# Chapitre 40

Arithmétique dans $\mathbb{Z}$.

## Sommaire.



Les propositions marquées de ★ sont au programme de colles.

## 1 Divisibilité dans $\mathbb{Z}$

### 1.1 Définition et propriétés élémentaires.

**Définition 1**

Soit $(a,b) \in \mathbb{Z}^2$. On dit que $b$ **divise** $a$ ($b \mid a$) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On dit aussi que $b$ est **diviseur** de $a$, ou que $a$ est **multiple** de $b$.

Notations pour les ensembles de diviseurs et multiples de $a \in \mathbb{Z}$:

$$\mathcal{D}(a) = \{b \in \mathbb{Z} : b \mid a\} \qquad \text{et} \qquad a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}.$$

**Proposition 2: Faits immédiats.**

Tous les entiers divisent 0 et 1 divise tous les entiers. Ajoutons que pour $(a,b,c) \in \mathbb{Z}^3$,

1. Si $b$ est diviseur de $a$ et si $a \neq 0$, alors $|b| \leq |a|$.
2. $b \mid a \iff a\mathbb{Z} \subset b\mathbb{Z}$.
3. Si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$, pour tous $u$ et $v$ dans $\mathbb{Z}$.

**Preuve :**

$\boxed{1.}$ Supposons que $b \mid a$ et $a \neq 0$, alors $\exists k \in \mathbb{Z} \mid a = bk$ et $|a| = |b||k|$.
De plus, $k \neq 0$ car $a \neq 0$, donc $|k| \geq 1$ et $|kb| \geq |b|$, on obtient bien $|a| \geq |b|$.

$\boxed{2.}$ Supposons que $b \mid a$, alors $\exists k \in \mathbb{Z} \mid a = bk$, soit $m \in a\mathbb{Z} : \exists k' \in \mathbb{Z} \mid m = ak'$ donc $m = bkk'$ donc $m \in b\mathbb{Z}$.
Supposons $a\mathbb{Z} \subset b\mathbb{Z}$, on a $a \in a\mathbb{Z}$ donc $a \in b\mathbb{Z}$ donc $b \mid a$.

$\boxed{3.}$ Supposons que $c \mid a$ et $c \mid b$ : $\exists k, k' \in \mathbb{Z} \mid a = kc,\ b = k'c$. Soient $u, v \in \mathbb{Z}$.
On a alors $au + bv = kuc + k'vc = (ku + k'v)c$ avec $ku + k'v \in \mathbb{Z}$, donc $c \mid au + bv$.

**Proposition 3: Plus une relation d'ordre!**

Sur $\mathbb{Z}$, la relation *divise* est réflexive, transitive, mais pas antisymétrique. On a

$$\forall (a,b) \in \mathbb{Z}^2 \quad (a \mid b \text{ et } b \mid a) \iff (a = b \text{ ou } a = -b).$$

Dans le cas où $(a \mid b)$ et $(b \mid a)$, ont dit que $a$ et $b$ sont **associés**.

**Preuve :**

$\boxed{\Longleftarrow}$ Trivial.
$\boxed{\Longrightarrow}$ Supposons que $a \mid b$ et $b \mid a$. Alors $\exists k, k' \in \mathbb{Z} \mid a = kb$ et $b = k'a$.
On a alors $b = bkk'$. Si $b = 0$, alors $a = 0$ donc $a = b$. Sinon, $kk' = 1$ donc $k = \pm 1$ et $a = \pm b$.

### 1.2 Division euclidienne.

**Théorème 4**

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que

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

Les entiers $q$ et $r$ sont appelés **quotient** et **reste** dans la division euclidienne de $a$ par $b$.

**Preuve :**

**Unicité:**
Soit $(q,r) \in \mathbb{Z}^2$ et $(q',r') \in \mathbb{Z}^2$ avec $0 \leq r, r' < b$ tels que $a = bq + r$ et $a = bq' + r'$.
On a $bq' + r' = bq + r$ donc $b(q' - q) = r - r'$. De plus, $0 \leq r, r' < b$ donc $-b < -r' \leq 0$.
Ainsi, $-b < r - r' < b$ donc $-b < b(q' - q) < b$ donc $-1 < q' - q < 1$ donc $q' = q$ car $q - q' \in \mathbb{Z}$.
Donc $r - r' = b \cdot 0 = 0$ donc $(q,r) = (q',r')$.

**Existence:**
On pose $q = \lfloor \frac{a}{b} \rfloor$ et $r = a - bq$. On a bien $a = bq + r$.
On a $\lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} < \lfloor \frac{a}{b} \rfloor + 1$ donc $q \leq \frac{a}{b} < q + 1$ donc $qb \leq a < qb + b$ donc $0 \leq a - bq < b$ donc $0 \leq r < b$.

**Proposition 5**

Soient $a$ et $b$ deux entiers relatifs.
L'entier $b$ divise $a$ si et seulement si le reste de la division euclidienne de $a$ par $|b|$ est nul.

**Preuve :**

$\boxed{\Longleftarrow}$ Trivial.
$\boxed{\Longrightarrow}$ Par unicité du reste.

### 1.3 PPCM de deux entiers.

**Définition 6**

Soient $a, b$ deux entiers relatifs.
1. Si $a$ et $b$ sont non nuls, on appelle **Plus Petit Commun Multiple** de $a$ et $b$, note $a \vee b$, ou encore $\mathrm{PPCM}(a,b)$, le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.
2. Si $a$ ou $b$ vaut 0, on pose $a \vee b = 0$.

**Proposition 7**

Soit $(a,b) \in \mathbb{Z}^2$. Leur PPCM $a \vee b$ est l'unique entier positif $m$ tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

**Preuve :**

**Unicité:**
Soient $m, m' \in \mathbb{N}$ tels que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$.
Alors $m\mathbb{Z} = m'\mathbb{Z}$ donc $m$ et $m'$ sont associés (et positifs) donc $m = m'$.

**Existence:**
On a $a\mathbb{Z}$ sous-groupe de $(\mathbb{Z}, +)$, $b\mathbb{Z}$ aussi, par intersection de groupes, $a\mathbb{Z} \cap b\mathbb{Z}$ l'est aussi.
Or les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$. Donc il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.
Vérifions que $m = \mathrm{PPCM}(a,b)$. Clair: $m$ est multiple commun de $a$ et $b$.
De plus, $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N} = m\mathbb{Z} \cap \mathbb{N} = \{0, m, 2m, ...\}$.
Donc si $m = 0$, $\mathrm{PPCM}(a,b) = 0$, sinon $\mathrm{PPCM}(a,b) = m$.

**Théorème 8**

Soient $a$ et $b$ deux entier relatifs. Leur PPCM $a \vee b$ est l'unique entier positif $m$ tel que
1. $a \mid m$ et $b \mid m$, *le PPCM est un multiple commun.*
2. $\forall \mu \in \mathbb{Z},\ (a \mid \mu$ et $b \mid \mu) \Longrightarrow m \mid \mu$, *tout multiple commun est multiple du PPCM.*

**Preuve :**

**Unicité:** Soient $m, m'$ satisfaisant 1. et 2.
On a $m \mid m'$ et $m' \mid m$, par antisymétrie sur $\mathbb{N}$, $m = m'$.

**Existence:** Posons $m = \mathrm{PPCM}(a,b)$.
Il satisfait 1. par définition. Soit $\mu \in \mathbb{Z}$ un multiple commun, alors $\mu \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, donc $m \mid \mu$.

### 1.4 PGCD de deux entiers.

**Définition 9**

Soient $a, b$ deux entiers relatifs.
1. Si $a$ et $b$ sont non nuls, on appelle **Plus Grand Commun Diviseur** de $a$ et $b$, note $a \wedge b$, ou encore $\mathrm{PGCD}(a,b)$, le plus grand élément positif de $\mathcal{D}(a) \cap \mathcal{D}(b)$.
2. Si $a = b = 0$, on pose $a \wedge b = 0$.

**Proposition 10**

$$\forall (a,b) \in \mathbb{Z}^2 \quad a \wedge b = |a| \wedge |b|$$

**Preuve :**

On a:

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(|a|) \cap \mathcal{D}(|b|).$$

On n'a plus qu'à passer au max.

**Proposition 11: Lemme d'Euclide.**

Soient $a, b, c, d$ quatre entiers relatifs. Si $a = bc + d$, alors on a $a \wedge b = b \wedge d$.

**Preuve :**

Supposons que $a = bc + d$. Se convaincre que $\mathcal{D}(a, b) = \mathcal{D}(b, d)$ puis passer au max.

**Méthode**

Ce lemme est l'idée principale de l'algorithme d'Euclide, vu dans le "petit" cours d'arithmétique.
Si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, on peut appliquer cet algorithme à $|a|$ et $|b|$ pour calculer $a \wedge b$.

**Proposition 12: Le sous-groupe de $\mathbb{Z}$ sous-jacent.**

Soit $(a, b) \in \mathbb{Z}^2$. Notons $a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ (u, v) \in \mathbb{Z}^2\}$. C'est un sous-groupe de $\mathbb{Z}$.

Le PGCD $a \wedge b$ est l'unique entier positif $d$ tel que

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

En particulier, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$ **(relation de Bézout)**.

**Preuve :**

On a $a\mathbb{Z} + b\mathbb{Z} = \{au + bv \mid (u, v) \in \mathbb{Z}^2\}$.
C'est un sous-groupe de $\mathbb{Z}$ car $0 = a \cdot 0 + b \cdot 0 \in a\mathbb{Z} + b\mathbb{Z}$ et,
Pour $(m, m') \in (a\mathbb{Z} + b\mathbb{Z})^2$, $\exists (u, v, u', v') \in \mathbb{Z} \mid m = au + bv$ et $m' = au' + bv'$
Donc $m - m' = a(u - u') + b(v - v') \in a\mathbb{Z} + b\mathbb{Z}$.

D'après le cours sur les structures algébriques, il existe $d \in \mathbb{N} \mid a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

**Unicité:** Si $d, d'$ conviennent, $d\mathbb{Z} = d'\mathbb{Z}$, ils sont associés et positits donc $d = d'$.

Montrons que $d = \text{PGCD}(a, b)$.
On a $d \mid a$ et $d \mid b$ car $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$, pareil pour $b\mathbb{Z}$.
Soit $\delta \in \mathbb{N}$ diviseur de $a$ et $b$, on a $\exists (u, v) \in \mathbb{Z}^2 \mid d = uv + bv$.
Puisque $\delta$ divise $a$ et $b$, alors $\delta$ divise $au + bv = d$.
Si $d \neq 0$, $\delta \mid d \Longrightarrow \delta \leq d$, sinon, $d = 0$ donc $a = b = 0$ donc $d = \text{PGCD}(a, b) = 0$.

**Méthode : Écriture effective d'une relation de Bézout.**

En *remontant* les divisions euclidiennes écrites lors de l'exécution de l'algorithme d'Euclide.

**Proposition 13**

$$\forall (a, b) \in \mathbb{Z}^2, \quad \forall k \in \mathbb{Z}, \quad \text{PGCD}(ka, kb) = |k| \cdot \text{PGCD}(a, b).$$

**Preuve :**

On a $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ donc $ka\mathbb{Z} + kb\mathbb{Z} = |k|(a \wedge b)\mathbb{Z}$.
On a aussi $ka \wedge kb = |k|(a \wedge b)$.

**Théorème 14: Une caractérisation du PGCD**

Soient $a$ et $b$ deux entiers relatifs. Leur PGCD $a \wedge b$ est l'unique entier positif $d$ tel que

1. $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$, *(le PGCD est un diviseur commun).*
2. $\forall \delta \in \mathcal{D}(a) \cap \mathcal{D}(b) \quad \delta \mid d$ *(tous les diviseurs communs divisent le PGCD).*

**Preuve :**

Notons $d = \text{PGCD}(a, b)$, montrons que $d$ satisfait 1. et 2..
Il satisfait 1. par définition.
Soit $\delta \in \mathbb{Z} \mid \delta \mid a$ et $\delta \mid b$, $\exists (u, v) \in \mathbb{Z}^2 \mid d = au + bv$.
Il est clair que $\delta \mid au + bv$ donc $\delta \mid d$, $d$ satisfait donc 2.

Soit $d \in \mathbb{N}$ un entier qui satisfait 1. et 2.
Si $d = 0$, alors $a = b = 0$ donc $d = \text{PGCD}(a, b) = 0$.
Si $d \neq 0$, alors $d \mid a$ et $d \mid b$, le plus grand d'après 2.

**Corrolaire 15**

$$\forall (a,b) \in \mathbb{Z}^2 \quad \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b).$$

**Preuve :**

$\boxed{\supset}$ claire par transitivité.
$\boxed{\subset}$ Soit $\delta \in \mathcal{D}(a) \cap \mathcal{D}(b)$, on a établi qu'un diviseur commun divise le PGCD, donc $\delta \in \mathcal{D}(a \wedge b)$.

**Proposition 16**

$$\forall (a,b) \in \mathbb{Z}^2, \quad \mathrm{PGCD}(a,b) \cdot \mathrm{PPCM}(a,b) = |ab|.$$

**Preuve :**

On note $d = a \wedge b$ et $m = a \vee b$.
Puisque $d \mid a$ et $d \mid b$, $\exists (a',b') \in \mathbb{Z}^2 \mid a = da'$ et $b = db'$.
On a $da'b' = ab' = a'b$ donc $da'b'$ est multiple de $a$ et $b$, donc $m \mid da'b'$.
Donc $md \mid (da')(db')$ donc $md \mid ab$.

On a $\exists (u,v) \in \mathbb{Z}^2 \mid d = au + bv$ et $\exists (k,k') \mid m = ak = bk'$, donc $md = amu + bmv = ab(k'u + kv)$ donc $md \mid ab$.

Alors $ab$ et $md$ sont associés, $ab = \pm md$ donc $md = |ab|$.

# 2 Entiers premiers entre eux.

## 2.1 Couples d'entiers premiers entre eux.

**Définition 17**

On dit que deux entiers sont **premiers entre eux** si leur PGCD vaut 1.

**Proposition 18**

Deux entiers naturels non nuls $a$ et $b$ sont premiers entre eux si et seulement si $a \vee b = |ab|$.

**Proposition 19**

Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ et $d = a \wedge b$.
Si $a'$ et $b'$ sont les deux entiers relatifs tels que $a = da'$ et $b = db'$, alors $a' \wedge b' = 1$.

**Preuve :**

On a $\mathrm{PGCD}(a,b) = d$ donc $\mathrm{PGCD}(da', db') = d$ donc $d\mathrm{PGCD}(a',b') = d$ or $d \neq 0$ car $(a,b) \neq (0,0)$.
On retrouve bien que $\mathrm{PGCD}(a',b') = 1$.

**Théorème 20: de Bézout.**

$$\forall (a,b) \in \mathbb{Z}^2 \quad a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1.$$

**Preuve :**

$\boxed{\Longleftarrow}$ Supposons qu'il existe $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.
Notons $d := a \wedge b$, il divise $a$ et $b$ donc $au + bv$. Donc $d \mid 1$, c'est 1.

$\boxed{\Longrightarrow}$ Supposons que $a \wedge b = 1$, alors $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$ donc $1 \in a\mathbb{Z} + b\mathbb{Z}$ donc $\exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$.

**Corrolaire 21**

Soit $(a,b,c) \in \mathbb{Z}^3$.

1. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.
2. Plus généralement, si $a$ est premier avec chacun des $m$ entiers $b_1, ..., b_m$ ($m \in \mathbb{N}^*$), alors il est premier avec leur produit $b_1 ... b_m$.
3. Si $a \wedge b = 1$, alors pour tout $(n,p) \in \mathbb{N}^2$, $a^n \wedge b^p = 1$.

**Preuve :**

$\boxed{1.}$ Supposons $a \wedge b = 1$ et $a \wedge c = 1$.
D'après le théorème de Bézout, $\exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$ et $\exists (u',v') \in \mathbb{Z}^2 \mid au' + cv' = 1$.
Donc $(au + bv)(au' + cv') = 1$ donc $a(auu' + ucv' + bu'v) + bc(vv') = 1$ donc $a \wedge bc = 1$.

$\boxed{2.}$ Tout pareil.

$\boxed{3.}$ Supposons $a \wedge b = 1$ alors $a \wedge b^p = 1$ et $b^p \wedge a = 1$ donc $b^p \wedge a^n = 1$ (d'après 2, par récurrence).
Donc $a^n \wedge b^p = 1$.

## 2.2 Produit de diviseurs, diviseurs d'un produit.

**Proposition 22: Produit de diviseurs premiers entre eux.**

$$\forall (a_1, a_2, b) \in \mathbb{Z}^3 \quad \begin{cases} a_1 \mid b \text{ et } a_2 \mid b \\ a_1 \wedge a_2 = 1 \end{cases} \Longrightarrow a_1 a_2 \mid b.$$

**Preuve :**

Supposons que $a_1 \mid b$ et $a_2 \mid b$ et $a_1 \wedge a_2 = 1$.
Alors $|a_1 a_2| = a_1 \vee a_2$, or le PPCM divise tous les multiples communs, en particulier, $a_1 a_2 \mid b$.

**Théorème 23: Lemme de Gauss.**

$$\forall (a,b,c) \in \mathbb{Z}^3, \quad \begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c.$$

**Preuve :**

Supposons que $a \mid bc$ et $a \wedge b = 1$ donc $\exists k \in \mathbb{Z} \mid bc = ak$.
D'après le théorème de Bézout, $\exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$.
On a $c = acu + bcv = a(cu + kv)$ donc $a \mid c$.

**Exemple 24**

1. Soit $P = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$.
Montrer que si $\frac{p}{q}$ est racine de $P$ avec $p \wedge q = 1$, alors $p \mid a_0$ et $q \mid a_n$.

2. Factoriser $X^3 + 2X^2 - 4X - 3$ dans $\mathbb{R}[X]$.

**Solution :**

$\boxed{1.}$ On a $P(\frac{p}{q}) = 0$ donc $a_n \left(\frac{p}{q}\right)^n + ... + a_0 = 0$ donc $a_n p^n + ... + a_0 q^n = 0$.
Ainsi, $p(a_n^{n-1} + ... + a_1 q^{n-1}) = -a_0 q^n$ donc $p \mid a_0 q^n$ or $p \wedge q^n = 1$ donc $p \mid a_0$.
En factorisant par $q$, on obtient aussi que $q \mid a_n$.

$\boxed{2.}$ D'après 1, $p \mid 3$ et $q \mid 1$ donc les seuls candidats : $\frac{p}{q} \in \{-3, -1, 1, 3\}$.
On a alos $P = (X+3)(X^2 - X - 1) = (X+3)(X - \varphi)(X - \psi)$ où $\varphi = \frac{1+\sqrt{5}}{2}$ et $\psi = \frac{1-\sqrt{5}}{2}$.

### 2.3 Le cas des diviseurs premiers.

**Définition 25**

On appelle **nombre premier** tout entier $p$ supérieur à 2 dont les diviseurs sont $1, p, -1$ et $-p$.

**Proposition 26**

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

**Preuve :**

On l'avait fait par récurrence forte au premier semestre.

**Proposition 27**

Deux entiers relatifs sont premiers entre eux si et seulement si ils n'admettent aucun nombre premier comme diviseur commun.

**Preuve :**

$\boxed{\implies}$ Par contraposée, supposons qu'il existe $p$ premier tel que $p \mid a$ et $p \mid b$.
Puisque $p$ divise les deux, il divise le PGCD, or $p \geq 2$ donc le PGCD est différent de 1.

$\boxed{\impliedby}$ Par contraposée, supposons que $a$ et $b$ ne sont pas premiers entre-eux, alors $a \wedge b \geq 2$.
D'après la proposition précédente, le PGCD a un diviseur premier $p$, donc $p \mid a$ et $p \mid b$.

**Proposition 28**

Si $a$ est un entier et $p$ un nombre premier, alors $p \mid a$ ou $p$ est premier avec $a$.

**Preuve :**

Notons $d = p \wedge a$, il divise $p$, alors $d = p$ ou $d = 1$.
Mais si $d = p$, alors $p \mid a$, sinon si $d = 1$, $a \wedge p = 1$.

**Proposition 29**

Soit $(a,b) \in \mathbb{Z}^2$ et $p$ un nombre premier.

1. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.
2. Si $p$ divise un produit d'entiers, alors il divise l'un des facteurs.

**Preuve :**

$\boxed{1.}$ Supposons que $p \mid ab$.
Si $p \mid a$, on a fini. Sinon, $p \wedge a = 1$ d'après 28, donc $p \mid b$ d'après 23.

$\boxed{2.}$ Récurrence, trivial.

### 2.4 Extension à un nombre fini de vecteurs.

**Définition 30**

Soit $n \in \mathbb{N}^*$ et $(a_1, ..., a_n) \in \mathbb{Z}^n \setminus \{(0, ..., 0)\}$.
Le plus grand diviseur positif commun à $a_1, ..., a_n$ est appelé leur **PGCD** et noté:

$$a_1 \wedge ... \wedge a_n.$$

On convient que le PGCD de $n$ entiers nuls vaut 0.

**Proposition 31**

Soit $n \in \mathbb{N}^*$, $(a_1, ..., a_n) \in \mathbb{Z}^n$. Leur PGCD est l'unique entier positif $d$ tel que

$$a_1\mathbb{Z} + ... + a_n\mathbb{Z} = d\mathbb{Z}$$

En particulier,

$$\exists (u_1, ..., u_n) \in \mathbb{Z}^n \quad d = a_1u_1 + ... + a_nu_n.$$

**Proposition 32**

$$\forall (a_1, ..., a_n) \in \mathbb{Z}^n, \quad \forall k \in \mathbb{Z}, \quad \mathrm{PGCD}(ka_1, ..., ka_n) = |k| \cdot \mathrm{PGCD}(a_1, ..., a_n).$$

**Proposition 33**

Soit $n \in \mathbb{N}^*$ et $a_1, ..., a_{n+1}$ des entiers relatifs. Alors,

$$a_1 \wedge ... \wedge a_n \wedge a_{n+1} = (a_1 \wedge ... \wedge a_n) \wedge a_{n+1}$$

**Preuve :**

Notons $d_n = a_1 \wedge ... \wedge a_n$, $d_{n+1} = a_1 \wedge ... \wedge a_n \wedge a_{n+1}$ et $d'_{n+1} = d_n \wedge a_{n+1}$.
D'une part, d'après la proposition précédente:

$$a_1\mathbb{Z} + ... + a_n\mathbb{Z} + a_{n+1}\mathbb{Z} = d_{n+1}\mathbb{Z}.$$

D'autre part,

$$\begin{aligned} a_1\mathbb{Z} + ... + a_n\mathbb{Z} + a_{n+1}\mathbb{Z} &= (a_1\mathbb{Z} + ... + a_n\mathbb{Z}) + a_{n+1}\mathbb{Z} \\ &= d_n\mathbb{Z} + a_{n+1}\mathbb{Z} \\ &= (d_n \wedge a_{n+1})\mathbb{Z} \\ &= d'_{n+1}\mathbb{Z}. \end{aligned}$$

Ceci amène que $d_{n+1}$ et $d'_{n+1}$ sont associés et donc égaux par positivité.

**Proposition 34**

Soit $n \in \mathbb{N}^*$, $(a_1, ..., a_n) \in \mathbb{Z}^n$ et $d$ leur PGCD, on a

$$\bigcap_{k=1}^{n} \mathcal{D}(a_k) = \mathcal{D}(d).$$

**Définition 35**

Des entiers relatifs $a_1, ..., a_n$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD est égal à 1, ou de manière équivalente si 1 et $-1$ sont les seuls diviseurs communs.

Ils sont **deux à deux premiers entre eux** si

$$\forall (i, j) \in [\![1, n]\!]^2, \ i \neq j \Longrightarrow a_i \wedge a_j = 1.$$

**Exemple 36**

Justifier que si $n$ entiers ($n \geq 2$) sont premiers entre eux deux-à-deux, ils le sont dans leur ensemble.

Les entiers 6, 10 et 15 sont premiers entre-eux dans leur ensemble, mais pas deux-à-deux.

**Solution :**

Soit $a_1, ..., a_n \in \mathbb{Z}^n$ premiers entre-eux deux-à-deux.
Soit $d = a_1 \wedge ... \wedge a_n$, alors $d \mid a_1$ et $d \mid a_2$ : il divise $a_1 \wedge a_2 = 1$ donc $d = 1$.

**Théorème 37**

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

$a_1, ..., a_n$ sont premiers entre eux dans leur ensemble $\iff \exists (u_1, ..., u_n) \in \mathbb{Z}^n \quad \sum_{i=1}^n a_i u_i = 1$.

**Proposition 38**

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

Si tous les $a_i$ divisent $b$, et si les $a_i$ sont deux-à-deux premiers entre eux, alors $a_1 ... a_n$ divise $b$.

**Preuve :**

Supposons que $a_1, ..., a_n$ divisent $b$ et sont deux-à-deux premiers entre eux.
Alors, $a_1 \mid b$, $a_2 \mid b$, et $a_1 \wedge a_2 = 1$ donc $a_1 a_2 \mid b$.
De plus, $a_1 a_2 \mid b$ et $a_3 \mid b$ et $a_1 a_2 \wedge a_3 = 1$ donc $a_1 a_2 a_3 \mid b$.
En itérant, on obtient le résultat.

# 3 Théorème fondamental de l'arithmétique et applications.

## 3.1 Le TFAr.

**Théorème 39: Théorème fondamental de l'arithmétique.**

Soit $n$ un entier supérieur à 2. Il existe un entier naturel $r$ non nul et $r$ nombres premiers $p_1 < ... < p_r$, ainsi que des entiers naturels non nuls $\alpha_1, ..., \alpha_r$ tels que

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

Cette décomposition de $n$ en facteurs premiers est unique.

**Preuve :**

**Existence:**
Si $n$ est premier c'est bon. Sinon, $\exists n_1, n_2 \in [\![2, n]\!] \mid n = n_1 n_2$.
Il faut raisonner sur $n_1$ et $n_2$ et les décomposer par récurrence forte.

**Unicité:** On considère deux décompositions $n = p_1^{\alpha_1} ... p_r^{\alpha_r} = q_1^{\beta_1} ... q_s^{\beta_s}$ où $r, s \in \mathbb{N}^*$ et les $p_i, q_i$ sont premiers.
On suppose les $p_i$ et $q_i$ distincts deux-à-deux.

Montrons que $\{p_1, ..., p_r\} = \{q_1, ..., q_s\}$. Pour $i \in [\![1, r]\!]$, on a que $p_i$ divise $q_1^{\beta_1} ... q_s^{\beta_s}$.
D'après le lemme d'euclide, $\exists j \in [\![1, s]\!] \mid p_i \mid q_j$ donc $p_j = q_j$ car ils sont tous les deux premiers.
On a donc $\{p_1, ..., p_r\} \subset \{q_1, ..., q_s\}$. On a l'autre inclusion de la même manière.
Finalement, $\{p_1, ..., p_r\} = \{q_1, ..., q_s\}$, donc $r = s$ par égalité de cardinaux.

On a $n = p_1^{\alpha_1} ... p_r^{\alpha_r} = p_1^{\beta_1} ... p_r^{\beta_r}$. Montrons que pour $i \in [\![1, r]\!]$, on a $\alpha_i = \beta_i$.
Supposons que $\alpha_i < \beta_i$ SPDG. Alors:

$$p_i^{\alpha_i} \prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i} \prod_{j \neq i} p_j^{\beta_j}.$$

Puisque $\mathbb{Z}$ est intègre et que $p_i^{\alpha_i} \neq 0$, on a:

$$\prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i - \alpha_i} \prod_{j \neq i} p_j^{\beta_j}.$$

Donc $p_i \mid \prod_{j \neq i} p_j^{\alpha_j}$, donc $p_i$ divise l'un des $p_j$ pour $j \neq i$, ce qui est absurde.
On a donc $\alpha_i = \beta_i$.