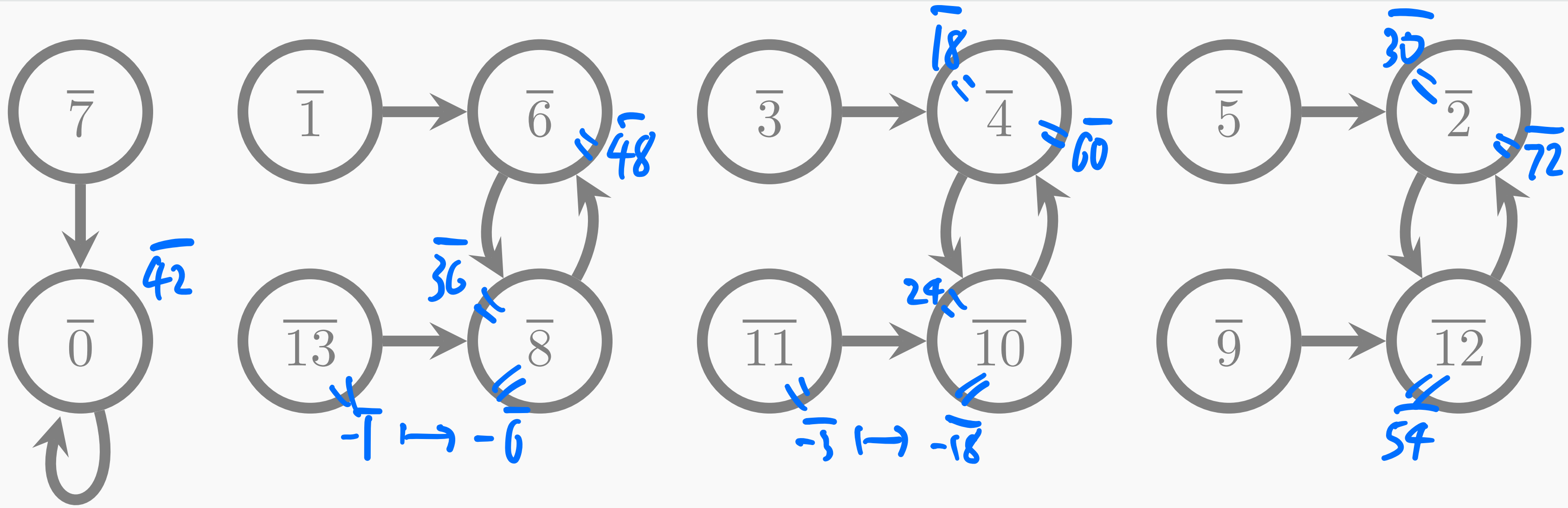
Multiplicative modular dynamic

Definition 4.4.1

A *multiplicative modular dynamic* is a dynamic given by

$$\boxed{\cdot a \pmod{m}} : \mathbb{Z}/m \longrightarrow \mathbb{Z}/m$$
$$\overline{x} \longmapsto \overline{x \cdot a}$$



$m = 14$ $a = 6$

Note that $\boxed{\cdot a \pmod{m}}$ is not invertible (this corresponds to the fact that $ax \equiv c \pmod{m}$ may be unsolvable). Hence, the dynamic could be complicated.

Definition 4.4.2

Let m be a modulus. We will use $\Phi(m)$ to denote the set of natural representatives of *units* in $\mathbb{Z}/m$. The *Euler totient function* $\varphi(m)$ counts its elements.

- Recall that a is invertible modulo m if and only if a is coprime to m (Theorem 4.2.8).
- The bijection $\mathbb{Z}/m \to \{0, 1, \cdots, m-1\}$ allows us to identify $\Phi(m)$ with the set $(\mathbb{Z}/m)^\times$ of units in $\mathbb{Z}/m$. Moreover, we may translate the monoid structure $((\mathbb{Z}/m)^\times, \cdot, 1)$ to the set $\Phi(m)$. In this way, we obtain an operation on $\Phi(m)$:

  $(a, b) \in \Phi(m) \times \Phi(m) \longmapsto$ natural representative of ab modulo m.

  We will denote this operation as $ab \pmod{m}$.

Theorem 4.4.3

A modulus m is a prime number if and only if $\varphi(m) = m - 1$.

Proof. If m is a prime number, then any positive integer larger than 1 can either be a multiple of m, or coprime to m since m has no proper divisor other than 1. Hence, all members of $\{1, \cdots, m-1\}$ are in $\Phi(m)$ since they are less than m.

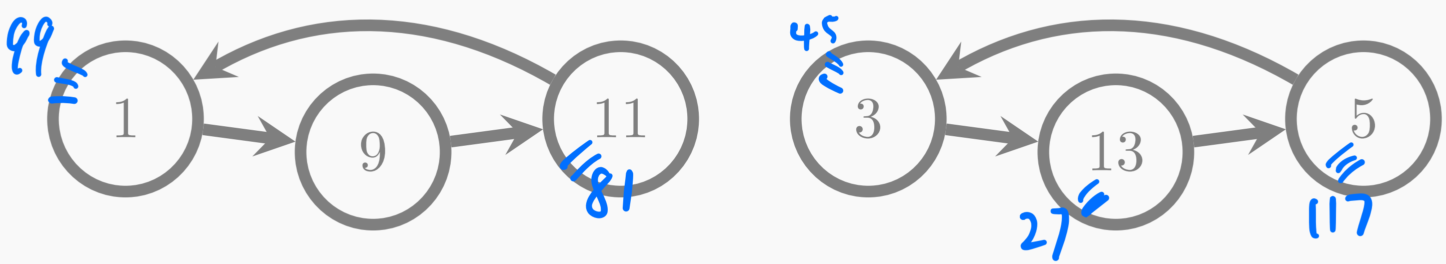
Conversely, suppose $\varphi(m) = m - 1$. Since 0 is never coprime to m, all other natural representatives must be in $\Phi(m)$. But this implies that there is no positive integer between 1 and m can divide m. Namely, m is a prime number. $\square$

Hence, it is more reasonable to consider the following:

Definition 4.4.4

An *multiplicative modular dynamic (on* $\Phi(m)$*)* is a dynamic given by

$$\boxed{\cdot a \pmod{m}} : \Phi(m) \longrightarrow \Phi(m)$$
$$x \longmapsto x \cdot a \pmod{m}$$



$m=14$ $a=9$ $\Phi=\{1,3,5,9,11,13\}$

Theorem 4.4.5

Let m be a modulus and a be an integer coprime to m. Then the dynamic of $\boxed{\cdot a \pmod{m}}$ *on* $\Phi(m)$ *consists of circles of the same length.*

Proof. First note that the function $\boxed{\cdot a \pmod{m}}$ is invertible. Hence, in this dynamic, any node must have exactly one input and one output. Therefore, the dynamic only consists of circles and lines. But the entire set $\Phi(m)$ is finite. Hence, the dynamic cannot contain any lines. It remains to show each circle has the same length.

$a^{\ell} \equiv 1 \bmod m$

Proof. We start with the circle $(a^i)_i$ and let ℓ be its length.

For any $b \in \Phi(m)$, we claim that the circle $(ba^i \pmod{m})_i$ has the same length ℓ. Indeed, since $a^{\ell} \equiv 1 \pmod{m}$, we have

$$ba^{\ell} \equiv b \pmod{m}.$$

Hence, the length k must be at most ℓ.

But whenever we have $ba^k \equiv b \pmod{m}$, we must have

$$a^k \equiv 1 \pmod{m}$$

due to the cancelling property of $b \in \Phi(m)$. Therefore, k cannot be less than ℓ. □

Definition 4.4.6

We will use $\ell_m(a)$ to denote the length of each circle contained in the dynamic of $\boxed{\cdot a \pmod{m}}$ on $\Phi(m)$.

Then theorem 4.4.5 tells us $\ell_m(a) \mid \varphi(m)$.

$\ell(9) = 3$

$\varphi(14) = 6$

Definition 4.4.6

We will use $\ell_m(a)$ to denote the length of each circle contained in the dynamic of $\boxed{\cdot a \pmod{m}}$ on $\Phi(m)$.

Then theorem 4.4.5 tells us $\ell_m(a) \mid \varphi(m)$.

Let's say $\varphi(m) = k \cdot \ell_m(a)$. Then we have

$$a^{\varphi(m)} = (a^{\ell_m(a)})^k \equiv 1^k = 1 \pmod{m}.$$

We thus proved:

Theorem 4.4.7 (Euler-Fermat)

Let m be a modulus and $a \in \Phi(m)$. Then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Example 4.4.8

Let 9 be the modulus. Then $\Phi(9) = \{1, 2, 4, 5, 7, 8\}$. Hence, $\varphi(9) = 6$.

- We have $2^{2023} \equiv 2 \pmod{9}$ since $2023 \equiv 1 \pmod{6}$.
- Note that $3^6 \equiv (3^2)^3 = 0 \pmod{9}$.

$\not\equiv$ 1 mod 9 ?

$3 \notin \Phi(9)$

Corollary 4.4.9 (Fermat's little theorem)

If p is a prime number, then for any integer a,

$$a^p \equiv a \pmod{p}.$$

Proof. When $p \mid a$, this is clear. When $p \nmid a$, the congruence follows from theorems 4.4.3 and 4.4.7 $\Phi(p) = \{\cdots \text{ coprime to } p\}$ □

$$a^{\varphi(p)} \equiv 1 \mod p$$