142. PGCD et PPCM. Algorithmes de calcul. Applications

I – Notions de PGCD et PPCM dans différents types d'anneaux

Dans cette section, A est un anneau intègre commutatif et $(a, b, \dots a_r)$ [illegible].

A – Première définition, existence dans des anneaux factoriels

Def 1 : PGCD, PPCM. Déf à partir [illegible] [Berhuy] [Rom. 2]
En particulier, PGCD, PPCM sont associatifs, commutatifs.

Rq 2 : Les PGCD, PPCM sont tous associés. [Rom]
Ex 3 : 2 est un PGCD de 6 et 4 dans $\mathbb{Z}$, −2 aussi.
Prop 3 : Si a et b ont un PPCM, alors ils ont un pgcd. [Rom]

Ex 4 : 3 et $2 + i\sqrt{5}$ ont un PGCD mais pas de PPCM. [Berhuy]
9 et $3(2 + i\sqrt{5})$ n'ont pas de PGCD.

Def 5 : $a_1, \dots a_r$ premiers entre eux 2 à 2, dans les anneaux [illegible] [Rom]
Thm 6 : Gauss. ?? [Rom]

Prop 7 : Anneau à pgcd ⟺ tout élément de A admet un ppcm [Rom]

Prop 8 : A factoriel ⟹ PGCD = max de $v_p(a)$ [Perrin]
PPCM = min des $v_p(a)$

Def 9 : si $A = \mathbb{Z}$ ou $K[X]$, le pgcd est choisi positif / unitaire.

B – Situation dans les anneaux principaux

Prop 10 : $m \in A$ ppcm de (a, b) ssi $aA \cap bA = mA$ [Berhuy]
$d \in A$ pgcd de (a, b) ssi $aA + bA = dA$.

Thm 11 : Bézout (équivalence) [Berhuy]
[illegible] particulier, $\exists u, v \in A$ tq $au + bv = a \wedge b$.
Un tel couple est appelé couple de Bézout de (a, b).

Appli 13 : Résolution de $ax + by = \mathbb{Z}$, $(a \wedge b = 1)$.

Appli 14 : Lemme des noyaux [Gourdon]

Thm 15 : Restes chinois effectif. [Rom]

Appli 16 : Résolution d'un système de congruences. [Gourdon p. 29]

Ex 17 : Interpolation de Lagrange [Rombaldi]

Appli 18 : Recherche de $P \in \mathbb{Z}/5\mathbb{Z}[X]$, tq $P(0) = 1$, $P(\bar{1}) = 0$, $P(\bar{2}) = 1$, de degré minimal. [Rombaldi]

19. $\forall (n, m) \in \mathbb{N}^2$, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/n \wedge m\mathbb{Z} \times \mathbb{Z}/n \vee m\mathbb{Z}$

II – Dans le cas euclidien, des algos de calcul efficaces

Dans cette section A est supposé euclidien. Soit $(a, b) \in A \times A^*$.

A – Algorithme d'Euclide

Lemme 10 : Lemme d'Euclide. [Rombaldi]

Algo 11 : Euclide [Rombaldi]

Prop 12 : L'algo termine et donne le PGCD. [Berhuy]

Ex 13 : $M_n \wedge M_m = M_{n \wedge m}$ où $M_n = 2^n - 1$.

Algo 24 : Euclide étendu [Rombaldi]

Appli 25 : Inversion modulaire dans $\mathbb{Z}/n\mathbb{Z}$ [Rombaldi] [Demazure]
Corps de rupture ?

B – Complexité des algorithmes dans $\mathbb{Z}$ ou $K[X]$

Def 26 : Suite de Fibonacci [Demazure]

La suite de Fibonacci représente le pire cas pour l'algo d'Euclide. [Demazure]

Thm 27 : Lamé (contraposée)

Corollaire 28 : L'algo d'Euclide nécessite $\frac{3}{2} \log_2 b + 1$ pas. [Dem]

Prop 29 : Complexité de l'Euclide dans [illegible] [GG] ?

Dans la pratique, on peut optimiser [illegible] grâce au binaire.

Algo 30 : PGCD binaire. [Dem]

Prop 31 : L'algo se termine en $2 \log N$ récursions, donc $O(\log N^2)$ opérations. [Dem]

Prop 32 : Algo d'Euclide à P, Q = complexité [illegible] étape [Dem] ?

C – Application à la factorisation de polynômes

Cadre

Thm 33 : Berlekamp. DEV 1 [BMP] [Beaumont]

III – Application à l'arithmétique et à la théorie des groupes

A – Systèmes diophantiens

B) Théorème de Liouville

Thm : Liouville [FGN]

C – Application à la théorie des groupes

Soit G un groupe abélien fini. On note [illegible] l'ordre de g dans G.

Lemme : Si $g_1, \dots g_r$ sont d'ordres $m_1, \dots m_r$, alors il existe g d'ordre ppcm des ordres.

Prop : Si G est abélien fini, $exp(G) := \max Ord(g) = ppcm(O(g))$.
i.e. il existe un élément dont l'ordre est l'exposant. [Beaumont]

Thm : Structure des groupes abéliens finis + unicité [Rombaldi]

Ex : Soit p un nombre premier. Un groupe abélien d'ordre p^2 est isomorphe à $\mathbb{Z}_{p^2}$ ou $\mathbb{Z}_p^2$.

Prop : Tout sous-groupe multiplicatif fini d'un corps est cyclique. [Oraux X-ENS]