

3.2.17 Calculer, après avoir déterminé la meilleure méthode pour ce faire à l'aide de la calculatrice.

- a) $53 \bmod 12$
- b) $-187 \bmod 7$
- c) $2333 \bmod 428$
- d) $-523 \bmod 13$

~~e) $-100 \bmod -15$~~

~~f) $1023 \bmod 117$~~

g) $1341234123411237 \bmod 2341234347$

a) $53 \equiv 5 \pmod{12}$

$$\begin{array}{r|l} 53 & 12 \\ \hline -48 & 4 \\ \hline \textcircled{5} & \end{array}$$

b)
$$\begin{array}{r|l} -523 & 13 \\ \hline \textcircled{-3} & -40 \end{array}$$

$$-523 + 40 \cdot 13 = -3$$

$$-523 + 41 \cdot 13 = 10$$

$$-3 \equiv 10 \pmod{13}$$

3.2.20 Soit n un entier positif. Soit encore a, b, c et d des entiers quelconques. Montrer que

- a) $a \equiv a \pmod{n}$; *reflexive*
 - b) si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$; *symétrique*
 - c) si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$; *transitive*
- d) tout nombre a est congru modulo n au reste de la division de a par n ;
- e) on a $a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste après division par n ;
- f) si $a \equiv c \pmod{n}$ et si $b \equiv d \pmod{n}$, alors $a + b \equiv c + d \pmod{n}$ et $a \cdot b \equiv c \cdot d \pmod{n}$.
- } relation d'équivalence

Définition : $a \equiv b \pmod{n}$ si $n \mid (a - b)$

$28 \equiv 13 \pmod{5}$ $5 \mid (28 - 13)$

a) $n \mid 0 \Rightarrow n \mid (a - a) \Rightarrow a \equiv a \pmod{n}$

b) $a \equiv b \pmod{n} \Rightarrow n \mid (a - b) \Rightarrow$ il existe z tel $z \cdot n = a - b$

$\Rightarrow (-z) \cdot n = b - a \Rightarrow n \mid b - a \Rightarrow b \equiv a \pmod{n}$

c) $a \equiv b \pmod{n} \Rightarrow n \mid (a - b) \Rightarrow \exists z_1$ tq $z_1 \cdot n = a - b$

$b \equiv c \pmod{n} \Rightarrow n \mid (b - c) \Rightarrow \exists z_2$ tq $z_2 \cdot n = b - c$

$\Rightarrow z_1 \cdot n + z_2 \cdot n = (z_1 + z_2) \cdot n = (a - b) + (b - c) = a - c$

$\Rightarrow$ posons $z_1 + z_2 = z$, $z \cdot n = a - c \Rightarrow n \mid a - c \Rightarrow$

$a \equiv c \pmod{n}$

f) si $a \equiv c \pmod{n}$ et si $b \equiv d \pmod{n}$, alors $a + b \equiv c + d \pmod{n}$ et $a \cdot b \equiv c \cdot d \pmod{n}$.

(i) $a \equiv c \pmod{n}$, $b \equiv d \pmod{n} \Rightarrow a + b \equiv c + d \pmod{n}$

En effet :

$$(*) \quad a \equiv c \pmod{n} \Rightarrow n \mid (a - c) \Rightarrow \exists z_1 \text{ tq } z_1 \cdot n = a - c$$

$$(**) \quad b \equiv d \pmod{n} \Rightarrow n \mid (b - d) \Rightarrow \exists z_2 \text{ tq } z_2 \cdot n = b - d$$

$$z_1 n + z_2 n = (z_1 + z_2) n = (a - c) + (b - d) = (a + b) - (c + d)$$

posons $z = z_1 + z_2$. On a $z \cdot n = (a + b) - (c + d) \Rightarrow a + b \equiv c + d \pmod{n}$

(ii) $a \equiv c \pmod{n}$, $b \equiv d \pmod{n} \Rightarrow ab \equiv cd \pmod{n}$

En effet

$$ab - cd = ab - \overbrace{ad}^{(**)} + \overbrace{ad}^{(*)} - cd = a(b - d) + d(a - c) = az_2 n + dz_1 n = (az_2 + dz_1) n$$

Posons $az_2 + dz_1 = z$. On a $zn = ab - cd \Rightarrow n \mid (ab - cd) \Rightarrow$

$$ab \equiv cd \pmod{n}$$

3.2.34 Résoudre les trois équations modulaires suivantes.

a) $4x \equiv 2 \pmod{7}$

b) $6x \equiv 9 \pmod{15}$

c) $4x \equiv 5 \pmod{14}$

a) Quel est l'inverse, s'il existe de 4 mod 7 ?

$$4 \cdot 2 \equiv 1 \pmod{7}$$

$$2 \cdot 4x \equiv 2 \cdot 2 \pmod{7}$$

$$(2 \cdot 4)x \equiv 4 \pmod{7}$$

$$1 \cdot x \equiv 4 \pmod{7}$$

$$2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$$

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1				
5	5					
6	6					

$\mathbb{Z}/_7\mathbb{Z}$

$$1 \cdot 1 \equiv 1 \pmod{7}$$

$$2 \cdot 4 \equiv 1$$

$$3 \cdot 5 \equiv 1$$

$$6 \cdot 6 \equiv 1$$

$$b) \underline{6}x \equiv \underline{9} \pmod{\underline{15}}$$

$$\text{pgdc}(\underline{6}; \underline{15}) = \underline{3} \quad \text{et} \quad \underline{3} \mid \underline{9}$$

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

$$3 \cdot 5 \mid 3 \cdot 2x - 3 \cdot 3$$

$$\begin{aligned} 3 \cdot 2x - 3 \cdot 3 &\equiv 0 & (\text{mod } 15) \\ 3(2x - 3) &\equiv 0 & (\text{mod } 3 \cdot 5) \end{aligned}$$

$$\Rightarrow 2x \equiv 3 \pmod{5}$$

$$\Rightarrow \underline{x \equiv 4 \pmod{5}}$$

$$\underline{x \equiv 4 \quad \text{ou} \quad x \equiv 9 \quad \text{ou} \quad x \equiv 14 \pmod{15}}$$