142 - PGCD et PPCM, algorithmes de calcul. Applications.

➤ Références	[Ulmer], [Obj_pas_chômage], [Perrin], [Combes], [Saux-picard]
📁 Section	Algèbre
📅 Date	@10 décembre 2024
☰ Statut leçon	Plan détaillé ok
☰ Enseignant	Lionel Fourquaux
➤ Développement choisis	Algorithme de Berlekamp, Forme normale de Smith (euclidien).
🔍 Nb choisis	2
➤ Autres développements à case comme item	Entiers de Gauss et Théorèmes des deux carrés.
➤ Développements	Algorithme de Berlekamp

Rapport de Jury

- différencier cadre théorique selon type anneau (dans le cadre principal pas d'algorithme contrairement à euclidien)
- $\mathbb{Z}$, $K[X]$ comme exemples
- algorithme: euclide, binaire, euclide étendu (remontée), évaluer nbr étapes et lien Fibonacci
- relation Bézout, équation diophantienne, inversion modulo, calcul inverse dans corps rupture et corps finis
- théorème chinois effectif, résolution systèmes congruence
- lien interpolation Lagrange
- plus loins: berlekamp, existence supplémentaire d'une droite dans $\mathbb{Z}^2$, compéler vecteur en une base, matrice à coeff dans un anneau, Hermite Smith et théoèreme base adapté et lien théorème invariants de similitudes, $\mathbb{Z}[X]$, $K[X,Y]$, résultant

Introduction

- relation de divisibilité: naturel de chercher le plus grand ou plus petit élément
- étend notion de pgcd connu sur les entiers à d'autres éléments

Plans

▼ Plan

Cadre: A anneau commutatif unitaire

I. Notion de pgcd et de ppcm

1. Définitions
2. Dans un anneau factoriel
3. Dans un anneau principal
4. Dans un anneau euclidien

II. Calcul algorithmique de pgcd

1. Algorithme d'Euclide
2. Algorithme d'Euclide étendu
3. Algorithme binaire

III. Applications à l'étude des polynômes

IV. Résolution d'équations et systèmes d'équations

1. Système de congruences
2. Smith
3. Exemple de résolution des deux carrés dans certains cas 1009 et $540+i$ dans $\mathbb{Z}[i]$

▼ Plan détaillé

▼ I.1. Définition

→ Ulmer / Perrin

- définition pgcd /ppcm [Ulmer]
- rq: définit par récurrence pgcd/ppcm de n éléments
- contre ex: existent pas toujours + ex [Perrin exo 4]
- rq quand existent: pas toujours uniques mais dans anneau intègre: sont associés: "def qu'aux inversibles près"
- prop: c est un ppcm ssi (a) inter (b) = (c). Admettent un ppcm ssi (a) inter (b) principal
- prop: dans un anneau intègre, si (a) + (b) principal = (d) alors d est un pgcd
- prop: A intègre: admet ppcm = > admet pgcd tq $ab = \text{ppcm} * \text{pgcd}$ (pas convaincue) **ref ?**
- def: a et b sont premiers entre eux si 1 est un pgcd

▼ I. 2. Dans un anneau factoriel

→ Ulmer

- def anneau factoriel [Ulmer] + ex anneau factoriel: $K[X_1, \dots, X_n, \dots]$ factoriel [Perrin un peu caché]+ décomposition avec valuation (irréductible=premier) [Ulmer]

- prop: dans un anneau factoriel: un pgcd et un ppcm d'éléments non nuls existent et sont donnés par truc avec valuation [Ulmer]
 - (toujours pas unique)
 - lemme d'Euclide et de Gauss [Ulmer]
 - petite app: genre cours de Théo intro ou l'ordre d'un produit ou cyclicité du groupe multiplicatif d'un corps fini. A définir, à mettre ici ou ailleurs
- ▼ I. 3. Dans un anneau principal
- définition anneau principal [Ulmer]
 - principal $\Rightarrow$ factoriel + contre ex $K[X, Y]$
 - décomposition de Bézout + identité de Bézout (Perrin, Ulmer, Combes)
 - contre ex dans $K[x, Y]$ [Perrin]
 - app: les inversibles de Z/nZ sont les éléments premiers avec n **ref ?**
 - app: lemme des noyaux **ref ?**
- ▼ I.4. Dans un anneau euclidien
- def euclidien et stathme [Ulmer]
 - ex Z , $K[X]$ et $Z[i]$ sont euclidiens avec stathme $|x|$, $\deg$, $N(z) = a^{**2} + b^{**2}$
 - euclidien $\Rightarrow$ principal + contre ex $Z[\frac{1+i\sqrt{19}}{2}]$ [Perrin]
 - rq/oral: connaît algorithme pour avoir relation de Bézout
- ▼ II. Algorithmes de calculs
- Algo Euclide:
 - $\rightarrow$ Saux Picard ?
 - principe: $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ avec division euclidienne
 - algorithme en annexe
 - complexité dans Z
 - ex ludique avec obj savoir si premiers entre eux
 - Algo d'Euclide étendu
 - principe
 - ex inversion dans quotient Ulmer exemple 4.42 ou exo 4.9 est-ce que peut faire avec euclide normal ? A tester ?
 - Algo binaire **ref ? (Sopiquet exo)**
 - principe et complexité (savoir pas si mal ordi)
 - ex ?
- ▼ III. 1. Contenu
- $\rightarrow$ Perrin ou Combes bien
 - définition contenu
 - contenu multiplicatif A^*
 - critère d'irréductibilité
 - (si devient fort: A factoriel $\Rightarrow A[X]$ factoriel)
 - app: Eisenstein ? Utilise démo Enoncé et c-ex ?
- ▼ III.3. Berlekamp
- $\rightarrow$ Objectif agreg
 - DEV
 - (oral: calcul des pgcd avec euclide)

- énoncé et exemple
- rq complexité de merde Lionel de merde
- cas avec facteur carrés

▼ IV.1. Systèmes de congruences

° La base

- équation diophantienne simple dans $\mathbb{Z}$: quand solution et expression solution ref ?
- app: résolution système 2×2 ref ?

° Pour les plus grands

- théorème chinois avec réciproque (Objectif Agreg sûrement)
- résolution d'un système de plus grande taille ref ?
- Problème des pirates ref ?

▼ VI. 2. Résolution de systèmes linéaire

→ Ref ? Objectif agreg à priori

- théorème de décomposition Smith DEV
- (rq ; généralisation d'euclide)
- ex ludique de résolution ou après Frobenius
- rq : reste vrai dans anneau principal mais on n'a plus l'algo
- app: Calcul d'invariant Frobenius

▼ VI. 3. Ex des deux carrés

- utilisation d'Hermite pour résoudre système de congruence / equa diophantienne demander à Martin
- garder en tête: calcul de résultant via algo d'Euclide
- regarder algorithme de Garner dans Ulmer: application interpolation polynomiale, partage de secrets