Introduction

Introduction

- Ce projet aborde l'analyse des sous-groupes du groupe $Z/nZ \times Z/nZ$, un sujet complexe par rapport à l'étude des sous-groupes d'un groupe cyclique.
- Théoriquement, nous utiliserons les vecteurs colonnes des matrices à coefficients entiers et les formes normales de Hermite pour générer et caractériser ces sous-groupes, et introduirons une formule pour les compter.
- Pratiquement, nous développerons un outil OCaml pour générer ces sous-groupes et leur treillis, en se basant sur un entier en paramètre.

Quelques simplifications du problème

Décomposition de n en éléments irréductibles

- Nous allons simplifier le problème aux cas où $n = p^m$ avec p un nombre premier et $m \in \mathbb{N}$.

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

- Nous avons priviligé l'utilisation de ρ*Pollardpourdécomposerunentierenfacteursirréductibles*

```
    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 loop P n x x 2 k (i+1) d
            Sinon
                Retourne rho_pollard P n x y k (i+1) d
```

Simplification des sous-groupes

Proposition

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

Remarque

le problème se résout à trouver les sous-groupes G de Z² tels que

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

$$et$$

$$n\mathbb{Z} \times n\mathbb{Z} \subseteq \mathbb{G} =< \begin{pmatrix} \overline{a} \\ \overline{b} \end{pmatrix}, \begin{pmatrix} \overline{c} \\ \overline{d} \end{pmatrix} >$$

Table des matières

Matrices à coefficients entier

- Contenu ici

Formes normales de Hermite

- Contenu ici

Table des matières

Génération des sous-groupes

- Dans cette section, nous supposerons que $n = pm$

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 $Ak0 \leq k \leq n$ *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

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

shadov

Énumération des sous-groupes

Theomème

Soit $\psi : \mathbb{N}^2 \to \mathbb{N}$ *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* $\psi(p,m)$

Énumération des sous-groupes

Theomème

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

Génération du treillis

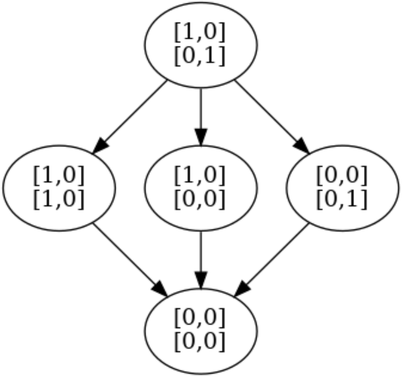
- Notre algorithme prend en paramètres l'ensemble des sous-groupes G ainsi que leur table de relation T

```
fonction creer_treillis (G T) =
    G ← Trier G par la cardinalit é
    L =
    Pour chaque u  G:
        Pour chaque v  T[u]:
            Si non (u, v0)  L tel que v0  v
                Alors L  { (u, v) }
    Retourner (G, L)
```

Table des matières

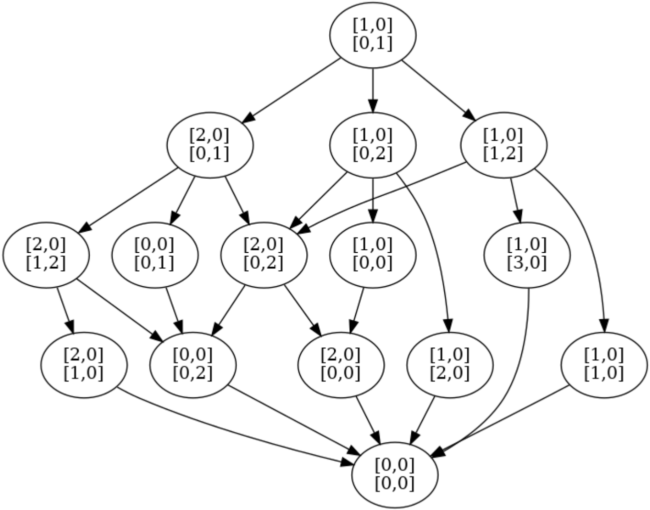
Pour $n = 2$

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



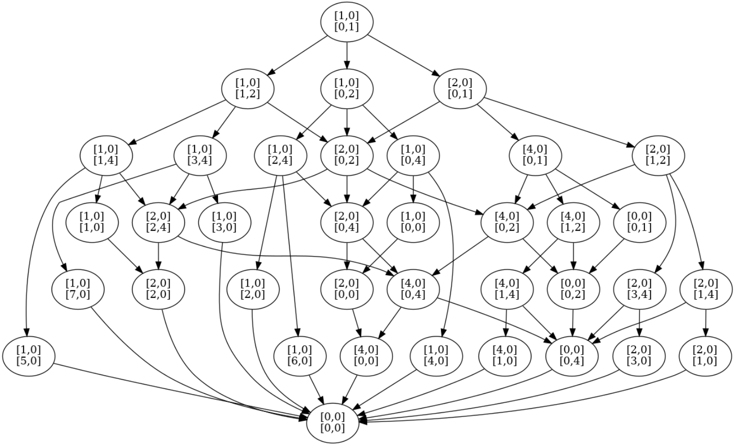
Pour n = 4

- Nombre de sous-groupe de $Z/4Z \times Z/4Z$: 15



Pour n = 8

- Nombre de sous-groupe de Z/8Z × Z/8Z : 37



Quelques valeur de la suite du nombre de sous-groupes

n	0	1	2	3	4	5	6	7	8	9	10
$\|Z/nZxZ/nZ\|$	*inf*	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 ; 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 Zm $\times$ Zn ; 2012