22. Arithmétique des entiers

1 Divisibilité dans $\mathbb{N}$

1.1 Définitions et premières propriétés

Définition 1.1 Soit $(a,b) \in \mathbb{N}^2$. On dit que a **divise** b si

$$\exists k \in \mathbb{N}, \qquad b = ka$$

On note $a \mid b$. On dit aussi que a est un **diviseur** de b, ou que b est **divisible** par a, ou que b est un **multiple** de a.

Exemple 1.2 Compléter les phrases suivantes.

a) 2 divise ____ mais 2 ne divise pas ____

b) Les diviseurs de 12 sont _____

c) Tout entier a divise 0 car _____

d) Soit $a \in \mathbb{N}$. Alors _____ divisent a.

Soit $a \in \mathbb{N}$. L'ensemble des multiples de a dans $\mathbb{N}$ est l'ensemble $\{0, a, 2a, 3a, 4a, \ldots\} = \{ak \mid k \in \mathbb{N}\}$ noté $a\mathbb{N}$.

Proposition 1.3 Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^*$. Si a divise b alors $0 \leq a \leq b$.

Démonstration. Supposons que a divise b. Alors il existe $k \in \mathbb{N}$ tel que $b = ka$. Comme b est non nul, k l'est également et $k \geq 1$. Donc $b = ka \geq a$. ■

Proposition 1.4 Soient a, b, c et d des éléments de $\mathbb{N}$. Alors

a) Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

b) Si $a \mid b$ et $b \mid a$ alors $a = b$.

c) Si $a \mid b$ et $c \mid d$ alors $ac \mid bd$.

d) Si $a \mid b$ alors pour tout $n \in \mathbb{N}$, $a^n \mid b^n$.

e) Si $a \mid b$ alors $a \mid bc$.

f) Si $ab \mid c$ alors $a \mid c$ et $b \mid c$.

La réciproque de la dernière proposition est fausse : en général, $a \mid c$ et $b \mid c$ n'implique pas $ab \mid c$. Par exemple,

$$4 \mid 12 \text{ et } 6 \mid 12 \text{ mais } 4 \times 6 = 24 \text{ ne divise pas } 12.$$

Exemple 1.5 Déterminer les entiers $n \in \mathbb{N}$ tels que $n-3$ divise $2n+3$.

1.2 Division euclidienne

Proposition 1.6 — Division euclidienne. Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{N} \times \mathbb{N}$ tel que

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

L'entier q est appelé le **quotient** et l'entier r est appelé le **reste** de la division euclidienne de a par b.

Le quotient vérifie $q = \left\lfloor \frac{a}{b} \right\rfloor$. En Python, `a//b` renvoie le quotient et `a%b` renvoie le reste de la division euclidienne de a par b.

Exemple 1.7 Effectuer les divisions euclidiennes suivantes.

Entiers a et b	Division euclidienne de a par b	Quotient	Reste
$a = 22$ et $b = 6$			
$a = 221$ et $b = 11$			
$a = 15$ et $b = 2$			

Proposition 1.8 Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$. Alors

$$b \mid a \iff \text{le reste dans la division euclidienne de } a \text{ par } b \text{ vaut } 0$$

? Cette propriété est particulièrement utile en informatique. Par exemple pour tester si un entier n est pair ou impair, on regarde le reste de la division euclidienne de n par 2 vaut 0 ou pas grâce à la commande `n%2==0`.

2 PGCD, PPCM

2.1 Plus grand diviseur commun

Définition 2.1 — PGCD. Soient a et b deux entiers naturels non tous deux nuls. On appelle PGCD (plus grand commun diviseur) de a et b le plus grand entier naturel qui divise a et b. On le note $\text{PGCD}(a,b)$.

Le PGCD est l'outil qui permet de simplifier des fractions.

Exemple 2.2 Calculer les PGCD suivants.

a) $\text{PGCD}(12,18) =$

b) $\text{PGCD}(2,4) =$

c) $\text{PGCD}(12,15) =$

d) $\forall a \in \mathbb{N}^*,\ \text{PGCD}(a,0) =$

e) $\text{PGD}(a,1) =$

f) $\text{PGCD}(a,b)$___$\text{PGCD}(b,a)$

2.2 Calcul du PGCD avec l'algorithme d'Euclide

Le PGCD peut se calculer de manière algorithmique. Il est basé sur le résultat suivant.

Proposition 2.3 Soient a et b deux éléments de $\mathbb{N}$. Notons r le reste de la division euclidienne de a par b. Alors,

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

L'**algorithme d'Euclide** permet de calculer le PGCD de deux entiers. Il est basé sur des divisions euclidiennes successives. D'après le lemme ci-dessus, le PGCD est le dernier reste non nul obtenu.

PRINCIPE DE L'ALGORITHME D'EUCLIDE. On pose $r_0 = a$ et $r_1 = b$. On calcule de proche en proche les divisions euclidiennes de r_n par r_{n+1} jusqu'à tomber sur un reste nul :

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \\
r_1 &= r_2 q_2 + r_3 \\
&\vdots \\
r_{n_0-2} &= r_{n_0-1} q_{n_0-1} + \boxed{r_{n_0}} \\
r_{n_0-1} &= r_{n_0} q_{n_0} + 0
\end{aligned}$$

La suite $(r_n)_{n\in\mathbb{N}}$ des restes obtenus est une suite strictement décroissante d'entiers positifs. Il existe donc un élément $n_0 \in \mathbb{N}$ tel que $r_{n_0+1} = 0$. Alors, d'après le lemme, $\text{PGCD}(a,b) = \text{PGCD}(b,r_2) = \ldots = \text{PGCD}(r_{n_0},0) = r_{n_0}$.

Exemple 2.4 Calculons le PGCD de 216 et 126 à l'aide de l'algorithme d'Euclide.

2.3 Entiers premiers entre eux

Définition 2.5 Soient a et b deux éléments de $\mathbb{N}$. On dit que a et b sont **premiers entre eux** si $\text{PGCD}(a,b) = 1$.

Exemple 2.6 Dire si les entiers suivants sont premiers entre eux.

a) 2 et 3

b) 6 et 4

c) 9 et 16

d) 9 et 12

Pour déterminer si deux entiers sont premiers entre eux, on peut utiliser l'algorithme d'Euclide pour déterminer leur PGCD et vérifier qu'il vaut 1.

Exemple 2.7 Montrer que 63 et 20 sont premiers entre eux.

Proposition 2.8 Soient $(a,b) \in (\mathbb{N}^*)^2$ et $d = PGCD(a,b)$. Alors, il existe un unique couple $(a',b') \in (\mathbb{N}^*)^2$ tel que

$$\begin{cases} a = da' \\ b = db' \\ PCGD(a',b') = 1 \end{cases}$$

? C'est cette proposition que l'on utilise sans le savoir pour simplifier au maximum une fraction :

$$\frac{78}{48} = \frac{6\times 13}{6\times 8} = \frac{13}{8}$$

2.4 Plus petit multiple commun

Définition 2.9 — PPCM. Soient a et b des éléments non nuls de $\mathbb{N}$. On appelle PPCM (plus petit commun multiple) de a et b le plus petit entier naturel non nul divisible par a et par b. Par convention, si a ou b est nul alors $\text{PPCM}(a,b) = 0$.

Exemple 2.10 Déterminer les PPCM suivants.

a) $\text{PPCM}(3,6) =$

b) $\text{PPCM}(4,6) =$

c) $\text{PPCM}(a,0) =$

d) $\text{PPCM}(a,1) =$

On dispose de la relation suivante qui lie PGCD et PPCM.

Proposition 2.11 Soient a et b des éléments de $\mathbb{Z}$. Alors,

$$\text{PGCD}(a,b) \times \text{PPCM}(a,b) = a \times b$$

En particulier, si a et b sont premiers entre eux, $\text{PPCM}(a,b) = ab$.

Exemple 2.12 Donner le PPCM de 63 et 20.

3 Nombres premiers

3.1 L'ensemble des nombres premiers

Définition 3.1 Soit $p \in \mathbb{N}$. On dit que p est un nombre **premier** si p est différent de 1 et si ses seuls diviseurs positifs sont 1 et p.

Exemple 3.2 Donner tous les nombres premiers entre 1 et 20.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Proposition 3.3 Tout entier $n \geq 2$ a au moins un diviseur premier.

Proposition 3.4 Tout entier $n \geq 2$ qui n'est pas premier a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

À l'aide du résultat précédent, on peut déterminer si un entier $n \geq 2$ est premier ou non : on effectue successivement la division euclidienne de n par tous les entiers premiers d tels que $1 < d \leq \sqrt{n}$, et si l'une des divisions donne un reste nul alors n n'est pas premier, sinon n est premier.

Exemple 3.5 Démontrer que 97 est un nombre premier.

Théorème 3.6 Il existe une infinité de nombres premiers.

3.2 Décomposition en produit de facteurs premiers

Théorème 3.7 — Théorème fondamental de l'arithmétique. Tout entier naturel $n \geq 2$ se décompose, de manière unique à l'ordre près des termes, en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_N^{\alpha_N}$$

où les p_i sont des nombres premiers deux à deux distincts et les α_i sont des entiers naturels non nuls.

Pour décomposer un nombre entier $n \geq 2$, on peut procéder de la façon suivante :

❶ On cherche la plus grande puissance $\alpha_1 \geq 0$ de 2 divisant n, on obtient $n = 2^{\alpha_1} \times n_1$ où $n_1 \in \mathbb{N}$ et n_1 n'est plus divisible par 2. Si $n_1 = 1$, on a terminé, sinon on passe à l'étape suivante.

❷ On cherche la plus grande puissance $\alpha_2 \geq 0$ de 3 divisant n_1, on obtient alors $n = 2^{\alpha_1} \times 3^{\alpha_2} \times n_2$ où $n_2 \in \mathbb{N}$ et n_2 n'est plus divisible par 3 (ni 2 par la première étape). Si $n_2 = 1$, on a terminé, sinon on passe à l'étape suivante.

❸ On cherche la plus grande puissance $\alpha_3 \geq 0$ de 5 divisant n_2, etc.

Exemple 3.8 Déterminer la décomposition en facteurs premiers de 360, 147 et 1575.

À partir de la décomposition en facteurs premiers, on peut récupérer facilement la liste des diviseurs d'un nombre à l'aide du résultat suivant.

Proposition 3.9 Soit un entier $n \geq 2$. On suppose que la décomposition de n en facteurs premiers est la suivante :

$$n = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$$

où les p_i sont des nombres premiers distincts deux à deux et les α_i des entiers naturels non nuls. Les diviseurs positifs de n sont les entiers de la forme

$$p_1^{\beta_1} \times \ldots \times p_N^{\beta_N} \qquad \text{avec, pour tout } i \in \{1, \ldots, N\},\ 0 \leq \beta_i \leq \alpha_i$$

Exemple 3.10 Déterminer l'ensemble des diviseurs de 45.

On peut aussi déterminer facilement le PGCD/PPCM de deux nombres à partir de leurs décomposition en facteurs premiers.

Proposition 3.11 Soient a et b deux entiers supérieurs ou égaux à 2. On suppose que

$$\begin{cases} a = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N} \\ b = p_1^{\beta_1} \times \ldots \times p_N^{\beta_N} \end{cases}$$

où les p_i sont des nombres premiers distincts deux à deux et les α_i et β_i sont des entiers naturels. Alors,

$$\text{PGCD}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \times \ldots \times p_N^{\min(\alpha_N,\beta_N)} \quad \text{et} \quad \text{PPCM}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \times \ldots \times p_N^{\max(\alpha_N,\beta_N)}$$

Exemple 3.12 Déterminer le PGCD et le PPCM de 147 et 1575.