- (Multiplicative Modular Dynamic)

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

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

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

<u>Prop.</u> Let m be a modulus, and $a \in \Phi(m)$. Then the dynamics of $\boxed{\cdot a \bmod m}$ consists of cycles of the same length.

Notation: $\ell_m(a)$ the length of each cycle in the dynamics of

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

Coro: $\ell_m(a) \mid \varphi(m)$

Thm (Euler-Fermat)

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

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

Proof. By prop. the dynamics of $\boxed{\cdot a \mod m}$ consists of cycles of the same length $\ell(a)$. Hence $\ell(a) \mid \varphi(m)$.

Say $\varphi(m) = d \cdot \ell(a)$. Then

$$\begin{aligned} a^{\varphi(m)} &\equiv (a^{\ell(a)})^d \mod m \\ &\equiv (1)^d \mod m \\ &\equiv 1 \mod m \end{aligned}$$

E.g. Find natural representation of $2^{2022} \bmod 9$.

$\varphi(9) = 6$ $\quad \Phi(9) = \{1, 2, 4, 5, 7, 8\}$

By Euler-Fermat, $2^6 \equiv 1 \bmod 9$.

$(\because 2022 \div 6\,) \quad \underset{\substack{\| \\ 2000 + 22}}{2022} \equiv 0 \bmod 6$

$2000 = 3\cdot 600 + \underline{200}$, $200 = 3\cdot 60 + \underline{20}$, $20 = 3\cdot 6 + 2$

$2^{2022} \equiv \cancel{2^0} \bmod 9$
1

If you use the fact that N is divided by 3 iff its sum of digits is divided by 3, then you see immediately.

What about $3^6 \bmod 9$ $\quad \varphi(9) = 6$

$$3^6 = 3^{2\cdot 3} = (3^2)^3 = 9^3 \equiv 0^3 = 0 \bmod 9$$

Not the expected $a^6 \equiv 1 \bmod 9$.

Coro. (Fermat's little theorem)

If p is a prime number. Then for any $a \in \Phi(p)$,

$$a^{p-1} \equiv 1 \mod p.$$ (a is coprime to p)

Another formulation:

If p is a prime number. Then for any integer a,

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

Proof: Apply the theorem to p and notice that $\varphi(p) = p-1$.

Application: Primality Testing.

Given a number N, determine whether N is a prime.

- Try to check all $1 < x < N$ if there is one $x \mid N$.

- Just check $1 < x \leq \sqrt{N}$. If no such x divides N, then N is prime.

(Sieve Method)

If N is composite, say $N = a \cdot b$. We may assume $a \leq b$

$a^2 \leq a \cdot b = N \Rightarrow a \leq \sqrt{N}$ and $a \mid N$.

- If there is some $1 < x < N$ s.t. $x^{N-1} \not\equiv 1 \mod N$, then N cannot be prime. (By Fermat's little theorem) N is NOT prime

This number x is called a Fermat witness for the compositeness of N

Otherwise (i.e. $x^{N-1} \equiv 1 \mod N$), x is called a Fermat liar. N ~~is~~ maybe prime

E.g. $N = 91$

$a = 2$ $\qquad 2^{90}$? looks difficult!

(Pingala's Algorithm)

$$90 = (1011010)_2 \quad 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0$$

$$2^{90} \equiv (2^{2^6})\cdot(2^{2^4})\cdot(2^{2^3})\cdot(2^{2^2}) \bmod 91$$

$$16 \cdot 16 \cdot (-17) \cdot 4$$

$$-17 \qquad 16$$

$$\equiv 64 \bmod 91$$

A composite !

$$2^1 \xrightarrow{\text{square}} 2^2 \xrightarrow{\text{square}} 2^4 \xrightarrow{\text{square}} 2^8 \xrightarrow{\text{square}} 2^{16} \xrightarrow{\text{square}} 2^{32} \xrightarrow{\text{square}} 2^{64} \bmod 91$$

$$2 \qquad 4 \qquad 16 \qquad 256 \qquad 289 \qquad -17 \qquad 16$$

$$256 = 2\cdot 91 + 74 \equiv -17$$

$$289 \equiv 3\cdot 91 + 16, \quad 273$$

$N = 91$.

$a = 3$ is a witness or not ?

$90 = (1011010)_2$

$$3^{90} \equiv (3^{2^6})\cdot(3^{2^4})\cdot(3^{2^3})\cdot(3^{2}) \mod 91$$

$$= \underbrace{\underbrace{\underbrace{-10 \cdot -10}_{9} \cdot 9}_{-10} \cdot 9}_{-90} \equiv 1 \mod 91$$

a prime

liar!

3	3^2	3^{2^2}	3^{2^3}	3^{2^4}	3^{2^5}	3^{2^6}	mod 91
3	9	$81 = -10$	$100 = 9$	-10	9	-10	

Dynamics on $\mathbb{N}$: $f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$

"collapse": the dynamics of f always stop after finite step.

Apply it to $N-1$, get: (e.g. $N=91$)

$s_1, s_2, \ldots, s_n = 1.$

90, 45, 44, 22, 11, 10, 5, 4, 2, 1

and then reversely Apply $\begin{cases} \text{square} & \text{if previous } s_i \text{ is even} \\ \text{multiplicate by } \bar{a} & \text{if } \text{- - - -} \ s_i \text{ is odd.} \end{cases}$

to $\bar{a}^{s_*}$ (e.g. $a=3$) Then finally, you get N.R. of $\bar{a}^{N-1} \bmod N$.

90, 45, 44, 22, 11, 10, 5, 4, 2, 1

1 27 $\overset{9}{\cancel{100}}$ -10 -30 $\overset{-10}{\cancel{900}}$ -30 $\overset{-10}{\cancel{81}}$ 9 3

- Advantage:

  Fermat's Primality Testing (with Pingala's Algorithm) is faster than Sieve Method. $O(k \cdot \log^2 n)$ k times

  $O(n \log \log n)$.

- Disadvantage:

  There are Fermat liars!

But we have:

So run it k times and not meet a witness $\sim (\frac{1}{2})^k$

Theorem: If there is a Fermat witness, then half of $\Phi(N)$ are Fermat witness!

Caution: There are composite number M (e.g. 561) s.t.

$$x^{M-1} \equiv 1 \mod M$$

for all $x \in \Phi(M)$.

They are called "Fermat pseudoprime"

After-class reading

- About how **Pingala's algorithm** implements the idea that computing modular exponential by squares and simple multiplications:

  1. You may notice that, to generate a table showing natural representatives of $a^{2^*} \mod N$, one only needs to repeat the process "square modulo N", whose dynamics finally falls into a cycle.
  2. By replace each a^{2^*} appearing in the decomposition of a^{N-1} with its natural representatives modulo N, one still need to do the multiplication cleverly: pairing the same factors to use the results from "square modulo N".
  3. The Pingala's algorithm packages these ideas into a systematic algorithm. One can show that they are essentially doing the same computation.

- You can read pp. 160–163 for more on primality testings.

- This webpage provides an animated illustration of modular dynamics.

- We will discuss **primitive root theorem** (but not its proof) and its application to **cryptography** next time. Please read the rest of **chapter 6** for preparing.