Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 10, 2023

What we have seen last time:

- Quadratic Reciprocity Laws and
- Their applications

Today, we will move to the proof of the ***third quadratic reciprocity law***.

Theorem 23.1 (Third Quadratic Reciprocity Law)

Let p and q be two distinct odd prime numbers. Then

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

Proof. We will interpret $(\frac{p}{q})$, $(\frac{q}{p})$, and $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ as the signs of three permutations α, β, and γ respectively. The three permutations have the relation

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

Hence, $\mathrm{sign}(\gamma) = \mathrm{sign}(\beta) \cdot \mathrm{sign}(\alpha)$, which gives the desired formula. □

Permutations

Definition 23.2

A ***permutation*** of a set S is a bijection from S to itself.

E.g. the additive modular dynamics $\boxed{+a \pmod{m}}$ are permutations of $\mathbb{Z}/m$, and the multiplicative modular dynamics $\boxed{\cdot a \pmod{m}}$ are permutations of $\Phi(m)$.

Permutations

To prove the third quadratic reciprocity law, we consider the following set:

$$S = \{0, 1, \cdots, pq - 1\} = \{\text{natural representatives modulo } pq\}.$$

We introduce the following three label systems of its elements.

- $[a, b]$ = the unique element in S congruent to a modulo p and congruent to b modulo q respectively.
- $[a, b\rangle := a + bp$. Note that $[a, b\rangle \equiv [a, b] \pmod{p}$.
- $\langle a, b] := aq + b$. Note that $\langle a, b] \equiv [a, b] \pmod{q}$.

Now, we define permutations α, β, and γ as follows:

- α maps each $[a, b\rangle$ to $[a, b]$. $\qquad [a, b] \longleftarrow [a, b\rangle$
- β maps each $[a, b]$ to $\langle a, b]$. $\qquad \langle a, b] \longleftarrow [a, b]$
- γ maps each $[a, b\rangle$ to $\langle a, b]$. $\qquad \langle a, b] \longleftarrow [a, b\rangle$

Then it is clear that

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

as desired.

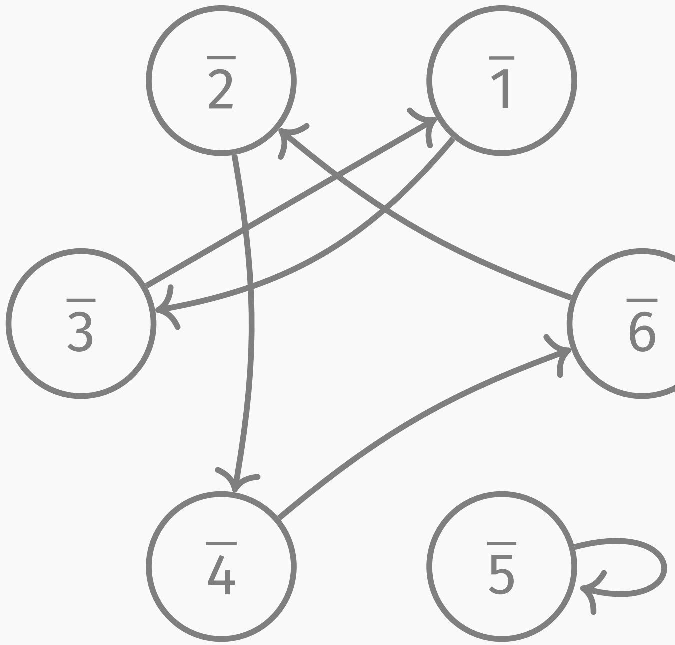
E.g. Let $p = 5$ and $q = 3$. We arrange elements of S in 5 columns and 3 rows according to the label system $[a, b]$.

$\langle 0,0]\ \ [0,0\rangle$ 0 $[0,0]$	$\langle 2,0]\ \ [1,1\rangle$ 6 $[1,0]$	$\langle 4,0]\ \ [2,2\rangle$ 12 $[2,0]$	$\langle 1,0]\ \ [3,0\rangle$ 3 $[3,0]$	$\langle 3,0]\ \ [4,1\rangle$ 9 $[4,0]$
$\langle 3,1]\ \ [0,2\rangle$ 10 $[0,1]$	$\langle 0,1]\ \ [1,0\rangle$ 1 $[1,1]$	$\langle 2,1]\ \ [2,1\rangle$ 7 $[2,1]$	$\langle 4,1]\ \ [3,2\rangle$ 13 $[3,1]$	$\langle 1,1]\ \ [4,0\rangle$ 4 $[4,1]$
$\langle 1,2]\ \ [0,1\rangle$ 5 $[0,2]$	$\langle 3,2]\ \ [1,2\rangle$ 11 $[1,2]$	$\langle 0,2]\ \ [2,0\rangle$ 2 $[2,2]$	$\langle 2,2]\ \ [3,1\rangle$ 8 $[3,2]$	$\langle 4,2]\ \ [4,2\rangle$ 14 $[4,2]$

Cycles in Permutations

Cycles in Permutations

E.g. consider $S = \{1, 2, 3, 4, 5, 6\}$ and the map f whose dynamic is displayed as left below.



We see that f consists of

- a cycle of length 1,
- a cycle of length 2, and
- a cycle of length 3.

"Permutations consist of cycles"

Definition 23.3

If a permutation consists of a cycle of length ℓ and all elements outside the cycle is fixed, then we say it is an ***ℓ-cycle***.

We use $(a_1 a_2 \cdots a_\ell)$ to denote the ℓ-cycle mapping

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_\ell \mapsto a_1.$$

If a permutation consists of multiple nontrivial cycles, we just put their notations together.

E.g. the permutation in previous slide is denoted by $(13)(246)$.

Note that every permutation consists of cycles.

Definition 23.4

The ***sign*** of a ℓ-cycle is $(-1)^{\ell-1}$. The ***sign*** of a permutation is the product of the signs of the cycles in it.

E.g. the sign of permutation in previous example is (13)(246)

$$(-1)^{3-1} \cdot (-1)^{2-1} = -1.$$

Example 23.5

Let p be an odd prime. Then the sign of the additive modular dynamic $\boxed{+a \pmod{p}} : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ is 1.

Proof. When $p \mid a$, $\boxed{+a \pmod{p}}$ is precisely the identity. Hence, its sign is 1.

When $p \nmid a$, by Theorem 13.6, $\boxed{+a \pmod{p}}$ is a p-cycle. Hence, its sign is $(-1)^{p-1} = 1$. □

odd − 1

Example 23.6

Let p be an odd prime and $a \in \Phi(p)$. Then the sign of the multiplicative modular dynamic $\boxed{\cdot a \pmod{p}} : \mathbb{F}_p \to \mathbb{F}_p$ is $\left(\frac{a}{p}\right)$.

Proof. First, since $\boxed{\cdot a \pmod{p}}$ maps $\bar{0}$ to $\bar{0}$, which is a trivial cycle, we may focus on the restriction of $\boxed{\cdot a \pmod{p}}$ to $\mathbb{F}_p^\times$, or equivalently on $\Phi(p)$.

Theorem 13.11 tells us that $\boxed{\cdot a \pmod{p}}$ consists of cycles of the same length. Let ℓ be the length and c be the number of cycles, namely $c = \frac{p-1}{\ell}$. Then we have

$$\operatorname{sign}\left(\boxed{\cdot a \pmod{p}}\right) = ((-1)^{\ell-1})^{c} = (-1)^{c},$$

where notice that $\ell \cdot c = p - 1$ is even.

If c is even, then we have $p-1 = \ell \cdot c$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = (a^{\ell})^{\frac{c}{2}} \equiv 1^{\frac{c}{2}} = 1 = \operatorname{sign}\left(\boxed{\cdot a \pmod{p}}\right) \pmod{p}.$$

If c is odd, then ℓ must have even since $\ell \cdot c = p - 1$ is even. Let b be the natural representative of $a^{\frac{\ell}{2}}$. Then $b^2 \equiv 1 \pmod{p}$. But the definition of ℓ tells us that $b \not\equiv 1 \pmod{p}$. Therefore, $b \equiv -1 \pmod{p}$. Hence,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = b^{c} \equiv (-1)^{c} = -1 = \operatorname{sign}\left(\boxed{\cdot a \pmod{p}}\right) \pmod{p}.$$

We thus conclude that $\operatorname{sign}\left(\boxed{\cdot a \pmod{p}}\right) = \left(\frac{a}{p}\right)$. □

Composition of permutations

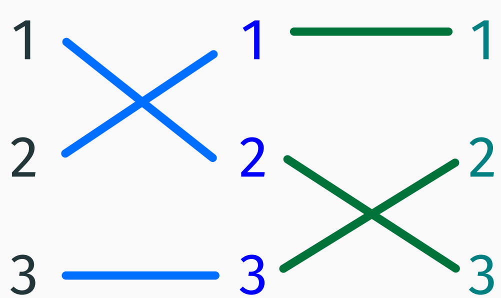
Lemma 23.7

If f and g are permutations of a set X, then so is $g \circ f$.

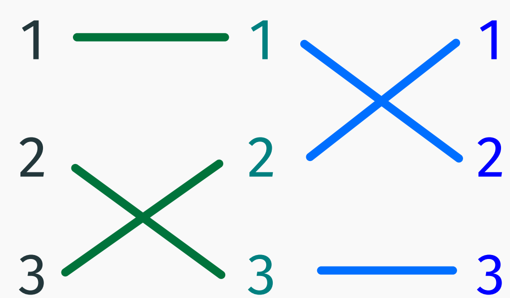
This lemma is clear. But please note that:

$$\text{in general,} \quad f \circ g \neq g \circ f.$$

E.g. Take $S = \{1, 2, 3\}$ and $f = (12)$, $g = (23)$.



$g \circ f = (132)$



$f \circ g = (123)$

Theorem 23.8

$$\mathrm{sign}(g \circ f) = \mathrm{sign}(g) \cdot \mathrm{sign}(f).$$

A special case of the theorem is clear: if a permutation f consists of cycles $C_1, \cdots, C_r$, then $\mathrm{sign}(f) = \mathrm{sign}(C_1) \cdots \mathrm{sign}(C_n)$.

We leave its proof to next time. Now, we apply it to show

Lemma 23.9

The signs of α and β are $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ respectively.

Proof of the lemma

Proof. We only prove the first. The second follows similarly.

We first arrange elements of S in p columns and q rows according to the label system $[a, b]$.

$\langle 0,0]\ \ [0,0\rangle$ 0 $[0,0]$	$\langle 2,0]\ \ [1,1\rangle$ 6 $[1,0]$	$\langle 4,0]\ \ [2,2\rangle$ 12 $[2,0]$	$\langle 1,0]\ \ [3,0\rangle$ 3 $[3,0]$	$\langle 3,0]\ \ [4,1\rangle$ 9 $[4,0]$
$\langle 3,1]\ \ [0,2\rangle$ 10 $[0,1]$	$\langle 0,1]\ \ [1,0\rangle$ 1 $[1,1]$	$\langle 2,1]\ \ [2,1\rangle$ 7 $[2,1]$	$\langle 4,1]\ \ [3,2\rangle$ 13 $[3,1]$	$\langle 1,1]\ \ [4,0\rangle$ 4 $[4,1]$
$\langle 1,2]\ \ [0,1\rangle$ 5 $[0,2]$	$\langle 3,2]\ \ [1,2\rangle$ 11 $[1,2]$	$\langle 0,2]\ \ [2,0\rangle$ 2 $[2,2]$	$\langle 2,2]\ \ [3,1\rangle$ 8 $[3,2]$	$\langle 4,2]\ \ [4,2\rangle$ 14 $[4,2]$

Proof of the lemma

Note that $[a,b\rangle \equiv [a,b] \pmod{p}$. Hence, α, which maps each $[a,b\rangle$ to $[a,b]$, maps from each column to itself.

Namely, if we restrict α to a column $[a,-]$ then it is a permutation of that column. Hence, $\mathrm{sign}(\alpha) = \prod_{a=0,\cdots,p-1} \mathrm{sign}\left(\alpha|_{[a,-]}\right)$

The column $[a,-]$ can be identified with $\mathbb{F}_q$ through the natural reduction modulo q:

$$[a,b] \longmapsto \overline{[a,b]} = \overline{b}.$$

Note that $[a,b\rangle$ is identified with $\overline{a+bp}$.

$$\underset{a+bp}{\overset{\parallel}{}}$$

Proof of the lemma

Therefore, $\alpha|_{[a,-]}$ is the inverse of the following permutation of $\mathbb{F}_q$:

$$\overline{b} \longmapsto \overline{a + bp},$$

which is the composition of $\boxed{+a \pmod{q}}$ and $\boxed{\cdot p \pmod{q}}$. Hence,

$$\begin{aligned} \operatorname{sign}(\alpha|_{[a,-]}) &= \operatorname{sign}\left(\alpha|_{[a,-]}^{-1}\right) \\ &= \operatorname{sign}\left(\boxed{+a \pmod{q}}\right) \cdot \operatorname{sign}\left(\boxed{\cdot p \pmod{q}}\right) \\ &= \left(\frac{p}{q}\right). \end{aligned}$$

Proof of the lemma

Therefore, we get

$$\mathrm{sign}(\alpha) = \prod_{a=0,\cdots,p-1} \mathrm{sign}\left(\alpha|_{[a,-]}\right) = \left(\frac{p}{q}\right)^{p} = \left(\frac{p}{q}\right),$$

here the last follows since p is odd.

A similar argument shows $\mathrm{sign}(\beta) = \left(\frac{q}{p}\right)$. $\square$

We have constructed permutations α, β, and γ such that

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

We have shown

$$\operatorname{sign}(\alpha) = \left(\frac{p}{q}\right) \qquad \text{and} \qquad \operatorname{sign}(\beta) = \left(\frac{q}{p}\right)$$

using Theorem 23.8.

It remains to

need 2nd characterization of sign.

- prove Theorem 23.8, and
- show that $\operatorname{sign}(\gamma) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

need 3rd char of sign.