

Sous groupes de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Projet Mathématiques-Informatique

Kevin Garnier
Charly Martin-Avila

Université Paris Cité

June 2, 2023

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

Quelques simplifications du problème

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

Décomposition de n en éléments irréductibles

Proposition

Soit $n = \prod_{i=1}^k p_i^{\alpha_i}$ avec p_i des nombres premiers distincts. Alors,

$$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cong \prod_{i=1}^k (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2$$

Décomposition de n en éléments irréductibles

```
fonction rho_pollard P n x y k i d
  Si d <> 1:
    Retourne d
  Sinon :
    x = P ( x ) mod n
    d = pgcd (| y - x | , n )
    Si i = k :
      Retourne rho_pollard P n x x 2k (i+1) d
    Sinon
      Retourne rho_pollard P n x y k (i+1) d
```

Proposition

$$\mathbb{Z}^2 / n\mathbb{Z} \times n\mathbb{Z} \cong \mathbb{Z} / n\mathbb{Z} \times \mathbb{Z} / n\mathbb{Z}$$

Proposition

$$\mathbb{Z}^2 / n\mathbb{Z} \times n\mathbb{Z} \cong \mathbb{Z} / n\mathbb{Z} \times \mathbb{Z} / n\mathbb{Z}$$

Remarque

*Le problème se résout à trouver les sous-groupes \mathbb{G} de \mathbb{Z}^2 tels que
et*

$$n\mathbb{Z} \times n\mathbb{Z} \subseteq \mathbb{G} = \left\langle \begin{pmatrix} \bar{a} \\ \bar{b} \end{pmatrix}, \begin{pmatrix} \bar{c} \\ \bar{d} \end{pmatrix} \right\rangle$$

Table des matières

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

Proposition

Soient $A \in M_{m,n}(\mathbb{Z})$ et $Q \in GL_n(\mathbb{Z})$ alors

$$\text{Im}(AQ) = \text{Im}(A)$$

Définition

Soit $A \in M_{m,n}(\mathbb{Z})$ alors, il existe une unique matrice échelonnée réduite suivant les colonnes $H \in M_{m,n}(\mathbb{Z})$ telle qu'il existe $Q \in GL_n(\mathbb{Z})$ avec $H = AQ$. La matrice H s'appelle la forme normale de Hermite de A .

Table des matières

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

Génération des sous-groupes

- Dans cette section, nous supposons que $n = p^m$

Theomème

Les seules matrices dont les colonnes génèrent un sous-groupe de $\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ sont les matrices de la forme

$$H = \begin{pmatrix} p^a & 0 \\ j & p^b \end{pmatrix} \quad \text{avec } a \leq m, b \leq m \text{ et } j < p^b$$

ou

$$H = \begin{pmatrix} p^a & 0 \\ jp^k & p^b \end{pmatrix} \quad \text{avec } a \leq m, b \leq m, k \leq m \text{ et } j < p^{(b-k)}$$

Corollaire

Soit la suite $(A_k)_{0 \leq k \leq n}$ telle que

$$A_0 = \{(a, b) \mid a + b \leq m\}$$

$$A_k = \{(a, b) \mid a \leq m, b \leq m, a + b = m + k\}$$

Alors, l'ensemble des matrices du théorème, c'est-à-dire, les matrices dont les colonnes génèrent les sous-groupes $\mathbb{Z}/p^m\mathbb{Z} \times p^m\mathbb{Z}$ est

$$M = \bigcup_{k=0}^m M_k$$

où

$$M_k = \left\{ \begin{pmatrix} p^a & 0 \\ jp^k & p^b \end{pmatrix} \mid (a, b) \in A_k, 0 \leq j \leq p^{(b-k)} \right\}$$

Theomème

Soit $\psi : \mathbb{N}^2 \rightarrow \mathbb{N}$ définie par

$$\psi(p, n) = \sum_{i=0}^n (n-i)p^i + \sum_{i=0}^n \frac{1-p^{n-i+1}}{1-p}$$

Alors, le nombre de sous groupe de $\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ est $\psi(p, m)$

Proposition

Soit $n = \prod_{i=1}^k p_i^{\alpha_i}$ avec p_i des nombres premiers distincts. Le nombre total de sous-groupes de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est

$$\prod_{i=1}^k \psi(p_i, \alpha_i) = \prod_{i=1}^k \left(\sum_{j=0}^{\alpha_i} (\alpha_i - j) p_i^j + \sum_{j=0}^{\alpha_i} \frac{1 - p_i^{\alpha_i - j + 1}}{1 - p_i} \right)$$

Génération du treillis

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

Génération du treillis

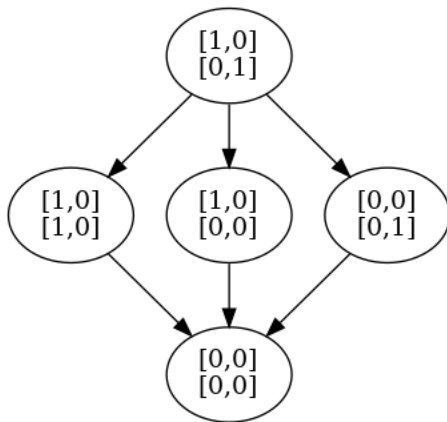
```
fonction creer_treillis (G T) =  
  G <- Trier G par la cardinalité  
  L = Vide  
  Pour chaque u dans G:  
    Pour chaque v dans T[u]:  
      Si not-exists (u, v0) dans L tel que v0 v  
        Alors L  $\cup$  {(u, v)}  
  Retourner (G, L)
```

Table des matières

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

Pour $n = 2$

- Nombre de sous-groupe de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: 5



Quelques valeurs de la suite du nombre de sous-groupes

n	0	1	2	3	4	5	6	7	8	9	10
$ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} $	∞	1	5	6	15	8	30	10	37	23	40

Table des matières

- 1 Quelques simplifications du problème
 - Décomposition de n en éléments irréductibles
 - Simplification des sous-groupes
- 2 Matrices à coefficients entier et forme normales de Hermite
 - Matrices à coefficients entier
 - Formes normales de Hermite
- 3 Génération et énumération des sous-groupes
 - Génération des sous-groupes
 - Énumération des sous-groupes
- 4 Génération du treillis
- 5 Quelques résultats
 - Pour $n = 2$
 - Quelques valeur de la suite du nombre de sous-groupes
- 6 Bibliographie

- COSTE Michel ; Algèbre linéaire sur les entiers ; Mars 2018
- Thomas H. Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein ; Algorithmique : cours avec 957 exercices et 158 problèmes, 3e édition, Paris : Dunod ; DL 2010
- PERNET Clément ; Calcul de formes normales matricielles : de l'algorithmique à la mise en pratique ; Séminaire SIESTE ; ENS-Lyon ; 12 février 2013
- BERHURY Grégory ; Algèbre le grand combat : Cours et exercices ; 2e édition ; Paris : Calvage Mounet ; 2020. 1215 p. (Mathématiques en devenir)
- Mario Hampejs, Nicki Holighaus, László Tóth, Christoph Wiesmeyr ; Representing and counting the subgroups of the group $\mathbb{Z}^m \times \mathbb{Z}^n$; 2012