PGCD, Th Bézout, Th Gauss

1 PGCD

1.1 le pgcd de deux entiers naturels

Définition : Pour tout entier naturel a , on note $D(a)$ l'ensemble de ses diviseurs.

On a : $D(1) = 1$ et $D(0) = \mathbb{N}$
$D(a)$ contient toujours 1 et a.
Lorsque $a \neq 0$, le plus grand élément de $D(a)$ est a.

Définition : Pour tous entiers naturels non nuls a et b, $D(a;b)$ est l'ensemble des diviseurs communs à a et b.

L'ensemble $D(a;b)$ est non vide, il contient toujours 1.
De plus, tous les nombres qu'il contient sont inférieurs ou égaux à a et b.
Comme toute partie non vide et majorée de $\mathbb{N}$ a un plus grand élément, $D(a;b)$ a un plus grand élément appelé PGCD de a et b.

Définition : a et b étant deux entiers non nuls. Le PGCD de a et b est noté PGCD(a ;b)

*) PGCD(a ;b)=PGCD(b ;a)
*) PGCD(a ;a)=a
*) si b divise a,alors $PGCD(a;b) = b$

exemple : $D(6;15) = \{1;3\}$ donc $PGCD(6;15) = 3$

1.2 Propriété de réduction

Propriété : Si a et b sont deux entiers relatifs non tous les deux nuls. $PGCD(a;b) = PGCD(a - kb;b)$ pour tout k de $\mathbb{Z}$

1.3 Recherche du PGCD : algorithme d'Euclide

Pour rechercher le PGCD de a et b (avec $a > b$), on utilise l'algorithme d'Euclide.

Théorème : a et b sont deux entiers naturels non nuls. La division euclidienne de a par b s'écrit : $a = bq + r$ avec $0 \leq r < b$ Alors $D(a;b) = D(b;r)$ Donc, on a : $PGCD(a;b) = PGCD(b;r)$

Démonstration

- Démontrons que si d divise a et b, alors d divise b et r.
  Si d divise a et b, d divise toute combinaison linéaire de a et b, en particulier $a - bq$, soit r.
  Il en résulte que $D(a;b) \subset D(b;r)$
- Démontrons que si δ divise b et r, alors δ divise a et b.
  Si δ divise b et r, δ divise toute combinaison linéaire de b et r, donc en particulier $bq + r$, soit a.
  Il en résulte que $D(b;r) \subset D(a;b)$
- La double inclusion équivaut à : $D(b;r) = D(a;b)$
  Ces deux ensembles de $\mathbb{N}$ sont identiques, donc ils ont le même plus grand élément.
  conclusion : $PGCD(a;b) = PGCD(b;r)$

On définit ainsi une suite d'entiers r_n telle que
$0 \leq ... < r_{k+1} < r_k < ... < r_2 < r_1 < r_0 < b$
Cette suite est une suite strictement décroissante d'entiers naturels. Donc c'est une suite finie et il existe un entier n tel que $r_n \neq 0$ et $r_{n+1} = 0$
Or $r_{n+1} = 0$ signifie que r_n divise r_{n-1}, d'où :
$PGCD(a;b) = PGCD(b, r_0) = PGCD(r_0; r_1) = ... = PGCD(r_{n-1}; r_n) = r_n$

Théorème : Lorsque b ne divise pas a, le PGCD de a et b est le dernier reste non nul dans l'algorithme d'Euclide.

Théorème : Conséquences de l'algorithme d'Euclide a et b sont deux entiers naturels non nuls. 1) L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de $PGCD(a;b)$ 2) Quel que soit l'entier $c > 0$, $PGCD(ac;bc) = c \times PGCD(a;b)$

démonstration du 1)
Dans l'algorithme d'Euclide : $D(a;b) = D(r_{n-1}; r_n) = D(r_n)$ car r_n divise r_{n-1} et $r_n = PGCD(a;b)$.

1.4 Nombres premiers entre eux

Définition : Dire que deux entiers naturels non nuls a et b sont premiers entre eux signifie que leur PGCD est égal à 1.

Théorème : a et b sont deux entiers naturels non nuls. $\Delta = PGCD(a;b) \Leftrightarrow$ il existe deux entiers a' et b' tels que $a = \Delta a'$, $b = \Delta b'$ et $PGCD(a';b') = 1$

2 Théorème de Bézout

Théorème : a et b sont deux entiers naturels non nuls. a et b sont premiers entre eux $\Leftrightarrow$ il existe deux entiers relatifs u et v tels que $au + bv = 1$

Démonstration :

- Supposons qu'il existe deux entiers u et v tels que $au + bv = 1$ et prouvons que a et b sont premiers entre eux. On note $\Delta = PGCD(a;b)$. Δ divise a et b donc Δ divise $au + bv$. Comme $au + bv = 1$, on a : $\Delta = 1$, donc a et b sont premiers entre eux.
- Supposons a et b premiers entre eux et démontrons que 1 s'écrit sous la forme $au + bv$. Soit $\mathscr{E}$ l'ensemble des nombres de la forme $au + bv$, avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$. L'ensemble $\mathscr{E}$ n'est pas vide car pour $u = 1$ et $v = 0$, $a \in \mathscr{E}$. (vrai aussi pour b) (rappel : Toute partie non vide de $\mathbb{N}$ contient un plus petit élément.)
  Ainsi $\mathscr{E}$ contient des entiers strictement positifs, et parmi eux, un plus petit que tous les autres. Notons $m = au_1 + bv_1$ ce plus petit élément. La division euclidienne de a par m s'écrit $a = mq + r$ avec $0 \leq r < m$ soit $r = a - mq = a - (au_1 + bv_1)q = a(1 - u_1q) + b(-v_1q)$.
  Ainsi $r \in \mathscr{E}$. Or m est le plus petit entier strictement positif de $\mathscr{E}$, donc $r = 0$. Ainsi, m divise a. On montre de même que m divise b.
  Comme a et b sont premiers entre eux, $m = 1$ et $au_1 + bv_1 = 1$

Exemple $a = 89$ et $b = 41$. Comment trouver u et v ?

Théorème (autre caractérisation du PGCD)
a et b sont deux entiers naturels non nuls.
$PGCD(a;b) = \Delta \Leftrightarrow \Delta$ est un diviseur de a et b et il existe deux entiers relatifs u et v tels que $\Delta = au + bv$

Démonstration :

- Supposons que Δ est le PGCD de a et b. Alors, par définition, Δ est un diviseur de a et b. De plus, il existe deux entiers naturels a' et b' tels que $a = \Delta a'$ et $b = \Delta b'$ et $PGCD(a';b') = 1$. Donc, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $a'u + b'v = 1$.
  Donc $\Delta a'u + \Delta b'v = \Delta$, soit $au + bv = \Delta$.
- Supposons que Δ divise a et b et qu'il existe des entiers relatifs u et v tels que $au + bv = \Delta$. Notons δ le PGCD de a et b. Δ divise a et b donc $\Delta \leq \delta$. Et puisque δ divise a et b, δ divise $au + bv = \Delta$, d'où $\delta \leq \Delta$.
  Donc $\Delta = \delta$ et $\Delta = PGCD(a;b)$

3 Théorème de Gauss

Théorème : a,b,c sont des entiers strictements positifs. Si a divise bc et a est premier avec b, alors a divise c.

Démonstration : Puisque a et b sont premiers entre eux, d'après le th de Bézout, il existe deux entiers relatifs u et v tels que : $au + bv = 1$ d'où $(ac)u + (bc)v = c$
Or a divise ac et bc donc a divise acu+bcv donc a divise c.

Corollaire du théorème de Gauss :
Si un entier naturel n est divisible par deux entiers naturels a et b premiers entre eux, il est divisible par leur produit.

Démonstration : Par hypothèse $n = aq$ et $n = bq'$ avec q et q' entiers naturels. Donc $aq = bq'$
Puisque b divise aq et que b est premier avec a, b divise q, donc $q = bp$ et $n = abp$ donc ab divise n

Application : Montrer que pour tout $n > 1$; $(n-1)n(n+1)$ est divisible par 6.