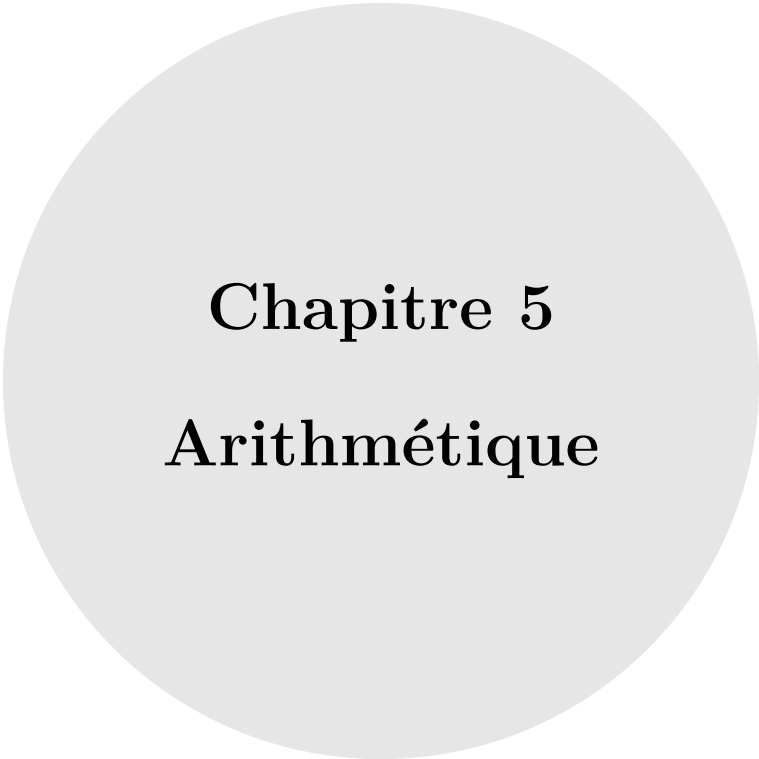




Chapitre 5

Arithmétique

Mathématiques avec M. Cacitti

PCSI du lycée Paul Eluard de Saint-Denis

Année scolaire 2026-2027

1 Diviseurs et multiples

Définition 1 : Diviseur et multiple

Soient $a, b \in \mathbb{Z}$. S'il existe $k \in \mathbb{Z}$ tel que

$$a = kb$$

alors on dit que :

- b **divise** a , ce que l'on note $b \mid a$;
- b est un **diviseur** de a ;
- a est un **multiple** de b .

Exemples.

- 1 et -1 divisent tous les entiers.
- 0 ne divise que 0 car $0 = 0 \times 0$ et, pour tous $a \in \mathbb{Z}^*$ et $k \in \mathbb{Z}$, $a \neq k \times 0$.
- Pour tout $b \in \mathbb{Z}$, $b \mid 0$ car $0 = 0 \times b$.

Exercice 1. Soit $a \in \mathbb{Z}$. On note $a\mathbb{Z}$ (ou $\mathcal{M}(a)$) l'ensemble des multiples de a et $\mathcal{D}(a)$ l'ensemble des diviseurs de a .

1. Ecrire $a\mathbb{Z}$ en écriture paramétrique et $\mathcal{D}(a)$ en compréhension par condition.
2. Soit $b \in \mathbb{Z}$. A quelle condition a-t-on une inclusion entre $a\mathbb{Z}$ et $b\mathbb{Z}$?
3. Même question pour $\mathcal{D}(a)$ et $\mathcal{D}(b)$.

Proposition 1 : Propriétés de la divisibilité

Soient $a, b, c \in \mathbb{Z}$. La divisibilité vérifie les propriétés suivantes.

- **Réflexivité** : $a \mid a$.
- **Antisymétrie** : si $a \mid b$ et $b \mid a$ alors $a = b$ ou $a = -b$.
- **Transitivité** : si $a \mid b$ et $b \mid c$ alors $a \mid c$.
- **Compatibilité avec l'addition** : si $a \mid b$ et $a \mid c$ alors $a \mid b + c$.

Démonstration. On raisonne en utilisant la définition de divisibilité avec des entiers k .

Exemple. $3 \mid 81$ et $81 \mid 162$ donc $3 \mid 162$ puis $3 \mid 81 + 162 = 243$.

Exercice 2. Soit $(a, b, c, \lambda, \mu) \in \mathbb{Z}^5$.

- Montrer que : $[c \mid a, c \mid b] \implies c \mid \lambda a + \mu b$.
- Montrer que si $a \mid b$ alors $a \mid bc$ même si a ne divise pas c .
- Montrer que la réciproque de la compatibilité avec l'addition est fausse.

2 Division euclidienne

Théorème 1 : Division euclidienne

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r$$

et

$$0 \leq r < |b|.$$

- L'égalité $a = bq + r$ est appelée la **division euclidienne** de a par b .
- L'entier q est appelé le **quotient** de cette division euclidienne.
- L'entier r est appelé le **reste** de cette division euclidienne.

Démonstration. On montre l'existence et l'unicité séparément.

- Pour l'existence, on traite d'abord le cas $b \geq 1$ en montrant, par récurrence forte, la propriété $P(a)$: « Il existe un couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$. ». On traite ensuite le cas $b \leq -1$ en utilisant $-b \geq 1$.
- Pour l'unicité, on suppose qu'il existe deux couples (q, r) et (q', r') vérifiant les propriétés souhaitées et on montre que nécessairement $r = r'$ et $q = q'$.

Exemples.

- Si $a, b > 0$ alors on procède classiquement. Par exemple, la division euclidienne de 951 par 9 donne :

$$\begin{array}{r} 9 \ 5 \ 1 \ | \ 9 \\ - \ 9 \\ \hline 0 \ 5 \\ - \ 0 \\ \hline 5 \ 1 \\ - \ 4 \ 5 \\ \hline 6 \end{array}$$

Donc

$$951 = 9 \times 104 + 6 \quad \text{et} \quad 0 \leq 6 < 9.$$

- Si $a < 0$ et $b > 0$ alors on effectue d'abord la division de $-a$ par b puis on se ramène à la division de a par b . Par exemple, pour la division euclidienne de -951 par 9, $951 = 9 \times 104 + 6$ donc

$$-951 = 9 \times (-104) - 6 = 9 \times (-105) + 9 - 6 = 9 \times (-105) + 3 \quad \text{et} \quad 0 \leq 3 < 9.$$

- Si $a > 0$ et $b < 0$ alors on écrit juste que $bq = (-b)(-q)$. Par exemple, pour la division euclidienne de 951 par -9 , $951 = 9 \times 104 + 6$ donc

$$951 = (-9) \times (-104) + 6 \quad \text{et} \quad 0 \leq 6 < |-9|.$$

- Si $a < 0$ et $b < 0$ alors on adapte les deux points précédents. Par exemple, pour la division euclidienne de -951 par -9 , nous avons $-951 = 9 \times (-105) + 3$ donc

$$-951 = (-9) \times 105 + 3 \quad \text{et} \quad 0 \leq 3 < |-9|.$$

Exercice 3. Déterminer les divisions euclidiennes suivantes : 17 par 4 ; 17 par -4 ; -17 par 4 ; -17 par -4 .

Proposition 2 : Algorithme en Python

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. La fonction Python suivante renvoie le quotient et le reste de la division euclidienne de a par b .

```
def div_eucl(a,b) :  
    q = 0  
    r = a  
    if a >= b :  
        while r >= b :  
            r = r - b  
            q = q + 1  
    else :  
        while r < 0 :  
            r = r + b  
            q = q - 1  
    return q,r
```

Démonstration. On procède par disjonction des cas ($a \geq b$ et $a < b$). Dans les deux cas on vérifie que nous avons les deux propriétés $a = bq + r$ et $0 \leq r < b$. Autrement dit $bq + r$ est un invariant de boucle qui vaut toujours a . De plus l'algorithme se termine bien car la quantité r est un entier qui va soit devenir strictement inférieur à b soit devenir strictement supérieur à 0.

Exemple. Pour effectuer la division euclidienne de 31 par 4 voici le tableau d'avancement des variables.

a	b	q	r
31	4	0	31
		1	27
		2	23
		3	19
		4	15
		5	11
		6	7
		7	3

Donc la division euclidienne de 31 par 4 est

$$31 = 4 \times 7 + 3 \quad \text{et} \quad 0 \leq 3 < 4.$$

Exercice 4. Dresser les tableaux d'avancement des variables pour les divisions euclidiennes suivantes : 30 par 7 et -23 par 3.

Proposition 3 : Divisibilité et division euclidienne

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. b divise a si et seulement si le reste dans la division euclidienne de a par b est nul.

Démonstration. On procède par double implication.

Exemples. Les divisions euclidiennes précédentes montrent que 9 ne divise pas 951 et que 4 ne divise pas 31.

Exercice 5. Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{Z}^*$. Montrer que les divisions euclidiennes de a par c et de b par c ont le même reste si et seulement si $c \mid a - b$.

3 PGCD

Définition 2 : Ensemble des diviseurs communs

Soient $a, b \in \mathbb{Z}$. L'ensemble $\mathcal{D}(a, b)$ est l'ensemble des entiers relatifs qui divisent à la fois a et b :

$$\mathcal{D}(a, b) = \{d \in \mathbb{Z} \mid d \mid a, d \mid b\} = \left\{d \in \mathbb{Z} \mid \exists (k, \ell) \in \mathbb{Z}^2, a = kd, b = \ell d\right\}.$$

Exemple. $\mathcal{D}(12, 18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Exercice 6. Soient $a, b \in \mathbb{Z}$.

1. A quoi est égal $\mathcal{D}(a, b)$ si $b \mid a$?
2. Dans le cas général, exprimer $\mathcal{D}(a, b)$ à l'aide de $\mathcal{D}(a)$ et $\mathcal{D}(b)$.

Définition 3 : PGCD

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Le **plus grand commun diviseur (PGCD)** des entiers a et b , noté $\text{PGCD}(a, b)$ ou $a \wedge b$, est l'entier naturel $\max(\mathcal{D}(a, b))$.

Exemple. Comme $\mathcal{D}(12, 18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$, $12 \wedge 18 = 6$.

Exercice 7. Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

1. Si $a \neq 0$ alors que vaut $a \wedge 0$?
2. Même question pour $a \wedge 1$.
3. Si $b \mid a$ alors que vaut $a \wedge b$?

Lemme 1

Soient $a, b, q, r \in \mathbb{Z}$ tels que $a = bq + r$. Alors $\mathcal{D}(a, b) = \mathcal{D}(b, r)$. Ainsi $a \wedge b = b \wedge r$.

Démonstration. On montre l'égalité des ensembles $\mathcal{D}(a, b)$ et $\mathcal{D}(b, r)$ par double inclusion.

Proposition 4 : Algorithme d'Euclide

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. L'algorithme suivant, appelé **algorithme d'Euclide**, permet de déterminer le PGCD entre a et b .

1. On pose $r_0 = a$ et $r_1 = b$.
2. On définit successivement des couples (q_k, r_k) de la façon suivante.
 - On écrit la division euclidienne de $a = r_0$ par $b = r_1$: il existe un (unique) couple $(q_2, r_2) \in \mathbb{Z}$ tel que

$$a = bq_2 + r_2 \quad \text{et} \quad 0 \leq r_2 < |b|.$$

Autrement dit

$$r_0 = r_1q_2 + r_2 \quad \text{et} \quad 0 \leq r_2 < |r_1|.$$

- Pour tout $k \geq 2$, si on a construit (q_k, r_k) et si $r_k \neq 0$ alors on construit (q_{k+1}, r_{k+1}) par la division euclidienne de r_{k-1} par r_k :

$$r_{k-1} = r_kq_{k+1} + r_{k+1} \quad \text{et} \quad 0 \leq r_{k+1} < r_k.$$

3. Comme les restes $r_k, k \geq 2$, forment une famille strictement décroissante d'entiers naturels, il existe un rang $n \geq 1$ tel que $r_n \neq 0$ et $r_{n+1} = 0$. Ainsi

$$a \wedge b = r_n.$$

Démonstration. On utilise le lemme précédent avec la famille $(r_k)_{0 \leq k \leq n}$.

Remarques. Autrement dit, on effectue des divisions euclidiennes successives jusqu'à obtenir un reste nul. Dans ce cas, le PGCD est le dernier reste non nul.

Exemple. Pour déterminer le PGCD entre 4539 et 1958 :

- $4539 = 1958 \times 2 + 623$ et $0 \leq 623 < 1958$;
- $1958 = 623 \times 3 + 89$ et $0 \leq 89 < 623$;
- $623 = 89 \times 7 + 0$ et $0 \leq 0 < 89$.

Donc $4539 \wedge 1958 = 89$.

Exercice 8. Déterminer le PGCD entre 233 et 144 à l'aide de l'algorithme d'Euclide.

Proposition 5 : Relation de Bézout

Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Il existe $(u, v) \in \mathbb{Z}^2$ (non unique) tel que

$$a \wedge b = au + bv.$$

Cette relation est appelée une **relation de Bézout** (ou **identité de Bézout**).

Démonstration admise.

Remarque. Elle peut être obtenue en « remontant » l'algorithme d'Euclide. Il s'agit alors de l'algorithme d'Euclide étendu pour obtenir une telle identité de Bézout.

Exemple. D'après l'exemple précédent, $4539 \wedge 1958 = 89$ et nous avons les divisions euclidiennes successives. Donc une identité de Bézout est donnée par :

$$\begin{aligned} 89 &= 1958 - 623 \times 3 \\ &= 1958 - (4539 - 1958 \times 2) \times 3 \\ &= 1958 \times 7 - 4539 \times 3. \end{aligned}$$

Exercice 9. On cherche à résoudre l'équation $19x + 41y = 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

1. Déterminer le PGCD entre 19 et 41.
2. Résoudre l'équation $19x + 41y = 0$ d'inconnue $(x, y) \in \mathbb{Z}^2$.
3. Déterminer une solution particulière de l'équation $19x + 41y = 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$.
4. En déduire une solution particulière de l'équation $19x + 41y = 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$.
5. Résoudre l'équation $19x + 41y = 2$ d'inconnue $(x, y) \in \mathbb{Z}$.

Exercice 10. Soit $(a, b, c) \in \mathbb{Z}^3$. On dit que a et b sont premiers entre eux si leur seul diviseur commun positif est 1. Autrement dit, si $a \wedge b = 1$. Montrer, à l'aide d'une relation de Bézout, le **lemme de Gauss** : $[a \mid bc, a \wedge b = 1] \implies a \mid c$.

Remarque. Attention si $d = au + bv$ alors d n'est pas nécessairement le PGCD de a et b . Dans ce cas, nous avons seulement que $a \wedge b \mid d$.

Exemple. $66 \times 2 - 42 \times 2 = 48$ n'est pas une relation de Bézout entre 66 et 42 car $66 \wedge 42 = 6 \neq 48$. Par contre $66 \times 2 - 42 \times 3 = 6$ en est une.

Corollaire 1 : Diviseur commun et PGCD

Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $d \in \mathbb{Z}^*$. L'entier d divise a et b si et seulement s'il divise $a \wedge b$.

Démonstration. On procède par double implication.

Exemple. $4539 \wedge 1958 = 89$ et les diviseurs de 89 sont $\pm 1, \pm 89$ donc il s'agit des seuls diviseurs communs de 4539 et 1958.

Exercice 11. Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Donner le lien entre $\mathcal{D}(a)$, $\mathcal{D}(b)$ et $\mathcal{D}(a \wedge b)$.

Proposition 6 : PGCD et multiplication

Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $k \in \mathbb{N}^*$. Alors le PGCD de ka et kb est k multiplié par le PGCD de a et b :

$$(ka) \wedge (kb) = k \times (a \wedge b).$$

Démonstration. En notant $d = a \wedge b$ et $d' = (ka) \wedge (kb)$, on utilise des identités de Bézout pour montrer que $d' \mid kd$ et $kd \mid d'$. Puis on conclut, par positivité, que $d' = kd$.

Exemple. Le PGCD de 24 et 33 est 3 car : $24 \wedge 33 = (3 \times 8) \wedge (3 \times 11) = 3 \times (8 \wedge 11) = 3 \times 1 = 3$.

Exercice 12.

1. Déterminer le PGCD entre 16 et 56.
2. En déduire le PGCD entre 32 et 112.
3. Déterminer une relation de Bézout entre 16 et 56 puis une relation de Bézout entre 32 et 112.

4 PPCM

Définition 4 : Ensemble des multiples communs

Soit $(a, b) \in \mathbb{Z}^2$. L'ensemble $\mathcal{M}(a, b)$ est l'ensemble des entiers relatifs qui sont des multiples à la fois de a et de b :

$$\mathcal{M}(a, b) = \{m \in \mathbb{Z} \mid a \mid m, b \mid m\} = \left\{m \in \mathbb{Z} \mid \exists (k, \ell) \in \mathbb{Z}^2, m = ka, m = \ell b\right\}.$$

Exemple. $\mathcal{M}(8, 12) = \{0, \pm 24, \pm 48, \pm 72, \pm 96, \dots\}$.

Exercice 13. Soit $(a, b) \in \mathbb{Z}^2$.

1. A quoi est égal $\mathcal{M}(a, 0)$?
2. Même question pour $\mathcal{M}(a, b)$ si $b \mid a$.
3. Dans le cas général, exprimer $\mathcal{M}(a, b)$ à l'aide de $a\mathbb{Z}$ et $b\mathbb{Z}$.

Définition 5 : PPCM

Soit $(a, b) \in (\mathbb{Z}^*)^2$. Le **plus petit commun multiple (PPCM)** des entiers a et b , noté $PPCM(a, b)$ ou $a \vee b$, est l'entier naturel $\min(\mathcal{M}(a, b) \cap \mathbb{N}^*)$.

Remarque. Le PPCM est défini dans $\mathbb{N}^*$ car sinon 0 serait le PPCM de tout couple d'entiers. Par convention, pour tout $a \in \mathbb{Z}$, on définit $a \vee 0 = 0$.

Exemple. Le PPCM de 8 et 12 est 24 car $8 \times 3 = 24 = 12 \times 1$ et 12 n'est pas un multiple de 8.

Exercice 14. Soient $(a, b) \in (\mathbb{Z}^*)^2$.

1. Déterminer $a \vee 1$.
2. Si $b \mid a$ alors que vaut $a \vee b$?

Proposition 7 : PGCD et PPCM

Soit $(a, b) \in (\mathbb{Z}^*)^2$. Alors $(a \wedge b) \times (a \vee b) = |ab|$.

Démonstration. En notant $d = a \wedge b$, il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$ avec a' et b' premiers entre eux. En utilisant le lemme de Gauss, on montre que $a \vee b = d|a'b'|$. Ainsi $d \times (a \vee b) = |da'db'| = |ab|$.

Exemples.

- $8 \vee 12 = 24$ et $8 \wedge 12 = 4$ donc nous avons bien $24 \times 4 = 96 = 8 \times 12$.
- $4539 \wedge 1958 = 89$ donc $4539 \vee 1958 = \frac{4539 \times 1958}{89} = 4539 \times \frac{1958}{89} = 4539 \times 22 = 99858$.

Exercice 15. Soient $(a, b) \in (\mathbb{Z}^*)^2$ et $k \in \mathbb{Z}^*$. Simplifier $(ka) \vee (kb)$.

5 Nombres premiers

Définition 6 : Nombre premier, nombre composé

Un entier p supérieur à 2 est **premier** si ses seuls diviseurs positifs sont 1 et p :

$$\mathcal{D}(p) \cap \mathbb{N} = \{1, p\}.$$

Sinon on dit que p est **composé**.

On note $\mathcal{P}$ l'ensemble des nombres premiers :

$$\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}.$$

Exemples. Le plus grand nombre premier inférieur à 100 est 97 et le plus grand nombre premier inférieur à 1000 est 997. 1 n'est ni un nombre premier (car n'admet qu'un seul diviseur positif) ni un nombre composé car il n'est pas supérieur à 2.

Exercice 16. Soient $(p, a, b) \in \mathbb{Z}$.

1. Montrer le **lemme d'Euclide** : $[p \in \mathcal{P}, p \mid bc] \implies [p \mid b \text{ ou } p \mid c]$.
2. Donner un exemple où l'implication $p \mid bc \implies [p \mid b \text{ ou } p \mid c]$ est fausse.

Définition 7 : Facteur premier

Soient n et p deux entiers supérieurs à 2. On dit que p est un **facteur premier** de n si p est premier et divise n :

$$p \in \mathcal{P} \quad \text{et} \quad p \mid n.$$

Exemples.

- 98 est un nombre composé qui admet 2 et 49 comme facteurs donc 2 et 7 comme facteurs premiers.
- 999 est un nombre composé qui admet 9 et 111 donc 3 et 37 comme facteurs premiers.

Exercice 17. On considère $\mathcal{P}_{10}$ les nombres premiers compris entre 2 et 10.

1. Ecrire l'ensemble $\mathcal{P}_{10}$ en extension et en compréhension par condition.
2. On considère E l'ensemble suivant : $E_{10} = \{pq \mid (p, q) \in \mathcal{P}_{10}^2\}$. Ecrire explicitement l'ensemble E .
3. Combien d'éléments possède l'ensemble E_{10} ?
4. A partir de n_{100} le nombre de nombres premiers compris entre 2 et 100, donner le nombre d'éléments de l'ensemble E_{100} .

Lemme 2

Soit n un entier supérieur à 2. Alors n admet un facteur premier :

$$\exists p \in \mathcal{P}, p \mid n.$$

Plus précisément, si n n'est pas premier alors n admet un facteur premier compris entre 2 et $\sqrt{n}$.

Démonstration. On procède par récurrence forte sur $n \geq 2$ pour la première partie du lemme. Pour la seconde partie, si n n'est pas premier alors il existe $p \in \mathcal{P}$ et $k \geq 2$ entier tel que $n = pk$. On raisonne alors par disjonction des cas ($p > \sqrt{n}$ ou $k > \sqrt{n}$).

Remarque. Nous pouvons appliquer le lemme précédent pour le crible d’Eratosthène. Par exemple tout nombre non premier inférieur à 100 possède un facteur premier inférieur à 10. Donc pour trouver les nombres premiers entre 1 et 100, il suffit d’éliminer les multiples (non triviaux) de 2, 3, 5 et 7.

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

Proposition 8 : Infinité de nombres premiers

Il existe une infinité de nombres premiers.

Démonstration. On raisonne par l’absurde avec $p_1, p_2, \dots, p_r \in \mathcal{P}$ et $p = p_1 p_2 \cdots p_r + 1$.

Exercice 18. Soit $n \in \mathbb{N}^*$.

1. Si on considère les n premiers nombres premiers $p_1, p_2, \dots, p_n$ alors $p = p_1 \times p_2 \times \cdots \times p_n + 1$ est-il un nombre premier ?
2. Montrer qu’il existe un nombre premier supérieur à n . En donner un explicitement.

Théorème 2 : Factorisation en nombres premiers

Soit $n \geq 2$ entier naturel. Alors il existe $m \in \mathbb{N}$, $p_1, \dots, p_m \in \mathcal{P}$ deux à deux distincts et $\nu_1, \dots, \nu_m \in \mathbb{N}^*$ tels que

$$n = \prod_{k=1}^m p_k^{\nu_k}.$$

De plus, cette factorisation (ou décomposition en produit) est unique à l’ordre des facteurs près.

Démonstration admise.

Exemples.

- La décomposition en facteurs premiers de 99 est $99 = 3^2 \times 11$ car $99 = 3 \times 33 = 3 \times 3 \times 11$.
- Celle de 231 est $231 = 3 \times 7 \times 11$ car $231 = 3 \times 77 = 3 \times 7 \times 11$.
- Celle de 17 est $17 = 17$ car 17 est un nombre premier.

Exercice 19. On considère $n = 10!$.

1. Déterminer la factorisation en nombres premiers de n .
2. Combien le nombre n a-t-il de diviseurs positifs ? De diviseurs ?

Remarque. On peut également noter $n = \prod_{p \in \mathcal{P}} p^{\nu_p}$ avec $\nu_p = 0$ pour les nombres premiers p qui ne sont pas des facteurs premiers de n . On dit que ν_p est la **valuation p -adique** de n .

Proposition 9 : Décomposition et diviseurs

Soient $n \geq 2$ entier et $n = \prod_{k=1}^m p_k^{\nu_k}$ sa décomposition en produit de facteurs premiers. Alors les diviseurs de n sont exactement les entiers de la forme $d = \prod_{k=1}^m p_k^{\mu_k}$ où, pour tout $k \in \llbracket 1, m \rrbracket$, $\mu_k \in \llbracket 0, \nu_k \rrbracket$.

Démonstration. On raisonne par analyse-synthèse en utilisant les factorisations de n et de d .

Exemples. Les diviseurs de 99 sont

$$3^0 \times 11^0 = 1, \quad 3^1 \times 11^0 = 3, \quad 3^2 \times 11^0 = 9, \quad 3^0 \times 11^1 = 11, \quad 3^1 \times 11^1 = 33, \quad 3^2 \times 11^1 = 99.$$

En particulier 99 admet 6 diviseurs positifs donc 12 diviseurs.

Exercice 20. On considère le nombre $n = 1225$.

1. Donner la décomposition de n en produit de nombres premiers.
2. En déduire la liste des diviseurs de n et leur nombre.

Corollaire 2 : Nombre de diviseurs

Soient $n \geq 2$ entier et $n = \prod_{k=1}^m p_k^{\nu_k}$ sa décomposition en produit de facteurs premiers. Alors le nombre de diviseurs positifs de n est $\prod_{k=1}^m (\nu_k + 1)$.

Démonstration. On utilise la proposition précédente et on dénombre les μ_k possibles.

Exemples.

- $99 = 3^2 \times 11$ donc admet 3 et 11 comme seuls facteurs premiers et leurs valuations sont $\nu_3 = 2$ et $\nu_{11} = 1$. Donc le nombre de diviseurs positifs de 99 est bien $6 = (2 + 1) \times (1 + 1)$.
- 1225 admet 5 et 7 comme seuls facteurs premiers et leurs valuations sont 2. Donc le nombre de diviseurs positifs de 1225 est bien $9 = (2 + 1) \times (2 + 1)$.

Exercice 21. Soient $a, b \geq 2$ entiers dont les factorisations sont notées $a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$ et $b = \prod_{p \in \mathcal{P}} p^{\nu_p(b)}$.

- Ecrire le nombre de diviseurs positifs de a à partir de sa factorisation.
- Faire de même avec $a \times b$. Autrement dit, quelle est l'expression de $\nu_p(a \times b)$?
- On suppose que $b \mid a$. On note $c \in \mathbb{N}$ tel que $a = bc$. Donner la factorisation de c en nombres premiers et son nombre de diviseurs positifs.

Proposition 10 : Décomposition, PGCD et PPCM

Soient $a, b \geq 2$ entiers et $a = \prod_{p \in \mathcal{P}} p^{\nu_p}$, $b = \prod_{p \in \mathcal{P}} p^{\mu_p}$ leurs décompositions en produit de nombres premiers.

Alors :

- $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)}$;
- $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}$.

Démonstration. On décompose $a \wedge b = \prod_{p \in \mathcal{P}} p^{\lambda_p}$ diviseur commun de a et b pour obtenir $\lambda_p \leq \min(\nu_p, \mu_p)$

pour tout $p \in \mathcal{P}$. Puis on raisonne par l'absurde pour montrer que $\lambda_p = \min(\nu_p, \mu_p)$. Pour le PPCM on utilise la propriété $(a \wedge b) \times (a \vee b) = ab$.

Exemples.

- $99 = 3^2 \times 11$ et $1225 = 5^2 \times 7^2$ donc $99 \wedge 1225 = 1$, autrement dit, ils sont premiers entre eux. Donc $99 \vee 1225 = 99 \times 1225$.
- $231 = 3 \times 7 \times 11$ donc $99 \wedge 231 = 3 \times 11 = 33$ et $99 \vee 231 = 3^2 \times 7 \times 11 = 693$.

Exercice 22. On considère les nombres $a = 120$ et $b = 700$.

1. Donner les décompositions en produit de nombres premiers de a et b .
2. En déduire le nombre de diviseurs positifs de a et b .
3. Donner les valeurs de $a \wedge b$ et $a \vee b$.

6 Exercices

6.1 Divisibilité

Exercice 23. Soit $n \in \mathbb{Z}$.

1. Montrer que $n(n+1)$ est pair.
2. Montrer que si n est impair alors $n^2 - 1$ est un multiple de 8.
3. Montrer que $n(n+1)(n+2)$ est un multiple de 6.
4. Montrer que si $n \geq 0$ alors $4^n - 1 - 3n$ est un multiple de 9.

Exercice 24.

1. Déterminer les entiers $n \in \mathbb{Z}$ tels que 6 divise $n+5$.
2. Déterminer les entiers $n \in \mathbb{Z}$ tels que $n-2$ divise $n+2$.
3. Déterminer les entiers $n \in \mathbb{Z}$ tels que $4n-2$ divise $5n+2$.

Exercice 25. Soient $n \in \mathbb{N}^*$, N le nombre de diviseurs positifs de n et P leur produit. Quelle relation existe-t-il entre n , N et P ?

Exercice 26. Résoudre dans $\mathbb{Z}^2$ les équations suivantes.

1. $xy = 3x + 2y$
2. $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$
3. $x^2 - y^2 - 4x - 2y = 5$

Exercice 27. Soit $n \in \mathbb{N}$.

1. Montrer :

$$\sqrt{n} \in \mathbb{Q} \iff \exists m \in \mathbb{N}, n = m^2.$$

2. En déduire que $\sqrt{2}$ et $\sqrt{3}$ sont irrationnels.

6.2 Division euclidienne

Exercice 28. Dans chacun des cas suivants, déterminer le quotient et le reste de la division euclidienne de a par b .

1. $a = 19$ et $b = 6$.
2. $a = -19$ et $b = 6$.
3. $a = 7500$ et $b = 33$.

Exercice 29. Déterminer les entiers $n \in \mathbb{N}$ tels que le quotient et le reste de la division euclidienne de n par 6 soient égaux.

Exercice 30.

1. Déterminer la division euclidienne de 1234 par 5.
2. En déduire, sans calculer 1234^2 , que le reste de la division euclidienne de 1234^2 par 5 vaut 1.
3. En déduire que le reste la division euclidienne de 1234^{2024} par 5 vaut 1.

Exercice 31. Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et q le quotient de la division euclidienne de $a-1$ par b . Déterminer, pour tout $n \in \mathbb{N}$, le quotient de la division euclidienne de $ab^n - 1$ par b^{n+1} .

Exercice 32. Soit $n \in \mathbb{N}^*$.

1. Montrer qu'il existe $p \in \mathbb{N}^*$ et $(a_1, \dots, a_p) \in \mathbb{N}^p$ tels que

$$n = \sum_{k=1}^p a_k \times k!$$

avec $a_k \in \llbracket 0, k \rrbracket$ pour tout $k \in \llbracket 1, p \rrbracket$, et $a_p \neq 0$. Cette écriture s'appelle son **développement factoriel**.

2. Vérifier l'unicité de cette écriture.

6.3 Algorithme d'Euclide et identité de Bézout

Exercice 33. Dans chacun des cas suivants, calculer $d = a \wedge b$ et déterminer une relation de Bézout.

1. $a = 33$ et $b = 24$.
2. $a = 342$ et $b = 95$.
3. $a = 888$ et $b = 264$.

Exercice 34. Soient $a, b, d \in \mathbb{Z}$ tels que $(a, b) \neq (0, 0)$. Montrer que les assertions suivantes sont équivalentes.

1. $\exists (u, v) \in \mathbb{Z}^2, au + bv = d$.
2. $(a \wedge b) \mid d$.

Exercice 35. Soient a et b deux entiers non nuls et $d = a \wedge b$. Notre but est de déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = d$.

1. Justifier l'existence d'un couple solution (u_0, v_0) .
2. Exprimer à partir de (u_0, v_0) tous les couples solutions.

Exercice 36. Soit $n \in \mathbb{N}$.

1. Montrer qu'il existe un unique couple $(a_n, b_n) \in \mathbb{N}^2$ tel que

$$(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}.$$

2. Calculer $a_n^2 - 2b_n^2$.
3. En déduire que a_n et b_n sont premiers entre eux.

Exercice 37. Soient $a, b \in \mathbb{N}$. Montrer, à l'aide d'identités de Bézout, que a et b sont premiers entre eux si et seulement si a et b^2 le sont.

6.4 PGCD et PPCM

Exercice 38. Déterminer tous les couples $(a, b) \in \mathbb{N}^2$ tels que $ab = 900$ et $a \wedge b = 15$.

Exercice 39. On considère un engrenage composé de deux roues dentées A et B . Les nombres de dents des deux roues sont respectivement $Z_A = 18$ et $Z_B = 21$. Combien de tours ont les deux roues quand l'engrenage revient pour la première fois dans sa position initiale ?

Exercice 40. Lister les couples $(x, y) \in \mathbb{N}^2$ qui vérifient $x \wedge y = 5$ et $x \vee y = 60$.

Exercice 41. Soit $n \in \mathbb{Z}$. Montrer que le PGCD de $2n + 4$ et $3n + 3$ ne peut être que 1, 2, 3 ou 6.

Exercice 42. Résoudre l'équation $x \wedge y + x \vee y = x + y$ d'inconnue $(x, y) \in \mathbb{N}^2 \setminus \{(0, 0)\}$.

6.5 Nombres premiers et factorisation

Exercice 43. Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}$.

1. Montrer que, pour tout $k \in \llbracket 1, p-1 \rrbracket$, p divise $\binom{p}{k}$.
2. En déduire, par récurrence, que p divise $n^p - n$.
3. En déduire que si p ne divise pas n alors p divise $n^{p-1} - 1$.

Exercice 44. Déterminer la décomposition en produit de facteurs premiers des nombres suivants et en déduire leur PGCD et leur PPCM.

1. $a = 42$ et $b = 60$.
2. $a = 210$ et $b = 225$.

Exercice 45. Soit $n \geq 2$ entier.

1. Montrer que si $2^n - 1$ est premier alors n est premier.
2. Etudier la réciproque.

Exercice 46. Soit $n \geq 2$ entier dont la factorisation en nombres premiers est $n = \prod_{k=1}^m p_k^{\nu_k}$. On note $\sigma(n)$ la somme des diviseurs positifs de n . Montrer que

$$\sigma(n) = \prod_{k=1}^m \frac{p_k^{\nu_k+1} - 1}{p_k - 1}.$$

Exercice 47. Soient $a, b \in \mathbb{Z}$ et $p \in \mathcal{P}$ tel qu'il existe $\alpha \in \mathbb{N}^*$ tel que p^α divise $a \vee b$. Montrer que p^α divise a ou b .

Table des matières

1	Diviseurs et multiples	2
2	Division euclidienne	3
3	PGCD	5
4	PPCM	8
5	Nombres premiers	9
6	Exercices	13

Programme officiel de ce chapitre

Contenus	Capacités et commentaires
Entiers naturels, entiers relatifs, divisibilité dans $\mathbb{Z}$, diviseurs, multiples.	
Théorème de la division euclidienne.	
PGCD de deux entiers relatifs dont l'un au moins est non nul.	Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbb{Z}$) de l'ensemble des diviseurs communs à a et b .
PPCM.	
Algorithme d'Euclide.	
Nombre premier.	
L'ensemble des nombres premiers est infini.	
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	La démonstration est hors programme. Application au calcul du PGCD et du PPCM.