Arithmétiques dans $\mathbb{Z}$

I) Diviseurs et multiples d'un entier :

1°) Définition :

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

- On dit que b divise a ou a est un multiple de b si :
  $\exists\, k \in \mathbb{Z}$ tq : $a = kb$. On écrit $b|a$.

- On note $D(a)$: l'ensemble des diviseurs de a
  $a\mathbb{Z}$: l'ensemble des multiples de a : $a\mathbb{Z} = \{ka / k \in \mathbb{Z}\}$

- Rq : • On a : $\forall b \in \mathbb{Z} : 0 = b \times 0$, donc : $\forall b \in \mathbb{Z} : b|0$.

- Propriétés :

i) $\forall a \in \mathbb{Z} : a|a$

ii) $\forall (a,b,c) \in \mathbb{Z}^3 : (a|b \text{ et } b|c \Rightarrow a|c)$

iii) $\forall (a,b) \in \mathbb{Z}^2 : a|b \text{ et } b|a \Leftrightarrow |a| = |b|$.

iv) $\forall (a,b,c,d) \in \mathbb{Z}^4 : a|b, c|d \Rightarrow ac|bd$.

v) $\forall (a,b,k,k') \in \mathbb{Z}^4 : a|b \text{ et } a|c \Rightarrow a|kb+k'c$.

2°) Division euclidienne :

Théo : Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.
Alors : $\exists!\, (q,r) \in \mathbb{Z}^2$ tq : $a = bq + r$ avec $0 \leqslant r < b$.

Preuve : *) Montrons l'unicité :

Si : $\exists (q,r), (q',r') \in \mathbb{Z}^2$ tq : $a = bq + r = bq' + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b$,

alors : $b(q-q') = r' - r$. Or $-b < r' - r < b$, alors, $-b < b(q-q') < b$

donc : $-1 < q - q' < 1$, par suite, $q = q'$ ensuite $r = r'$.

Scanned with CamScanner

*) Montrons l'existence: Soit $a\in\mathbb{Z}$, $b\in\mathbb{N}^*$.

1ère cas: Si $a\in\mathbb{N}$: considérons l'ensemble $A=\{n\in\mathbb{N} / nb\leq a\}$.

→ $A\subset\mathbb{N}$, $A\neq\emptyset$ (car $0\in A$), et A est majorée (para)

→ donc A admet un plus grand élt $q\in A$.

→ Comme $(q+1)\notin A$, alors, $(q+1)b>a$, donc: $b>a-qb$.

→ Posons $r=a-qb$. On a donc: $0\leq r<b$.

D'où l'existence d'un couple (q,r).

2ème cas: Si $a\in\mathbb{Z}^*$: alors $-a\in\mathbb{N}^*$.

Donc: $\exists!\,(q,r)\in\mathbb{Z}^2$ tq: $-a=bq+r$ avec $0\leq r<b$.

Donc: $a=b.(-q)+(-r)$.

→ Si $r=0$: $a=(-q)b+0$. C'est fini.

→ Si $r\neq 0$: alors $a=(-q)b-r=\underbrace{(-q-1)}_{q'}b+\underbrace{b-r}_{r'}=q'b+r'$ avec $0<r'<b$. ■

---

3) PGCD:

Soit $(a,b)\in\mathbb{Z}^2$ avec $(a,b)\neq(0,0)$.

→ On note $D(a,b)$: l'ensemble des diviseurs communs à a et b.

→ $D(a,b)\neq\emptyset$ (car $1\in D(a,b)$), $D(a,b)\subset\mathbb{Z}$, $D(a,b)$ est majorée (par $|a|$)

donc $D(a,b)$ admet un plus grand élt.

Déf: Le plus grand élt de $D(a,b)$ st appelé le plus grand commun diviseur de a et b, on le note $pgcd(a,b)$ ou $a\wedge b$.

Rq: Par convention: si $a=b=0$, $a\wedge b=0$.

Exples: $pgcd(3,12)=3$, $pgcd(-5,15)=5$

→ **Algorithme d'Euclide:**

Soit $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$. Donc $\exists!\,(q,r)\in\mathbb{Z}^2$: $a=bq+r$ avec $0\leq r<b$.

On a le théo. suivant:

/2

Scanned with CamScanner

Théo: $a \wedge b = b \wedge r$.

Preuve: Mq $D(a,b) = D(b,r)$.

→ Soit $d \in D(a,b)$.

$d \in D(a,b) \Rightarrow d|a$ et $d|b$

$\Rightarrow d|a-bq$ et $d|b$.

$\Rightarrow d|r$ et $d|b$

$\Rightarrow d \in D(b,r)$. Donc $D(a,b) \subset D(b,r)$.

→ Soit $d' \in D(b,r)$. $d' \in D(b,r) \Rightarrow d'|b$ et $d'|r$

$\Rightarrow d'|bq$ et $d'|r$ or $d'|b$.

$\Rightarrow d'|bq+r$ et $d'|b$

$\Rightarrow d'|a$ et $d'|b$

$\Rightarrow d' \in D(a,b)$. Donc $D(b,r) \subset D(a,b)$.

→ D'où $D(a,b) = D(b,r)$, par suite $pgcd(a,b) = pgcd(b,r)$. ■

Rq: L'algorithme d'Euclide permet de calculer le pgcd de deux entiers: soit $(a,b) \in \mathbb{N}^{*2}$ tq $a \geq b$. Donc:

$$\begin{cases} a = bq_1 + r_1 \\ 0 \leq r_1 < b \end{cases} \xrightarrow{\text{ensuite}} \begin{cases} b = r_1 q_2 + r_2 \\ 0 \leq r_2 < r_1 \end{cases} \longrightarrow \begin{cases} r_1 = r_2 q_3 + r_3 \\ 0 \leq r_3 < r_2 \end{cases} \quad \dots\dots$$

Ainsi, on a une suite d'entiers $(r_k)_{k \geq 1}$ telle que: $b > r_1 > r_2 > r_3 > \dots\dots \geq 0$.

donc: $\exists n \in \mathbb{N}^*$ tq: $b > r_1 > r_2 > \dots > r_{n-1} > r_n = 0$.

Et l'algorithme s'arrête donc.

→ Alors: (d'après le théo), $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-2} \wedge r_{n-1} = r_{n-1}$

(car $r_{n-2} = r_{n-1} \cdot q_n + \underbrace{r_n}_{=0}$)

[le dernier reste non nul]

Exemple: $pgcd(366;43) = ?$.

$366 = 43 \times 8 + 22 \longrightarrow 43 = 22 \times 1 + 21 \longrightarrow 22 = 21 \times 1 + 1 \longrightarrow$

$21 = 21 \times 1 + 0$, donc: $\boxed{366 \wedge 34 = 1}$.

Scanned with CamScanner

Théo: (Caractérisation du PGCD)

Soit $(a,b)\in\mathbb{Z}^2$, $d\in\mathbb{N}$. Les p.s.s.e :

i) $a\wedge b = d$

ii) $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$

iii) $\forall c\in\mathbb{N} : (c\mid a \text{ et } c\mid b \Rightarrow c\mid d)$

$a\mathbb{Z}+b\mathbb{Z} = \{ak+bk' / k,k'\in\mathbb{Z}\}$

Preuve : i) $\Rightarrow$ ii) On suppose $a\wedge b = d$.

• Mq $a\mathbb{Z}+b\mathbb{Z}\subset d\mathbb{Z}$: $d = a\wedge b \Rightarrow d\mid a$ et $d\mid b$.

$\Rightarrow d\mid ak+bk',\ \forall k,k'\in\mathbb{Z}$

~~$\Rightarrow ak+bk'\in a\mathbb{Z}+b\mathbb{Z}$~~

$\Rightarrow \forall k,k'\in\mathbb{Z} : ak+bk'\in d\mathbb{Z}$.

donc : $\boxed{a\mathbb{Z}+b\mathbb{Z}\subset d\mathbb{Z}}$.

• Mq $d\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}$:

→ Vérifier, d'abord, que $a\mathbb{Z}+b\mathbb{Z}$ est un sous-gpe de $(\mathbb{Z},+)$. (Exercice).

→ Donc : $\exists n\in\mathbb{Z}$ tq : $a\mathbb{Z}+b\mathbb{Z} = n\mathbb{Z}$.

→ mq : $d\mathbb{Z}\subseteq n\mathbb{Z}$?

* si $a=b=0$, alors, $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z} = \{0\}$.

* si $(a,b)\neq(0,0)$, alors, $n\in\mathbb{N}^*$.

On a $n\in n\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$, donc, $n = ak+bk'$ avec $(k,k')\in\mathbb{Z}^2$.

Or : $d\mid a$ et $d\mid b$, alors, $d\mid n$, donc $\boxed{d\leq n}$ ①

D'autre part : $\begin{cases} a\in a\mathbb{Z}+b\mathbb{Z} = n\mathbb{Z} \\ b\in a\mathbb{Z}+b\mathbb{Z} = n\mathbb{Z} \end{cases} \Rightarrow n\mid a$ et $n\mid b$

$\Rightarrow n\in D(a,b)$

$\Rightarrow \boxed{n\leq d}$ ②.

De ① et ②, on a : $d=n$ et donc $\boxed{d\mathbb{Z} = n\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}}$.

ii) $\Rightarrow$ iii) : On suppose $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$. Soit $c\in\mathbb{N}$ tq $c\mid a$ et $c\mid b$.

$c\mid a$ et $c\mid b \Rightarrow c\mid au+bv,\ \forall u,v\in\mathbb{Z}$

$\Rightarrow au+bv\in c\mathbb{Z}$, " "

$\Rightarrow a\mathbb{Z}+b\mathbb{Z}\subset c\mathbb{Z}$

$\Rightarrow d\mathbb{Z}\subset c\mathbb{Z} \Rightarrow \boxed{c\mid d}$

Scanned with CamScanner

iii) $\Rightarrow$ i) : exercice.

Conséquence : (Relation de Bezout)

Soit $(a,b) \in \mathbb{Z}^2$ et $d = a \wedge b$.
Alors : $\exists (u,v) \in \mathbb{Z}^2$ tq : $d = au + bv$.
Un tel couple (u,v) n'est pas unique.

Exemple : on a déjà vu : $366 \wedge 43 = 1$. Cherchons un couple $(u,v) \in \mathbb{Z}^2$ tq : $366u + 43v = 1$.

→ On a : $366 = 43 \times 8 + 22$, $43 = 22 \times 1 + 21$, $22 = 21 \times 1 + \boxed{1}$ "d

→ donc : $1 = 22 - 21 \times 1$
$= 22 - (43 - 22) = -43 + 2 \times 22$
$= -43 + 2(366 - 43 \times 8)$
$= -17 \times 43 + 2 \times 366$. On prend $x = -17$ et $y = 2$.

Généralisation :

→ Soient $a_1, \dots, a_n \in \mathbb{Z}$. $D(a_1, \dots, a_n)$ l'ensemble des diviseurs communs des a_i.

→ $D(a_1, \dots, a_n) \neq \emptyset$ (contient 1), majoré par $|a_1 \times \dots \times a_n|$, donc, admet un plus grand élt, appelé, le plus grand commun diviseur de $a_1, \dots, a_n$, noté : $\text{pgcd}(a_1, \dots, a_n)$.

→ **Théo :** $a_1, \dots, a_n \in \mathbb{Z}$ et $d \in \mathbb{N}$. Les p.s.s.e :

i) $\text{pgcd}(a_1, \dots, a_n) = d$
ii) $\sum_{i=1}^{n} a_i \mathbb{Z} = d\mathbb{Z}$
iii) $\forall c \in \mathbb{N} : (\forall i \in [\![1;n]\!], c \mid a_i \Rightarrow c \mid d)$.

Scanned with CamScanner

4) PPCM :

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

↦ L'ensemble des multiples communs à $a_1, \dots, a_n$ est :

$$a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = \bigcap_{i=1}^{n} a_i \cdot \mathbb{Z} .$$

↦ Soit M l'ensemble : $M = \left(\bigcap_{i=1}^{n} a_i \cdot \mathbb{Z}\right) \cap \mathbb{N}^*$.

↦ $M \subset \mathbb{N}$, $M \neq \emptyset$ (car $\prod_{i=1}^{n} a_i \in M$), donc M admet un plus petit élt, appelé le plus petit ~~élt~~ commun multiple de $a_1, \dots, a_n$, noté : $\text{ppcm}(a_1, \dots, a_n)$.

Rq : $\text{ppcm}(a_1, \dots, a_n) \geq 0$

↦ Si $n=2$: on note aussi : $\text{ppcm}(a_1, a_2) = a_1 \vee a_2$.

↦ Exemples : $3 \vee 4 = 12$, $(-11) \vee 5 = 55$.

Théo : (Caractérisation du ppcm).

Soit $(a,b) \in \mathbb{Z}^2$, $m \in \mathbb{N}$. Alors les p.s.s. e :

i) $\text{ppcm}(a,b) = m$ ii) $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

iii) $\forall c \in \mathbb{N} : (a|c \text{ et } b|c \Rightarrow m|c)$

Preuve : i) ⇒ ii) : on suppose (i).

→ On sait que : $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous gpe de $(\mathbb{Z}, +)$ (intersection de sous-gpes est un sous-gpe)

donc : $\exists n \in \mathbb{N}$ tq $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$. Montrons donc : $n\mathbb{Z} = m\mathbb{Z}$.

→ On a : $a|m$ et $b|m \Rightarrow m \in a\mathbb{Z} \cap b\mathbb{Z}$
$\Rightarrow m \in n\mathbb{Z}$
$\Rightarrow n|m \Rightarrow \boxed{n \leq m}$.

→ D'autre part : $n \in n\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ donc n est un multiple commun de a et b donc $\boxed{m \leq n}$

Scanned with CamScanner

D'où $m=n$.

ii) $\Rightarrow$ iii) : On suppose (ii). Soit $c\in\mathbb{N}$ tq $a|c$ et $b|c$.

→ Donc : $\begin{cases} c\in a\mathbb{Z} \\ c\in b\mathbb{Z} \end{cases}$, donc, $c\in a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$

par suite : $m|c$.

iii) $\Rightarrow$ i) : exercice.

Rq : $(a|c \text{ et } b|c \Rightarrow a\vee b|c)$.

→ **Généralisation :**

Théo : Soient $a_1,\dots,a_n\in\mathbb{Z}$, $m\in\mathbb{N}$. Les p.s.s.e :

i) $ppcm(a_1,\dots,a_n)=m$

ii) $\bigcap_{i=1}^{n} a_i\mathbb{Z}=m\mathbb{Z}$.

iii) $(\forall c\in\mathbb{N}) : (\forall i,\ a_i|c \Rightarrow m|c)$

Exercice : Soit $a_1,\dots,a_n\in\mathbb{Z}$ et $k\in\mathbb{Z}$.

Mq : a) $pgcd(ka_1,\dots,ka_n)=|k|\,pgcd(a_1,\dots,a_n)$.

b) $ppcm(ka_1,\dots,ka_n)=|k|\,ppcm(a_1,\dots,a_n)$

Solution :

a) On pose $pgcd(a_1,\dots,a_n)=d$ et $pgcd(ka_1,\dots,ka_n)=\Delta$.

On a donc : $\Delta\mathbb{Z}=\sum_{i=1}^{n}(ka_i)\mathbb{Z}\overset{\text{(à vérifier)}}{=}k\sum_{i=1}^{n}a_i\mathbb{Z}$

$\Delta\mathbb{Z}=k(d\mathbb{Z})=(kd)\mathbb{Z}$, donc :

$|\Delta|=|kd|$, d'où $\Delta=|k|d$ (car $\Delta\geq 0$ et $d\geq 0$).

b) On pose $ppcm(a_1,\dots,a_n)=m$ et $ppcm(ka_1,\dots,ka_n)=M$

donc $M\mathbb{Z}=\bigcap_{i=1}^{n}(ka_i\mathbb{Z})=k\left(\bigcap_{i=1}^{n}a_i\mathbb{Z}\right)$ (à vérifier).

$=k(m\mathbb{Z})$

donc : $M\mathbb{Z}=(km)\mathbb{Z}$, donc $|M|=|km|$

d'où $M=|k|m$ (car $m\geq 0$ et $M\geq 0$)

4