

César

Algorithme

← PUBLIC

RSA

DH

AES

Clef

← PRIVÉ

César  $f: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$

clef:  $c \in \mathbb{Z}_{26}^*$  25 clefs

BONJOUR

César,  $c = 11$

↓  
M

1  
A B C D E F G H I J K L M N O ...  
L M N ...

$m = [1; 14; \dots]$

$ch = [12; 25; \dots]$

lettre

$f(z) = (z + c) \bmod 26$

11

clef

A	B	C	...
↓	↓	↓	
0	1	2	

↓  
MZ

$$z \in \mathbb{Z}_{26}$$

$$f_c: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

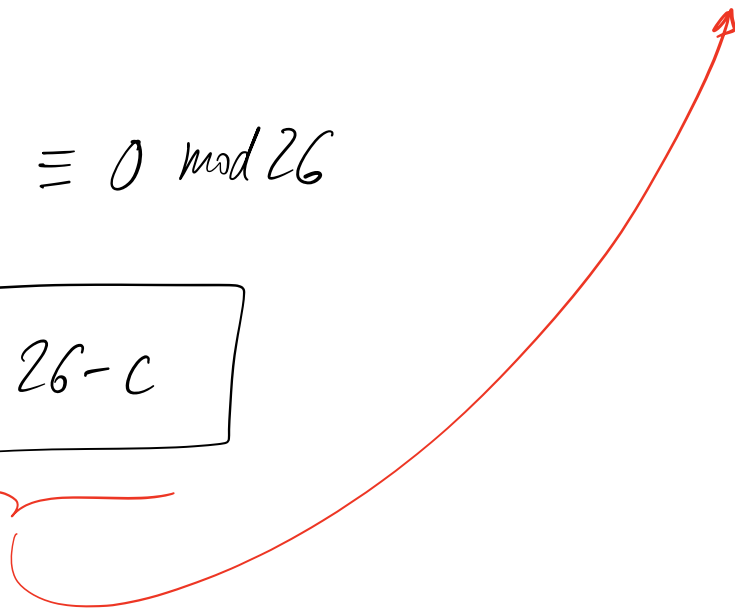
$$z' = f(z) = (z + c) \pmod{26}$$

$$\text{avec } c \in \mathbb{Z}_{26}^*$$

$$z = f^{-1}(z') = (z' - c) \pmod{26} = (z' + c') \pmod{26}$$

$$(c + c') \equiv 0 \pmod{26}$$

$$c' = 26 - c$$



Chiffrement affine

Monalphabétique

$$f: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

bijection

$$z \mapsto (2 \cdot z + 6) \bmod 26 \quad 2, 6 \in \mathbb{Z}_{26}$$

Quels sont les inversibles de  $\mathbb{Z}_{26}$  ?

$$2 \cdot 2' \equiv 1 \pmod{26}$$

$$2z + 6 = z'$$

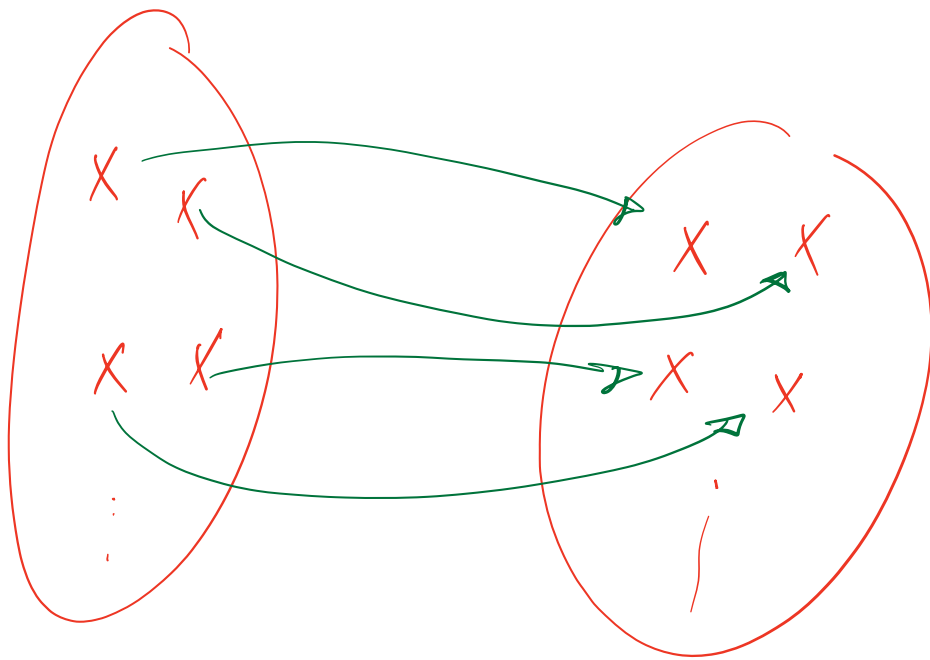
mod 26

$$2z = z' - 6$$

$$\exists ? \ 2' \text{ tq. } 2' \cdot 2 \equiv 1 \pmod{26}$$

$$z = 2' \cdot (z' - 6) \quad ?$$

$$\mathbb{Z}_{26} = \{0; 1; \dots; 25\}$$



$$f: \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto 2x + b \quad \text{avec } a, b \in \mathbb{R}$$

$$a \neq 0$$

$$f: \mathbb{R} \rightarrow \mathbb{R} \quad \text{réciproque } f^{-1}$$

$$f^{-1}(f(x)) = x$$

$$f(f^{-1}(y)) = y$$

$$y = f(x)$$

$$y = 2x + b$$

isoler x

$$y - b = 2x$$

$$x = \frac{y - b}{2}$$

$$x = \frac{y}{2} - \frac{b}{2} \quad / \quad x = f^{-1}(y)$$

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto 2x + b$$

$f(x)$

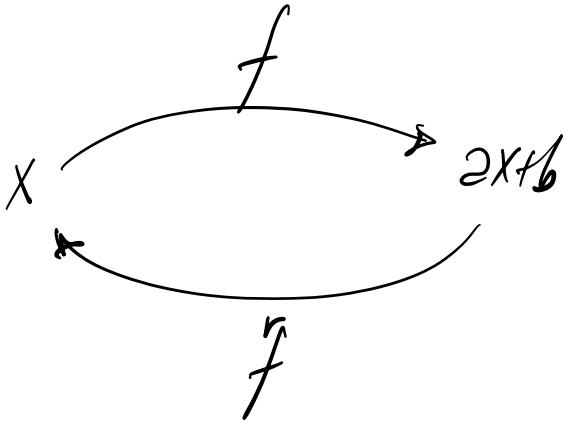
$$f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto \frac{x}{2} - \frac{b}{2}$$

$f^{-1}(x)$

$$f(f(x)) = f(2x+b) = \frac{(2x+b)}{2} - \frac{b}{2}$$

$$= \frac{2x}{2} + \frac{b}{2} - \frac{b}{2} = x$$

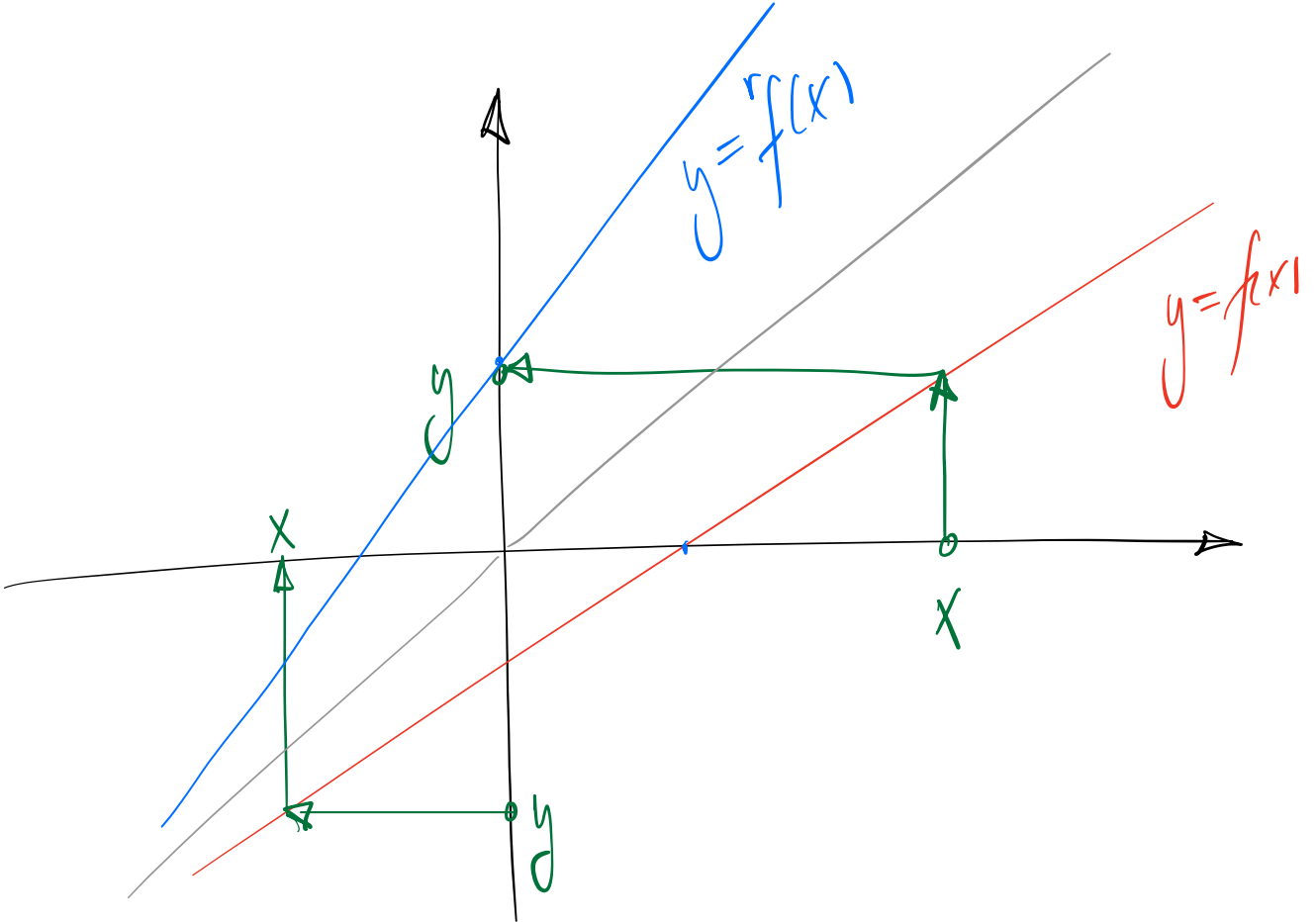


$$f(f(x)) = f\left(\frac{x}{2} - \frac{b}{2}\right)$$

$$= 2 \cdot \left(\frac{x}{2} - \frac{b}{2}\right) + b$$

$$= \cancel{2} \cdot \frac{x}{\cancel{2}} - \cancel{2} \cdot \frac{b}{\cancel{2}} + b$$

$$= x - b + b = x$$



Quels sont les inversibles de  $\mathbb{Z}_{26}$  ?

$$a, b \in \mathbb{Z}_{26}$$

$a, b$  qcq dans  $\mathbb{Z}_{26}$

$$a \cdot b \equiv 1 \pmod{26}$$

$f(z) = (a \cdot z + b) \pmod{26}$  admet une fonction réciproque ?

---

$$2x \equiv 1 \pmod{26} \quad x \in \mathbb{Z}$$

$$26 \mid 2x - 1$$

$$2x - 1 = k \cdot 26$$

$$2x - k \cdot 26 = 1$$

$$2(x - 13k) = 1 \quad x, k \in \mathbb{Z}$$

par      impar      ↓

---

1.1

---

$$3 \cdot 9 = 27 \equiv 1 \pmod{26}$$

---

1 mod 26

5

$$4 \cdot 26 = 104$$

$$5 \cdot 21 = 105$$

$$5 \cdot 21 - 4 \cdot 26 = 1$$

$$5 \cdot 21 = 1 + 4 \cdot 26$$

$$5 \cdot 21 \equiv 1 \pmod{26}$$

$$a \equiv b \pmod{n}$$

$$\Leftrightarrow n \mid (a - b)$$

$$\Leftrightarrow a - b = k \cdot n$$



$$\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

~~multiples de 2~~

~~13~~

$$\left. \begin{array}{l} \text{multiples de 2} \\ \text{13} \end{array} \right\} 26 = 2 \cdot 13$$

Chiffre affine

$$z \in \mathbb{Z}_{26}$$

(nombre associé à la lettre)

$$f(z) = a \cdot z + b$$

Chiffre

$$\begin{array}{l} a \in \mathbb{Z}_{26}^* \rightarrow a' \\ b \in \mathbb{Z}_{26} \end{array} \quad \begin{array}{l} \text{tg.} \\ aa' \equiv 1 \pmod{26} \end{array}$$

clef (a; b)

$$\begin{array}{c} \uparrow \quad \uparrow \\ 12 \cdot 26 \end{array}$$

$$f^{-1}(z) = \dots$$

Soit  $a'$  l'inverse de  $a \pmod{26}$ .

$$y = a \cdot z + b \quad | \quad a \cdot z = y - b \quad | \quad \underbrace{a' \cdot a \cdot z}_{1 \pmod{26}} = a'y - a'b$$

$$z = a'y - a'b$$

3.4.1  $a'$  3.4.5

$$f(x) = 2x + 3$$

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

$$\mathbb{Z}_5 \rightarrow \mathbb{Z}_5$$

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$z \mapsto 2z + 3$$

$z$	$f(z)$
0	3
1	0
2	2
3	4
4	1

$z$	$f^{-1}(z)$
0	1
1	4
2	2
3	0
4	3

$$2 \cdot 3 \equiv 1 \pmod{5}$$

$$\boxed{2^{-1} = 3} \pmod{5}$$

$$-3 \pmod{5} = 2$$

$$y = 2z + 3 \quad / \quad y - 3 = 2z \pmod{5}$$

$$y + 2 = 2z \pmod{5}$$

$$3y + 6 = 6z = z \pmod{5}$$

$$\boxed{z = 3y + 1}$$

$$f(z) = 3z + 1$$

$$f(f(z)) = 3(2z + 3) + 1 = (3 \cdot 2)z + 3 \cdot 3 + 1$$

$\pmod{5}$

$$= z + 4 + 1 = z + 5 = z \pmod{5}$$

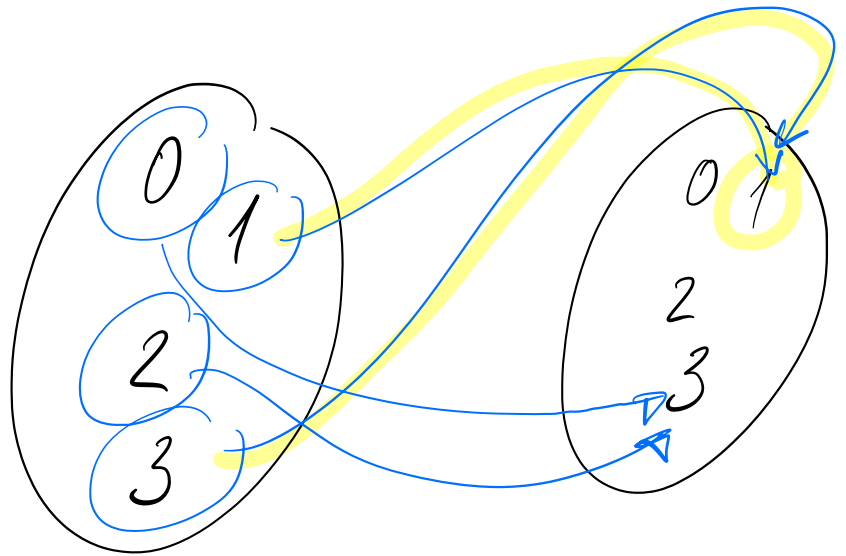
$$\uparrow$$
$$0 \pmod{5}$$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$a$	$a'$
1	1
2	3
4	4

$z$	$2z+3$
0	3
1	1
2	3
3	1

mod 4



$z$	$3z+2$	✓
0	2	
1	5	
2	8	
3	11	