Rq: $\mathbb{Z}$ est un anneau principal
$m\mathbb{Z}$ ssgr de $\mathbb{Z}$ de plus
$q(m\mathbb{Z}) \subset m\mathbb{Z}$ $\forall q \in \mathbb{Z}$ ie $m\mathbb{Z}$ stable
par multi, est ie $m\mathbb{Z}$ idéal
de l'anneau $(\mathbb{Z}, +, \cdot)$

Exposé 11

PGCD et PPCM de deux entiers naturels. Nombres premiers entre eux. Application. Illustration avec calculatrice

0 - Pré-Requis :

- Division euclidienne
- Les sous groupes de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$
- Prop : $\forall m, n \in \mathbb{Z}$, $m \mid n$ ssi $n\mathbb{Z} \subset m\mathbb{Z}$

I PGCD de deux entiers naturels

Prop : Soit $(a,b) \in \mathbb{N}^2$, il existe un unique $c \in \mathbb{N}$ tq $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$. De plus c est le plus grand diviseur commun à a et b.

Notation : On note $c = \text{pgcd}(a,b)$ ou $c = a \wedge b$

[[1) $a\mathbb{Z} + b\mathbb{Z}$ ss groupe de $(\mathbb{Z},+)$ (facile à vérifier, non vide car $a \in a\mathbb{Z}+b\mathbb{Z}$ ...)
d'où l'existence et l'unicité de c d'après le thm pré-requis.

2) On a $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ or $a\mathbb{Z} \cup b\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$

On a donc $\left.\begin{array}{l} a\mathbb{Z} \subset c\mathbb{Z} \\ b\mathbb{Z} \subset c\mathbb{Z} \end{array}\right\} \Rightarrow \left.\begin{array}{l} c \mid a \\ c \mid b \end{array}\right) \Rightarrow c$ diviseur commun à a et b.

3) Soit $c' \in \mathbb{N}$ un diviseur commun à a et b.
$a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ donc $c \in a\mathbb{Z} + b\mathbb{Z}$ ie $\exists \lambda, \mu \in \mathbb{Z}$ tq $c = a\lambda + b\mu$
$c' \mid a$ ie $\exists q \in \mathbb{Z}$ tq $a = c'q$
$c' \mid b$ ie $\exists q' \in \mathbb{Z}$ tq $b = c'q'$ dc $c = a\lambda + b\mu = c'(\lambda q + \mu q')$ dc $c' \mid c$
$\Rightarrow c$ est le plus grand diviseur commun à a et b.]]

Propriétés du PGCD : soit $a, b, c, m \in \mathbb{N}$

0) $\text{pgcd}(a,0) = a$

i) $\text{pgcd}(a,b) = \text{pgcd}(b,a)$

ii) $\text{pgcd}(a, \text{pgcd}(b,c)) = \text{pgcd}(\text{pgcd}(a,b), c)$

iii) $\text{pgcd}(ma, mb) = m\,\text{pgcd}(a,b)$

[[Vient de la définition du PGCD]]

Pour le calcul du PGCD de deux entiers on utilise :

Thm d'Euclide :
Soit $a, b, q, r \in \mathbb{N}^*$ $a = bq + r \Rightarrow \text{pgcd}(a,b) = \text{pgcd}(b,r)$
On va se servir de ce théorème pour établir l'algorithme suivant.

Algorithme d'Euclide :
Soit $a, b \in \mathbb{N}^*$, $\exists!(q_1, r_1) \in \mathbb{N}^2$ tq $a = bq_1 + r_1$ $0 \leq r_1 < b$ (div eucl de a par b)

- Si $r_1 = 0$ alors $\text{pgcd}(a,b) = b$
- si $r_1 \neq 0$ $\text{pgcd}(a,b) = \text{pgcd}(b, r_1)$ (Thm d'Euclide)

  $\exists!(q_2, r_2) \in \mathbb{N}^2$ tq $b = r_1 q_2 + r_2$ $0 \leq r_2 < r_1$ (div eucl de b par r_1)
  - si $r_2 = 0$ alors $\text{pgcd}(a,b) = \text{pgcd}(b, r_1) = r_1$

  ...

Donc on construit une suite $(r_n)_n$ strictement décroissante et minorée. De plus $(r_n)_n$ est une suite d'entiers positifs.

donc $\exists k \in \mathbb{N}$ tq $r_k \neq 0$ et $r_{k+1} = 0$

De plus on a $pgcd(a,b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \dots = pgcd(r_k, r_{k+1}) = r_k$ (ie dernier reste non nul).

Exemple $a = 93$ et $b = 66$

$93 = 66 \times 1 + 27$ $\quad 93 \wedge 66 = 66 \wedge 27$

$66 = 27 \times 2 + 12$ $\quad 66 \wedge 27 = 27 \wedge 12$

$27 = 12 \times 2 + \boxed{3}$ $\quad 27 \wedge 12 = 12 \wedge 3 = \boxed{3}$

$12 = 3 \times 4 + 0$

II PPCM de deux entiers naturels :

Prop : Soit $(a,b) \in \mathbb{N}^2$, il existe un unique $m \in \mathbb{N}$ tq $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

m est le plus petit commun multiple de a et b.

Notation : On note $m = ppcm(a,b)$ ou $m = a \vee b$.

Propriétés : soit $(a,b,c) \in \mathbb{N}^3$

i) $0 \vee a = 0$

ii) $1 \vee a = a$

iii) $a \vee b = b \vee a$

iv) $(a \vee b) \vee c = a \vee (b \vee c)$

v) $(ca \vee cb) = c(a \vee b)$

[Découle de la définition du PPCM]

III Nombres premiers entre eux :

Def. Soit $a, b \in \mathbb{N}$, a et b st premiers entre eux ssi $pgcd(a,b) = 1$

Thm de Bezout : Soit $a, b \in \mathbb{Z}$. a et b sont premiers entre eux ssi $\exists (u,v) \in \mathbb{Z}^2$ tq $au + bv = 1$

Rq : – le couple (u,v) n'est pas unique.

– u et v peuvent être trouvé par l'algorithme d'Euclide.

Thm de Gauss : Si $a | bc$ et $a \wedge b = 1$ alors $a | c$

[$a \wedge b = 1$ ie $\exists u, v \in \mathbb{Z}$ tq $au + bv = 1$ (Bezout)

$acu + bcv = c$ or $a | bc$ ie $bc = aq, q \in \mathbb{Z}$

ie $a(cu + qv) = c$ ie $a | c$]

Théorèmes caractéristiques du PGCD et du PPCM :

Soit $(a,b) \in \mathbb{N}^2$, Soit d un diviseur commun à a et b tq $a = dk, b = dk'$ $\quad k, k' \in \mathbb{Z}$

et m un multiple commun à a et b tq $m = aq$, $m = bq'$ $\quad q, q' \in \mathbb{Z}$

i) d est le $pgcd(a,b)$ alors $k \wedge k' = 1$

ii) m est le $ppcm(a,b)$ alors $q \wedge q' = 1$

Prop : Soit $a, b \in \mathbb{N}^*$ $\quad ab = ppcm(a,b) \times pgcd(a,b)$

[Dans la démonstration on se sert notamment du thm précédent] /

IV Applications :

1) Equation diophantienne :

Soit $(A,B,C) \in \mathbb{Z}^3$ résoudre l'équation $Ax+By=C$, $(x,y)\in\mathbb{Z}^2$

2) Congruence :

Trouver l'ensembl des entiers x tq $x \equiv k\,[m]$, $x \equiv l\,[n]$; k, l, m, n donnés et $m \wedge n = 1$

3) La racine carré d'un nombre premier n'est pas un rationnel.

ie Si p premier $\sqrt{p} \notin \mathbb{Q}$

Exercice 1 :

Soit $(A,B,C)\in\mathbb{Z}^3$ et $d = pgcd(A,B)$ ie $A = da$, $B = db$ $(a,b)\in\mathbb{Z}$

$a\wedge b = 1$ (d'après Thm car PGCD)

Donc $Ax+By=C \iff d(ax+by)=C$

Donc $d|C$

Donc Condition necessaire : C divisible par d (Sinon il n'y a pas de solution)

si C divisible par d, $C = dc$ avec $c\in\mathbb{Z}$

On est donc amené à résoudre :

$ax+by=c$ $(x,y)\in\mathbb{Z}^2$ et $a\wedge b=1$.

De plus $a\wedge b=1$ Donc (Bezout) $\exists u,v\in\mathbb{Z}$ tq $au+bv=1$

ie $acu+bcv=c$

dc $\begin{cases} ax+by=c \\ acu+bcv=c \end{cases} \iff a(x-cu)=b(cv-y)$

donc $a\,|\,b(cv-y)$ et $a\wedge b=1 \xRightarrow{GAUSS} a\,|\,(cv-y)$

ie $\exists k\in\mathbb{Z}$ tq $cv-y=ak$

ie $y = cv-ak$

or $a(x-cu)=b(cv-y)$
$= b(\cancel{cv}-\cancel{cv}+ak)$

$\cancel{a}(x-cu)=b\cancel{a}k$ $\quad x = bk+cu$

$S = \{x = cu+bk$ et $y = cv-a\,k \mid k\in\mathbb{Z}\}$

On en déduit $S = \{(x,y) \in \mathbb{Z}^2 \text{ tq } x = bk + cu,\ y = cv - ak,\ k \in \mathbb{Z}\}$

Exercice 2 :

Trouver $x \in \mathbb{Z}$ tq $x \equiv k\,[m]$, $x \equiv l\,[n]$; k, l, m, n donnés et $m \wedge n = 1$

[$m \wedge n = 1$ ie $\exists u, v \in \mathbb{Z}$ tq $mu + nv = 1$

Donc $mu \equiv 1\,[n]$

$nv \equiv 1\,[m]$

$lmu \equiv l\,[n]$ $knv \equiv k\,[m]$

Donc si on prend $x_0 = lmu + knv$ alors x_0 solution en effet $x_0 \equiv k\,[m]$, $x_0 \equiv l\,[n]$

De plus $x \equiv k\,[m]$, $x \equiv l\,[n]$ et $x_0 \equiv k\,[m]$, $x_0 \equiv l\,[n]$

$x - x_0 \equiv 0\,[m]$, $x - x_0 \equiv 0\,[n]$ De plus $m \wedge n = 1$

$\Rightarrow x - x_0$ est divisible par mn

ie $x - x_0 = mnq$ $q \in \mathbb{Z}$

ie $\underline{x = mnq + x_0,\ q \in \mathbb{Z}}$

Réciproquement on vérifierait que si $x = mqn + x_0, q \in \mathbb{Z}$ alors x solution...

Exercice 3 :

Soit p un nombre premier $\underline{\text{Mq } \sqrt{p} \notin \mathbb{Q}}$

On raisonne par l'absurde et on suppose que $\sqrt{p} \in \mathbb{Q}$

c'est dire qu'il existe $(a,b) \in \mathbb{Z}$ tq $\sqrt{p} = \frac{a}{b}$ et $a \wedge b = 1$

$p = \frac{a^2}{b^2}$ ie $a^2 = b^2 p$

~~or $a \wedge b = 1$~~ donc $p \mid a$ (car $a^2 = b^2 p$ ie p divise a^2 or p premier)

ie $a = pq$, $q \in \mathbb{Z}$

$a^2 = b^2 p$ ie $p^2 q^2 = b^2 p$ ie $pq^2 = b^2$ ie $p \mid b$ car p premier.

donc $p \mid a$ et $p \mid b$ absurde car $a \wedge b = 1$]

Démonstrations :

Prop : Soit $a, b \in \mathbb{N}^*$, $ab = a \wedge b \times a \vee b$

[[On pose $d = \text{pgcd}(a,b)$ et $m = \text{ppcm}(a,b)$

$\exists (a', b') \in \mathbb{N}^{*2}$ tq $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$

et $\exists (x, y) \in \mathbb{N}^{*2}$ tq $m = ax$ et $m = by$

$ab = d\underbrace{a'db'}_{m'}$ Reste à montrer que $m = m'$

- $m' = da'b' = ab' = ba'$ ie m' multiple de a et de b
  or m est le plus petit ie $m' = mk$ $k \in \mathbb{Z}$
- D'autre part $m = a''a$ et $m = b''b$ car $m = a \vee b$

$\begin{cases} \text{On a déjà vu } m' = ab' = ba' \\ \text{et } m' = km = ka''a = kb''b \end{cases}$

$\Downarrow \begin{cases} ka''\cancel{a} = \cancel{a}b' & \text{ie } k \mid b' \\ kb''\cancel{b} = a'\cancel{b} & \text{ie } k \mid a' \end{cases}$ ie $k = 1$ car $a' \wedge b' = 1$

ie $\boxed{m = m'}$]]

Thm : $a \wedge b = 1$ et $a \wedge c = 1$ alors $a \wedge bc = 1$

[[ie $\exists (k_1, k_2) \in \mathbb{Z}^2$ et $(q_1, q_2) \in \mathbb{Z}^2$ tq $1 = ak_1 + bk_2$ et $1 = aq_1 + cq_2$

$1 = (ak_1 + bk_2)(aq_1 + cq_2) = a^2k_1q_1 + ack_1q_2 + bak_2q_1 + bcq_2k_2$

$1 = a(ak_1q_1 + ck_1q_2 + bk_2q_1) + bc(q_2k_2)$

ie $a \wedge bc = 1$]]

Propriétés du PGCD :

[[i) Trivial.

ii) et iii) viennent de : $(xa)\mathbb{Z} + (xb)\mathbb{Z} = x[(a \wedge b)\mathbb{Z}] = [x(a \wedge b)]\mathbb{Z}$

et $((a \wedge b) \wedge c) = (a \wedge b + (c)) = (a) + (b) + (c) = a + (b \wedge c) = (a \wedge (b \wedge c))$

où $(a) = a\mathbb{Z}$]]

Thm d'Euclide :

[[i) $\begin{matrix} a \wedge b \mid a \\ a \wedge b \mid b \end{matrix} \Rightarrow a \wedge b \mid bq$ or $r = a - bq$ dc $\begin{matrix} a \wedge b \mid r \\ a \wedge b \mid b \end{matrix} \Rightarrow$ $a \wedge b$ div. commun à r et b donc $a \wedge b \mid r \wedge b$

ii) $\begin{matrix} r \wedge b \mid r \\ r \wedge b \mid b \end{matrix} \Rightarrow r \wedge b \mid bq$ or $a = bq + r$ dc $\begin{matrix} r \wedge b \mid a \\ r \wedge b \mid b \end{matrix} \Rightarrow$ $r \wedge b$ div commun à a et b dc $r \wedge b \mid a \wedge b$]]

Prop: PPCM de deux entiers :
Soit $(a,b)\in\mathbb{N}^2$, $\exists!\, m\in\mathbb{N}$ tq $a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$. m est le plus petit commun multiple de a et b.

[1) $a\mathbb{Z}$ ss gr de $(\mathbb{Z},+)$, $b\mathbb{Z}$ ss gr de $(\mathbb{Z},+)$ $\Rightarrow$ $a\mathbb{Z}\cap b\mathbb{Z}$ ss gr de $(\mathbb{Z},+)$ comme intersection de 2 ssgr $\Rightarrow$ Existence et unicité de $m\in\mathbb{N}$ tq $a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$.

2) $a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$
Donc $m\mathbb{Z}\subset a\mathbb{Z}$ ie $a|m$, $m\mathbb{Z}\subset b\mathbb{Z}$ ie $b|m$ $\Rightarrow$ m multiple commun de a et b

3) soit $m'\in\mathbb{N}$ un multiple commun à a et b.
ie $m'\in a\mathbb{Z}$ et $m'\in b\mathbb{Z}$ $\Rightarrow$ $m'\in a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$
$m'\in m\mathbb{Z}\Rightarrow m'$ multiple de m $\Rightarrow$ m plus petit commun multiple de a et b.

Thm de Bezout: Soit $(a,b)\in\mathbb{Z}^2$
a et b premiers entre eux ssi $\exists(u,v)\in\mathbb{Z}^2$ tq $au+bv=1$

[$\Rightarrow$ pgcd $(a,b)=1$ ie $a\mathbb{Z}+b\mathbb{Z}=\mathbb{Z}$
$1\in\mathbb{Z}$ dc $1\in a\mathbb{Z}+b\mathbb{Z}$ ie $\exists(u,v)\in\mathbb{Z}^2$ tq $au+bv=1$

$\Leftarrow$ On suppose que $au+bv=1$
Soit d un div commun à a et b ie $a=kd$ et $b=k'd$ avec $k,k'\in\mathbb{Z}$
$1=au+bv=dku+dk'v=d(ku+k'v)$ dc $d|1$ ie $d=1$
ie pgcd $(a,b)=1$]

Thm Caractéristique du PGCD et PPCM:
Soit $(a,b)\in\mathbb{N}^2$, d un div commun à a et b tq $a=dk$, $b=dk'$, $k,k'\in\mathbb{Z}$
m — multi ——— $m=aq$, $m=bq'$, $q,q'\in\mathbb{Z}$
i) Si d est le pgcd (a,b) alors $k\wedge k'=1$
ii) Si m — ppcm (a,b) alors $q\wedge q'=1$.

[i) On suppose que d est le pgcd (a,b)
On raisonne par l'absurde et on suppose que $k\wedge k'=d'$ avec $d'>1$
ie $k=d'\tilde{k}$, $\tilde{k}\in\mathbb{Z}$ et $k'=d'\tilde{k}'$, $\tilde{k}'\in\mathbb{Z}$
donc $a=dd'\tilde{k}$ $b=dd'\tilde{k}'$
ie dd' div commun à a et b de plus $d'>1$ d $d<dd'$
ce qui contredit le fait que d soit le plus grand diviseur commun.

ii) On suppose que $m=a\vee b$. On raisonne par l'absurde et on suppose que $q\wedge q'=m'>1$
c'est dire que $m=a\,m'\underbrace{\tilde{q}}_{q}$ et $m=b\,m'\underbrace{\tilde{q}'}_{q'}$ donc m divisible par m'
dc $\frac{m}{m'}=a\tilde{q}$ et $\frac{m}{m'}=b\tilde{q}'$ dc $\frac{m}{m'}$ multiple commun de a et b de plus $m'>1$
dc $\frac{m}{m'}<m$ ABSURDE.]