



UNIVERSITÉ PARIS CITÉ

PROJET MATHÉMATIQUES - INFORMATIQUE

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

Kevin Garnier
Charly Martin Avila

Dirigé par
Olivier BRUNAT

Année 2023

Table des matières

1	Introduction	3
2	Quelques simplifications du problème	3
2.1	Décomposition de n en éléments irréductibles	3
2.2	Simplification des sous-groupes	3
3	Matrices à coefficients entier et forme normales de Hermite	4
4	Generation et Enumeration des sous-groupes	4
5	Quelques résultats	4

1 Introduction

Il est très facile de décrire tous les sous-groupes d'un groupe cyclique d'ordre n : il y en a exactement un par diviseur positif de n . Pourtant, étonnamment, décrire tous les sous-groupes d'un groupe abélien est en général un problème difficile.

Dans ce projet, nous se proposons de considérer cette question pour le groupe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

D'un point de vue théorique, nous mettrons en avant la générations et la caractérisations de sous-groupes grâce aux vecteurs colonne des matrices à coefficients entier et en particulier aux formes normales de Hermite. Nous montrerons aussi une formule permettant de les compter.

D'un point de vue pratique, nous créerons un programme OCAML capable de générer les sous-groupes de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ainsi que leur treillis à partir d'un entier donné en paramètres.

2 Quelques simplifications du problème

2.1 Décomposition de n en éléments irréductibles

Nous pouvons tout d'abord simplifier le problème aux cas où $n = p^m$ avec p un nombre premier et $m \in \mathbb{N}$. En effet, soit

$$n = \prod_i^k p_i^{\alpha_i}$$

Par le théorème des restes chinois, on a

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

En particulier,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\simeq (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \\ &\simeq (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2 \end{aligned}$$

En pratique, pour décomposer en entier en facteurs irréductibles, nous avons utilisé la procédure de ρ -POLLARD pour obtenir un diviseur de n :

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

Dans notre implémentation, $P(X) = X^2 - 1$.

Puis nous répétons la procédure jusqu'à que les diviseurs soient premier. En triant et en regroupant les nombres premier, nous obtenons donc les différents $p_i^{\alpha_i}$

2.2 Simplification des sous-groupes

Soit

$$\begin{aligned} \varphi : \mathbb{Z}^2 &\rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ (a, b) &\mapsto (\bar{a}, \bar{b}) \end{aligned}$$

φ est surjective par définition de la casse d'équivalence de a et b

- 3 Matrices à coefficients entier et forme normales de Hermite
- 4 Generation et Enumeration des sous-groupes
- 5 Quelques résultats