Modular dynamic

Definition 4.3.1

A *dynamic* on a set X means to keep track of elements under a function $f\colon X \longrightarrow X$:

$$X \xrightarrow{f} X \xrightarrow{f} X \xrightarrow{f} X \xrightarrow{f} \cdots$$

Example 4.3.2 (Collatz conjecture)

Consider the set $X = \mathbb{N}$ and the function

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 3n+1 & \text{if } n \text{ is odd.} \end{cases}$$

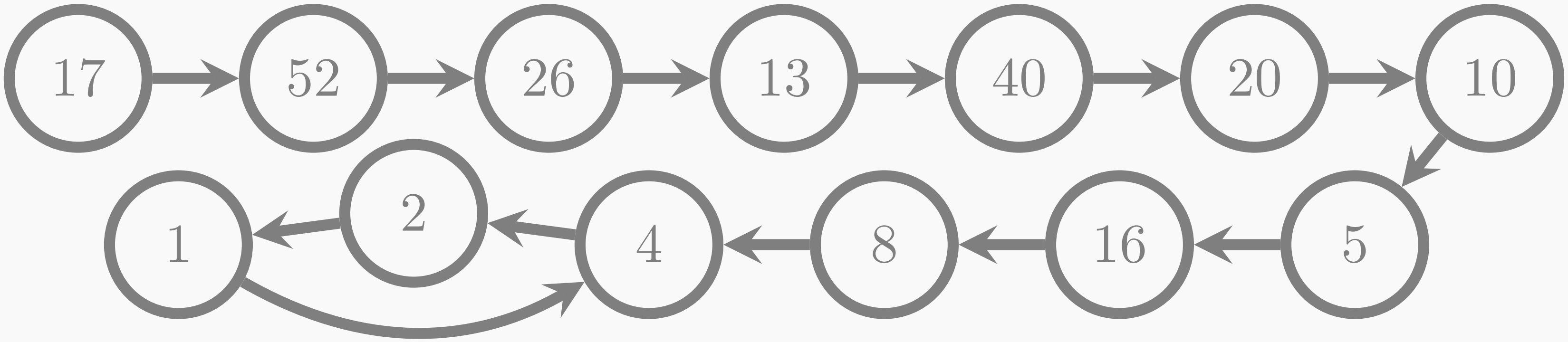
It is conjectured that the dynamic of any $n \in \mathbb{N}$ under f eventually falls in repeating cycle $4 \to 2 \to 1 \to 4$.

Example 4.3.2 (Collatz conjecture)

Consider the set $X = \mathbb{N}$ and the function

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 3n+1 & \text{if } n \text{ is odd.} \end{cases}$$

It is conjectured that the dynamic of any $n \in \mathbb{N}$ under f eventually falls in repeating cycle $4 \to 2 \to 1 \to 4$.



Definition 4.3.3

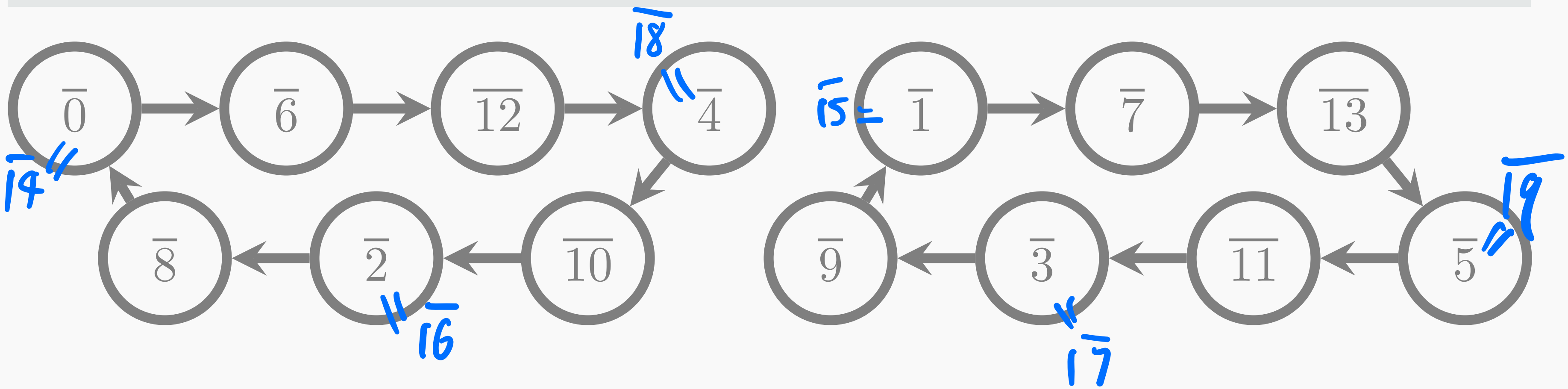
An *additive modular dynamic* is a dynamic given by

$$\begin{aligned} \boxed{+a \pmod{m}} : \mathbb{Z}/m &\longrightarrow \mathbb{Z}/m \\ \bar{x} &\longmapsto \overline{x+a} \end{aligned}$$

Definition 4.3.3

An *additive modular dynamic* is a dynamic given by

$$\begin{aligned} \boxed{+a \pmod{m}} : \mathbb{Z}/m &\longrightarrow \mathbb{Z}/m \\ \overline{x} &\longmapsto \overline{x+a} \end{aligned}$$



$m=14 \quad a=6$

Theorem 4.3.4

Let m be a modulus and a be an integer. Then the dynamic of $\boxed{+a \pmod{m}}$ *consists of* $\gcd(a, m)$ *circles of the same length.*

$$\| \quad \frac{m}{\gcd(a,m)}$$

Theorem 4.3.4

Let m be a modulus and a be an integer. Then the dynamic of $\boxed{+a \pmod{m}}$ consists of $\gcd(a, m)$ circles of the same length.

Proof. First note that the function $\boxed{+a \pmod{m}}$ 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 $\mathbb{Z}/m$ is finite. Hence, the dynamic cannot contain any lines. It remains to show each circle has the same length.

Let's look at the circle containing $\overline{b}$ (for any $b \in \mathbb{Z}$):

$$\overline{b} \longmapsto \overline{b+a} \longmapsto \overline{b+2a} \longmapsto \cdots \longmapsto \overline{b+\ell a} = \overline{b} \longmapsto \cdots$$

Here ℓ is the length of the circle.

Let's look at the circle containing $\overline{b}$ (for any $b \in \mathbb{Z}$):

$$\overline{b} \longmapsto \overline{b+a} \longmapsto \overline{b+2a} \longmapsto \cdots \longmapsto \overline{b+\ell a} = \overline{b} \longmapsto \cdots$$

Here ℓ is the length of the circle.

The identity $\overline{b+\ell a} = \overline{b}$ implies that $m \mid \ell a$. On the other hand, for any $0 < k < \ell$, we must have $m \nmid ka$, otherwise the length of the circle will be at most k. Therefore, ℓa is the smallest common multiple of a and m, hence $\operatorname{lcm}(a, m)$.

Let's look at the circle containing $\overline{b}$ (for any $b \in \mathbb{Z}$):

$$\overline{b} \longmapsto \overline{b+a} \longmapsto \overline{b+2a} \longmapsto \cdots \longmapsto \overline{b+\ell a} = \overline{b} \longmapsto \cdots$$

Here ℓ is the length of the circle.

The identity $\overline{b+\ell a} = \overline{b}$ implies that $m \mid \ell a$. On the other hand, for any $0 < k < \ell$, we must have $m \nmid ka$, otherwise the length of the circle will be at most k. Therefore, ℓa is the smallest common multiple of a and m, hence $\operatorname{lcm}(a, m)$.

Since we start with an arbitrary $b \in \mathbb{Z}$, all circles have the same length. Then the number of circles is $m / \frac{\operatorname{lcm}(a,m)}{a} = \gcd(a, m)$. $\square$