II PGCD et algorithme d'Euclide

- **Notation.** Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a. *Exemple :* $\mathscr{D}(4) =$ $\mathscr{D}(0) =$

1 Définition du PGCD

Définition 1

Soient $a, b \in \mathbb{Z}$ avec $(a,b) \neq (0,0)$. On appelle PGCD de a et b le :

On le note :

Exemple 1 — Calculer le PGCD de 16 et 12.

- **Remarques:** 1. Si $a \in \mathbb{N}^*$: $a \wedge 0 =$ 2. Par convention : $0 \wedge 0 =$
- **Remarque.** On peut toujours supposer a et b positifs car : $a \wedge b =$

Théorème 1

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{Z}$:

Exercice 1 — Etablir l'égalité pour $b \neq 0$.

Exemple 2 *SF 6* — Soit $n \in \mathbb{Z}$. Montrer : $(7n-5) \wedge (3n+2) = (n-9) \wedge 29$.

2 Algorithme d'Euclide pour le calcul du PGCD

- **Objectif.** Etant donnés $a, b \in \mathbb{N}^*$, on cherche à écrire un algorithme pour calculer $a \wedge b$.

Algorithme d'Euclide

On définit une suite finie (r_k) d'entiers naturels. On pose : $r_{-1} = a$ et $r_0 = b$.

- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la D.E. de r_{k-1} par r_k *i.e.*

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :*
2. *L'algorithme fournit le PGCD :*

Exercice 2 — Démontrer les deux points du théorème.

Exemple 3 *SF 5* — Calculer $1659 \wedge 504$

3 Propriétés du PGCD

Théorème 3 : Relation de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe $(u,v) \in \mathbb{Z}^2$ tel que :

Exemple 4 *SF 5* — Déterminer une relation de Bézout entre $a = 1659$ et $b = 504$.

Idée de la preuve du théorème dans le cas où $a, b \in \mathbb{N}^*$. Par récurrence double sur k, on montre que pour tout $k \in [\![-1, n]\!]$, il existe $u_k, v_k \in \mathbb{Z}$ tels que $r_k = au_k + bv_k$. Lorsque $k = n$, on obtient la relation désirée : $a \wedge b = r_n = au_n + bv_n$. □

Exemple 5 ☢ ***Attention*** ☢ — Donner deux relation de Bézout entre les entiers $a = 4$ et $b = 6$.

Théorème 4 : Les diviseurs communs sont les diviseurs du PGCD

Soient $a, b \in \mathbb{Z}$. Pour tout $d \in \mathbb{Z}$:

Exercice 3 — Démontrer l'équivalence ci-dessus.

- **Reformulation.** La relation de divisibilité | est une relation d'ordre sur $\mathbb{N}$. Lorsque $a, b \in \mathbb{N}$, le théorème affirme que $a \wedge b$ est le plus grand élément de l'ensemble des diviseurs communs à a et b au sens de la divisibilité

Théorème 5 : Factorisation

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{N}^*$:

Exercice 4 *SF 6* — Démontrer la relation ci-dessus.