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

Félix Larose-Gervais

Mai 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

- $Sym(X)$ le groupe de bijections de X dans lui-même
- $Sym(m)$ le groupe de bijections $Sym(\{1, \ldots, m\})$
- $\mathbb{Z}_n$ 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*

$$\exists a \in [a] : \forall [a^i] \in E_a : [a^i] \in \mathfrak{J}$$

*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*

$$\forall [a^i] \in E_a : [a^i] \in \overline{\mathfrak{J}}$$

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

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

1.4 Résultats connus

Résultats utiles, dûs à Habib Jaber.

Proposition 1. *Soit* $a_1, a_2 \in \mathbb{Z}$, $\gcd(a_1, a_2) = 1$, *alors*

$$[(a_1, a_2)]_{a_1+a_2} \in \mathfrak{J}$$

Exemple 1. $\gcd(2,1) = 1 \implies [(2,1)]_3 \in \mathfrak{J}$

Proposition 2.

$$[(a_1, a_2)]_n \in \mathfrak{J} \iff \forall k \in \mathbb{Z} : [(a_1, a_2)]_{n+ka_1a_2} \in \mathfrak{J}$$

Exemple 2. $[(2,1)]_3 \in \mathfrak{J} \implies [(2,1)]_5 \in \mathfrak{J},\ [(2,1)]_7 \in \mathfrak{J}, \ldots$

2 Propositions

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

2.1 Existence d'un éclatement

Proposition 3. *Toute singularité isolée admet un éclatement*

Preuve. Soit $[a] = ([a_1], \ldots, [a_m]) \in S_n^m$
Prenons $(a_1, \ldots, a_m) \in [a]$ son représentant naturel
On cherche $(b_1, \ldots, b_m) \in [a]$ 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 $b = (b_1, \ldots, b_m)$ un éclatement de $[a]$ □

2.2 Invariants

2.2.1 Ordre des poids

Soit $\sigma \in Sym(m)$, $\pi_\sigma \in Sym(S_n^m)$,

Proposition 4. *Le réarrangement des poids préserve le type $\mathfrak{J}$*
Notons $[b] = \pi_\sigma([a])$

$$[a] \in \mathfrak{J} \implies [b] \in \mathfrak{J}$$

Preuve. Il suffit d'observer que $E_a \cong E_b$ □

2.2.2 Ajout de poids

Proposition 5. *L'ajout de poids congrus à 1 modulo n préserve le type $\mathfrak{J}$*
Notons $[b] = ([a_1], \ldots, [a_m], [1]) \in S_n^{m+1}$

$$[a] \in \mathfrak{J} \implies [b] \in \mathfrak{J}$$

Preuve. Il suffit d'observer que $E_a \cong E_b$ □

2.2.3 Retrait de poids

Proposition 6. *Le retrait de poids préserve le type $\mathfrak{J}$*
Notons $[b] = ([a_1], \ldots, [a_{m-1}]) \in S_n^{m-1}$

$$[a] \in \mathfrak{J} \implies [b] \in \mathfrak{J}$$

Preuve. TODO □

2.3 Caractérisation stricte

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

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

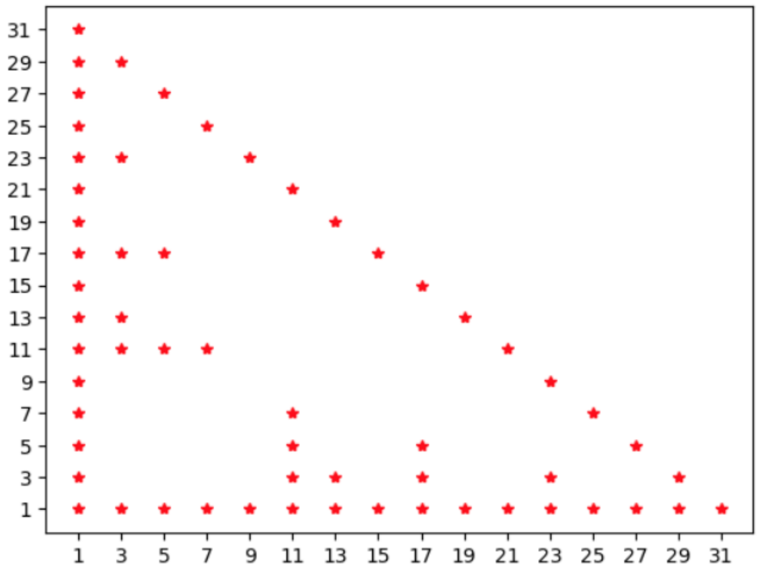
Preuve. Par contraposée, supposons $n < a_1 + a_2$ $(\star)$

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



3 Conjectures

Conjecture 1. *Soit* $[a] \in S_n^m$ *de représentant naturel* $a = (a_1, \ldots, a_m) \in \mathbb{Z}^m$

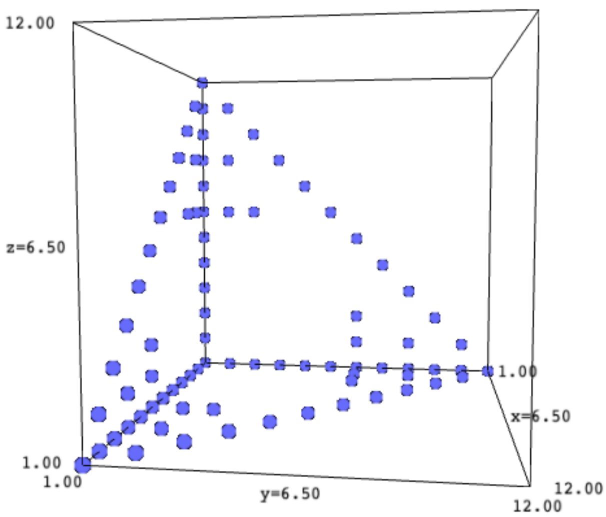
$$[a] \in \overline{\mathfrak{J}} \implies |\{a_i \in a \mid a_i > 1\}| \leq 2$$

Preuve. Par contraposée, supposons $1 < a_1, a_2, a_3$ $(\star)$

- Si $\exists i \neq j : a_i = a_j \neq 1$
  Alors $[a] \notin \overline{\mathfrak{J}}$
- Sinon $(\forall i \neq j, a_i \neq 1 : a_i \neq a_j)$
  Supposons sans perdre de généralité $a_1 > a_2 > a_3 > \cdots \geq a_m$ (Donc $a_1 \geq 4$)
  Considérons a^1 l'éclatement naturel de $[a^1] \in E_a$ la singularité associée à a_1
  On a $a^1 = (-n \mod a_1, a_2 \mod a_1, \ldots, a_m \mod a_1) = (-n \mod a_1, a_2, \ldots, a_m)$
  On sait que $(-n \mod a_1) \neq 0$ car $a_1 \perp n$
  Il suffit de montrer que $(-n \mod a_1) \neq 1$ pour que $[a^1]$ vérifie $(\star)$
  Impossible (contre-exemple: (5, 3, 2) mod 29)
  Tous ces éclatements ont m=2, or pas j strict

$\square$

Figure 2: Singularités $s \in S_{13}^3$ telles que $s \in \overline{\mathfrak{J}}$



Corollaire 1. *Soit la singularite* $[a] \in S_n^m$ *de représentant naturel* $a = (a_1, a_2, \ldots, a_m) \in \mathbb{Z}^m$
Supposons sans perdre de généralité que $a_1 > a_2 > \cdots > a_m$*, alors*

$$[a] \in \overline{\mathfrak{J}} \iff a_3 = \cdots = a_m = 1 \text{ et } [(a_1, a_2)]_n \in \overline{\mathfrak{J}}$$

Preuve. D'après les proposition précédentes

- ($\Longleftarrow$) Si $a_3 = \cdots = a_m = 1$ et $[(a_1, a_2)]_n \in \overline{\mathfrak{J}}$
  Comme $[(a_1, a_2)]_n \in \overline{\mathfrak{J}}$, on a $[a] \in \overline{\mathfrak{J}}$ (par ajout de poids à 1)
- ($\Longrightarrow$) Si $[a] \in \overline{\mathfrak{J}}$
  Alors $a = (a_1, a_2, 1, \ldots, 1)$ (par la conjecture)
  Et $[(a_1, a_2)] \in \overline{\mathfrak{J}}$ (par retrait de poids)

$\square$

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