

1. ARITHMÉTIQUE

DES ENTIERS

I. Division

A. Généralités

1. Définition

Si $(a, b) \in \mathbb{Z}^2$ on dit que b **divise** a ou que a est **multiple** de b , et on écrit $b|a$, s'il existe un élément q de \mathbb{Z} tel que $a = bq$.

Remarques

- 0 ne divise que lui-même et est multiple de tout entier.
- 1 divise tout entier et n'est multiple que de lui-même et de -1 .
- $b|a \iff (-b)|a \iff b|(-a) \iff (-b)|(-a) \iff |b|$ divise $|a|$.
- La relation de divisibilité est transitive mais $(a|b$ et $b|a) \iff a \in \{-b, b\}$.
Sa restriction à \mathbb{N} est donc une relation d'ordre.

2. Théorème de division euclidienne

Si $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ alors il existe un unique élément de $\mathbb{Z} \times \llbracket 0, b \llbracket$ tel que $a = bq + r$. Cette égalité $a = bq + r$ est appelée **égalité de division euclidienne** de a par b , q est le **quotient** et r le **reste**.

Démonstration

Définissons l'ensemble $\{q \in \mathbb{Z} \mid bq \leq a\}$ que l'on note Q .

Comme $bq \rightarrow -\infty$ (resp. $+\infty$) lorsque $q \rightarrow -\infty$ (resp. $+\infty$) l'ensemble Q est d'une part non vide et d'autre part majoré, donc admet un maximum que l'on note q . C'est bien sûr $\left\lfloor \frac{a}{b} \right\rfloor$.

Posons également $r = a - bq$, alors, par définition $r \in \mathbb{N}$ et, comme $q + 1 \notin Q$ on a $a < b(q + 1)$ i.e. $r < b$. Cela prouve que le couple (q, r) est solution.

Si (q', r') est une autre solution alors, par différence, $b(q - q') = r' - r$ d'où $b|q - q'| = |r' - r| < b$ puis $|q - q'| < 1$ i.e. $q = q'$ et, donc, $r = r'$.

On a établi l'existence et l'unicité d'une solution (q, r) . \square

Remarques

- $b|a$ si, et seulement si, le reste de la division euclidienne de a par b est nul.
- on peut étendre le théorème précédent au cas où $b \in \mathbb{Z}^*$ en imposant $0 \leq r < |b|$ quitte à remplacer q par $-q$.

B. Sous groupes additifs et idéaux de \mathbb{Z}

1. Définition

| Si $a \in \mathbb{Z}$ on note $a\mathbb{Z}$ l'ensemble $\{aq | q \in \mathbb{Z}\}$ des multiples de a .

Remarques

- $0\mathbb{Z} = \{0\}$, $2\mathbb{Z}$ est l'ensemble des entiers pairs et, si $a \in \mathbb{Z}$, alors $a\mathbb{Z} = |a|\mathbb{Z}$.
- Si $(a, b) \in \mathbb{Z}^2$ alors $b|a \iff a \in b\mathbb{Z} \iff a\mathbb{Z} \subset b\mathbb{Z}$,
et donc $a\mathbb{Z} = b\mathbb{Z} \iff |a| = |b|$.
- Si $a \in \mathbb{Z}$ alors $a\mathbb{Z}$ est le plus petit sous-groupe additif et aussi le plus petit idéal de \mathbb{Z} contenant a ie. $a\mathbb{Z}$ est le sous-groupe additif et l'idéal de \mathbb{Z} engendré par a .

2. Théorème

| H est un sous-groupe additif de \mathbb{Z} si, et seulement s'il existe un élément a de \mathbb{N} tel que $H = a\mathbb{Z}$.

Démonstration

Si $H = \{0\}$ alors $H = 0\mathbb{Z}$.

Sinon, comme H est stable par $x \mapsto -x$, on remarque que $H \cap \mathbb{N}^*$ est non vide et, donc, admet un plus petit élément ; on le note a et, ainsi, $a \in \mathbb{N}^*$.

Immédiatement $a\mathbb{Z} \subset H$.

Si $h \in H$ et si l'égalité de la division euclidienne de h par a est $h = aq + r$ alors $r = h - aq \in H \cap \mathbb{N}$ et $r < \min(H \cap \mathbb{N}^*)$ donc $r = 0$. Ainsi $h \in a\mathbb{Z}$ et, en définitive, $H = a\mathbb{Z}$. \square

Remarque

L'entier a précédent est unique car $a\mathbb{Z} = b\mathbb{Z} \iff (a|b \text{ et } b|a) \iff a = b$; on dit que a est le générateur (positif) du sous-groupe.

3. Corollaire

| \mathbb{Z} est un anneau principal

Démonstration

Un idéal de \mathbb{Z} est *a fortiori* un sous-groupe additif de \mathbb{Z} et, si $a \in \mathbb{Z}$, alors $a\mathbb{Z}$ est un idéal de \mathbb{Z} . Les sous-groupes de \mathbb{Z} se confondent avec ses idéaux. \square

II. PGCD et PPCM

(a, b) désigne systématiquement un élément de \mathbb{Z}^2 .

A. Généralités

Remarques

- $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe additif de $a\mathbb{Z}$ et de $b\mathbb{Z}$, par suite il existe un unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. C'est l'ensemble des multiples communs à a et b . Autrement dit un multiple commun à a et b est un multiple de m . Cela montre que m est le plus petit (au sens de la divisibilité) de ces multiples communs.

- De même $a\mathbb{Z} + b\mathbb{Z}$ est le plus petit sous-groupe additif de \mathbb{Z} contenant $a\mathbb{Z} \cup b\mathbb{Z}$, il existe un unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Bien sûr d est un diviseur commun à a et b car a et b sont éléments de $a\mathbb{Z} + b\mathbb{Z}$.

Si d' est un diviseur commun à a et b alors d' divise tout élément de $a\mathbb{Z} + b\mathbb{Z}$, et donc d . Cela montre que d est le plus grand (au sens de la divisibilité) diviseur commun à a et b .

1. Définitions

Avec les notations précédentes d est appelé **plus grand commun diviseur** de a et b et noté $\text{pgcd}(a, b)$.

L'entier m est appelé **plus petit commun multiple** de a et b et noté $\text{ppcm}(a, b)$.

2. Généralisation

Si $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n$ le générateur positif du sous-groupe de \mathbb{Z} , $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z}$ est appelé **plus grand commun multiple** de a_1, a_2, \dots, a_n et noté $\text{pgcd}(a_1, \dots, a_n)$.

De même le générateur positif de $\bigcap_{i=1}^n a_i\mathbb{Z}$ est appelé **plus petit commun multiple** de a_1, a_2, \dots, a_n et noté $\text{ppcm}(a_1, \dots, a_n)$.

Remarque

Vu les propriétés de la somme de sous-groupes de \mathbb{Z} le pgcd est, en quelque sorte, associatif et commutatif.

Plus précisément $\text{pgcd}(a_1, \text{pgcd}(a_2, a_3)) = \text{pgcd}(a_1, a_2, a_3)$ et, si $\sigma \in \mathfrak{S}_n$, alors $\text{pgcd}(a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)}) = \text{pgcd}(a_1, \dots, a_n)$.

Il en va de même pour le ppcm .

B. Algorithme d'Euclide

1. Lemme

Si $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ et si $a = bq + r$ est l'égalité de division euclidienne de a par b alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Démonstration

$a\mathbb{Z} + b\mathbb{Z} = (a - bq)\mathbb{Z} + b\mathbb{Z}$ tout simplement. \square

2. Algorithme

Remarques

- $\text{pgcd}(a, 0) = 0$.
- $\text{pgcd}(a, b) = \text{pgcd}(b, a) = \text{pgcd}(|a|, |b|)$, cela permet de se limiter au cas où $0 < b \leq a$, ce que l'on suppose pour décrire l'algorithme :

Tant que le reste, noté r , de la division euclidienne de a par b est non nul remplacer (a, b) par (b, r) .

Comme la suite des restes est strictement décroissante et à valeurs dans \mathbb{N} elle est finie et $\text{pgcd}(a, b)$ est, d'après le lemme et la première remarque, égal au dernier reste non nul.

3. Exemple élémentaire

Suivons l'algorithme si $a = -21$ et $b = 15$:

$(a, b) = (21, 15)$ et $r = 6$,

$(a, b) = (15, 6)$ et $r = 3$,

$(a, b) = (6, 3)$ et $r = 0$ d'où $\text{pgcd}(-21, 15) = 3$.

On reviendra plus en détail sur cet algorithme dans le cadre du théorème de Bézout qui va suivre.

III. Primalité

Ici aussi (a, b) désigne un élément de \mathbb{Z}^2 .

A. Nombres premiers entre eux

1. Définition

a et b sont dits **premiers entre eux** si 1 est leur pgcd ie. si les seuls communs diviseurs sont 1 et -1 .

2. Généralisation

Soient $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n$.

1. a_1, a_2, \dots, a_n sont dits **premiers entre eux dans leur ensemble** si $\text{pgcd}(a_1, \dots, a_n) = 1$.

2. a_1, a_2, \dots, a_n sont dits **premiers entre eux deux à deux** si pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$ tel que $i < j$, on a $\text{pgcd}(a_i, a_j) = 1$.

Remarque

Si a_1, a_2, \dots, a_n sont premiers entre eux deux à deux alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fautive comme le prouve l'exemple $(a, b, c) = (6, 10, 15)$.

En effet $\text{pgcd}(a, b, c) = \text{pgcd}(6, \text{pgcd}(10, 15)) = \text{pgcd}(6, 5) = 1$ alors que les nombres 6, 10 et 15 ne sont pas deux à deux premiers entre eux, voire pire.

3. Théorème de Bézout

| a et b sont premiers entre eux si, et seulement s'il existe un couple (u, v) d'entiers tel que $au + bv = 1$.

Démonstration

$\text{pgcd}(a, b) = 1 \iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \Rightarrow \exists(u, v) \in \mathbb{Z}^2, au + bv = 1$.

Réciproquement si $au + bv = 1$ alors $1 \in a\mathbb{Z} + b\mathbb{Z}$ d'où $\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$ et, comme l'inclusion réciproque est immédiate, il vient $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ ie. $\text{pgcd}(a, b) = 1$. \square

Corollaire

| Si a est premier avec les entiers b et c alors il est premier avec bc .

Démonstration

On utilise les deux sens du théorème de Bézout.

On choisit (u, v, u', v') dans \mathbb{Z}^4 tel que $au + bv = au' + cv' = 1$ et alors, par produit, $a(auu' + cuv' + bu'v) + (bc)(vv') = 1$, par suite $\text{pgcd}(a, bc) = 1$. \square

4. Théorème de Gauss

| Si $(a, b, c) \in \mathbb{Z}^3$, a divise bc et a est premier avec b alors a divise c .

Démonstration

Si $au + bv = 1$ comme dans le théorème de Bézout alors $acu + bcv = c \in a\mathbb{Z}$ car $bc \in a\mathbb{Z}$. \square

Corollaire

| Si a, b, c sont des entiers, $a|c$, $b|c$ et $\text{pgcd}(a, b) = 1$ alors $ab|c$.

Démonstration

On écrit $c = ak$. Alors $b|ak$ et b est premier avec a donc $b|k$ d'où $ab|c$. \square

5. Retour à l'algorithme d'Euclide

On reprend l'algorithme décrit dans le cas où $0 < b \leq a$ et on écrit la suite des égalités de division euclidienne en posant $r_0 = a$ et $r_1 = b$, le dernier reste non nul est noté r_n :

$$r_0 = r_1q_1 + r_2 \quad (1)$$

$$r_1 = r_2q_2 + r_3 \quad (2)$$

$$\vdots$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad (n-1)$$

$$r_{n-1} = r_nq_n + 0 \quad (n)$$

avec $0 = r_{n+1} < r_n < \dots < r_1$ et $r_n = \text{pgcd}(a, b)$.

De l'égalité $(n-1)$ on tire $r_n = r_{n-2} + r_{n-1}(-q_{n-1})$ or l'égalité $(n-2)$ fournit $r_{n-1} = r_{n-3} + r_{n-2}(-q_{n-2})$ d'où $r_n = r_{n-3}(-q_{n-1}) + r_{n-2}(1 + q_{n-1}q_{n-2})$.

En itérant ce procédé on arrive à une égalité $\text{pgcd}(a, b) = r_n = r_0u + r_1v$, soit $\text{pgcd}(a, b) = au + bv$.

En particulier lorsque a et b sont premiers entre eux cela fournit un procédé de calcul d'un couple (u, v) d'entiers vérifiant $au + bv = 1$.

6. Équation diophantienne

c désigne un entier et on suppose $ab \neq 0$. On se propose de déterminer l'ensemble $\{(x, y) \in \mathbb{Z}^2 \mid ax + by = c\}$ noté S .

Si l'on pose $d = \text{pgcd}(a, b)$ alors, immédiatement, $S \neq \emptyset \Rightarrow c \in d\mathbb{Z}$.

Supposons désormais $c \in d\mathbb{Z}$, écrivons $(a, b, c) = d(a', b', c')$, remarquons que a' et b' sont premiers entre eux et choisissons (u, v) dans \mathbb{Z}^2 tel que $a'u + b'v = 1$.

Théorème

$$\mid S = \{(uc' + kb', vc' - ka') \mid k \in \mathbb{Z}\} = c'(u, v) + (b', -a')\mathbb{Z}.$$

Démonstration

Comme $a'uc' + b'vc' = c'$, par différence :

$$(x, y) \in S \iff a'(x - uc') = b'(vc' - y).$$

Si $(x, y) \in S$, comme b' divise $a'(x - uc')$ et $\text{pgcd}(a', b') = 1$, le théorème de Gauss montre que b' divise $x - uc'$ et donc il existe un entier k tel que $x = uc' + kb'$.

Réciproquement si $x = uc' + kb'$ alors $(x, y) \in S \iff a'b'k = b'(vc' - y)$, ce qui équivaut à $y = vc' - ka'$ car $b' \neq 0$. Le résultat en découle. \square

B. Nombres premiers

1. Généralités

1.1. Définition

Un entier naturel p est dit **premier** s'il a exactement deux diviseurs 1 et p dans \mathbb{N} (et donc exactement quatre diviseurs dans \mathbb{Z}). On note \mathcal{P} l'ensemble des nombres premiers.

Exemples

Les nombres 2, 3, 5, 7, 11, 13, 17, 19, 23, 1234567891 sont premiers (courage pour le dernier).

1.2. Proposition

| Si $p \in \mathcal{P}$ et $k \in \llbracket 1, p-1 \rrbracket$ alors $\binom{p}{k} \in p\mathbb{N}$.

Démonstration

$(p-k) \binom{p}{k} = p \binom{p-1}{k}$. Comme p et $p-k$ sont premiers entre eux le théorème de Gauss fournit le résultat. \square

2. Décomposition

2.1. Proposition

| Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.

Démonstration

L'ensemble D des diviseurs de n dans $\llbracket 2, n \rrbracket$ est fini et non vide car n en est élément. D admet donc un plus petit élément, noté p , au sens de la divisibilité. Nécessairement p est un nombre premier. \square

Remarque

Si on examine le nombre p défini dans la démonstration précédente, ou bien $p = n$ si $n \in \mathcal{P}$, ou bien $p \leq \sqrt{n}$ car il existe q dans $\llbracket p, n \rrbracket$ tel que $n = pq$.

2.2. Corollaire

| L'ensemble \mathcal{P} est infini

Démonstration

Sinon et si p_1, \dots, p_n est la liste des éléments de \mathcal{P} alors $1 + \prod_{i=1}^n p_i$ est un entier supérieur à 2 sans diviseur premier, ce qui est impossible. \square

2.3. Théorème de décomposition

| Tout nombre entier $n \geq 2$ admet une unique décomposition en produit de nombres premiers (à l'ordre près des facteurs), autrement dit il existe une unique application ω_n de \mathcal{P} dans \mathbb{N} à support fini telle que
$$n = \prod_{p \in \mathcal{P}} p^{\omega_n(p)}.$$

Démonstration

Commençons par démontrer l'existence de l'application ω_n par récurrence sur n .

$\omega_2 : p \mapsto \begin{cases} 1 & \text{si } p = 2 \\ 0 & \text{sinon} \end{cases}$ convient.

Soit $n \geq 2$ tel que tout élément de $\llbracket 2, n \rrbracket$ admet une décomposition en produit de nombres premiers.

Si $n + 1 \in \mathcal{P}$ alors $\omega_{n+1} : p \mapsto \begin{cases} 1 & \text{si } p = n + 1 \\ 0 & \text{sinon} \end{cases}$ convient.

Sinon soit p_0 un diviseur premier de $n + 1$ et soit $m = \frac{n + 1}{p_0}$, alors $m \in \llbracket 2, n \rrbracket$

d'où $m = \prod_{p \in \mathcal{P}} p^{\omega_m(p)}$ et, en posant $\omega_{n+1} : p \mapsto \begin{cases} \omega_m(p_0) + 1 & \text{si } p = p_0 \\ \omega_m(p) & \text{sinon} \end{cases}$ on a

$n + 1 = \prod_{p \in \mathcal{P}} p^{\omega_{n+1}(p)}$, ce qui établit l'hérédité de la propriété.

Reste à établir l'unicité de ω_n pour tout entier $n \geq 2$.

Supposons que ω et ω' sont deux applications de \mathcal{P} dans \mathbb{N} à supports finis telles que $\prod_{p \in \mathcal{P}} p^{\omega(p)} = \prod_{p \in \mathcal{P}} p^{\omega'(p)}$.

Soit $p_0 \in \mathcal{P}$ tel que $\omega(p_0) \geq 1$. Alors p_0 divise $p_0^{\omega'(p_0)} \prod_{p \neq p_0} p^{\omega'(p)}$ et p_0 est

premier avec $\prod_{p \neq p_0} p^{\omega'(p)}$ donc, d'après le théorème de Gauss, p_0 divise $p_0^{\omega'(p_0)}$ i.e. $\omega'(p_0) \geq 1$.

Par suite $p_0^{\omega(p_0)-1} \prod_{p \neq p_0} p^{\omega(p)} = p_0^{\omega'(p_0)-1} \prod_{p \neq p_0} p^{\omega'(p)}$ et, en itérant le procédé précédent si $\omega(p_0) \geq 2$ on aboutit à $\omega'(p_0) \geq \omega(p_0)$. Par raison de symétrie $\omega(p_0) \geq \omega'(p_0)$ i.e. $\omega(p_0) = \omega'(p_0)$.

Comme cela est valable dès que $\omega(p_0) \geq 1$ ou, par symétrie, dès que $\omega'(p_0) \geq 1$, on en déduit que ω et ω' ont même support et que $\omega = \omega'$. \square

Remarques

- Si ω_1 est l'application nulle de \mathcal{P} dans \mathbb{N} on a également $1 = \prod_{p \in \mathcal{P}} p^{\omega_1(p)}$.

- Si $ab \neq 0$ on a les décompositions $|a| = \prod_{p \in \mathcal{P}} p^{\omega_a(p)}$ et $|b| = \prod_{p \in \mathcal{P}} p^{\omega_b(p)}$.

Alors $\text{pgcd}(a, b) = \prod_{p \in \mathcal{P}} p^{\min(\omega_a(p), \omega_b(p))}$ et $\text{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{\max(\omega_a(p), \omega_b(p))}$.

2.4. Corollaire

| On a toujours $|ab| = \text{pgcd}(a, b) \text{ppcm}(a, b)$.

Démonstration

C'est immédiat si $ab = 0$ et cela découle de la dernière remarque dans le cas contraire car alors $|ab| = \prod_{p \in \mathcal{P}} p^{\omega_a(p) + \omega_b(p)} = \text{pgcd}(a, b) \text{ppcm}(a, b)$. \square