Leçon n° 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Soit A un anneau commutatif intègre.

I/ Notion de PGCD et PPCM dans différents types d'anneaux.

A/ Premières définitions et cas des anneaux factoriels. [ROM]

Définition 1 : Définition du PGCD et du PPCM, commutativité et associativité.

Remarque 2 : Les PGCD et PPCM sont uniques à association près.

Proposition 3 : $ab = (a \wedge b)(a \vee b)$.

Remarque 4 : Connaître le PGCD, c'est connaître le PPCM.

Exemple 5 : $(1-i \wedge 2+i) = 1-i$ dans $\mathbb{Z}[i]$, $2 \wedge 3 = 1$ dans $\mathbb{Z}$.

Proposition 6 : Existence des PGCD et PPCM dans les anneaux factoriels et expression.

Corollaire 7 : Homogénéité du PGCD et du PPCM.

Définition 8 : Premiers entre eux dans leur ensemble.

Proposition 9 : Lemme de Gauss.

Définition 10 : Le PGCD dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.

B/ Situation dans les anneaux principaux. [ROM]

Proposition 11 : Les anneaux principaux sont factoriels donc existence du PGCD et du PPCM.

Proposition 12 : Expression en termes d'idéaux.

Corollaire 13 : Si δ est le PGCD de $a_1, \dots, a_r$, alors il existe $u_1, \dots, u_r$ tels que $\sum_{i=1}^{r} u_i a_i = \delta$.

Théorème 14 : Théorème de Bézout.

Remarque 15 : Réciproque fausse : par exemple $3(2) + 2(-2) = 2$ et $2 \wedge 3 = 1$.

Application 16 : Résolution d'équations diophantiennes $ax + by = c$.

Application 17 : Lemme des noyaux.

Corollaire 18 : Si $a \wedge c = 1$, alors $a \wedge b = a \wedge (bc)$.

Théorème 19 : Théorème des restes chinois et expression réciproque.

Application 20 : Systèmes de congruence sur $\mathbb{Z}$.

Application 21 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n!H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

Application 22 : Le polynôme interpolateur de Lagrange est solution du système de congruence $P \equiv y_i \mod (X - x_i)$.

Proposition 23 : $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/(n \wedge m)\mathbb{Z} \times \mathbb{Z}/(n \vee m)\mathbb{Z}$.

II/ Cas des anneaux euclidiens : algorithmes de calcul.

A/ Algorithme d'Euclide. [ROM] [DEM]

Lemme 24 : Lemme d'Euclide.

Algorithme 25 : Algorithme d'Euclide dans les anneaux euclidiens.

Application 26 : $X^{p^n} - X \wedge X^{p^m} - X = X^{p^{n \wedge m}} - X$.

Algorithme 27 : Algorithme d'Euclide étendu.

Application 28 : Inverse dans les corps de rupture.

Algorithme 29 : Algorithme binaire.

B/ Coût de l'algorithme dans $\mathbb{Z}$ et $\mathbb{K}[X]$. [DEM]

Proposition 30 : Théorème de Lamé.

Corollaire 31 : L'algorithme d'Euclide étendu pour deux éléments a et b dans $\mathbb{Z}$ nécessite $O(\min(\log(a),\log(b)))$ opérations dans $\mathbb{Z}$.

Proposition 32 : L'algorithme d'Euclide étendu pour deux polynômes A et B nécessite $O((\deg(A)+1)(\deg(B)+1))$ opérations dans $\mathbb{K}$.

III/ Applications à d'autres domaines des mathématiques.

A/ Facteurs invariants. [OBJ]

Développement 1

Proposition 33 : Forme normale de Smith : existence et unicité.

Application 34 : Base adaptée.

Application 35 : Théorème de structure des groupes abéliens finis.

B/ Factorisation des polynômes sur un corps fini. [OBJ]

Développement 2

Algorithme 36 : Algorithme de Berlekamp.

Références :

- [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 224 et p. 237-251
- [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244 et p. 285
- [DEM] Demazure Cours d'Algèbre p. 33-42