Chapitre 14 Arithmétique dans l'ensemble des entiers

14.1 Diviseurs et multiples

Définition 14.1 - Diviseur, multiple.

Soit $a, b \in \mathbf{Z}$. On dit que a est un **diviseur** de b, ou que a **divise** b ou encore que b est un **multiple** de a, s'il existe $k \in \mathbf{Z}$ tel que $b = ka$.
Le cas échéant, on note $a \mid b$.
L'ensemble des multiples entiers de a est l'ensemble

$$\{a \cdot n \ : \ n \in \mathbf{Z}\}.$$

Exemple 14.2.

- 1 et -1 divisent tous les entiers mais ils ne sont divisibles que par 1 et -1.
- 0 est un multiple de tout entier mais n'est le diviseur que de lui-même.
- L'ensemble des diviseurs de 6 est $\{1, 2, 3, 6, -1, -2, -3, -6\}$.

Exercice d'application 14.3. Montrer que pour tout entier impair n, $n^2 - 1$ est un multiple de 8.

➥

Proposition 14.4 - Diviseur d'une combinaison linéaire.

Soit $a, b, d, \lambda, \mu \in \mathbf{Z}$. Si d divise a et b, alors d divise $\lambda a + \mu b$.

Démonstration.

Proposition 14.5 - Quelques critères de divisibilité.

Soit n un entier naturel dont l'écriture décimale est $n = \overline{a_p \ldots a_1 a_0}$, ce qui signifie que

$$n = a_p 10^p + \cdots + a_1 10^1 + a_0 10^0,$$

avec $a_i \in [\![0, 9]\!]$ pour tout $i \in [\![0, p]\!]$.

(a) n est un multiple de 2 si et seulement si a_0 est un multiple de 2, *i.e.* $a_0 \in \{0; 2; 4; 6; 8\}$.

(b) n est un multiple de 3 si et seulement si $\sum_{k=0}^{p} a_k$ est un multiple de 3.

(c) n est un multiple de 5 si et seulement si a_0 est un multiple de 5, *i.e.* $a_0 \in \{0; 5\}$.

(d) n est un multiple de 9 si et seulement si $\sum_{k=0}^{p} a_k$ est un multiple de 9.

(e) n est un multiple de 10 si et seulement si a_0 est un multiple de 10, *i.e.* $a_0 = 0$.

(f) n est un multiple de 11 si et seulement si $\sum_{k=0}^{p} (-1)^k a_k$ est un multiple de 11.

Démonstration.

Proposition 14.6 - Lien entre divisibilité et égalité pour des entiers naturels.

Soit $(a, b) \in \mathbf{Z}^2$. On a

$$(a \mid b \text{ et } b \mid a) \iff |a| = |b|.$$

Démonstration.

Proposition 14.7 - Lien entre divisibilité et ordre.

Soit $a, b \in \mathbf{Z}$ non nuls. Si b divise a alors $|b| \leqslant |a|$.

Démonstration.

14.2 Division euclidienne

Lemme 14.8 - Existence d'un plus grand élément, d'un plus petit dans une partie de N.

1. Toute partie non vide de $\mathbf{N}$ admet un plus petit élément.
2. Toute partie non vide majorée de $\mathbf{N}$ admet un plus grand élément.

Démonstration ☕.
Soit A une partie non vide de $\mathbf{N}$.

1. Supposons que A ne possède pas de plus petit élément. Posons pour tout $n \in \mathbf{N}$, H_n : « pour tout $x \in A$, $x \geqslant n$ ». Puisque $A \subset \mathbf{N}$, tout élément de A est supérieur à 0 ce qui prouve que H_0 est vraie. Soit $n \in \mathbf{N}$ tel que H_n soit vraie. On a pour tout $x \in A$, $x \geqslant n$. Puisque a ne possède pas de plus petit élément, $x \neq n$, donc $x > n$, d'où $x \geqslant n+1$. Ainsi, H_{n+1} est vraie. Le principe de récurrence assure finalement que pour tout $x \in A$, $x \geqslant n$, ce qui est absurde car si $x \in A$ est fixé, $n = x+1$ est strictement supérieur à x. Finalement, A possède un plus petit élément.
2. Supposons que A est majorée. Notons $B = \{x \in \mathbf{N} \mid \forall n \in A,\ n \leqslant x\}$ l'ensemble des majorants de A. Puisque A est majoré, $B \neq \varnothing$ et le point précédent assure qu'il existe m qui est le plus petit élément de a.
   Si $m = 0$, alors pour tout $x \in a$, $x \leqslant m$ donc $A = \{0\}$, ce qui entraîne que m est aussi le plus grand élément de A.
   Supposons $m > 0$. Alors $m-1 \notin B$ (puisque m est le plus petit élément de B), donc $m-1$ ne majore pas A. Il existe donc $a \in A$ tel que $m-1 < a \leqslant m$. Cet encadrement dans les entiers fournit $a = m$. Comme m majore A, m est bien le plus grand élément de A.
   Finalement, dans tous les cas, A possède un plus grand élément. □

Théorème 14.9 - Division euclidienne dans Z.

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

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

- q est appelé **quotient** de la division euclidienne de a par b.
- r est appelé **reste** de la division euclidienne de a par b.
- Dans ce contexte, b est le **diviseur** et a le **dividende**.

Démonstration.

Proposition 14.10 - Lien entre reste de la division euclidienne et divisibilité.

Soit $a \in \mathbf{Z}$ et $b \in \mathbf{N}^\star$. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Démonstration.
Notons q et r respectivement le quotient et le reste de la division euclidienne de a par b.
Si $r = 0$ alors on a $a = bq$ donc $b|a$.
Réciproquement, supposons que $b|a$. Alors il existe $k \in \mathbf{Z}$ tel que $a = bk + 0$. Comme $0 \in [0\,;\, b[$, par unicité du quotient et du reste dans la division euclidienne de a par b, k est le quotient de la division de a par b et 0 est le reste. □

Exemple 14.11. On peut poser l'opération :

$$\begin{array}{r|l} \overline{3\,2\,6}\,5\,6 & 1\,5\,7 \\ \cline{2-2} -\,3\,1\,4 & 2\,0\,8 \\ \cline{1-1} \quad 1\,2\,5 & \\ -\quad\;\; 0 & \\ \cline{1-1} \quad 1\,2\,5\,6 & \\ -\,1\,2\,5\,6 & \\ \cline{1-1} \qquad\;\; 0 & \end{array}$$

Ainsi, la division euclidienne de 32 656 par 157 s'écrit $32\,656 = 157 \times 208 + 0$. (32 656 est le dividende, 157 le diviseur, 208 le quotient et 0 le reste. On obtient donc que 157 divise 32 656.

Proposition 14.12 - Lien entre reste de la division euclidienne et congruences.

Soit $a \in \mathbf{Z}$, $b \in \mathbf{N}^\star$ et $r \in [\![0, b-1]\!]$. $a \equiv r\ [b]$ si et seulement si r est le reste de la division euclidienne de a par b.

Démonstration.

Remarque 14.13. En particulier, b divise a si et seulement si $a \equiv 0\ [b]$.

On peut de plus traduire certaines propriétés démontrées sur les congruences en termes de divisibilité.

Remarque 14.14. Soit $a, b, d, \lambda \in \mathbf{Z}$ avec $\lambda \neq 0$. On rappelle que si $a \equiv b\ [d]$, alors $\lambda a \equiv \lambda b\ [d]$.

Exercice d'application 14.15. Montrer que la somme des cubes de trois entiers consécutifs est toujours divisible par 9.

➥

14.3 Plus grand commun diviseur

Définition 14.16 - Plus grand commun diviseur.

Soit $(a, b) \in \mathbf{Z}^2 \setminus \{(0, 0)\}$. Soit A l'ensemble des diviseurs qui sont communs à a et b. On appelle **plus grand commun diviseur** de a et b, et on note $\text{PGCD}(a, b)$, le plus grand élément de A.

Démonstration.
L'ensemble A est non vide (il contient 1) et majoré (par $|a|$ ou $|b|$), donc il contient un plus grand élément (cf. Lemme 14.8). □

Remarque 14.17. Si a et b sont non nuls, $1 \leqslant \text{PGCD}(a, b) \leqslant \min(|a|, |b|)$. Pour tout entier $a \neq 0$, $\text{PGCD}(a, 0) = |a|$.

Exemple 14.18. Les diviseurs de 15 sont 1, 3, 5, 15, -1, -3, -5, -15 et ceux de -12 sont 1, 3, 4, 6, 12, -1, -3, -4, -6, -12. donc $\text{PGCD}(15, -12) = 3$.

Lemme 14.19 - « Simplification » du PGCD pour l'algorithme d'Euclide.

Soit $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$. On note r le reste de division euclidienne de a par b. On a

$$\text{PGCD}(a, b) = \text{PGCD}(b, r).$$

Démonstration.

Proposition 14.20 - Algorithme d'Euclide.

Soit a, b deux entiers naturels non nuls. Pour déterminer $\text{PGCD}(a, b)$, on utilise le lemme précédent et on simplifie le PGCD à déterminer jusqu'à arriver à une forme $\text{PGCD}(\alpha, 0)$, qu'on sait être égal à α :

```
tant que b > 0
    r ← reste de la division euclidienne de a par b
    a ← b
    b ← r
fin tant que
```

Une implémentation possible en Python est la suivante :

Script Python

```python
def euclide(a: int, b: int) -> int:
    while (b > 0):
        a, b = b, a % b
    return a
```

Exemple 14.21. Calculons $\text{PGCD}(210, 154)$. On a, avec l'algorithme d'Euclide

$$\begin{array}{rrcll} & 210 & = & 154 \times 1 + 56 & \text{donc } \text{PGCD}(210, 154) = \text{PGCD}(154, 56) \\ \text{puis} & 154 & = & 56 \times 2 + 42 & \text{donc } \text{PGCD}(210, 154) = \text{PGCD}(56, 42) \\ \text{puis} & 56 & = & 42 \times 1 + 14 & \text{donc } \text{PGCD}(210, 154) = \text{PGCD}(42, 14) \\ \text{puis} & 42 & = & 14 \times 3 + 0 & \text{donc } \text{PGCD}(210, 154) = \text{PGCD}(14, 0) = 14 \end{array}$$

Finalement, $\text{PGCD}(210, 154) = 14$ (14 est le dernier reste non nul obtenu).

Exercice d'application 14.22. Calculer le PGCD de 758 et 306.

➥

Définition 14.23 - Nombres premiers entre eux.

Soit $a, b \in \mathbf{Z}^\star$. On dit que a et b sont **premiers entre eux** lorsque $\text{PGCD}(a, b) = 1$.

Exemple 14.24. **1.** Montrons que 15 et 34 sont premiers entre eux. Les seuls diviseurs de 15 sont 1, 3, 5 et 15. Parmi ceux-ci, le seul qui divise aussi 34 est 1, donc $\text{PGCD}(15, 34) = 1$, ce qui montre que 15 et 34 sont premiers entre eux.

2. 123 et 369 ne sont pas premiers entre eux, puisque 3 divise 123 (critère de divisibilité par 3 : $1+2+3=6$ divisible par 3) et 369 aussi ($3+6+9=18$ divisible par 3). Ainsi, $\text{PGCD}(123, 369) \geqslant 3$.

Exercice d'application 14.25. Les nombres 300 et 291 sont-ils premiers entre eux ? Même question avec 45 et 14.

➥

Définition 14.26 - Fraction irréductible.

On dit qu'une fraction $\frac{a}{b}$ de deux entiers est **irréductible** lorsque a et b sont premiers entre eux.

Exercice d'application 14.27. Simplifier, si possible les fractions suivantes : $A = \frac{45}{14}$, $B = \frac{220}{165}$.

➥

14.4 Plus petit commun multiple

Définition 14.28 - Plus petit commun multiple.

Soit $a, b \in \mathbf{Z}^\star$. Soit M l'ensemble des multiples strictement positifs qui sont communs à a et b. On appelle **plus petit commun multiple** de a et b, et on note $\text{PPCM}(a, b)$ le plus petit élément de M.

Démonstration.
L'ensemble M est un ensemble non vide car il contient $|ab|$ et minoré par 0 (ou par $|a|$, ou par $|b|$), donc il contient bien un plus petit élément. □

Remarque 14.29. $\max(|a|, |b|) \leqslant \text{PPCM}(a, b) \leqslant |ab|$

Exemple 14.30. Les multiples strictement positifs de 6 sont 6, 12, 18, 24, 30… et ceux de 8 sont 8, 16, 24, 32… donc $\text{PPCM}(6, 8) = 24$.

14.5 Nombres premiers

Définition 14.31 - Nombre premier.

On appelle **nombre premier** tout entier naturel non nul admettant exactement 2 diviseurs entiers naturels distincts : 1 et lui-même.

Exemple 14.32. Les premiers nombres premiers sont 2, 3, 5, 7, 11...

ATTENTION

Les nombres 0 et 1 ne sont pas premiers !

Remarque 14.33. Deux nombres premiers distincts sont premiers entre eux.

Lemme 14.34 - Existence d'un diviseur premier.

Tout nombre entier supérieur ou égal à 2 est divisible par un nombre premier.

Démonstration.

Théorème 14.35 - Théorème d'Euclide.

Il existe une infinité de nombres premiers.

Démonstration.

Pour déterminer les nombres premiers inférieurs à un entier n fixé, on peut réaliser un **crible d'Ératosthène**. Le principe est le suivant :

- on écrit tous les nombres de 2 à n ;
- on conserve le nombre premier 2 et on raye tous les multiples de 2 (qui ne sont donc pas premiers) ;

- pour chaque nombre suivant p non rayé, on conserve p et on raye les multiples de p ;
- lorsque l'algorithme s'arrête (on est arrivé à n), tous les nombres non rayés sont les nombres premiers inférieurs à n.

Voici une implémentation en Python :

SCRIPT PYTHON

```
def eratosthene(N: int) -> list:
    # tableau de booléen qui indique si le nombre est premier ou non
    premier = (N+1) * [True]
    premier[0] = False # 0 n'est pas premier
    premier[1] = False # 1 n'est pas premier
    k = 2
    while k**2 <= N:
        for m in range(2*k, N+1, k):
            premier[m] = False # les multiples de k ne sont pas premiers
        k = k+1
    # on ne renvoie que les premiers
    return [k for k in range(N+1) if premier[k]]
```

Exemple 14.36. On a appliqué ci-après l'algorithme d'Ératosthène pour déterminer les nombres premiers inférieurs à 100. On a coloré, dans cet ordre, tous les multiples de 2, 3, 5, 7 strictement supérieurs à ces valeurs.

	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

Théorème 14.37 - Décomposition d'un nombre en produit de nombres premiers.

Tout entier naturel n supérieur ou égal à 2 admet une décomposition en facteurs premiers de la forme $n = q_1 q_2 \dots q_k$ où $q_1, \dots, q_k$ sont des nombres premiers. Cette décomposition est unique à l'ordre près des facteurs.
On peut également écrire cette décomposition sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où $p_1, \dots, p_r$ sont des nombres premiers distincts deux à deux et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls.

Démonstration.
Admis. □

Exemple 14.38. Déterminons la décomposition en facteurs premiers de $n = 277\,200$.

On a $n = 100 \times 2\,772 = 2^2 \cdot 5^2 \cdot 396$. De plus, 2 772 est pair, d'où $n = 2^3 \cdot 5^2 \cdot 1\,386$, puis comme 1 386 est pair, $n = 2^4 \cdot 5^2 \cdot 693$. Or 693 est divisible par 11, d'où $n = 2^4 \cdot 5^2 \cdot 11 \cdot 63$. Finalement,

$$n = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11.$$

Exercice d'application 14.39. Décomposer en produit de nombres premiers les entiers 360 et 9 295.

➥

Proposition 14.40 - PGCD, PPCM à partir de la décomposition en facteurs premiers.

Soit $(a,b) \in (\mathbf{N}\backslash\{0,1\})^2$, dont on écrit $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$ les décompositions en facteurs premiers (quitte à choisir $\alpha_i = 0$ ou $\beta_i = 0$ pour que les mêmes nombres premiers apparaissent dans les deux décompositions). On a :

$$\text{PGCD}(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \qquad \text{et} \qquad \text{PPCM}(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}.$$

Démonstration.
Admis. □

Exercice d'application 14.41. Déterminer PGCD(360, 336) et PPCM(360, 336).

➥

Soit m, n, a, b quatre nombres entiers naturels non nuls. On veut mettre au même dénominateur les deux fractions $\frac{m}{a}$ et $\frac{n}{b}$. Le dénominateur commun « optimal » n'est pas nécessairement ab : c'est PPCM(a,b).

« Optimal » signifie ici que lorsqu'on additionne ou qu'on soustrait les deux fractions, la fraction obtenue avec pour dénominateur ab est simplifiable et que cette simplification peut être évitée en prenant pour dénominateur commun PPCM(a,b) (cela n'empêche pas que la fraction obtenue peut ne pas être irréductible).

Exercice d'application 14.42. Calculer $A = \frac{11}{360} - \frac{5}{336}$.

➥

Corollaire 14.43 - Lien entre PGCD et PPCM.

Pour tout $(a,b) \in \mathbf{N}^2$, PGCD$(a,b) \times$ PPCM$(a,b) = a \times b$.

Démonstration.
On utilise les mêmes notations que dans la proposition précédente.

$$\begin{aligned}\text{PGCD}(a,b)\times\text{PPCM}(a,b) &= p_1^{\min(\alpha_1,\beta_1)}\dots p_r^{\min(\alpha_r,\beta_r)}\times p_1^{\max(\alpha_1,\beta_1)}\dots p_r^{\max(\alpha_r,\beta_r)}\\ &= p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)}\dots p_r^{\min(\alpha_r,\beta_r)+\max(\alpha_r,\beta_r)}\\ &= p_1^{\alpha_1+\beta_1}\dots p_r^{\alpha_r+\beta_r}\\ &= p_1^{\alpha_1}\dots p_r^{\alpha_r}\times p_1^{\beta_1}\dots p_r^{\beta_r}\\ &= a\times b\end{aligned}$$

□

Corollaire 14.44 - PPCM de nombres premiers entre eux.

Soit a et b deux nombres entiers naturels non nuls. Si a et b sont premiers entre eux, alors $\text{PPCM}(a,b)=ab$.

Démonstration.
Immédiat avec le corollaire précédent, puisque a et b premiers entre eux signifie que $\text{PGCD}(a,b)=1$. □

Corollaire 14.45.

Soit a et b deux nombres entiers naturels non nuls premiers entre eux et n un entier naturel.
Si $a \mid n$ et $b \mid n$, alors $ab \mid n$.

Démonstration.
Immédiat avec $\text{PPCM}(a,b)=ab$. □

Questions de cours

1. Définir la notion de diviseur, de multiple.
2. Énoncer le théorème de division euclidienne dans $\mathbf{Z}$.
3. Définir la notion de plus grand commun diviseur de deux entiers a et b dont un au moins est non nul.
4. Soit $(a,b)\in\mathbf{Z}\times\mathbf{N}^\star$. On note r le reste de la division euclidienne de a par b. Compléter l'égalité suivante, utile dans l'algorithme d'Euclide :
$$\text{PGCD}(a,b)=\dots$$
5. Définir la notion de plus petit commun multiple de deux entiers a et b non nuls.
6. Définir la notion de nombre premier.
7. Énoncer le théorème de décomposition d'un entier naturel supérieur ou égal à 2 en produit de nombres premiers.
8. Énoncer le théorème permettant d'obtenir le PGCD et le PPCM de deux entiers naturels non nuls à partir de leur décomposition en produit de nombres premiers.
9. Donner le lien entre PGCD et PPCM de deux entiers naturels.