A finite set S can be identified with a subset of positive numbers by numbering its elements. "linear order" = a bijection from S to $\{1, 2, \cdots, n\}$

$$S = \{a_1, a_2, \cdots, a_n\} \xrightarrow{\sim} \{1, 2, \cdots, n\}$$

e.g. : $a_i \mapsto i$

Defn. Let f be a permutation of S (identified with $\{1, 2, \cdots, n\}$)

An **inversion** of f is a pair (a, b) in S s.t.

$$a < b \quad \text{and} \quad f(a) > f(b).$$

Then $\text{inv}(f) :=$ # inversions of f.

e.g. $S = \{\pi, \mathbb{C}, \text{today}\}$

$\{1, 2, 3\}$

f: $\pi \to \text{today}$, $\text{today} \to \mathbb{C}$, $\mathbb{C} \to \pi$

$(\pi, \mathbb{C})$ is an inversion!

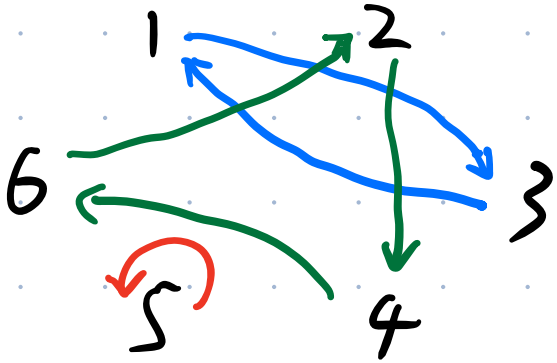
$(\pi, \mathbb{C})$ $\quad \pi < \mathbb{C}$

$1 \quad 2 \qquad 1 < 2$

$(\text{today}, \mathbb{C})$ $\quad \text{today} > \mathbb{C}$

$3 \quad 2 \qquad 3 > 2$

E.g. $S = \{1, 2, 3, 4, 5, 6\}$



f

Fill in $(f(a), f(b))$ for $1 \le a < b \le 6$

a \ b	2	3	4	5	6
1	(3,4)	(3,1)	(3,6)	(3,5)	(3,2)
2		(4,1)	(4,6)	(4,5)	(4,2)
3			(1,6)	(1,5)	(1,2)
4				(6,5)	(6,2)
5					(5,2)

$\neg$ "$a < b$"

Find all inversions of f

$\text{inv}(f) = 7$

Goal: To show $\operatorname{sign}(f) = (-1)^{\operatorname{inv}(f)}$.

Defn. Let τ be a transposition of S (identified with $\{1, 2, \cdots, n\}$).

Then τ is called an **adjacent transposition** if it switches 2 **consecutive** numbers.

E.g. $S = \{1, 2, 3, 4, 5, 6\}$

$(1\ 2)$ switching 1 & 2 is an adjacent transposition.

$(1\ 6)$ switching 1 & 6 is NOT an adjacent transposition.

Q: How the inversion changes when composite with an adjacent transposition.

Lemma: Let f be a permutation of $\{1, 2, \cdots, n\}$ and $\tau = (a\ a+1)$.

Then
$$\mathrm{inv}(\tau \circ f) - \mathrm{inv}(f) = \begin{cases} 1 & \text{if } f^{-1}(a) < f^{-1}(a+1) \\ -1 & \text{if } f^{-1}(a) > f^{-1}(a+1) \end{cases}$$

Proof. Let (s, t) be a pair s.t. $1 \le s < t \le n$.

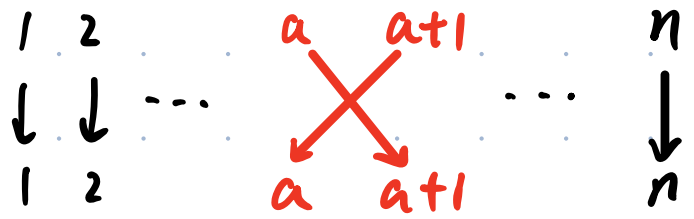
Then (s,t) is an inversion of $\tau \circ f \iff \tau(f(s)) > \tau(f(t))$.

So we consider the set $\{f(s), f(t)\}$. $\begin{cases} \{f(s), f(t)\} = \{a, a+1\} \\ \{f(s), f(t)\} \neq \{a, a+1\} \end{cases}$

two cases:

1) $\{f(s), f(t)\} \neq \{a, a+1\}$.

Then τ does not change the order relation between $f(s)$ and $f(t)$.



$f(s) < f(t) \Rightarrow \tau f(s) < \tau f(t) \quad | \quad f(s) > f(t) \Rightarrow \tau f(s) > \tau f(t)$

$s < t$

2) $\{f(s), f(t)\} = \{a, a+1\}$.

2.1) $\begin{cases} f(s) = a \\ f(t) = a+1 \end{cases}$ Then $\begin{cases} \tau(f(s)) = a+1 \\ \tau(f(t)) = a \end{cases}$

$f(s) < f(t)$ $\quad$ $\tau \circ f(s) > \tau \circ f(t)$

(s,t) is NOT an inversion of f $\quad$ (s,t) is an inversion of $\tau \circ f$

2.2) $\begin{cases} f(s) = a+1 \\ f(t) = a \end{cases}$ Then $\begin{cases} \tau(f(s)) = a \\ \tau(f(t)) = a+1 \end{cases}$

$f(s) > f(t)$ $\quad$ $\tau \circ f(s) < \tau \circ f(t)$

(s,t) is an inversion of f $\quad$ (s,t) is NOT an inversion of $\tau \circ f$

Conclusion:

$$\text{inv}(\tau \circ f) - \text{inv}(f) = \begin{cases} 1 & \text{if } f^{-1}(a) < f^{-1}(a+1) \\ -1 & \text{if } f^{-1}(a) > f^{-1}(a+1) \end{cases}$$

Decompose ordered sets & permutations

- Suppose we have a finite set S and a decomposition:

$$S = S_1 \cup S_2 \cup \cdots \cup S_t$$

- Suppose we have a permutation f and a decomposition:

$$f = f_1 \circ f_2 \circ \cdots \circ f_t$$

- Suppose each f_i fixes all elements NOT in S_i.

We fix an identification $S \xrightarrow{\sim} \{1, 2, \cdots, n\}$

For each $S_i \subseteq S$, saying its image is $\{a_1, a_2, \cdots, a_{m_i}\}$

and suppose $a_1 < a_2 < \cdots < a_{m_i}$. Then further identify S_i with $\{1, 2, \cdots, m_i\}$.

Now, we have TWO versions of $\mathrm{inv}(f_i)$:

1) The one view f_i as a permutation of S and use the identification $S \xrightarrow{\sim} \{1, 2, \cdots, n\}$.

2) The one view f_i as a permutation of S_i and use the identification $S_i \xrightarrow{\sim} \{1, 2, \cdots, m_i\}$.

They coincide!

Indeed, since f_i fixes all elements NOT in S_i, (s,t) is an inversion of f_i in the first sense $\Leftrightarrow$ $s, t \in S_i$ and $\begin{cases} f_i(s) > f_i(t) \\ s < t \end{cases} \Leftrightarrow (s,t)$ is an inversion of f_i in the second sense.

Lemma. Any permutation f of a finite set S (identified with $\{1,2,\cdots,n\}$) can be written as the composition of $\text{inv}(f)$ adjacent transpositions.

Recall: $(123\cdots n) = (12)(23)\cdots(n-1\ n)$

Proof: Induction on $\text{inv}(f)$:

Base: $\text{inv}(f) = 0$, namely f preserves the order. Then f has to be id_S.

And id_S is the composition of 0 adjacent transpositions.

Now, suppose $\text{inv}(f) > 0$. The $f \neq id_S$ and $\exists\, a \in S$ s.t.

$$f^{-1}(a) > f^{-1}(a+1)$$

Then by the previous lemma,

$$\text{inv}((a\ a+1) \circ f) = \text{inv}(f) - 1.$$

By induction hypothesis, $(a\ a+1) \circ f$ is the composition of

$\text{inv}(f) - 1$ adjacent transpositions.

Then $f = (a \;\; a+1) \circ (a \;\; a+1) \circ f$

$= (a \;\; a+1) \circ ((a \;\; a+1) \circ f)$

↓ one adj. transp. ↘ composition of $\mathrm{inv}(f) - 1$ adj. transp.s

□

Thm. (3rd Defn of sign)

Let f be a permutation of a finite set S (identified with $\{1, 2, \cdots, n\}$).

Then $$\mathrm{Sign}(f) = (-1)^{\mathrm{inv}(f)}$$

Proof: By the previous lemma,

f is the composition of $\mathrm{inv}(f)$ adjacent transpositions.

By 2nd defn of sign, $\mathrm{Sign}(f) = (-1)^{\mathrm{inv}(f)}$.

□

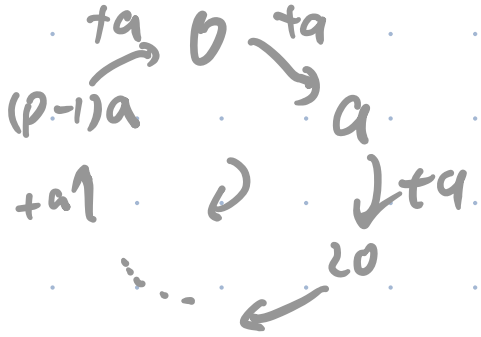
Back to Number Theory (from Algebra)

Let p be an odd prime number.

$$\boxed{+a \bmod p} : \mathbb{Z}/p \longrightarrow \mathbb{Z}/p$$

$$\bar{x} \longmapsto \overline{x+a}$$

This is a permutation. (why?)



Prop. $\operatorname{Sign}\left(\underbrace{\boxed{+a \bmod p}}_{\text{"}f\text{"}}\right) = 1.$

Proof: If $a \equiv 0 \bmod p$, then f is id. Thus $\operatorname{sign}(f) = 1$

If $a \not\equiv 0 \bmod p$, then a is mult. invertible and thus

$$\{\bar{0}, \bar{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$$

must be the entire $\mathbb{Z}/p$. Hence, f is a cyclic permutation of length p.

$$\Rightarrow \operatorname{sign}(f) = (-1)^{\overbrace{p-1}^{\text{even.}}} = 1$$

Let $f : S \to S$ be one of the following:

1) $\boxed{\cdot a \bmod p} : \Phi(p) \longrightarrow \Phi(p)$

$$\overline{x} \longmapsto \overline{x \cdot a}$$

2) $\boxed{\cdot a \bmod p} : \mathbb{Z}/p \longrightarrow \mathbb{Z}/p$

$$\overline{x} \longmapsto \overline{x \cdot a}$$

Then we know that f is a permutation.

Since $\boxed{\cdot a \bmod p}$ is bijective when a is mult. invertible.

Zolotarev's Lemma.

$$\text{Sign}(\boxed{\cdot a \bmod p}) = \left(\frac{a}{p}\right)$$

Proof: First, we may only consider 1) since in 2), $\bar{0} \longmapsto \bar{0}$ contributes factor 1 to the sign and hence f in 1) & 2) have the same sign.

recall:
- $\ell(a)$ = length of each cycle in the dynamics of $\boxed{\cdot a \bmod p}$
- $c(a)$ = number of cycles in the dynamics of $\boxed{\cdot a \bmod p} \cong f$

Then, $\ell \cdot c = p - 1$. (which is even)

By the 1st defn of sign,

$$(\ell-1)\cdot c = \underbrace{\ell \cdot c}_{\text{even}} - c \equiv c \bmod 2$$

$$\text{Sign}(f) = ((-1)^{\ell-1})^c = (-1)^c.$$

Divide into two cases: c even or odd.

a) If c is even, then $\text{sign}(f) = 1$ and

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{l \cdot \frac{c}{2}} = (a^l)^{\frac{c}{2}} \equiv 1^{\frac{c}{2}} = 1 \bmod p$$

Euler's Thm

↑ bec. c is even

b) If c is odd, then $\text{sign}(f) = -1$.

Since $l \cdot c = p - 1$ is even and c is odd, l has to be even.

Then let b = nat. repn. of $a^{l/2} \bmod p$

Now, $b^2 \equiv a^l \equiv 1 \bmod p \Rightarrow b \equiv \pm 1 \bmod p$

But the defn of $l \Rightarrow b \not\equiv 1 \bmod p$

$\Rightarrow b \equiv -1 \bmod p$.

Now, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^c \equiv (-1)^c = -1 \bmod p$.

In either case, $\text{sign}(f) = \left(\frac{a}{p}\right)$

Back to Quadratic Reciprocity law:

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \quad \text{where } p^* := (-1)^{\frac{p-1}{2}} \cdot p$$

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

Plan: Find permutations α, β, γ s.t.

$$\text{Sign}(\alpha) = \left(\frac{q}{p}\right)$$

$$\text{Sign}(\beta) = \left(\frac{p}{q}\right)$$

$$\text{Sign}(\gamma) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

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

$$\text{Sign}(\alpha) = \text{Sign}(\gamma) \cdot \text{Sign}(\beta)$$

Let $S = \{0, 1, \cdots pq-1\}$ the nat. reprs of $\mathbb{Z}/_{pq}$

$[a,b]$:= the unique inter in S congruent to a mod p and b mod q.

$\langle a,b] := aq + b$. $\quad \langle a,b] \equiv [a,b]$ mod q

$[a,b\rangle := a + bp$. $\quad [a,b\rangle \equiv [a,b]$ mod p

Every element in S can be uniquely expressed in each notation. (why?)

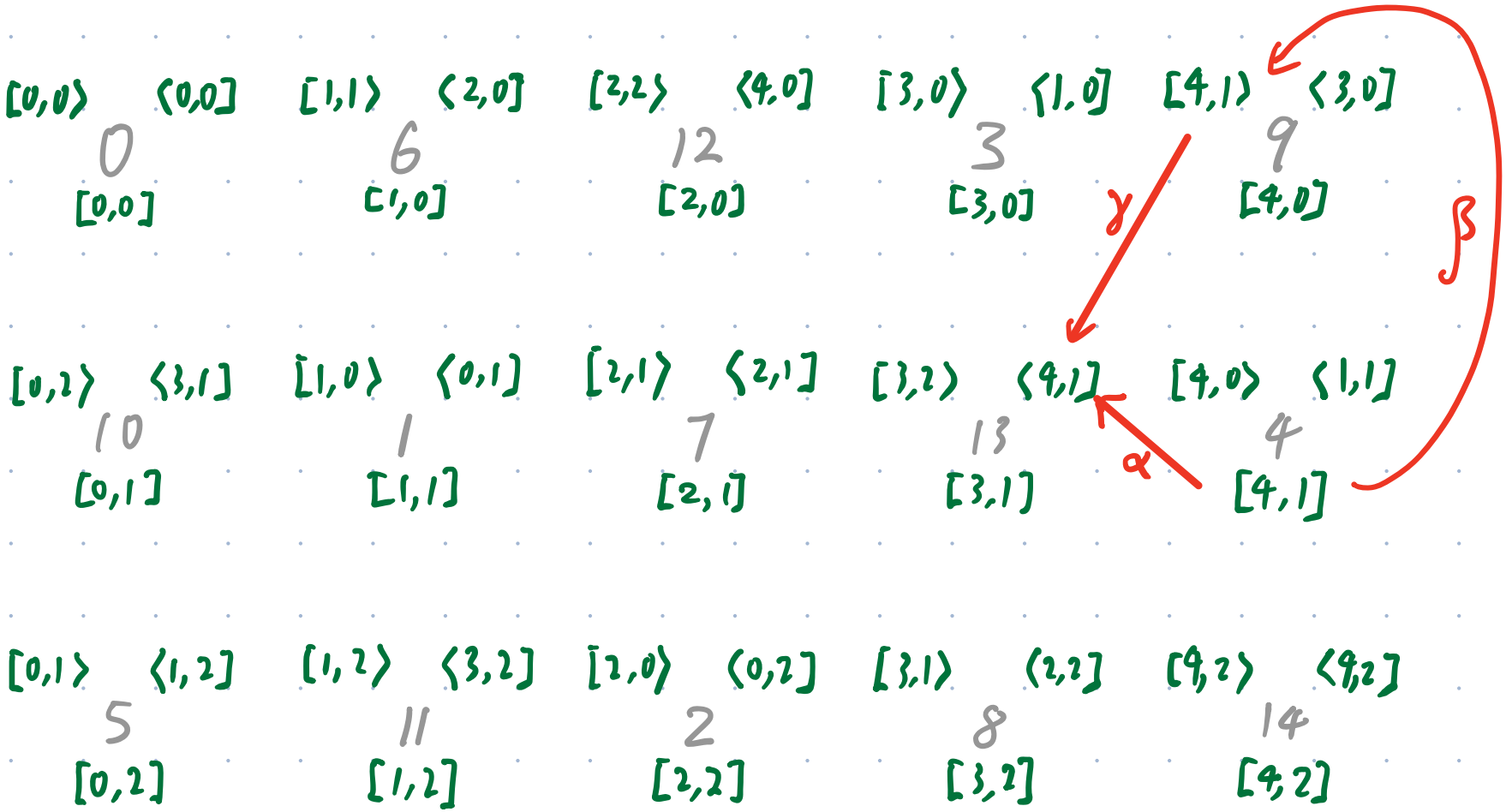
α: send each $[a,b]$ to $\langle a,b]$

β: send each $[a,b]$ to $[a,b\rangle$

γ: send each $[a,b\rangle$ to $\langle a,b]$

Permutations of S satisfying $\alpha = \gamma \circ \beta$

E.g. $p = 5$, $q = 3$

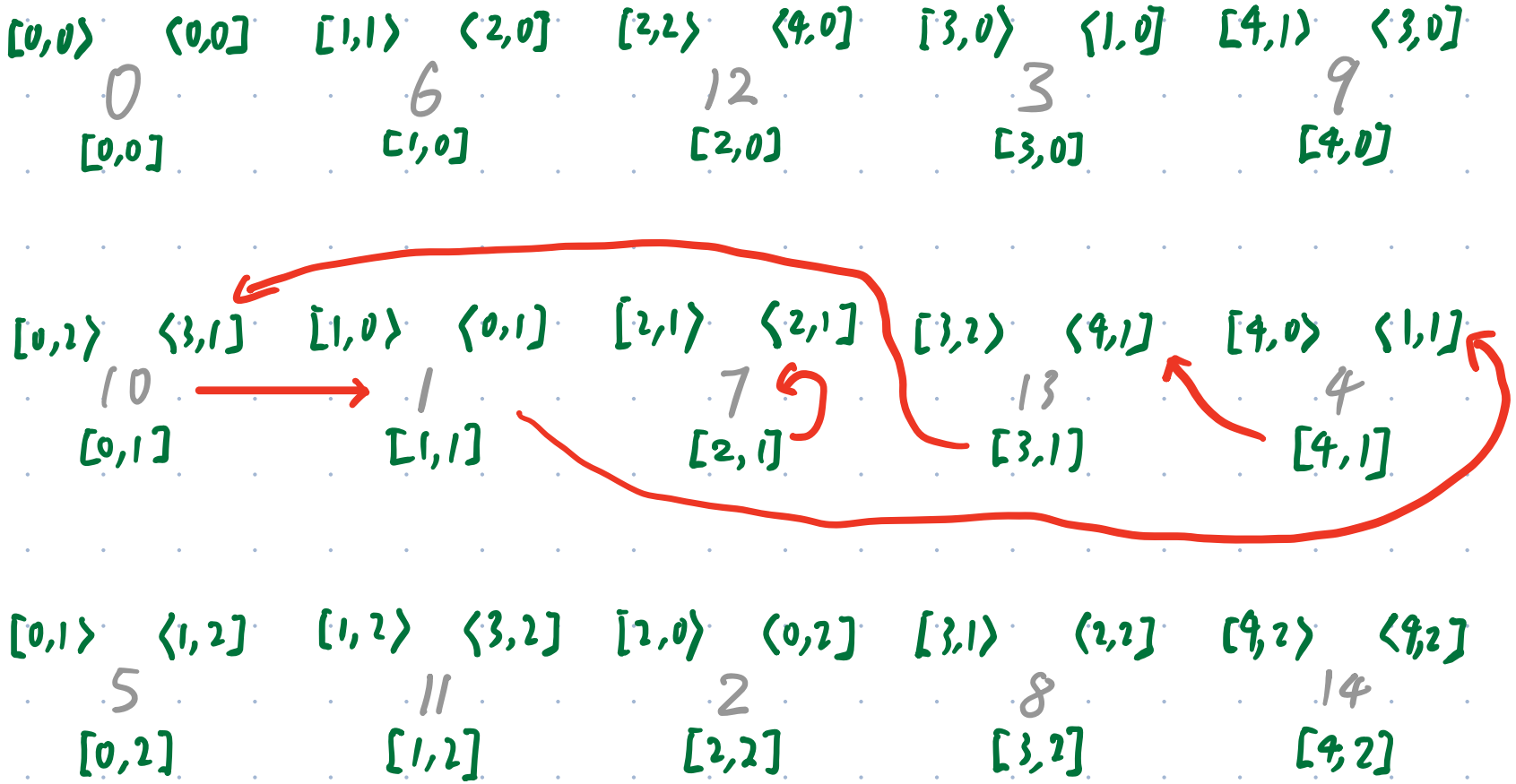


arranged into p columns and q rows, as determined by CRT.

Lemma. $\text{sign}(\alpha) = \left(\frac{q}{p}\right)$ $\text{sign}(\beta) = \left(\frac{p}{q}\right)$

Proof: We will prove the first, the second follows in similar argument.

Rearrange elements of S into p columns and q rows according to $[*,*]$.



More precisely, an element $n \in S$ is

- in the column $[a, -]$ iff $n \equiv a \bmod p$
- in the row $[-, b]$ iff $n \equiv b \bmod q$

Note that: $\langle a,b] \equiv [a,b] \bmod q$

Hence, α, which maps each $[a,b]$ to $\langle a,b]$, maps each element to one in the SAME row.

Namely, if we restrict α to the row $[-,b]$, then it is also a permutation up that row. We can identify row b with $\mathbb{Z}/p$ by $[a,b] \mapsto \bar{a}$.

In the row b, each column a is maped to the column $aq + b \bmod p$.

Using words from $\mathbb{Z}/p$, α acts as $\bar{a} \longmapsto \overline{aq+b}$, which can be viewed as the composition of "$\overline{\times q}$" and "$\overline{+b}$".

We have $\alpha|_{\text{row } b} = \text{"} + b \bmod p \text{"} \circ \text{"} \times q \bmod p \text{"}$

Then $\text{Sign}(\alpha|_{\text{row } b}) = \text{Sign}(\text{"} + b \bmod p \text{"})\,\text{Sign}(\text{"} \times q \bmod p \text{"})$

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

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

Since we have q rows,

$$\text{Sign}(\alpha) = \text{Sign}(\alpha|_{\text{row } 0}) \cdots\cdots \text{Sign}(\alpha|_{\text{row } q-1})$$

$$= \left(\frac{q}{p}\right)^q$$

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

Lemma. $\mathrm{Sign}(\gamma) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Proof. We'll use the 3rd characterization of sign.

First, for any $x, x' \in S$, write $x = aq + b$ & $x' = a'q + b'$.

Then $x < x' \iff$ either $a < a'$

or $a = a'$ but $b < b'$ (*)

Now, we want to compare $\gamma(x)$ & $\gamma(x')$:

$\gamma(x) = a + bp$ v.s. $\gamma(x') = a' + b'p$

Then $\gamma(x) > \gamma(x') \iff$ either $b > b'$ (*')

or $b = b'$ but $a > a'$

Combine (*) & (*'), (x, x') is an inversion of $\gamma \iff a < a'$ & $b > b'$

$x < x'$ & $\gamma(x) > \gamma(x')$

The # of (a, a', b, b') s.t. $0 \le a < a' \le p-1$

and $0 \le b' < b \le q-1$

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

Hence, $inv(\gamma) = \frac{p-1}{2} \cdot \frac{q-1}{2}$. Then

$$Sign(\gamma) = (-1)^{inv(\gamma)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof of Quadratic Reciprocity Law:

$$\alpha = \gamma \circ \beta \Rightarrow Sign(\alpha) = Sign(\gamma)\, Sign(\beta)$$

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