

Caractérisation des singularités de type \mathfrak{J}

Félix Larose-Gervais

Mai 2023

Contents

1	Introduction	3
1.1	Notations	3
1.2	Définitions	3
1.3	Rappels d'arithmétique	4
1.3.1	Algorithme d'Euclide et PGCD	4
1.3.2	Théorème des restes chinois	4
1.4	Résultats connus	4
2	Propositions	5
2.1	Existence d'un éclatement	5
2.2	Caractérisation des singularités de type \mathfrak{J} à 1 poids	5
2.3	Ordre des poids	6
3	Conjectures	7

1 Introduction

1.1 Notations

Soit $a, b \in \mathbb{Z}$ on note la relation de coprimauté \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 $Sym(\{1, \dots, m\})$
- \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 les m-uplets de X ($\underbrace{X \times \dots \times X}_{m \text{ fois}}$)

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

1.2 Définitions

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

- n la **racine** de la singularité
- $[a_1], \dots, [a_m]$ les **poïds** 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 $a = (a_1, \dots, a_m)$ 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:

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

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

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

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

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

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

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

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 $m, n_1, \dots, n_m \in \mathbb{N}$ et $a_1, \dots, a_m \in \mathbb{Z}$, 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. $[(2, 1)]_3 \in \mathfrak{J} \implies [(2, 1)]_5 \in \mathfrak{J}, [(2, 1)]_7 \in \mathfrak{J}, \dots$

2 Propositions

2.1 Existence d'un éclatement

Question: La condition de coprimauté 2-à-2 est-elle contraignante? Existe-t-il des singularités n'admettant aucun éclatement?

Proposition 3. *Toute singularité isolée admet un éclatement*

Proof. Soit $[a] = ([a_1], \dots, [a_m]) \in S_n^m$

Prenons $(a_1, \dots, a_m) \in [a]$ son représentant naturel

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 coprimautés nécessaires 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 $[a]$

□

2.2 Caractérisation des singularités de type \mathfrak{J} à 1 poids

On sait déjà que la condition de coprimauté est nécessaire à être de type \mathfrak{J} .

On montre maintenant qu'elle est en fait suffisante (pour 1 poids)

Proposition 4. *Soit $a, n \in \mathbb{Z}$, alors*

$$a \perp n \implies [a]_n \in \mathfrak{J}$$

Proof. Soit $[a] \in S_n^1$, on prend $a \in [a]$ son représentant naturel ($a < n$)

Si $a = 1$, alors $[a] \in \mathfrak{J}$

Sinon, prenons le singleton $E_a = \{(-n \bmod a) \in S_n^1\}$

Il suffit de montrer que $(-n \bmod a) \perp a$ pour répéter le raisonnement

Or on a, grâce aux propriétés de gcd

$$\begin{aligned} a \perp n &\implies a \perp n - a \\ &\implies a \perp a - n \\ &\implies a \perp (-n \bmod a) \\ &\implies (-n \bmod a) \perp a \end{aligned}$$

□

2.3 Ordre des poids

Soit $\sigma \in \text{Sym}(m)$, et ces permutations associées $\pi_\sigma \in \text{Sym}(S_n^m)$

Proposition 5. *L'ordre des poids d'une singularité n'affecte pas le type \mathfrak{J}*

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

Proof. Pour $a = (a_1, \dots, a_m) \in [a]$ tel que $\forall [a^i] \in E_a : [a^i] \in \mathfrak{J}$, on a

1. Cas de base: $E_a = \emptyset$

On a donc $a = (1, \dots, 1)$

Ainsi $[a] = ([1], \dots, [1]) = \pi_\sigma([a]) \in \mathfrak{J}$

2. Induction structurelle

Supposons $\forall [a^i] \in E_a : [a^i] \in \mathfrak{J} \implies \pi_\sigma([a^i]) \in \mathfrak{J}$

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

Considérons, pour $b = (b_1, \dots, b_m) = (a_{\sigma(1)}, \dots, a_{\sigma(m)}) \in \pi_\sigma([a])$

$$\begin{aligned} E_b &= \{[b^i] \in S_{b_i}^m \mid \forall i = 1..m, b_i > 1\} \\ [b^i] &= ([b_1^i], \dots, [b_m^i]) \\ [b_j^i] &\equiv \begin{cases} -n & \text{si } i = j \\ b_j & \text{sinon} \end{cases} \pmod{b_i} \quad \forall j = 1..m \\ &\equiv \begin{cases} -n & \text{si } \sigma(i) = \sigma(j) \\ a_{\sigma(j)} & \text{sinon} \end{cases} \pmod{a_{\sigma(i)}} \\ &\equiv [a_{\sigma(j)}^{\sigma(i)}] \\ [b^i] &= ([a_{\sigma(1)}^{\sigma(i)}], \dots, [a_{\sigma(m)}^{\sigma(i)}]) \\ &= \pi_\sigma([a^{\sigma(i)}]) \in \mathfrak{J} \end{aligned}$$

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

□

Exemple 3. Sachant $[(3, 2)]_5 \in \mathfrak{J}$, on en déduit $[(2, 3)]_5 \in \mathfrak{J}$

Proposition 6. (*strict, rework*) Soit $a = (a_0, a_1, a_2)$, alors

$$a \in \mathfrak{J} \implies a_0 \geq a_1 + a_2$$

Proof. Supposons $a_0 < a_1 + a_2$

Si $a_1 = a_2$, alors $\neg \mathfrak{J}(a)$

Sinon, $a_1 \neq a_2$, supposons sans perdre de généralité que $a_1 > a_2$

Considérons l'éclatement $a^1 = (a_1, -a_0 \bmod a_1, a_2 \bmod a_1) \in E_a$

$$\begin{aligned} a_1 > a_2 &\implies 2a_1 > a_1 + a_2 \\ &\implies (-a_0 \bmod a_1) = 2a_1 - a_0 \\ a_1 > a_2 &\implies (a_2 \bmod a_1) = a_2 \end{aligned}$$

On a donc $a^1 = (a_1, 2a_1 - a_0, a_2)$

Puisque $a_0 < a_1 + a_2$, on a $a_1 < 2a_1 - a_0 + a_2$

Donc a^1 vérifie la condition initiale, on répète le raisonnement avec a^1 □

Exemple 4. $(5, 4, 3) \notin \mathfrak{J}$ car $5 < 7$

3 Conjectures

Conjecture 1. Soit $a = (a_0, a_1, a_2)$ un éclatement d'une singularité $[a]$

Posons $s = a_1 + a_2 + \gcd(a_0 - a_1, a_0 - a_2)$

Supposons $a_0 < s$

Alors $[a]$ est de type $\mathfrak{J} \implies s = a_0 + 1$

On constate que la réciproque n'est pas vraie, par exemple prenons $(13, 7, 4)$, on a $s = 14$, vérifiant donc $a_0 < 14$ et $a_0 + 1 = 14$, or elle n'est pas de type \mathfrak{J} .

Conjecture 2. Soit $a = (a_0, a_1, a_2)$ un éclatement d'une singularité $[a]$

Alors $[a]$ est de type $\mathfrak{J} \implies \exists p, q : a_0 = p * a_1 + q * a_2$

Conjecture 3. (*strict*) Soit $[a] = ([a_1], \dots, [a_m]) \in \mathfrak{J}, m \geq 2$

Alors $|\{a_i \in [a] \mid a_i = 1\}| \geq m - 2$

Conjecture 4. Si $[a] \in \mathfrak{J}$, alors son représentant naturel $a \in [a]$ offre une suite d'éclatement montrant $[a] \in \mathfrak{J}$