Grands théorèmes de l'arithmétique

I- PGCD , algorithme d'Euclide

1) Pgcd

Définition : Soient a et b deux entiers non nuls

- L'ensemble des diviseurs communs à a et à b possède un plus grand élément noté pgcd(a,b) (*plus grand commun diviseur*)
- Deux entiers sont premiers entre eux si et seulement si leur pgcd vaut 1

Première conséquence : Soient a et b deux entiers non nuls et d leur pgcd. d divise donc a et b d'où $\begin{cases} a = da' \\ b = db' \end{cases}$

avec a' et b' **entiers premiers entre eux**.

Propriétés :

1) **pgcd(a,b) =** $|b|$ **⇔ b divise a**
2) **pgcd(a,b) =** $pgcd(|a|,|b|)$
3) **soit k un entier naturel non nul. pgcd (ka , kb) = k pgcd (a , b) .**

Preuve :

2) Calcul effectif du pgcd

Lemme d'Euclide :

Soient a et b deux entiers naturels non nuls

Si a = bq+ r alors pgcd (a , b) = pgcd (b , r)

Preuve : Si c divise a et b alors c divise toute combinaison linéaire de a et b donc c divise a − bq = r

Réciproquement, si c divise b et r alors c divise bq+r = a. Ainsi l'ensemble des diviseurs communs à a et à b et celui des diviseurs communs à b et à r sont les mêmes. Ils possèdent donc le même plus grand élément.

Théorème (algorithme d'Euclide) :

L'itération du théorème précédent permet de trouver le pgcd de a et b comme le dernier reste non nul .

Preuve :

Conséquence : Un théorème fondammental : Ensemble de diviseurs communs à deux entiers

Soient a et b deux entiers naturles non nuls

L'ensemble des diviseurs de a et de b est l'ensemble des diviseurs de PGCD(a;b)

Démonstration

II- Grands théorèmes de l'arithmétique

1) Le Théorème de Bezout

a) Identité de Bezout

Identité de Bezout

a et b désignent deux entiers relatifs non nuls.

Si d = PGCD(a;b) alors il existe des entiers relatifs u et v tels que **au + bv = d**

Démonstration

Remarque :

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

  Par exemple, pour a=3 et b=2, on obtient PGCD(2;3)=1 et $1 \times 3 - 1 \times 2 = 1$ ou encore $-1 \times 3 + 2 \times 2 = 1$

- **La réciproque est fausse**

  Pour a = 4 et b = 5 , on a $3 \times 4 - 2 \times 5 = 2$ et pourtant PGCD(4;5)≠2

b) Le théorème de Bezout

Théorème de Bezout

Deux entiers relatifs a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que au + bv = 1

Démonstration

Remarque : Un théorème qui permet de montrer facilement que deux entiers sont premiers entre eux

Par exemple, pour tout entier naturel n non nul, n et 2n+1 sont premiers entre eux car $(2n+1) \times 1 - n \times 2 = 1$

2) Le théorème de Gauss

a) Le théorème

Théorème de Gauss

a , b et c désignent trois entiers relatifs non nuls.

Si **a divise le produit bc** et si **a est premier avec b** alors **a divise c**

Démonstration

b) Conséquences

Propriété: a , b et c désignent trois entiers relatifs non nuls

Si **b et c sont premiers entre eux et divisent a** alors **bc divise a**

Démonstration

Exemple :

Le nombre 1 573 875 est divisible par 5 puisqu'il se termine par 5 et il est divisible par 9 car la somme de ses chiffres est divisible par 9. Or 5 et 9 sont premiers entre eux donc 1 573 875 est divisible par 9×5 cad 45