# *Projet*

# Calcul de PGCD, Identité de Bézout, Algorithmes de calculs.

Jean-Paul CALVI

Briefing :

- Définition pgcd

- Méthodes de calcul du pgcd : décomposition en facteurs premiers, algorithmes « des différences »

- Tout polynôme est scindé sur C. Sur R, on peut scinder un polynôme en binôme de degré 1 et trinôme de e degré 2 à discriminant négatif.

Plan du projet :

I-Anneaux des entiers/Anneaux des polynômes

(Z,+, .) (K[X],+, .)

- Définitions de ces deux anneaux

- Théorème de la division euclidienne (démontrer l'existence et l'unicité)

II-PGCD

- Définition du PGCD (pour les polynômes : c'est le polynôme unitaire de plus haut degré qui divise les polynômes considérés).

- Calcul du pgcd à partir de la décomposition en facteurs premiers/polynôme irréductible.

- Théorème fondamental : aZ+bZ= pgcd(a,b)Z

$$P(X)*K[X] + Q(X)*K[X] = pgcd(P(X),Q(X))*K[X]$$

- Corollaire : l'identité de Bézout : au+bv=pgcd(a,b)

Si a et b sont premiers entre eux alors il existe u et v tels que au+bv=1

III-Applications

- Calculer les inverses modulo n (via Bézout) où n est premier

- Soit une pièce rectangulaire de longueur L et de largeur l, on cherche le longueur du côté des carreaux les plus grand possibles qu'on puisse mettre pour recouvrir toute le pièce

- Applications de l’arithmétique des polynômes ?

IV-Algorithmique

Algorithme « des différences » (à démontrer)

Algorithme d’Euclide (à démontrer et programmer sur tableur et sur un autre logiciel)

Algorithme d’Euclide amélioré : en plus du pgcd il donne les coefficients de l’identité de Bézout.

Ouvrage :

*Mathématiques pour le calcul formel* de Maurice MIGNOTTE

*Mathématiques pour le CAPES et l’Agrégation interne* de Jean de BIASI