LN V a

§1.6 Rivest-Shamir-Adleman (RSA)

public key code

- Everybody can encrypt.
- Only one can decode

Construction code

1) p, q primes (100 digits or more)
2) $n = pq$ $\quad \phi(n) = (p-1)(q-1)$
3) choose a $\quad (a, \phi(n)) = 1.$
4) $ax + \phi(n) y = 1.$ $\quad$ ⊛
5) Publish (n, a) Public key

Encode a Message

1) Use a fixed method to write the message as a sequence of numbers $0, 1, \dots, 9$.

(Say $a \mapsto 00$ $? \mapsto 27$
$b \mapsto 01$
$\vdots$ etc)
$z \mapsto 26$.

2) Cut in blocks of length

$L = \min(\# \text{digits } p, \# \text{digits } q) \overset{\text{Say.}}{=} 100$

3) encode each block β.

$$m = \beta^a \bmod n. \quad < n$$

4) Send m

Decode a Message

$$\beta = m^x \bmod n$$

where x from 4 $(*)$.

Pf] $m^x = (\beta^a)^x = \beta^{ax} = \beta^{1-\phi(n)y}$

$$= (\beta^{\phi(n)})^{-y} \cdot \beta = \beta \qquad \square$$

In practice x is unknown.

(n,a) is known. In principle x can be calculated. In practice not.

$\phi(n)$ is unknown.

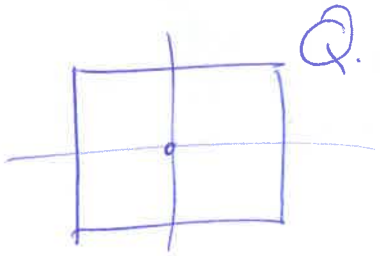
To find $\phi(n)$ one needs to factorize $n=pq$. This is difficult!

$$\boxed{ax + \phi(n)y = 1}$$

Project III

The symmetry of a figure is described by the set of maps which preserves it. "Symmetry Group"

Example Square

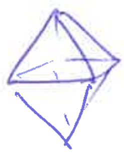


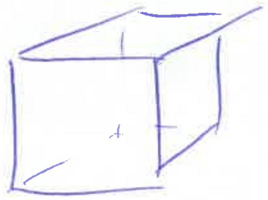
$$\{Id, R_{90}, R_{180}, R_{270}, -Id = F, R_{90}\circ F, R_{180}\circ F, R_{270}\circ F\} = \mathcal{S}_Q$$

$$\#\mathcal{S}_Q = 8$$

$$\#\mathcal{S}_\Delta = 6$$

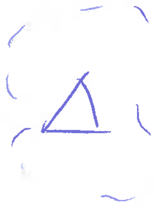
Platonic Solids

 tetrahedron  octahedron



Cube

dodecahedron
(12-faces) (pentagon)



isocahedron
(20 faces) (triangles).

Project: #8p.?

LN IV b

§4.1

X a finite set.

$\pi : X \longrightarrow X$ bijection

π is called a permutation.

Ex $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$

Rmk: all numbers appear exactly onces in the second row.

$S(n)$ set of all permutations of $X = \{1, 2, \ldots, n\}$.

Thm:

1) $\pi, \sigma \in S(n) \Longrightarrow \pi\sigma \in S(n)$
2) $\pi \in S(n) \Longrightarrow \pi^{-1} \in S(n)$
3) $id \in S(n)$.

Ex)
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & \boxed{3} \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 2 & 4 \end{pmatrix}$$

$\pi^{-1}(3) =$ "what goes to 3"

$=$ look what is above 3

$= 6$

Ex)
$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

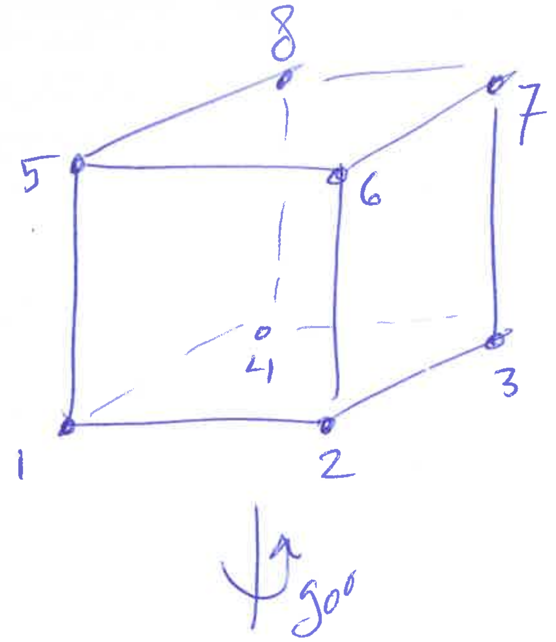
$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\pi\sigma \neq \sigma\pi$$

permutations might <u>not</u> commute.

Ex]



$R_{90°}$

Symmetry of the cube (See Project III)

Let X be the set of vertices of the cube

$$X = \{1,2,3,4,5,6,7,8\}$$

$$R_{90°} = \pi : X \longrightarrow X$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

$\pi : X \to X$

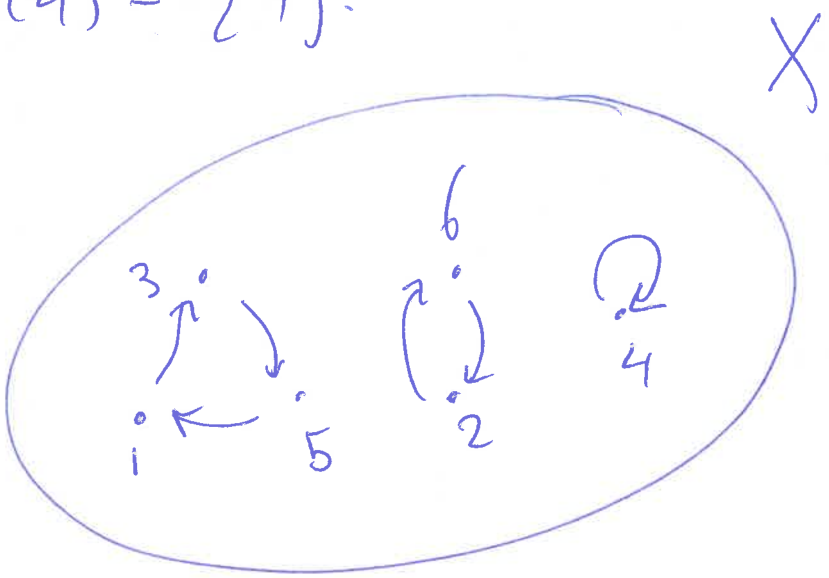
Orbit of x $\quad \mathcal{O}(x) = \{\pi^k(x) \mid k \in \mathbb{Z}\}$.

Ex) $\quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$

$\mathcal{O}(1) = \{1, 3, 5\} = \mathcal{O}(3) = \mathcal{O}(5)$

$\mathcal{O}(2) = \{2, 6\}$

$\mathcal{O}(4) = \{4\}$.



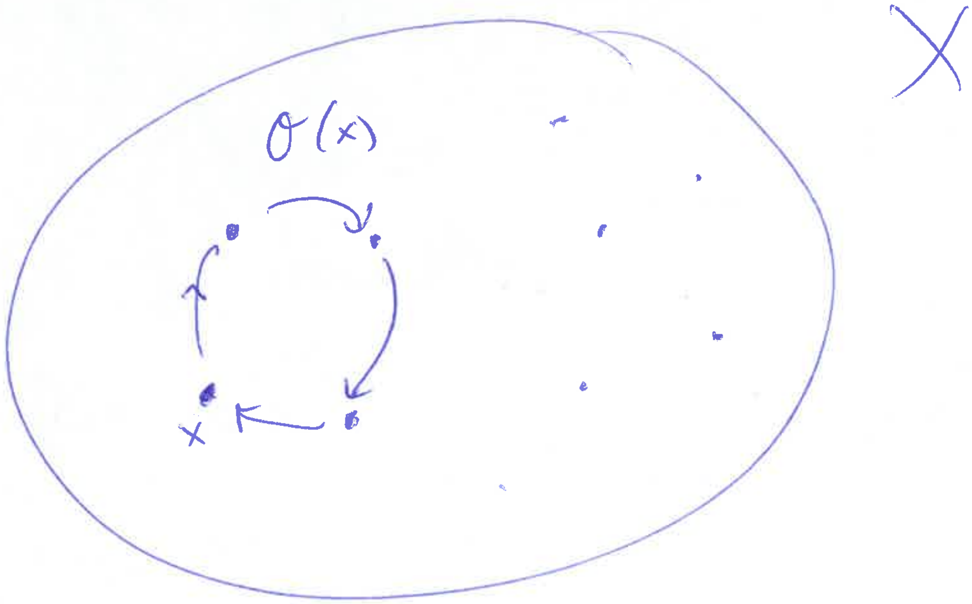
The orbits are cycles.

Lemma $\pi : X \to X$

a permutation.

$\forall x \in X$ let $p = \#\mathcal{O}(x)$. Then

$\forall y \in \mathcal{O}(x) \quad \pi^{p}(y) = y$.



Pf) Claim: $\pi^{p}(x) = x$

$\mathcal{O}(x) = \{x, \pi(x), \dots, \pi^{p-1}(x)\}$. So

$\exists\, k < p$. $\quad \pi^{p}(x) = \cancel{x}\ \pi^{k}(x)$.

So $\pi^{p-k}(x) = x$. $\therefore$ $\#\mathcal{O}(x) = p - k = p$

So $k = 0$ $\therefore$ $\pi^{p}(x) = x$.

[illegible]

let $y = \pi^t(x)$

The $\pi^p(y) = \pi^p(\pi^t(x)) = \pi^{p+t}(x)$

$= \pi^t(\pi^p(x)) = \pi^t(x) = y.$ $\square$

Each cycles defines a -g- permutation.

$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix}$$

$$\mathrm{Fix}(\gamma_1) = \{2, 4, 6\}$$

$$\gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix}$$

$$\mathrm{Fix}(\gamma_2) = \{1, 3, 4, 5\}$$

~~γ_3~~ Observe

$$\pi = \gamma_1 \gamma_2 = \gamma_2 \gamma_1$$

The permutation associated with each cycle commute.

$$\gamma_1 = (1\ 3\ 5) \qquad \gamma_2 = (2\ 6)$$

Cycle Notation

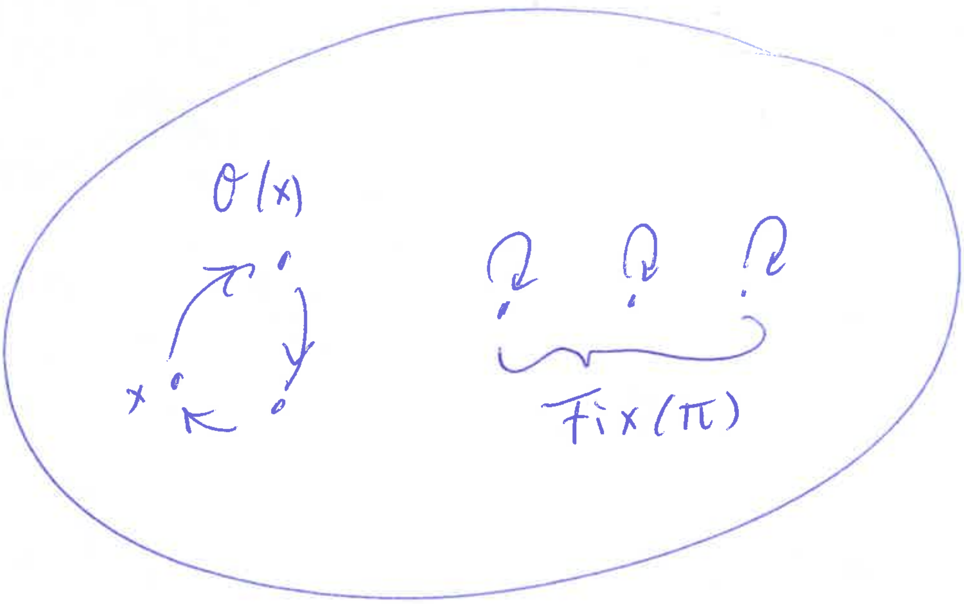
$$\pi = (135)(26)$$

γ_1, γ_2 are called cycles of π

<u>Def:</u> $\pi : X \to X$ permution is called a *cycle* if

$$X = \mathrm{Fix}(\pi) \cup \mathcal{O}(x).$$

where $\mathrm{Fix}(\pi) = \{ y \mid \pi(y) = y \}$.



Structure Theorem Permutation

$$\pi : X \longrightarrow X$$

There exists cycles $\gamma_1, \dots, \gamma_m$ s.t.

$$\pi = \gamma_1 \gamma_2 \cdots \gamma_m$$

- γ_i, γ_j commute.
- The decomposition is unique.

Ex $\quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 7 & 4 & 10 & 9 & 6 & 11 & 8 & 3 & 2 & 1 \end{pmatrix}$

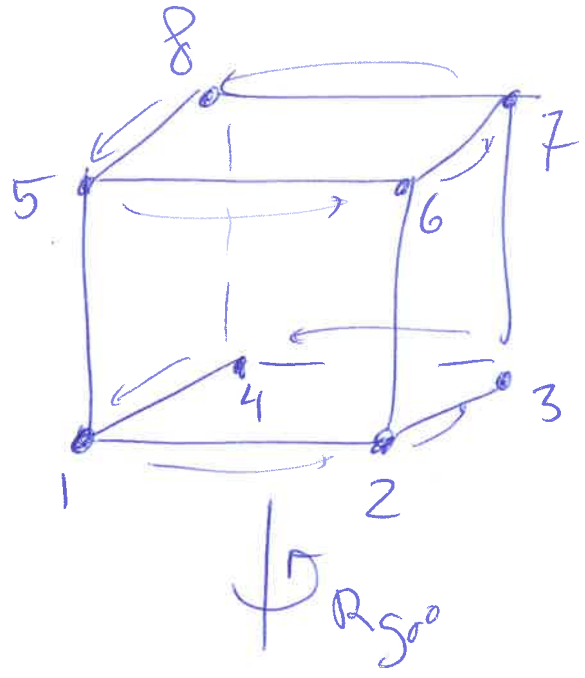
$$= (1\ 5\ 9\ 3\ 4\ 10\ 2\ 7\ 11\ 1)\,(6).$$

Ex $\quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 9 & 1 & 2 & 5 & 3 & 8 & 6 \end{pmatrix}$

$$= (1\ 4)\,(2\ 7\ 3\ 9\ 6\ 5)\,(8)$$

$$= (1\ 4)\,(2\ 7\ 3\ 9\ 6\ 5)$$

Ex)



X set of vertices of the cube

$$X = \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

$$R_{90^\circ} = \pi : X \longrightarrow X$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

$$= \underbrace{(1\ 2\ 3\ 4)}_{\text{bottom vertices form a cycle of } \pi}\underbrace{(5\ 6\ 7\ 8)}_{\text{top vertices form a cycle of } \pi}$$