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

Projet Mathématiques - Informatique

Kevin Garnier
Charly Martin Avila

Dirigé par Olivier Brunat

Année 2023

Quelques simplifications du problème

Décomposition de n en éléments irréductibles

Proposition

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

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

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
```

Simplification des sous-groupes

Proposition

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

Simplification des sous-groupes

Proposition

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

Remarque

Ainsi le problème se résout à trouver les sous-groupes G de $\mathbb{Z}^2$ tels que

$$H = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

et

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

Table des matières

Matrices à coefficients entier

Proposition

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

$$\operatorname{Im} AQ = \operatorname{Im} A$$

Formes normales de Hermite

Définition

Soit $A \in \mathscr{M}_{m,n}(\mathbb{Z})$. Alors, il existe une unique matrice échelonnée réduite suivant les colonnes $H \in \mathscr{M}_{m,n}(\mathbb{Z})$ 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

Génération des sous-groupes

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

Théorème

Les seules matrices dont les colonnes génèrent un sous-groupe de $\mathbb{Z}^2/p^m\mathbb{Z} \times p^m\mathbb{Z}$ sont les matrices de la forme

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

ou

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

Corollaire

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

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

$$A_k = \left\{ (a,b) \;\middle|\; \begin{matrix} a \leq m, b \leq m \\ a+b = m+k \end{matrix} \right\}$$

Alors, l'ensemble des matrices du théorème, c'est-à-dire, les matrices dont les colonnes génèrent les sous-groupes de $\mathbb{Z}^2/p^m\mathbb{Z} \times p^m\mathbb{Z}$ est

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

où

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

Énumération des sous-groupes

Théorème

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

$$\psi : \mathbb{N}^2 \to \mathbb{N}$$
$$(p, n) \mapsto \sum_{i=0}^{n} (n-i)p^i + \sum_{i=0}^{n} \frac{1-p^{n-i+1}}{1-p}$$

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*

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

Génération du treillis

Génération du treillis

```
fonction creer_treillis G T =
    G ← Trier G par la cardinalité
    L = ∅
    Pour chaque u ∈ G:
        Pour chaque v ∈ T[u]:
            Si ∄(u, v') ∈ L tel que v' ⊂ v
                Alors L ∪ { (u, v) }
    Retourner (G, L)
```

Table des matières

Pour n = 2

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

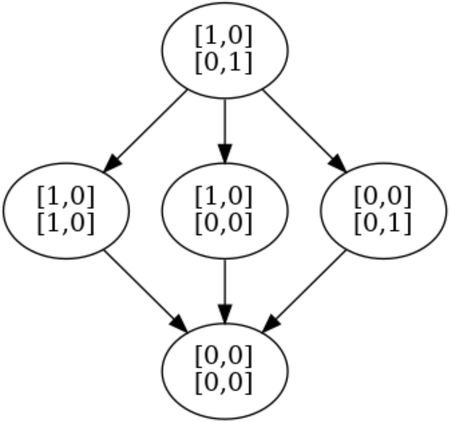

FIGURE – Treillis des sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec les forme normale de Hermite correspondantes

Quelques valeur de la suite du nombre de sous-groupes

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

Table des matières

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 ;
- Mario Hampejs, Nicki Holighaus, László Tóth, Christoph Wiesmeyr ; *Representing and counting the subgroups of the group* $Z_m \times Z_n$; 2012