = 3$

Define:

$$\alpha([a,b]) = \langle a,b]$$

e.g. $\alpha(12) = \alpha([2,0]) = \langle 2,0] = 6$

$$\beta([a,b]) = [a,b\rangle$$

e.g. $\beta(12) = \beta([2,0]) = [2,0\rangle = 2$

$$\gamma(\langle a,b]) = [a,b\rangle$$

e.g. $\gamma(12) = \gamma(\langle 4,0]) = [4,0\rangle = 4$

Relationship:

$$\gamma \circ \alpha = \beta$$

(Since $\gamma \circ \alpha([a,b]) = \gamma(\langle a,b]) = [a,b\rangle$)

Claim: $\operatorname{sgn}(\alpha) = \left(\frac{q}{p}\right)$ and $\operatorname{sgn}(\beta) = \left(\frac{p}{q}\right)$

Why?

① α permutes each row independently

$$\left(\begin{array}{l} [a,b] \text{ as } a \text{ varies} = b^{th} \text{ row} \\ \langle a,b] \text{ as } a \text{ varies} = b^{th} \text{ row} \end{array} \right)$$

② In b^{th} row:

a^{th} position $= [a,b]$

$$\alpha(a^{th} \text{ position}) = \alpha([a,b]) = \langle a,b] = aq + b$$

So:

$$\operatorname{sgn}(\alpha \text{ on } b^{th} \text{ row}) \quad \text{(one big odd cycle or identity)}$$

$$= \operatorname{sgn}\left((x \xrightarrow[\text{mod } p]{} x+b) \right) \operatorname{sgn}\left((x \xrightarrow[\text{mod } p]{} qx) \right)$$

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

So $\operatorname{sgn}(\alpha) = \left(\frac{q}{p}\right)^{q} = \left(\frac{q}{p}\right)$. ($q$ ← # q rows)

Claim: $\operatorname{sgn}(\gamma) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Why? $\gamma(aq+b) = a + pb$

Let $x, x' \in S$.

$x = aq+b$

$x' = a'q+b'$

Then $x < x' \iff \left(a<a' \text{ OR } \begin{cases} a=a' \\ b<b' \end{cases}\right)$

$\gamma(x) = a + bp$

$\gamma(x') = a' + b'p$

Then $\gamma(x) > \gamma(x') \iff \left(b>b' \text{ OR } \begin{cases} b=b' \\ a>a' \end{cases}\right)$

So inversion $\iff \begin{cases} a<a' \\ b'<b \end{cases}$

$\leftarrow \frac{p(p-1)}{2}$ way

$\leftarrow \frac{q(q-1)}{2}$ way

Hence

$$\operatorname{sgn}(\gamma) = (-1)^{\operatorname{Inv}(\gamma)} = (-1)^{p\cdot\frac{p-1}{2}\cdot q\cdot\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Summary:

$$\mathrm{sgn}(\alpha) = \left(\frac{q}{p}\right) \qquad \mathrm{sgn}(\beta) = \left(\frac{p}{q}\right)$$

$$\mathrm{sgn}(\gamma) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$\gamma \circ \alpha = \beta$$

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