# $\boxed{\mathbb{Z}}$

<u>Motivation</u> $(\mathbb{N}, +)$ "n'est pas un groupe" : il existe des naturels qui n'ont pas d'opposé

<u>Solution</u> On "ajoute les opposés" des naturels strictement positifs et on prolonge canoniquement $+, \cdot, \leq$

<u>Coût</u> La divisibilité sur $\mathbb{Z}$ est seulement un préordre.

## I Structure

### 1 Structure algébrique

$\mathbb{Z} = \mathbb{N} \cup \{-n,\ n \in \mathbb{N}^*\}$ où $-n$ est une construction syntaxique.

Pour $a \leq b$ dans $\mathbb{N}$, on note

- $a+b$ la somme de $a$ et $b$ dans $\mathbb{N}$
- $(-a)+b$ est l'unique $c \in \mathbb{N}$ tq $a+c=b$
- $a+(-b) = -((-a)+b)$
- $(-a)+(-b) = -(a+b)$

$$\left.\begin{array}{l} \cdot\ b+(-a) = (-a)+b \\ \cdot\ (-b)+a = a+(-b) \\ \cdot\ (-b)+(-a) = (-a)+(-b) \\ \cdot\ b+a = a+b \end{array}\right\} \text{on complète pour que } + \text{ soit commutative.}$$

**thm** $(\mathbb{Z}, +)$ est un groupe commutatif.

i.e.

1 $+$ a un élément neutre : $0$ — $(\mathbb{Z}, +)$ est un groupe

$\forall a \in \mathbb{Z},\ a+0=a$

2 Tout élément $a \in \mathbb{Z}$ a un symétrique par $+$ : $-a$

$\forall a \in \mathbb{Z},\ a+(-a)=0$

3 $+$ est associative

$\forall a,b,c \in \mathbb{Z},\ a+(b+c)=(a+b)+c$

4 $+$ est commutative

$\forall a,b \in \mathbb{Z},\ a+b=b+a$

De même, on définit la multiplication de la seule façon possible pour que le théorème suivant soit vrai

**thm** $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif

i.e.

1 $(\mathbb{Z}, +)$ est un groupe — $(\mathbb{Z}, +, \cdot)$ est un anneau

2 $\cdot$ a un élément neutre : $1$

$\forall a \in \mathbb{Z},\ a\cdot 1=a$

3 $\cdot$ est associative

4 $\cdot$ est distributive sur $+$

$$\forall a,b,c \in \mathbb{Z},\ \begin{cases} a\cdot(b+c)=a\cdot b+a\cdot c \\ (a+b)\cdot c=a\cdot c+b\cdot c \end{cases}$$

5 $\cdot$ est commutative

## 2 Ordre standard

On prolonge l'ordre standard $\leqslant$ de $\mathbb{N}$ à $\mathbb{Z}$ de la seule façon qui rende vraie :

<u>thm</u> $(\mathbb{Z}, +, \cdot, \leqslant)$ est un anneau ordonné

i.e.

1 $(\mathbb{Z}, +, \cdot)$ est un anneau

2 On peut additionner des inégalités

$$\forall a,b,c,d \in \mathbb{Z}, \quad \begin{cases} a \leqslant b \\ c \leqslant d \end{cases} \Rightarrow a+c \leqslant b+d$$

3 On peut multiplier une inégalité par un positif

$$\forall a,b,c \in \mathbb{Z}, \quad \begin{cases} a \leq b \\ 0 \leq c \end{cases} \Rightarrow a \cdot c \leq b\ c$$

⚠ On ne peut pas <u>soustraire</u> ou <u>multiplier</u> brutalement des inégalités

<u>eg</u> $\begin{cases} -3 \leq -2 \\ -3 \leq 2 \end{cases}$ mais $9 > -4$

$\begin{cases} -3 \leq -2 \\ -3 \leq 2 \end{cases}$ mais $0 > -4$

**thm** Propriété fondamentale de $\mathbb{Z}$

1. Toute partie non vide et minorée de $\mathbb{Z}$ a un plus petit élément
2. ........................ et majorée ..................grand......

## 3 Divisibilité

**def** *Rappel*

Soient $a, b \in \mathbb{Z}$.

$$a \mid b \iff \exists k \in \mathbb{Z},\ b = ka$$

On dit a divise b ou b est un multiple de a

**notatn** Ensembles

1. $D(n)$ l'ensemble des diviseurs de $n$
2. $D_+(n)$ .................. positifs ...
3. $n\mathbb{Z}$ ............... multiples de $n$
4. $|n|\mathbb{Z}_+$ .................. positifs de $n$

⚠ 0 divise 0 ce qui ne signifie pas qu'on peut diviser par 0
« On peut diviser a par b » ssi $\exists!\, k \in \mathbb{Z},\ b = ak$

**prop** *Rappel*

$\mid$ est un préordre sur $\mathbb{Z}$ et même un ordre si on le restreint à $\mathbb{N}$

**thm** Propriétés algébriques de |

1 | est stable par combinaison linéaire

$\forall a, b, c, \lambda, \mu \in \mathbb{Z}, \begin{cases} a \mid b \\ a \mid c \end{cases} \Rightarrow a \mid \lambda b + \mu c$

2 | est stable par produit

$\forall a, b, c, d \in \mathbb{Z}, \begin{cases} a \mid b \\ c \mid d \end{cases} \Rightarrow ac \mid bd$

3 | est stable par puissances

$\forall a, b \in \mathbb{Z}, \forall n \in \mathbb{N}, a \mid b \Rightarrow a^n \mid b^n$

**dem** Propriétés algébriques de |

1 Soient $a, b, \lambda, \mu, c \in \mathbb{Z}$

Supposons $\begin{cases} \lambda b = \lambda k a & \text{pour un certain } k \in \mathbb{Z} \\ \mu c = \mu k' a & \dots\dots\dots\dots\dots\dots \ k' \in \mathbb{Z} \end{cases}$

$\lambda b + \mu c = a(\lambda k + \mu k')$

Posons $K = \lambda k + \mu k' \in \mathbb{Z}$

$\lambda b + \mu c = aK \Rightarrow a \mid \lambda b + \mu c$

2 Soient $a, b, c, d \in \mathbb{Z}$

Supposons $\begin{cases} a \mid b \Leftrightarrow \text{il existe } k \in \mathbb{Z}_* \text{ tq } a \cdot k = b \\ c \mid d \Leftrightarrow \dots\dots\dots \ k' \in \mathbb{Z} \text{ tq } c \cdot k' = d \end{cases}$

On a $b \cdot d = (a \cdot k) \cdot (c \cdot k')$

$\Leftrightarrow (a \cdot c) \cdot (k \cdot k') = b \cdot d$

Or $k \cdot k' \in \mathbb{Z} \Rightarrow ac \mid bd$

3 Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$

Supposons, pour $k \in \mathbb{Z}$, $b = ka$

Donc $b^n = (ka)^n$

$\Leftrightarrow b^n = k^n a^n$

$\Leftrightarrow b^n = Ka \qquad K \overset{\text{déf}}{=} k^n \in \mathbb{Z}$

Donc $a^n | b^n$

<u>thm</u> de division euclidienne dans $\mathbb{Z}$

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*, \ \exists! (q,r) \in \mathbb{Z}^2, \ \begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$$

⚠ Il y a des variantes pour la condition sur le reste

- On peut demander $-\frac{b}{2} < r \leqslant \frac{b}{2}$
- On peut demander $\begin{cases} |r| < |b| \\ \operatorname{sgn} r = \operatorname{sgn} b \end{cases}$ : <u>PYTHON</u> fait ça !

<u>dem</u> de la division euclidienne dans $\mathbb{Z}$

Unicité

$\rightarrow$ même preuve que dans $\mathbb{N}$

3 Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$

Supposons, pour $k \in \mathbb{Z}$, $b = ka$

Donc $b^n = (ka)^n$

$\Leftrightarrow b^n = k^n a^n$

$\Leftrightarrow b^n = Ka \qquad K \overset{\text{def}}{=} k^n \in \mathbb{Z}$

Donc $a^n | b^n$

thm de division euclidienne dans $\mathbb{Z}$

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*, \ \exists! \ (q,r) \in \mathbb{Z}^2, \ \begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$$

⚠ Il y a des variantes pour la condition sur le reste

- On peut demander $-\frac{b}{2} < r \leqslant \frac{b}{2}$
- On peut demander $\begin{cases} |r| < |b| \\ \operatorname{sgn} r = \operatorname{sgn} b \end{cases}$ : PYTHON fait ça !

dem de la division euclidienne dans $\mathbb{Z}$

Unicité

$\rightarrow$ même preuve que dans $\mathbb{N}$

<u>dem</u>

<u>Existence</u>

Traitons 4 cas.

<u>1er cas</u> ($a \geqslant 0$ et $b > 0$) : cf cours sur $\mathbb{N}$

<u>2e cas</u> ($a < 0$ et $b > 0$) :

On effectue dans $\mathbb{N}$ la div. euclid. <u>dans $\mathbb{N}$</u> de $-a$ par $b$

il existe $(p', q') \in \mathbb{N}^2$ tq $-a = bq' + r'$

$$\cdot(-1) \Rightarrow a = b(-q') + (-r')$$

Si $r' = 0$, on pose $\begin{cases} q = -q' \\ r = -r' = 0 \end{cases}$

Sinon $0 < r' < b$ mais

$$a = b(-q'-1) + \underbrace{b - r'}_{0< \quad <b} \qquad \text{on a ajouté } -b+b$$

donc on pose $\begin{cases} p = -q' - 1 \\ r = b - r' \end{cases}$

<u>3e cas</u> ($a \geqslant 0$ et $b < 0$) :

On effectue <u>dans $\mathbb{N}$</u> la div. euclid. de $a$ par $-b$

il existe $(q', r') \in \mathbb{N}^2$ tq $a = -bq' + r'$

$$u = (-b)q' + r' = -q' \cdot b + r'$$

avec $0 < r' < -b = |b|$

On pose $\begin{cases} q = -q' \\ r = r' \end{cases}$

<u>$4^e$ cas</u> ($a<0$ et $b<0$):

On fait la div. euclid. de $-a$ par $-b$ <u>dans $\mathbb{N}$</u>.
Alors il existe $(q', r') \in \mathbb{N}^2$ tq

$$-a = -bq' + r'$$
$$\Leftrightarrow \quad a = bq' - r'$$

Si $r' = 0$:

$0 \leq r' < |b|$ si $r' = 0$, on pose $\begin{cases} q = q' \\ r = r' = 0 \end{cases}$

Sinon:

$a = b(q'+1) - b - r'$ On pose $\begin{cases} q = q'+1 \\ r = -b - r' \end{cases}$

<u>thm</u> Lien div. euclid $\Leftrightarrow$ divisibilité

Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ Alors

$$b|a \Leftrightarrow rem(a,b) = 0$$

<u>dem</u>

Notons $a = bq + r$ la div euclid de $a$ par $b$

$\boxed{\Leftarrow}$ si $ren(a,b) = r = 0$, alors $a = bq \Leftrightarrow b|a$

$\boxed{\Rightarrow}$ Supp $b|a$ Ainsi il existe $k \in \mathbb{Z}$ tq $a = bk \Rightarrow a = bk + 0$

# 5 Congruences dans $\mathbb{Z}$

**def** *Rappel*

Soit $n \in \mathbb{Z}$. La relation de congruence modulo n est $\cdot \equiv \cdot\cdot [n]$

$$a \equiv b\,[n] \overset{def}{\iff} \exists k \in \mathbb{Z},\ a = bk + n$$

$$\iff n \mid a - b$$

**coroll**

Soit $n \in \mathbb{Z}^*$.

$$a \equiv b\,[n] \iff \text{rem}(a, n) = \text{rem}(b, n)$$

**dem** Notons $\begin{cases} a = nq + r \\ b = nq' + r' \end{cases}$ les DE de a et b par n

$\Leftarrow$ : Supp $r = r'$.

$$a - b = n(q - q') + \underbrace{r - r'}_{0}$$

$$= n \underbrace{(q - q')}_{\in \mathbb{Z}}$$

$\Rightarrow n \mid a - b$ ie $a \equiv b\,[n]$

$\Rightarrow$ : Supp $a \equiv b\,[n]$

Ainsi il existe $k \in \mathbb{Z}$ tq $a = bk + n$

Or $b = nq' + r'$

Donc $a = n(q' + k) + r'$

par unicité de la DE, $\begin{cases} q = q' + k \\ r = r' \end{cases} \Rightarrow r = r'$

**thm**

Pour tout $n \in \mathbb{N}$, $\cdot \equiv \cdot\cdot [n]$ est une relation d'équivalence.

**dem**

Déjà vu (vrai pour $\cdot \equiv \cdot\cdot [t]$ avec $t \in \mathbb{R}$ (et $\mathbb{Z} \subset \mathbb{R}$))

**thm** propriétés algébriques de la congruence.

1 Stable par somme

$\forall a,b,c,d \in \mathbb{Z},\ \begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Rightarrow a+c \equiv b+d\ [n]$

2 Stable par produit

$\begin{cases} \forall k \in \mathbb{Z}^*, \forall a,b \in \mathbb{Z},\ a \equiv b\ [n] \Leftrightarrow ka \equiv kb\ [kn] \\ \forall a,b,c,d \in \mathbb{Z},\ \begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Rightarrow ac \equiv bd\ [n] \end{cases}$

3 Stable par puissance

$\forall p \in \mathbb{N}, \forall a,b \in \mathbb{Z},\quad a \equiv b\ [n] \Rightarrow a^p \equiv b^p\ [n]$

<u>dem</u>

1 Déjà vu (vrai dans $\mathbb{R}$)

2 Déjà vu (vrai dans $\mathbb{R}$)

Soient $a,b,c,d \in \mathbb{Z}$ tels que $\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases}$

Il existe $\begin{cases} k \in \mathbb{Z} \text{ tq } a = b + kn \\ k' \in \mathbb{Z} \text{ tq } c = d + k'n \end{cases}$

$$ac = (b+kn)(d+k'n) = bd + bk'n + dkn + kk'n^2$$
$$= bd + n\underbrace{(bk' + dk + kk'n)}_{\in \mathbb{Z}}$$

$$\Rightarrow ac \equiv bd\ [n]$$

3 Par récurrence ~~immédiate~~

On veut mtq $\forall a,b \in \mathbb{Z},\ a \equiv b\ [n] \Rightarrow \forall p \in \mathbb{N},\ a^p \equiv b^p\ [n]$

Soient $a,b \in \mathbb{Z}$ et supp $a \equiv b\ [n]$. Mt par récurrence $\forall p \in \mathbb{N}, a^p \equiv b^p\ [n]$

<u>init</u> $a^0 = 1 \equiv 1 = b^0\ [n]$

<u>her</u> Soit $p \in \mathbb{N}$ Supp $a^p \equiv b^p\ [n]$. On sq $a \equiv b\ [n]$. Par stab. par produit.
$a^{p+1} \equiv b^{p+1}\ [n]$ d'où l'her.

**app** Critère de divisibilité par 9

Soit $n \in \mathbb{N}$.

Notons $n = \overline{a_r \cdots a_2 a_1 a_0}^{10}$ (nombre aux chiffres $a_r, \ldots, a_2, a_1, a_0$)

On veut mtq $9 | n \iff 9 | \sum_{i=0}^{n} a_i$

Montrons plus généralement

$n = \sum_{i=0}^{n} a_i \ [9]$

(En effet, cela implique qu'ils ont le même reste dans la ⊢ par 9 et donc en particulier que le reste de l'un des deux est nul ssi le reste l'est aussi)

On a $n = \overline{a_r \cdots a_2 a_1 a_0}^{10}$ ie $n = a_r 10^r + \cdots + a_2 10^2 + a_1 10 + a_0$

On a $10 \equiv 1 \ [9]$. Par stab. de la puissance, $\forall i$, $10^i \equiv 1 \ [9]$

du produit, $\forall i$, $a_i 10^i \equiv a_i \ [9]$

de la somme, $n = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \ [9]$

## 6 Anneau $\mathbb{Z}/n\mathbb{Z}$

**idée** on change l'égalité : On fait comme si deux entiers modulo n étaient égaux

**notatn** $\mathbb{Z}/n\mathbb{Z}$

Ensemble des classes d'équivalences de la congruence modulo n

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

où $\begin{cases} \overline{0} = n\mathbb{Z} & = \overline{n} & = \cdots \\ \overline{1} = n\mathbb{Z} + 1 & = \overline{n+1} & = \cdots \\ \vdots & \vdots & \vdots \\ \overline{n-1} = n\mathbb{Z} + (n-1) & = \overline{2n-1} & = \cdots \end{cases}$

**def** Addition et multiplication sur $\mathbb{Z}/n\mathbb{Z}$

$$+ \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) \mapsto \overline{a+b} \end{cases} ; \quad \times \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) \mapsto \overline{a \times b} \end{cases}$$

**prop** $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ sont bien définies

**dem** On veut mtq $\forall a, b, c, d \in \mathbb{Z}$, $\begin{cases} \overline{a} = \overline{c} \\ \overline{b} = \overline{d} \end{cases} \Rightarrow \begin{cases} \overline{a+b} = \overline{c+d} \\ \overline{a \times b} = \overline{c \times d} \end{cases}$

On a $\begin{cases} \overline{a} = \overline{c} \\ \overline{b} = \overline{d} \end{cases} \underset{1}{\iff} \begin{cases} a \equiv c \ [n] \\ b \equiv d \ [n] \end{cases} \underset{2}{\Rightarrow} \begin{cases} a+b \equiv c+d \ [n] \\ a \times b \equiv c \times d \ [n] \end{cases} \underset{1}{\Rightarrow} \begin{cases} \overline{a+b} = \overline{c+d} \\ \overline{a \times b} = \overline{c \times d} \end{cases}$

rappel cela signifie

1 $(\mathbb{Z}/n\mathbb{Z}, +)$ forme un groupe abélien

- $+$ a un élément neutre
- $+$ est associative
- $+$ est commutative
- Tout les elt $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ a un sym. par $+$ $\overline{-a}$

2 $\times$ a un élément neutre $\overline{1}$

3 $\times$ est associative

4 $\times$ est distributive sur $+$

5 $\times$ est commutative

dem

# TRIVIAL

dem. eg distributivité

Soient $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$.

$$\begin{aligned}
\overline{a} \times (\overline{b} + \overline{c}) &= \overline{a} \times \overline{b+c} && \text{par déf} \\
&= \overline{a \times (b+c)} && \text{par déf} \\
&= \overline{ab + ac} && \text{par distrib de } \times \text{ sur } + \text{ dans } \mathbb{Z} \\
&= \overline{ab} + \overline{ac} && \text{par déf} \\
&= \overline{a} \times \overline{b} + \overline{a} \times \overline{c}
\end{aligned}$$

# II Nombres premiers

## 1 Définition et 1ères propriétés

def Rappel

Un nombre premier est un entier positif $p$ ayant exactement 2 diviseurs positifs : $1$ et $p$

eg

- $0$ n'est pas premier : il a $\infty$ diviseurs positifs
- $1$ n'est pas premier : il a $1$ diviseur positif
- $2$ est premier
- $3$ est premier
- $4$ n'est pas premier : il a $\{1, 2, 4\}$

notatn Ensemble des nombres premier : $\mathbb{P}$

prop Reformulation de la déf : Soit $p \in [\![2, +\infty[\![$

1 $p \in \mathbb{P} \Leftrightarrow \forall u, v \in \mathbb{Z},\ p = uv \Rightarrow |u| = 1 \text{ ou } |v| = 1$ $\quad p \in \mathbb{P}$ ssi $p$ irréductible

2 $p \in \mathbb{P} \Leftrightarrow \forall d \in [\![2, \lfloor\sqrt{p}\rfloor]\!],\ d \nmid p$ [1]

[1] Ne divise pas.

dem

1 $\boxed{\Rightarrow}$ Supp $p \in \mathbb{P}$ ie $D_+(p) = \{1, p\}$. Soient $u, v \in \mathbb{Z}$ et supp $p = uv$. Alors $u | p \Rightarrow |u| | p$

donc $|u| \in \{1, p\} \Rightarrow |u| = 1$ ou $|u| = p$ ie $|u| = 1$ ou $|v| = \frac{p}{|u|} = 1$

$\boxed{\Leftarrow}$ Supp $\forall u, v \in \mathbb{Z},\ p = u \cdot v \Rightarrow |u| = 1$ ou $|v| = 1$. Mq $D_+(p) \subset \{1, p\}$. Soit $d \in D_+(p)$

ie $d \geq 0$ et $d | p$ ie il existe $k \in \mathbb{Z} / p = kd$. D'ap l'hyp. $|k| = 1$ ou $|d| = 1$

ie $\left|\frac{p}{d}\right| = 1$ ou $|d| = 1$ ie $\frac{p}{d} = 1$ ou $d = 1$ ie $d = p$ ou $d = 1$ ie $d \in \{1, p\}$

2 $\boxed{\Rightarrow}$ Supp $p \in \mathbb{P}$ ie $D_+(p) = \{1, p\}$. Soit $d \in [\![2, \lfloor\sqrt{2}\rfloor]\!]$

En particulier $1 < 2 \leq d \leq \sqrt{p} < p$

Donc $d \notin \{1, p\}$ ie. $d \notin D_+(p)$

$\boxed{\Leftarrow}$ Par contraposition. Supp $p \notin \mathbb{P}$

Ainsi il existe un diviseur $k \geq 0$ de $p$ / $k \notin \{1, p\}$

Traitons deux cas :

<u>1er cas</u> ($k \leq \sqrt{p}$):

Posons $d = k$

On a $d \in [\![2, \lfloor\sqrt{p}\rfloor]\!]$ et $d | p$

<u>2e cas</u> ($k > \sqrt{p}$):

On a $p = k \underbrace{\frac{d}{k}}_{\in \mathbb{N}}$

Posons $d = \frac{p}{k}$

On a $k > \sqrt{p} \Rightarrow \underbrace{\frac{p}{k}}_{d} < \frac{p}{\sqrt{p}} = \sqrt{p}$

On a donc $d \in [\![2, \lfloor\sqrt{p}\rfloor]\!]$ et $d | p$

<u>lemme</u> Soit $n \in [\![2, +\infty[\![$. Alors $n$ a un diviseur premier

<u>dem</u> Déjà vu ("lemme 2" de $\mathbb{N}$)

<u>thm</u> (Fondamental de la cryptomonnaie)

$\# \mathbb{P} = +\infty$

<u>dem</u> cf. TD "Rédaction"

<u>coroll</u> (du lemme). Eratostène

$p \in \mathbb{P} \Leftrightarrow \forall d \in [\![2, \lfloor\sqrt{p}\rfloor]\!] \cap \mathbb{P}, \ d \nmid p$

<u>app</u> $101 \in \mathbb{P}$

$\lfloor\sqrt{101}\rfloor = 10$. Nombres premiers $\leqslant 10$ : $\{2, 3, 5, 7\}$

$$\begin{cases} 101 \equiv 1 \ [2] \Rightarrow 2 \nmid 101 \\ 101 \equiv 2 \ [3] \Rightarrow 3 \nmid 101 \\ 101 \equiv 1 \ [5] \Rightarrow 5 \nmid 101 \\ 101 \equiv 3 \ [7] \Rightarrow 7 \nmid 101 \end{cases} \Leftrightarrow 101 \in \mathbb{P}$$

• $103 \in \mathbb{P}$

$$\begin{cases} 103 \equiv 1 \ [2] \Rightarrow 2 \nmid 103 \\ 103 \equiv 1 \ [3] \Rightarrow 3 \nmid 103 \\ 103 \equiv 3 \ [5] \Rightarrow 5 \nmid 103 \\ 103 \equiv 5 \ [7] \Rightarrow 7 \nmid 103 \end{cases} \Leftrightarrow 103 \in \mathbb{P}$$

dem

1 Existence Mq tout entier $n \geq 1$ a une DFP[1] par récurrence forte

Hérédité forte Soit $n \in \mathbb{N}^*$ et supposons que tt $k \in [\![1, n[\![$ on une DFP

Traitons deux cas

deux cas $n = 1 \Rightarrow$ prod $\emptyset$ ; $n \geq 2 \Rightarrow$ leme 2

1er cas ($n = 1$):

$n = \prod_{\emptyset}$ est une DFP

2e cas ($n \geq 2$):

Donc $n$ a un diviseur premier $p$ et $p \in [\![1, n[\![$

donc par hdrf $\frac{n}{p}$ a une DFP

On note $\frac{n}{p} = p_1 p_2 \cdots p_r$

où les $p_i$ sont premiers on a

$n = p p_1 p_2 \cdots p_r$ qui est une DFP

Unicité preuve de Zermello par l'absurde.

On supp qu'il existe un entier $n \geq 1$ ayant au moins deux DFPs

{ d'après la ppte du bon ordre, il existe un plus petit entier $N$ ayant au moins deux DFP

remq Si $k_1, k_2 \in \mathbb{N}$, $k_1 k_2 < N \Rightarrow$

- $k_1$ a une unique DFP
- $k_2$ - - - - - - - - -

- $k_1 k_2$ a une unique DFP, c'est la concaténation de $k_1$ et $k_2$ (par unicité)

[1] Décomposition en facteurs premiers

Notons $\begin{cases} N = pP \\ N = qQ \end{cases}$ où $\begin{cases} p \neq q \\ P = p_1 p_2 \cdots p_r \\ Q = q_1 q_2 \cdots q_r \end{cases}$ est un produit de fact. premiers

À renommage près, on peut supposer $p < q$

On a $p \notin \{q_1, \dots, q_s\}$ sinon $\frac{N}{p}$ aurait deux DFP

Notons $K = N - pQ \geq 1$
On a $(p-q) Q = K = p(P-Q)$.

D'après la remq, $K$ a une unique DFP obtenue par concaténations de la DFP de $p-q$ et $q_1 q_2 \cdots q_s$ et également obtenue par concat. de $P-Q$ et $p$

Donc $p$ apparaît dans la DFP de $q-p$ donc $p | q-p$
Or $p | p$ donc par stabilité de $|$ par somme

$$p | (q-p) + p = q \quad \text{or} \quad D_+(q) = \{1, q\}$$

donc $p = q$ Imp!

## 2 Facile en utilisant $\boxed{1}$

## 3 Valuations $p$-adiques

**prop-def**

Soit $p \in \mathbb{P}$ et $n \in \mathbb{Z}^*$
Alors il existe un plus grand entier $\alpha$ tq $p^\alpha | n$.
Cet entier est appelé valuation $p$-adique noté $V_p(n)$

**dem**

$\mathcal{A} = \{\alpha \in \mathbb{N},\ p^\alpha | n\}$ et

$\begin{cases} \mathcal{A} \neq \emptyset & \text{car } 0 \in \mathcal{A} \\ \mathcal{A} \text{ majoré} & \text{car } n \neq 0 \end{cases}$

**eg**

- $n = 100$ : $n = 2^2 \cdot 5^2$

$v_2(100) = 2$ car $2^2 | 100$ mais $2^3 \nmid 100$

$v_3(100) = 0$ car $3^1 \nmid 100$

$v_5(100) = 2$ car $5^2 | 100$ mais $5^3 \nmid 100$

- $n = 360$

$n = 3^3 \cdot 3^2 \cdot 5$

$v_2(360) = 3$ ; $v_3(360) = 2$, $v_5(360) = 1$

**remq** Reformulation de la déf.

$v_p(n)$ est l'exposant de $p$ dans la DFP de $n$

**remq** Reformulation du TFAr

Soit $n \in \mathbb{Z}^*$

Alors $n = \operatorname{sgn}(n) \prod_{p \in \mathbb{P}} p^{v_p(n)}$

**thm**

Soient $a, b \in \mathbb{Z}^*$

1. $a | b \Leftrightarrow \forall p \in \mathbb{P},\ v_p(a) \leq v_p(b)$
2. $\forall p \in \mathbb{P},\ v_p(ab) = v_p(a) + v_p(b)$

3 $\forall p \in \mathbb{P}, \forall n \in \mathbb{N}, v_p(a^n) = n\, v_p(a)$

4 $a+b \neq 0 \Rightarrow \forall p \in \mathbb{P}, v_p(a+b) \geqslant \max\{v_p(a), v_p(b)\}$

dem

1 $\boxed{\Rightarrow}$ Supp $a|b$. Soit $p \in \mathbb{P}$

$v_p(a)$ est tq $p^{v_p(a)} \mid a$

par Ⓣ de $|$ sur $\mathbb{Z}$, $p^{v_p(a)} \mid p$

par définition $v_p(b) \geqslant v_p(a)$

$\boxed{\Leftarrow}$ Supp $\forall p \in \mathbb{P}, v_p(a) \leqslant v_p(a)$

$$|b| = \prod_{p \in \mathbb{P}} p^{v_p(b)} = \prod_{p \in \mathbb{P}} p^{\overbrace{v_p(b) - v_p(a)}^{\geqslant 0} + v_p(a)}$$

$$= \underbrace{\left(\prod_{p \in \mathbb{P}} p^{v_p(b) - v_p(a)}\right)}_{\in \mathbb{N}} \cdot \underbrace{\left(\prod_{p \in \mathbb{P}} p^{v_p(a)}\right)}_{|a|}$$

$$\Rightarrow |a| \mid |b|$$

$$\Rightarrow a \mid b$$

2 Soit $p \in \mathbb{P}$

$$|a| = \prod_{p \in \mathbb{P}} p^{v_p(a)} \ ; \ |b| = \prod_{p \in \mathbb{P}} p^{v_p(b)}$$

$$|ab| = \prod_{p \in \mathbb{P}} p^{v_p(a) + v_p(b)} \Rightarrow v_p(a) + v_p(b) = v_p(ab)$$

par unicité de la DFP

3 Par récurrence immédiate #Couprie

4 Soit $p \in \mathbb{P}$

$$\begin{cases} a = p^{\nu_p(a)} P & \text{où } p \nmid P \\ b = p^{\nu_p(b)} Q & \text{où } p \nmid Q \end{cases}$$

À renommage près, $\nu_p(a) \leqslant \nu_p(b)$

$$a+b = p^{\nu_p(a)} (\underbrace{P + p^{\nu_p(b)-\nu_p(a)} Q}_{\in \mathbb{N}})$$

app

- Soient $a, b \geqslant 1$ tq
  $a \mid b^2 \mid a^3 \mid b^4 \mid a^5 \mid b^6 \mid \dots$

Mtq $a = b$

Soit $p \in \mathbb{P}$. On a $\forall n \in \mathbb{N}$, $\begin{cases} a^{2n+1} \mid b^{2n+2} \\ b^{2n} \mid a^{2n+1} \end{cases}$

Donc $\forall n \in \mathbb{N}$, $\begin{cases} (2n+1)\nu_p(a) \leqslant (2n+2)\nu_p(b) \\ 2n\,\nu_p(b) \leqslant (2n+1)\nu_p(a) \end{cases}$

$\Rightarrow \forall n \in \mathbb{N}$, $\dfrac{2n\,\nu_p(b)}{2n+1} \leqslant \nu_p(a) \leqslant \dfrac{(2n+2)\nu_p(b)}{2n+1}$

Les inégalités larges passent à la limite :
Avec $n \to +\infty$.

$$\nu_p(b) \leqslant \nu_p(a) \leqslant \nu_p(b) \Rightarrow \nu_p(a) = \nu_p(b)$$

Ceci est vrai pour tout nombre premier $p$
donc $a = b$

- Par combien de 0 se termine $2020!$ ?

3 Par récurrence immédiate #couprie

4 Soit $p \in \mathbb{P}$

$$\begin{cases} a = p^{v_p(a)} P & \text{où } p \nmid P \\ b = p^{v_p(b)} Q & \text{où } p \nmid Q \end{cases}$$

À renommage près, $v_p(a) \leq v_p(b)$

$$a+b = p^{v_p(a)} (\underbrace{P + p^{v_p(b)-v_p(a)} Q}_{\in \mathbb{N}})$$

app

- Soient $a, b \geq 1$ tq
  $a \mid b^2 \mid a^3 \mid b^4 \mid a^5 \mid b^6 \mid \cdot$

  Mtq $a=b$

  Soit $p \in \mathbb{P}$. On a $\forall n \in \mathbb{N}$, $\begin{cases} a^{2n+1} \mid b^{2n+2} \\ b^{2n} \mid a^{2n+1} \end{cases}$

  Donc $\forall n \in \mathbb{N}$, $\begin{cases} (2n+1)\, v_p(a) \leq (2n+2)\, v_p(b) \\ 2n\, v_p(b) \leq (2n+1)\, v_p(a) \end{cases}$

$\Rightarrow \forall n \in \mathbb{N}$, $\dfrac{2n\, v_p(b)}{2n+1} \leq v_p(a) \leq \dfrac{(2n+2)\, v_p(b)}{2n+1}$

Les inégalités larges passent à la limite:

Avec $n \to +\infty$ :

$$v_p(b) \leq v_p(a) \leq v_p(b) \Rightarrow v_p(a) = v_p(b)$$

Ceci est vrai pour tout nombre premier $p$

donc $a=b$

- Par combien de 0 se termine $2020!$ ?

$\#\#\mathbb{Z}\#\#$

On cherche $\max\{n \in \mathbb{N},\ 10^n \mid 2020!\} = v_{10}(2020!)$

Mais ⚠ $10 \notin \mathbb{P}$, donc $v_{10}$ n'a <u>pas</u> les ppte usu. eg $v_{10}(2\cdot 5) \neq v_{10}(2) + v_{10}(5)$

<u>Par contre</u> $v_{10}(n) = \min\{v_2(n), v_5(n)\}$

<u>ici</u> $n = 2020!$

$v_2(2020!) \geqslant v_5(2020!)$

Finalement, on cherche $v_5(2020!)$

$2020! = 1\times 2\times 3\times 4\times 5\times \cdots \times 10 \times \cdots \times 15 \times \cdots \times 20 \times \cdots \times 25$

| contributions à $v_5(2020!)$ | $1$ | $1$ | $1$ | $1$ | $2$ |
|---|---|---|---|---|---|
| | $\underline{5}\cdot 1$ | $\underline{5}\cdot 2$ | $\underline{5}\cdot 3$ | $\underline{5}\cdot 4$ | $\underline{5}\cdot\underline{5}$ |

On cherche combien il y a de multiples de $5 \leqslant 2020$

$$\left\lfloor \frac{2020}{5} \right\rfloor = 404$$

On rajoute le nombre ~~de~~ de multiples de $5^2 \leqslant 2020$

$$\left\lfloor \frac{2020}{5^2} \right\rfloor = \left\lfloor \frac{404}{5} \right\rfloor = 80$$

Pareil pour $5^3$

$$\left\lfloor \frac{2020}{5^3} \right\rfloor = \left\lfloor \frac{80}{5} \right\rfloor = 16$$

Pour $5^4$

$$\left\lfloor \frac{2020}{5^4} \right\rfloor = \left\lfloor \frac{16}{5} \right\rfloor = 3$$

C'est fini : $5^5 = 3125 > 2020$

On les sommes :

$$v_{10}(2020!) = v_5(2020!) = 404 + 80 + 16 + 3 = 503$$

remq Généralisation de l'epp

On montre de même

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$ au bout d'un moment y'a que des 0

avec $p \in \mathbb{P}$

# III PGCD, PPCM

## 1 Définition et 1ères pptes

<u>def</u>

Soient $a, b \in \mathbb{Z}$

1 $d \in \mathbb{Z}$ est un pgcd de $a, b \in \mathbb{Z}$ si $d$ est un plus grand diviseur commun de $a$ et $b$ <u>pour</u> $|$

2 $d \in \mathbb{Z}$ est un ppcm de $a, b \in \mathbb{Z}$ si $d$ est un plus petit multiple commun de $a$ et $b$ <u>pour</u> $|$

<u>eg</u>

- $D(18) = \{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}$
  $D(24) = \{-24, -12, -8, -6, -4, -3, -2, -1, 1, 1, 2, 3, 4, 6, 8, 12, 24\}$

  Les diviseurs commun forment l'ensemble
  $D(18) \cap D(24) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$

  Un pgcd de 18 et 24 est 6
  Un autre est $-6$

- pgcd de 18 et 0
  $D(18) = \{-18, .., 18\}$ ; $D(0) = \mathbb{Z}$
  $D(18) \cap D(0) = D(18)$
  Un pgcd de 18 et 0 est 18

- pgcd de 0 et 0
  $D(0) \cap D(0) = \mathbb{Z}$ $\quad \max_{(\mathbb{Z}, |)} \mathbb{Z} = 0$

thm-def

Soient $a, b \in \mathbb{Z}$. Il existe un unique[0] pgcd positif de a et b.
On l'appelle le pgcd de a et b et on le note $PGCD(a,b)$ ou $a \wedge b$.

1 $\begin{cases} a \wedge 0 = a \\ 0 \wedge b = b \end{cases}$

2 Si $a, b \in \mathbb{Z}^*$

$$a \wedge b = \prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}}$$

demo

0 Unicité dans $\mathbb{N}$ la divisibilité est un ordre

Existence

1 $D(a) \cap D(0) = D(a) \cap \mathbb{Z} = D(a) \Rightarrow a \wedge 0 = a$

de même $0 \wedge b = b$

2 $d | a \Leftrightarrow \forall p \in \mathbb{P}, v_p(d) \leq v_p(a)$

$d | b \Leftrightarrow \forall p \in \mathbb{P}, v_p(d) \leq v_p(b)$

donc d divise a et b $\Leftrightarrow \forall p \in \mathbb{P}, v_p(d) \leq \min\{v_p(a), v_p(b)\}$
donc le plus grand diviseur commun est le plus grand diviseur de

$$\prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}}$$

truc hors-programme

$(\mathbb{Z}, \text{pgcd}, \text{ppcm})$ est un algèbre de Boole

**thm-def**

Soient $a, b \in \mathbb{Z}$. Il existe un unique ppcm positif de $a$ et $b$. On l'appelle le ppcm de $a$ et $b$, noté $PPCM(a,b)$ ou $a \vee b$.

1 $\begin{cases} a \vee 0 = 0 \\ 0 \vee b = 0 \end{cases}$

2 Si $a, b \in \mathbb{Z}^*$

$$a \vee b = \prod_{p \in \mathbb{P}} p^{\max\{v_p(a),\, v_p(b)\}}$$

**dem** par raisonnement analogue.

**eg**

$$18 = 2^{1} \cdot 3^{2}$$
$$24 = 2^{3} \cdot 3^{1}$$

$$\Rightarrow 18 \wedge 24 = 2^{1} \cdot 3^{1} = 6$$

$$123 = 3 \cdot 41$$
$$45 = 3^2 \cdot 9$$
$$\Rightarrow 123 \wedge 45 = 3^{1} \cdot 5^{0} \cdot 41^{0} = 3$$

**coroll**

Soient $a, b \in \mathbb{Z}$

$$(a \wedge b)(a \vee b) = |a \cdot b|$$

**dem** Si $\begin{cases} a = 0 \\ \text{ou} \\ b = 0 \end{cases}$ ok.

Sinon $\forall p \in \mathbb{P}$, $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)$

Donc $|a \cdot b| = |a||b| = \prod_{p \in \mathbb{P}} p^{v_p(a)} \cdot \prod_{p \in \mathbb{P}} p^{v_p(b)} = \prod_{p \in \mathbb{P}} p^{v_p(a) + v_p(b)}$ (*)

$$(a \wedge b)(a \vee b) = \prod_{p\in\mathbb{P}} p^{\min\{\nu_p(a),\nu_p(b)\}} \prod_{p\in\mathbb{P}} p^{\max\{\nu_p(a),\nu_p(b)\}}$$

$$= \prod_{p\in\mathbb{P}} p^{\min\{\nu_p(a),\nu_p(b)\}+\max\{\nu_p(a),\nu_p(b)\}}$$

$$= \prod_{p\in\mathbb{P}} p^{\nu_p(a)+\nu_p(b)}$$

$$= |a\cdot b| \quad \text{d'aprèi } (*)$$

**thm**

Soit schmu $\in$ {ppcm, pgcd}

1 schmu est commutatif

$\forall a,b \in \mathbb{Z},\ a \mathbin{\hat{\vee}} b = b \mathbin{\hat{\vee}} a$

2 schmu est associatif

$\forall a,b,c \in \mathbb{Z},\ (a \mathbin{\hat{\vee}} b) \mathbin{\hat{\vee}} c = a \mathbin{\hat{\vee}} (b \mathbin{\hat{\vee}} c)$

3 schmu est homogène

$\forall a,b,k \in \mathbb{Z},\ (ka) \mathbin{\hat{\vee}} (kb) = |k|(a \mathbin{\hat{\vee}} b)$

**dem** "Exercice facile"

**prop**

Soient $a,b \in \mathbb{Z}$ et $d \in \mathbb{N}$

Sont équivalentes:

i/ $d = a \wedge b$

ii/ $D(a) \cap D(b) = D(d)$

iii/ $d = \inf_{(\mathbb{N},|)} \{|a|,|b|\}$

iv/ $\begin{cases} d|a \text{ et } d|b \\ \forall \delta \in \mathbb{Z},\ (\delta|a \text{ et } \delta|b) \Rightarrow \delta|b \end{cases}$

d est un diviseur commun

d est plus grand que tt div. commun

## 2 Algorithme d'Euclide

Un algoritme pour calculer $a \wedge b$

<u>init</u> on pose $\begin{cases} r_0 = a \\ r_1 = b \end{cases}$

<u>tant que</u> $r_n \neq 0$

on pose $r_{n+1} = \text{rem}(r_{n-1}, r_n)$

Le dernier reste non-nul est le pgcd.

<u>eg</u> $18 \wedge 24$

$$\underbrace{18}_{r_0} = 0 \cdot \underbrace{24}_{r_1} + \underbrace{18}_{r_2}$$
$$\overbrace{24}^{r_1} = 1 \; \overbrace{18}^{r_2} + \overbrace{6}^{r_3} \longleftarrow \text{PGCD}$$
$$\overbrace{18}^{r_2} = 3 \cdot \overbrace{6}^{r_3} + \overbrace{\underline{\underline{0}}}^{r_4}$$

<u>eg</u> $123 \wedge 45$

$$123 = 2 \cdot 45 + 33$$
$$45 = 1 \cdot 33 + 12$$
$$33 = 2 \cdot 12 + 9$$
$$12 = 1 \cdot 9 + 3 \longleftarrow \text{PGCD}(123, 45) = r_5$$
$$9 = 3 \cdot 3 + \underline{\underline{0}}$$

<u>eg</u> $123\,456 \wedge 78\,910$

↳ En Python. \o/

```
def pgcd(a, b):
    p, q = a, b
    while q != 0:
        p, q = q, p % q
    return abs(p)
```

← p%q n'est pas tj positif!!!!!1

<u>thm</u> l'algo d'Euclide c'est pas de la merde

L'algorithme d'Euclide <u>termine</u> et <u>est correct</u>

<u>lemme</u>

1. Pour $d \in \mathbb{N}$ on a $d \wedge 0 = d$
2. Pour $a, b \in \mathbb{Z}$, $a \wedge b = b \wedge \text{rem}(a, b)$

dem du lemme

1 Déjà vu

2 Il suffit de mtq $D(a) \cap D(b) = D(b) \cap D(\text{rem}(a,b))$

$\subset$ : Si $\delta \in D(a) \cap D(b)$

Alors $\delta \in D(b)$ par déf

et $\delta | a$ et $\delta | b$

$\delta | a - bq = r$ par stabilité par combi lin. de $|$ sur

donc $\delta \in D(r)$ d'où $\delta \in D(b) \cap D(r)$

$\supset$ : Si $\delta \in D(b) \cap D(r)$

Alors $\delta \in D(b)$ par déf

et $\delta | b$ et $\delta | r$ donc par stab par combi lin.

$\delta | bq + r = a$

donc $\delta \in D(a)$

d'où $\delta \in D(a) \cap D(b)$

dem du théorème

Terminaison par l'absurde.

Supp que l'algo. ne termine pas.

On définit alors $(r_n)_{n \in \mathbb{N}}$ la suite des restes dans l'algo.

donc $r \in \searrow(\mathbb{N}, \mathbb{N})$ imp

Correction Notons $b = a \wedge b$. On a:

$$\begin{aligned} d &= r_0 \wedge r_1 \\ &= r_1 \wedge r_2 \quad \text{d'ap lemme 2} \\ &= r_1 \wedge r_3 \quad \text{d'ap lemme 2} \\ &\vdots \end{aligned}$$

$\vdots$

$= r_{n-1} \wedge r_n$

$= r_n \wedge r_{n+1}$

$= r_n \wedge 0$ par déf.

$= r_n$ d'ap lemme 1

**remq** Complexité de l'algo

L'algo d'Euclide est efficace.

**thm** d'Eudoxe (sur la relation de Bézout)

Soient $a, b \in \mathbb{Z}$ et $d = a \wedge b$

Alors il existe $(u, v) \in \mathbb{Z}^2$

tq $au + bv = d$

ie on peut expr le pgcd de deux entiers come CL avec deux autres

**dem**

En reprennant la notation de l'algo d'Euclide.

$d = r_n$ est une CL[1] de $r_{n-2}$ et $r_{n-1}$

or $r_{n-1}$ " " " " $r_{n-3}$ " $r_{n-2}$

$\Rightarrow d$ " " " " $r_{n-3}$ " $r_{n-2}$

or $r_{n-2}$ " " " " $r_{n-4}$ " $r_{n-3}$

$\Rightarrow d$ " " " " $r_{n-4}$ " $r_{n-3}$

$\vdots$

par récurrence immédiate,

$d$ est une CL de $r_0 = a$ et $r_1 = b$

ie $d = au + bv$

**eg** Relation de Bézout pour $123 \wedge 45 = 3$

---

[1] combi. lin.

$123 = 2 \cdot 45 + 33 \Leftrightarrow 33 = 123 - 2 \cdot 45$ donc $3 = -4 \cdot 123 + 11 \cdot 45$

$45 = 1 \cdot 33 + 12 \Leftrightarrow 12 = 45 - 1 \cdot 33$ donc $3 = 3 \cdot 45 - 4 \cdot 33$

$33 = 2 \cdot 12 + 9 \Leftrightarrow 9 = 33 - 2 \cdot 12$ donc $3 = -33 + 3 \cdot 12$

$12 = 1 \cdot 9 + 3 \Leftrightarrow 3 = 12 - 1 \cdot 9$ réinjection

$9 = 3 \cdot 3 + \underline{0}$

exo bonus Écrire une function Pyth. qui calc pgcd & une rel de Bézout

Il n'y a pas d'unicité d'un couple $(u, v)$

remq
Soit $a, b \in \mathbb{Z}$ et $d \in \mathbb{N}$. S'il existe $(u, v) \in \mathbb{Z}^2$ tels que $d = au + bv$ alors :

$$a \wedge b \mid d$$

dem

$d = au + bv$ or $\begin{cases} a \wedge b \mid a \\ a \wedge b \mid b \end{cases}$

par stabilité de la CL : $a \wedge b \mid au + bv = d$

thm Reformulation du thm d'Eudoxe.
Soient $a, b \in \mathbb{Z}$ & $d = a \wedge b$
Alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

dem

Meth 1 Utilisation d'Eudoxe et sa réciproque partielle

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv, (u, v) \in \mathbb{Z}^2\}$$

d'ap Eudoxe $d \in a\mathbb{Z} + b\mathbb{Z}$
donc $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$

d'ap la réciproque partielle d'Eudoxe :
$\forall \delta \in a\mathbb{Z} + b\mathbb{Z}, \ d \mid \delta \Leftrightarrow \forall \delta \in a\mathbb{Z} + b\mathbb{Z}, \ \delta \in d\mathbb{Z}$ ie $d\mathbb{Z} \supset a\mathbb{Z} + b\mathbb{Z}$

## Meth 2 Caractérisation des sous-groupes de $(\mathbb{Z}, +)$

On observe que la somme de deux sous-groupes est tj s-g[1]

$\begin{cases} a\mathbb{Z} \text{ est un s-g } (\mathbb{Z},+) \\ b\mathbb{Z} \text{ est un s-g } (\mathbb{Z},+) \end{cases}$

$\Rightarrow a\mathbb{Z} + b\mathbb{Z}$ est un s-g $(\mathbb{Z},+)$

d'ap la carac. des s-g $(\mathbb{Z},+)$,

il existe $d \in \mathbb{N}$ tq

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

Mtq $d = a \wedge b$

On a $\begin{cases} a \in a\mathbb{Z} + b\mathbb{Z} \Rightarrow a \in d\mathbb{Z} \Rightarrow d \mid a \\ b \in b\mathbb{Z} + a\mathbb{Z} \Rightarrow b \in d\mathbb{Z} \Rightarrow d \mid b \end{cases}$

Soit $\delta \in \mathbb{Z}$ tel que $\delta \mid a$ et $\delta \mid b$

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

donc il existe $(u, v) \in \mathbb{Z}^2$ tels que

$d = au + bv$ or $\begin{cases} \delta \mid a \\ \delta \mid b \end{cases}$

Par stabilité par CL de $\mid$ :

$\delta \mid d$

## 3 Entiers premiers entre eux

**def**

Soient $a, b \in \mathbb{Z}$. $a$ et $b$ sont p.e.e.[2] ssi $a \wedge b = 1$

**prop** Lien premier $\leftrightarrow$ p.e.e.

Soit $p \geq 2$. On a $p \in \mathbb{P} \Leftrightarrow \forall a \in \mathbb{Z} \setminus p\mathbb{Z},\ a \wedge p = 1$

**dem**

$\Rightarrow$ : Supp $p \in \mathbb{P}$ ie $D_+(p) = \{1, p\}$

---

[1] sous-groupe [2] premiers entre eux

Soit $a \in \mathbb{Z} \setminus p\mathbb{Z}$

$D_+(a) \cap D_+(p) \subset D_+(p) = \{1, p\}$

$\subset D_+(a)$ et $a \notin p\mathbb{Z}$

donc $p \notin D_+(a)$

Donc $D_+(a) \cap D_+(b) \subset \{1\}$

$\Leftarrow$ : Par contraposition.

Supp $p \notin \mathbb{P}$

Ainsi $p$ a un diviseur positif $d \notin \{1, p\}$

$\Rightarrow d \in \{2, \quad, p-1\}$

$\Rightarrow d \in \mathbb{Z} \setminus p\mathbb{Z}$

$\Rightarrow d \mid p$

$\Rightarrow d \wedge p \neq 1$

**remq**

Si $a, b \in \mathbb{Z}$ alors $\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b} = 1$

**dem**

Par homogénéité du pgcd. Notons $d = \frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b}$

On a $a \wedge b = \left((a \wedge b)\frac{a}{a \wedge b}\right) \wedge \left((a \wedge b)\frac{b}{a \wedge b}\right)$

$= (a \wedge b)\left[\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b}\right]$

$= (a \wedge b) \cdot d$

$\Rightarrow d = \frac{a \wedge b}{a \wedge b} = 1$

**thm de Bézout**

Soient $a, b \in \mathbb{Z}$

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

**dem**

$\Rightarrow$ : Eudoxe

$\Leftarrow$ : Si il existe $(u, v) \in \mathbb{Z}^2$ tq $au + bv = 1$ alors $a \wedge b \mid 1$

$\Rightarrow a \wedge b = 1$

app de l'enfer

Soient $a, b \in \mathbb{Z}$.

Mtq $a \wedge b = 1 \iff (a+b) \wedge ab = 1$

$\Leftarrow$ : Supp $(a+b) \wedge ab = 1$.

d'ap le sens direct de Bézout

il existe $(U, V) \in \mathbb{Z}^2$ tq $(a+b)U + abV = 1$

ie. $aU + b(U + aV) = 1$

Posons $\begin{cases} u = U \in \mathbb{Z} \\ v = U + aV \in \mathbb{Z} \end{cases}$

On a $au + bv = 1$

d'ap le sens réciproque de Bézout

On a $a \wedge b = 1$

$\Rightarrow$ : Supp $a \wedge b = 1$

Donc d'ap le sens direct de Bézout

il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

donc $a^2u^2 + b^2v^2 + 2uvab = (au+bv)^2 = 1^2 = 1$

ie $(a+b)(au^2 + bv^2) - bau^2 - abv^2 + 2uvab = 1$

ie $(a+b)(au^2 + bv^2) - (u^2 + v^2 - 2uv)ab = 1$

ie $(a+b)(au^2 + bv^2) - (u-v)^2 ab = 1$

Posons $\begin{cases} U = au^2 + bv^2 \in \mathbb{Z} \\ V = -(u-v)^2 \in \mathbb{Z} \end{cases}$

On a $(a+b)U + abV = 1$

Donc d'après le sens réciproque de Bézout :

$(a+b) \wedge ab = 1$

coroll de Bézout

1 Soient $a, b_1, b_2, \dots, b_q \in \mathbb{Z}$ tels que

$\begin{cases} a \wedge b_1 = 1 \\ a \wedge b_2 = 1 \\ \vdots \\ a \wedge b_q = 1 \end{cases}$

Alors $a \wedge b_1 b_2 \cdots b_q = 1$

2 Soient $a, b \in \mathbb{Z}$ et $p, q \in \mathbb{N}$ tels que $a \wedge b = 1$ alors $a^p \wedge b^q = 1$

dem

1 D'après le sens direct de Bézout il existe $u_1, v_1, u_2, v_2, u_3, \dots, u_q, v_q \in \mathbb{Z}$ tels que.

$$\begin{cases} au_1 + b_1 v_1 = 1 \\ au_2 + b_2 v_2 = 1 \\ \vdots \\ au_q + b_q v_q = 1 \end{cases}$$

$$a(\underbrace{a^{q-1} u_1 \cdots u_q +}_{U} \quad ) + \underbrace{b_1 b_2 \quad b_q v_1 v_2 \quad \cdot v_q}_{V} = 1 \quad \text{par produit}$$

d'après Bézout, réciproque OK

## 2 "exo facile"

**Lemme de Gauss**

Soient $a, b, c \in \mathbb{Z}$

Si $\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases}$ alors $a \mid c$

**dem**

Supp $\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases}$ donc $\begin{cases} \text{il existe } k \in \mathbb{Z},\ ak = \boxed{bc} \\ \cdots\cdots\cdots (u,v) \in \mathbb{Z}^2,\ au + bv = 1 \end{cases}$

On multiplie par $acu + \boxed{bc}v = c$

$$\Leftrightarrow a(\underbrace{cu + kv}_{\in \mathbb{Z}}) = c$$

$$\Rightarrow a \mid c$$

coroll de Gauss

Soient $a, b, x, y \in \mathbb{Z}$ tels que $a \wedge b = 1$.

$$ax = by \Leftrightarrow \exists k \in \mathbb{Z}, \begin{cases} x = bk \\ y = ak \end{cases}$$

dem

$\Leftarrow$ : Supp qu'il existe $k \in \mathbb{Z}, \begin{cases} x = bk \\ y = ak \end{cases}$. Alors $ax = abk = bak = by$.

$\Rightarrow$ : Supp $ax = by$

On a $a | ax \Rightarrow \begin{cases} a | by \\ a \wedge b = 1 \end{cases}$

donc $a | y$ d'après Gauss

Alors il existe $k \in \mathbb{Z} \ / \ y = ak$

Or $ax = by$ donc en réinjectant,

$$ax = abk$$

Si $a \neq 0$ on tire bien $x = bk$

Sinon $b = \pm 1$, $y = 0$ et il suffit de poser $k = 0$.

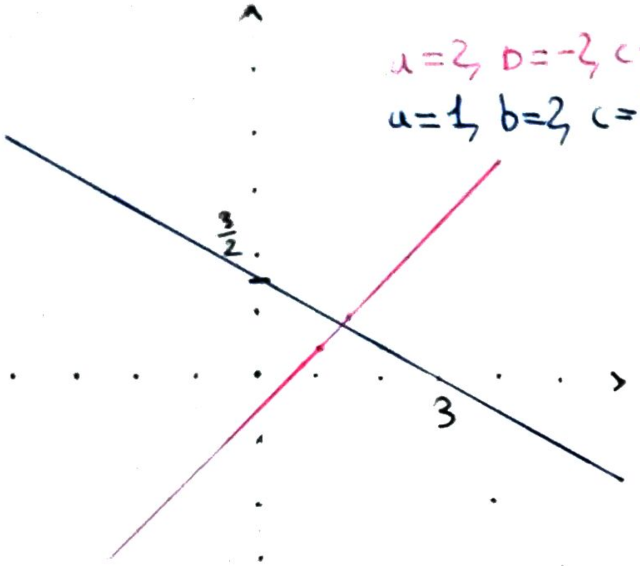
## 4 Équations diophantiennes affines

Le problème pour $a, b, c \in \mathbb{Z}$, on veut résoudre dans $\mathbb{Z}^2$ l'équation

$$ax + by = c.$$

$a=2,\ b=-2,\ c=1\quad D : 2x-2y=1$

$a=1,\ b=2,\ c=3\quad D_2 : x+2y=3$




meth

Deux cas

1^er cas ($a \wedge b \nmid c$) :

D'après Eudoxe, il n'y a pas de solutions.

2^e cas ($a \wedge b \mid c$) :

1. On note $\begin{cases} a' = \frac{a}{a \wedge b} \\ b' = \frac{b}{a \wedge b} \\ c' = \frac{c}{a \wedge b} \end{cases}$ L'équation équivaut à $a'x + b'y = c'$

2. On cherche une solution particulière
   - On remonte l'algo d'Euclide pour trouver $a'u + b'v = 1$
   
   et on pose $\begin{cases} x_0 = c'u \\ y_0 = c'v \end{cases}$
   
   ou
   - Par contemplation

3. On soustrait la solution particulière.

   On a $a'x_0 + b'y_0 = c'$

$$\Rightarrow a'x + b'y = c'$$

$$\Leftrightarrow a'(x - x_0) + b'(y - y_0) = 0$$

$$\Leftrightarrow a'(x - x_0) = b'(y_0 - y)$$

$$\Leftrightarrow \exists k \in \mathbb{Z}, \begin{cases} x - x_0 = b'k \\ y_0 - y = a'k \end{cases}$$

$$\Leftrightarrow \exists k \in \mathbb{Z}, \begin{cases} x = x_0 + b'k \\ y = y_0 - a'k \end{cases}$$ d'après le coroll de Gauss car $a' \wedge b' = 1$

4. On conclut

$$S = \{(x_0 + b'k, y_0 - a'k), k \in \mathbb{Z}\}$$

<u>variante</u> Systèmes de congruences

$$\begin{cases} x \equiv \alpha \, [a] \\ x \equiv \beta \, [b] \end{cases}$$ avec $a, b \in \mathbb{Z}$ et $a \wedge b = 1$

On peut se ramener à une équation diophantienne affine

En effet, $\begin{cases} x \equiv \alpha \, [a] \Leftrightarrow \exists k \in \mathbb{Z}, x = ak + \alpha \\ x \equiv \beta \, [b] \Leftrightarrow \exists k \in \mathbb{Z}, x = bk + \beta \end{cases}$

Par soustraction il existe $k, k' \in \mathbb{Z}$ tel que

$$0 = ak - bk' + \alpha - \beta \quad \text{ie} \quad ak - bk' = \beta - \alpha$$

<u>meth</u>

1 On trouve une solution particulière $x_0$

2 L'équation équivaut à $\begin{cases} x - x_0 \equiv 0 \, [a] \\ x - x_0 \equiv 0 \, [b] \end{cases}$

$$\Leftrightarrow ab \mid x - x_0$$ car $a \vee b = \frac{ab}{a \wedge b} = ab$

$$S = \{x_0 + ab\eta,\ \eta \in \mathbb{Z}\}$$

## 5 Petit théorème de Fermat

Lemme

$$\forall p \in \mathbb{P},\ \forall k \in [\![1, p[\![,\ p \mid \binom{p}{k}$$

demo

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

ie $p(p-1)\cdots(p-k+1) = k!\binom{p}{k}$

$$\Rightarrow p \mid k!\binom{p}{k}$$

$p \wedge k = 1$ car $k \notin p\mathbb{Z}$ (lien $\mathbb{P}$ / p.e.e)

$p \wedge (k-1) = 1$ car $(k-1) \notin p\mathbb{Z}$ (...... - - -)

$\vdots$

$p \wedge 1 = 1$ car $1 \notin p\mathbb{Z}$ (............)

donc d'ap. le coroll de Bézout:

$$p \wedge (k \times (k-1) \times \cdots \times 1) = 1$$

ie $p \wedge k! = 1$

Ainsi $\begin{cases} p \mid k!\binom{p}{k} \\ p \wedge k! = 1 \end{cases}$

donc d'après le lemme de Gauss

$$p \mid \binom{p}{k}$$

thm petit théorème de Fermat

Soit $p \in \mathbb{P}$. Alors

1 $\forall n \in \mathbb{Z},\ n^p \equiv n\,[p]$

2 $\forall a \in \mathbb{Z} \setminus p\mathbb{Z},\ a^{p-1} \equiv 1\,[p]$

dem

1 Mq $\forall n \in \mathbb{N},\ n^p \equiv n\,[p]$ par récurrence.

Init $(n=0)$:

$0^p \equiv 0\,[p]$

Her Soit $n \in \mathbb{N}$ et supp $n^p \equiv n\,[p]$. Mq $(n+1)^p \equiv (n+1)\,[p]$

On a $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$

$= \underbrace{1}_{k=0} + \sum_{k=1}^{p-1} \binom{p}{k} n^k + \underbrace{n^p}_{k=p}$

1. BdN

2. Sep la some, pied + $\sum$ + tête

On a pour $k \in [\![1, p[\![$, $\binom{p}{k} \equiv 0\,[p]$

et donc $\binom{p}{k} n^k \equiv 0\,[p]$ par stabilité du produit

donc par stabilité par somme $\sum_{k=1}^{p-1} \binom{p}{k} n^k \equiv 0\,[p]$

construire $\underbrace{\sum_{k=1}^{p-1} \binom{p}{k} n^k}$ $\equiv 0\,[p]$

donc $(n+1)^p \equiv 1 + 0 + n^p\,[p]$ par stabilité par somme

rajouter pied & tête à $\equiv 0\,[p]$

$\equiv 1 + n\,[p]$ par hdr

$\equiv n+1\,[p]$ car $(\mathbb{Z}, +)$ est un groupe abélien.

d'où l'hérédité.

<u>Conclusion partielle</u> On a cette propriété init & héré donc

$\forall n \in \mathbb{N}, n^p \equiv n \ [p]$

Soit $n \in \mathbb{Z} \setminus \mathbb{N} \in -\mathbb{N}$

Mais $n = -|n|$.

<u>Traitons deux cas:</u>

<u>1er cas</u> $(p = 2)$:

$n^p = n^2 = |n|^2 \equiv |n| \ [2]$

Et $-1 \equiv 1 \ [2]$

$\Rightarrow \underbrace{-|n|}_{n} \equiv |n| \ [2]$

Finalement $n^p \equiv |n| \equiv n \ [p]$

<u>2e cas</u>$(p \neq 2)$:

$p \in 2\mathbb{N}+1 \Rightarrow n^p = (-|n|)^p = (-1)^p |n|^p = -|n|^p \equiv -|n| \ [p]$

2 Soit $a \in \mathbb{Z} \setminus p\mathbb{Z}$

d'ap 1, $p \mid a^p - a$

ie $p \mid a(a^{p-1} - 1)$

or $p \wedge a = 1$ d'ap le lien $\mathbb{P}$-p.e.e

d'ap le lemme de Gauss:

$p \mid a^{p-1} - 1$ ie $a^{p-1} \equiv 1 \ [p]$

## 6 Anneau $\mathbb{Z}/p\mathbb{Z}$ avec $p \in \mathbb{P}$

rpl
$$\begin{cases} \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\} \\ \bar{a} + \bar{b} = \overline{a+b} \\ \bar{a} \times \bar{b} = \overline{ab} \\ (\mathbb{Z}/p\mathbb{Z}, +, \times) \text{ est un anneau commutatif} \end{cases}$$

app

$$p \in \mathbb{P} \Rightarrow \forall \bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \exists \bar{u} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \bar{a} \times \bar{u} = \bar{1}$$

remq terminologie

Un anneau commutatif non-nul dans lequel tout élément a un inverse est appelé un corps

dem

Soit $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.

Ainsi $a \in \mathbb{Z} \setminus p\mathbb{Z}$

donc, d'après le lien $\mathbb{P}$ - p.e.e., $a \wedge p = 1$.

d'ap le sens direct du th de Bézout, $(u, v) \in \mathbb{Z}^2$ tq

$$au + pv = 1$$

d'où $\overline{au + pv} = \bar{1}$

ie $\bar{a} \times \bar{u} + \bar{p} \times \bar{v} = \bar{1}$

Or $\bar{p} = \bar{0} \Rightarrow \bar{u} \times \bar{v} = \bar{1}$

## 7 PGCD/PPCM de n entiers

def - thm

Soient $a_1, \dots, a_n \in \mathbb{Z}$.

1 $\exists! d \in \mathbb{N}$, $d$ est un pgcd de $a_1, \dots, a_n$.

On l'appelle le pgcd de $a_1, \dots, a_n$, noté $a_1 \wedge \dots \wedge a_n$

2 $\exists! m \in \mathbb{N}$, $m$ est un ppcm de $a_1, \dots, a_n$

On l'appelle ppcm de $a_1, \dots, a_n$, noté $a_1 \vee \dots \vee a_n$

En général

$(a_1 \wedge \dots \wedge a_n) \times (a_1 \vee \dots \vee a_n) \neq |a_1 \cdots a_n|$

eg $(1 \wedge 2 \wedge 4) \cdot (1 \vee 2 \vee 4) = 1 \cdot 4 \neq 8 = 1 \cdot 2 \cdot 4$

thm

Le pgcd est

1 Associatif

$a_1 \wedge (a_2 \wedge (\dots) \wedge a_n) = a_1 \wedge a_2 \wedge \dots \wedge a_n$

2 Commutatif

$\forall \sigma \in S_n$, $a_{\sigma(1)} \wedge a_{\sigma(2)} \wedge \dots \wedge a_{\sigma(n)} = a_1 \wedge a_2 \wedge \dots \wedge a_n$

3 Homogène

$(k a_1) \wedge \dots \wedge (k a_n) = |k| (a_1 \wedge \dots \wedge a_n)$

ppcm possède les mêmes propriétés.

**thm** Eudoxe généralisé

Soient $a_1, \dots, a_n \in \mathbb{Z}$. et $d = a_1 \wedge \dots \wedge a_n$

1 Il existe $u_1, u_2, \dots, u_n$ tq $a_1 u_1 + \dots + a_n u_n = d$

2 $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$.

**def**

Soient $a_1, \dots, a_n \in \mathbb{Z}$.

1 On dit que $a_1, \dots, a_n$ sont p.e.e dans leur ensemble
quand $a_1 \wedge \dots \wedge a_n = 1$
eg 6, 10, 15

2 On dit que $a_1, \dots, a_n$ soint p.e.e deux à deux
quand $\forall i \neq j \in [\![1, n]\!]$, $a_i \wedge a_j = 1$
eg 8, 9, 25