Modular Dynamics focus on subsets of $\mathbb{Z}/m$.

- (Additive Modular Dynamics)

  Let m be a modulus, and a an integer. Consider

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

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

Prop. Let m be a modulus, and a an integer.

The dynamics of $\boxed{+a \bmod m}$ consists of $\underline{\gcd(a,m)}$ many cycles of the same length $\underline{\frac{\operatorname{lcm}(a,m)}{a}}$ (or $\frac{m}{\gcd(a,m)}$).

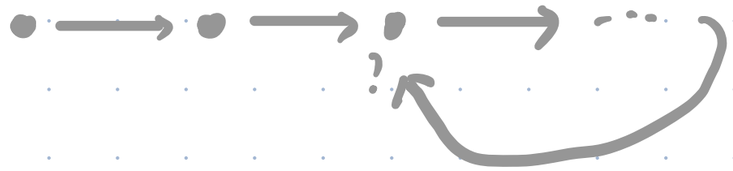
Pf: Suppose we start with $\overline{b} \in \mathbb{Z}/m$. Then

(*) $\overline{b} \longrightarrow \overline{b+a} \longrightarrow \overline{b+2a} \longrightarrow \cdots\cdots$

After k step, we get $\overline{b+ka}$.

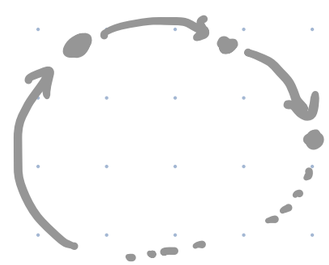
Since $\mathbb{Z}_m$ is a finite set, the set $\{\overline{b+ka} : k \geq 0\}$ is also finite.

In particularly, the process (*) will return to certain term and forms a cycle after that :



But $+a \bmod m$ is reversible, so for any node, there can be only one inflow.

So the entire process (*) is a circle.



Let l be its length. Then

$\overline{b} = \overline{b+la}$ and $\overline{b} \neq \overline{b+ka}$ $(0<k<l)$

$$\overline{b} = \overline{b+la} \Rightarrow m \mid (b+la)-b = la$$

$$\overline{b} \neq \overline{b+ka} \ (0<k<l) \Rightarrow m \nmid ka$$

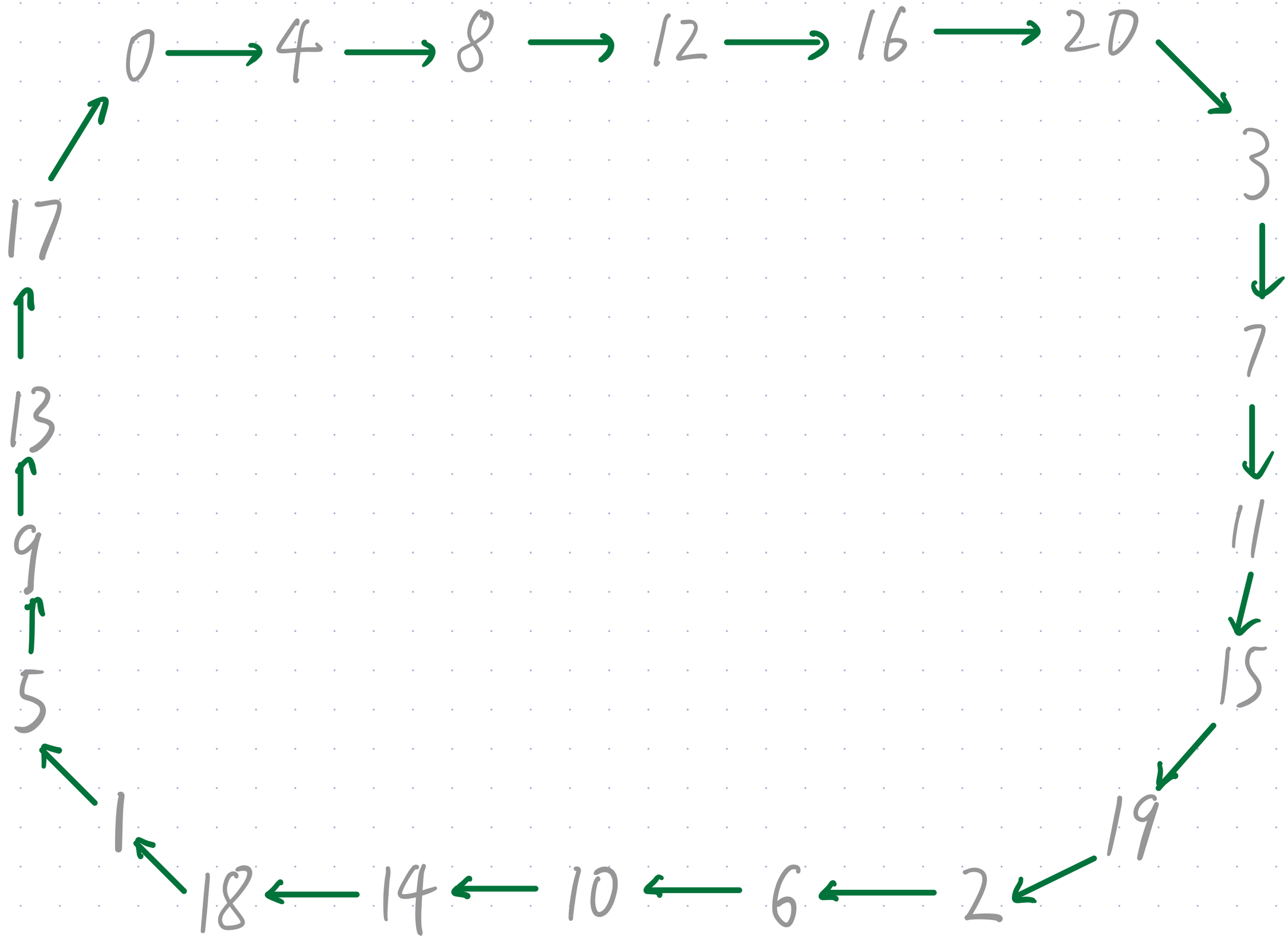
$\Rightarrow la$ is the LCM (a, m)

So $l = \dfrac{\mathrm{LCM}(a,m)}{a} = \dfrac{m}{\mathrm{GCD}(a,m)}$.

This applies to all $\overline{b} \in \mathbb{Z}/m$. Namely, each element is in a cycle of length l. Hence there are $m/l = \mathrm{GCD}(a,m)$ many cycles.

Coro. If $\mathrm{GCD}(a,m)=1$, then $\boxed{+a \bmod m}$ has exactly one cycle of length m.

e.g. $X = \mathbb{Z}/21$, $a = 4$ Function $= +4 \bmod 21$


0
4
8
12
16
20
3
7
11
15
19
2
6
10
14
18
1
5
9
13
17

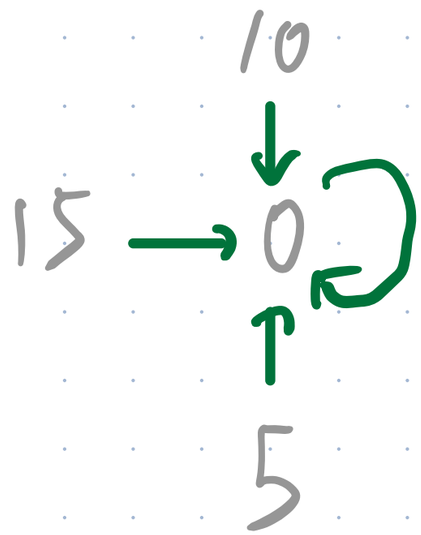
- (Multiplicative Modular Dynamic)

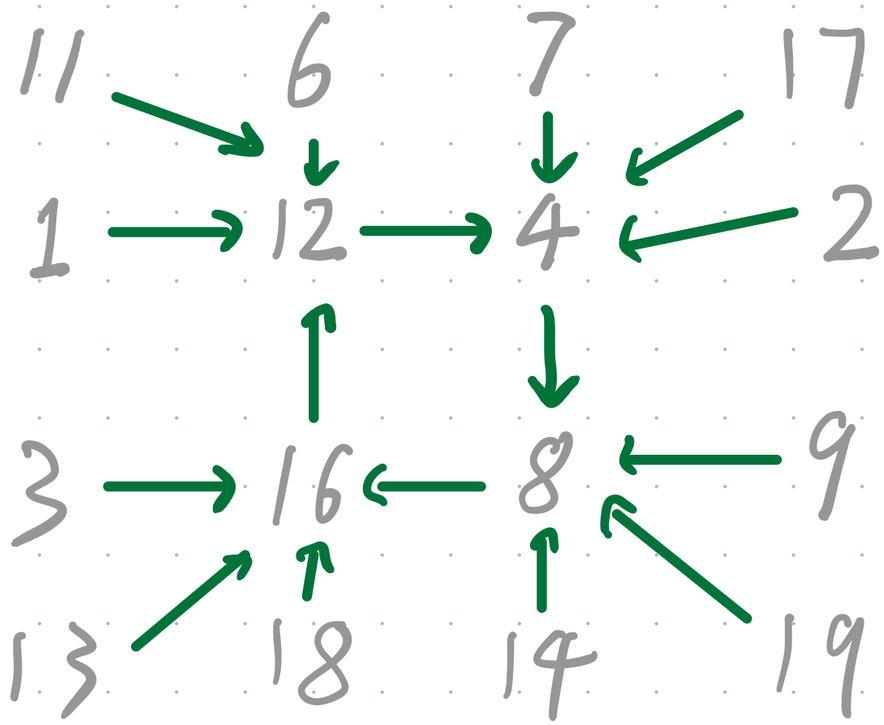
Let m be a modulus, and a an integer. Consider

$$\boxed{\cdot a \bmod m} : \mathbb{Z}/m \longrightarrow \mathbb{Z}/m$$

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

e.g. $X = \mathbb{Z}/20$ $\quad a = 12$





Difficulty: • $a \bmod m$ may be NOT reversible.

Since: $ax \equiv c \bmod m$ could be unsolvable.

Defn: Let m be a modulus.

$$\Phi(m) := \{\text{natural representations of units in } \mathbb{Z}/m\}$$

= elements having multiplicative inverse

Thm. Let m be a modulus, and a an integer.

(1) a is invertible modulo m if and only if $GCD(a,m)=1$.

(2) If a is invertible modulo m, then any multiplicative inverses of a modulo m are congruence to each other modulo m.

$$\Phi(m) = \{a \in \mathbb{Z} : 0 \le a < m \ \&\ GCD(a,m)=1\}$$

$$\phi(m) := \#\Phi(m).$$

e.g: $\Phi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\phi(20) = 8.$

Coro. Let m be a modulus and a an integer s.t. $0 \leq a < m$.

Then $\boxed{\bullet\, a \bmod m}$ is reversible $\iff$ $a \in \mathbb{I}(m)$.

Prop. The modulus m is a prime number if and only if $\phi(m) = m-1$.

Pf: "$\Rightarrow$" If m is a prime number, then any integer x s.t. $0 < x < m$ is coprime to m. Hence x has multiplicative inverse modulo m.

On the other hand, $0 \notin \mathbb{I}(m)$. Therefore, $\phi(m) = m-1$.

"$\Leftarrow$" If $\phi(m) = m-1$, then $\mathbb{I}(m) = \{1, 2, \cdots, m-1\}$ since $0 \notin \mathbb{I}(m)$.

If m is composite, saying $a \mid m$ with $1 < a < m$, then

$GCD(a, m) = a \Rightarrow$ (by Thm (1)) $a \notin \mathbb{I}(m) = \{1, 2, \cdots, m-1\}$.

A contradiction! Hence m has to be a prime number.

Prop. (The set $\overline{\Phi}(m)$ is closed under multiplication modulo m)

If $a, b \in \overline{\Phi}(m)$, then there is a unique $c \in \overline{\Phi}(m)$ such that

$$ab \equiv c \mod m$$

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{c}$$

Proof: (Existence)

Just take c to be the natural representation of ab mod m.

Need to show: c is invertible modulo m.

To do that, let a', b' be the multiplicative inverse of a, b mod m respectively. Then we have

$$\begin{aligned} a'b'c &\equiv a'b'ab \mod m \\ &\equiv (a'a)(b'b) \mod m \\ &\equiv 1 \mod m \end{aligned}$$

Hence, c invertible modulo m.

(Uniqueness)

follow from uniqueness of natural representations.

Rmk: Whenever you have a ring $(R, +, \cdot, 0, 1)$, you have a unit group $(R^\times, \cdot, 1)$, where the underlying set $R^\times$ is the subset of R consisting of units.

$$(\mathbb{Z}/m)^\times \underset{\text{modular class}}{\overset{\text{natural rep.}}{\rightleftarrows}} \Phi(m)$$

$$[a] \longleftrightarrow a$$

This is an **isomorphism** (Not just bijective, but also preserve operations, i.e. $[a \cdot_m b] = [a] \cdot [b]$ and $[1_m] = \mathbb{1}$)

($\cdot$: multiplication in $\mathbb{Z}/m$; $\cdot_m$: multiplication modulo m; $\mathbb{1}$: identity in $\mathbb{Z}/m$; 1_m: identity in $\Phi(m)$)

- (Multiplicative Modular Dynamic)

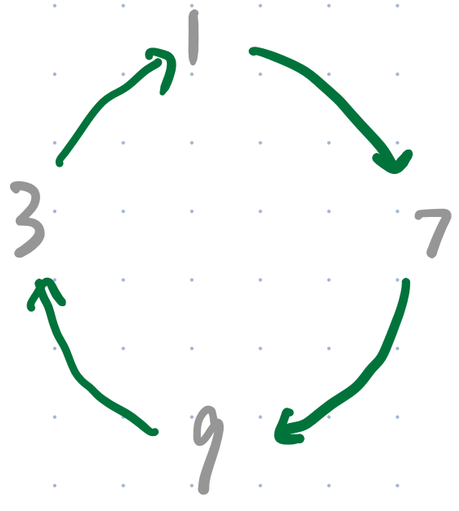
Let m be a modulus, and $a \in \underline{\Phi}(m)$. Consider

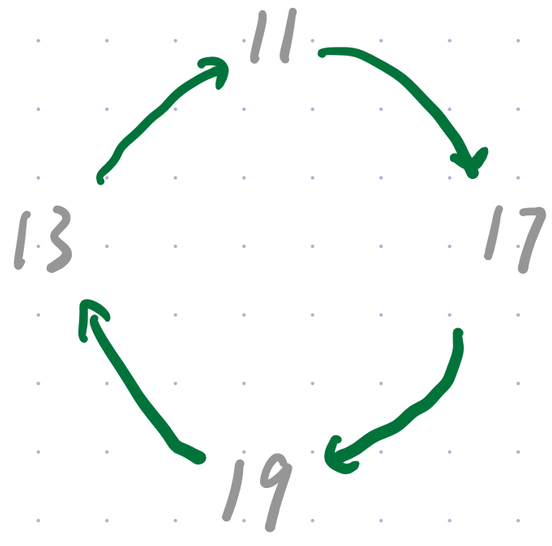
$\boxed{\cdot a \bmod m}$: $\underline{\Phi}(m) \longrightarrow \underline{\Phi}(m)$

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

e.g. $X = \underline{\Phi}(20)$ $a = 7$

$\underline{\Phi}(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $3 \cdot 7 \equiv 1 \bmod 20$.





Prop. Let m be a modulus, and $a \in \mathfrak{F}(m)$. Then the dynamics of $\boxed{\cdot a \bmod m}$ consists of cycles of the same length.

Proof: Initialising the dynamics at 1, we obtain a sequence

$$1, a, a^2, a^3, \cdots, a^n, \cdots \qquad (\star)$$

But $\mathfrak{F}(m)$ is a finite set, there must be repetition.

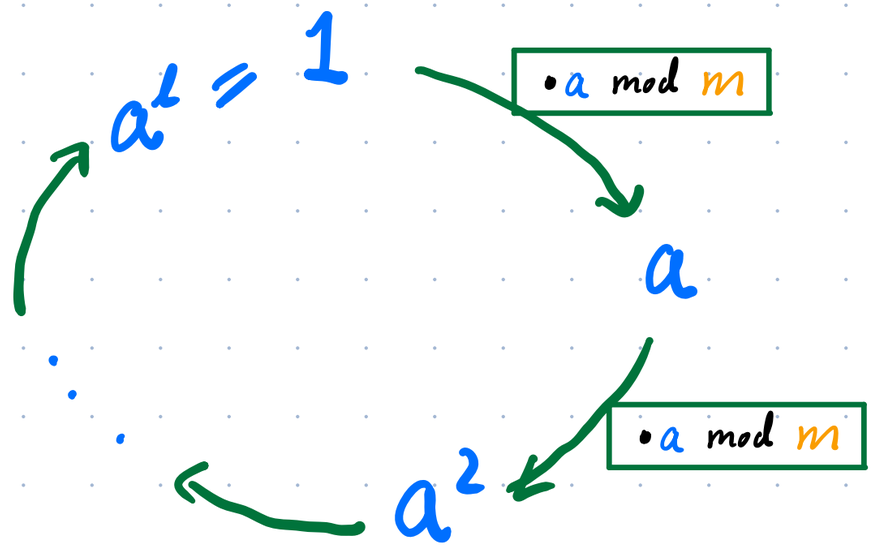
Namely, there are integers $1 \leq e < f$ such that

$$a^f \equiv a^e \bmod m .$$

But $a \in \mathfrak{F}(m)$ implies the CANCELING property of a. Repeat it e times, we get

$$a^{f-e} \equiv 1 \bmod m .$$

Therefore, there is a cycle of length $l = f - e$ in $(\star)$



Let l_0 be the smallest positive integer in

$$\{\, l \mid \text{there is a cycle of length } l \text{ in } (\star) \,\}$$

$$\| \quad \text{(leave proof to you)}$$

$$\{\, l \mid a^l \equiv 1 \bmod m \,\}$$

Claim: For any $0 \le e < f < l_0$, $a^e \not\equiv a^f \bmod m$.

By the claim,

$(\star)$ just repeats a cycle of length l_0.

Now, for any $b \in \mathbb{I}(m)$, consider the sequence.

$$b, ba, ba^2, \cdots, ba^n, \cdots \qquad (\star\star)$$

Since $a^{l_0} \equiv 1 \bmod m$, $(\star\star)$ contains a cycle of length l_0.

If there is a cycle of length $k < l_0$ in $(\star\star)$, then by $b \in \mathbb{I}(m)$.

in particularly the CANCELING property of b, we have. $a^k b \equiv b$

$$a^k \equiv 1 \bmod m.$$

That's why consider $X = \mathbb{I}(m)$ instead of $\mathbb{Z}/m$

But l_0 is the smallest such positive integer. $\Rightarrow\Leftarrow$

Hence $(\star\star)$ just repects a cycle of length l_0.

Since b varies along the entire $\mathbb{I}(m)$, all its element is in some seq as in $(\star\star)$. Hence $\mathbb{I}(m)$ is the union of some cycles of the same length l_0.