Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 10, 2023

What we have seen last time

- Higher Diophantine equations
- Modular world
    - congruence and modulus
    - modular arithmetic

Today's topics

- Modular arithmetic
  - Division in $\mathbb{Z}/m$
- Modular dynamic
  - Additive dynamic
  - Multiplicative dynamic
  - Euler's totient φ
  - Euler-Fermat theorem

Modular Arithmetic

Question (Linear congruent equation)

Find integer $x \in \mathbb{Z}$ such that

$$ax \equiv b \pmod{m}.$$

Equivalently, find congruence class $X \in \mathbb{Z}/m$ such that

$$[a]_m \cdot X = [b]_m.$$

Theorem 13.1 (Cancelling)

If a is invertible modulo m, then

$$a \cdot x \equiv a \cdot y \pmod{m} \implies x \equiv y \pmod{m}.$$

$3 \cdot 3 \equiv 3 \cdot 0 \mod 9 \xrightarrow[3 \not\equiv 0 \mod 9]{} 3 \not\equiv 0 \mod 9$

Example 13.2

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

1. Verify if 15 is coprime to 37. i.e. invertible mod 37

$$37 = 2 \cdot 15 + 7 \qquad 1 = 15 - 2 \cdot 7$$
$$15 = 2 \cdot 7 + 1 \qquad = 15 - 2 \cdot (37 - 2 \cdot 15)$$
$$7 = 7 \cdot 1 + 0 \qquad = 5 \cdot 15 - 2 \cdot 37.$$

2. Find a multiplicative inverse of 15 modulo 37.
3. Cancelling: = mult with its inverse

$$15 \cdot x \equiv 4 \pmod{37} \implies x \equiv 5 \cdot 4 \equiv 20 \pmod{37}.$$

Modular dynamic

Definition 13.3 of the function f

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

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

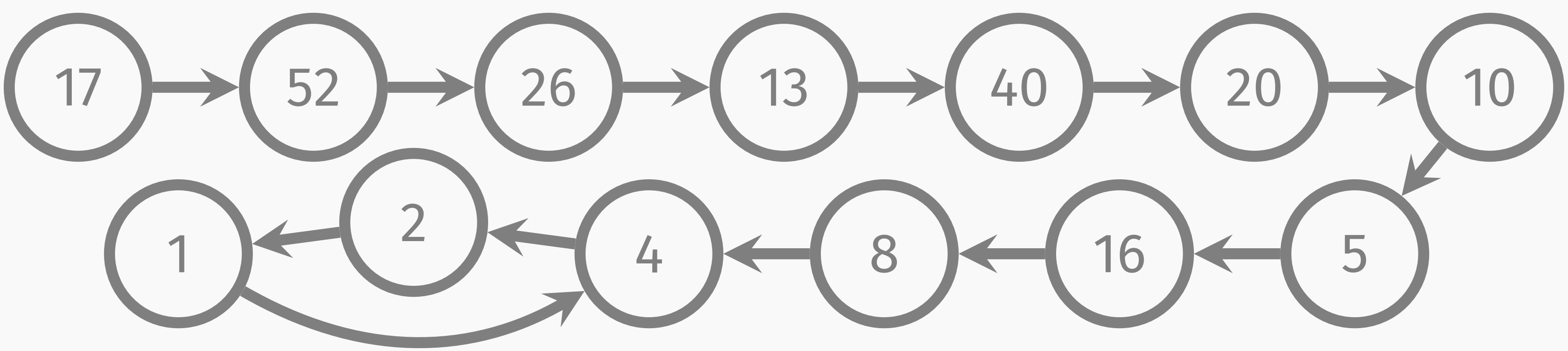
Modular dynamic

Example 13.4 (Collatz conjecture)

Consider the set $X = \cancel{\mathbb{N}}\ \mathbb{Z}_+$ 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 $4 \to 2 \to 1 \to 4$.

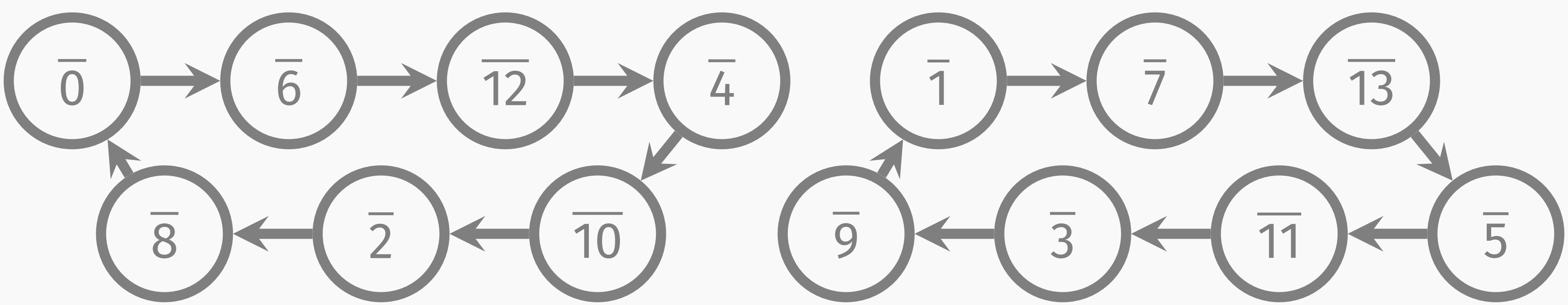


Modular dynamic

Definition 13.5

An ***additive modular dynamic*** is a dynamic given by

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



$m = 14$ $\quad a = 6$ $\qquad \gcd(6, 14) = 2$

Theorem 13.6

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.

Proof. 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 $\overline{b+\ell a} = \overline{b}$ means $m \mid \ell a$. 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 $\operatorname{lcm}(a, m)$.

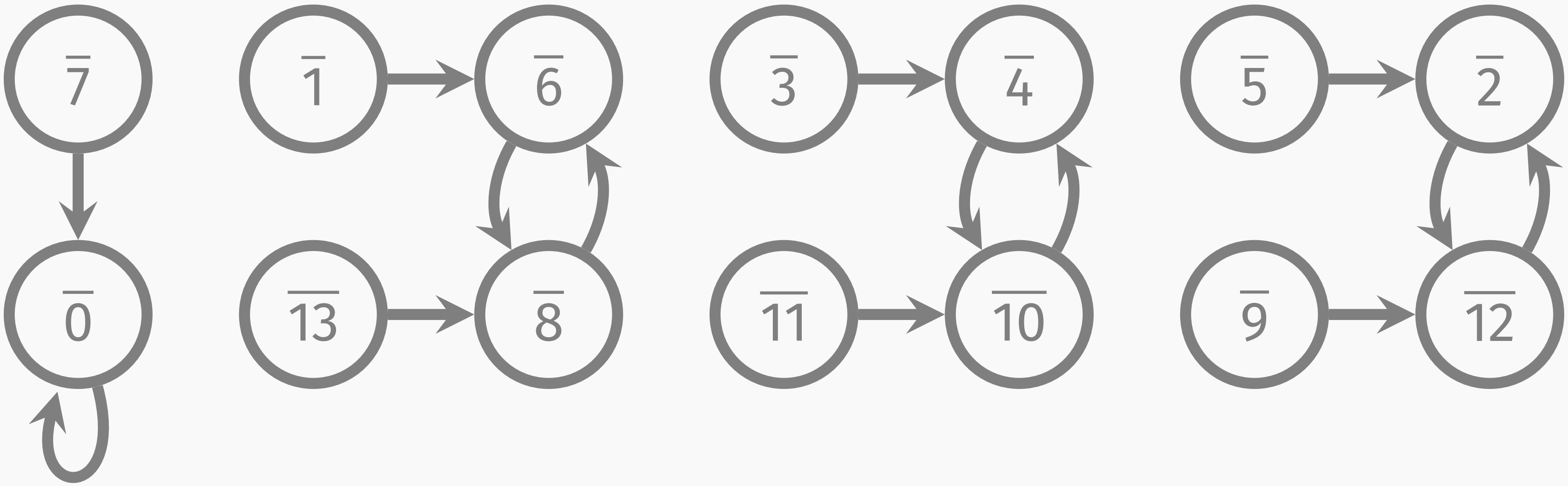
Since we start with an arbitrary $b \in \mathbb{Z}$, all circles have the same length. Then the number of circles is $m / \frac{\operatorname{lcm}(a,m)}{a} = \gcd(a, m)$. $\square$

Modular dynamic

Definition 13.7

An ***multiplicative modular dynamic*** on $\mathbb{Z}/m$ 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 13.8

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.

$\Phi(m) = \{0 \leq a < m \mid a \text{ invertible mod } m\}$

Modular dynamic

- Recall that a is invertible modulo m if and only if a is coprime to m (Theorem 12.18).
- 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 $((\mathbb{Z}/m)^{\times}, \cdot, \mathbf{1})$ to the set $\Phi(m)$. In this way, we obtain an operation on $\Phi(m)$:

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

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

Theorem 13.9

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. $\square$

Multiplicative modular dynamic

Multiplicative modular dynamic

Hence, it is more reasonable to consider the following:

Definition 13.10

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

$\in \Phi(m)$

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

$m = 14$ $a = 9$

Theorem 13.11

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.

$1 \to a \to a^2 \to \cdots \to a^\ell \equiv 1$

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 $b \to ba \to ba^2 \to \cdots \to ba^\ell \equiv b$

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

Hence, the length k must be at most ℓ. $\underbrace{k}_{\text{length}} \leq \ell$ $b \to ba \to ba^2 \to \cdots \to ba^k \equiv b$

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

cancel $b \in \Phi(m)$

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

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

Multiplicative modular dynamic

Definition 13.12

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 13.11 tells us $\ell_m(a) \mid \varphi(m)$.

$m = 14 \quad a = 9$

$\ell_{14}(9) = 3$

Definition 13.12

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 13.11 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 13.13 (Euler-Fermat)

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

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

Example 13.14

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 $2023 \equiv 1 \pmod{6}$. $2^6 \equiv 1 \bmod 9$
- Note that $3^6 \equiv (3^2)^3 = 0 \pmod{9}$. $3 \notin \Phi(9)$

Corollary 13.15 (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 13.9 and 13.13 ∎

then a is coprime to p

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

After Class Work

Exercise 13.1

1. Compute the length of the cycles in the dynamics of $\boxed{\times a \pmod{8}}$ for every $a \in \Phi(8)$. Compare the length with $\varphi(8)$.
2. Compute the length of the cycles in the dynamics of $\boxed{\times a \pmod{14}}$ for every $a \in \Phi(14)$. Compare their length with $\varphi(14)$.
3. Compute the natural representative of $3^{10^{10^{10}}}$ modulo 8 and 14 respectively.

Terminology

Let $(R, +, 0, \cdot, 1)$ be a (commutative) ring. Then the set $R^\times$ of units in $(R, \cdot, 1)$ inherits the monoid structure of $(R, \cdot, 1)$. Moreover, $(R^\times, \cdot, 1)$ is a group, called the ***unit group*** in the ring $(R, +, 0, \cdot, 1)$.

Example 13.16

$((\mathbb{Z}/m)^\times, \cdot, \mathbf{1})$ is the unit group in the residue ring $(\mathbb{Z}/m, +, \mathbf{0}, \cdot, \mathbf{1})$.