COURS • 3ÈME ANNÉE MATHÉMATIQUES

Chapitre 19 — Arithmétique

◆ **Sommaire**

- 1. Raisonnement par récurrence
- 2. Divisibilité dans $\mathbb{N}$
- 3. Division euclidienne
- 4. PGCD — algorithme d'Euclide
- 5. Entiers premiers entre eux — PPCM
- 6. Nombres premiers — décomposition en facteurs premiers
- 7. Fiche mémo

◆ **L'essentiel à retenir — Objectifs du programme officiel**

- Mener un raisonnement par récurrence.
- Utiliser la divisibilité et la division euclidienne ; déterminer un reste.
- Calculer un PGCD (algorithme d'Euclide), un PPCM ; reconnaître des entiers premiers entre eux.
- Reconnaître un nombre premier ; décomposer un entier en produit de facteurs premiers.

1 Raisonnement par récurrence

◆ **Théorème — principe de récurrence**

Soit $\mathscr{P}(n)$ une propriété dépendant de l'entier naturel n, et $n_0 \in \mathbb{N}$. Si :

- **initialisation** : $\mathscr{P}(n_0)$ est vraie ;
- **hérédité** : pour tout $n \geq n_0$, si $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ est vraie ;

alors $\mathscr{P}(n)$ est vraie pour tout entier $n \geq n_0$.

◆ **Exemple corrigé**

Montrer que pour tout $n \in \mathbb{N}$, $4^n - 1$ est divisible par 3.

Solution.

- Initialisation : $4^0 - 1 = 0 = 3 \times 0$.
- Hérédité : supposons $4^n - 1 = 3k$. Alors $4^{n+1} - 1 = 4 \times 4^n - 1 = 4(3k+1) - 1 = 3(4k+1)$, divisible par 3 .
- Conclusion : la propriété est vraie pour tout $n \in \mathbb{N}$.

◆ **Exemple corrigé — une somme**

Montrer que pour tout $n \geq 1$: $1+2+\ldots+n=\dfrac{n(n+1)}{2}$.

Solution. Vrai pour $n=1$. Si c'est vrai au rang n, alors $1+\ldots+n+(n+1)=\dfrac{n(n+1)}{2}+(n+1)=\dfrac{(n+1)(n+2)}{2}$: vrai au rang $n+1$.

2 Divisibilité dans IN

◆ **Propriété — pour tous a, b de IN**

$a+b=0 \Rightarrow a=b=0$; $ab=0 \Rightarrow a=0$ ou $b=0$; $ab=1 \Rightarrow a=b=1$.

◆ **Définition**

Soit $a \in \mathbb{N}$ et $d \in I N^{*}$. On dit que d **divise** a (noté $d \mid a$) s'il existe $k \in \mathbb{N}$ tel que $a=kd$. On dit aussi que d est un **diviseur** de a et que a est un **multiple** de d.

◆ **Propriété**

- $1 \mid a$ et $a \mid a$ $(a \neq 0)$; si $a \mid b$ et $b \neq 0$ alors $1 \leq a \leq b$.
- Si $a \mid b$ et $b \mid a$ alors $a=b$; si $a \mid b$ et $b \mid c$ alors $a \mid c$.
- Si $c \mid a$ et $c \mid b$ alors $c \mid (xa+yb)$ pour tous x, y de IN, et $c \mid (a-b)$ si $a \geq b$.
- Si $c \mid a$ et c ne divise pas b, alors c ne divise pas $a+b$.

◆ **Exemple corrigé**

Trouver les entiers n tels que $n+1$ divise $n+7$. Comme $n+1 \mid n+1$, on a $n+1 \mid (n+7)-(n+1)=6$: $n+1 \in \{1;2;3;6\}$, soit $n \in \{0;1;2;5\}$ (on vérifie que ces valeurs conviennent).

3 Division euclidienne

◆ **Théorème**

Soit $a \in \mathbb{N}$ et $b \in I N^{*}$. Il existe un **unique** couple $(q;r)$ d'entiers naturels tel que $a=bq+r$ et $0 \leq r < b$.

q est le **quotient** et r le **reste** de la division euclidienne de a par b. On a $q=E\left(\dfrac{a}{b}\right)$ (partie entière) et $r=a-bq$.

◆ **Démonstration — unicité**

Si $a=bq+r=bq'+r'$ avec $0 \leq r, r' < b$, alors $b \mid q-q' \mid = \mid r'-r \mid < b$, donc $\mid q-q' \mid < 1$: $q=q'$, puis $r=r'$.

◆ Remarque

$b \mid a$ si et seulement si le reste de la division de a par b est nul. Tout entier s'écrit $2k$ ou $2k+1$; $3k$, $3k+1$ ou $3k+2$; etc.

◆ Exemple corrigé

Montrer que $n(n+1)(n+2)$ est divisible par 3 : si $n=3k$, $3 \mid n$; si $n=3k+1$, $3 \mid n+2$; si $n=3k+2$, $3 \mid n+1$.

4 PGCD — algorithme d'Euclide

◆ Définition

Soit a, b dans $I\!N^*$. Le **PGCD** de a et b, noté $a \wedge b$, est le plus grand de leurs diviseurs communs. Les diviseurs communs à a et b sont exactement les diviseurs de $a \wedge b$.

◆ Théorème — lemme d'Euclide

Si r est le reste de la division euclidienne de a par b, alors $a \wedge b = b \wedge r$ (avec la convention $b \wedge 0 = b$).

◆ Démonstration

$r = a - bq$: tout diviseur commun de a et b divise r ; et $a = bq + r$: tout diviseur commun de b et r divise a. Les deux couples ont donc les mêmes diviseurs communs.

◆ Méthode — algorithme d'Euclide

On effectue les divisions successives $a = bq_1 + r_1$, $b = r_1 q_2 + r_2$, $r_1 = r_2 q_3 + r_3$, … La suite des restes est strictement décroissante dans $I\!N$, donc elle atteint 0. Le PGCD est le **dernier reste non nul**.

Division	Quotient	Reste
$385 = 140 \times 2 + 105$	2	105
$140 = 105 \times 1 + 35$	1	35
$105 = 35 \times 3 + 0$	3	0

Le dernier reste non nul est 35 : $385 \wedge 140 = 35$.

◆ Propriété

- $(ka) \wedge (kb) = k(a \wedge b)$ pour $k \in I\!N^*$.
- Si $d = a \wedge b$, alors $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$.

5 Entiers premiers entre eux — PPCM

◆ Définition

- a et b sont **premiers entre eux** (ou étrangers) si $a \wedge b = 1$.
- Le **PPCM** de a et b, noté $a \vee b$, est le plus petit multiple commun non nul de a et b. Les multiples communs à a et b sont les multiples de $a \vee b$.

◆ Théorème

Pour tous a, b de $I N^{*}$: $(a \wedge b) \times (a \vee b) = ab$.

◆ Exemple corrigé

- $385 \wedge 144$: $385 = 144 \times 2 + 97$, $144 = 97 \times 1 + 47$, $97 = 47 \times 2 + 3$, $47 = 3 \times 15 + 2$, $3 = 2 \times 1 + 1$, $2 = 1 \times 2 + 0$: le PGCD vaut 1, ces nombres sont premiers entre eux.
- $385 \vee 140 = \dfrac{385 \times 140}{35} = 1540$.

6 Nombres premiers — décomposition en facteurs premiers

◆ Définition

Un entier naturel p est **premier** s'il admet exactement deux diviseurs : 1 et p. (1 n'est pas premier.)

◆ Théorème

- Tout entier $n \geq 2$ admet au moins un diviseur premier ; si n n'est pas premier, il admet un diviseur premier p tel que $p^2 \leq n$.
- Il existe une infinité de nombres premiers.
- Tout entier $n \geq 2$ se décompose en produit de facteurs premiers, de manière unique à l'ordre près : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

◆ Démonstration — infinité des nombres premiers

Supposons qu'il n'y en ait qu'un nombre fini $p_1, \dots, p_k$. L'entier $N = p_1 p_2 \dots p_k + 1 \geq 2$ admet un diviseur premier p_i ; alors p_i divise $N - p_1 \dots p_k = 1$: absurde.

◆ Méthode — reconnaître un nombre premier

On teste la divisibilité de n par les nombres premiers p tels que $p^2 \leq n$. Si aucun ne divise n, alors n est premier. Exemple : 211 n'est divisible ni par $2, 3, 5, 7, 11, 13$ ($17^2 = 289 > 211$) : 211 est premier.

crible d'Ératosthène : les 25 nombres premiers inférieurs à 100

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

◆ Propriété — PGCD et PPCM par décomposition

$a \wedge b$ est le produit des facteurs premiers communs affectés du plus petit exposant ; $a \vee b$ est le produit de tous les facteurs premiers affectés du plus grand exposant. Exemple : $36 = 2^2 \times 3^2$, $24 = 2^3 \times 3$: $36 \wedge 24 = 2^2 \times 3 = 12$ et $36 \vee 24 = 2^3 \times 3^2 = 72$.

◆ Propriété — nombre de diviseurs

Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, le nombre de diviseurs de n est $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$. Exemple : $36 = 2^2 \times 3^2$ a $3 \times 3 = 9$ diviseurs.

★ Fiche mémo

Notion	À retenir
Récurrence	initialisation + hérédité
Division euclidienne	$a = bq + r,\ 0 \le r < b$ (unique)
Euclide	$a \wedge b = b \wedge r$; PGCD = dernier reste non nul
PGCD × PPCM	$(a \wedge b)(a \vee b) = ab$
Premiers entre eux	$a \wedge b = 1$
Test de primalité	diviseurs premiers p avec $p^2 \le n$
Décomposition	unique ; diviseurs : $(\alpha_1 + 1) \dots (\alpha_k + 1)$