a set of numbers e.g. $\mathbb{Z}$, $\mathbb{Q}$, $\cdots$

Terminology: An S-linear combination of a and b is an expression

$$s \cdot a + t \cdot b \qquad (s, t \in S)$$

We say R can be written as an S-linear combination of a and b if there are $s, t \in S$ such that $s \cdot a + t \cdot b = R$.

We say a and b are S-linearly independent if

$$\forall s, t \in S, \text{"} s \cdot a + t \cdot b = 0 \text{"} \Rightarrow \text{"} s, t = 0 \text{"}$$

Ref. Linear algebra textbooks.

Thm (Euler-Fermat)

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

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

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

for any integers b & c s.t. $b \equiv c \mod \varphi(m)$,

$$a^b \equiv a^c \mod m$$

$b - c = k \cdot \varphi(m)$

$a^b = a^{c + k\cdot\varphi(m)} = a^c \cdot (a^{\varphi(m)})^k$

Rmk: Be aware of the modulus. It is NOT TRUE that

$$b \equiv c \mod m \implies a^b \equiv a^c \mod m$$

e.g. $10 \equiv 3 \mod 7$ but $2^{10} \not\equiv 2^3 \mod 7$

(and $2 \in \Phi(7)$)

Recall the additive modular dynamics:

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.

Compare it to the multiplicative modular dynamics:

Prop. 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.

Does the Coro suggests that $\left\{ \begin{array}{l} \text{additive modular dynamics in } \mathbb{Z}/\varphi(m) \\ \text{multiplicative modular dynamics in } \Phi(m) \end{array} \right.$

are "isomorphic"?

No really,

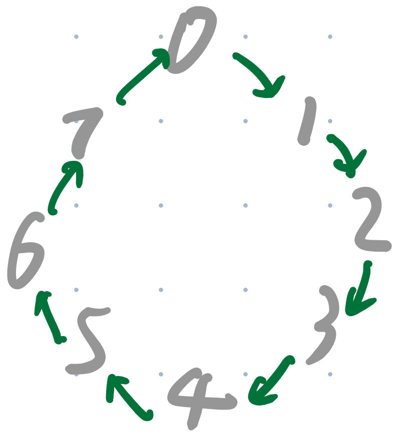
e.g. $m = 20$

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

$$\varphi(20) = 8.$$

The dynamics of $\underline{+1 \bmod 8}$

consists of only one cycle



But no $a \in \Phi(m)$ such that $\underline{\cdot\, a \bmod 20}$ consists of only one cycle.

Indeed:

- $a=1$: 8 cycles of length 1.
- $a=3$: 2 cycles of length 4.

$$\begin{tikzcd} 1 \arrow[r] & 3 \arrow[d] \\ 7 \arrow[u] & 9 \arrow[l] \end{tikzcd} \qquad \begin{tikzcd} 11 \arrow[r] & 13 \arrow[d] \\ 17 \arrow[u] & 19 \arrow[l] \end{tikzcd}$$

- $a=7$: 2 cycles of length 4.

$$\begin{tikzcd} 1 \arrow[d] & 3 \arrow[l] \\ 7 \arrow[r] & 9 \arrow[u] \end{tikzcd} \qquad \begin{tikzcd} 11 \arrow[d] & 13 \arrow[l] \\ 17 \arrow[r] & 19 \arrow[u] \end{tikzcd}$$

- $a=9$: 4 cycles of length 2.

$$\begin{tikzcd} 1 \arrow[r, shift right] & 9 \arrow[l, shift right] \end{tikzcd} \qquad \begin{tikzcd} 3 \arrow[r, shift right] & 7 \arrow[l, shift right] \end{tikzcd}$$

$$\begin{tikzcd} 11 \arrow[r, shift right] & 19 \arrow[l, shift right] \end{tikzcd} \qquad \begin{tikzcd} 13 \arrow[r, shift right] & 17 \arrow[l, shift right] \end{tikzcd}$$

$a=11$: 4 cycles of length 2.

$$\begin{tikzcd} 1 \arrow[r, shift left] & 11 \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} 3 \arrow[r, shift left] & 13 \arrow[l, shift left] \end{tikzcd}$$

$$\begin{tikzcd} 7 \arrow[r, shift left] & 17 \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} 9 \arrow[r, shift left] & 19 \arrow[l, shift left] \end{tikzcd}$$

$a=13$: 2 cycles of length 4.

$$\begin{tikzcd} 1 \arrow[r] & 13 \arrow[d] \\ 17 \arrow[u] & 9 \arrow[l] \end{tikzcd} \qquad \begin{tikzcd} 11 \arrow[r] & 3 \arrow[d] \\ 7 \arrow[u] & 19 \arrow[l] \end{tikzcd}$$

$a=17$: 2 cycles of length 4.

$$\begin{tikzcd} 1 \arrow[r] & 17 \arrow[d] \\ 13 \arrow[u] & 9 \arrow[l] \end{tikzcd} \qquad \begin{tikzcd} 11 \arrow[r] & 7 \arrow[d] \\ 3 \arrow[u] & 19 \arrow[l] \end{tikzcd}$$

$a=19$: 4 cycles of length 2.

$$\begin{tikzcd} 1 \arrow[r, shift left] & 19 \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} 3 \arrow[r, shift left] & 17 \arrow[l, shift left] \end{tikzcd}$$

$$\begin{tikzcd} 11 \arrow[r, shift left] & 9 \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} 13 \arrow[r, shift left] & 7 \arrow[l, shift left] \end{tikzcd}$$

Primitive Roots

For p a prime and $a \in \Phi(p)$, recall that

$\ell(a) =$ the length of each cycle in the dynamics of $\boxed{\cdot a \bmod p}$

While proving Euler-Fermat Theorem, we have seen.

$$\ell(a) \mid \varphi(p) = p-1.$$

Defn. Say $a \in \Phi(p)$ is a primitive root modulo p if $\ell(a) = p-1$. Namely, there is only one cycle in the dynamics of $\boxed{\cdot a \bmod p}$

e.g. $p = 7$ $\quad \Phi(7) = \{1, 2, 3, 4, 5, 6\}$

$a = 1$ $\quad \ell(a) = 1$

$a = 2$ $\quad \ell(2) = 3$

$1 \to 2 \to 4 \to 1$

$a = 3$ $\quad \ell(3) = 6$

primitive root !

$1 \to 3 \to 2 \to 6 \to 4 \to 5 \to 1$

$a = 4$ $\quad \ell(4) = 3$

$1 \to 4 \to 2 \to 1$

$a = 5$ $\quad \ell(5) = 6$

primitive root !

$1 \to 5 \to 4 \to 6 \to 2 \to 3 \to 1$

$a = 6$ $\quad \ell(6) = 2$

$1 \to 6 \to 1$

$\mathbb{Z}/6$ $\quad +a \bmod 6$

$a = 1.$ length 6

$1 \to 2 \to 3 \to 4 \to 5 \to 0 \to 1$

$a = 2$ length 3

$0 \to 2 \to 4 \to 0$

$a = 3$ length 2

$0 \to 3 \to 0$

$a = 4$ length 3

$0 \to 4 \to 2 \to 0$

$a = 5$ length 6

$0 \to 5 \to 4 \to 3 \to 2 \to 1 \to 0$

$a = 0$ length 1

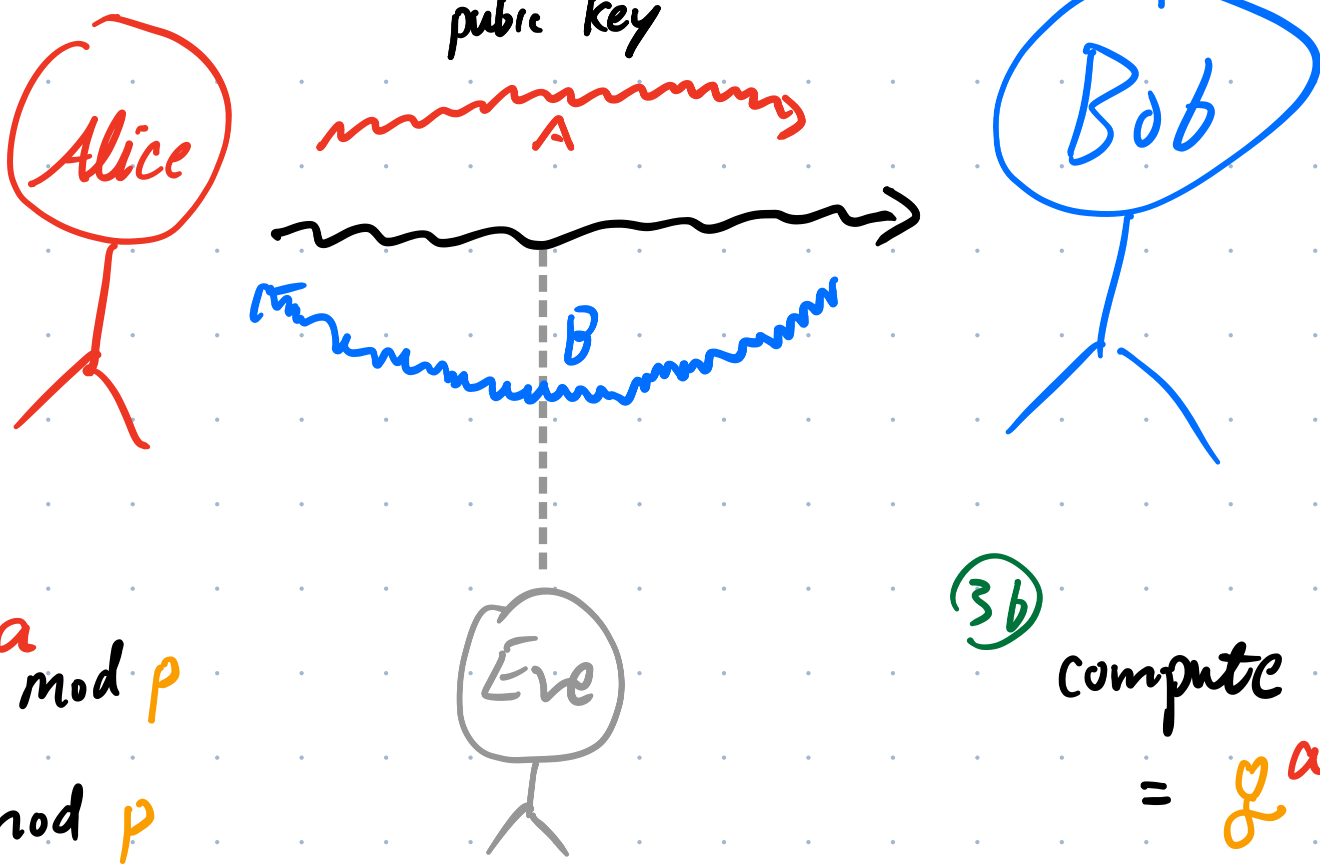
$0 \to 0$

Application (public key system):

① pick a large ($\sim 2^{2048}$) prime p such that $\varphi(p)$ has a large prime factor.
Then find a primitive root g mod p. Publish the pair

(p, g)
public key

②a choose $a \bmod \varphi(p)$ "private key" and compute $A := g^a \bmod p$



②b Choose $b \bmod \varphi(p)$ "private key" and compute $B := g^b \bmod p$

③a compute $B^a \bmod p$
$= g^{ab} \bmod p$
"the secret" S

CAN Eve know S ?

③b compute $A^b \bmod p$
$= g^{ab} \bmod p$
"the secret" S

Rmk:

① How do we generate a public key?

safe prime

- "Sophie Germain prime" is a prime q s.t. $p = 2q+1$ is also a prime.

Upshot: $\varphi(p) = 2 \cdot q$. If q is large, so is p.

And we have fast primality testing.

②③ The computation of A & B is fast, thanks to Pingala's algorithm.
(and S)

However, compute a (resp. b) from A (resp. B) is difficult!

<u>Discrete logarithm</u>: $g^x \equiv a \mod p$

Especially when $\varphi(p)$ has a large prime factor.

E.g. $p = 17$. Then $\varphi(p) = 2^4$.

$g = 3$ is a primitive root. $\ell(3) \mid \varphi(p) = 2^4$, so $\ell(3) = 2^{[?]}$

3^{2^*}	mod 17
3	3
3^2	9
3^{2^2}	13
3^{2^3}	-1

But $3^{2^3} \equiv -1 \mod 17$,

therefore, $\ell(3)$ has to be 2^4.

(Pohlig-Hellman Algorithm) $\varphi(p) = q^e$

Want to find x in $g^x \equiv a \mod p$.

1. set $x_0 = 0$ and compute $\gamma := g^{q^{e-1}} \mod p$
2. For every $k \in \{0, \cdots, e-1\}$, do:
   i) compute $a_k = (g^{-x_k} a)^{q^{e-1-k}} \mod p$
   ii) Find $d_k \in \{0, \cdots, q-1\}$ s.t. $\gamma^{d_k} \equiv a_k \mod p$
   iii) set $x_{k+1} = x_k + q^k d_k$.

Then x_e would be a solution.

Back to the example: Let's pick $a = 2$

Solve: $3^x \equiv 2 \mod 17$

$3^{-1} \equiv 6 \mod 17$.

0. $x_0 = 0$ $\gamma = 3^{2^{4-1}} \equiv -1 \mod 17$ $d_k \in \{0, \cdots, 2-1\}$

$2^4 \equiv -1 \Rightarrow 2^8 \equiv 1 \mod 17$

1. $a_0 = (3^{-0} \cdot 2)^{2^{4-1-0}} \equiv 1 \equiv \gamma^0 \mod 17$ $d_0 = 0$.

$x_1 = \overset{x_0}{0} + 2^0 \cdot 0 = 0$

2^4

2. $a_1 = (3^{-0} \cdot 2)^{2^{4-1-1}} \equiv -1 \equiv \gamma^1 \mod 17$ $d_1 = 1$

$x_2 = \overset{x_1}{0} + 2^1 \cdot 1 = 2$

3. $a_2 = (3^{-2} \cdot 2)^{2^{4-1-2}} \equiv (6^2 \cdot 2)^2 \equiv 4^2 \mod 17$

$\equiv -1 \equiv \gamma^1 \mod 17 \quad d_2 = 1$

$x_3 = \overset{x_2}{2} + 2^2 \cdot 1 = 6.$

4. $a_3 = (3^{-6} \cdot 2)^{2^{4-1-3}} \equiv 6^6 \cdot 2 \equiv 3^6 \cdot 2^7 \mod 17$

$\equiv -1 \equiv \gamma^1 \mod 17$

$d_3 = 1$

$x_4 = 6 + 2^3 \cdot 1 = \boxed{14}$

$3^x = 3^{2^3 + 2^2 + 2} = (-1)(13)(9) \equiv 2 \mod 17$

After-class reading

- This webpage provides an animated illustration of modular dynamics.
- On *similarity between additive modular dynamics and multiplicative modular dynamics*: according to computation in today's lecture, can you give a **bijection** f from $\Phi(20)$ to $\mathbb{Z}/\varphi(20)$ so that f preserves the dynamics on both of them. Namely, $f(ab) = f(a) + f(b)$.
- On *Pohlig-Hellman algorithm*: can you see **why** for $\gamma := g^{q^{e-1}} \pmod p$, the equation

$$\gamma^d \equiv a \pmod p$$

  has a solution d in $\{0, 1, 2, \cdots, q-1\}$?

- We will discuss the **proof** of **primitive root theorem** next time. Please read the last part (polynomials over $\mathbb{F}_p$) of **chapter 5** and the rest of **chapter 6** for preparing.