

**TD no 8**  
**Théorème de Bezout**  
**Algorithme d'Euclide Etendu**

**Théorème 1 (Identité de Bezout)** Soient  $a$  et  $b$  deux entiers relatifs et  $d$  leur PGCD alors il existe deux entiers  $u$  et  $v$  tels que :  $au + bv = d$ .

**Théorème 2 (Résolution d'une équation diophantienne)** Soient  $a$ ,  $b$  et  $c$  des entiers, et  $d$  le PGCD de  $a$  et  $b$ , alors l'équation  $au + bv = c$  admet des solutions entières si et seulement si  $c$  est un multiple de  $d$ .

**Théorème 3 (Théorème de Bezout)** Soient  $a$  et  $b$  deux entiers relatifs non nuls.  $a$  et  $b$  sont premiers entre eux si, et seulement si, il existe deux entiers  $u$  et  $v$  tels que  $au + bv = 1$ .

**Proposition 1 (Solutions multiples pour  $u$  et  $v$ )** Il n'y a pas solution unique pour  $(u, v)$ , mais une infinité  $(u + kb, v + ka)$  avec  $k \in \mathbb{Z}$

**Théorème 4 (Théorème de Gauss)** Si un nombre  $a$  divise un produit de facteurs et si  $a$  est premier avec l'un des deux facteurs alors  $a$  divise le deuxième facteur.

L'algorithme d'Euclide permet de calculer le P.G.C.D. de deux entiers naturels  $a$  et  $b$  tels que  $a > b$ . Il consiste à répéter les manipulations suivantes :

\* Effectuer la division euclidienne de  $a$  par  $b$ . Soit  $r$  le reste.

\* Remplacer  $a$  par  $b$  et  $b$  par  $r$ . On a  $b > r$  d'après la définition de la division euclidienne.

Le P.G.C.D. est le dernier reste non nul.

L'algorithme d'Euclide Etendu permet de calculer les coefficients  $u$  et  $v$  de Bezout.

$r_{-2} := b; r_{-1} := a; u_{-2} := 0; u_{-1} := 1; v_{-2} := 1; v_{-1} := a \operatorname{div} b$

$k := -1$

Tant que  $r_k > 0$  faire

Début

$k := k + 1$

$r_{k-2} = q_k r_{k-1} + r_k$  (avec  $q_k = r_{k-2} \operatorname{div} r_{k-1}$  et  $r_k = r_{k-2} \operatorname{mod} r_{k-1}$ )

$u_k := u_{k-2} - q_k u_{k-1}$

$v_k := v_{k-2} - q_k v_{k-1}$

On a la relation:  $r_k = au_k + bv_k$

Fin

$u = u_{k-1} q_k$

$v = v_{k-1} q_k$

**Exercice 1 [ Algorithme d'Euclide ]**

- Appliquez l'algorithme d'Euclide pour trouver le ppcd de 112 et 84.
- Prouvez que l'algorithme d'Euclide donne bien le ppcd.

**Exercice 2 [ Algorithme d'Euclide étendu ]**

- Appliquez l'algorithme d'Euclide étendu pour trouver  $u$  et  $v$  tels que

$$35u + 13v = 1.$$

- Prouvez que l'algorithme d'Euclide étendu donne bien les coefficients  $u$  et  $v$  de Bezout.

**Exercice 3 [ Théorème de Gauss ]**

Démontrez le théorème de Gauss.