142 : PGCD et PPCM, algorithmes de calculs. Applications

I - Arithmétique dans les anneaux

$(A, +, \times)$ un anneau commutatif

a) Divisibilité, pgcd et ppcm

$a, b, c, d, \pi \in A$

Def. 1 : On dit que a divise b (noté $a|b$) si $(a) \subset (b)$

Def. 2 : a, b sont dit associés si $(a) = (b)$.

Def. 3 : On dit que a et b sont premiers entre eux si pour tout $d \in A$ on a : $d|a$ et $d|b$ alors $d \in A^\times$.

Def. 4 : On dit que $d \in A$ est un pgcd de a et b si :
- $d|a$ et $d|b$
- pour tout $c \in A$ tq $c|a$ et $c|b$ alors $c|d$.

On dit que $m \in A$ est un ppcm de a et b si :
- $a|m$ et $b|m$
- pour tout $c \in A$ tq $a|c$ et $b|c$ alors $m|c$

CBERS p.515 - 523

Rmq. 5 : Dans le cas général d'un anneau, rien n'assure l'existence d'un pgcd ou d'un ppcm.

Rmq. 6 : Si un pgcd ou un ppcm existe alors ils sont unique à association près.

Rmq. 7 : a, b premier entre eux si un pgcd de a, b est 1.

Def. 8 : π est dit irréductible s'il est non nul, non inversible et si $(\forall a,b)$ $\pi = ab$ alors $a \in A^\times$ ou $b \in A^\times$

Def. 9 : π est dit premier s'il est non nul, non inversible et si pour tout $a, b \in A$ $\pi | ab$ alors $\pi | a$ ou $\pi | b$.

b) Anneaux factoriels et pgcd, ppcm

$a, b, c, \pi \in A$.

CBERS p.528

Def. 10 : On appelle système complet de représentant irréductible (scri) un sous ensemble P de A tq :
- tout élément de P est irréductible
- tout élément de A irréductible est associé à un élément de P.

On note P un scri pour A.

CBERS p.542 - 545

Def. 11 : On dit que A est factoriel s'il est intègre et si pour tout $a \in A$, il existe un unique $u \in A^\times$ et $(\pi_\pi)_{\pi \in P} \in \mathbb{N}^{(P)}$ (sous nul sauf un nombre fini) tq $a = u \prod_{\pi \in P} \pi^{\pi_\pi}$. π_π est appelé valuation π-adique de a et noté $v_\pi(a)$.

On se place jusqu'à la fin de cette sous partie dans un anneau factoriel

Lemme 12 : (Euclide) Soient π irréductible. Si $\pi | ab$ alors $\pi | a$ ou $\pi | b$.

Lemme 13 : (Gauss) Si a, b premiers entre eux et $a | bc$ alors $a | c$.

Rmq 14 : $a | b$ ssi pour tout $\pi \in P$ $v_\pi(a) \leq v_\pi(b)$

Prop. 15 : Tout couple de A admet un pgcd et un ppcm. De plus

$$\text{pgcd}(a,b) = \prod_{\pi \in P} \pi^{\min(v_\pi(a), v_\pi(b))} \quad \text{et} \quad \text{ppcm}(a,b) = \prod_{\pi \in P} \pi^{\max(v_\pi(a), v_\pi(b))}$$

c) Anneaux principaux : une nouvelle caractérisation du pgcd et ppcm

$a, b \in A$.

CBERS p.404

Def. 16 : A est dit principal s'il est intègre et tout ses idéaux sont principaux

Dans cette sous partie on considère A principal.

CBERS p.547

Thm. 17 : Tout anneau principal est factoriel

Rmq. 18 : Ainsi toutes les propriétés définissant pour un anneau factoriel sont valable pour un anneau principal. Notamment l'existence d'un pgcd et d'un ppcm.

CBERS p.526

Prop. 19 : Soient $d, m \in A$ tq $(a)+(b) = (d)$ et $(a) \cap (b) = (m)$. Alors d est un pgcd de a, b et m ppcm de a, b.

Cor. 20 : (Bezout) a, b sont premiers entre eux ssi il existe $u, v \in A$ tq $au + bv = 1$.

d) Le cadre idéal, les anneaux euclidiens

CBERS p.528 - 530

Def. 21 : Un anneau euclidien est un couple (A, δ) où A est intègre et $\delta : A \setminus \{0\} \to \mathbb{N}$ tq pour tout $a, b \in A$ et $b \neq 0$, il existe $q, r \in A$ tq $a = bq + r$ tq $r = 0$ ou $\delta(r) \in \delta(b)$.

Ex. 22 : $(\mathbb{Z}, |.|)$ est euclidien et $(\mathbb{Z}[i], N)$ est euclidien pour $N : z \mapsto z\bar{z}$

Thm. 23 : Tout anneaux euclidien est principal

Rmq. 24 : Tout ce qu'on a obtenue précédement est encore valable.

CBERS p.53

C-ex. 25 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal pas euclidien.

Rmq. 26 : L'avantage d'un anneau euclidien est l'existence d'un algorithme pour le calcul du pgcd et des coefficients de Bezout

II - Algorithme de calcul dans un anneau euclidien

(A, δ) euclidien

a) Algorithme d'Euclide

$a, b \in A \setminus \{0\}$

CBERS p.552 - 554

Algorithme 27 : (Euclide) Tant que c'est possible (ie tant que l'on ne divise pas par 0) on définit q_i et r_{i+1} comme suit par divisions euclidiennes successive en posant :

$r_{-1} = a$, $r_0 = b$, $r_{i-1} = q_i r_i + r_{i+1}$ (avec $r_i \neq 0$ on a $r_{i+1} = 0$ ou $\delta(r_{i+1}) \in \delta r_i$)

Pour tout $i \geq -1$ tq $r_i \neq 0$, on définit u_i et v_i par rec :

$$\begin{cases} u_{-1} = 1, & u_0 = 0, & u_{i+1} = -q_i u_i + u_{i-1} \\ v_{-1} = 0, & v_0 = 1, & v_{i+1} = -q_i v_i + v_{i-1} \end{cases}$$

Prop. 28 : $\exists$ existe $i \geq 1$ tq $r_i = 0$. Si $n \geq 0$ est le plus grand entier tq $r_n \neq 0$ en posant $d = r_n$, $u = u_n$, $v = v_n$. On a $d = \text{pgcd}(a,b)$ et $ua + vb = d$.

Ex. 29: Dans $\mathbb{Z}$ $\text{pgcd}(32,7) = 1$ et $32\times 2 + 7\times(-9) = 1$ (cf Annexe 1)

Ex. 30: Dans $\mathbb{Z}[i]$, $\text{pgcd}(12+65i, 9+12i) = -i$ et $(12+65i)(3-9i) + (-127+19i)(9+12i) = -i$ (cf. Annexe 2)

b) Coût de l'algorithme sur $\mathbb{Z}$ et $\mathbb{K}[X]$

Prop. 31: (Lamé) Soient $x \geq y \in \mathbb{N}^*$ et d leur pgcd. Si l'algo. d'Euclide (usuel) de x, y s'arrête au bout de n étapes, on a: $x \geq d F_{n+2}$, $y \geq d F_{n+1}$ (où F_n est la suite Fibonacci)

Cor. 32: Soit $x \geq y \in \mathbb{N}^*$ l'algo. d'Euclide du pgcd (x,y) prend au plus $\frac{3}{2}\log y + 1$ étapes.

Prop. 33: Pour l'algorithme d'Euclide (étendu ou non) le nombre d'étape est majoré par $c(\log(M))^2$ où c est une constante et M le maximum des deux éléments pour lesquelles on a calculé le pgcd.

(*)

III - Applications

a) Algèbre linéaire E un $\mathbb{K}$-ev

Thm. 34: (Lemme des noyaux) Soit $f \in \mathcal{L}(E)$, $P = P_1 \cdots P_k \in \mathbb{K}[X]$ où les P_i sont premier entre eux 2 à 2. Alors $\text{Ker } P(f) = \bigoplus_{i=1}^{+\infty} \text{Ker } P_i(f)$

Appli. 35: Soit $f \in \mathcal{L}(E)$. f est diagonalisable ssi il existe $P \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$ ayant toutes ses racines simple tq $P(f) = 0$

b) Théorème chinois $(A, +, .)$ Anneau commutatifs

Def. 36: On dit que I_1 et I_2 sont des idéaux comaximaux si I_1, I_2 sont des idéaux de A et $I_1 + I_2 = A$.

Thm. 37: (Chinois) Soient $I_1, \dots, I_n$ des idéaux de A 2 à 2 comaximaux. Pour $i \in \{1, \dots, n\}$ et pour tout $a \in A$ on note $\bar{a}_i$ la réduction de a modulo I_i. Le morphisme

$$f : A \longrightarrow \frac{A}{I_1} \times \cdots \times \frac{A}{I_n} \quad \text{est surjectif.}$$
$$a \longmapsto (\bar{a}_1, \dots, \bar{a}_n)$$

$\text{Ker}(f) = \bigcap_{i=1}^{n} I_i$.

Rmq 38: Si I_1, I_2 sont comaximaux tq $I_1 = (a)$ et $I_2 = (b)$ alors il existe $u, v \in A$ tq $ua + vb = 1$

Thm. 39: Soient $n_1, \dots, n_r \in \mathbb{N}^* \setminus \{1\}$ et $n = n_1 \cdots n_r$. les n_i sont premiers entre eux 2 à 2 ssi $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et $\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}}$ sont isomorphes.

Dans ce cas,

$$\Psi : \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_r\mathbb{Z}} \quad \text{est un isomorphisme d'anneau}$$
$$\bar{x}^{n} \longmapsto (\bar{x}_{n_1}, \dots, \bar{x}_{n_r})$$

d'inverse,

$$\Psi^{-1} = \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_r\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$$
$$(\bar{a}_1^{n_1}, \dots, \bar{a}_r^{n_r}) \longmapsto \overline{x_1 u_1 \frac{n}{n_1} + \cdots + x_r u_r \frac{n}{n_r}}^{n}$$

où $u_1 \frac{n}{n_1} + \cdots + u_r \frac{n}{n_r} = 1$.

c) Equations diophantiennes et systèmes de congruences

6 points, cf L120

Réf. [ROU] p.288
[CVA] p.201-204

+ DEV 2 est le même.

[DEV] p.38-41

[DEV] [GOU] p.185

[ROU] p.289

(*): voir fin pour ajout (euclide binaire et pop.)

d) Application en théorie des groupes

$(G,\times)$ un groupe et $a \in G$

Prop. 46 : Pour tout $d \geq 1$, a^d est d'ordre fini (si a d'ordre fini) et $o(a^d) = \frac{o(a)}{\text{pgcd}(d, o(a))}$.

En particulier : si $d \mid o(a)$ on a $o(a^d) = \frac{o(a)}{d}$

si $\text{pgcd}(d, o(a)) = 1$ on a $o(a^d) = o(a)$

[CBER] p.151

Prop. 47 : Si x et y sont d'ordres finis tq $xy = yx$. Alors xy est d'ordre fini et :

(i) si $\langle x \rangle \cap \langle y \rangle = \{1_G\}$ alors $o(xy) = \text{ppcm}(o(x), o(y))$

(ii) si $\text{pgcd}(o(x), o(y)) = 1$ alors $o(xy) = o(x)\,o(y)$.

Thm. 48 : [ADMISS] Si G est abélien fini alors il existe $d_1 | \dots | d_s$ des entiers supérieurs ou égal à 2 tq

$$G \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{d_s\mathbb{Z}}$$

$(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G

[ZBER] p.358

Def. 49 : $d_1, \dots, d_s$ sont appelés invariant de similitudes de G

Cor. 50 : Deux groupes abéliens sont isomorphes ssi ils ont même invariant de similitude.

Ex. 51 : $G = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \times \frac{\mathbb{Z}}{3\mathbb{Z}}$

$\simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^3 \times \frac{\mathbb{Z}}{8\mathbb{Z}}$

[CBER] p.365

Ajouts :

Rmq : Il existe un algorithme d'Euclide binaire avec la même complexité que l'algorithme d'Euclide classique, mais en pratique il va plus vite. (cf Annexe 1 pour l'algorithme)

[COHE] p.36

Algorithme : (Stricto sensu) Soient $P_0, P_1 \in \mathbb{K}[X]$ tq $\deg(P_1) \leq \deg(P_0)$

Par division euclidienne successive 2 suites de polynômes $(P_i)_{i \geq 2}$ et $(Q_i)_{i \geq 1}$ tq

$$\begin{cases} P_{i-1} = P_i Q_i + P_{i+1} \\ \deg(Q_i) = \deg(P_{i-1}) - \deg(P_i) \end{cases}$$

$\deg(P_{i+1}) < \deg(P_i)$

on continue tant que $P_i \neq 0$.

Rmq : Puisque les degrés des P_i sont strictement décroissants l'algo. termine.

[COHE] p.53

Annexe :

Annexe 1 :

```
def eucl_bin(u,v):  ## u>0, v≥3 impair
    if u%2 == 0:
        return eucl_bin(u/2, v)
    if u%2 != 0 and u > v:
        return eucl_bin((u-v)/2, v)
    if u%2 != 0 and u < v:
        return eucl_bin((v-u)/2, u)
    if u == v:
        return u
```

Références :

[CBER] : Berhuy, Algèbre le grand combat

[DEMJ] : Demazure, Cours d'algèbre

[GOUX] : Gourdon, Algèbre et probas

[ROMB] : Rombaldi, Algèbre et géométrie

[CVAL] : Caldero, Carnet de voyage en Algébrie.