Caractérisation des singularités de type $\mathfrak{J}$

Félix Larose-Gervais

Été 2023

Contents

1 Introduction

1.1 Notations

Soit $a, b \in \mathbb{Z}$ on note la relation de coprimalité $\perp$

$$a \perp b \iff \gcd(a,b) = 1$$

Soit $m, n \in \mathbb{N}$, X un ensemble, notons

- S_m le groupe symmétrique à m lettres
- $\mathbb{Z}_n$ l'anneau des entiers modulo n ($\mathbb{Z}/n\mathbb{Z}$)
- $\mathbb{Z}_n^\times$ son groupe d'inversibles ($\{a \in \mathbb{Z}_n \mid a \perp n\}$)
- X^m l'ensemble des m-uplets de X ($\underbrace{X \times \cdots \times X}_{m fois}$)

On notera aussi S_n^m l'ensemble des m-uplets d'inversibles modulo n ($(\mathbb{Z}_n^\times)^m$)

1.2 Définitions

Définition 1. *Une **singularité** est un $[a] = ([a_1], \ldots, [a_m]) \in S_n^m$, on appelle*

- *n la **racine** de la singularité*
- *$[a_1], \ldots, [a_m]$ les **poids** de la singularité*

Définition 2. *Un **éclatement** $a \in \mathbb{Z}^m$ d'une singularité $[a] \in S_n^m$ (noté $a \in [a]$) est un choix de représentant $a = (a_1, \ldots, a_m)$ tel que*

$$\forall i \neq j : a_i \perp a_j$$

On note E_a l'ensemble des singularités associées à l'éclatement a comme suit:

$$\begin{aligned} &E_a = \{[a^i] \in S_{a_i}^m \mid \forall i = 1..m,\ a_i > 1\} \\ &[a^i] = ([a_1^i], \ldots, [a_m^i]) \\ &[a_j^i] \equiv \begin{cases} -n & si\ i = j \\ a_j & sinon \end{cases} \pmod{a_i} \quad \forall j = 1..m \end{aligned}$$

*On appelle $a = (a_1, \ldots, a_m)$ **l'éclatement naturel** de $[a]$ si les $a_1, \ldots, a_m$ sont les plus petits représentant positifs de leurs classes*

Définition 3. *Un éclatement $a \in [a]$ est dit **lisse** si $a = (1, \ldots, 1)$*

Définition 4. *La singularité $[a]$ est dite de **type** $\mathfrak{J}$ (noté $[a] \in \mathfrak{J}$) ssi*

$$\exists a \in [a] : E_a \subset \mathfrak{J}$$

*On parlera de **type** $\mathfrak{J}$ **strict** (noté $[a] \in \overline{\mathfrak{J}}$) lorsque pour $a \in [a]$ l'éclatement naturel de $[a]$ on a*

$$E_a \subset \overline{\mathfrak{J}}$$

1.3 Rappels d'arithmétique

1.3.1 Algorithme d'Euclide et PGCD

Soit $a, b \in \mathbb{Z}$, on calcule le PGCD comme suit

$$\gcd(a,b) := \begin{cases} a & \text{si } b = 0 \\ \gcd(b, a \mod b) & \text{sinon} \end{cases}$$

Avec $k \in \mathbb{Z}$, on a les propriétés suivantes:

$$\begin{aligned} \gcd(a,1) &= 1 \\ \gcd(a,b) &= \gcd(b,a) \\ \gcd(a,b) &= \gcd(a,-b) \\ \gcd(a,b) &= \gcd(a,b+ka) \end{aligned}$$

De la dernière on déduit directement, pour $n \in \mathbb{N}$

$$a \equiv b \pmod n \implies \gcd(a,n) = \gcd(b,n)$$

1.3.2 Théorème des restes chinois

Soit $m, n_1, \ldots, n_m \in \mathbb{N}$ et $a_1, \ldots, a_m \in \mathbb{Z}$, notons le produit $n = n_1 \cdots n_m$

Si $\forall i \neq j : n_i \perp n_j$, alors $\exists! x \in \mathbb{Z}_n$ tel que

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_m \pmod{n_m} \end{aligned}$$

Cette solution, pour $m = 2$ est obtenue comme suit

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

Puisque $n_1 \perp n_2$, on a $s, t \in \mathbb{Z}$ tels que $1 = sn_1 + tn_2$

Et donc $x = a_1 t n_2 + a_2 s n_1$ est l'unique solution $\pmod{n_1 n_2}$

Cette méthode nous laisse $m - 1$ équations dans le système

Il suffit d'itérer le processus jusqu'à ce qu'il n'est reste qu'une pour $m > 2$

1.4 Résultats connus

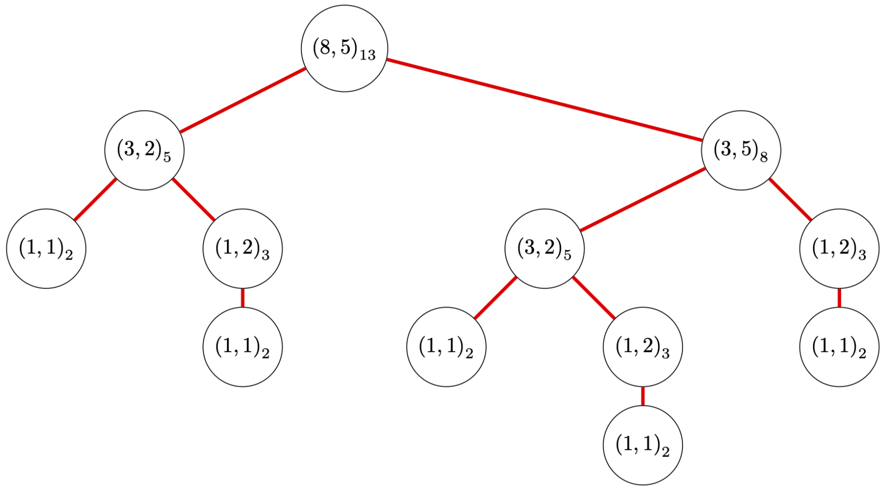
Résultats utiles, dûs à Habib Jaber.

Proposition 1. *Soit* $a, b \in \mathbb{Z}$

$$a \perp b \implies (a,b)_{a+b} \in \overline{\mathfrak{J}}$$

Exemple 1. $8 \perp 5 \implies (8,5)_{13} \in \overline{\mathfrak{J}}$

Figure 1: Illustration avec la suite de Fibonacci

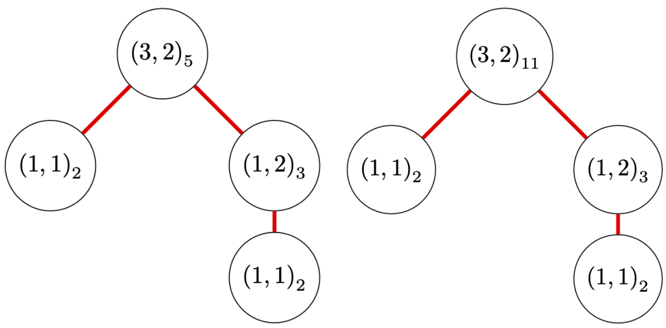


Proposition 2. *Soit* $a, b \in \mathbb{Z}$

$$(a,b)_n \in \overline{\mathfrak{J}} \implies \forall k \in \mathbb{Z}^\times : (a,b)_{n+kab} \in \overline{\mathfrak{J}}$$

Exemple 2. $[(3,2)]_5 \in \overline{\mathfrak{J}} \implies (3,2)_{11} \in \overline{\mathfrak{J}}$

Figure 2: $(3,2)_5 \cong (3,2)_{11}$



2 Propositions

Soit $m, n \in \mathbb{N}$ tels que $m, n \geq 2$ et une singularité $[a] = ([a_1], \dots, [a_m])_n \in S_n^m$

2.1 Existence d'un éclatement

Proposition 3. *Toute singularité isolée admet un éclatement*

Preuve. Prenons $(a_1, \dots, a_m) \in [a]$ le représentant naturel de $[a]$
On cherche $(b_1, \dots, b_m) \in [a]$ tels que $\forall i \neq j : b_i \perp b_j$ et $\forall i : b_i \perp n$
Il suffit de prendre $b_1 = a_1$ et $\forall i = 2..m$, un b_i vérifiant

$$\begin{aligned} b_i &\equiv a_i \pmod{n} \\ b_i &\equiv 1 \pmod{b_1} \\ &\vdots \\ b_i &\equiv 1 \pmod{b_{i-1}} \end{aligned}$$

De tels b_i existent par le théorème des restes chinois
On vérifie les coprimalités nécéssaires grâce aux propriétés de gcd
On a par la première congruence $\forall i : b_i \perp n$ (puisque $\forall i : a_i \perp n$)
Et par les suivantes $\forall i \neq j : b_i \perp b_j$
On a donc $b = (b_1, \dots, b_m)$ un éclatement de $[a]$ $\square$

2.2 Propriétés

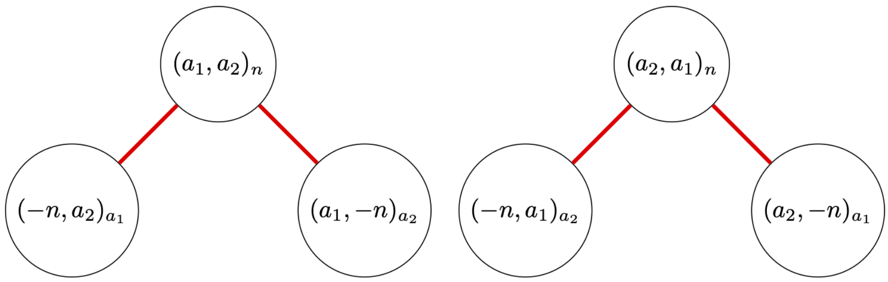
2.2.1 Symmétrie

Proposition 4. *Le réarrangement des poids préserve le type $\mathfrak{J}$. Soit $\sigma \in S_m$, on a*

$$[a] \in \mathfrak{J} \implies \sigma([a]) \in \mathfrak{J}$$

Preuve. Prenons $a \in [a]$ tel que $E_a \subset \mathfrak{J}$
Il suffit d'observer que $E_a \cong E_{\sigma(a)}$ $\square$

Figure 3: Illustration avec $a = (a_1, a_2)$, $\sigma = (12)$



2.2.2 Ajout de poids

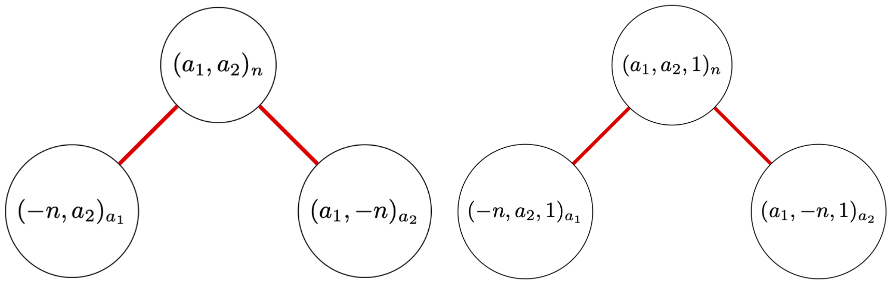
Proposition 5. *L'ajout de poids de valeur 1 préserve le type* $\mathfrak{J}$

$$([a_1], \ldots, [a_m])_n \in \mathfrak{J} \implies ([a_1], \ldots, [a_m], [1])_n \in \mathfrak{J}$$

Preuve. Prenons $a \in [a]$ tel que $E_a \subset \mathfrak{J}$, $b = (a_1, \ldots, a_m, 1)$

Il suffit d'observer que $E_a \cong E_b$ $\square$

Figure 4: Illustration avec $a = (a_1, a_2)$



2.2.3 Retrait de poids

Proposition 6. *Le retrait de poids préserve le type* $\mathfrak{J}$

$$([a_1], \ldots, [a_m])_n \in \mathfrak{J} \implies ([a_1], \ldots, [a_{m-1}])_n \in \mathfrak{J}$$

Preuve. Prenons $a \in [a]$ tel que $E_a \subset \mathfrak{J}$

La preuve se fait par induction structurelle

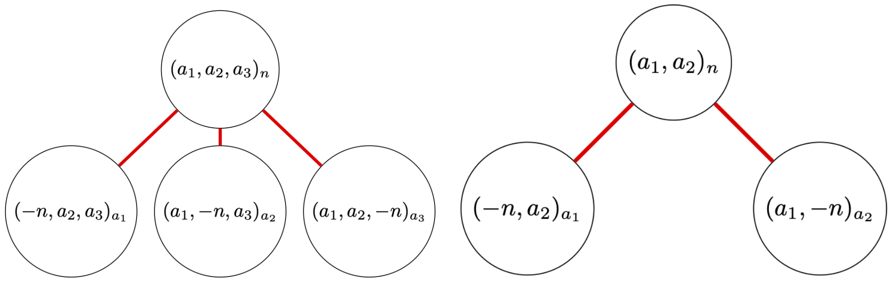
D'abord, on observe $([1], \ldots, [1])_n \in \mathfrak{J}$

Puis on suppose que $\forall [b] \in E_a : [b] \in \mathfrak{J} \implies ([b_1], \ldots, [b_{m-1}])_n \in \mathfrak{J}$

On en conclut $([a_1], \ldots, [a_{m-1}])_n \in \mathfrak{J}$

$\square$

Figure 5: Illustration pour $m = 3$



2.3 Caractérisation stricte

2.3.1 Frontière

Proposition 7. *Soit* $[a] \in S_n^2$, *d'éclatement naturel* $a = (a_1, a_2) \in [a]$

$$[a] \in \overline{\mathfrak{J}} \implies n \geq a_1 + a_2$$

Preuve. Par contraposée, supposons $n < a_1 + a_2$ $(\star)$

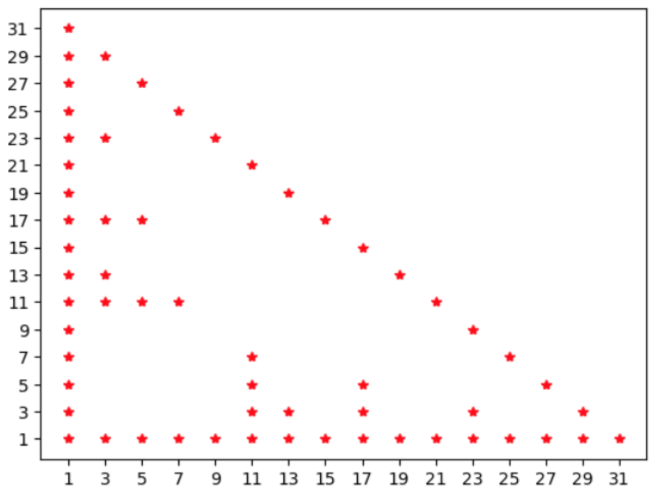
- Si $a_1 = a_2$ ($\neq 1$ par $(\star)$)
  Alors $[a] \notin \overline{\mathfrak{J}}$
- Sinon, $a_1 \neq a_2$, supposons sans perdre de généralité que $a_1 > a_2$
  Considérons a^1 l'éclatement naturel de $[a^1] \in E_a$ la singularité associée à a_1
  On a $a^1 = (-n \mod a_1,\ a_2 \mod a_1)$
  - Puisque $a_1 > a_2$, on a $2a_1 > a_1 + a_2 > n$, donc $a_1 < n < 2a_1$
    On en déduit $(-n \mod a_1) = 2a_1 - n$
  - Aussi, $(a_2 \mod a_1) = a_2$ car $a_1 > a_2$

  On a donc $a^1 = (2a_1 - n,\ a_2)$
  Puisque $n < a_1 + a_2$, on a $a_1 < 2a_1 - n + a_2$
  Donc $[a^1] \in S_{a_1}^2$ vérifie la condition $(\star)$, on répète le raisonnement avec $[a^1]$

□

Exemple 3. $(4,3)_5 \notin \overline{\mathfrak{J}}$ *car* $5(4+3$

Figure 6: Singularités $s \in S_{32}^2$ telles que $s \in \overline{\mathfrak{J}}$



3 Conjectures

3.1 Combinaison linéaire

Conjecture 1. *Soit* $(a,b)_n \in \overline{\mathfrak{J}}$, *alors* $\exists \alpha, \beta \in \mathbb{N}_{>0}$ *tels que*

$$\alpha a + \beta b = n$$

Preuve. Puisque $a \perp b$, prenons $s, t \in \mathbb{Z}$ tels que $1 = as + bt$ (par Bézout)

Considérons les systèmes modulaires suivants

$$\begin{aligned} x &\equiv 0 \pmod a & y &\equiv n \pmod a \\ x &\equiv n \pmod b & y &\equiv 0 \pmod b \end{aligned}$$

Par le Théorème des restes chinois, les uniques solutions sont

$$\begin{aligned} x &\equiv nas \pmod{ab} \\ y &\equiv nbt \pmod{ab} \end{aligned}$$

On a donc (toujours modulo ab)

$$\begin{aligned} x + y &\equiv nas + nbt \\ &\equiv n(as + bt) \\ &\equiv n \end{aligned}$$

Et comme $a|x$ et $b|y$, prenons $\alpha = \frac{x}{a}$ et $\beta = \frac{y}{b}$, des entiers

$$\begin{aligned} n &\equiv x + y \\ &\equiv \frac{x}{a}a + \frac{y}{b}b \\ &\equiv \alpha a + \beta b \end{aligned}$$

Il reste à montrer que cette égalité n'est pas seulement vraie dans $\mathbb{Z}_{ab}$ mais aussi dans $\mathbb{Z}$ □

Une piste de recherche explorée jusqu'ici sans succès passe par le probème des pièces de monnaie, on peut reformuler la conjecture comme suit: $(a,b)_n \in \overline{\mathfrak{J}}$ implique que n est représentable par a et b, même si $n < g(a,b)$ le nombre de Frobenius. Il est connu que la moitié de ces nombres $a + b < n < g(a,b)$ (ceux de la forme $n = ab - ka - qb$) sont non-représentables. Montrer que ces $(a,b)_n \notin \overline{\mathfrak{J}}$ suffirait à montrer la conjecture.

3.2 Anti-symmétrie

Corollaire 1. *Soit* $[s] \in S_n^2$ *d'éclatement naturel* $(a,b) \in [s]$, *avec* $a, b > 1$, *alors*

$$(a,b)_n \in \overline{\mathfrak{J}} \implies (-a,b)_n \notin \overline{\mathfrak{J}}$$

Preuve. Supposons $(a,b)_n \in \overline{\mathfrak{J}}$

La chaine d'éclatements à gauche successifs de $(-a,b)_n$ est, pour $i > 0$, $n - ia > 0$

$$(n - ia, b)_{n-(i-1)a}$$

Prenons $\alpha, \beta \in \mathbb{N}_{>0}$ tels que $\alpha a + \beta b = n$

On a que, lorsque $i = \alpha$, $n - ia = n - \alpha a = \beta b$

Donc $b|n - ia$, $b \not\perp n - ia$, $(n - ia, b)_n \notin \overline{\mathfrak{J}}$ et $(-a,b)_n \notin \overline{\mathfrak{J}}$ □

3.3 Échange racine-poids

Corollaire 2. *Soit $[s] \in S_n^2$ d'éclatement naturel $(a,b) \in [s]$, avec $a,b > 1$, alors*

$$(a,b)_n \in \overline{\mathfrak{I}} \implies (n,b)_a \notin \overline{\mathfrak{I}}$$

Preuve. Supposons $(a,b)_n \in \overline{\mathfrak{I}}$
Donc son éclatement $(-n,b)_a \in \overline{\mathfrak{I}}$
Par Anti-symmétrie, $(n,b)_a \notin \overline{\mathfrak{I}}$ □

3.4 Restriction au bord

Corollaire 3. *Soit $[s] \in S_n^3$ d'éclatement naturel $(a,b,c) \in [s]$, avec $a,b,c > 1$, alors*

$$(a,b,c)_n \notin \overline{\mathfrak{I}}$$

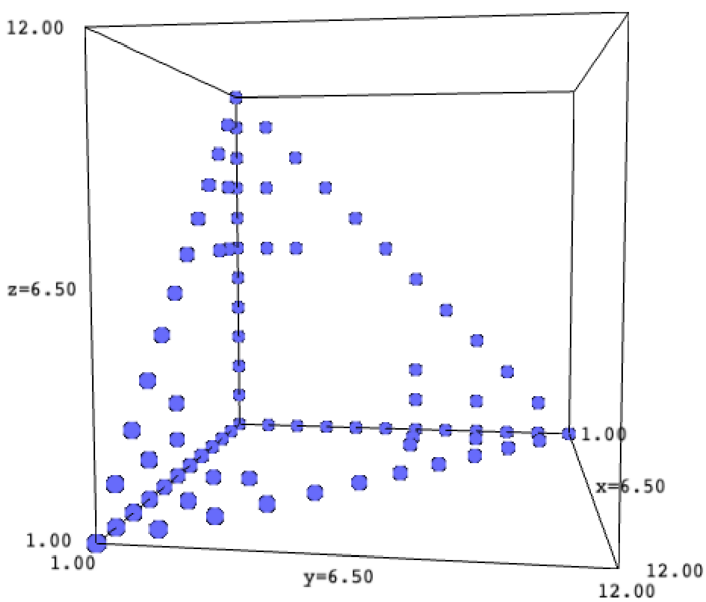
Preuve. Si $(a,b,c)_n \in \overline{\mathfrak{I}}$, alors ses éclatements $(-n,b,c)_a \in \overline{\mathfrak{I}}$ et $(a,-n,c)_b \in \overline{\mathfrak{I}}$
Par retrait de poids, $(b,c)_a \in \overline{\mathfrak{I}}$ et $(a,c)_b \in \overline{\mathfrak{I}}$
Contradiction avec Échange racine-poids □

Corollaire 4. *Pour être de type $\overline{\mathfrak{I}}$, une singularité ne peut avoir plus de 2 poids supérieurs à 1.*

Preuve. Si une singularité de type $\overline{\mathfrak{I}}$ contient les poids $a,b,c > 1$
Alors, par retrait de poids $(a,b,c)_n \in \overline{\mathfrak{I}}$, contradiction □

Exemple 4. *On observe que les singularités de type $\overline{\mathfrak{I}}$ de S_n^3 sont sur le bord*

Figure 7: Singularités $s \in S_{13}^3$ telles que $s \in \overline{\mathfrak{I}}$



Conjecture 2. *Si $[a] \in \overline{\mathfrak{I}}$, alors $[a] \in \mathfrak{I}$, donc $\mathfrak{I} = \overline{\mathfrak{I}}$*