

Arithmétique (partie 2)

1. La division euclidienne

■ THÉORÈME :

Soient a un entier positif ou nul et b un entier strictement positif.

Il existe un unique couple d'entiers naturels $(q; r)$ tel que

$$\begin{cases} a = b \times q + r \\ 0 \leq r < b \end{cases}$$

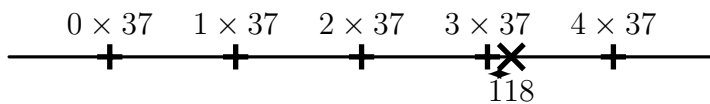
q est appelé le **quotient** et r est appelé le **reste** dans la division euclidienne de a par b .

Exemple :

La division euclidienne de 118 par 37 a pour quotient 3 et pour reste 7 car :

$$118 = 3 \times 37 + 7 \text{ et } 0 \leq 7 < 37$$

Graphiquement, on peut interpréter cette division par l'encadrement de 118 par deux multiples consécutifs de 37, le reste 7 étant la distance de 118 au multiple de 37 inférieur le plus proche.



Effectuer de même la division euclidienne de 23 par 37 puis de 407 par 27 avec l'interprétation graphique.

Pour 23 par 37 :

$$\text{on a } 23 = 0 \times 37 + 23 \text{ et } 0 \leq 23 < 37.$$

Pour 407 par 27 :

$$\text{on a } 407 = 15 \times 27 + 2 \text{ et } 0 \leq 2 < 27.$$

Démonstration. Existence :

Observons tout d'abord que si $b = 1$, alors

$$a = 1 \times a + 0 \text{ et } 0 \leq 0 < 1$$

donc le couple $(q; r) = (a; 0)$ convient.

On suppose désormais que $b > 1$.

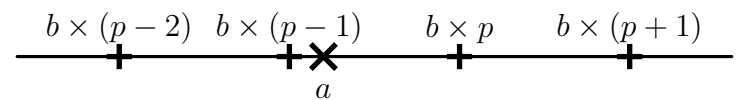
Soit $E = \{n \in \mathbb{N} \mid b \times n > a\}$. Observons que l'ensemble E est une partie de $\mathbb{N}$, qu'elle contient a , donc est non vide. Ainsi, d'après l'axiome du plus petit élément, E contient un minimum, que l'on notera p .

Observons que $p \neq 0$, sinon on aurait $b \times 0 = 0 > a$, donc $a < 0$ et ainsi, si on pose $q = p - 1$, l'entier q est un entier positif ou nul.

Par définition de p , q n'est pas un élément de E donc : $b \times q \leq a$.

Enfin, comme $b \times p > a$, on a : $a < b \times p = b \times (q + 1)$.

Finalement : $b \times q \leq a < b \times (q + 1)$ où $q \in \mathbb{N}$ et donc $0 \leq a - b \times q < b$.



Notons $r = a - bq$. Alors on a bien un couple d'entiers naturels $(q; r)$ tel que

$$\begin{cases} a = b \times q + r \\ 0 \leq r < b \end{cases}$$

Unicité :

Supposons qu'il existe un autre couple d'entiers positifs $(q'; r')$ tel que

$$\begin{cases} a = b \times q' + r' \\ 0 \leq r' < b \end{cases}$$

On déduit de $a = b \times q + r$ et $a = b \times q' + r'$ que $b \times q + r = b \times q' + r'$ et donc que $b(q - q') = r' - r$.

Cette égalité montre que : b divise $r' - r$. Or, comme $0 \leq r < b$ et $0 \leq r' < b$, on a

$$-b < r' - r < b$$

et le seul multiple de b compris strictement entre $-b$ et b est 0. Donc $r' - r = 0$ et ainsi $r' = r$.

D'où : $b(q - q') = 0$ et comme $b \neq 0$, alors $q = q'$.

Ainsi, le couple $(q; r) \in \mathbb{N}^2$ vérifiant

$$\begin{cases} a = b \times q + r \\ 0 \leq r < b \end{cases}$$

est unique. □

Exemple :

Déduire de la division euclidienne de 118 par 37, les entiers q et r tels que :

- $-118 = -37 \times q + r$ et $0 \leq r < |-37|$
- $-118 = 37 \times q + r$ et $0 \leq r < |37|$
- $-118 = -37 \times q + r$ et $0 \leq r < |-37|$

De $118 = 3 \times 37 + 7$:

- On a
$$\begin{aligned} -118 &= -37 \times 3 - 7 \\ &= -37 \times 4 + 37 - 7 \\ &= -37 \times 4 + 30 \end{aligned}$$
- donc $q = 4$ et $r = 30$.
- $-118 = 37 \times (-4) + 30$ donc $q = -4$ et $r = 30$.
- $-118 = -37 \times 4 + 30$ donc $q = 4$ et $r = 30$.

■ THÉORÈME :

Soit a un entier et b un entier non nul.

Il existe un unique couple d'entiers $(q; r)$ tel que

$$\begin{cases} a = b \times q + r \\ 0 \leq r < |b| \end{cases}$$

q est appelé le **quotient** et r est appelé le **reste** dans la division euclidienne de a par b .

Exemple :

- Effectuer la division euclidienne de -17 par 5 ; de 17 par -5 ; de -17 par -5 .
 - $-17 = 5 \times (-4) + 3$
car $-17 = -20 + 3$ et $0 \leq 3 < 5$.
 - $17 = (-5) \times (-3) + 2$
car $17 = 15 + 2$ et $0 \leq 2 < 5$.
 - $-17 = (-5) \times 4 + 3$
car $-17 = -20 + 3$ et $0 \leq 3 < 5$.
- On divise 394 par un entier naturel non nul b : le quotient est 17 et le reste est r .
Déterminer les valeurs possibles de b et r .
On a $394 = 17b + r$ avec $0 \leq r < b$.
Donc $r = 394 - 17b$ et $0 \leq 394 - 17b < b$,
i.e. $394 - 17b \geq 0$ et $394 - 17b < b$.
D'après la première inégalité :
 $b \leq \frac{394}{17} \approx 23,18$, donc $b \leq 23$.
De la seconde inégalité :
 $394 < 18b$, donc $b > \frac{394}{18} \approx 21,89$, donc $b \geq 22$.
Ainsi $b \in \{22; 23\}$.
Si $b = 22$, $r = 394 - 17 \times 22 = 394 - 374 = 20$.
Si $b = 23$, $r = 394 - 17 \times 23 = 394 - 391 = 3$.

2. Congruences

■ DÉFINITION :

Soient $n \in \mathbb{N}^*$, a et a' des entiers relatifs.

On dit que a et a' sont **congrus modulo n** si les divisions euclidiennes de a et a' par n ont le même reste. On note alors : $a \equiv a' [n]$.

Exemple :

Montrer que $14 \equiv 2 [6]$, que $-2 \equiv 5 [7]$ et que $9 \equiv -1 [10]$.

- $14 = 6 \times 2 + 2$ et $2 = 6 \times 0 + 2$, donc même reste 2.
- $-2 = 7 \times (-1) + 5$ et $5 = 7 \times 0 + 5$, donc même reste 5.
- $9 = 10 \times 0 + 9$ et $-1 = 10 \times (-1) + 9$, donc même reste 9.

■ PROPRIÉTÉ :

Soient $n \in \mathbb{N}^*$, a et a' des entiers relatifs. Alors :

$$a \equiv a' [n] \iff n | (a - a')$$

Démonstration. ($\Rightarrow$) Montrons que si

$$\begin{cases} a = n \times q + r \\ 0 \leq r < n \end{cases}, \quad \begin{cases} a' = n \times q' + r' \\ 0 \leq r' < n \end{cases}$$

et $a \equiv a' [n]$, alors : $n | (a - a')$.

Si $a \equiv a' [n]$, alors $r = r'$.

Donc $a - a' = nq + r - nq' - r' = n(q - q')$.

Ainsi n divise $(a - a')$.

($\Leftarrow$) Réciproquement, montrons que si

$$a = n \times q + r \text{ et } 0 \leq r < n$$

et n divise $(a - a')$, alors r est aussi le reste dans la division euclidienne de a' par n .

Donc $a \equiv a' [n]$.

Si $n | (a - a')$, alors $a - a' = nk$ pour un certain entier k . Donc

$$a' = a - nk = nq + r - nk = n(q - k) + r$$

Comme $0 \leq r < n$, r est bien le reste de la division de a' par n . Donc $a \equiv a' [n]$. $\square$

Exemple :

- Les congruences suivantes sont-elles vérifiées ?

$$27 \equiv 37 [3] \quad 145 \equiv 1315 [5] \quad -5 \equiv -4 [2]$$

- $37 - 27 = 10$ et $3 \nmid 10$, donc faux.
- $1315 - 145 = 1170 = 5 \times 234$, donc $5 | 1170$, donc vrai.
- $-4 - (-5) = 1$ et $2 \nmid 1$, donc faux.

Exemple :

- Si r est le reste dans la division euclidienne de a par n , alors $a \equiv r [n]$. Vrai ou faux ?
La réciproque est-elle vraie ?

Vrai car $a = nq + r$

donc $a - r = nq$ et $n|(a - r)$.

La réciproque est fautive car la condition $0 \leq r < n$ n'est pas assurée.

Contre-exemple : $16 \equiv 8 [4]$

Compléter en utilisant cette propriété :

$$27 \equiv \dots [3] \quad ; \quad -3 \equiv \dots [8] \quad ; \quad 21 \equiv \dots [5]$$

$$27 \equiv 0 [3] ; -3 \equiv 5 [8] ; 21 \equiv 1 [5]$$

- « a est divisible par n » s'exprime en termes de congruences par $a \equiv 0 [n]$

3. Propriétés des congruences

Exemple :

- Montrer que si $a \equiv b [n]$ et $b \equiv c [n]$, alors :
 $a \equiv c [n]$.

Si $a \equiv b [n]$ et $b \equiv c [n]$, alors $n|(a-b)$ et $n|(b-c)$.

Donc $n|((a-b) + (b-c))$ i.e. $n|(a-c)$.

Ainsi $a \equiv c [n]$.

- Montrer que si $a \equiv b [n]$ et $a' \equiv b' [n]$ alors :
 $a + a' \equiv b + b' [n]$ et $a \times a' \equiv b \times b' [n]$.

Si $a \equiv b [n]$ et $a' \equiv b' [n]$, alors $n|(a-b)$ et $n|(a'-b')$. Donc

$$n|((a-b) + (a'-b')) = n|((a+a') - (b+b'))$$

Ainsi $a + a' \equiv b + b' [n]$.

Puis,

$$\begin{aligned} aa' - bb' &= aa' - ab' + ab' - bb' \\ &= a(a' - b') + b'(a - b) \end{aligned}$$

Comme $n|(a' - b')$ et $n|(a - b)$, on a $n|(aa' - bb')$.

Donc $aa' \equiv bb' [n]$.

■ PROPRIÉTÉ :

Si $a \equiv b [n]$ et $a' \equiv b' [n]$ alors :

- $a + a' \equiv b + b' [n]$
- $a - a' \equiv b - b' [n]$
- $a \times a' \equiv b \times b' [n]$
- Pour tout entier naturel k non nul : $a^k \equiv b^k [n]$

Exemples :

- a et b ont pour restes respectifs 17 et 15 dans la division euclidienne par 19.

Quels sont les restes dans la division par 19 de :

$$a + b : 17 + 15 = 32 \equiv 13 [19]$$

$$ab : 17 \times 15 = 255 = 13 \times 19 + 8 \equiv 8 [19]$$

$$2a - 5b : 2 \times 17 - 5 \times 15 = 34 - 75 = -41 \\ = -41 + 3 \times 19 \equiv 16 [19]$$

$$b^2 : 15^2 = 225 = 11 \times 19 + 16 \equiv 16 [19]$$

$$a^3 : 17^3 = 4913 = 258 \times 19 + 11 \equiv 11 [19]$$

- Montrer à l'aide des congruences que, pour tout entier naturel $n : 7|(3^{2n} - 2^n)$

Soit $n \in \mathbb{N}$.

On a $3^2 = 9 \equiv 2 [7]$.

Donc $3^{2n} = (3^2)^n \equiv 2^n [7]$.

Ainsi $3^{2n} - 2^n \equiv 2^n - 2^n = 0 [7]$.

Donc $7|(3^{2n} - 2^n)$.

- Justifier que tout entier naturel n vérifie
 $n \equiv 0 [6]$, ou bien $n \equiv 1 [6]$, ou bien $n \equiv 2 [6]$,
ou bien $n \equiv 3 [6]$, ou bien $n \equiv 4 [6]$, ou bien
 $n \equiv 5 [6]$.

En déduire que, pour tout entier naturel n ,
6 divise $n(n^2 + 5)$.

Par la division euclidienne, tout entier n peut s'écrire sous la forme $n = 6q + r$ où $q \in \mathbb{Z}$ et $r \in \{0, 1, 2, 3, 4, 5\}$. Cela signifie que $n \equiv r [6]$ avec $r \in \{0, 1, 2, 3, 4, 5\}$.

Vérifions que $n(n^2 + 5) \equiv 0 [6]$ pour chaque cas :

- Si $n \equiv 0 [6]$,

$$n(n^2 + 5) \equiv 0 \times (0^2 + 5) \equiv 0 \times 5 \equiv 0 [6]$$

- Si $n \equiv 1 [6]$

$$n(n^2 + 5) \equiv 1 \times (1^2 + 5) \equiv 1 \times 6 \equiv 0 [6]$$

- Si $n \equiv 2 [6]$,

$$n(n^2 + 5) \equiv 2 \times (2^2 + 5) \equiv 2 \times 9 \equiv 18 \equiv 0 [6]$$

- Si $n \equiv 3 [6]$,

$$n(n^2 + 5) \equiv 3 \times (3^2 + 5) \equiv 3 \times 14 \equiv 42 \equiv 0 [6]$$

- Si $n \equiv 4 [6]$,

$$n(n^2 + 5) \equiv 4 \times (4^2 + 5) \equiv 4 \times 21 \equiv 84 \equiv 0 [6]$$

- Si $n \equiv 5 [6]$,

$$n(n^2 + 5) \equiv 5 \times (5^2 + 5) \equiv 5 \times 30 \equiv 150 \equiv 0 [6]$$

Dans tous les cas, $n(n^2 + 5) \equiv 0 [6]$, donc $6|n(n^2 + 5)$ pour tout entier naturel n .

- On souhaite calculer le reste de la division de 2^{47} par 7.

Vérifier que $2^3 \equiv 1 [7]$ puis compléter les congruences suivantes, où $k \in \mathbb{N}$.

$$2^{3k} \equiv \dots [7] \quad 2^{3k+1} \equiv \dots [7] \quad 2^{3k+2} \equiv \dots [7]$$

$$2^3 = 8 = 7 + 1 \equiv 1 [7].$$

Donc :

- $2^{3k} = (2^3)^k \equiv 1^k = 1 [7]$
- $2^{3k+1} = 2^{3k} \times 2^1 \equiv 1 \times 2 = 2 [7]$
- $2^{3k+2} = 2^{3k} \times 2^2 \equiv 1 \times 4 = 4 [7]$

En déduire la réponse au problème posé.

$$47 = 3 \times 15 + 2, \text{ donc } 2^{47} = 2^{3 \times 15 + 2} \equiv 4 [7].$$

Le reste est 4.



Attention

On a $14 \equiv 8 [6]$ et $\frac{14}{2} = 7$ et $\frac{8}{2} = 4$. Or, $7 \not\equiv 4 [6]$.
D'une manière générale, si d est un diviseur de a et b et $a \equiv b [n]$, on n'a pas $\frac{a}{d} \equiv \frac{b}{d} [n]$.

4. Application : Critères de divisibilité

On considère un entier naturel n qui s'écrit sous forme décimale : $n = \overline{a_k a_{k-1} a_{k-2} \dots a_1 a_0}$ où $a_0, a_1, \dots$ et a_k sont ses chiffres dans cette écriture.

Exemples :

- 1. Montrer que $n \equiv a_0 + a_1 + \dots + a_k [9]$.
 $n = a_0 + 10a_1 + 10^2a_2 + \dots + 10^k a_k$.
Or $10 \equiv 1 [9]$, donc $10^i \equiv 1^i = 1 [9]$ pour tout i . Ainsi $n \equiv a_0 + a_1 + \dots + a_k [9]$.
- 2. En termes de congruence, comment se traduit la phrase : « n est divisible par 9 » ?
Retrouver ainsi le critère de divisibilité par 9.
« n est divisible par 9 » se traduit par $n \equiv 0 [9]$. D'après le résultat précédent, ceci équivaut à $a_0 + a_1 + \dots + a_k \equiv 0 [9]$.
Donc : n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.
- Montrer le critère de divisibilité par 3.
De même, $10 \equiv 1 [3]$, donc

$$n \equiv a_0 + a_1 + \dots + a_k [3]$$

Ainsi : n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

- Montrer le critère de divisibilité par 5.
 $10 \equiv 0 [5]$, donc $10^i \equiv 0 [5]$ pour $i \geq 1$. Ainsi

$$n = a_0 + 10a_1 + \dots + 10^k a_k \equiv a_0 [5]$$

Donc : n est divisible par 5 si et seulement si son chiffre des unités est divisible par 5 (i.e. vaut 0 ou 5).

- Montrer que $n \equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k [11]$.
En déduire le critère de divisibilité par 11.
 $10 \equiv -1 [11]$, donc $10^i \equiv (-1)^i [11]$. Ainsi

$$\begin{aligned} n &= a_0 + 10a_1 + 10^2a_2 + \dots + 10^k a_k \\ &\equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k [11] \end{aligned}$$

Donc : n est divisible par 11 si et seulement si la somme alternée de ses chiffres (en partant des unités) est divisible par 11.

Sans calculatrice, déterminer si l'entier 978 542 257 est divisible par 11.

$$\begin{aligned} 978\,542\,257 &\equiv 7 - 5 + 2 - 2 + 4 - 5 + 8 - 7 + 9 [11] \\ &\equiv 7 - 5 + 2 - 2 + 4 - 5 + 8 - 7 + 9 [11] \\ &\equiv 11 [11] \\ &\equiv 0 [11] \end{aligned}$$

Donc 978 542 257 est divisible par 11.