$a \equiv b \mod n$ $\qquad 76 \equiv 50 \mod 26$ 4.2.20 fl

$c \equiv d \mod n$ $\qquad 127 \equiv 75 \mod 26$

$a+c \equiv b+d \mod n$ $\qquad \mathbb{Z}_{26} = \{0; \dots; 25\}$

A' démontrer

0

$5+7 \mod 26 = 12 \mod 26$

$52+12 = 64 = 31+33 \mod 26$

$12 = 5+7$

Preuve: $\quad a \equiv b \mod n \Rightarrow n \mid (a-b) \Rightarrow_{①} a-b = z \cdot n$

$c \equiv d \mod n \Rightarrow n \mid (c-d) \Rightarrow_{②} c-d = w \cdot n$

$z, w \in \mathbb{Z}$

①+②

$\Rightarrow a+c-b-d = z \cdot n + w \cdot n$

$\Leftrightarrow (a+c) - (b+d) = (z+w) \cdot n \Rightarrow n \mid [(a+c)-(b+d)]$

$\Rightarrow a+c \equiv b+d \mod n$ $\square$

4.2.20 fs deuxième partie

$a \equiv c \mod n \iff n \mid (a-c) \iff a - c = z \cdot n$

$b \equiv d \mod n \iff n \mid (b-d) \iff b - d = w \cdot n$ $\quad z, w \in \mathbb{Z}$

But

$ab \equiv cd \mod n \Rightarrow n \mid (ab - cd) \Rightarrow ab - cd = k \cdot n$ $\quad k \in \mathbb{Z}$

À DÉMONTRER

$(a-c)\cdot(b-d) = ab - ad - bc + cd = zw \cdot n^2$

$= ab - cd + cd - ad - bc + cd = zw \cdot n^2$

$= ab - cd - d(a-c) - c(b-d) = zw \cdot n^2$

$= ab - cd - d \cdot z \cdot n - c \cdot w n = zw \cdot n^2$

$\iff ab - cd = n(dz + cw + zwn)$ $\quad dz + cw + zwn \in \mathbb{Z}$

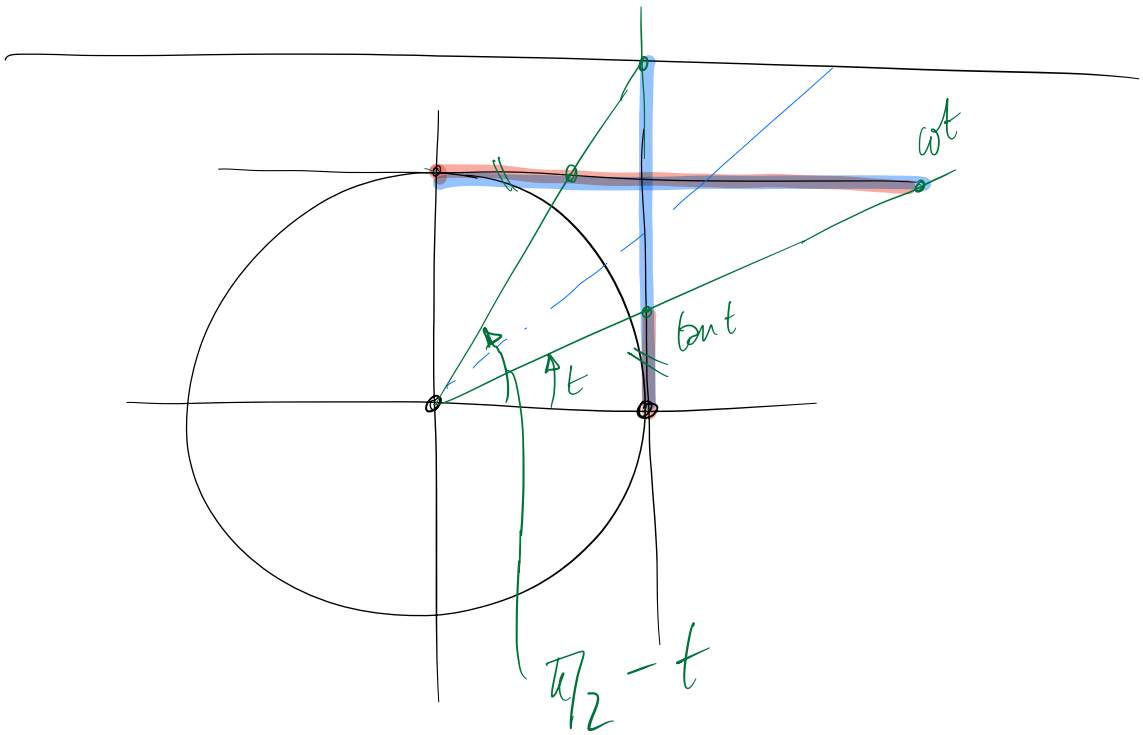
$\Rightarrow n \mid (ab - cd)$

$\iff ab \equiv cd \mod n$

César: chiffrer, déchiffrer, cesser $\quad (z+k) \bmod 26$

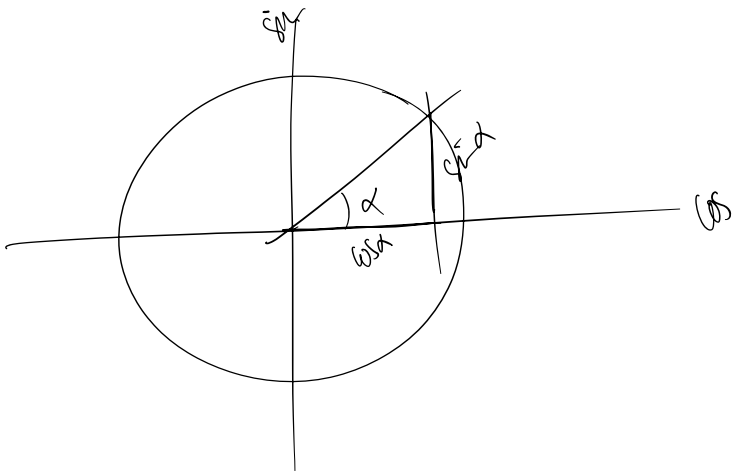
Affine $\quad z \in \mathbb{Z}_{26}$

$$z \mapsto (a \cdot z + b) \bmod 26$$



$$\tan(t) = \cot(\pi/2 - t)$$

$$\cot(t) = \tan(\pi/2 - t)$$


sin α
α
cos α