Nom:

LARIVÉ

Prénom:

Pierre

Numéro de Jury:

Numéros des sujets tirés:

142 - 161

Intitulé du sujet choisi:

PGCD et PPCM, algorithmes de calcul. Applications.

Soit $(A,+,\times)$ un anneau intègre.

I - Définition, existence, caractérisations.

Définition 1 : Soit $r \geq 1$ et $(a_1,\dots,a_r) \in A\setminus\{0\}$.
On dit que $\delta \in A\setminus\{0\}$ est un pgcd de $a_1,\dots,a_r$ si :
- $\forall k \in [\![1,r]\!]$, $\delta \mid a_k$
- tout diviseur commun à $a_1,\dots,a_r$ divise δ.

On dit que $m \in A\setminus\{0\}$ est un ppcm de $a_1,\dots,a_r$ si :
- $\forall k \in [\![1,r]\!]$, $a_k \mid m$
- tout multiple commun à $a_1,\dots,a_r$ est multiple de m.

Proposition 2 : Deux pgcd de $(a_k)_{k\in[\![1,r]\!]} \in A^r\setminus\{0\}$ sont associés.

Exemple 3 :
- Dans $\mathbb{Z}$, les pgcd de 10 et 25 sont 5 et -5.
- Dans $\mathbb{Z}[i]$, les pgcd de $2i$ et $-1+3i$ sont $1+i$, $-1+i$, $1-i$, $-1-i$.

Remarque 4 : Dans $\mathbb{Z}$ et $K[X]$ où K est un corps, on parlera du pgcd pour désigner le pgcd positif ou unitaire.

Contre-exemple 5 : Le pgcd et le ppcm n'existent pas toujours : dans $\mathbb{Z}[i\sqrt{5}]$, 2 et $1+i\sqrt{5}$ n'ont pas de ppcm.

Théorème 6 : Soit A un anneau principal. Alors le pgcd et le ppcm d'une famille d'éléments existe.

Proposition 7 : Soit A un anneau principal et $(a_1,\dots,a_r) \in A\setminus\{0\}$. Soit $d \sim \text{pgcd}(a_k)$ et $m = \text{ppcm}(a_k)$. Alors :
$(d) = \sum_{k=1}^{r} (a_k)$ et $(m) = \bigcap_{k=1}^{r} (a_k)$.

~~**Théorème 8 (Bézout) : Soit A un anneau principal et**~~

Définition 8 : Soit $(a_1,\dots,a_r) \in A^r\setminus\{0\}$. On dit que $a_1,\dots,a_r$ sont premiers entre eux dans leur ensemble lorsque $\text{pgcd}(a_1,\dots,a_r) \sim 1$.

Théorème 9 (Bézout) : Soit A un anneau principal et $a_1,\dots,a_r \in A$. Alors $a_1,\dots,a_r$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $u_1,\dots,u_r \in A$ tels que $\sum_{k=1}^{r} u_k a_k = 1$.

Corollaire 10 : Soit A un anneau principal et $a,b,c \in A\setminus\{0\}$. Si $\text{pgcd}(a,c) = 1$, alors $\text{pgcd}(a,b) = \text{pgcd}(a,bc)$.

Corollaire 11 (Théorème de Gauss) : Soit A un anneau principal et $a,b,c \in A\setminus\{0\}$. Si $a \mid bc$ et $\text{pgcd}(a,b) = 1$, alors $a \mid c$.

Application 12 (Lemme de décomposition des noyaux) Soit K un corps et $P = P_1 \cdots P_r \in K[X]$ où les P_k sont 2 à 2 premiers entre eux. Soit $u \in \mathcal{L}(E)$ où E est un K-espace vectoriel de dimension finie. Alors :

$$\operatorname{Ker} P(u) = \bigoplus_{k=1}^{r} \operatorname{Ker} P_k(u)$$

et les projecteurs associés à la décomposition sont dans $K[u]$.

Théorème 13 : Soit A un anneau factoriel et $a, b \in A \setminus \{0\}$. En écrivant la décomposition de a et b en produits d'irréductibles $a = \alpha \prod_{k=1}^{r} p_k^{\alpha_k}$ et $b = \beta \prod_{k=1}^{r} p_k^{\beta_k}$ où $\alpha, \beta \in A^\times$, $p_1, \dots, p_r$ sont des irréductibles deux à deux différents et $\alpha_k, \beta_k \in \mathbb{N}$, on a

$$\operatorname{pgcd}(a,b) = \prod_{k=1}^{r} p_k^{\min(\alpha_k, \beta_k)} \quad \text{et} \quad \operatorname{ppcm}(a,b) = \prod_{k=1}^{r} p_k^{\max(\alpha_k, \beta_k)}$$

Corollaire 14 : Soit A factoriel et $a, b, c \in A^\times$. Alors $\operatorname{pgcd}(ac, bc) = c \operatorname{pgcd}(a,b)$.

II - Algorithmes de calcul dans le cadre euclidien.

Dans cette partie, on suppose A euclidien de stathme v.

Théorème 15 : Un anneau euclidien est principal.

Exemple 16 : $\mathbb{Z}$, $K[X]$, $\mathbb{Z}[i]$ sont euclidiens donc principaux.

Algorithme 17 (algorithme d'Euclide) : Soit $(a,b) \in A \times A \setminus \{0\}$. L'algorithme suivant calcule un pgcd de a et b :

- division euclidienne de a par b : $a = bq + r$ où $q, r \in A$, $r = 0$ ou $v(r) < v(b)$.
- si $r = 0$, renvoyer b
- si $r \neq 0$, recommencer avec $(a,b) \leftarrow (b,r)$.

Proposition 18 : Soit $x > y > 0$ dans $\mathbb{Z}$ et $d = \operatorname{pgcd}(x,y)$. Si l'algorithme d'Euclide s'arrête au bout de n pas, on a $x \geq d F_{n+2}$ et $y \geq d F_{n+1}$ où $(F_n)_n$ désigne la suite de Fibonacci.

Corollaire 19 : Soit $x \geq y \geq 0$. L'algorithme d'Euclide prend au plus $\frac{3}{2} \log y + 1$ pas.

Remarque 20 : On peut étendre l'algorithme d'Euclide pour obtenir une relation de Bézout entre x et y, lorsque ces derniers sont premiers entre eux.

Application 21 : On utilise cet algorithme pour calculer un inverse dans les corps de la forme $K[X]/(P)$. Pour $K = \mathbb{Q}$ et $P = X^3 - 3X + 4$, en notant $\alpha = \overline{X}$ dans $L = \mathbb{Q}[X]/(P)$, on a :

$$(\alpha^2 + \alpha + 1)^{-1} = -\frac{3}{49}\alpha^2 - \frac{5}{49}\alpha + \frac{17}{49}.$$

Application 22 (Forme de Smith) Soit $M \in \mathcal{M}_n(A)$. Il existe une unique suite finie $(d_1, \dots, d_s)$ de $A \setminus \{0\}$ telle que $d_1 | \cdots | d_s$ et que M soit équivalente à $\begin{bmatrix} d_1 & & (0) \\ & \ddots & \\ (0) & & d_s \\ & & (0) \end{bmatrix}$.

DVT 1

III - Théorème d'isomorphisme chinois.

Théorème 23 : Soit A un anneau principal, $r \geq 1$ et $a_1, \dots, a_r \in A \setminus \{0\}$ 2 à 2 premiers entre eux. L'application :

$$\varphi : \left| \begin{array}{ccc} A/(a_1 \cdots a_r) & \longrightarrow & A/a_1 \times \cdots \times A/a_r \\ (x \bmod a_1 \cdots a_r) & \mapsto & (x \bmod a_1, \dots, x \bmod a_r) \end{array} \right.$$

est un isomorphisme d'anneaux bien défini.

Intercalaire N°

Remarque 24 : Lorsque l'anneau est euclidien, on peut calculer algorithmiquement l'antécédent modulo $a_1 \cdots a_r$ d'une donnée $(\beta_1, \dots, \beta_r) \in A/a_1 \times \cdots \times A/a_r$.

Application 25 : Résolution de systèmes de congruences dans un anneau euclidien.

Exemple 26 : Les solutions dans $\mathbb{Z}$ du système $\begin{cases} u \equiv 1 \bmod 3 \\ u \equiv 3 \bmod 5 \\ u \equiv 0 \bmod 7 \end{cases}$ sont les entiers de la forme $28 + 105k$, $k \in \mathbb{Z}$.

Application 27 (interpolation polynomiale) : Soit K un corps, $\alpha_0, \dots, \alpha_n \in K$ distincts et $\beta_0, \dots, \beta_n \in K$. Il existe un unique polynôme $g \in K[X]$ de degré $\leq n$ tel que $\forall k \in [\![0, n]\!]$, $g(\alpha_k) = \beta_k$, et les polynômes solutions du problème d'interpolation sont de la forme $g + h \prod_{k=0}^{n} (X - \alpha_k)$ pour $h \in K[X]$.

Exemple 28 : Le polynôme $f = \bar{2} + \bar{4}X + \bar{4}X^2$ est l'unique polynôme de $\mathbb{F}_5[X]$ de degré ≤ 2 tel que $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{0}$ et $f(\bar{2}) = \bar{1}$.

DVT 2

Application 29 (Algorithme de Berlekamp) : Soit p un nombre premier, $q = p^s$ où $s \geq 1$ et $\mathbb{F}_q$ le corps fini à q éléments. Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés dans sa décomposition en produit de facteurs irréductibles. Alors on peut calculer algorithmiquement cette décomposition.

IV - Applications arithmétiques

1) Ordre d'éléments d'un groupe.

Soit G un groupe.

Proposition 30 : Soit $g, h \in G$ d'ordre fini m, n.
Pour $k \geq 1$, l'ordre de g^k est $\frac{m}{\text{pgcd}(m,k)}$.

Si $gh = hg$, l'ordre de gh est $\text{ppcm}(m, n)$.

Application 31 : Calcul de l'ordre d'une permutation dans $\mathfrak{S}_n$.

2) Equations diophantiennes.

Exemple 32 : $\sqrt{2}$ est irrationnel

~~Exemple 33~~

Théorème 33 : L'équation diophantienne $ax = b$ [n] admet des solutions $x \in \mathbb{Z}$ si et seulement si $\text{pgcd}(a, n) \mid b$. Dans ce cas, l'ensemble des solutions de l'équation est
$S = \{b'x_0' + kn' \mid k \in \mathbb{Z}\}$ où x_0' est une solution particulière de $a'x \equiv 1 \bmod n'$ et où $a' = \frac{a}{\delta}$, $b' = \frac{b}{\delta}$, $n' = \frac{n}{\delta}$ avec $\delta = \text{pgcd}(a, n)$.

Intercalaire N°