Exposé 11 : PGCD et PPCM de deux entiers naturels. Nombres premiers entres eux. Applications. Illustration avec la calculatrice.

Prérequis[1] :
-Notion de diviseur multiple et de nombre premier
-Division Euclidienne dans $\mathbb{N}$
-Toute partie non vide de $\mathbb{N}$ admet un plus petit élément
-Toute suite décroissante de $\mathbb{N}$ est stationnaire à partir d'un certain rang
Cadre : $(a,b) \in \mathbb{N}^2$. On se place dans $\mathbb{N}$ (on pourra prendre $(a,b) \neq \{(0,0)\}$ pour éviter les problèmes de pgcd nons définis).

1 PGCD

1.1 Définition et calcul du PGCD

Définition : Tout entier divisant à la fois a et b est appelé diviseur commun de a et de b.

Notation : On notera $Div\{a,b\}$ l'ensemble des diviseurs communs à a et b (et $Div\{c\}$ l'ensemble des diviseurs de c, $c \in \mathbb{N}$).

Lemme : Soit r le reste de la division euclidienne de a par b, $b \neq 0$. Alors : $Div\{a,b\} = Div\{b,r\}$

Théorème : Il existe un unique entier d plus grand élément de $Div\{b,r\}$ pour la relation "est diviseur de", et on a $Div\{b,r\} = Div\{d\}$.

Définition : d est appelé le plus grand diviseur de a et b, noté $pgcd(a,b) = d$

preuve(THÉORÈME) :
Existence Si $b = 0$, $Div\{a,b\} = D\{a\}$, si $a = 0$, $Div\{a,b\} = D\{b\}$. Supposons que $a \geq b > 0$
Si $b|a$, alors $Div\{a,b\} = Div\{b\}$, sinon $\exists!(q_1,r_1)$, $a = bq_1 + r_1$, $0 \geq r_1 \geq b$ par division euclidienne. Par le lemme, on a $Div\{a,b\} = Div\{b,r_1\}$. On pose $b = r_0$, et l'on construit ainsi $(r_n)_n, (q_n)_n$ tels que $r_0 = r_1q_1 + r_2$, $r_{n-1} = r_nq_{n+1} + r_{n+1}$ avec $0 \leq r_{n+1} < r_n$. Or $(r_n)_n$ est une suite strictement décroissante et minorée (positive) de $\mathbb{N}$, donc $\exists k \in \mathbb{N}$ tel que $r_k \neq 0$ et $r_{k+1} = 0$ (et $\forall n \geq K+1$, $r_n = 0$).r_{k-1} est donc le dernier reste non nul.
Donc $Div\{a,b\} = Div\{b,r_1\} = ... = Div\{r_{k-2},r_{k-1}\} = Div\{r_{k-1}\}$.
Unicité Supposons qu'il existe deux $pgcd(a,b) = d_1$ et d_2
$d_1|a$ et $d_1|b$ or $d_2 = pgcd(a,b) \Rightarrow d_1|d_2$
$d_2|a$ et $d_2|b$ or $d_1 = pgcd(a,b) \Rightarrow d_2|d_1$ donc $d_1 = d_2$

En fait, la preuve est constructive car en plus de prouver l'existence du *pgcd*, elle nous donne une méthode pour l'obtenir.

[1] L'exposé a été présenté à Bordeaux(1) en février 2005 par Johann, corrigée par M.B, et a été tapé par Gwendal Haudebourg. Il s'inspire très largement d'un exposé de Lionel. Réalisé avec LaTeX. Mise à jour le 31/07/2007

1.2 Propriétés du PGCD

Trois propriétés importantes :

1. $pgcd(a,b) = pgcd(b,a)$ (COMMUTATIVITÉ)
2. $pgcd(na,nb) = n.pgcd(a,b)$
3. $pgcd(a, pgcd(b,c)) = pgcd(pgcd(a,b),c)$ (ASSOCIATIVITÉ))

preuve
(2) : on multiplie par n toutes les divisions euclidiennes de l'algorithme d'Euclide :
$na = nbq + nr$, $nb = nrq_1 + nr_1$, $nr = nr_1q_2 + nr_2 ... nr_{N-2} = nr_{N-1}q_N$
donc $pgcd(na,nb) = n.r_{N-1} = n.pgcd(a,b)$

Deux autres propriétés : $pgcd(a,0) = a$ et $pgcd(a,1) = 1$

1.3 Nombres premiers entres eux

Définition : a et b sont dits premiers entres eux si $pgcd(a,b) = 1$

1.3.1 Théorème de Bezout

Théorème de Bezout : a et b sont premiers entres eux $\iff \exists (u,v) \in \mathbb{Z}^2$ tels que $au + bv = 1$

preuve(THÉORÈME DE BEZOUT) :
Si $au + bv = 1$ alors toute division de a et b divise 1, donc est égale à 1, donc $pgcd(a,b) = 1$
Réciproquement, $pgcd(a,b) = 1$, donc dans l'algorithme d'euclide, $r_{N-1} = 1$
On va vérifier par récurrecne sur m que les r_m sont combinaisons linéaires de a et b
$r = a - bq$, $r_1 = b - q_1 r = b - q_1 a + bqq_1 = -q_1 a + (1 + qq_1)b$, $r_2 = r - r_1 q_2$, donc on suppose que $\forall k \leq m, \exists u_k, v_k \in \mathbb{N}$ tels que $r_k = au_k + bv_k$.
$r_{m+1} = r_{m-1} - r_m q_{m+1} = (au_{m-1} + bv_{m-1}) - (au_m + bv_m).q_{m+1} = a(u_{m-1} - u_m q_{m+1}) + b(v_{m-1} - v_m q_{m+1})$,
donc de même, $\exists (u,v)$ tq $r_{N-1} = 1 = au + bv$

Corollaire : $pgcd(a,b) = 1$ et $pgcd(a,c) = 1 \Rightarrow pgcd(a,bc) = 1$

1.3.2 Théorème de Gauss

Théorème de Gauss : Si $pgcd(a,b) = 1$ et si $a|bc$ alors $a|c$

preuve : $au + bv = 1 \Rightarrow auc + bvc = c \Rightarrow a|a$ et $a|bc \Rightarrow a|c$

2 PPCM

2.1 Définitions-Théorèmes

Définition : Tout entier multiple à la fois de a et de b est appelé multiple commun de a et b

Notation : $mult\{a,b\}$

Théorème : Il existe un unique entier m plus petit élément de $mult\{a,b\}$ pour la relation divise, tel que $mult\{m\} = mult\{a,b\}$

Définition : m est appelé le plus petit multiple commun de a et de b, et est noté $ppcm(a,b) = m$

preuve(THÉORÈME) : on suppose que a ou b n'est pas nul (si $a = b = 0 \Rightarrow m + 0$ trivial)
Existence : on a $\mu \in mult(a,b) \Leftrightarrow \exists u, v \in \mathbb{N}\ \mu = ua = vb$
Notons d le $pgcd(a,b)$ et posons $a = da'$ et $b = db'$, donc on a $ua' = vb'$ avec $pgcd(a',b') = 1$. Par Gauss, $\exists w$ tq $u = wb'$ donc $\mu = ua = wda'b'$.
Réciproquement, $\mu = wda'b'$ entraîne l'existence de u et v tq $\mu = ua = vb$, donc $\mu \in mult(a,b) \Leftrightarrow \exists w, \mu = wda'b' \Leftrightarrow \mu \in mult(da'b')$. On pose $m = da'b'$
Unicité : $mult(m) = mult(m') \Leftrightarrow \exists u, v \in \mathbb{N}$ tq $m = um'$ et $m' = vm$ d'où $m = uvm \Rightarrow m = uvm \Rightarrow u = v = 1$ car $m \neq 0$ donc $m = m'$.

2.2 Propriétés

1. $m(a,b) = m(b,a)$
2. $m(a, m(b,c)) = m(m(a,b), c)$
3. $m(ka, kb) = k.m(a,b)$

2.3 Relation entre ppcm et pgcd

Thérême : $ppcm(a,b).pgcd(a,b) = a.b$

preuve : dans le théorème, on a trouvé que $m = da'b' \Rightarrow md = da'db' = ab$

3 Applications

3.1 Fraction

Toute fraction $\frac{a}{b}$ peut s'écrire sous la forme d'une fraction irréductible :
$\frac{a}{b} = \frac{a'.pgcd(a,b)}{b'.pgcd(a,b)} = \frac{a'}{b'}$ avec $pgcd(a',b') = 1$

3.2 Equations diophantiennes

Résolution dans $\mathbb{Z}$ de $ax + by = c$, $(a,b) \in \mathbb{N}^{*2}$

L'équation admet des solutions si $pgcd(a,b)|c$
Soit $d = pgcd(a,b)$, $a = da'$, $b = db'$. $d(a'x + by') = c \Rightarrow d|c$ et $c = dc'$. $pgcd(a',b') = 1 \Rightarrow \exists (u,v) \in \mathbb{Z}^2$ tq. $a'u + b'v = 1$
d'où $a(c'u) + b(c'v) = c'$ donc $a(c'u) + b(c'v) = c$ donc $(c'u, cv)$ est solution de l'équation.
Résolution de l'équation : (x_0, y_0) solution particulière.
$\forall (x,y) \in \mathbb{Z}^2$, $a'(x - x_0) = b'(y - y_0)$. $b'|a'(x - x_0)$ et $pgcd(a',b') = 1$ implique $b'|(x - x_0)$ donc $\exists k$ tq. $x - x_0 = kb'$.
$a'|b'(y - y_0)$ et $pgcd(a',b') = 1$ implique $a'|(y - y_0)$ donc $\exists k'$ tq. $y - y_0 = a'k'$
donc $x = kb' + x_0$ et $y = k'a' + y_0$

3.3 $\sqrt{p}$, avec p premier, est irrationnel

Montrons par l'absurde que $\sqrt{p} \notin \mathbb{Q}$:
Supposons qu'il existe $(a,b) \in \mathbb{Z}^2$ tq. $\sqrt{p} = \frac{a}{b}$. On a alors $p = \frac{a^2}{b^2}$ donc $pb^2 = a^2$ donc $p|a^2$ or p premier donc $p|a$ (lemme de Gauss)
De plus, $a = pq$ donc $pb^2 = p^2q^2$, $b^2 = pq^2$ d'où $p|b$.
Or $pgcd(a,b) = 1$ d'où la contradiction (car $p|a$ et $p|b$).

4 Compléments

4.1 Un procédé de recherche : l'algorithme d'Euclide

Algorithme pour la calculatrice (on prendra comme entrée $a \geq b$, $b \neq 0$)

Entrée a, b
$a \to p$
$b \to q$
$a - E(\frac{a}{b}).b \to R$
$1 \to K$
Tant que $R \neq 0$ faire
$Q \to P$
$R \to Q$
$P - E(\frac{P}{Q}).Q \to R$
$K + 1 \to K$
Fin tant que
Afficher K, Q

ex : $pgcd(131228, 1912) = 4$, $K = 9$

4.2 Application

On peut aussi mettre les congruences comme applications (cf oral écrit 2005/2006)
Un autre point de vue peut-être pris pour cette leçon : parler de la relation d'orde "|"

4.3 Commentaires M.B.

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément : c'est ce que l'on appelle **une structure de bon ordre** (la relation d'odre sur $\mathbb{N}$ étant "|" (div. Eulclidienne$\to$ odre partiel) ou "$\leqslant$" (ordre total).

Toute ensemble peut-être muni d'une structure de bon-ordre$\Leftrightarrow$ axiome du choix
Axiome du choix : $(E_i)_i$ ensemble, $E_i \neq \emptyset$. Alors il existe f : $\begin{array}{ccc} I & \to & \bigcup_{i\in I} E_i \\ i & \mapsto & f(i) \in E_i \end{array}$

Quand (E_i) infini, on est incapable d'exhiber une telle fonction (ex : f).

4.4 Exercices supplémentaires

L'ensemble $\left\{2n+1, 2n^2+2n\right\}$ est composé de couple d'entiers premiers entres eux :
$2n^2 + 2n = n(2n+1) + n$
$n = \frac{1}{2}(2n+1) - \frac{1}{2}$
donc $2n^2 + 2n = (n + \frac{1}{2})(2n+1) - \frac{1}{2}$ donc $(2n+1)(2n+1) - 2(2n^2+2n) = 1$
d'où $pgcd(2n^2 + 2n, 2n+1) = 1$ Cela montre par ailleurs qu'il existe une infinité de couples (a, b) de nombres premiers.

De même pour l'ensemble $\left\{2n+5, n^2+5n+6\right\}$:

n^2+5n+6	$2n+5$
$\frac{5}{2}n+6$	$\frac{n}{2}+\frac{5}{4}$
$\frac{-1}{4}$	

donc $n^2 + 5n + 6 = (2n + 5)(\frac{n}{2} + \frac{5}{4}) - \frac{1}{4}$
d'où $-4(n^2 + 5n + 6) - (2n + 5)(n + 5) = 1$ d'où $pgcd(2n + 5, n^2 + 5n + 6) = 1$