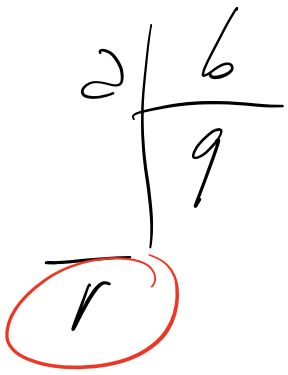
$a \in \mathbb{Z}$

$b \in \mathbb{N}^*$ $(b > 0)$



$a = q \cdot b + r$

$0 \leq r < b$

q et r sont uniques

3.2.19

congru ↓ modulo ↓

$a \equiv b \mod n \Leftrightarrow n \mid (b-a) \Leftrightarrow b - a = k \cdot n$ $k \in \mathbb{Z}$

$\Leftrightarrow a = b + ny$ $y \in \mathbb{Z}$

3.2.20

a) $a \equiv a \mod n$ ← à démontrer

Preuve :

$a \equiv a \mod n \Leftrightarrow n \mid (a-a) \Leftrightarrow n \mid 0$, ce qui est

vrai car $0 = 0 \cdot n$ et $0 \in \mathbb{Z}$

CQFD

b) $a \equiv b \mod n \Rightarrow b \equiv a \mod n$

Preuve :

$a \equiv b \mod n \Leftrightarrow n \mid (b-a) \Leftrightarrow b-a = k \cdot n \quad k \in \mathbb{Z}$

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

La relation est symétrique. $\Leftrightarrow a-b = (-k) \cdot n$

$\Leftrightarrow n \mid (a-b)$ car $-k \in \mathbb{Z}$ si $k \in \mathbb{Z}$

$\Leftrightarrow b \equiv a \mod n$

CQFD

c) $\left.\begin{array}{l} a \equiv b \bmod n \\ b \equiv c \bmod n \end{array}\right\} \Rightarrow a \equiv c \bmod n$

divise

Preuve: Par déf :

$n \mid (b-a)$ et $n \mid (c-b) \iff$ déf de l'opérateur

$$\begin{cases} b-a = kn & L_1 \\ \text{et } c-b = l \cdot n & L_2 \end{cases} \quad k, l \in \mathbb{Z}$$

La somme des deux lignes donne

$L_1 + L_2$

$$b-a+c-b = k \cdot n + ln$$

$\Leftrightarrow$ $c-a = (k+l) \cdot n$

$(k+l) \in \mathbb{Z}$ car si $k, l \in \mathbb{Z}$, alors $k+l \in \mathbb{Z}$

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

$\Leftrightarrow$ $a \equiv c \bmod n$

CQFD

d) D'après l'exercice 3.2.7 :

↗ $\exists$ q, r (uniques) tq. $\boxed{a = q \cdot n + r}$ et $0 \leq r < n$

Il existe

$\Rightarrow \quad r - a = -(q \cdot n)$

$\Leftrightarrow \quad r - a = (-q) \cdot n \quad \Leftrightarrow \quad n \mid (r-a)$

$\Leftrightarrow \quad a \equiv r \mod n$

e) ⚠ Si et seulement si : « deux sens » à démontrer.

① $a \equiv b \mod n \Rightarrow$ a, b ont même reste après division par n

② a, b ont même reste après division par $n \Rightarrow a \equiv b \mod n$

preuve de ① :

$a \equiv b \mod n \Leftrightarrow n \mid (b-a) \Leftrightarrow b - a = k \cdot n \Leftrightarrow b = a + k \cdot n$

Or, d'après le 3.2.7, $b = q \cdot n + r$ avec q, r uniques et $0 \leq r < n$

$\Rightarrow \quad a + k \cdot n = q \cdot n + r$

$\Rightarrow \quad a = (q-k) n + r \quad \Rightarrow \quad a = q' \cdot n + r$ avec $0 \leq r < n$

Donc r est le reste de la division de a par n,

car l'écriture $a = q' \cdot n + r$ avec $0 \leq r < n$ est unique.

CQFD pour (1)

Preuve de (2) : Supposons que a et b ont même reste après division par n.

$$a = q_1 \cdot n + r \qquad 0 \leq r < n$$

$$b = q_2 \cdot n + r$$

La différence de ces deux lignes donne :

$$b - a = (q_2 - q_1) \cdot n + (r - r) = \underbrace{(q_2 - q_1)}_{\in \mathbb{Z}} \cdot n$$

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

CQFD pour (2)

Donc CQFD « tout court »

f) $\left.\begin{array}{l} a \equiv c \mod n \\ b \equiv d \mod n \end{array}\right\} \Rightarrow a+b \equiv c+d \mod n$

Preuve :

$$n \mid (c-a) \Rightarrow \boxed{c-a = k \cdot n} \text{ pour } k \in \mathbb{Z}$$

$$n \mid (d-b) \Rightarrow \boxed{d-b = l \cdot n} \text{ pour } l \in \mathbb{Z}$$

On fait la somme des lignes de l'encadré rouge :

$$(c-a) + (d-b) = kn + ln$$

$$\Leftrightarrow (c+d) - (a+b) = (k+l) \cdot n = m \cdot n$$

Clairement, $m \in \mathbb{Z}$ et donc

$$n \mid \big((c+d) - (a+b)\big)$$

$$\Leftrightarrow a+b \equiv c+d \mod n$$

CQFD

$$\left.\begin{array}{l} a \equiv c \bmod n \\ b \equiv d \bmod n \end{array}\right\} \Longrightarrow a \cdot b \equiv c \cdot d \bmod n$$

Preuve:

On a $n \mid (c-a)$ et $n \mid (d-b)$, ce qui implique que

$$c - a = k \cdot n \quad \text{pour } k \in \mathbb{Z}$$

$$d - b = l \cdot n \quad \text{pour } l \in \mathbb{Z}$$

De plus,

$$cd - ab =$$

$$cd - ad + ad - ab =$$

$$d(c-a) + a(d-b)$$

Ce qui fait que

$$cd - ab = d \cdot k \cdot n + a \cdot l \cdot n$$

$$= (dk + al) \cdot n$$

Posons $m = dk + 2 \cdot l$. Clairement, $m \in \mathbb{Z}$

En effet,

$$cd - 2b = m \cdot n \quad \text{avec } m \in \mathbb{Z}$$

$$\Leftrightarrow \quad n \mid (cd - 2b)$$

$$\Leftrightarrow \quad 2b \equiv cd \mod n$$

CQFD

équivalence logique ↓

$\cos(2\alpha) = 2\cos^2\alpha - 1$ à démontrer $\forall \alpha \in \mathbb{R}$

$\Leftrightarrow \quad \cos(\alpha+\alpha) = 2\cos^2\alpha - 1$

$\overset{(1)}{\Leftrightarrow} \quad \cos\alpha\cos\alpha - \sin\alpha\sin\alpha = 2\cos^2\alpha - 1$

$\Leftrightarrow \quad \cos^2\alpha - \sin^2\alpha = 2\cos^2\alpha - 1$

$\overset{(2)}{\Leftrightarrow} \quad \cos^2\alpha - (1-\cos^2\alpha) = 2\cos^2\alpha - 1$

$\Leftrightarrow \quad 2\cos^2\alpha - 1 = 2\cos^2\alpha - 1$ ← Vrai

$\cos^2 x + \sin^2 x = 1$

$\Leftrightarrow \sin^2 x = 1 - \cos^2 x$

e)

$$a = q_1 \cdot n + r \qquad 0 \le r < n$$

$$b = q_2 \cdot n + r$$

Indications

$\Leftrightarrow$ $a \equiv b \mod n$

SSI

$\Rightarrow$

$$b - a = (q_2 - q_1) \cdot n$$

$\Rightarrow n \mid (b-a) \Rightarrow a \equiv b \mod n$

CQFD

« facile »

$\Leftarrow$

« moins facile »

$\Leftarrow$

$$a \equiv b \mod n$$

$\Leftrightarrow b - a = k \cdot n \qquad k \in \mathbb{Z}$

$\Leftrightarrow b = a + kn$

On sait (3.2.7) qu'il existe q, r uniques tq. $b = q \cdot n + r$ avec $0 \le r < n$

$\Rightarrow a + kn = qn + r$

$\Rightarrow a = (q-k) \cdot n + r$

$a = \underbrace{q' \cdot n + r}$ avec $0 \leq r < n$

écriture de la division de a par n à cause de l'unicité de r

$\Rightarrow a$ et b ont même reste.