# *MOD et DIV sur une calculatrice*

Soit $m > 0$ et $a$ un entier. Soit $r$ le reste de $a$ après division par $m$ et $q$ tel que $a = qm + r$.

Calculatrice : $r$ est ($a$ MOD $m$) et $q$ est ($a$ DIV $m$).

Donnera quoi $(a \text{ DIV } m) * m + (a \text{ MOD } m)$?

Réponse : $a$.

Le reste est l'unique nombre naturel $r$ tel que $m|(a-r)$ et $0 \leq r < m$. Donc associer le nombre $r$ à $a$ est vraiment une fonction avec domaine $\mathbb{Z}$ et avec codomaine les nombres naturels entre 0 et $m-1$.

On devrait écrire quelque chose comme

$$\text{Reste-après-division-par-}m : \mathbb{Z} \to \{0, 1, 2, \ldots, m-1\}$$

$a \rightsquigarrow r$

où

$$\text{Reste-après-division-par-}m(a) = r.$$

Pour des raisons historiques on écrit $(a \bmod m) = r$, ou même

$$r = a \bmod m.$$

(Le manuel le fait malheureusement, mais moi j'essaie d'éviter cette notation.)

Malheureusement ça introduit une confusion avec la notation

$$r \equiv a \bmod m$$

pour la relation d'équivalence $r \equiv_m a$.

Il faut faire attention :

On écrit $r \equiv a \bmod m$ si $m|(a-r)$ (seulement).

On écrit $r = a \bmod m$ si $m|(a-r)$ et $0 \leq r < m$.

✓ $1 = 3 \bmod 2$

$3 = \cancel{1} \bmod 2$

!!

✓

$3 \equiv 1 \bmod 2$

Donc il faut comprendre :

On a

$r = a \bmod m$ si et seulement si $r \equiv a \mod m$ et $0 \leq r < m$.

Et aussi

$a \equiv b \mod m$ si et seulement si $(a \mod m) = (b \mod m)$.

Soient $a, b$ deux nombres entiers non-zéro. Posons $d = \mathrm{pgcd}(a, b)$.
Alors $d$ est un maximum

$$d = \mathrm{Max}(\{m \in \mathbb{N} | \ m|a \text{ et } m|b\}).$$

Mais $d$ est aussi un minimum (pour une autre propriété) :

$$d = \mathrm{Min}(\{m \in \mathbb{N} | \ m > 0 \text{ et } \exists (s, t) \in \mathbb{Z}^2 \ : m = sa + tb\})$$

Démonstration.

Soit $E = \{m \in \mathbb{N} |\ \exists (s,t) \in \mathbb{Z}^2\ m = sa + tb\}$ et posons $d' = \mathrm{Min}(E)$.

Par let thm. de Bézout $d \in E$, donc $\boxed{d' \leq d}$.

Aussi il existe $s', t'$ tels que $d' = s'a + t'b$. Donc $d | d'$ ce qui implique $\boxed{d \leq d'}$. Donc $d = d'$. □

d | a

d | b

alors d | s'a + t'b = d'

Problème :

Un marchand vend deux types de T-shirts, l'un avec un C, l'autre avec un O. Celui avec un C coûte $33 chacun, et celui avec un O coûte $29 chacun. Dans une après-midi il a vendu pour $508 de marchandise.

Combien de T-shirts a-t-il vendu ?

Une equation à resoudre ...

Si $u$ le nombre de T-shirts de type C vendus, et $v$ le nombre de T-shirts de type O vendus :

$$33u + 29v = 508$$

Trouve $u + v$.
(Ici $u \in \mathbb{N}$ et $v \in \mathbb{N}$ certainement).

•Trouver une solution entière particulière, c.-à-d., trouver deux entiers $x$ et $y$ tels que

$$33x + 29\cancel{x}\,y = 508$$

C'est une question du type Bézout : il y a façon de trouver une solution entière !

Par la méthode de Bézout :

$$\begin{aligned}
1 \cdot 33 + 0 \cdot 29 &= 33 \\
0 \cdot 33 + 1 \cdot 29 &= 29 \\
1 \cdot 33 + (-1) \cdot 29 &= 4 \;(= 33 - 29) \\
\boxed{(-7) \cdot 33 + (8) \cdot 29 = 1} &\;(= 29 - 7 \cdot 4)
\end{aligned}$$

donc pgcd$(33, 29) = 1$. On multiplie par 508

$$(-7 \cdot 508) \cdot 33 + (8 \cdot 508) \cdot 29 = 508.$$

Ou $x = -7 \cdot 508 = -3556$ et $y = (8 \cdot 508) = 4064$ est une solution particulière de l'équation.

Mais ici $x < 0$, ce n'est pas ce qu'on veut !

- Quelles sont les autres solutions ? Solution générale : Chaque autre paire de solutions est de la forme (preuve plus tard) $\underbrace{x' = -3556}_{x} + 29 \cdot a$ et $\underbrace{y' = 4064}_{y} - 33 \cdot a$ où $a \in \mathbb{Z}$.
- Solution positive : Cherchons un $a \in \mathbb{Z}$ tel que

$+29a \cdot 33$

$-33a \cdot 29$

$$x' = -3556 + 29a \geq 0$$

$$y' = 4064 - 33a \geq 0$$

$+$ $\overline{\phantom{xxxx}}$ $0$

ou

$$a \geq \frac{3556}{29} = 122.62\ldots$$

$$a \leq \frac{4064}{33} = 123.141\ldots.$$

Donc $a = 123$ est la seule possibilité ou $x' \geq 0$ et $y' \geq 0$ !

Conclusion : $u = -3556 + 123 \cdot 29 = 11$ et
$v = 4064 - 123 \cdot 33 = 5$.

Le vendeur a vendu 11 T-shirts de type C et 5 T-shirts de type O, donc en total il y a vendu 16 T-shirts. $\square$

!

Mais il reste encore à montrer :

"Chaque autre paire de solutions est de la forme
$x' = -3556 + a \cdot 29$ et $y' = 4064 - a \cdot 33$ où $a \in \mathbb{Z}$."

Preuve :

On a $(-3556)\cdot 33+(4064)\cdot 29=508$. Si aussi $x'\cdot 33+y'\cdot 29=508$, alors

$$x'\cdot 33+y'\cdot 29 = (-3556)\cdot 33+(4064)\cdot 29$$
$$(x'+3556)\cdot 33 = (-y'+4064)\cdot 29.$$

En particulier $29|((x'+3556)\cdot 33)$. Parce que $\mathrm{pgcd}(33,29)=1$ ou parce que 29 est premier, il suit (par un cor. du thm. de Bézout)

$$29|(x'+3556),$$

c.-à.d. il existe en entier $a$ tel que $29a=x'+3556$, ou

$$x'=-3556+a\cdot 29.$$

Et $a\cdot 29\cdot 33=(x'+3556)\cdot 33=-(y'-4064)\cdot 29$, donc

$$y'=4064-a\cdot 33.$$

Montrer : Pour chaque nombre naturel $n$ le nombre

$$\boxed{4^{n+2} + 5^{2n+1}}$$

est divisible pas 21. (Check : $n = 0$ : 21; $n = 1$ : $189 = 9 \cdot 21$).

Calculons modulo 21 :

$$\begin{aligned}
4^{n+2} + 5^{2n+1} &\equiv_{21} 4^{n+2} + 25^{n} \cdot 5 \\
&\equiv_{21} (4^{n} \cdot 4^{2}) + 4^{n} \cdot 5 \\
&\equiv_{21} 4^{n}(16 + 5) \\
&\equiv_{21} 4^{n} \cdot 21 \\
&\equiv_{21} 0
\end{aligned}$$

$$x^{a+b} = x^{a} \cdot x^{b}$$

(parce que $5^{2n+1} = 5^{2n} \cdot 5^{1} = (25)^{n} \cdot 5$ et $25 \equiv_{21} 4$).

Donc 21 divise $4^{n+2} + 5^{2n+1}$. $\square$

Problème : Soit $n = (13^{27} + 199 \cdot 23 - 311) \cdot (2345 + 11^5)$. Quel est le dernier chiffre de $n$ (dans la représentation décimale) ?

Réponse : On a $n > 0$ donc nous cherchons le nombre $0 \leq r < 10$ tel que $n \equiv r \mod 10$. Calculons modulo 10.

$$
\begin{aligned}
n &\equiv_{10} (3^{27} + 9 \cdot 3 - 1) \cdot (5 + 1^5) \\
&\equiv_{10} ((3^2)^{13} \cdot 3 + 27 - 1) \cdot (5 + 1) \\
&\equiv_{10} ((-1)^{13} \cdot 3 + 7 - 1) \cdot 6 \\
&\equiv_{10} (-3 + 6) \cdot 6 \\
&\equiv_{10} 18 \\
&\equiv_{10} 8
\end{aligned}
$$

$9 \equiv -1 \mod 10$

$199 \equiv_{10} 9$

$3^{27} = 3^{2 \cdot 13 + 1} = 3^{2 \cdot 13} \cdot 3^1 = (3^2)^{13} \cdot 3 = 9^{13} \cdot 3$

Conclusion : le dernier chiffre est 8.

Problème : Soit $n = (13^{27} + 199 \cdot 23 - 311) \cdot (2345 + 11^5)$. Quel est le dernier chiffre de $n$ dans la représentation hexadécimale ?

Réponse : On a $n > 0$ donc nous cherchons le nombre $0 \leq r < 16$ tel que $n \equiv r \mod 16$. Calculons modulo 16.

$$
\begin{aligned}
n &\equiv_{16} ((-3)^{27} + 7 \cdot 7 - 7) \cdot (9 + (-5)^5) \\
&\equiv_{16} ((9)^{13} \cdot (-3) + 42) \cdot (9 + (25)^2 \cdot (-5)) \\
&\equiv_{16} ((81)^6 \cdot 9 \cdot (-3) + 10) \cdot (9 + (9)^2 \cdot (-5)) \\
&\equiv_{16} ((1)^6 \cdot (-27) + 10) \cdot (9 + (81) \cdot (-5)) \\
&\equiv_{16} (-17) \cdot (9 + (1) \cdot (-5)) \\
&\equiv_{16} (-1) \cdot (4) \\
&\equiv_{16} -4 \\
&\equiv_{16} 12
\end{aligned}
$$

$27 = 2 \cdot 13 + 1$

$-3^{27} = ((-3)^2)^{13} \cdot -3$

Donc le dernier chiffre est $C$(douze).

## *Une règle de divisibilité par 7.*

Soit $b > 0$ un nombre tel que $b \equiv_7 1$ (par exemple $b = 8$).
Soit le nombre naturel $N$ représenté sur la base $b > 0$ comme $N = [c_r, c_{r-1}, \ldots, c_1, c_0]_b$.

Alors $N$ est divisible par 7 si et seulement si la somme des chiffres est divisible pas 7. Et même : $N$ et la somme de ses chiffres ont le même reste après division par 7 :

$$N \equiv_7 (c_0 + c_1 + c_2 + \ldots + c_r).$$

Preuve :

$$N = \sum_{i=0}^{r} c_i b^i \equiv_7 \sum_{i=0}^{r} c_i 1^i = (c_0 + c_1 + c_2 + \ldots + c_r).$$

$$3^3 \equiv_7 10^3$$

$$\cancel{3^{15} \equiv_7 3^8}$$

$$a \equiv_6 b$$

$$3^a \equiv_7 3^b$$

Fermat

$$3 \cdot 3 \cdot 3 \equiv_7 10 \cdot 3 \cdot 3 \equiv_7 10 \cdot 10 \cdot 3 \equiv_7 10 \cdot 10 \cdot 10$$

$p$ premier

$n \not\equiv 0 \mod p$

$n^{p-1} \equiv 1 \mod p$

Si $a \equiv_m b$ alors $a + c \equiv_m b + d$

$c \equiv_m d$ $\qquad a \cdot c \equiv_m b \cdot d$

$$a^n \equiv_m b^n$$

Rappelons :

Les propriétés considérées *essentielles* de l'ensemble des nombres naturels $\mathbb{N} = \{0, 1, 2, 3, \ldots, n, n+1, \ldots\}$ sont les suivantes :

1. Chaque nombre naturel $n$ a un unique *successeur* dans $\mathbb{N}$, noté $n+1$.
2. Il existe un nombre naturel spécial, noté 0, et
3. chaque nombre naturel $n$ différent de 0 a un unique *prédécesseur* dans $\mathbb{N}$, noté $n-1$. On a $(n+1)-1 = n$, pour tout $n \in \mathbb{N}$ et $(n-1)+1 = n$ pour tout $n \in \mathbb{N}$ tel que $n \neq 0$.
4. **Si $E \subseteq \mathbb{N}$ est un sous-ensemble de $\mathbb{N}$ tel que (i) $0 \in E$ et (ii) pour chaque $n \in E$ aussi $n+1 \in E$, alors nécessairement $E = \mathbb{N}$.**

Le reste d'aujourd'hui ne sera pas matière d'examen.

À partir de seulement les propriétés essentielles de $\mathbb{N}$ nous allons déduire les autres propriétés de $\mathbb{N}$ bien connues par vous.
Un peu longue, mais pas vraiment dur.

La définition de l'addition.

### Definition

Fixons $a \in \mathbb{N}$. Nous allons définir pour chaque $n \in \mathbb{N}$ l'élément $a + n \in \mathbb{N}$. Au début $a + 0 = a$ et $a + 1$ est le successeur de $a$ (qui existe et est unique par une des propriétés essentielles de $\mathbb{N}$). Puis supposons pour $n \in \mathbb{N}$ on a déjà défini $a + n$, alors on définit $a + (n + 1)$ comme le successeur de $a + n$, c.-à-d., par définition

$$a + (n + 1) := (a + n) + 1.$$

Ainsi on a défini $a + n$ pour chaque $n \in \mathbb{N}$.

### Démonstration.

En effet l'addition $a + n$ est définie pour $n = 0$, et si c'est définie pour $n$ alors c'est aussi définie pour $n + 1$. Par le principe d'induction, l'addition $a + n$ a été définie pour chaque $n \in \mathbb{N}$. $\square$

La définition de la multiplication.

### Definition

Fixons $a \in \mathbb{N}$. Nous allons définir pour chaque $n \in \mathbb{N}$ l'élément $a \cdot n \in \mathbb{N}$. Au début on définit $a \cdot 0 := 0$, $a \cdot 1 := a$. Supposons pour $n \in \mathbb{N}$ on a déjà défini $a \cdot n$, alors on définit $a \cdot (n+1) := (a \cdot n) + a$. Ainsi on a défini $a \cdot n$ pour chaque $n \in \mathbb{N}$.

L'associativité de l'addition :

## Théorème

*Pour tous les nombres naturels $a, b, c$ on a*

$$(a+b)+c = a+(b+c).$$

## Démonstration.

Fixons $a$ et $b$. Nous allons montrer par induction sur $n$ que $(a+b)+n = a+(b+n)$.
Début : Si $n=0$ c'est vrai : $(a+b)+0 = a+b = a+(b+0)$, car par définition $N+0=N$ pour chaque nombre naturel $N$.
Étape d'induction. Supposons $\underbrace{(a+b)+n = a+(b+n)}_{\text{hyp ind}}$, pour $n \geq 0$. Alors

$$(a+b)+(n+1) \overset{\text{def}}{=} ((a+b)+n)+1 \overset{\text{hyp ind}}{=} ((a+(b+n))+1 =$$

$$= a+((b+n)+1) = a+(b+(n+1)).$$

### Lemme

*Pour chaque nombre naturel $n$ on a*

$$\underline{0+n=n+0=n} \quad \textit{et} \quad \underline{1+n=n+1}.$$

### Démonstration.

Rappel : par définition de l'addition on a $n+0=n$ et $0+(n+1)=(0+n)+1$ pour chaque nombre naturel $n$.
On montre que $0+n=n+0=n$ par induction.
Début : si $n=0$ c'est une tautologie : $0+0=0+0$.
Étape d'induction : Supposons par induction que $0+n=n+0=n$. Donc

$$0+(n+1)=(0+n)+1=n+1=(n+1)+0.$$

On conclut par induction. $\square$

(suite).

Puis, on montre que $1+n=n+1$ par induction.
Début. Si $n=0$ on a : $1+0=1=0+1$, car par définition 1 est le successeur de 0.
Étape d'induction : Supposons par induction que $1+n=n+1$.
Alors par L'hypothèse d'inducton et l'associativité :

$$(n+1)+1=(1+n)+1=1+(n+1).$$

Et donc par induction on conclut : $1+n=n+1$ pour chaque nombre naturel $n$. □

La commutativité de l'addition :

### Théorème

*Pour tous nombres naturels $n$ et $m$ on a*

$$m + n = n + m.$$

### Démonstration.

Fixons $m$. Nous allons montrer le théorème par induction sur $n$.
Début : c'est le lemme précécent.
Étape d'induction : Supposons par induction que $m + n = n + m$, pour $n \geq 0$. Donc par définition de l'addition, l'hypothése d'induction, l'associativité de l'addition, et le lemme

$$m + (n + 1) = (m + n) + 1 = (n + m) + 1 = 1 + (n + m) =$$

$$= (1 + n) + m = (n + 1) + m.$$

Donc par induction théorème est vrai.

La distributivité :

### Théorème

*Pour tous nombres naturels $a, b, n$ on a*

$$(a + b) \cdot n = (a \cdot n) + (b \cdot n).$$

### Démonstration.

Par induction sur $n$.

Début. Pour $n = 0$ on a : $(a + b) \cdot 0 = 0 = 0 + 0 = (a \cdot 0) + (b \cdot 0)$.
Étape d'induction. Supposons $(a + b) \cdot n = (a \cdot n) + (b \cdot n)$.. On a par définition de la multiplication, l'associativité et la commutativité de l'addition, et l'hypothèse d'induction :

$$(a+b)\cdot(n+1) = ((a+b)\cdot n)+(a+b) = ((a\cdot n)+(b\cdot n))+(a+b) =$$

$$= ((a \cdot n) + a) + ((b \cdot n) + b) = ((a \cdot (n + 1)) + ((b \cdot (n + 1)).$$

Donc par le principe d'induction, le théorème est vrai.

L'associativité de la multiplication :

Théorème

*Pour tous nombres naturels $a, b, n$ on a*

$$(a \cdot b) \cdot n = a \cdot (b \cdot n).$$

Démonstration.

Par induction sur $n$.

Début. Pour $n = 0$ on a : $(a \cdot b) \cdot 0 = 0 = a \cdot 0 = a \cdot (b \cdot n)$.
Étape d'induction. Supposons $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Alors par définition de la multiplication, l'hypothèse d'induction et la distributivité :

$$\underline{(a \cdot b) \cdot (n+1)} = ((a \cdot b) \cdot n) + (a \cdot b) = (a \cdot (b \cdot n)) + (a \cdot b) =$$

$$= a \cdot ((b \cdot n)) + b) = \underline{a \cdot (b \cdot (n+1))}.$$

Donc par le principe d'induction, le théorème est vrai.

## Lemme

*Pour chaque nombre naturel n on a*

a(n+1) = an + a

$$0 \cdot n = n \cdot 0 = 0 \quad \textit{et} \quad 1 \cdot n = n \cdot 1 = n$$

## Démonstration.

Rappel : par définition de la multiplication on a $n \cdot 0 = 0$ et $n \cdot 1 = n$.

On montre que $0 \cdot n = 0$ par induction. Début : si $n = 0$ on a en effet $0 \cdot 0 = 0$. Étape d'induction : Supposons par induction que $0 \cdot n = 0$. Alors par définition de la multiplication, l'hypothèse d'induction, et par définition de l'addition

$$0 \cdot (n+1) = (0 \cdot n) + 0 = 0 + 0 = 0.$$

Donc par le principe d'induction, c'est vrai que $0 \cdot n$ pour chaque nombre naturel $n$.

On montre que $1 \cdot n = n$ par induction. Début : si $n = 0$ on a en

La commutativité de la multiplication :

## Théorème

*Pour tous nombres naturels $a, n$ on a*

$$a \cdot n = n \cdot a$$

## Démonstration.

Par induction sur $n$. Début si $n = 0$ on a en effet $a \cdot 0 = 0 = 0 \cdot a$ par le lemme. Aussi si $n = 1$ on a en effet $a \cdot 1 = a = 1 \cdot a$ par le lemme. Étape d'induction : Supposons par induction que $a \cdot n = n \cdot a$. Alors par définition de la multiplication, l'hypothèse d'induction, le lemme, la distributivité

MA

$$a \cdot (n+1) = (a \cdot n) + a = (n \cdot a) + 1 \cdot a = (n+1) \cdot a.$$

✓

Donc par le principe d'induction, le théorème est vrai. □