Références : ULMER - Anneaux, corps, résultant // PERRIN - Cours d'algèbre // ROMBALDI - Algèbre et géométrie // BERCK-MALICK-PEYRE Objectif Agreg (abrégé en OA) // DEMAZURE - Cours d'algèbre // BOSTAN et cie - Algorithmes efficaces en calcul formel (abrégé en AECF) // FRANCINOU-GIANELLA-NICOLAS - Oraux X-ENS Algèbre 1

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

1. Cadre théorique : anneaux factoriel et principal

1.1. Anneau intègre

Ulmer

1. Définition. Définition d'un ppcm et pgcd
2. Exemple. Trouver exemple
3. Remarque. N'existe pas toujours
4. Définition. Premiers entre eux etc.
5. Proposition. Caractérisation de l'existence du ppcm
6. Remarque. Pas de caractérisation de l'existence d'un pgcd

Rombaldi

7. Théorème. Toute paire d'éléments admet un ppcm ssi toute paire d'éléments admet un pgcd

1.2. Anneau factoriel

Perrin

8. Définition. Anneau factoriel
9. Exemple. Anneau factoriel
10. Proposition. Factoriel : Ppcm et pgcd par rapport à la décomposition en irréductibles
11. Exemple. Exemple bateau
12. Proposition. Lemme de Gauss

1.3. Anneau principal

Perrin

13. Définition. Anneau principal
14. Exemple.
15. Proposition. Principal => factoriel
16. Remarque. Les pgcd et ppcm existent : nouvelle expression
17. Théorème. Bezout
18. Corollaire. Identité de Bezout
19. Exemple. Quelques petits pgcd calculés, déduction du ppcm

OA

20. Théorème. Théorème Chinois OA
21. Application. Résolution de systèmes de congruence OA

2. Algorithmique

2.1. Algorithme d'Euclide

Demazure

22. Définition. Anneau euclidien
23. Exemple. Anneau euclidien
24. Lemme. $\gcd(u-v,v) = \gcd(u,v)$
25. Application. Algorithme d'Euclide Binaire
26. Remarque. Compleixité en $O(\log(\max(u,v))^2)$
27. Théorème. Algorithme d'Euclide étendu Ulmer
28. Exemple. Ulmer
29. Théorème. Fibonacci et Lamé

2.2. Résultant

AEFC

30. Définition. Résultant
31. Proposition. Sur un corps, lien avec le pgcd dans la forme échelonnée
32. Théorème. Existence de U et V tq $PU + VQ = \mathrm{Res}(P,Q)$.
33. Corollaire. A et B premier entre eux ssi $\mathrm{Res}(A,B) = 0$.
34. Application. Trouver des points d'intersection
35. Application. Réciprocité quadratique via le résultant

3. En arithmétique

3.1. Sur Z

X-ENS 1 Alg 1

36. Théorème. Résolution de système de congruence via la méthode de Lagrange/Newton
37. Exemple. Exemples
38. Lemme. $a \wedge b = 1$ et ab puissance k-ème impliquent a et b puissances k-èmes
39. Théorème. DEVELOPPEMENT Sophie-Germain (X-ENS Alg 1)

3.2. Sur $K[X]$

OA

40. Théorème. Résultat préliminaire à Berlekamp
41. Corollaire. DEVELOPPEMENT Algorithme de Berlekamp (OA)