I. PLUS GRAND DIVISEUR COMMUN

a) Définition pgcd

Soient a et b deux entiers positifs non nuls :
le plus grand des diviseurs communs à a et à b est appelé pgcd de a et de b, noté pgcd(a,b)

Exemple : Déterminer le PGCD et 18 et de 30.

Cas où l'un des deux est nul ?

PROPRIETE : Pour a ≠ 0, pgcd(a,0) = a

Dem : tous les entiers sont diviseurs de 0 ;
Les diviseurs communs à 0 et a sont les diviseurs de a, dont le plus grand est a.

2. Premières propriétés :

soient a et b deux entiers naturels tels que a > b.

*** pgcd(a,b)= pgcd(b,a)**
*** si a divise b alors pgcd(a,b) = a**
*** PGCD (ka, kb) = k pgcd (a,b)**

3. Nombres premiers entre eux :

Définition : Deux entiers a et b sont premiers entre eux lorsque pgcd(a,b) = 1.

Exemple : pgcd(18;35) =1

II. ALGORITHMES

1. Algorithme par soustraction :

Propriété des diviseurs : si c divise a et b alors c divise ua+vb,
En particulier: si c divise a et b alors c divise a+b, a-b, (mais aussi 2a+3b, 5a-4b , ...)

PROPRIETE : **pgcd(a,b) = pgcd(a-b,b)**

On doit ici démontrer l'égalité de deux ensembles :
L'ensemble des diviseurs communs à a et b = l'ensemble des diviseurs communs à a-b et b:
Or dans deux ensembles contenant les mêmes éléments, le plus grand élément est le même!
Le procédé général est de démontrer une « double inclusion » :
chaque élément de l'un est contenu dans l'autre ; et réciproquement, chaque élément de l'autre est contenu dans l'un. Les deux ensembles sont alors bien identiquement les mêmes.

Dem : si d divise a et b alors d divise aussi a-b → si d divise a et b alors d divise b et a-b ;
si d divise b et a-b alors d divise aussi a → si d divise b et a-b alors d divise a et b
→ {div (a,b)} = {div(a-b;b) } → pgcd(a,b) = pgcd(a-b,b)

Exemples :
1) PGCD (245, 105) = PGCD (105, 140) =PGCD (105, 40) = PGCD(40, 65) =PGCD(40, 25)
=PGCD (25, 15) = PGCD (15, 10) = PGCD(10, 5) = PGCD (5, 0) = 5
2) Soit n un entier non nul. Déterminer le PGCD de 2n et 2n+1 :

2. Algorithme d'Euclide :

PROPRIETE :	**Soient a et b deux entiers naturels** **Si a = b q + r alors pgcd(a ; b) = pgcd(b ; r)**

Démonstration :
si d divise a et b alors (PROP) d divise aussi r = 1.a-q.b
=> si d divise a et b alors d divise b et r ;
si d divise b et r alors d divise aussi a = qb+1r
=> si d divise b et r alors d divise a et b
d'où {div (a,b)} = {div(b,r) }
donc pgcd(a,b) = pgcd(b,r)

Remarque intéressante : cette propriété est valable si a=bq+r, même si la condition $0 \nleq r \nleq b-1$ n'est pas respectée (donc même si ce n'est pas une écriture de division euclidienne);

Autre remarque : En particulier, en écrivant a=1*b + (a-b), on retrouve la propriété « pgcd et soustraction ». Mais l'algorithme d'Euclide est plus rapide.

Exemple : pgcd(145,15) = pgcd(15,10) = pgcd (10,5) = pgcd(5,0) = 5

III. PGCD ET DIVISIBILITÉ

PROPRIETE :	**pgcd(ka,kb) = k*pgcd (a,b)**

Démonstration :
L'égalité a= b q + r équivaut à ka = k b q + k r, donc pgcd(ka , kb) = pgcd (kb , kr)
Conséquence : la succession d'égalités de l'algorithme d'Euclide conduit à un dernier reste non nul égal à k* ….

PROPRIETE :	**si d divise a et b alors d divise pgcd(a,b)**

Démonstration :
Si d divise a et b alors a = da' et b = db' donc pgcd(a,b) = d*pgcd(a',b')
ce qui montre que d divise pgcd(a,b)
la réciproque est évidente :
si d divise le pgcd de a et de b, comme le pgcd de a et b est lui-même un diviseur de a (et de b), par transitivité d divise a (et b)

PROPRIETE : CARACTERISATION DU PGCD **pgcd(a,b)= Δ Si et Seulement Si a=Δ a' et b=Δ b' avec pgcd(a' , b')=1** (C'est à dire a' et b' premiers entre eux)

Démonstration : on va montrer la double implication
* Si **Δ** = pgcd(a,b) alors a=**Δ**a' et b=**Δ**b' et l'égalité pgcd(a,b) = **Δ***pgcd(a',b') = **Δ** donne pgcd(a',b') = 1
* Réciproquement, si a=**Δ**a' et b=**Δ**b' avec pgcd (a', b')=1 alors pgcd(a,b) = **Δ***pgcd(a',b') = **Δ***1 = **Δ.**

Exemple : Pgcd(18,30) = 6 et on a bien 18=6*3 et 30=6*5 avec 3 et 5 premiers entre eux.

II. Le théorème de BEZOUT

1. Identité de BEZOUT

Soient a et b deux entiers naturels non nuls.
Si d = PGCD (a ;b)
Alors il existe des nombres entiers relatifs u et v tels que au + bv =d.

!!! Le couple (u ;v) n'est pas unique !!!

Démonstration : - voir livre

2. Théorème de BEZOUT

Soient a et b deux entiers naturels non nuls.
Dire que a et b sont premiers entre eux EQUIVAUT à DIRE qu'il existe deux entiers relatifs u et v tels que au + bv = 1.

Démonstration : => et <=
- voir livre.

Exercice 1 : Comment trouver les coefficients de Bezout u et v ?
A = 145 et b =55 déterminer u et v tels que au+bv = 1
ETAPE 1) algo d'euclide pour calculer PGCD de a et b.

a	b	reste	
145	55	35	145 = 55x2 + 35
55	35	20	55 = 35 x1 + 20
35	20	15	35 = 20 x1 + 15
20	15	5	20 = 15 x 1 + 5
15	5	0	15 = 5 x 3

Donc PGCD (a ; b) = 5

ETAPE 2) On remonte l' algo d'euclide
5 = 20 – 15 x 1 or 15 = 35 – 20 x 1
D'où 5 = 20 – (35 – 20 x 1) x1
5 = -35 + 20 x 2

or 20 = 55 – 35 x 1
D'où 5 = -35 + (55 – 35 x 1) x 2
5 = 55 x 2 – 35 x 3

Or 35 = 145 – 55 x 2
D'où 5 = 55 x 2 – (145 – 55 x 2) x 3
5 = 55 x 2 – 145 x 3 + 55 x 6
5 = 55 x 8 – 145 x 3

Donc : **5 = 55 x 8 +145 x (-3)**

Exercice 2 : Démontrer que deux nombres sont premiers entre eux.

n désigne un nombre entier naturel non nul. Démontrer que a = 2n+1 et b = 3n + 2 sont premiers entre eux.

FABRIQUER UNE COMBINAISON LINEAIRE : - 3a +2b = …….. = 1
Donc d'après le théorème de BEZOUT, 2n+1 et 3n+2 sont premiers entre eux.

III. Théorème de Gauss :

Théorème de Gauss

Soient a, b et c des entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux alors a divise c.

Si a | bc et pgcd(a ;b) = 1 Alors a | c

$$\begin{cases} a \mid bc \\ \text{et} \\ \text{pgcd}(a\ ;b) = 1 \end{cases} \Leftrightarrow \quad a \mid c$$

On s'en sert pour résoudre des équations du type : $7x - 11y = 0$ avec x et y des entiers relatifs.

- Si $7x = 11y$ alors 11 divise 7x.
  Or 7 et 11 sont premiers entre eux, donc d'après les théorème de Gauss 11 divise x.
  Par conséquent, il existe un entier relatif k tel que $x = 11k$.
  Et l'équation devient : $7.11k = 11y$ soit $7k = y$
- Réciproquement :
  Tous les couples $(11k ; 7k)$ sont solutions de $7x = 11y$.
  En effet : $7 . 11k = 11 . 7k$.

CONCLUSION : Les solutions de l'équation $7x - 11y = 0$ sont les couples $(11k ; 7k)$ avec $k \in \mathbb{Z}$

Et son Corollaire :

Soient a, b et c des entiers relatifs non nuls.
Si b et c sont premiers entre eux et divisent a alors bc divise a.