Nom:

MARIT

Prénom:

Amaël

Numéro de Jury:

1

Numéros des sujets tirés:

101 / 142

Intitulé du sujet choisi:

142 - PGCD et PPCM. Algorithmes de calcul. Applications

I- Cadre théorique

1- Anneaux à pgcd

On fixe A un anneau (commutatif unitaire)

Définition 1 (pgcd, ppcm) : Soit $(a,b) \in A$

On appelle pgcd de a et b tout élément $g \in A$ tel que :

(i) $g \mid a$ et $g \mid b$

(ii) $\forall d \in A$, $d \mid a$ et $d \mid b \Rightarrow d \mid g$

On appelle ppcm de a et b tout élément $m \in A$ tel que $a \mid m$ et $b \mid m$ et si $m \in A$ est tel que $a \mid m$ et $b \mid m$, $m \mid m$

Remarque 2 : un pgcd et un ppcm est défini modulo l'association

Exemples 3 : 2 et -2 sont des pgcd de 4 et 6 dans $\mathbb{Z}$. Dans $\mathbb{Z}[\sqrt{3}]$, 4 et $2(1+\sqrt{3})$ n'ont pas de pgcd

Définition 4 (anneau à pgcd) : A est dit à pgcd si tout couple non nul d'éléments de A admet un pgcd.

Lemme 5 : A est à pgcd si, et seulement si, tout couple non nul d'éléments de A admet un ppcm

Lemme 6 : Soit $(a,b) \in A^2$ des éléments d'un anneau à pgcd premiers entre eux pour $x \in A$ non nul. Pgcd$(xa, xb) = x$.

Définition 7 (éléments irréductibles, premiers)

Soit $p \in A \setminus \{0\}$ non inversible. On dit que p est

(i) irréductible si $p = ab \Rightarrow a$ ou $b \in A^\times$

(ii) premier si $\langle p \rangle$ est un idéal premier

Théorème 8 (Gauss)

Si A est à pgcd et $(a,b,c) \in A^3$ sont tels que

(i) pgcd$(a,b) = 1$

(ii) $a \mid bc$

Alors $a \mid c$.

Corollaire 9 :

Dans un anneau à pgcd tout élément irréductible est premier. La réciproque est vraie en toute généralité

Théorème 10 : Un anneau factoriel est à pgcd

Application 11 $\mathbb{Z}[X]$ et $K[X,Y]$ (où K est un corps) sont à pgcd

2- Domaines de Bézout

Définition 12 (Domaine de Bézout) : Un anneau A est appelé domaine de Bézout si (i) A est intègre

(ii) Tout idéal de type fini de A est principal

Théorème 13 (Bézout) : Soit A un domaine de Bézout. Soit $(a,b) \in A^2$. Alors :

(i) a et b admettent un pgcd si $(a,b) \neq (0,0)$

(ii) dans ce cas, il existe u et $v \in A$ tels que

$$au + bv = 1$$

Exemples 14 : $\mathbb{Z}$ est un domaine de Bézout

$K[X,Y]$ est à pgcd mais n'est pas un domaine de Bézout.

Remarque 15 : Soient a et b des éléments d'un domaine de Bézout non tous deux nuls. Alors $g \in A$ est un pgcd de a et b si, et seulement si :

$$\langle a \rangle + \langle b \rangle = \langle g \rangle$$

Application 16 : Soit $n \in \mathbb{Z} \setminus \{0\}$. Un entier $k \in \mathbb{Z}$ est inversible modulo n si, et seulement si, pgcd$(n,k) = 1$

Intercalaire N°

Définition 17 (éléments comaximaux)
Deux éléments a et b d'un anneau A sont dits comaximaux lorsque :
$$\langle a\rangle + \langle b\rangle = A$$

Proposition 18 : Deux éléments comaximaux sont premiers entre eux. La réciproque est vraie dans un domaine de Bezout

Contre-exemple 19 : Dans $K[X,Y]$, X^2 et Y^2 sont premiers entre eux mais pas comaximaux

Théorème 20 (Chinois)
Soit A un domaine de Bezout. Soit $(a_1, \dots, a_m) \in A^m$ une famille d'éléments premiers entre eux dans leur ensemble. On a un isomorphisme de A-algèbres :
$$A/\langle \prod_{i=1}^{m} a_i \rangle \xrightarrow{\sim} \prod_{i=1}^{m} A/\langle a_i\rangle$$
$$(x \bmod \prod_{i=1}^{m} a_i) \longmapsto (x \bmod a_1, \dots, x \bmod a_m)$$

Application 21 : Algorithme de Berlekamp

DEV 1

Soit q une puissance non nulle d'un nombre premier et $\mathbb{F}_q$ un corps à q éléments. On considère l'algorithme :
Entrée : $P \in \mathbb{F}_q[X] \setminus \mathbb{F}_q$ sans facteur carré
Sortie : Liste des facteurs irréductibles de P
1 - Calculer s la dimension de l'espace propre associé à 1 de :
$$\mathbb{F}_q[X]/\langle P\rangle \longrightarrow \mathbb{F}_q[X]/\langle P\rangle$$
$$\overline{Q}^P \longmapsto (\overline{Q}^P)^q$$
2 - Si $s = 1$, retourner P
3 - Sinon, soit $\overline{V}^P \in \mathbb{F}_q[X]/\langle P\rangle$ qui n'est pas dans cet espace propre. Retourner [pgcd$(V-\alpha, P)$; $\alpha \in \mathbb{F}_q$ | ce pgcd est non constant]
Cet algorithme est correct et terminal

Théorème 22 : Soit A un anneau intègre. Les assertions suivantes sont équivalentes :
(i) A est principal
(ii) A est un domaine de Bezout noethérien

II - Cas des anneaux euclidiens et principaux

1 - Anneau euclidien

Théorème 23 : Soit A un anneau. Alors A euclidien $\Rightarrow$ A principal $\Rightarrow$ A factoriel et de Bezout.

Exemples 24
$\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$ sont euclidiens, $K[X,Y]$ ne l'est pas.

Algorithme 25 (euclide)
Soient a et b des éléments non tous deux nuls d'un anneau euclidien. On considère l'algorithme :
1. Calculer la division euclidienne $a = bq + r$
2 - Si $r = 0$ retourner b
3 - Sinon, retour à l'étape 1 avec $a \leftarrow b$, $b \leftarrow r$
Cet algorithme termine et renvoie un pgcd de a et b

Remarque 26 en modifiant l'algorithme on peut en plus calculer des coefficients de Bezout

Application 27 : Résolvons
$$3x + 5y = 6 \quad , (x,y) \in \mathbb{Z}^2$$

2 - Anneaux principaux

Proposition 28

DVT 2

Soit $\begin{pmatrix} a \\ b \end{pmatrix} \in A^2 \setminus \{0\}$ où A un domaine de Bezout. Il existe $B \in GL_2(A)$ telle que $B\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$ où d est un pgcd de a et b

Théorème 29 (forme de Smith)

DVT 2

Soit A un anneau principal. Soit $M \in \mathcal{M}_{n,p}(A)$. Il existe $r \le n, p$, il existe $a_r \mid \dots \mid a_1 \in A^*$ tels que M est équivalente à la matrice

DVT 2

$$\left(\begin{array}{ccc|c} a_1 & & 0 & \\ & a_2 \ddots & & 0 \\ 0 & & a_n & \\ \hline & 0 & & 0 \end{array}\right)$$

Définition 30: Soit $A \in \mathcal{M}_{n,p}(A)$ et soit $k \leq n, p$. On note Δ_k l'idéal engendré par les mineurs de taille k de A

Application 31 (unicité de la forme de Smith) La forme de Smith d'une matrice à coefficients dans un anneau principal est unique dans le sens où r est unique et les (a_i) sont uniques modulo l'association. On les appelle les facteurs invariants.

Corollaire 32: deux matrices à coefficients dans un anneau principal sont équivalentes si, et seulement si, elles ont les mêmes facteurs invariants

Exemple 33: la matrice $\begin{pmatrix} 6 & 15 & 7 & -10 \\ 2 & 7 & 3 & -6 \\ 16 & 31 & 15 & 18 \end{pmatrix}$ a pour facteurs invariants $(1, 4)$.

Application 34: Soit $(M, N) \in \mathcal{M}_n(K)$. Ces deux matrices sont semblables si, et seulement si, les matrices $XI_n - M$ et $XI_n - N$ sont équivalentes dans $\mathcal{M}_n(K[X])$

Application 35: Soit $MX = B$ un système linéaire à coefficients entiers. Soient (P, Q) inversibles à coefficients entiers tels que:

$$PMQ = \left(\begin{array}{ccc|c} a_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & a_n & \\ \hline & 0 & & 0 \end{array}\right)$$

soit sous forme de Smith. Ce système admet des solutions entières si, et seulement si:

(i) a_i divise le i-ème coefficient de PB

(ii) les coefficients d'indice plus grand que r de PB sont nuls

III - Contenu d'un polynôme

Définition 36 (Contenu): soit $P \in A[X]$ avec A un anneau à pgcd. On note $c(P)$ un pgcd des coefficients de P. Si $c(P)$ est inversible, on dit que P est primitif.

Remarque 37: Un polynôme unitaire est primitif

Exemple 38: $XY + X^2 \in K[X][Y]$ est de contenu λX pour tout $\lambda \in K^\times$

Théorème 39: Soit $(P, Q) \in A[X]^2$. Alors $c(PQ) = c(P)\,c(Q)$ si A factoriel

Application 40: Soit $\alpha \in \mathbb{C}$ un nombre algébrique. Alors α est un entier algébrique si, et seulement si, son polynôme minimal est à coefficients entiers

Exemple 41: $\sqrt{2/3}$ n'est pas un entier algébrique

Application 42: Soit A un anneau factoriel de corps des fractions K. Soit $P \in A[X] \setminus A$. On a équivalence:

(i) P est irréductible sur $A[X]$

(ii) P est irréductible sur $K[X]$ et est primitif

Exemple 43: $2X + 3$ est irréductible dans $\mathbb{Z}[X]$. Le n-ième polynôme cyclotomique

$$\Phi_n := \prod_{\omega \in \mu_n^*} (X - \omega)$$

où μ_n^* est l'ensemble des générateurs du groupe des racines n-ièmes de l'unité est irréductible dans $\mathbb{Z}[X]$.