



Arithmétique

1 Divisibilité dans \mathbb{Z}

1.1 Multiples d'un entier relatif

Définition 1 Soit $n \in \mathbb{Z}$. $m \in \mathbb{Z}$ est un multiple de n s'il existe $k \in \mathbb{Z}$ tel que $m = kn$.

On note $n\mathbb{Z}$ l'ensemble des multiples de n .

Définition 2 Soit $n \in \mathbb{Z}$. $d \in \mathbb{Z}^*$ est un diviseur de n s'il existe $q \in \mathbb{Z}$ tel que $n = qd$.

On note alors $d \mid n$. On note $\text{Div}(n)$ l'ensemble des diviseurs de n .

$$\begin{aligned} m \text{ multiple de } n &\Leftrightarrow n \text{ diviseur de } m \\ m \in n\mathbb{Z} &\Leftrightarrow n \in \text{Div}(m) \end{aligned}$$

Remarque 1 $\text{Div}(0) = \mathbb{Z}$

Notation : On note $\text{Div}(a, b) = \text{Div}(a) \cap \text{Div}(b)$ l'ensemble des diviseurs communs à a et à b .

1.2 Propriétés de la divisibilité

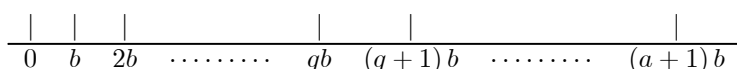
- $d \mid n \Leftrightarrow -d \mid n$
- $\begin{cases} d \mid n \\ n \neq 0 \end{cases} \Rightarrow |d| \leq |n|$. Donc tout entier non nul admet un nombre fini de diviseurs.
Si d et n sont des entiers naturels, $d \mid n \Rightarrow d \leq n$.
- $\begin{cases} d \mid n \\ n \mid d \end{cases} \Rightarrow n = d \text{ ou } n = -d$
- $\begin{cases} a \mid b \\ b \mid c \end{cases} \Rightarrow a \mid c$
- $a \in \text{Div}(b, c) \Rightarrow a \mid bx + cy$ pour tout $(x, y) \in \mathbb{Z}^2$. En particulier, $a \mid b + c$ et $a \mid b - c$
- $d \mid n \Rightarrow \forall c \in \mathbb{Z}^* : dc \mid nc$.

2 Division euclidienne dans \mathbb{N}

Théorème 1 Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. $\exists ! (q, r) \in \mathbb{N}^2$ tel que

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

Démonstration. $b > 0$ donc les multiples positifs de b forment une suite strictement croissante. Ecrivons les multiples de b de 0 jusqu'à $(a + 1)b$.



$(a + 1)b = ab + b > ab \geq a$ (car $b \geq 1$). Donc a est nécessairement, soit l'un des multiples écrits, soit compris entre deux multiples consécutifs, c'est à dire qu'il existe q unique tel que $a \in [qb; (q + 1)b[$.
Soit $r = a - bq$ (r est donc unique). $bq \leq a < b(q + 1) \Rightarrow 0 \leq r < b$
Donc $a = bq + r$ avec $0 \leq r < b$

3 PGCD de deux entiers naturels

3.1 Diviseurs communs à deux entiers naturels

Soient a et b deux entiers naturels non tous les deux nuls.

$\text{Div}(a, b) = \text{Div}(a) \cap \text{Div}(b)$ est une partie de \mathbb{Z} non vide (elle contient 1) et ses éléments sont tous inférieurs ou égaux à a et à b . Donc $\text{Div}(a, b)$ possède un plus grand élément.

Définition 3 Soient a et b deux entiers non tous nuls. Le plus grand élément de $\text{Div}(a, b)$ est le PGCD de a et b . On le note $a \wedge b$.

Théorème 2 $\forall c \in \mathbb{N} : \boxed{\text{Div}(c, 0) = \text{Div}(c)}$

Théorème 3 $\boxed{a \mid b \Rightarrow a \wedge b = a}$

Démonstration. $a \mid b \Rightarrow \text{Div}(a) \subset \text{Div}(b) \Rightarrow \text{Div}(a) \cap \text{Div}(b) = \text{Div}(a)$.
 $a \wedge b$ est donc le plus grand élément de $\text{Div}(a)$ c'est à dire a .

Théorème 4 $\boxed{a = bq + r \Rightarrow \text{Div}(a, b) = \text{Div}(b, r)}$

Démonstration.

$$\left. \begin{array}{l} d \in \text{Div}(a, b) \\ r = a - bq \end{array} \right\} \Rightarrow \left. \begin{array}{l} d \in \text{Div}(a, b) \\ d \mid r \end{array} \right\} \Rightarrow d \in \text{Div}(b, r) \text{ donc } \text{Div}(a, b) \subset \text{Div}(b, r)$$

$$\left. \begin{array}{l} d \in \text{Div}(b, r) \\ a = bq + r \end{array} \right\} \Rightarrow \left. \begin{array}{l} d \in \text{Div}(b, r) \\ d \mid a \end{array} \right\} \Rightarrow d \in \text{Div}(a, b) \text{ donc } \text{Div}(b, r) \subset \text{Div}(a, b)$$

3.2 Algorithme d'Euclide

Si $b \mid a : a \wedge b = b$ sinon : $\left. \begin{array}{l} a = bq + r \\ 0 \leq r < b \end{array} \right\} \Rightarrow \text{Div}(a, b) = \text{Div}(b, r)$

Si $r \mid b : b \wedge r = r$ sinon : $\left. \begin{array}{l} b = rq_1 + r_1 \\ 0 \leq r_1 < r \end{array} \right\} \Rightarrow \text{Div}(b, r) = \text{Div}(r, r_1)$

Si $r_1 \mid r : r \wedge r_1 = r_1$ sinon $\left. \begin{array}{l} r = r_1q_2 + r_2 \\ 0 \leq r_2 < r_1 \end{array} \right\} \Rightarrow \text{Div}(r, r_1) = \text{Div}(r_1, r_2)$.

La suite (r_n) étant strictement décroissante et positive, on obtient donc de proche en proche :

$$\text{Div}(a, b) = \text{Div}(b, r) = \text{Div}(r, r_1) = \text{Div}(r_1, r_2) = \dots = \text{Div}(r_{n-1}, r_n) = \text{Div}(r_n, 0)$$

$r, r_1, r_2, \dots, r_{n-1}, r_n$ sont les restes obtenus dans les divisions successives.

Or $\text{Div}(r_n, 0) = \text{Div}(r_n)$ et puisque r_n est le plus grand élément de $\text{Div}(r_n) : r_n$ est le plus grand élément de $\text{Div}(a, b)$ donc $r_n = a \wedge b$.

3.3 Conséquences de l'algorithme d'Euclide

Théorème 5 Lorsque b ne divise pas $a : \boxed{a \wedge b \text{ est le dernier reste non nul obtenu par l'algorithme}}$

Théorème 6 $\boxed{\text{Div}(a, b) = \text{Div}(a \wedge b)}$

Démonstration. $\text{Div}(a, b) = \text{Div}(r_n, 0) = \text{Div}(r_n) = \text{Div}(a \wedge b)$.

4 Nombres premiers entre eux

Définition 4 Deux entiers naturels a et b sont dits premiers entre eux lorsque $a \wedge b = 1$

Théorème 7 (Bezout) $\boxed{a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 : au + bv = 1}$

Démonstration.



1. Si $\exists (u, v) \in \mathbb{Z}^2 : au + bv = 1$. Alors : $\left. \begin{matrix} a \wedge b \mid a \\ a \wedge b \mid b \end{matrix} \right\} \Rightarrow a \wedge b \mid au + bv \Rightarrow a \wedge b \mid 1 \Rightarrow a \wedge b = 1$
2. Si $a \wedge b = 1$, notons d le plus petit élément strictement positif de $a\mathbb{Z} + b\mathbb{Z}$. ($a\mathbb{Z} + b\mathbb{Z}$ contient des entiers strictement positifs car $a \in a\mathbb{Z} + b\mathbb{Z}$ et $b \in a\mathbb{Z} + b\mathbb{Z}$).
Puisque $d \in a\mathbb{Z} + b\mathbb{Z}$, $d = au + bv$.
Montrons que $d \mid a$ et $d \mid b$. Il en résultera $d = 1$ et donc $1 \in a\mathbb{Z} + b\mathbb{Z}$.
La division euclidienne de a par d donne : $a = dq + r$ avec $0 \leq r < d$
 $r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq) \in a\mathbb{Z} + b\mathbb{Z}$
 d étant le plus petit élément strictement positif de $a\mathbb{Z} + b\mathbb{Z}$ on ne peut avoir $0 < r < d$.
On a donc obligatoirement $r = 0$. Donc $a = dq$ et $d \mid a$. De même : $d \mid b$.

5 Caractérisations et propriétés du PGCD

Théorème 8
$$d = a \wedge b \Leftrightarrow \begin{cases} a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases}$$

Démonstration.

1. Supposons que $d = a \wedge b$.
 $d \in \text{Div}(a, b) \Rightarrow a = da'$ et $b = db'$.
 $d' \in \text{Div}(a', b') \Rightarrow \left. \begin{matrix} a' = d'a'' \\ b' = d'b'' \end{matrix} \right\} \Rightarrow \left. \begin{matrix} a = dd'a'' \\ b = dd'b'' \end{matrix} \right\} \Rightarrow dd' \in \text{Div}(a, b)$
 d étant le plus grand élément de $\text{Div}(a, b)$, $dd' \leq d$. Donc $d' = 1$ d'où $a' \wedge b' = 1$.
2. Supposons $a = da'$, $b = db'$ et $a' \wedge b' = 1$. On a évidemment $d \in \text{Div}(a, b)$.
Bézout $\Rightarrow a'u + b'v = 1 \Rightarrow au + bv = da'u + db'v = d(a'u + b'v) = d$
Soit $\delta \in \text{Div}(a, b)$. Alors $\delta \mid au + bv = d$ et donc $\delta \leq d$.
 d est donc le plus grand élément de $\text{Div}(a, b)$. Donc $d = a \wedge b$.

Corollaire 1
$$d = a \wedge b \Leftrightarrow \begin{cases} d \in \text{Div}(a, b) \\ d \in a\mathbb{Z} + b\mathbb{Z} \end{cases}$$

Démonstration.

$$d = a \wedge b \Leftrightarrow \begin{cases} a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases} \Leftrightarrow \begin{cases} a = da' \\ b = db' \\ a'u + b'v = 1 \end{cases} \Leftrightarrow \begin{cases} a = da' \\ b = db' \\ au + bv = d \end{cases} \Leftrightarrow \begin{cases} d \in \text{Div}(a, b) \\ d \in a\mathbb{Z} + b\mathbb{Z} \end{cases}$$

Théorème 9 $\forall c \in \mathbb{N}^* : (ca) \wedge (cb) = c(a \wedge b)$

Démonstration. $d = a \wedge b \Rightarrow \begin{cases} d \in \text{Div}(a, b) \\ d \in a\mathbb{Z} + b\mathbb{Z} \end{cases} \Rightarrow \begin{cases} dc \in \text{Div}(ac, bc) \\ dc \in ac\mathbb{Z} + bc\mathbb{Z} \end{cases} \Rightarrow dc = (ac) \wedge (bc)$.

6 Théorème de Gauss

Théorème 10 (Gauss) Si $(a, b, c) \in \mathbb{N}^{*3} : \begin{matrix} a \mid bc \\ a \wedge b = 1 \end{matrix} \Rightarrow a \mid c$

Démonstration. $au + bv = 1 \Rightarrow auc + bvc = c$.

$a \mid auc$ de manière évidente et $a \mid bvc$ par hypothèse. Donc $a \mid auc + bvc = c$

Corollaire 2 Si $n \in \mathbb{N}$ est divisible par a et b premiers entre eux, alors il est divisible par ab .

Démonstration. $n = ap$ et $n = bq$. Donc $ap = bq$.

$b \mid ap$ et $a \wedge b = 1$ donc $b \mid p$ (Gauss)

Donc $p = bp'$ et $n = ap = abp'$. Donc $ab \mid n$.

Définition 5 La fraction $\frac{a}{b}$ est dite irréductible lorsque $a \wedge b = 1$.

7 PPCM de deux entiers naturels

7.1 Multiples communs de deux entiers naturels

Soient a et b deux entiers naturels non nuls. L'ensemble des multiples strictement positifs communs à a et b est une partie non vide de \mathbb{N} car elle contient $ab \in \mathbb{N}^*$. Donc cet ensemble possède un plus petit élément.

Définition 6 Soient a et b deux entiers naturels non nuls. Le plus petit élément de l'ensemble des multiples strictement positifs communs à a et b est le PPCM de a et b et se note $a \vee b$ ou $\text{PPCM}(a; b)$

7.2 Propriétés du PPCM

Théorème 11 Si $(a, b) \in \mathbb{N}^{*2}$:

$$\left. \begin{array}{l} d = a \wedge b \\ a = da' \\ b = db' \end{array} \right\} \Rightarrow a \vee b = da'b'$$

Démonstration.

- $m = da'b'$ est multiple commun à a et b car $a = da'$ et $b = db'$.
- Si μ est un multiple commun à a et b : $\mu = ap = bq$. Montrons que $\mu \geq m$
 $ap = bq \Rightarrow da'p = db'q \Rightarrow a'p = b'q \Rightarrow a' \mid b'q \Rightarrow a' \mid q$ (Gauss).
 $q = ka' \Rightarrow \mu = bq = bka' = db'ka' = km \geq m$ car $k \in \mathbb{N}^*$.
 m est donc le plus petit commun multiple de a et b .

Corollaire 3 Tout multiple commun à a et b est multiple de $m = a \vee b$

Démonstration. Soit μ un multiple de a et b ... voir alors la démonstration précédente.

Corollaire 4 $(a \wedge b)(a \vee b) = ab$

Démonstration. $ab = da'db' = d(da'b') = d(a \vee b) = (a \wedge b)(a \vee b)$.

Corollaire 5 $a \wedge b = 1 \Leftrightarrow a \vee b = ab$

Proposition 1 $\forall c \in \mathbb{N}^* : (ca) \vee (cb) = c(a \vee b)$

Démonstration. $(ca \wedge cb)(ca \vee cb) = c(a \wedge b)(ca \vee cb)$ d'après le théorème 9

$(ca \wedge cb)(ca \vee cb) = c^2ab$ d'après le corollaire 4

D'où $c(a \wedge b)(ca \vee cb) = c^2ab$.

De plus $(a \wedge b)(a \vee b) = ab$. d'après le corollaire 4

D'où $c(a \wedge b)(ca \vee cb) = c^2(a \wedge b)(a \vee b)$ puis le résultat après simplification.

Proposition 2 $m = a \vee b \Leftrightarrow \begin{cases} m = \alpha a \\ m = \beta b \\ \alpha \wedge \beta = 1 \end{cases}$

Démonstration.

- Si $m = a \vee b$ il existe α et β entiers tels que $m = \alpha a = \beta b$
 En posant $d = a \wedge b$, on a $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$.
 $md = ab \Rightarrow \alpha ad = adb' \Rightarrow \alpha = b'$
 $md = ab \Rightarrow \beta bd = da'b \Rightarrow \beta = a'$
 Donc $\alpha \wedge \beta = b' \wedge a' = 1$
- Supposons $m = \alpha a = \beta b$ avec $\alpha \wedge \beta = 1$
 m est un multiple de $a \vee b$ d'après le corollaire 3
 Donc $m = k(a \vee b) = kda'b'$ en posant $d = a \wedge b$ et $a = da'$ et $b = db'$
 $\left. \begin{array}{l} \alpha a = kda'b' = kab' \Rightarrow \alpha = kb' \\ \beta b = kda'b' = ka'b \Rightarrow \beta = ka' \end{array} \right\} \Rightarrow \alpha \wedge \beta = (kb') \wedge (ka') = k(a' \wedge b') = k$
 Comme $\alpha \wedge \beta = 1$ on en déduit $m = a \vee b$.

8 Nombres premiers

Définition 7 Un nombre premier est un nombre entier strictement supérieur à 1 et qui admet exactement deux diviseurs : 1 et lui même.

Remarque 2 Un entier non premier admet au moins un diviseur autre que 1 et que lui même. Un tel diviseur est appelé diviseur strict.

Théorème 12 Tout entier n tel que $n \geq 2$ admet un diviseur premier.

Démonstration. Si n est premier, le diviseur est alors n .

Si n n'est pas premier, n admet au moins un diviseur strict.

L'ensemble des diviseurs stricts de n est donc non vide et minoré par 1.

Soit p le plus petit diviseur strict de n .

Si p n'est pas premier, alors p admet un diviseur strict d . On a donc $d < p < n$

Mais alors $d | p$ et $p | n$ donc $d | n$. Contradiction avec le fait que p soit le plus petit des diviseurs stricts de n . Donc p est premier.

Théorème 13 Tout entier n supérieur ou égal à 2 est premier ou produit de nombres premiers.

Démonstration. Si n n'est pas premier, il admet un diviseur premier p_1 d'après le théorème précédent..

On a alors $n = p_1 q$, et $q < n$ car $p_1 > 1$.

Si q est premier alors n est produit de nombres premiers.

Si q n'est pas premier, $q = q_1 q_2$ avec q_1 premier et $1 < q_2 < q$. D'où $n = p_1 q_1 q_2$.

Si q_2 est premier alors n est produit de nombres premiers.

Si q_2 n'est pas premier, on recommence.

Les quotients successifs forment une suite strictement décroissante de nombres entiers strictement positifs.

Le procédé va donc se terminer après un nombre fini de divisions pour amener au résultat.

Théorème 14 Tout nombre entier se décompose de façon **unique**, comme produit de nombres premiers

Théorème 15 L'ensemble des nombres premiers est infini.

Démonstration. Supposons que l'ensemble des nombres premiers est fini.

Soit alors p le plus grand nombre premier.

Posons $N = (2 \times 3 \times 5 \times 7 \times \dots \times p) + 1$ où $2 \times 3 \times 5 \times 7 \times \dots \times p$ est le produit \prod de tous les nombres premiers.

N admet un diviseur premier q car $N \geq 2$.

Aucun des nombres premiers formant le produit \prod n'est un diviseur de N car le reste de la division de N par n'importe lequel de ces nombres est 1 d'après la définition de N . Donc $q > p$. Contradiction.

Théorème 16 Si p est premier et si n est un entier naturel non divisible par p : $p \wedge n = 1$

Démonstration. Soit d un diviseur commun à p et n .

$d | p \Rightarrow d = 1$ ou $d = p$. On ne peut avoir $d = p$ car alors $p | n$. Donc $d = 1$.

Théorème 17 Si a et b sont deux entiers naturels et si p est premier : $p | ab \Rightarrow p | a$ ou $p | b$

Démonstration. Si $p | a$ le résultat est évident.

Si p ne divise pas a alors $p \wedge a = 1$ (théorème vu précédemment).

Mais alors $p | b$ (théorème de Gauss)

Corollaire 6 Si a, b et p sont premiers : $p | ab \Rightarrow p = a$ ou $p = b$.

Démonstration. $p | a$ ou $p | b$ d'après le théorème précédent.

Or a et b sont premiers et $p \neq 1$. Donc $p = a$ ou $p = b$

Théorème 18 Soit n un entier non premier de décomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$.

Les diviseurs de n sont les nombres $p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ avec $0 \leq \beta_k \leq \alpha_k$.

Démonstration. Si $d \mid n$ et $d > 1$, on a $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \dots p_s^{\beta_s}$ où les p_k sont premiers distincts et les β_k entiers éventuellement nuls.

$n = dk$ et $k = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} p_{r+1}^{\gamma_{r+1}} \dots p_s^{\gamma_s} p_{s+1}^{\gamma_{s+1}} \dots p_{t+1}^{\gamma_{t+1}}$ où les $\gamma_k \geq 0$.

D'où $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \dots p_s^{\beta_s} p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} p_{r+1}^{\gamma_{r+1}} \dots p_s^{\gamma_s} p_{s+1}^{\gamma_{s+1}} \dots p_{t+1}^{\gamma_{t+1}}$
 $= p_1^{\beta_1 + \gamma_1} p_2^{\beta_2 + \gamma_2} \dots p_r^{\beta_r + \gamma_r} p_{r+1}^{\beta_{r+1} + \gamma_{r+1}} \dots p_s^{\beta_s + \gamma_s} p_{s+1}^{\gamma_{s+1}} \dots p_{t+1}^{\gamma_{t+1}}$

L'unicité de la décomposition en facteurs premiers implique

$\beta_{r+1} + \gamma_{r+1} = \dots = \beta_s + \gamma_s = \gamma_{s+1} = \dots = \gamma_{t+1} = 0$.

Donc $\beta_{r+1} = \dots = \beta_s = 0$ car les exposants sont tous positifs ou nuls. Donc $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$.

De plus $\beta_k + \gamma_k = \alpha_k$ toujours à cause de l'unicité de la décomposition en facteurs premiers.

Donc $0 \leq \beta_k \leq \alpha_k$

Corollaire 7 Soient a et b deux entiers naturels non nuls.

1. $a \wedge b$ est le produit des facteurs premiers communs à a et à b , chacun étant affecté de son plus petit exposant.
2. $a \vee b$ est le produit des facteurs premiers figurant dans les décompositions de a ou de b , chacun d'eux étant affecté de son plus grand exposant.