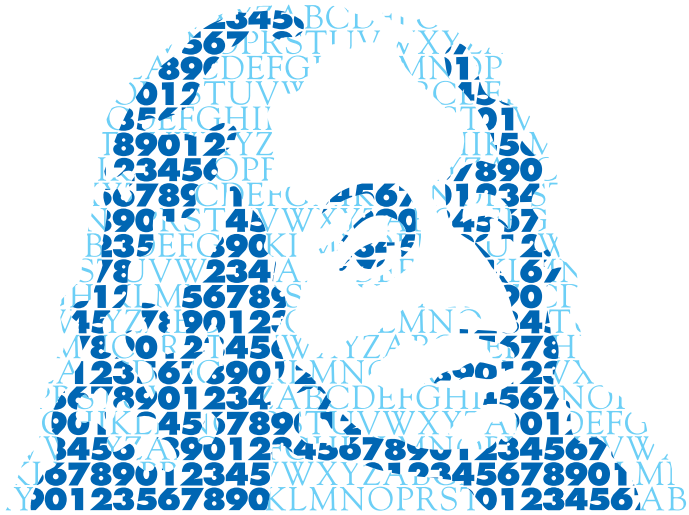
ANNALES MATHÉMATIQUES



BLAISE PASCAL

Flavien Mabilat

Combinatoire des sous-groupes de congruence du groupe modulaire

Volume 28, nº 1 (2021), p. 7-43.

<http://ambp.centre-mersenne.org/item?id=AMBP_2021__28_1_7_0>

Publication éditée par le laboratoire de mathématiques Blaise Pascal
de l'université Clermont Auvergne, UMR 6620 du CNRS
Clermont-Ferrand — France

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/

Annales mathématiques Blaise Pascal **28**, 7-43 (2021)

Combinatoire des sous-groupes de congruence du groupe modulaire

Flavien Mabilat

Résumé

Dans cet article, on étudie la combinatoire des sous-groupes de congruence du groupe modulaire en généralisant des résultats obtenus dans le cas non modulaire. On définit pour cela une notion de solutions irréductibles à partir desquelles on peut construire l'ensemble des solutions. En particulier, on donne une solution particulière, irréductible pour N quelconque, et la description explicite des solutions irréductibles pour $N \leq 6$.

Combinatorics of congruence subgroups of the modular group

Abstract

In this paper, we study the combinatorics of congruence subgroups of the modular group by generalizing results obtained in the non-modular case. For this, we define a notion of irreducible solutions from which we can build all the solutions. In particular, we give a particular solution, irreducible for any N, and the list of irreducible solutions for $N \leq 6$.

« *Puisque ces mystères nous dépassent, feignons d'en être l'organisateur.* »
Jean Cocteau, *Les Mariés de la tour Eiffel*

1. Introduction

La connaissance de parties génératrices à deux éléments du groupe modulaire

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

est l'une des propriétés les plus remarquables de ce groupe. On peut notamment choisir les deux éléments suivants (voir par exemple [1]) :

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

On déduit de ce choix que pour tout élément A de $\mathrm{SL}_2(\mathbb{Z})$ il existe un entier strictement positif n et des entiers strictement positifs $a_1, \ldots, a_n$ tels que

$$A = T^{a_n} S T^{a_{n-1}} S \cdots T^{a_1} S = \begin{pmatrix} a_n & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Mots-clés : groupe modulaire, sous-groupe de congruence, quiddité.
Classification Mathématique (2020) : 05A05.

On utilisera la notation $M_n(a_1, \dots, a_n)$ pour désigner la matrice

$$\begin{pmatrix} a_n & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Remarquons que l'écriture d'un élément de $\mathrm{SL}_2(\mathbb{Z})$ sous cette forme n'est pas unique (pour une façon d'assurer l'unicité d'une écriture de cette forme on peut consulter [12]).

L'écriture des éléments du groupe modulaire sous cette forme et l'absence d'unicité incite, d'une part, à essayer de trouver toutes les écritures d'une matrice sous la forme $M_n(c_1, \dots, c_n)$ et, d'autre part, à chercher des descriptions combinatoires des solutions en utilisant l'idée générale que des entiers strictement positifs comptent des objets (notamment géométriques). V. Ovsienko (voir [13]) a donné notamment les solutions (et une description combinatoire de celles-ci en terme de découpages de polygones) de l'équation suivante :

$$M_n(a_1, \dots, a_n) = \pm \mathrm{Id}\,. \tag{1.1}$$

En particulier, ce résultat généralise un théorème antérieur dû à Conway et Coxeter (voir [2, 3, 6]). On dispose également de résultats analogues sur l'équation suivante (voir [9]) :

$$M_n(a_1, \dots, a_n) = \pm S. \tag{1.2}$$

Une autre façon d'exploiter l'écriture des éléments du groupe modulaire sous la forme $M_n(a_1, \dots, a_n)$ est de chercher toutes les écritures des éléments d'un sous-groupe donné. Notre objectif ici est de mener à bien cette démarche dans le cas des sous-groupes de congruence suivants :

$$\widehat{\Gamma}(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \text{ tel que } A = \pm \mathrm{Id} \pmod N\}.$$

Ce problème est équivalent à la résolution de l'équation suivante dans $\mathbb{Z}/N\mathbb{Z}$:

$$M_n(a_1, \dots, a_n) = \pm \mathrm{Id}\,. \tag{E_N}$$

Notons que l'équation (E_N) apparaît naturellement dans la théorie des frises de Coxeter (voir [10, 11]). Les solutions de (E_N) étant invariantes par permutations circulaires on considère les solutions $(a_1, \dots, a_n)$ comme des séquences infinies n-périodiques. On dispose déjà des solutions dans le cas où $N = 2$ (voir [8] et la section 4). Pour mener à bien la résolution de cette équation, on définit une notion de solution irréductible à partir de laquelle on pourra construire l'ensemble des solutions (voir section suivante). On s'intéressera en particulier à la résolution de (E_N) pour les petites valeurs de N (voir section 4) et à la recherche de solutions irréductibles dans le cas général (voir section 3).

2. **Résultats principaux**

L'objectif de cette section est de définir la notion d'irréductibilité évoquée dans la section précédente et d'énoncer les résultats principaux de ce texte. Cette notion d'irréductibilité repose sur la notion de somme introduite dans [4] (voir aussi [14]). Sauf mention contraire, N désigne un entier naturel supérieur à 2 et si $a \in \mathbb{Z}$ on note $\bar{a} := a + N\mathbb{Z}$.

Définition 2.1 ([14, définition 1.8])**.** Soient $(\overline{a_1}, \dots, \overline{a_n}) \in (\mathbb{Z}/N\mathbb{Z})^n$ et $(\overline{b_1}, \dots, \overline{b_m}) \in (\mathbb{Z}/N\mathbb{Z})^m$. On définit l'opération suivante :

$$(\overline{a_1}, \dots, \overline{a_n}) \oplus (\overline{b_1}, \dots, \overline{b_m}) := (\overline{a_1 + b_m}, \overline{a_2}, \dots, \overline{a_{n-1}}, \overline{a_n + b_1}, \overline{b_2}, \dots, \overline{b_{m-1}}).$$

Le $(n + m - 2)$-uplet obtenu est appelé la somme de $(\overline{a_1}, \dots, \overline{a_n})$ avec $(\overline{b_1}, \dots, \overline{b_m})$.

Exemple 2.2. Voici quelques exemples de somme :

- $(\bar{1}, \bar{2}, \bar{1}) \oplus (\bar{2}, \bar{0}, \bar{1}, \bar{2}) = (\bar{3}, \bar{2}, \bar{3}, \bar{0}, \bar{1})$,
- $(\bar{3}, \bar{2}, \bar{1}, \bar{1}) \oplus (\bar{1}, \bar{0}, \bar{1}) = (\bar{4}, \bar{2}, \bar{1}, \bar{2}, \bar{0})$,
- $n \geq 2$, $(\overline{a_1}, \dots, \overline{a_n}) \oplus (\bar{0}, \bar{0}) = (\bar{0}, \bar{0}) \oplus (\overline{a_1}, \dots, \overline{a_n}) = (\overline{a_1}, \dots, \overline{a_n})$.

Remarque 2.3. L'opération ci-dessus n'est pas commutative. En effet, on a dans [14] l'exemple suivant :

$$(\bar{1}, \bar{1}, \bar{1}) \oplus (\bar{2}, \bar{1}, \bar{2}, \bar{1}) = (\bar{2}, \bar{1}, \bar{3}, \bar{1}, \bar{2}) \neq (\bar{3}, \bar{1}, \bar{2}, \bar{2}, \bar{1}) = (\bar{2}, \bar{1}, \bar{2}, \bar{1}) \oplus (\bar{1}, \bar{1}, \bar{1}), \ (N \neq 1).$$

On montre en particulier que la somme de deux solutions est encore une solution (voir [4, lemme 2.7] et section suivante). Avant de définir la notion de solution irréductible on a encore besoin de la définition suivante :

Définition 2.4 ([14, définition 1.5])**.** Soient $(\overline{a_1}, \dots, \overline{a_n}) \in (\mathbb{Z}/N\mathbb{Z})^n$ et $(\overline{b_1}, \dots, \overline{b_n}) \in (\mathbb{Z}/N\mathbb{Z})^n$. On dit que $(\overline{a_1}, \dots, \overline{a_n}) \sim (\overline{b_1}, \dots, \overline{b_n})$ si $(\overline{b_1}, \dots, \overline{b_n})$ est obtenu par permutation circulaire de $(\overline{a_1}, \dots, \overline{a_n})$ ou de $(\overline{a_n}, \dots, \overline{a_1})$.

On peut montrer ([14, lemme 1.7]) que $\sim$ est une relation d'équivalence. En particulier, si on a $(\overline{a_1}, \dots, \overline{a_n}) \sim (\overline{b_1}, \dots, \overline{b_n})$ alors $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_N) si et seulement si $(\overline{b_1}, \dots, \overline{b_n})$ est solution de (E_N) (voir [4, proposition 2.6] et également la section 3). On peut maintenant définir la notion d'irréductibilité annoncée dans l'introduction.

Définition 2.5 ([4, définition 2.9])**.** Une solution $(\overline{c_1}, \dots, \overline{c_n})$ avec $n \geq 3$ de (E_N) est dite réductible s'il existe deux solutions de (E_N) $(\overline{a_1}, \dots, \overline{a_m})$ et $(\overline{b_1}, \dots, \overline{b_l})$ telles que

- $(\overline{c_1}, \dots, \overline{c_n}) \sim (\overline{a_1}, \dots, \overline{a_m}) \oplus (\overline{b_1}, \dots, \overline{b_l})$,

- $m \geq 3$ et $l \geq 3$.

Une solution est dite irréductible si elle n'est pas réductible.

Remarque 2.6. $(\bar{0}, \bar{0})$ n'est pas considérée comme étant une solution irréductible de (E_N).

Cette notion d'irréductibilité est celle que l'on va utiliser pour résoudre (E_N).

Pour $N = 1$, l'équation (E_N) n'a pas d'intérêt et, pour $N = 0$, l'équation se ramène à la résolution dans $\mathbb{Z}$ de l'équation $M_n(a_1, \ldots, a_n) = \pm \mathrm{Id}$. On dispose dans ce cas du résultat suivant :

Théorème 2.7 (Cuntz, Holm [4, Théorème 3.2])**.** *L'ensemble des solutions irréductibles de* (E_0) *est*

$$\{(1,1,1), (-1,-1,-1), (a,0,-a,0), (0,-a,0,a), a \in \mathbb{Z} - \{\pm 1\}\}.$$

On dispose également d'une description combinatoire de ces solutions (voir [5, théorème 7.3]).

On s'intéresse donc dans cette article aux cas $N \geq 2$. On va établir les résultats suivants :

Théorème 2.8.

(i) *Les solutions irréductibles de* (E_2) *sont* $(\bar{1}, \bar{1}, \bar{1})$ *et* $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$.

(ii) *Les solutions irréductibles de* (E_3) *sont* $(\bar{1}, \bar{1}, \bar{1})$, $(\overline{-1}, \overline{-1}, \overline{-1})$ *et* $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$.

(iii) *Les solutions irréductibles de* (E_4) *sont* $(\bar{1}, \bar{1}, \bar{1})$, $(\overline{-1}, \overline{-1}, \overline{-1})$, $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$, $(\bar{0}, \bar{2}, \bar{0}, \bar{2})$,$(\bar{2}, \bar{0}, \bar{2}, \bar{0})$ *et* $(\bar{2}, \bar{2}, \bar{2}, \bar{2})$.

(iv) *Les solutions irréductibles de* (E_5) *sont (à permutations cycliques près)* $(\bar{1}, \bar{1}, \bar{1})$, $(\overline{-1}, \overline{-1}, \overline{-1})$, $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$, $(\bar{0}, \bar{2}, \bar{0}, \bar{3})$, $(\bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{2})$, $(\bar{3}, \bar{3}, \bar{3}, \bar{3}, \bar{3})$, $(\bar{3}, \bar{2}, \bar{2}, \bar{3}, \bar{2}, \bar{2})$, $(\bar{2}, \bar{3}, \bar{3}, \bar{2}, \bar{3}, \bar{3})$, $(\bar{2}, \bar{3}, \bar{2}, \bar{3}, \bar{2}, \bar{3})$.

(v) *Les solutions irréductibles de* (E_6) *sont (à permutations cycliques près)* $(\bar{1}, \bar{1}, \bar{1})$, $(\overline{-1}, \overline{-1}, \overline{-1})$, $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$, $(\bar{2}, \bar{4}, \bar{2}, \bar{4})$, $(\bar{2}, \bar{3}, \bar{4}, \bar{3})$, $(\bar{0}, \bar{2}, \bar{0}, \bar{4})$, $(\bar{0}, \bar{3}, \bar{0}, \bar{3})$, $(\bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{2})$, $(\bar{3}, \bar{3}, \bar{3}, \bar{3}, \bar{3}, \bar{3})$, $(\bar{4}, \bar{4}, \bar{4}, \bar{4}, \bar{4}, \bar{4})$.

Ces résultats sont démontrés dans la section 4. On donne également en section 4 les solutions irréductibles de (E_7) obtenues avec assistance informatique.

On montre également dans la section 3 le résultat suivant :

Théorème 2.9. *Si* $N \geq 3$, $(\bar{2}, \ldots, \bar{2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ *est une solution irréductible de* (E_N).

3. **Résultats généraux sur l'équation** (E_N)

Dans cette partie, N est un entier naturel supérieur ou égal à 2. On dira qu'une solution de (E_N) est de taille n si cette solution est un n-uplet d'éléments de $\mathbb{Z}/N\mathbb{Z}$ solution de (E_N).

3.1. **Solutions de** (E_N) **pour les petites valeurs de** n

On va essayer dans cette sous-partie de rechercher les solutions de $M_n(\overline{a_1}, \dots, \overline{a_n}) = \pm \mathrm{Id}$ pour les petites valeurs de n. On voit facilement que (E_N) n'a pas de solution pour $n = 1$. On va maintenant résoudre (E_N) pour $n = 2$ et $n = 3$.

Proposition 3.1. $(\overline{0}, \overline{0})$ *est la seule solution de* (E_N) *de taille 2.*

Démonstration.

$$\begin{pmatrix} \overline{a_2} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{a_2 a_1 - 1} & \overline{-a_2} \\ \overline{a_1} & \overline{-1} \end{pmatrix}.$$

Si $(\overline{a_1}, \overline{a_2})$ est solution de (E_N) alors $\overline{a_1} = \overline{a_2} = \overline{0}$ et $(\overline{0}, \overline{0})$ est solution de (E_N). □

Proposition 3.2. $(\overline{1}, \overline{1}, \overline{1})$ *et* $(\overline{-1}, \overline{-1}, \overline{-1})$ *sont les seules solutions de* (E_N) *de taille 3.*

Démonstration.

$$\begin{aligned} \begin{pmatrix} \overline{a_3} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \begin{pmatrix} \overline{a_2} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} &= \begin{pmatrix} \overline{a_3 a_2 - 1} & \overline{-a_3} \\ \overline{a_2} & \overline{-1} \end{pmatrix} \begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \\ &= \begin{pmatrix} \overline{a_3 a_2 a_1 - a_3 - a_1} & \overline{-a_3 a_2 + 1} \\ \overline{a_2 a_1 - 1} & \overline{-a_2} \end{pmatrix}. \end{aligned}$$

Si $(\overline{a_1}, \overline{a_2}, \overline{a_3})$ est solution de (E_N) alors soit $\overline{a_2} = \overline{1}$ et dans ce cas $\overline{a_1} = \overline{1}$ et $\overline{a_3} = \overline{1}$, soit $\overline{a_2} = \overline{-1}$ et dans ce cas $\overline{a_1} = \overline{-1}$ et $\overline{a_3} = \overline{-1}$. On vérifie que $(\overline{1}, \overline{1}, \overline{1})$ et $(\overline{-1}, \overline{-1}, \overline{-1})$ sont solutions de (E_N). □

Pour $n = 4$, on dispose du résultat suivant :

Proposition 3.3. *Les solutions de* (E_N) *pour* $n = 4$ *sont les 4-uplets suivants* $(\overline{-a}, \overline{b}, \overline{a}, \overline{-b})$ *avec* $\overline{a}\overline{b} = \overline{0}$ *et* $(\overline{a}, \overline{b}, \overline{a}, \overline{b})$ *avec* $\overline{a}\overline{b} = \overline{2}$.

Démonstration.

$$\begin{aligned} M_4(\overline{a_1},\overline{a_2},\overline{a_3},\overline{a_4}) &= \begin{pmatrix} \overline{a_4a_3-1} & \overline{-a_4} \\ \overline{a_3} & \overline{-1} \end{pmatrix}\begin{pmatrix} \overline{a_2} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix}\begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \\ &= \begin{pmatrix} \overline{a_4a_3a_2-a_4-a_2} & \overline{-a_4a_3+1} \\ \overline{a_3a_2-1} & \overline{-a_3} \end{pmatrix}\begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \\ &= \begin{pmatrix} \overline{a_4a_3a_2a_1-a_4a_1-a_2a_1-a_4a_3+1} & \overline{-a_4a_3a_2+a_4+a_2} \\ \overline{a_3a_2a_1-a_1-a_3} & \overline{1-a_3a_2} \end{pmatrix}. \end{aligned}$$

Si $(\overline{a_1},\overline{a_2},\overline{a_3},\overline{a_4})$ est solution de (E_N) alors on a deux possibilités :

- $\overline{a_3}\overline{a_2}=\overline{0}$ et dans ce cas on a $\overline{-a_4a_3a_2}+\overline{a_4}+\overline{a_2}=\overline{a_4}+\overline{a_2}=\overline{0}$ et donc $\overline{a_4}=\overline{-a_2}$ et on a également $\overline{a_3}\overline{a_2}\overline{a_1}-\overline{a_1}-\overline{a_3}=-\overline{a_1}-\overline{a_3}=\overline{0}$ et donc $\overline{a_1}=-\overline{a_3}$.
- $\overline{a_3}\overline{a_2}=\overline{2}$ et dans ce cas on a $\overline{-a_4a_3a_2}+\overline{a_4}+\overline{a_2}=-\overline{a_4}+\overline{a_2}=\overline{0}$ et donc $\overline{a_4}=\overline{a_2}$ et on a également $\overline{a_3}\overline{a_2}\overline{a_1}-\overline{a_1}-\overline{a_3}=\overline{a_1}-\overline{a_3}=\overline{0}$ et donc $\overline{a_1}=\overline{a_3}$.

On vérifie en faisant le calcul que $(\overline{-a},\overline{b},\overline{a},\overline{-b})$ avec $\overline{a}\overline{b}=\overline{0}$ et $(\overline{a},\overline{b},\overline{a},\overline{b})$ avec $\overline{a}\overline{b}=\overline{2}$ sont solutions. □

Remarque 3.4. Pour $n=4$, les solutions dépendent de la structure de $\mathbb{Z}/N\mathbb{Z}$. Par exemple, si N est premier alors $\overline{a_3}\overline{a_2}=\overline{0}$ implique $\overline{a_2}=\overline{0}$ ou $\overline{a_3}=\overline{0}$ mais si $N=4$ alors on a par exemple $\overline{2}\times\overline{2}=\overline{0}$.

Proposition 3.5.

(i) *Les solutions de (E_N) de taille 3 sont irréductibles.*

(ii) *Une solutions de (E_N) de taille 4 réductible contient $\overline{1}$ ou $\overline{-1}$.*

Démonstration. (i). Si un 3-uplet est somme d'un m-uplet avec un l-uplet alors $3=m+l-2$ et donc $m+l=5$ ce qui implique $m\leq 2$ ou $l\leq 2$. Donc, les solutions de (E_N) de taille 3 sont irréductibles.

(ii). Soit $(\overline{a_1},\overline{a_2},\overline{a_3},\overline{a_4})$ une solution de (E_N).

Si $(\overline{a_1},\overline{a_2},\overline{a_3},\overline{a_4})$ est réductible alors $(\overline{a_1},\overline{a_2},\overline{a_3},\overline{a_4})$ est équivalent à la somme d'un m-uplet solution de (E_N) avec un l-uplet solution de (E_N) avec $m,l\geq 3$. On a $m+l-2=4$ donc $m+l=6$ et comme $m,l\geq 3$ on a nécessairement $m=l=3$. Comme un 3-uplet solution de (E_N) contient $\overline{1}$ ou $\overline{-1}$, une solution réductible de (E_N) de taille 4 contient $\overline{1}$ ou $\overline{-1}$. □

Remarque 3.6. On démontre dans la proposition 3.10 la réciproque de (ii).

3.2. **Opérations sur les solutions**

L'objectif de cette partie est de justifier un certain nombre d'assertions présentes dans la section précédente et de donner des façons de construire des solutions à partir de solutions connues. La plupart de ces résultats ont déjà été démontrés dans [5] et [14] mais on les redémontre ici afin d'avoir une présentation complète.

Proposition 3.7. *Si* $(\overline{a_1}, \dots, \overline{a_n})$ *et* $(\overline{b_1}, \dots, \overline{b_m})$ *sont solutions de* (E_N) *alors le* $(m+n)$*-uplet* $(\overline{a_1}, \dots, \overline{a_n}, \overline{b_1}, \dots, \overline{b_m})$ *est solution de* (E_N)*. En particulier, le* $2n$*-uplet* $(\overline{a_1}, \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_n})$ *est solution de* (E_N)*.*

Démonstration. $\exists\ (\epsilon, \mu) \in \{\pm 1\}$ tels que $M_n(\overline{a_1}, \dots, \overline{a_n}) = \overline{\epsilon}\,\mathrm{Id}$ et $M_m(\overline{b_1}, \dots, \overline{b_m}) = \overline{\mu}\,\mathrm{Id}$ (car $(\overline{a_1}, \dots, \overline{a_n})$ et $(\overline{b_1}, \dots, \overline{b_m})$ sont solutions de (E_N)). Donc, on a

$$M_{n+m}(\overline{a_1}, \dots, \overline{a_n}, \overline{b_1}, \dots, \overline{b_m}) = M_m(\overline{b_1}, \dots, \overline{b_m}) M_n(\overline{a_1}, \dots, \overline{a_n}) = \overline{\epsilon\mu}\,\mathrm{Id}\,.$$

Donc, comme $\epsilon\mu \in \{\pm 1\}$, $(\overline{a_1}, \dots, \overline{a_n}, \overline{b_1}, \dots, \overline{b_m})$ est solution de (E_N). □

Proposition 3.8.

(i) $(\overline{a_1}, \dots, \overline{a_n})$ *est solution de* (E_N) *si et seulement si* $(\overline{a_n}, \dots, \overline{a_1})$ *est solution de* (E_N)*.*

(ii) $(\overline{a_1}, \dots, \overline{a_n})$ *est solution de* (E_N) *si et seulement si* $(\overline{-a_1}, \dots, \overline{-a_n})$ *est solution de* (E_N)*.*

(iii) *Si* $(\overline{a_1}, \dots, \overline{a_n}) \sim (\overline{b_1}, \dots, \overline{b_n})$ *alors* $(\overline{a_1}, \dots, \overline{a_n})$ *est solution de* (E_N) *si et seulement si* $(\overline{b_1}, \dots, \overline{b_n})$ *est solution de* (E_N)*.*

Démonstration. La preuve suivante est une adaptation de la remarque 2.6 de [5].

(i). On pose $K = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Supposons $(\overline{a_1}, \dots, \overline{a_n})$ solution de (E_N). On a $\begin{pmatrix} \overline{a} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix}^{-1} = \overline{K} \begin{pmatrix} \overline{a} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \overline{K}$ et $\overline{K}^2 = \mathrm{Id}$. Donc,

$$\begin{aligned} M_n(\overline{a_n}, \dots, \overline{a_1}) &= \left(\overline{K}\begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix}^{-1} \overline{K}\right) \dots \left(\overline{K}\begin{pmatrix} \overline{a_n} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix}^{-1} \overline{K}\right) \\ &= \overline{K}\left(\begin{pmatrix} \overline{a_n} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix} \dots \begin{pmatrix} \overline{a_1} & \overline{-1} \\ \overline{1} & \overline{0} \end{pmatrix}\right)^{-1} \overline{K} \\ &= \overline{K} M_n(\overline{a_1}, \dots, \overline{a_n})^{-1} \overline{K} \\ &= \pm\,\mathrm{Id} \ \text{ car } (\overline{a_1}, \dots, \overline{a_n}) \text{ solution de } (E_N). \end{aligned}$$

Donc, $(\overline{a_n}, \dots, \overline{a_1})$ est solution de (E_N).

Si $(\overline{a_n}, \dots, \overline{a_1})$ est solution de (E_N) alors par ce qui précède $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_N).

(ii). Si $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on note A^T la transposée de A. On a,

$$\begin{aligned}
M_n(\overline{-a_1}, \dots, \overline{-a_n}) &= \begin{pmatrix} \overline{-a_n} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \cdots \begin{pmatrix} \overline{-a_1} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \\
&= (\overline{-1})^n \begin{pmatrix} \overline{a_n} & \bar{1} \\ \overline{-1} & \bar{0} \end{pmatrix} \cdots \begin{pmatrix} \overline{a_1} & \bar{1} \\ \overline{-1} & \bar{0} \end{pmatrix} \\
&= (\overline{-1})^n \begin{pmatrix} \overline{a_n} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}^T \cdots \begin{pmatrix} \overline{a_1} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}^T \\
&= (\overline{-1})^n \left(\begin{pmatrix} \overline{a_1} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \cdots \begin{pmatrix} \overline{a_n} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \right)^T \\
&= (\overline{-1})^n M_n(\overline{a_n}, \dots, \overline{a_1})^T .
\end{aligned}$$

Donc, $(\overline{-a_1}, \dots, \overline{-a_n})$ est solution de (E_N) si et seulement si $(\overline{a_n}, \dots, \overline{a_1})$ est solution de (E_N). Par (i), $(\overline{-a_1}, \dots, \overline{-a_n})$ est solution de (E_N) si et seulement si $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_N).

(iii). C'est une conséquence de (i) et de l'invariance par permutations circulaires des solutions. □

Proposition 3.9. *Soit $(\overline{b_1}, \dots, \overline{b_m})$ une solution de (E_N). Soit $(\overline{a_1}, \dots, \overline{a_n}) \in (\mathbb{Z}/N\mathbb{Z})^n$ alors la somme $(\overline{a_1}, \dots, \overline{a_n}) \oplus (\overline{b_1}, \dots, \overline{b_m})$ est solution de (E_N) si et seulement si $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_N).*

Démonstration. La preuve suivante est adaptée de la preuve du lemme 2.7 de [4] et de la preuve du lemme 1.9 de [14].

$(\overline{b_1}, \dots, \overline{b_m})$ est une solution de (E_N) donc il existe μ appartenant à $\{\pm 1\}$ tel que $M_m(\overline{b_1}, \dots, \overline{b_m}) = \bar{\mu}\,\mathrm{Id}$.

Si $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_N). $\exists\, \epsilon \in \{\pm 1\}$ tel que $M_n(\overline{a_1}, \dots, \overline{a_n}) = \bar{\epsilon}\,\mathrm{Id}$. On vérifie que

$$\begin{aligned}
M_1(\overline{a_n + b_1}) &= \overline{-1} \times M_1(\overline{b_1}) M_1(\bar{0}) M_1(\overline{a_n}) = \overline{-1} \times M_1(\overline{a_n}) M_1(\bar{0}) M_1(\overline{b_1}), \\
M_1(\overline{a_1 + b_m}) &= \overline{-1} \times M_1(\overline{a_1}) M_1(\bar{0}) M_1(\overline{b_m}) = \overline{-1} \times M_1(\overline{b_m}) M_1(\bar{0}) M_1(\overline{a_1}).
\end{aligned}$$

Notons $M = M_{n+m-2}(\overline{a_1+b_m}, \overline{a_2}, \ldots, \overline{a_{n-1}}, \overline{a_n+b_1}, \overline{b_2}, \ldots, \overline{b_{m-1}})$. On a

$$\begin{aligned}
M &= M_{m-2}(\overline{b_2}, \ldots, \overline{b_{m-1}})M_1(\overline{a_n+b_1})M_{n-2}(\overline{a_2}, \ldots, \overline{a_{n-1}})M_1(\overline{a_1+b_m}) \\
&= M_{m-2}(\overline{b_2}, \ldots, \overline{b_{m-1}})M_1(\overline{b_1})M_1(\bar{0})M_1(\overline{a_n})M_{n-2}(\overline{a_2}, \ldots, \overline{a_{n-1}}) \\
&\quad M_1(\overline{a_1})M_1(\bar{0})M_1(\overline{b_m}) \\
&= M_{m-1}(\overline{b_1}, \ldots, \overline{b_{m-1}})M_1(\bar{0})M_n(\overline{a_1}, \ldots, \overline{a_n})M_1(\bar{0})M_1(\overline{b_m}) \\
&= M_{m-1}(\overline{b_1}, \ldots, \overline{b_{m-1}})M_1(\bar{0})(\bar{\epsilon}\,\mathrm{Id})M_1(\bar{0})M_1(\overline{b_m}) \\
&= \bar{\epsilon}M_{m-1}(\overline{b_1}, \ldots, \overline{b_{m-1}})M_2(\bar{0}, \bar{0})M_1(\overline{b_m}) \\
&= \bar{\epsilon}M_{m-1}(\overline{b_1}, \ldots, \overline{b_{m-1}})(\overline{-1}\,\mathrm{Id})M_1(\overline{b_m}) \\
&= \overline{-\epsilon}M_m(\overline{b_m}, \overline{b_1}, \ldots, \overline{b_{m-1}}) \\
&= \overline{-\mu\epsilon}\,\mathrm{Id}\,.
\end{aligned}$$

Donc, $(\overline{a_1}, \ldots, \overline{a_n}) \oplus (\overline{b_1}, \ldots, \overline{b_m})$ est solution de (E_N).

Si $(\overline{a_1}, \ldots, \overline{a_n}) \oplus (\overline{b_1}, \ldots, \overline{b_m})$ est solution. $(\overline{a_1+b_m}, \overline{a_2}, \ldots, \overline{a_{n-1}}, \overline{a_n+b_1}, \overline{b_2}, \ldots, \overline{b_{m-1}})$ est solution de (E_N) donc $(\overline{a_2}, \ldots, \overline{a_{n-1}}, \overline{a_n+b_1}, \overline{b_2}, \ldots, \overline{b_{m-1}}, \overline{a_1+b_m})$ est solution de (E_N). $\exists\ \alpha \in \{\pm 1\}$ tel que $M_{n+m-2}(\overline{a_2}, \ldots, \overline{a_{n-1}}, \overline{a_n+b_1}, \overline{b_2}, \ldots, \overline{b_{m-1}}, \overline{a_1+b_m}) = \bar{\alpha}\,\mathrm{Id}$. On a

$$\begin{aligned}
\bar{\alpha}\,\mathrm{Id} &= M_1(\overline{a_1+b_m})M_{m-2}(\overline{b_2}, \ldots, \overline{b_{m-1}})M_1(\overline{a_n+b_1})M_{n-2}(\overline{a_2}, \ldots, \overline{a_{n-1}}) \\
&= M_1(\overline{a_1})M_1(\bar{0})M_1(\overline{b_m})M_{m-2}(\overline{b_2}, \ldots, \overline{b_{m-1}})M_1(\overline{b_1})M_1(\bar{0})M_1(\overline{a_n}) \\
&\quad M_{n-2}(\overline{a_2}, \ldots, \overline{a_{n-1}}) \\
&= M_1(\overline{a_1})M_1(\bar{0})M_m(\overline{b_1}, \ldots, \overline{b_m})M_1(\bar{0})M_{n-1}(\overline{a_2}, \ldots, \overline{a_n}) \\
&= \bar{\mu}M_1(\overline{a_1})M_2(\bar{0}, \bar{0})M_{n-1}(\overline{a_2}, \ldots, \overline{a_n}) \\
&= \overline{-\mu}M_n(\overline{a_2}, \ldots, \overline{a_n}, \overline{a_1}).
\end{aligned}$$

Ainsi, $M_n(\overline{a_2}, \ldots, \overline{a_n}, \overline{a_1}) = \overline{-\alpha\mu}\,\mathrm{Id}$. Donc, $(\overline{a_2}, \ldots, \overline{a_n}, \overline{a_1})$ est solution de (E_N) et donc $(\overline{a_1}, \ldots, \overline{a_n})$ est solution de (E_N). □

On déduit de ce résultat qu'une solution $(\overline{c_1}, \ldots, \overline{c_n})$ avec $n \geq 3$ de (E_N) est réductible s'il existe une solution de (E_N) $(\overline{b_1}, \ldots, \overline{b_l})$ et un m-uplet $(\overline{a_1}, \ldots, \overline{a_m})$ tels que $m \geq 3$ et $l \geq 3$ et

$$(\overline{c_1}, \ldots, \overline{c_n}) \sim (\overline{a_1}, \ldots, \overline{a_m}) \oplus (\overline{b_1}, \ldots, \overline{b_l}).$$

On en déduit le résultat suivant

Proposition 3.10.

(i) *Si $n \geq 4$ alors une solution de (E_N) contenant $\overline{1}$ ou $\overline{-1}$ est réductible.*

(ii) *Si $n \geq 5$ alors une solution de (E_N) contenant $\overline{0}$ est réductible.*

Démonstration. (i). Soit $(\overline{a_1}, \dots, \overline{a_n})$ (avec $n \geq 4$) une solution de (E_N). Si $\exists\, \epsilon \in \{\pm\overline{1}\}$ et si $\exists\, i \in [\![1; n]\!]$ tels que $\overline{a_i} = \overline{\epsilon}$ alors on a

$$(\overline{a_{i+1}} \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_i}) = (\overline{a_{i+1} - \epsilon} \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_{i-1} - \epsilon}) \oplus (\overline{\epsilon}, \overline{\epsilon}, \overline{\epsilon}).$$

Donc, $(\overline{a_1}, \dots, \overline{a_n})$ est réductible.

(ii). Soit $(\overline{a_1}, \dots, \overline{a_n})$ (avec $n \geq 5$) une solution de (E_N). Si $\exists\, i \in [\![1; n]\!]$ tel que $\overline{a_i} = \overline{0}$ alors on a

$$(\overline{a_{i+2}} \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_i}, \overline{a_{i+1}}) = (\overline{a_{i+2}} \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_{i-1} + a_{i+1}}) \oplus (\overline{-a_{i+1}}, \overline{0}, \overline{a_{i+1}}, \overline{0}).$$

Donc, $(\overline{a_1}, \dots, \overline{a_n})$ est réductible. □

Remarque 3.11. La réciproque est fausse. Par exemple, si $N = 4$, $(\overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2})$ ne contient pas $\overline{1}$, $\overline{-1}$ ou $\overline{0}$ mais est une solution de (E_4) réductible puisqu'on a

$$(\overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2}) = (\overline{0}, \overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{0}) \oplus (\overline{2}, \overline{2}, \overline{2}, \overline{2}).$$

3.3. **Solutions monomiales minimales**

Dans cette sous-partie, on s'intéresse aux solutions dont toutes les composantes sont identiques. En particulier, on cherche à connaître des solutions valables pour tout N (ou au moins pour des valeurs de N vérifiant certaines propriétés) et à savoir si elles sont ou non irréductibles.

3.3.1. **Définitions et premiers résultats**

On commence par la définition suivante :

Définition 3.12. Soient $n \in \mathbb{N}^*$ et $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$. On appelle solution $(n, \overline{k})$-monomiale un n-uplet d'éléments de $\mathbb{Z}/N\mathbb{Z}$ constitué uniquement de $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$ et solution de (E_N).

On appelle solution monomiale une solution pour laquelle il existe $m \in \mathbb{N}^*$ et $\overline{l} \in \mathbb{Z}/N\mathbb{Z}$ tels qu'elle est $(m, \overline{l})$-monomiale.

On appelle solution $\overline{k}$-monomiale minimale une solution $(n, \overline{k})$-monomiale avec n le plus petit entier pour lequel il existe une solution $(n, \overline{k})$-monomiale.

On appelle solution monomiale minimale une solution $\overline{k}$-monomiale minimale pour un $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$.

Exemple 3.13. $(\bar{1},\bar{1},\bar{1},\bar{1},\bar{1},\bar{1})$ est une solution $(6,\bar{1})$-monomiale de (E_N) et $(\bar{1},\bar{1},\bar{1})$ est une solution $\bar{1}$-monomiale minimale de (E_N).

Remarques 3.14.

(i) Si $(\bar{k},\dots,\bar{k}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est une solution $\bar{k}$-monomiale minimale de (E_N) alors, par la proposition 3.8(ii), $(\overline{-k},\dots,\overline{-k}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est une solution $\overline{-k}$-monomiale minimale de (E_N).

(ii) La taille d'une solution $\bar{k}$-monomiale minimale de (E_N) est l'ordre de $\begin{pmatrix} \bar{k} & \bar{-1} \\ \bar{1} & \bar{0} \end{pmatrix}$ dans le groupe $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. En particulier, si N est premier alors la taille d'une solution $\bar{k}$-monomiale minimale de (E_N) est inférieure à N car N est l'ordre maximal des éléments de $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ (voir [7]). Cela n'est plus vrai si N n'est pas premier. Par exemple, si $N = 10$, une solution $\bar{3}$-monomiale minimale de (E_{10}) est de taille 15.

On commence par le résultat suivant donnant une solution valable dans le cas où N est un carré.

Proposition 3.15. *Si $N = l^2$ avec $l \geq 2$ alors $(\bar{l},\dots,\bar{l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l}$ est solution de (E_N).*

Démonstration. On a

$$\begin{aligned}
M_{2l}(\bar{l},\dots,\bar{l}) &= \left(\begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}\begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}\right)^l \\
&= \begin{pmatrix} \overline{l^2-1} & \overline{-l} \\ \bar{l} & \overline{-1} \end{pmatrix}^l \\
&= \begin{pmatrix} \overline{-1} & \overline{-l} \\ \bar{l} & \overline{-1} \end{pmatrix}^l \\
&= \overline{(-\mathrm{Id}+lS)^l} \\
&= \overline{\sum_{k=0}^{l}\binom{l}{k}(-1)^{l-k}(lS)^k} \text{ (binôme de Newton)} \\
&= \overline{(-1)^l\binom{l}{0}\mathrm{Id}+(-1)^{l-1}\binom{l}{1}lS + l^2\sum_{k=2}^{l}\binom{l}{k}(-1)^{l-k}l^{k-2}S^k} \\
&= \overline{(-1)^l\,\mathrm{Id}+(-1)^{l-1}l^2S} \\
&= \overline{(-1)^l\,\mathrm{Id}}.
\end{aligned}$$

□

La question de l'irréductibilité de ces solutions est résolue dans la proposition suivante.

Proposition 3.16. *Soit $N = l^2$ avec $l \geq 2$. $(\bar{l}, \dots, \bar{l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l}$ est irréductible si et seulement si $l = 2$.*

Démonstration. Si $l = 2$, alors la solution est $(\overline{2}, \overline{2}, \overline{2}, \overline{2})$ et elle est irréductible puisqu'elle ne contient pas $\pm\overline{1}$. Si $l \geq 3$ alors la solution n'est pas irréductible car

$$(\bar{l}, \dots, \bar{l}) = (\overline{2l}, \bar{l}, \dots, \bar{l}, \overline{2l}) \oplus (\overline{-l}, \bar{l}, \bar{l}, \overline{-l})$$

et $(\overline{-l}, \bar{l}, \bar{l}, \overline{-l})$ est solution (par la proposition 3.3) et $(\overline{2l}, \bar{l}, \dots, \bar{l}, \overline{2l})$ est de taille $2l - 2 \geq 4$. □

Remarque 3.17. La démonstration précédente montre également que si $N = l^2$ avec $l \geq 3$ alors le $(2l-2)$-uplet $(\overline{2l}, \bar{l}, \dots, \bar{l}, \overline{2l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l-2}$ est solution de (E_N).

On va maintenant donner une généralisation de la proposition 3.15. Avant cela on a besoin du résultat classique suivant :

Lemme 3.18. *Soient $n \in \mathbb{N}^*$ et $k \in [\![1; n]\!]$, $\frac{n}{\operatorname{pgcd}(n,k)}$ divise $\binom{n}{k}$.*

Démonstration.

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{\frac{n}{\operatorname{pgcd}(n,k)}}{\frac{k}{\operatorname{pgcd}(n,k)}}\binom{n-1}{k-1}.$$

Donc, comme $\binom{n}{k} \in \mathbb{N}^*$, on a $\frac{k}{\operatorname{pgcd}(n,k)}$ divise $\frac{n}{\operatorname{pgcd}(n,k)}\binom{n-1}{k-1}$. Comme $\frac{k}{\operatorname{pgcd}(n,k)}$ et $\frac{n}{\operatorname{pgcd}(n,k)}$ sont premiers entre eux, on a, par le lemme de Gauss, $\frac{k}{\operatorname{pgcd}(n,k)}$ divise $\binom{n-1}{k-1}$. Donc, $\frac{n}{\operatorname{pgcd}(n,k)}$ divise $\binom{n}{k}$. □

Avec ce lemme on peut démontrer le lemme suivant :

Lemme 3.19. *Soient $n \in \mathbb{N}^*$, $n \geq 2$, $l \in \mathbb{N}^*$, $l \geq 2$ et $j \in [\![1; n-1]\!]$, on a l^{n-j} divise $\binom{l^{n-1}}{j}$.*

Démonstration. Si $j = 1$ alors $\binom{l^{n-1}}{j} = l^{n-1}$ et donc le résultat est vrai. Si $j = 2$ alors

$$\binom{l^{n-1}}{j} = \frac{l^{n-1}(l^{n-1}-1)}{2}.$$

Si l est pair on a $\frac{l^{n-1}(l^{n-1}-1)}{2} = l^{n-2}\frac{l}{2}(l^{n-1}-1)$ et si l est impair alors $(l^{n-1}-1)$ est pair et on a $\frac{l^{n-1}(l^{n-1}-1)}{2} = l^{n-1}\frac{l^{n-1}-1}{2}$. Dans tous les cas, l^{n-2} divise $\binom{l^{n-1}}{j}$. On peut donc supposer $n \geq 4$ et $j \geq 3$.

Par le lemme précédent, $\frac{l^{n-1}}{\operatorname{pgcd}(l^{n-1}, j)}$ divise $\binom{l^{n-1}}{j}$. Notons $l = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de l en facteurs premiers. $\exists\, (\beta_1, \dots, \beta_r) \in \mathbb{N}^r$ tel que $\operatorname{pgcd}(l^{n-1}, j) = p_1^{\beta_1} \dots p_r^{\beta_r}$.

Montrons que $\forall\, i \in [\![1;r]\!]$, $\beta_i \leq \alpha_i(j-1)$. Supposons par l'absurde qu'il existe un entier i dans $[\![1;r]\!]$ tel que $\beta_i > \alpha_i(j-1)$. Par récurrence, on montre que si $j \geq 3$ on a $p_i^{j-1} > j$. On a $p_i^{\alpha_i(j-1)} \geq p_i^{j-1} > j$ et donc $\operatorname{pgcd}(l^{n-1}, j) > j$ ce qui est absurde.

Ainsi, $\forall\, i \in [\![1;r]\!]$, $\beta_i \leq \alpha_i(j-1)$ et donc l^{n-j} divise $\frac{l^{n-1}}{\operatorname{pgcd}(l^{n-1},j)}$. On en déduit que l^{n-j} divise $\binom{l^{n-1}}{j}$. □

Proposition 3.20. *Si $N = l^n$ avec $l \geq 2$ et $n \geq 2$ alors $(\bar{l}, \ldots, \bar{l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}}$ est solution de (E_N).*

Démonstration. On a

$$
\begin{aligned}
M_{2l^{n-1}}(\bar{l}, \ldots, \bar{l}) &= \left(\begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}\begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}\right)^{l^{n-1}} \\
&= \begin{pmatrix} \overline{l^2-1} & \overline{-l} \\ \bar{l} & \overline{-1} \end{pmatrix}^{l^{n-1}} \\
&= \overline{\left(-\operatorname{Id} + l\begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}\right)^{l^{n-1}}} \\
&= \overline{\sum_{k=0}^{l^{n-1}} \binom{l^{n-1}}{k} l^k (-1)^{l^{n-1}-k} \begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}^k} \text{ (binôme de Newton)} \\
&= \overline{\sum_{k=0}^{n-1} \binom{l^{n-1}}{k} l^k (-1)^{l^{n-1}-k} \begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}^k} \\
&= \overline{(-1)^{l^{n-1}} \operatorname{Id} + \sum_{k=1}^{n-1} \binom{l^{n-1}}{k} l^k (-1)^{l^{n-1}-k} \begin{pmatrix} \bar{l} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}^k} \\
&= \overline{(-1)^{l^{n-1}} \operatorname{Id}} \text{ car } l^{n-k} \text{ divise } \binom{l^{n-1}}{k} \text{ par le lemme 3.19.}
\end{aligned}
$$
□

Notons que d'après le théorème 2.9 (démontré dans la sous-section suivante), la solution ci-dessus est irréductible si $l = 2$.

On cherche maintenant à étudier l'irréductibilité des solutions monomiales minimales. On a besoin pour cela du résultat suivant sur l'expression de la matrice $M_n(a_1, \ldots, a_n)$

en terme de déterminant. On pose $K_{-1} = 0$, $K_0 = 1$ et on note pour $i \geq 1$

$$K_i(a_1, \ldots, a_i) = \begin{vmatrix} a_1 & 1 & & & \\ 1 & a_2 & 1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{i-1} & 1 \\ & & & 1 & a_i \end{vmatrix}.$$

$K_i(a_1, \ldots, a_i)$ est le continuant de $a_1, \ldots, a_i$. On dispose de l'égalité suivante (voir [12, 13])

$$M_n(a_1, \ldots, a_n) = \begin{pmatrix} K_n(a_1, \ldots, a_n) & -K_{n-1}(a_2, \ldots, a_n) \\ K_{n-1}(a_1, \ldots, a_{n-1}) & -K_{n-2}(a_2, \ldots, a_{n-1}) \end{pmatrix}.$$

Ceci nous permet d'avoir le résultat préliminaire suivant :

Proposition 3.21. *Soient $n \in \mathbb{N}^*$, $n \geq 3$ et $(\bar{a}, \bar{b}, \bar{k}) \in (\mathbb{Z}/N\mathbb{Z})^3$.*
Si $(\bar{a}, \bar{k}, \bar{k}, \ldots, \bar{k}, \bar{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N) alors $\bar{a} = \bar{b}$ et on a

$$\bar{a}(\bar{a} - \bar{k}) = \bar{0}.$$

Démonstration. Comme $(\bar{a}, \bar{k}, \bar{k}, \ldots, \bar{k}, \bar{b})$ est solution de (E_N), $\exists\, \epsilon \in \{-1, 1\}$ tel que

$$\bar{\epsilon}\,\mathrm{Id} = M_n(\bar{a}, \bar{k}, \bar{k}, \ldots, \bar{k}, \bar{b}) = \begin{pmatrix} K_n(\bar{a}, \bar{k}, \ldots, \bar{k}, \bar{b}) & -K_{n-1}(\bar{k}, \ldots, \bar{k}, \bar{b}) \\ K_{n-1}(\bar{a}, \bar{k}, \ldots, \bar{k}) & -K_{n-2}(\bar{k}, \ldots, \bar{k}) \end{pmatrix}.$$

Donc,

$$K_{n-1}(\bar{a}, \bar{k}, \ldots, \bar{k}) = -K_{n-1}(\bar{k}, \ldots, \bar{k}, \bar{b}) = \bar{0} \quad \text{et} \quad K_{n-2}(\bar{k}, \ldots, \bar{k}) = -\bar{\epsilon}.$$

Or,

$$K_{n-1}(\bar{a}, \bar{k}, \ldots, \bar{k}) = \bar{a}K_{n-2}(\bar{k}, \ldots, \bar{k}) - K_{n-3}(\bar{k}, \ldots, \bar{k}) = \overline{-\epsilon a} - K_{n-3}(\bar{k}, \ldots, \bar{k}).$$

Ainsi, comme $\bar{\epsilon}^2 = \bar{1}$, on a

$$\bar{a} = \overline{-\epsilon} K_{n-3}(\bar{k}, \ldots, \bar{k}).$$

De même,

$$K_{n-1}(\bar{k}, \ldots, \bar{k}, \bar{b}) = \bar{b}K_{n-2}(\bar{k}, \ldots, \bar{k}) - K_{n-3}(\bar{k}, \ldots, \bar{k}) = \overline{-\epsilon b} - K_{n-3}(\bar{k}, \ldots, \bar{k}).$$

Il en découle que,

$$\bar{b} = \overline{-\epsilon} K_{n-3}(\bar{k}, \ldots, \bar{k}).$$

Donc,

$$\bar{a} = \bar{b}.$$

De plus, on a $\overline{-\epsilon} = K_{n-2}(\bar{k},\dots,\bar{k}) = \bar{k}K_{n-3}(\bar{k},\dots,\bar{k}) - K_{n-4}(\bar{k},\dots,\bar{k})$ et

$$M_{n-2}(\bar{k},\bar{k},\dots,\bar{k}) = \begin{pmatrix} K_{n-2}(\bar{k},\dots,\bar{k}) & -K_{n-3}(\bar{k},\dots,\bar{k}) \\ K_{n-3}(\bar{k},\dots,\bar{k}) & -K_{n-4}(\bar{k},\dots,\bar{k}) \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Ainsi, $-K_{n-2}(\bar{k},\dots,\bar{k})K_{n-4}(\bar{k},\dots,\bar{k}) + K_{n-3}(\bar{k},\dots,\bar{k})^2 = \bar{1}$.
Or, comme $K_{n-2}(\bar{k},\dots,\bar{k}) = \overline{-\epsilon}$, on a

$$\bar{\epsilon}K_{n-4}(\bar{k},\dots,\bar{k}) + K_{n-3}(\bar{k},\dots,\bar{k})^2 = \bar{1}$$

c'est-à-dire

$$K_{n-4}(\bar{k},\dots,\bar{k}) = \bar{\epsilon}(\bar{1} - K_{n-3}(\bar{k},\dots,\bar{k})^2).$$

Donc, on a

$$\begin{aligned} \overline{-\epsilon} &= \bar{k}K_{n-3}(\bar{k},\dots,\bar{k}) - K_{n-4}(\bar{k},\dots,\bar{k}) \\ &= \bar{k}K_{n-3}(\bar{k},\dots,\bar{k}) - \bar{\epsilon}(\bar{1} - K_{n-3}(\bar{k},\dots,\bar{k})^2) \\ &= \bar{k}K_{n-3}(\bar{k},\dots,\bar{k}) - \bar{\epsilon} + \bar{\epsilon}K_{n-3}(\bar{k},\dots,\bar{k})^2 \\ &= -\overline{\epsilon k a} - \bar{\epsilon} + \overline{\epsilon a^2}. \end{aligned}$$

On en déduit, $\bar{0} = -\overline{\epsilon k a} + \overline{\epsilon a^2} = \bar{\epsilon}\bar{a}(\bar{a} - \bar{k})$ et donc $\bar{0} = \bar{a}(\bar{a} - \bar{k})$. □

Remarque 3.22. Il est possible que $\bar{a} \neq \bar{0}$ et $\bar{a} \neq \bar{k}$. Par exemple, si $N = 9$, $(\bar{6},\bar{3},\bar{3},\bar{6})$ est solution de (E_9).

Théorème 3.23. *Si N est premier alors toute solution monomiale minimale de (E_N) différente de $(\bar{0},\bar{0})$ est irréductible.*

Démonstration. Soient $\bar{k} \in \mathbb{Z}/N\mathbb{Z}$, $\bar{k} \neq \bar{0}$ et $n \in \mathbb{N}^*$ tels que $(\bar{k},\dots,\bar{k}) \in (\mathbb{Z}/N\mathbb{Z})^n$ soit monomiale minimale. On suppose par l'absurde que cette solution peut s'écrire comme une somme de deux solutions non triviales.

Il existe $(\overline{a_1},\dots,\overline{a_l})$ et $(\overline{b_1},\dots,\overline{b_{l'}})$ solutions de (E_N) différentes de $(\bar{0},\bar{0})$ avec $l + l' = n + 2$ et $l, l' \geq 3$ telles que

$$(\bar{k},\dots,\bar{k}) = (\overline{b_1 + a_l}, \overline{b_2},\dots,\overline{b_{l'-1}}, \overline{b_{l'} + a_1}, \overline{a_2},\dots,\overline{a_{l-1}}).$$

On a donc $\overline{a_2} = \dots = \overline{a_{l-1}} = \bar{k}$. Comme $(\overline{a_1},\dots,\overline{a_l})$ est solution de (E_N), on a par la proposition précédente $\overline{a_1} = \overline{a_l} = \bar{a}$ et $\bar{0} = \bar{a}(\bar{a} - \bar{k})$.

Puisque N est premier, $\mathbb{Z}/N\mathbb{Z}$ est intègre et donc l'équation $\bar{0} = \bar{a}(\bar{a} - \bar{k})$ a pour solutions $\bar{a} = \bar{0}$ et $\bar{a} = \bar{k}$. Si $\bar{a} = \bar{0}$ alors

$$(\bar{0}, \overline{a_2},\dots,\overline{a_{l-1}}, \bar{0}) \sim (\overline{a_2},\dots,\overline{a_{l-1}}) \oplus (\bar{0},\bar{0},\bar{0},\bar{0}).$$

Par la proposition 3.9, $(\overline{a_2},\dots,\overline{a_{l-1}}) = (\bar{k},\dots,\bar{k}) \in (\mathbb{Z}/N\mathbb{Z})^{l-2}$ est encore solution de (E_N) ce qui contredit la minimalité de la solution.

Ainsi, $\overline{a} = \overline{k}$ et par minimalité de la solution on a $l \geq n$ ce qui implique $l' \leq 2$. Donc, $l' = 2$ et $(\overline{b_1}, \ldots, \overline{b_{l'}}) = (\overline{0}, \overline{0})$ ce qui est absurde. □

Remarque 3.24. Si N n'est pas premier alors une solution monomiale minimale n'est pas forcément irréductible. Par exemple, si $N = 9$, $(\overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3})$ est monomiale minimale mais pas irréductible car $(\overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3}) = (\overline{6}, \overline{3}, \overline{3}, \overline{6}) \oplus (\overline{6}, \overline{3}, \overline{3}, \overline{6})$.

On peut améliorer la proposition 3.21 pour traiter le cas où $N = pq$ avec p et q deux nombres premiers distincts.

Lemme 3.25. *Soient p et q deux nombres premiers distincts et $N = pq$. Soient $n \in \mathbb{N}^*$, $n \geq 3$ et $(\overline{a}, \overline{b}) \in (\mathbb{Z}/N\mathbb{Z})^2$.*

(i) *Si $(\overline{a}, \overline{p}, \overline{p}, \ldots, \overline{p}, \overline{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N) alors $\overline{a} = \overline{b}$ et $\overline{a} \in \{\overline{0}, \overline{p}\}$.*

(ii) *Si $(\overline{a}, \overline{q}, \overline{q}, \ldots, \overline{q}, \overline{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N) alors $\overline{a} = \overline{b}$ et $\overline{a} \in \{\overline{0}, \overline{q}\}$.*

Démonstration. Si $(\overline{a}, \overline{p}, \overline{p}, \ldots, \overline{p}, \overline{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N). Par la proposition 3.21, $\overline{a} = \overline{b}$ et $\overline{a}(\overline{a} - \overline{p}) = \overline{0}$.

Supposons par l'absurde que $\overline{a}$ est un élément inversible de $\mathbb{Z}/N\mathbb{Z}$. Dans ce cas, on a

$$\overline{a}(\overline{a} - \overline{p}) = \overline{0} \iff (\overline{a} - \overline{p}) = \overline{0} \iff \overline{a} = \overline{p}.$$

Or, $\overline{p}$ n'est pas inversible dans $\mathbb{Z}/N\mathbb{Z}$ ce qui est absurde. Donc, $\overline{a}$ n'est pas un élément inversible de $\mathbb{Z}/N\mathbb{Z}$.

Donc, soit il existe un entier i dans $[\![0; q-1]\!]$ tel que $\overline{a} = \overline{ip}$ soit il existe un entier j dans $[\![1; p-1]\!]$ tel que $\overline{a} = \overline{jq}$.

Si $\exists\, i \in [\![0; q-1]\!]$ tel que $\overline{a} = \overline{ip}$. On a

$$\overline{a}(\overline{a} - \overline{p}) = \overline{ip}(\overline{ip} - \overline{p}) = \overline{ip^2}(\overline{i} - \overline{1}) = \overline{0}.$$

Donc, pq divise $ip^2(i-1)$ et, en particulier, q divise $ip^2(i-1)$. Comme q et p^2 sont premiers entre eux, on a, par le lemme de Gauss, q divise $i(i-1)$. Si $i \neq 0$ alors q et i sont premiers entre eux (puisque $i \in [\![0; q-1]\!]$), et donc, par le lemme de Gauss, q divise $(i-1)$ ce qui implique $i = 1$. Donc, $i = 0$ ou $i = 1$.

Si $\exists\, j \in [\![1; p-1]\!]$ tel que $\overline{a} = \overline{jq}$. On a

$$\overline{a}(\overline{a} - \overline{p}) = \overline{jq}(\overline{jq} - \overline{p}) = \overline{0}.$$

Donc, pq divise $jq(jq-p)$ et, en particulier, p divise $jq(jq-p)$. Comme p et q sont premiers entre eux, on a, par le lemme de Gauss, p divise $j(jq-p)$. Comme p et j sont premiers entre eux (puisque $j \in [\![1; p-1]\!]$), on a, par le lemme de Gauss, p divise $(jq-p)$ et donc p divise jq ce qui est absurde.

Donc, $\overline{a} \in \{\overline{0}, \overline{p}\}$. On procède de façon analogue pour (ii). □

Proposition 3.26. *Soient p et q deux nombres premiers distincts et $N = pq$. Toute solution $\overline{k}$-monomiale minimale de (E_N) avec $\overline{k} \in \{\overline{p}, \overline{q}\}$ est irréductible.*

Démonstration. Soit $n \in \mathbb{N}^*$ tels que $(\overline{p}, \dots, \overline{p}) \in (\mathbb{Z}/N\mathbb{Z})^n$ soit monomiale minimale. On suppose par l'absurde que cette solution peut s'écrire comme une somme de deux solutions non triviales.

Il existe $(\overline{a_1}, \dots, \overline{a_l})$ et $(\overline{b_1}, \dots, \overline{b_{l'}})$ solutions de (E_N) différentes de $(\overline{0}, \overline{0})$ avec $l + l' = n + 2$ et $l, l' \geq 3$ telles que

$$(\overline{p}, \dots, \overline{p}) = (\overline{b_1 + a_l}, \overline{b_2}, \dots, \overline{b_{l'-1}}, \overline{b_{l'} + a_1}, \overline{a_2}, \dots, \overline{a_{l-1}}).$$

On a donc $\overline{a_2} = \dots = \overline{a_{l-1}} = \overline{p}$. Comme $(\overline{a_1}, \dots, \overline{a_l})$ est solution de (E_N), on a par le lemme précédent $\overline{a_1} = \overline{a_l} = \overline{a}$ avec $\overline{a} = \overline{0}$ ou $\overline{a} = \overline{p}$.

Si $\overline{a} = \overline{0}$ alors

$$(\overline{0}, \overline{a_2}, \dots, \overline{a_{l-1}}, \overline{0}) \sim (\overline{a_2}, \dots, \overline{a_{l-1}}) \oplus (\overline{0}, \overline{0}, \overline{0}, \overline{0}).$$

Par la proposition 3.9, $(\overline{a_2}, \dots, \overline{a_{l-1}}) = (\overline{p}, \dots, \overline{p}) \in (\mathbb{Z}/N\mathbb{Z})^{l-2}$ est encore solution de (E_N) ce qui contredit la minimalité de la solution.

Donc, $\overline{a} = \overline{p}$ et par minimalité de la solution on a $l \geq n$ ce qui implique $l' \leq 2$. Donc, $l' = 2$ et $(\overline{b_1}, \dots, \overline{b_{l'}}) = (\overline{0}, \overline{0})$ ce qui est absurde.

On procède de la même façon dans le cas d'une solution $\overline{q}$-monomiale minimale. □

Remarque 3.27. Si $N = pq$ et $\overline{k} \notin \{\overline{p}, \overline{q}\}$ alors une solution $\overline{k}$-monomiale minimale de (E_N) n'est pas forcément irréductible. Par exemple, si $N = 10 = 2 \times 5$, une solution $\overline{3}$-monomiale minimale (qui est de taille 15) n'est pas irréductible car on peut l'écrire comme une somme à l'aide de la solution $(\overline{8}, \overline{3}, \overline{3}, \overline{3}, \overline{8})$.

3.3.2. **Démonstration du théorème 2.9**

Dans le cas des solutions $\overline{2}$-monomiales on peut améliorer les résultats précédents.

Lemme 3.28. *Soit $n \in \mathbb{N}^*$ alors $M_n(2, \dots, 2) = \begin{pmatrix} n+1 & -n \\ n & -n+1 \end{pmatrix}$.*

Démonstration. On raisonne par récurrence sur n.

Si $n = 1$ alors le résultat est vrai.

On suppose qu'il existe $n \in \mathbb{N}^*$ tel que $M_n(2,\dots,2) = \left(\begin{smallmatrix} n+1 & -n \\ n & -n+1 \end{smallmatrix}\right)$. On a

$$\begin{aligned} M_{n+1}(2,\dots,2) &= M_n(2,\dots,2)\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} n+1 & -n \\ n & -n+1 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 2n+2-n & -n-1 \\ 2n-n+1 & -n \end{pmatrix} \\ &= \begin{pmatrix} (n+1)+1 & -(n+1) \\ n+1 & -(n+1)+1 \end{pmatrix}. \end{aligned}$$

La formule est vraie pour $n+1$ et donc par récurrence elle est vraie pour tout n. □

De ce calcul, on déduit l'existence d'une solution particulière pour N quelconque.

Corollaire 3.29. *$(\bar{2},\dots,\bar{2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ est solution de (E_N).*

Démonstration.

$$M_N(\bar{2},\dots,\bar{2}) = \begin{pmatrix} \overline{N+1} & \overline{-N} \\ \overline{N} & \overline{-N+1} \end{pmatrix} = \mathrm{Id}\,. \qquad \square$$

Pour montrer l'irréductibilité de cette solution, on va utiliser une version améliorée de la proposition 3.21 utilisant l'hypothèse $\bar{k} = \bar{2}$.

Lemme 3.30. *Soient $n \in \mathbb{N}^*$, $n \geq 3$ et $(\bar{a},\bar{b}) \in (\mathbb{Z}/N\mathbb{Z})^2$.*

$(\bar{a},\bar{2},\bar{2},\dots,\bar{2},\bar{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N) si et seulement si $\bar{a} = \bar{b} = \bar{2}$ et $n \equiv 0[N]$ ou $\bar{a} = \bar{b} = \bar{0}$ et $n \equiv 2[N]$.

Démonstration. Supposons que $(\bar{a},\bar{2},\bar{2},\dots,\bar{2},\bar{b})$ est solution de (E_N).

Par la proposition 3.21, $\bar{a} = \bar{b}$. On a

$$\begin{aligned} M_n(\bar{a},\bar{2},\dots,\bar{2},\bar{a}) &= \begin{pmatrix} \bar{a} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} M_{n-2}(\bar{2},\dots,\bar{2}) \begin{pmatrix} \bar{a} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix}\begin{pmatrix} \overline{n-1} & \overline{-n+2} \\ \overline{n-2} & \overline{-n+3} \end{pmatrix}\begin{pmatrix} \bar{a} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \\ &= \begin{pmatrix} \overline{an-a-n+2} & \overline{-an+2a+n-3} \\ \overline{n-1} & \overline{-n+2} \end{pmatrix}\begin{pmatrix} \bar{a} & \overline{-1} \\ \bar{1} & \bar{0} \end{pmatrix} \\ &= \begin{pmatrix} \bar{x} & \bar{y} \\ \overline{an-a-n+2} & \overline{1-n} \end{pmatrix}. \end{aligned}$$

On a deux cas :

- $\overline{1-n} = \bar{1}$. Dans ce cas, $\bar{n} = \bar{0}$ c'est-à-dire $n \equiv 0[N]$ et $\bar{0} = \overline{an - a - n + 2} = \overline{-a+2}$ et donc $\bar{a} = \bar{2}$.

- $\overline{1-n} = \overline{-1}$. Dans ce cas, $\bar{n} = \bar{2}$ c'est-à-dire $n \equiv 2[N]$ et $\bar{0} = \overline{an - a - n + 2} = \bar{a}$.

Supposons que $\bar{a} = \bar{b} = \bar{2}$ et $n \equiv 0[N]$ ou $\bar{a} = \bar{b} = \bar{0}$ et $n \equiv 2[N]$. D'après le corollaire précédent, $(\bar{2}, \dots, \bar{2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ est solution de (E_N) et $(\bar{0}, \bar{0}) \in (\mathbb{Z}/N\mathbb{Z})^2$ est solution de (E_N). Donc, $(\bar{a}, \bar{2}, \bar{2}, \dots, \bar{2}, \bar{b})$ est solution de (E_N) (proposition 3.7). □

Ce théorème montre en particulier que $(\bar{2}, \dots, \bar{2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ est une solution monomiale minimale de (E_N).

On peut maintenant démontrer le théorème 2.9.

Démonstration du théorème 2.9. Si $N = 3$ alors le résultat est vrai (proposition 3.5) et on suppose maintenant $N \geq 4$. On suppose par l'absurde que cette solution peut s'écrire comme une somme de deux solutions non triviales.

Il existe $(\overline{a_1}, \dots, \overline{a_l})$ et $(\overline{b_1}, \dots, \overline{b_{l'}})$ solutions de (E_N) différentes de $(\bar{0}, \bar{0})$ avec $l + l' = N + 2$ et $l, l' \geq 3$ telles que

$$(\bar{2}, \dots, \bar{2}) = (\overline{b_1 + a_l}, \overline{b_2}, \dots, \overline{b_{l'-1}}, \overline{b_{l'} + a_1}, \overline{a_2}, \dots, \overline{a_{l-1}}).$$

On a donc $\overline{a_2} = \dots = \overline{a_{l-1}} = \bar{2}$. Comme $(\overline{a_1}, \dots, \overline{a_l})$ est solution de (E_N), on a par le lemme précédent $l \equiv 2[N]$ ou $l \equiv 0[N]$. Comme $l \geq 3$ on a nécessairement $l \geq N$ et donc $l' \leq 2$. Donc, $l' = 2$ et $(\overline{b_1}, \dots, \overline{b_{l'}}) = (\bar{0}, \bar{0})$ ce qui est absurde. □

On en déduit le corollaire suivant qui donne une autre solution irréductible dans le cas général.

Corollaire 3.31. *Si $N \geq 3$, $(\overline{N-2}, \dots, \overline{N-2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ est une solution irréductible de (E_N).*

Démonstration. Par la proposition 3.8, $(\overline{N-2}, \dots, \overline{N-2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ est une solution de (E_N). On s'intéresse maintenant à l'irréductibilité de la solution.

Si $N = 3$ alors le résultat est vrai (proposition 3.5) et on suppose maintenant $N \geq 4$. On suppose par l'absurde que cette solution peut s'écrire comme une somme de deux solutions non triviales.

Il existe $(\overline{a_1}, \dots, \overline{a_l})$ et $(\overline{b_1}, \dots, \overline{b_{l'}})$ solutions de (E_N) différentes de $(\bar{0}, \bar{0})$ avec $l + l' = N + 2$ et $l, l' \geq 3$ telles que

$$(\overline{N-2}, \dots, \overline{N-2}) = (\overline{b_1 + a_l}, \overline{b_2}, \dots, \overline{b_{l'-1}}, \overline{b_{l'} + a_1}, \overline{a_2}, \dots, \overline{a_{l-1}}).$$

On a donc $\overline{a_2} = \dots = \overline{a_{l-1}} = \overline{N-2}$.

De plus, $(\overline{-a_1}, \ldots, \overline{-a_l})$ est solution de (E_N) et $\overline{-a_2} = \ldots = \overline{-a_{l-1}} = \bar{2}$. Donc par le lemme 3.30, $l \equiv 2[N]$ ou $l \equiv 0[N]$. Comme $l \geq 3$, on a nécessairement $l \geq N$ et donc $l' \leq 2$. Donc, $l' = 2$ et $(\overline{b_1}, \ldots, \overline{b_{l'}}) = (\bar{0}, \bar{0})$ ce qui est absurde. □

4. Solution de (E_N) pour $N \in [\![2; 7]\!]$

4.1. Cas où $N = 2$

On commence par le cas $N = 2$ étudié dans [8].

Théorème 4.1 (voir [8, proposition 5.3])**.** *Les solutions irréductibles de* (E_2) *sont* $(\bar{1}, \bar{1}, \bar{1})$ *et* $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$.

Ce cas possède une description combinatoire particulièrement élégante nécessitant la définition suivante :

Définition 4.2.

(i) ([8, définition 3.1]) On appelle décomposition de type (3|4) le découpage d'un polygone convexe P à n sommets par des diagonales ne se coupant qu'aux sommets et tel que les sous-polygones soient des triangles ou des quadrilatères.

(ii) ([8, définition 3.3]) À chaque sommet de P on associe un élément $\bar{c}$ de $\mathbb{Z}/2\mathbb{Z}$ de la façon suivante

$$\bar{c} = \begin{cases} \bar{1}, & \text{si le nombre de triangles utilisant ce sommet est impair;} \\ \bar{0}, & \text{si le nombre de triangles utilisant ce sommet est pair.} \end{cases}$$

On parcourt les sommets, à partir de n'importe lequel d'entre eux, dans le sens horaire ou le sens trigonométrique, pour obtenir le n-uplet $(\overline{c_1}, \ldots, \overline{c_n})$. Ce n-uplet est la quiddité de la décomposition de type (3|4) de P.

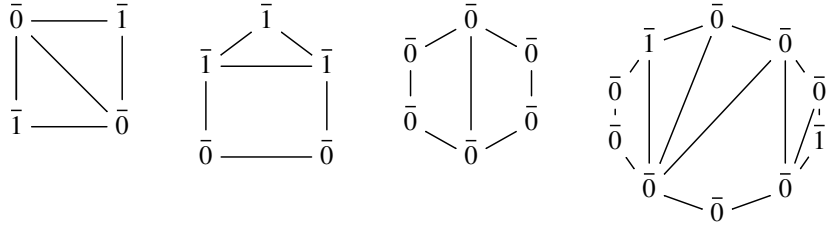
Remarque 4.3. Si $(\overline{c_1}, \ldots, \overline{c_n})$ est la quiddité d'une décomposition de type (3|4) de P alors tout n-uplet équivalent à $(\overline{c_1}, \ldots, \overline{c_n})$ est aussi la quiddité de cette décomposition de P.

Théorème 4.4 ([8, théorème 1])**.** *Soit* $n \geq 2$.

(i) *Une solution de* (E_2) *de taille n est la quiddité d'une décomposition de type* (3|4) *d'un polygone convexe à n sommets.*

(ii) *La quiddité d'une décomposition de type* (3|4) *d'un polygone convexe à n sommets est une solution de* (E_2) *de taille n.*

Exemples 4.5. Voici quelques exemples de décomposition de type (3|4) avec leur quiddité :



Remarque 4.6. On peut améliorer le théorème précédent. En effet, si $(\overline{c_1}, \ldots, \overline{c_n})$ est une solution de (E_2) et s'il existe un entier i dans $[\![1; n]\!]$ tel que $\overline{c_i} \neq \overline{0}$ alors $(\overline{c_1}, \ldots, \overline{c_n})$ est la quiddité d'une décomposition de type (3|4) d'un polygone convexe à n sommets ne contenant que des triangles (voir [8, remarque 5.4]).

4.2. **Cas** $N = 3$

On passe maintenant au cas $N = 3$.

4.2.1. **Démonstration du théorème 2.8(ii)**

Démonstration. Par la proposition 3.5, $(\overline{1}, \overline{1}, \overline{1})$, $(\overline{-1}, \overline{-1}, \overline{-1})$ et $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$ sont irréductibles. Par les propositions 3.2, 3.3, 3.5 et 3.10, il n'y a pas d'autres solutions irréductibles pour $n = 3, 4$. Soient $n \geq 5$ et $(\overline{a_1}, \ldots, \overline{a_n})$ une solution de (E_3). $(\overline{a_1}, \ldots, \overline{a_n})$ contient $\overline{0}$, $\overline{1}$ ou $\overline{-1}$, donc, par la proposition 3.10, $(\overline{a_1}, \ldots, \overline{a_n})$ est réductible. □

On en déduit le résultat suivant :

Proposition 4.7. *Si* $(\overline{a_1}, \ldots, \overline{a_n})$ *est solution de* (E_3) *alors* $\overline{a_1} + \ldots + \overline{a_n} = \overline{0}$.

Démonstration. On raisonne par récurrence sur n.

Le résultat est vrai pour $n = 2$, $n = 3$ et $n = 4$.

On suppose maintenant $n \geq 5$. Soit $(\overline{a_1}, \ldots, \overline{a_n})$ une solution de (E_3). $(\overline{a_1}, \ldots, \overline{a_n})$ est équivalent à la somme d'un k-uplet $(\overline{b_1}, \ldots, \overline{b_k})$ solution de (E_3) ($k = n - 1$ ou $k = n - 2$) avec une des solutions irréductibles de (E_3), $(\overline{c_1}, \ldots, \overline{c_l})$ ($l = 3$ ou $l = 4$).

$\overline{b_1} + \ldots + \overline{b_k} = \overline{0}$ (par hypothèse de récurrence) et $\overline{c_1} + \ldots + \overline{c_l} = \overline{0}$ (par l'initialisation). On a,

$$\overline{a_1} + \ldots + \overline{a_n} = \overline{b_1} + \ldots + \overline{b_k} + \overline{c_1} + \ldots + \overline{c_l} = \overline{0}.$$

Donc, si $(\overline{a_1}, \ldots, \overline{a_n})$ est solution de (E_3) alors $\overline{a_1} + \ldots + \overline{a_n} = \overline{0}$. □

4.2.2. **Description combinatoire des solutions**

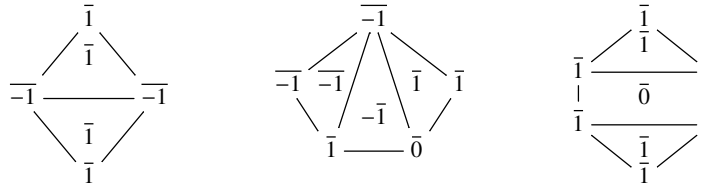
Définition 4.8.

(i) On appelle décomposition pondérée de type (3|4) de première espèce le découpage d'un polygone convexe P à n sommets par des diagonales ne se coupant qu'aux sommets et tel que les sous-polygones soient des triangles de poids $\overline{1}$ ou $\overline{-1}$ ou des quadrilatères de poids $\overline{0}$.

(ii) On choisit un sommet de P que l'on numérote par 1 puis on numérote les autres sommets de P en suivant le sens horaire ou le sens trigonométrique. La quiddité de la décomposition pondérée de type (3|4) de première espèce de P est le n-uplet $(\overline{c_1}, \dots, \overline{c_n})$ avec $\overline{c_i}$ la somme des poids des sous-polygones utilisant le sommet i.

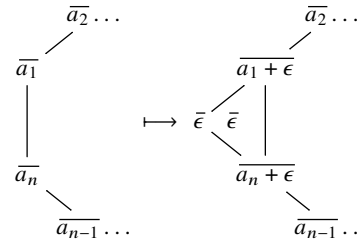
Remarque 4.9. Si $(\overline{c_1}, \dots, \overline{c_n})$ est la quiddité de la décomposition pondérée de type (3|4) de première espèce de P alors tout n-uplet équivalent à $(\overline{c_1}, \dots, \overline{c_n})$ est aussi la quiddité de cette décomposition de P.

Exemples 4.10. Voici quelques exemples :

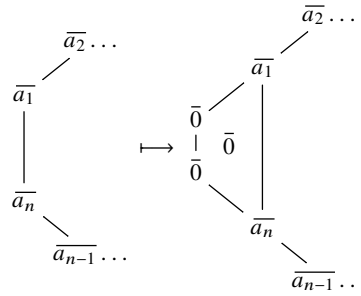


Pour relier les solutions de (E_3) aux découpages de polygones on a besoin d'interpréter géométriquement la somme de deux solutions (voir aussi [4, section 4]). Soit $(\overline{a_1}, \dots, \overline{a_n})$ la quiddité d'une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe P à n sommets.

- Si $\epsilon \in \{\pm 1\}$ alors $(\overline{a_1}, \dots, \overline{a_n}) \oplus (\overline{\epsilon}, \overline{\epsilon}, \overline{\epsilon})$ est la quiddité de la décomposition pondérée de type (3|4) de première espèce du polygone convexe à $(n+1)$ sommets obtenue en rajoutant un triangle de poids $\overline{\epsilon}$ sur le segment reliant le sommet 1 de P au sommet n de P.



- $(\overline{a_1}, \ldots, \overline{a_n}) \oplus (\overline{0}, \overline{0}, \overline{0}, \overline{0})$ est la quiddité de la décomposition pondérée de type (3|4) de première espèce du polygone convexe à $(n+2)$ sommets obtenue en rajoutant un quadrilatère de poids $\overline{0}$ sur le segment reliant le sommet 1 de P au sommet n de P.



Théorème 4.11. *Soit $n \geq 3$.*

(i) *Toute solution de (E_3) de taille n est la quiddité associée à une décomposition pondérée de type* (3|4) *de première espèce d'un polygone convexe à n sommets.*

(ii) *Toute quiddité associée à une décomposition pondérée de type* (3|4) *de première espèce d'un polygone convexe à n sommets est une solution de taille n de (E_3).*

Démonstration. (i). On raisonne par récurrence sur n.

Si $n = 3$ on a deux solutions $(\overline{1}, \overline{1}, \overline{1})$ qui est la quiddité associée à un triangle de poids $\overline{1}$ et $(\overline{-1}, \overline{-1}, \overline{-1})$ qui est la quiddité associée à un triangle de poids $\overline{-1}$.

Si $n = 4$ on a (à permutations cycliques près) trois solutions :

- $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$ qui est la quiddité associée à un quadrilatère de poids $\overline{0}$.
- $(\overline{1}, \overline{-1}, \overline{1}, \overline{-1})$ qui est la quiddité associée à un quadrilatère découpé en deux triangles de poids $\overline{1}$.
- $(\overline{0}, \overline{-1}, \overline{0}, \overline{1})$ qui est la quiddité associée à un quadrilatère découpé en un triangle de poids $\overline{1}$ et un triangle de poids $\overline{-1}$.

Soient $n \geq 5$ et $(\overline{a_1}, \ldots, \overline{a_n})$ une solution de (E_3). $(\overline{a_1}, \ldots, \overline{a_n})$ est équivalent à la somme d'un k-uplet $(\overline{b_1}, \ldots, \overline{b_k})$ ($k = n-1$ ou $k = n-2$) avec une des solutions irréductibles de (E_3). $(\overline{b_1}, \ldots, \overline{b_k})$ est toujours solution de (E_3) (proposition 3.9) donc il correspond par hypothèse de récurrence à une quiddité associée à une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe à k sommets. Par la discussion précédente, $(\overline{a_1}, \ldots, \overline{a_n})$ est aussi associée à une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe à n sommets.

(ii). On raisonne par récurrence sur n.

Si $n = 3$, les quiddités associées aux décompositions pondérées de type (3|4) de premières espèces sont $(\overline{1}, \overline{1}, \overline{1})$ et $(\overline{-1}, \overline{-1}, \overline{-1})$. Ce sont des solutions de (E_3). Si $n = 4$, les quiddités associées aux décompositions pondérées de type (3|4) de premières espèces sont (à permutation cyclique près) $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$, $(\overline{1}, \overline{-1}, \overline{1}, \overline{-1})$ et $(\overline{0}, \overline{-1}, \overline{0}, \overline{1})$ (le découpage d'un carré en deux triangles de poids $\overline{-1}$ donnant aussi $(\overline{1}, \overline{-1}, \overline{1}, \overline{-1})$). Ce sont des solutions de (E_3).

Considérons une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe P à n sommets et $(\overline{a_1}, \dots, \overline{a_n})$ la quiddité associée.

Si P est le seul sous-polygone intervenant dans la décomposition alors $n = 4$ ou $n = 3$ et donc la quiddité associée à la décomposition est solution de (E_3).

Sinon on peut trouver un sous-polygone dont tous les cotés sauf un sont des cotés de P. Ce polygone est soit un quadrilatère (cas 1) soit un triangle de poids $\overline{\epsilon}$ avec $\overline{\epsilon} \in \{\pm\overline{1}\}$ (cas 2). On considère le polygone P' obtenu en ne conservant de ce sous-polygone que le coté qui n'était pas un coté de P. La décomposition de P donne alors une décomposition pondérée de type (3|4) de première espèce de P' et la quiddité $(\overline{b_1}, \dots, \overline{b_k})$ associée à cette décomposition est solution de (E_3) (par hypothèse de récurrence). Comme $(\overline{a_1}, \dots, \overline{a_n})$ est équivalente à la somme de $(\overline{b_1}, \dots, \overline{b_k})$ avec $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$ (dans le cas 1) ou à la somme de $(\overline{b_1}, \dots, \overline{b_k})$ avec $(\overline{\epsilon}, \overline{\epsilon}, \overline{\epsilon})$ (dans le cas 2) on a que $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_3). □

Proposition 4.12. *Si $(\overline{c_1}, \dots, \overline{c_n})$ est une solution de (E_3) et s'il existe un entier i dans $[\![1; n]\!]$ tel que $\overline{c_i} \neq \overline{0}$ alors $(\overline{c_1}, \dots, \overline{c_n})$ est la quiddité d'une décomposition pondérée de type* (3|4) *de première espèce d'un polygone convexe à n sommets ne contenant que des triangles.*

Démonstration. On raisonne par récurrence sur n.

Si $n = 3$ alors (E_3) a deux solutions $(\overline{1}, \overline{1}, \overline{1})$ et $(\overline{-1}, \overline{-1}, \overline{-1})$. $(\overline{1}, \overline{1}, \overline{1})$ est la quiddité associée un triangle de poids $\overline{1}$ et $(\overline{-1}, \overline{-1}, \overline{-1})$ est la quiddité associée à un triangle de poids $\overline{-1}$.

Supposons qu'il existe un $n \in \mathbb{N}^*$, $n \geq 3$, tel que toute solution de (E_3) de taille n possédant au moins un élément différent de $\overline{0}$ est la quiddité d'une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe à n sommets ne contenant que des triangles.

Soit $(\overline{a_1}, \dots, \overline{a_{n+1}})$ une solution de (E_3) telle qu'il existe un entier i dans $[\![1\ ;\ n+1]\!]$ tel que $\overline{a_i} = \overline{\epsilon}$ avec $\epsilon \in \{\pm 1\}$. On a

$$(\overline{a_1}, \dots, \overline{a_{n+1}}) \sim (\overline{a_{i+1} - \epsilon}, \dots, \overline{a_{n+1}}, \overline{a_1}, \dots, \overline{a_{i-1} - \epsilon}) \oplus (\overline{\epsilon}, \overline{\epsilon}, \overline{\epsilon}).$$

Donc, par la proposition 3.9, $(\overline{a_{i+1}-\epsilon},\dots,\overline{a_n},\overline{a_1},\dots,\overline{a_{i-1}-\epsilon})$ est une solution de (E_3) et donc par invariance circulaire $(\overline{a_1},\dots,\overline{a_{i-1}-\epsilon},\overline{a_{i+1}-\epsilon},\dots,\overline{a_{n+1}})$ est une solution de (E_3). On a deux cas :

(A) $(\overline{a_1},\dots,\overline{a_{i-1}-\epsilon},\overline{a_{i+1}-\epsilon},\dots,\overline{a_{n+1}})$ possède au moins un élément différent de $\bar{0}$. Par hypothèse de récurrence, ce n-uplet est la quiddité d'une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe à n sommets P ne contenant que des triangles. $(\overline{a_1},\dots,\overline{a_{n+1}})$ est la quiddité d'une décomposition pondérée de type (3|4) de première espèce d'un polygone convexe à $(n+1)$ sommets ne contenant que des triangles construit en rajoutant un triangle de poids $\bar{\epsilon}$ sur le segment reliant le sommet $i-1$ de P au sommet i de P.

(B) $(\overline{a_1},\dots,\overline{a_{i-1}-\epsilon},\overline{a_{i+1}-\epsilon},\dots,\overline{a_{n+1}})$ ne contient que $\bar{0}$. Dans ce cas,

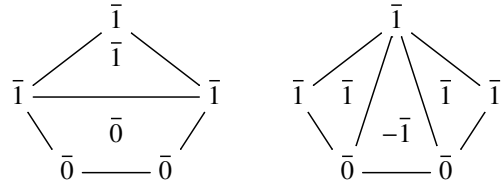
$$(\overline{a_1},\dots,\overline{a_{n+1}}) = (\bar{0},\dots,\bar{0},\bar{\epsilon},\bar{\epsilon},\bar{\epsilon},\bar{0},\dots,\bar{0})$$

c'est-à-dire $\overline{a_i} = \overline{a_{i-1}} = \overline{a_{i+1}} = \bar{\epsilon}$ et tous les autres $\overline{a_j}$ sont égaux à $\bar{0}$. On a

$$(\overline{a_1},\dots,\overline{a_{n+1}}) \sim (\overline{a_{i+2}-\epsilon},\dots,\overline{a_{n+1}},\overline{a_1},\dots,\overline{a_{i-1}},\overline{a_i-\epsilon}) \oplus (\bar{\epsilon},\bar{\epsilon},\bar{\epsilon}).$$

Ainsi, $(\overline{a_1},\dots,\overline{a_{i-1}},\overline{a_i-\epsilon},\overline{a_{i+2}-\epsilon},\dots,\overline{a_{n+1}})$ est une solution de (E_3) contenant $\overline{a_{i-1}} = \bar{\epsilon}$. Donc, on peut procéder comme en (A). □

Exemple 4.13. Par exemple,



4.3. **N=4**

On étudie maintenant le cas $N = 4$.

4.3.1. **Démonstration du théorème 2.8(iii)**

Démonstration. Par les propositions 3.5 et 3.10, $(\bar{1},\bar{1},\bar{1})$, $(\overline{-1},\overline{-1},\overline{-1})$, $(\bar{0},\bar{0},\bar{0},\bar{0})$, $(\bar{0},\bar{2},\bar{0},\bar{2})$,$(\bar{2},\bar{0},\bar{2},\bar{0})$ et $(\bar{2},\bar{2},\bar{2},\bar{2})$ sont irréductibles. Par les propositions 3.2, 3.3, 3.5 et 3.10, il n'y a pas d'autres solutions irréductibles pour $n = 3,4$. Soient $n \geq 5$ et $(\overline{a_1},\dots,\overline{a_n})$ une solution de (E_4). On a deux cas :

- Si $(\overline{a_1}, \dots, \overline{a_n})$ contient $\overline{0}$, $\overline{1}$ ou $\overline{-1}$ alors, par la proposition 3.10, $(\overline{a_1}, \dots, \overline{a_n})$ est réductible.

- Si $(\overline{a_1}, \dots, \overline{a_n})$ ne contient pas $\overline{0}$, $\overline{1}$ ou $\overline{-1}$ alors $\forall\ i \in [\![1; n]\!]\ \overline{a_i} = \overline{2}$ et donc $(\overline{a_1}, \dots, \overline{a_n})$ est réductible puisqu'on peut l'écrire comme la somme du $(n-2)$-uplet $(\overline{0}, \overline{2}, \dots, \overline{2}, \overline{0})$ $(n - 2 \geq 3)$ avec $(\overline{2}, \overline{2}, \overline{2}, \overline{2})$. □

4.3.2. **Description combinatoire des solutions**

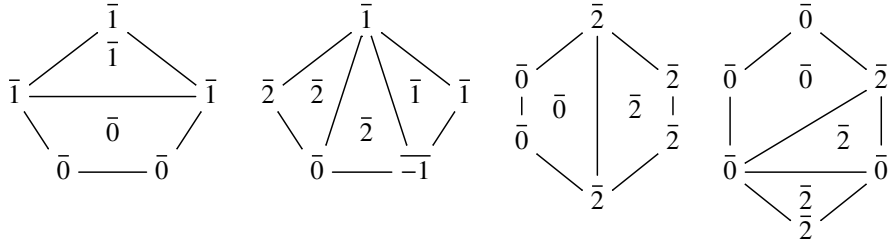
Définition 4.14.

(i) On appelle décomposition pondérée de type (3|4) de seconde espèce le découpage d'un polygone convexe à n sommets par des diagonales ne se coupant qu'aux sommets et tel que les sous-polygones soient des triangles de poids $\overline{1}$ ou $\overline{-1}$, des quadrilatères de poids $\overline{0}$ ou $\overline{2}$ ou des quadrilatères découpés en deux triangles de poids $\overline{2}$.

(ii) On choisit un sommet de P que l'on numérote par 1 puis on numérote les autres sommets de P en suivant le sens horaire ou le sens trigonométrique. La quiddité de la décomposition pondérée de type (3|4) de seconde espèce de P est le n-uplet $(\overline{c_1}, \dots, \overline{c_n})$ avec $\overline{c_i}$ la somme des poids des sous-polygones utilisant le sommet i.

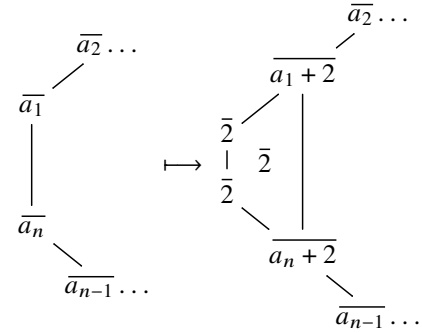
Remarque 4.15. Si $(\overline{c_1}, \dots, \overline{c_n})$ est la quiddité de la décomposition pondérée de type (3|4) de seconde espèce de P alors tout n-uplet équivalent à $(\overline{c_1}, \dots, \overline{c_n})$ est aussi la quiddité de cette décomposition de P.

Exemples 4.16. Voici quelques exemples :

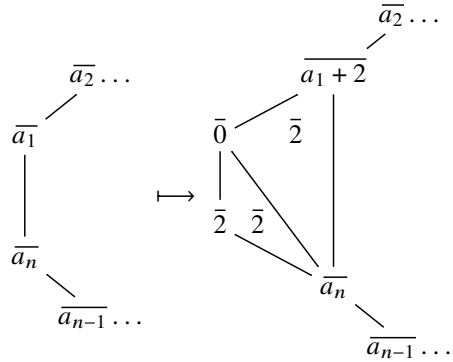


Les considérations géométriques données après la définition 4.8 s'adaptent naturellement au cas des décompositions pondérées de type (3|4) de seconde espèce. Pour relier les solutions de (E_4) aux découpages de polygones on a besoin en plus des considérations suivantes :

- $(\overline{a_1}, \ldots, \overline{a_n}) \oplus (\overline{2}, \overline{2}, \overline{2}, \overline{2})$ est la quiddité de la décomposition pondérée de type (3|4) de seconde espèce du polygone convexe à $(n+2)$ sommets obtenue en rajoutant un quadrilatère de poids $\overline{2}$ sur le segment reliant le sommet 1 de P au sommet n de P.



- $(\overline{a_1}, \ldots, \overline{a_n}) \oplus (\overline{0}, \overline{2}, \overline{0}, \overline{2})$ est la quiddité de la décomposition pondérée de type (3|4) de seconde espèce du polygone convexe à $(n+2)$ sommets obtenue en rajoutant un quadrilatère découpés en deux triangles de poids $\overline{2}$ sur le segment reliant le sommet 1 de P au sommet n de P.



Théorème 4.17. *Soit $n \geq 3$.*

(i) *Toute solution de (E_4) de taille n est la quiddité associée à une décomposition pondérée de type* (3|4) *de seconde espèce d'un polygone convexe à n sommets.*

(ii) *Toute quiddité associée à une décomposition pondérée de type* (3|4) *de seconde espèce d'un polygone convexe à n sommets est une solution de taille n de (E_4).*

Démonstration. (i). On raisonne par récurrence sur n.

Si $n = 3$, (E_4) a deux solutions $(\overline{1}, \overline{1}, \overline{1})$ qui est la quiddité associée à un triangle de poids $\overline{1}$ et $(\overline{-1}, \overline{-1}, \overline{-1})$ qui est la quiddité associée à un triangle de poids $\overline{-1}$.

Si $n = 4$, on a (à permutations cycliques près) six solutions $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$, $(\overline{1}, \overline{2}, \overline{1}, \overline{2})$, $(\overline{0}, \overline{2}, \overline{0}, \overline{2})$, $(\overline{0}, \overline{1}, \overline{0}, \overline{-1})$, $(\overline{2}, \overline{-1}, \overline{2}, \overline{-1})$ et $(\overline{2}, \overline{2}, \overline{2}, \overline{2})$ qui sont chacune une quiddité d'une décomposition pondérée de type (3|4) de seconde espèce d'un quadrilatère.

Soient $n \geq 5$ et $(\overline{a_1}, \dots, \overline{a_n})$ une solution de (E_4). $(\overline{a_1}, \dots, \overline{a_n})$ est équivalent à la somme d'un k-uplet $(\overline{b_1}, \dots, \overline{b_k})$ ($k = n - 1$ ou $k = n - 2$) avec une des solutions irréductibles de (E_4). $(\overline{b_1}, \dots, \overline{b_k})$ est toujours solution de (E_4) (proposition 3.9) donc il correspond par hypothèse de récurrence à une quiddité associée à une décomposition pondérée de type (3|4) de seconde espèce d'un polygone convexe à k sommets. Par la discussion géométrique précédente, $(\overline{a_1}, \dots, \overline{a_n})$ est aussi associée à une décomposition pondérée de type (3|4) de seconde espèce d'un polygone convexe à n sommets.

(ii). On raisonne par récurrence sur n.

Si $n = 3$, les quiddités associées aux décompositions pondérées de type (3|4) de seconde espèce sont $(\overline{1}, \overline{1}, \overline{1})$ et $(\overline{-1}, \overline{-1}, \overline{-1})$. Ce sont des solutions de (E_4). Si $n = 4$, les quiddités associées aux décompositions pondérées de type (3|4) de seconde espèce sont (à permutation cyclique près) $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$, $(\overline{1}, \overline{2}, \overline{1}, \overline{2})$, $(\overline{0}, \overline{2}, \overline{0}, \overline{2})$, $(\overline{0}, \overline{1}, \overline{0}, \overline{-1})$, $(\overline{2}, \overline{-1}, \overline{2}, \overline{-1})$ et $(\overline{2}, \overline{2}, \overline{2}, \overline{2})$. Ce sont des solutions de (E_4).

Considérons une décomposition pondérée de type (3|4) de seconde espèce d'un polygone convexe P à n sommets et $(\overline{a_1}, \dots, \overline{a_n})$ la quiddité associée.

Si P est le seul sous-polygone intervenant dans la décomposition alors $n = 4$ ou $n = 3$ et donc la quiddité associée à la décomposition est solution de (E_4).

Sinon on peut trouver un sous-polygone dont tous les cotés sauf un sont des cotés de P. Ce polygone est soit un quadrilatère de poids $\overline{0}$ (cas 1) soit un quadrilatère de poids $\overline{2}$ (cas 2) soit un triangle de poids $\overline{\epsilon}$ avec $\epsilon \in \{\pm 1\}$ (cas 3) soit un triangle de poids $\overline{2}$.

Si l'on est dans les cas 1, 2 ou 3. On considère le polygone P' obtenu en ne conservant de ce sous-polygone que le coté qui n'était pas un coté de P. La décomposition de P donne alors une décomposition pondérée de type (3|4) de seconde espèce de P' et la quiddité $(\overline{b_1}, \dots, \overline{b_k})$ associée à cette décomposition est solution de (E_4) par hypothèse de récurrence. Comme $(\overline{a_1}, \dots, \overline{a_n})$ est équivalente à la somme de $(\overline{b_1}, \dots, \overline{b_k})$ avec $(\overline{0}, \overline{0}, \overline{0}, \overline{0})$ (dans le cas 1), $(\overline{2}, \overline{2}, \overline{2}, \overline{2})$ (dans le cas 2) ou $(\overline{\epsilon}, \overline{\epsilon}, \overline{\epsilon})$ (dans le cas 3) on a que $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_4).

Si l'on n'est pas dans les cas 1, 2 ou 3. Il existe un triangle extérieur de poids $\overline{2}$ adjacent à un triangle de poids $\overline{2}$ dont l'un des côtés est un côté de P. Si ces deux triangles sont les deux seuls sous-polygones intervenant dans la décomposition de P alors $n = 4$ et la quiddité associée est solution de (E_4). Sinon on considère le polygone P' obtenu en

supprimant ces deux triangles. La décomposition de P donne alors une décomposition pondérée de type (3|4) de seconde espèce de P' et la quiddité $(\overline{b_1}, \dots, \overline{b_k})$ associée à cette décomposition est solution de (E_4) par hypothèse de récurrence. Comme $(\overline{a_1}, \dots, \overline{a_n})$ est équivalente à la somme de $(\overline{b_1}, \dots, \overline{b_k})$ avec $(\bar{0}, \bar{2}, \bar{0}, \bar{2})$ on a que $(\overline{a_1}, \dots, \overline{a_n})$ est solution de (E_4). □

On ne peut malheureusement pas étendre la proposition 4.12 pour $N = 4$. En effet, $(\bar{2}, \bar{2}, \bar{2}, \bar{2})$ est solution de (E_4) mais n'est pas la quiddité d'une décomposition pondérée de type (3|4) de seconde espèce d'un quadrilatère ne contenant que des triangles. On dispose cependant du résultat suivant :

Proposition 4.18. *Si $(\overline{c_1}, \dots, \overline{c_n})$ est une solution de (E_4) et s'il existe un entier i dans $[\![1; n]\!]$ tel que $\overline{c_i} \in \{\pm\bar{1}\}$ alors $(\overline{c_1}, \dots, \overline{c_n})$ est la quiddité d'une décomposition pondérée de type* (3|4) *de seconde espèce d'un polygone convexe à n sommets ne contenant que des triangles.*

Démonstration. On raisonne par récurrence sur n.

Si $n = 3$ alors (E_4) a deux solutions $(\bar{1}, \bar{1}, \bar{1})$ et $(\overline{-1}, \overline{-1}, \overline{-1})$. $(\bar{1}, \bar{1}, \bar{1})$ est la quiddité associée à un triangle de poids $\bar{1}$ et $(\overline{-1}, \overline{-1}, \overline{-1})$ est la quiddité associée à un triangle de poids $\overline{-1}$.

Supposons qu'il existe un $n \in \mathbb{N}^*$ $n \geq 3$ tel que toute solution de (E_4) de taille n possédant au moins un élément valant $\pm\bar{1}$ est la quiddité d'une décomposition pondérée de type (3|4) de seconde espèce d'un polygone convexe à n sommets ne contenant que des triangles.

Soit $(\overline{a_1}, \dots, \overline{a_{n+1}})$ une solution de (E_4) possédant au moins un élément valant $\pm\bar{1}$. $\exists\, i \in [\![1; n+1]\!]$ tel que $\overline{a_i} = \bar{\epsilon}$ avec $\epsilon \in \{\pm 1\}$. On a

$$(\overline{a_1}, \dots, \overline{a_{n+1}}) \sim (\overline{a_{i+1} - \epsilon}, \dots, \overline{a_{n+1}}, \overline{a_1}, \dots, \overline{a_{i-1} - \epsilon}) \oplus (\bar{\epsilon}, \bar{\epsilon}, \bar{\epsilon}).$$

Donc, par la proposition 3.9, $(\overline{a_{i+1} - \epsilon}, \dots, \overline{a_{n+1}}, \overline{a_1}, \dots, \overline{a_{i-1} - \epsilon})$ est une solution de (E_4) et donc par invariance circulaire $(\overline{a_1}, \dots, \overline{a_{i-1} - \epsilon}, \overline{a_{i+1} - \epsilon}, \dots, \overline{a_{n+1}})$ est une solution de (E_4). On a deux cas :

(A) $(\overline{a_1}, \dots, \overline{a_{i-1} - \epsilon}, \overline{a_{i+1} - \epsilon}, \dots, \overline{a_{n+1}})$ possède au moins un élément valant $\pm\bar{1}$. Par hypothèse de récurrence, ce n-uplet est la quiddité d'une décomposition pondérée de type (3|4) de seconde espèce d'un polygone convexe à n sommets P ne contenant que des triangles. $(\overline{a_1}, \dots, \overline{a_{n+1}})$ est la quiddité d'une décomposition pondérée de type (3|4) de seconde espèce d'un polygone convexe à $(n + 1)$ sommets ne contenant que des triangles construit en rajoutant un triangle de poids $\bar{\epsilon}$ sur le segment reliant le sommet $i - 1$ de P au sommet i de P.

(B) $(\overline{a_1}, \dots, \overline{a_{i-1}-\epsilon}, \overline{a_{i+1}-\epsilon}, \dots, \overline{a_{n+1}})$ ne contient pas d'élément valant $\pm\overline{1}$. Dans ce cas, $\overline{a_{i-1}} = \overline{\alpha} \in \{\pm\overline{1}\}$ et $\overline{a_{i+1}} = \overline{\beta} \in \{\pm\overline{1}\}$ (car $\overline{a_{i-1}-\epsilon} \in \{\overline{0}, \overline{2}\}$ et $\overline{a_{i+1}-\epsilon} \in \{\overline{0}, \overline{2}\}$) et tous les autres $\overline{a_j}$ ($j \neq i, i-1, i+1$) sont égaux à $\overline{0}$ ou $\overline{2}$. On a

$$(\overline{a_1}, \dots, \overline{a_{n+1}}) \sim (\overline{a_{i+2}-\beta}, \dots, \overline{a_{n+1}}, \overline{a_1}, \dots, \overline{a_{i-1}}, \overline{a_i-\beta}) \oplus (\overline{\beta}, \overline{\beta}, \overline{\beta}).$$

Ainsi, $(\overline{a_1}, \dots, \overline{a_{i-1}}, \overline{a_i-\beta}, \overline{a_{i+2}-\beta}, \dots, \overline{a_{n+1}})$ est une solution de (E_4) contenant $\overline{a_{i-1}} = \overline{\alpha}$. Donc, on peut procéder comme en (A). □

4.4. **Cas** $N = 5$

Démonstration du théorème 2.8(iv). Par les propositions 3.2, 3.3, 3.5 et 3.10, les seules solutions irréductibles de (E_5) de taille 3 et 4 sont celles données dans l'énoncé. $(\overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2})$ est une solution irréductible (Théorème 2.9) et $(\overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3})$ est une solution irréductible (Corollaire 3.31).

Un simple calcul montre que $(\overline{3}, \overline{2}, \overline{2}, \overline{3}, \overline{2}, \overline{2})$, $(\overline{2}, \overline{3}, \overline{3}, \overline{2}, \overline{3}, \overline{3})$ et $(\overline{2}, \overline{3}, \overline{2}, \overline{3}, \overline{2}, \overline{3})$ sont solutions de (E_5). Supposons par l'absurde $(\overline{3}, \overline{2}, \overline{2}, \overline{3}, \overline{2}, \overline{2})$ réductible. Comme $(\overline{3}, \overline{2}, \overline{2}, \overline{3}, \overline{2}, \overline{2})$ ne contient pas $\overline{1}$ ou $\overline{-1}$, elle est équivalente à la somme de deux solutions de taille 4 ne contenant pas $\overline{1}$ ou $\overline{-1}$. Elle contient alors nécessairement $\overline{0}$ ce qui est absurde. On montre de la même façon que $(\overline{2}, \overline{3}, \overline{3}, \overline{2}, \overline{3}, \overline{3})$ et $(\overline{2}, \overline{3}, \overline{2}, \overline{3}, \overline{2}, \overline{3})$ sont irréductibles.

Soit $(\overline{a_1}, \dots, \overline{a_n})$ une solution de (E_5).

Si $n = 5$. S'il existe un entier i dans $[\![1; n]\!]$ tel que $\overline{a_i} \in \{\overline{1}, \overline{-1}, \overline{0}\}$ alors $(\overline{a_1}, \dots, \overline{a_5})$ est réductible par la proposition 3.10. Si $\forall\, i \in [\![1; n]\!]$ $\overline{a_i} \notin \{\overline{1}, \overline{-1}, \overline{0}\}$ alors les $\overline{a_i}$ valent $\overline{2}$ ou $\overline{3}$. On a donc 32 possibilités et si on effectue le calcul pour chacune de ces possibilités on trouve seulement 2 solutions : $(\overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2})$ et $(\overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3})$.

Si $n \geq 6$. Si un des $\overline{a_i}$ est égal à $\overline{0}$, $\overline{1}$ ou $\overline{-1}$ alors $(\overline{a_1}, \dots, \overline{a_n})$ est réductible par la proposition 3.10.

Si $\forall\, i \in [\![1; n]\!]$ $\overline{a_i} \notin \{\overline{1}, \overline{-1}, \overline{0}\}$. On a plusieurs cas :

- Si $(\overline{a_1}, \dots, \overline{a_n})$ contient trois $\overline{2}$ (respectivement $\overline{3}$) consécutifs alors $(\overline{a_1}, \dots, \overline{a_n})$ est réductible puisqu'il est équivalent à la somme d'un $(n-3)$-uplet ($n - 3 \geq 3$) avec $(\overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{2})$ (respectivement $(\overline{3}, \overline{3}, \overline{3}, \overline{3}, \overline{3})$).

- Si $(\overline{a_1}, \dots, \overline{a_n})$ ne contient ni trois $\overline{2}$ consécutifs ni trois $\overline{3}$ consécutifs mais contient deux $\overline{2}$ (respectivement $\overline{3}$) consécutifs. Dans ce cas, $(\overline{a_1}, \dots, \overline{a_n})$ contient $(\overline{3}, \overline{2}, \overline{2}, \overline{3})$ (respectivement $(\overline{2}, \overline{3}, \overline{3}, \overline{2})$). Donc, $(\overline{a_1}, \dots, \overline{a_n})$ est équivalent à la somme d'un $(n-4)$-uplet avec $(\overline{2}, \overline{3}, \overline{2}, \overline{2}, \overline{3}, \overline{2})$ (respectivement $(\overline{3}, \overline{2}, \overline{3}, \overline{3}, \overline{2}, \overline{3})$. Si $n = 6$ alors $n - 4 = 2$ et donc $(\overline{a_1}, \dots, \overline{a_n})$ est équivalent à $(\overline{2}, \overline{3}, \overline{2}, \overline{2}, \overline{3}, \overline{2})$

(respectivement $(\overline{3},\overline{2},\overline{3},\overline{3},\overline{2},\overline{3})$). Si $n \geq 7$ alors $n-4 \geq 3$ et $(\overline{a_1},\dots,\overline{a_n})$ est réductible.

- Si on n'est dans aucun de ces deux cas alors n est pair et $(\overline{a_1},\dots,\overline{a_n})$ est équivalent au n-uplet constitué de la répétition de $(\overline{2},\overline{3})$. Si $n=6$ alors $(\overline{a_1},\dots,\overline{a_n})$ est équivalent à $(\overline{2},\overline{3},\overline{2},\overline{3},\overline{2},\overline{3})$. Si $n \geq 7$ alors $(\overline{a_1},\dots,\overline{a_n})$ est équivalent à la somme d'un $(n-4)$-uplet avec $(\overline{3},\overline{2},\overline{3},\overline{2},\overline{3},\overline{2})$ et $n-4 \geq 3$. Donc, $(\overline{a_1},\dots,\overline{a_n})$ est réductible. □

4.5. **cas** $N = 6$

Démonstration du Théorème 2.8(v). Par les propositions 3.2, 3.3, 3.5 et 3.10, les seules solutions irréductibles de (E_6) pour $n=3$ et $n=4$ sont celles données dans l'énoncé. $(\overline{2},\overline{2},\overline{2},\overline{2},\overline{2},\overline{2})$ est une solution irréductible (Théorème 2.9) et $(\overline{4},\overline{4},\overline{4},\overline{4},\overline{4},\overline{4})$ est une solution irréductible (Corollaire 3.31). On vérifie que $(\overline{3},\overline{3},\overline{3},\overline{3},\overline{3},\overline{3})$ est solution. De plus, celle-ci est irréductible (car (E_6) n'a pas de solutions de la forme $(\overline{a},\overline{3},\overline{b})$ ou $(\overline{a},\overline{3},\overline{3},\overline{b})$).

Soit $n \geq 5$. Soit $(\overline{a_1},\dots,\overline{a_n})$ une solution de (E_6).

(A) Si un des $\overline{a_i}$ est égal à $\overline{0}$, $\overline{1}$ ou $\overline{-1}$ alors $(\overline{a_1},\dots,\overline{a_n})$ est réductible par la proposition 3.10.

(B) Sinon les $\overline{a_i}$ ne peuvent valoir que $\overline{2}$, $\overline{3}$ ou $\overline{4}$. On a trois cas :

(i) Il existe un entier i dans $[\![1;n]\!]$ tel que $\overline{a_i}=\overline{2}$.

S'il existe un entier i dans $[\![1;n]\!]$ tel que $\overline{a_i}=\overline{2}$ et $\overline{a_{i-1}} \neq \overline{2}$ ou $\overline{a_{i+1}} \neq \overline{2}$ alors $(\overline{a_1},\dots,\overline{a_n})$ est réductible. En effet, si $\overline{a_{i+1}}=\overline{3}$ alors

$$(\overline{a_{i+2}},\dots,\overline{a_n},\overline{a_1},\dots,\overline{a_{i-1}},\overline{a_i},\overline{a_{i+1}}) = (\overline{a_{i+2}-4},\dots,\overline{a_n},\overline{a_1},\dots,\overline{a_{i-1}-3}) \oplus (\overline{3},\overline{2},\overline{3},\overline{4}).$$

On procède de façon analogue si $\overline{a_{i-1}}=\overline{3}$. Si $\overline{a_{i+1}}=\overline{4}$ alors

$$(\overline{a_{i+2}},\dots,\overline{a_n},\overline{a_1},\dots,\overline{a_{i-1}},\overline{a_i},\overline{a_{i+1}}) = (\overline{a_{i+2}-2},\dots,\overline{a_n},\overline{a_1},\dots,\overline{a_{i-1}-4}) \oplus (\overline{4},\overline{2},\overline{4},\overline{2}).$$

On procède de façon analogue si $\overline{a_{i-1}}=\overline{4}$.

Sinon tous les $\overline{a_i}$ sont égaux à $\overline{2}$. Dans ce cas, on a $n \equiv 0\ [N]$ par le lemme 3.30. Si $n=6$ alors $(\overline{a_1},\dots,\overline{a_n})$ est irréductible (Théorème 2.9) et sinon $n \geq 12$ et $(\overline{a_1},\dots,\overline{a_n})$ est réductible puisqu'on peut l'écrire comme la somme du $(n-4)$-uplet $(\overline{0},\overline{2},\dots,\overline{2},\overline{0})$ avec $(\overline{2},\overline{2},\overline{2},\overline{2},\overline{2},\overline{2})$ et $n-4 \geq 3$.

(ii) Pour tout entier i compris entre 1 et n, $\overline{a_i} \in \{\bar{3}, \bar{4}\}$ et il existe un entier i dans $[\![1; n]\!]$ tel que $\overline{a_i} = \bar{3}$.

S'il existe un entier i dans $[\![1; n]\!]$ tel que $\overline{a_i} = \bar{3}$ et $\overline{a_{i-1}} = \bar{4}$ ou $\overline{a_{i+1}} = \bar{4}$. Dans ce cas, la solution est réductible. En effet, si $\overline{a_{i+1}} = \bar{4}$ alors

$$(\overline{a_{i+2}}, \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_{i-1}}, \overline{a_i}, \overline{a_{i+1}}) = (\overline{a_{i+2} - 3}, \dots, \overline{a_n}, \overline{a_1}, \dots, \overline{a_{i-1} - 2}) \oplus (\bar{2}, \bar{3}, \bar{4}, \bar{3}).$$

On procède de façon analogue si $\overline{a_{i-1}} = \bar{4}$.

Sinon tous les $\overline{a_i}$ sont égaux à $\bar{3}$. Comme $M_5(\bar{3}, \bar{3}, \bar{3}, \bar{3}, \bar{3}) = \begin{pmatrix} \bar{0} & \bar{-1} \\ \bar{1} & \bar{3} \end{pmatrix} \neq \pm \mathrm{Id}$, on a $n \geq 6$. Si $n = 6$ alors la solution est irréductible. Si $n \geq 7$ alors la solution est réductible puisqu'on peut l'écrire comme la somme du $(n-4)$-uplet $(\bar{0}, \bar{3}, \dots, \bar{3}, \bar{0})$ avec $(\bar{3}, \bar{3}, \bar{3}, \bar{3}, \bar{3}, \bar{3})$ et $n - 4 \geq 3$.

(iii) Pour tout entier i compris entre 1 et n, $\overline{a_i} = \bar{4}$. On a $n \geq 6$ car sinon $(\overline{-a_1}, \dots, \overline{-a_n})$ est un 5-uplet solution ne contenant que des $\bar{2}$ ce qui est impossible (lemme 3.30). Si $n = 6$ alors la solution est irréductible (corollaire 3.31). Si $n \geq 7$ alors la solution est réductible puisqu'on peut l'écrire comme la somme du $(n-4)$-uplet $(\bar{0}, \bar{4}, \dots, \bar{4}, \bar{0})$ avec $(\bar{4}, \bar{4}, \bar{4}, \bar{4}, \bar{4}, \bar{4})$ et $n - 4 \geq 3$. □

Remarque 4.19. Le cas $N = 6$ montre en particulier qu'il peut exister un entier n tel que (E_N) ne possède pas de solution irréductible de taille n mais en possède de taille strictement supérieure à n.

4.6. **Cas** $N = 7$

Théorème 4.20. *Les solutions irréductibles de* (E_7) *sont (à permutations cycliques prés) :*

- $n = 3$ *:* $(\bar{1}, \bar{1}, \bar{1})$ *et* $(\overline{-1}, \overline{-1}, \overline{-1})$
- $n = 4$ *:*
  $(\bar{3}, \bar{3}, \bar{3}, \bar{3})$, $(\bar{4}, \bar{4}, \bar{4}, \bar{4})$,
  $(\bar{5}, \bar{0}, \bar{2}, \bar{0})$,
  $(\bar{4}, \bar{0}, \bar{3}, \bar{0})$,
  $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$,
- $n = 5$ *:* $(\bar{2}, \bar{2}, \bar{5}, \bar{4}, \bar{5})$, $(\bar{5}, \bar{5}, \bar{2}, \bar{3}, \bar{2})$

- $n = 6$
  $(\bar{2},\bar{2},\bar{2},\bar{4},\bar{3},\bar{4})$, $(\bar{5},\bar{5},\bar{5},\bar{3},\bar{4},\bar{3})$,
  $(\bar{2},\bar{3},\bar{4},\bar{5},\bar{4},\bar{3})$,
  $(\bar{2},\bar{3},\bar{5},\bar{2},\bar{5},\bar{3})$, $(\bar{5},\bar{4},\bar{2},\bar{5},\bar{2},\bar{4})$,
  $(\bar{2},\bar{3},\bar{5},\bar{3},\bar{2},\bar{4})$, $(\bar{5},\bar{4},\bar{2},\bar{4},\bar{5},\bar{3})$,
  $(\bar{2},\bar{4},\bar{2},\bar{4},\bar{2},\bar{4})$, $(\bar{5},\bar{3},\bar{5},\bar{3},\bar{5},\bar{3})$,
  $(\bar{2},\bar{5},\bar{2},\bar{5},\bar{2},\bar{5})$

- $n = 7$:
  $(\bar{2},\bar{2},\bar{2},\bar{2},\bar{2},\bar{2},\bar{2})$, $(\bar{5},\bar{5},\bar{5},\bar{5},\bar{5},\bar{5},\bar{5})$,
  $(\bar{2},\bar{2},\bar{2},\bar{3},\bar{5},\bar{5},\bar{3})$, $(\bar{5},\bar{5},\bar{5},\bar{4},\bar{2},\bar{2},\bar{4})$,
  $(\bar{2},\bar{2},\bar{3},\bar{4},\bar{2},\bar{4},\bar{3})$, $(\bar{5},\bar{5},\bar{4},\bar{3},\bar{5},\bar{3},\bar{4})$

- $n = 8$:
  $(\bar{2},\bar{2},\bar{3},\bar{4},\bar{3},\bar{2},\bar{2},\bar{4})$, $(\bar{5},\bar{5},\bar{4},\bar{3},\bar{4},\bar{5},\bar{5},\bar{3})$,
  $(\bar{2},\bar{3},\bar{4},\bar{3},\bar{4},\bar{5},\bar{3},\bar{4})$, $(\bar{5},\bar{4},\bar{3},\bar{4},\bar{3},\bar{2},\bar{4},\bar{3})$,
  $(\bar{2},\bar{4},\bar{3},\bar{5},\bar{2},\bar{4},\bar{3},\bar{5})$, $(\bar{5},\bar{3},\bar{4},\bar{2},\bar{5},\bar{3},\bar{4},\bar{2})$,
  $(\bar{3},\bar{4},\bar{3},\bar{4},\bar{3},\bar{4},\bar{3},\bar{4})$

- $n = 9$:
  $(\bar{2},\bar{2},\bar{2},\bar{2},\bar{3},\bar{4},\bar{3},\bar{4},\bar{3})$, $(\bar{5},\bar{5},\bar{5},\bar{5},\bar{4},\bar{3},\bar{4},\bar{3},\bar{4})$,
  $(\bar{2},\bar{2},\bar{3},\bar{5},\bar{4},\bar{3},\bar{4},\bar{5},\bar{3})$, $(\bar{5},\bar{5},\bar{4},\bar{2},\bar{3},\bar{4},\bar{3},\bar{2},\bar{4})$,
  $(\bar{2},\bar{2},\bar{3},\bar{5},\bar{4},\bar{3},\bar{5},\bar{2},\bar{4})$, $(\bar{5},\bar{5},\bar{4},\bar{2},\bar{3},\bar{4},\bar{2},\bar{5},\bar{3})$,
  $(\bar{2},\bar{2},\bar{4},\bar{2},\bar{2},\bar{4},\bar{2},\bar{2},\bar{4})$, $(\bar{5},\bar{5},\bar{3},\bar{5},\bar{5},\bar{3},\bar{5},\bar{5},\bar{3})$,
  $(\bar{2},\bar{2},\bar{4},\bar{2},\bar{5},\bar{3},\bar{4},\bar{5},\bar{3})$, $(\bar{5},\bar{5},\bar{3},\bar{5},\bar{2},\bar{4},\bar{3},\bar{2},\bar{4})$,
  $(\bar{2},\bar{2},\bar{4},\bar{2},\bar{5},\bar{3},\bar{5},\bar{2},\bar{4})$, $(\bar{5},\bar{5},\bar{3},\bar{5},\bar{2},\bar{4},\bar{2},\bar{5},\bar{3})$,
  $(\bar{2},\bar{3},\bar{4},\bar{2},\bar{3},\bar{4},\bar{2},\bar{3},\bar{4})$, $(\bar{5},\bar{4},\bar{3},\bar{5},\bar{4},\bar{3},\bar{5},\bar{4},\bar{3})$,
  $(\bar{2},\bar{4},\bar{3},\bar{2},\bar{4},\bar{3},\bar{2},\bar{4},\bar{3})$, $(\bar{5},\bar{3},\bar{4},\bar{5},\bar{3},\bar{4},\bar{5},\bar{3},\bar{4})$.

Démonstration. On commence par vérifier que la liste précédente ne contient que des solutions irréductibles. Les propositions 3.1 à 3.5 et la proposition 3.10 montrent que les éléments donnés dans le théorème sont bien les solutions irréductibles de (E_7) pour $n \leq 4$. On vérifie par un calcul direct que les éléments donnés dans le théorème sont bien des solutions de (E_7) puis on établit informatiquement la liste de toutes les solutions de (E_7) pour $n \leq 9$. À partir de celles-ci, on vérifie que les solutions présentes dans le théorème ne peuvent pas s'obtenir comme une somme de deux solutions de taille supérieure à 3. La liste du théorème ne contient donc que des solutions irréductibles.

Montrons que les solutions du théorème sont les seules solutions irréductibles de (E_7). Soit $(\overline{a_1}, \ldots, \overline{a_n})$ une solution de (E_7) avec $n \geq 9$. Si un des $\overline{a_i}$ est égal à $\bar{0}$, $\bar{1}$ ou $\overline{-1}$ alors

$(\overline{a_1}, \ldots, \overline{a_n})$ est réductible et on suppose donc que cela n'est pas le cas. On peut obtenir la liste de toutes les possibilités pour $(\overline{a_2}, \ldots, \overline{a_8})$ en établissant informatiquement la liste des 7-uplets d'éléments compris dans $\{\overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Dans cette liste, on élimine toutes les possibilités permettant d'écrire $(\overline{a_1}, \ldots, \overline{a_n})$ comme étant équivalent à la somme d'une solution avec une des solutions irréductibles de la liste ci-dessus. Une fois tout ces éléments retirés il reste :

$$(\overline{2}, \overline{3}, \overline{5}, \overline{4}, \overline{3}, \overline{5}, \overline{4}), (\overline{2}, \overline{3}, \overline{5}, \overline{5}, \overline{4}, \overline{2}, \overline{3}), (\overline{2}, \overline{5}, \overline{3}, \overline{4}, \overline{5}, \overline{3}, \overline{4}), (\overline{2}, \overline{5}, \overline{3}, \overline{5}, \overline{2}, \overline{4}, \overline{3}),$$
$$(\overline{3}, \overline{4}, \overline{2}, \overline{3}, \overline{4}, \overline{2}, \overline{5}), (\overline{3}, \overline{4}, \overline{2}, \overline{5}, \overline{3}, \overline{5}, \overline{2}), (\overline{3}, \overline{2}, \overline{4}, \overline{3}, \overline{2}, \overline{4}, \overline{5}), (\overline{3}, \overline{2}, \overline{4}, \overline{5}, \overline{5}, \overline{3}, \overline{2}),$$
$$(\overline{3}, \overline{2}, \overline{2}, \overline{4}, \overline{2}, \overline{2}, \overline{4}), (\overline{4}, \overline{3}, \overline{5}, \overline{4}, \overline{3}, \overline{5}, \overline{2}), (\overline{4}, \overline{3}, \overline{5}, \overline{2}, \overline{4}, \overline{2}, \overline{5}), (\overline{4}, \overline{5}, \overline{3}, \overline{4}, \overline{5}, \overline{3}, \overline{2}),$$
$$(\overline{4}, \overline{5}, \overline{3}, \overline{2}, \overline{2}, \overline{4}, \overline{5}), (\overline{5}, \overline{4}, \overline{2}, \overline{3}, \overline{4}, \overline{2}, \overline{3}), (\overline{5}, \overline{4}, \overline{2}, \overline{2}, \overline{3}, \overline{5}, \overline{4}), (\overline{5}, \overline{3}, \overline{2}, \overline{2}, \overline{4}, \overline{2}, \overline{2}),$$
$$(\overline{5}, \overline{2}, \overline{4}, \overline{3}, \overline{2}, \overline{4}, \overline{3}), (\overline{5}, \overline{2}, \overline{4}, \overline{2}, \overline{5}, \overline{3}, \overline{4}).$$

Pour chacun de ces 7-uplets on peut considérer les 4 possibilités pour le 7-uplet $(\overline{a_1}, \ldots, \overline{a_7})$ (ou le 7-uplet $(\overline{a_3}, \overline{a_1}, \ldots, \overline{a_9})$). Chacune de ces possibilités contient un k-uplet permettant d'écrire $(\overline{a_1}, \ldots, \overline{a_n})$ comme étant équivalent à une somme d'une solution avec une des solutions irréductibles de la liste ci-dessus.

Donc, $(\overline{a_1}, \ldots, \overline{a_n})$ est équivalent à la somme d'un k-uplet avec un l-uplet avec $3 \leq l \leq 9$. En particulier, si $n \geq 10$ alors $k \geq 3$ et $(\overline{a_1}, \ldots, \overline{a_n})$ est réductible. Donc, les solutions irréductibles de (E_7) sont celles données dans la liste ci-dessus. □

5. **Quelques conjectures et problèmes ouverts**

Tous les cas traités dans la section précédente nous amènent aux deux conjectures suivantes :

Conjecture 5.1. *Soit $N \in \mathbb{N}^*$, $N \geq 2$. (E_N) possède un nombre fini de solutions irréductibles.*

Conjecture 5.2. *Il existe un entier strictement positif K tel que pour tout entier N supérieur à 2 les solutions irréductibles de (E_N) sont de taille inférieure à $N + K$.*

Comme $\forall\ n \in \mathbb{N}^*$, (E_N) a un nombre fini de solutions de taille n, la conjecture 2 implique la conjecture 1.

Les solutions monomiales minimales sont des solutions particulièrement intéressantes de (E_N). On sait que si N est premier alors elles sont de taille inférieure ou égale à N. Il serait intéressant d'avoir plus d'informations sur leur taille dans les cas N premier et N non premier. Ceci nous amène à formuler le problème suivant :

Problème 1. *Étudier les tailles des solutions monomiales minimales de* (E_N) *dans le cas* N *premier et dans le cas général.*

En particulier, dans le cas où $N = l^n$, avec $l \geq 2$, on a une solution monomiale donnée dans la proposition 3.20. Il serait intéressant d'avoir plus d'informations sur ces solutions.

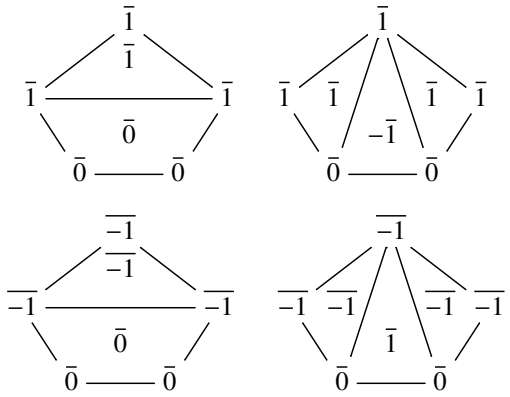
Problème 2. *Les solutions données dans la proposition 3.20 sont-elles monomiales minimales ? Si oui, sont-elles irréductibles ?*

Un autre problème ouvert est la généralisation des propositions 4.12 et 4.18. Pour cela on définit la notion de solution compatible avec une triangulation. Une solution de (E_N) de taille n est dite compatible avec une triangulation s'il existe un découpage d'un polygone convexe à n sommets n'utilisant que des triangles de poids $\overline{1}$ ou $\overline{-1}$ dont elle est la quiddité. Le problème se formule alors de la façon suivante :

Problème 3. *Soit* $N \geq 2$*. Caractériser les solutions de* (E_N) *compatibles avec une triangulation.*

On peut remarquer que l'on peut généraliser l'argument de la proposition 4.12 de la façon suivante. Soit $(\overline{a_1}, \ldots, \overline{a_n})$ une solution de (E_N) telle que celle-ci est la quiddité d'un découpage d'un polygone convexe à n sommets n'utilisant que des triangles de poids $\overline{1}$ ou $\overline{-1}$ et des quadrilatères de poids $\overline{0}$. Si $(\overline{a_1}, \ldots, \overline{a_n}) \neq (\overline{0}, \ldots, \overline{0})$ alors elle est la quiddité d'un découpage d'un polygone convexe à n sommets n'utilisant que des triangles de poids $\overline{1}$ ou $\overline{-1}$.

En effet, si la décomposition contient un quadrilatère alors elle contient nécessairement un triangle qui partage un côté avec un quadrilatère (sinon celle-ci ne contiendrait que des quadrilatères et aurait donc pour quiddité $(\overline{0}, \ldots, \overline{0})$). On procède alors à la transformation ci-dessous (suivant le poids du triangle) :



On recommence ce procédé tant qu'il reste des quadrilatères.

Remerciements

Je remercie Valentin Ovsienko et Michael Cuntz pour leurs suggestions et leurs conseils avisés.

Références

[1] Michel Alessandri. *Agrégation de mathématiques. Thèmes de géométrie. Groupes en situation géométrique*. Agrégation de mathématiques. Dunod, 1999.

[2] John H. Conway and Harold S. M. Coxeter. Triangulated polygons and frieze patterns. *Math. Gaz.*, 57(400) :87–94 et 175–183, 1973.

[3] Harold S. M. Coxeter. Frieze patterns. *Acta Arith.*, 18(1) :297–310, 1971.

[4] Michael Cuntz. A combinatorial model for tame frieze patterns. *Münster J. Math.*, 12(1) :49–56, 2019.

[5] Michael Cuntz and Thorsten Holm. Frieze patterns over integers and other subsets of the complex numbers. *J. Comb. Algebra.*, 3(2) :153–188, 2019.

[6] Claire-Soizic Henry. Coxeter friezes and triangulations of polygons. *Am. Math. Mon.*, 120(6) :553–558, 2013.

[7] William M. Kantor and Ákos Seress. Large element orders and the characteristic of Lie-typesimple groups. *J. Algebra*, 322(3) :802–832, 2009.

[8] Flavien Mabilat. Combinatorial description of the principal congruence subgroup $\gamma(2)$ in $SL(2, Z)$. `https://arxiv.org/abs/1911.06717`, à paraître dans *Commun. Math.*, 2020.

[9] Flavien Mabilat. Quelques éléments de combinatoire des matrices de $SL(2, Z)$. *Bull. Sci. Math.*, 167 : article no. 102958 (18 pages), 2021.

[10] Sophie Morier-Genoud. Coxeter's frieze patterns at the crossroads of algebra, geometry and combinatorics. *Bull. Lond. Math. Soc.*, 47(6) :895–938, 2015.

[11] Sophie Morier-Genoud. Counting Coxeter's friezes over a finite field via moduli spaces. *Algebr. Comb.*, 4(2) :225–240, 2021.

[12] Sophie Morier-Genoud and Valentin Ovsienko. Farey Boat : Continued fractions and triangulations, modular group and polygon dissections. *Jahresber. Dtsch. Math.-Ver.*, 121(2) :91–136, 2019.

[13] Valentin Ovsienko. Partitions of unity in $SL(2, Z)$, negative continued fractions, and dissections of polygons. *Res. Math. Sci.*, 5(2) : article no. 21 (25 pages), 2018.

[14] Moritz Weber and Mang Zhao. Factorization of frieze patterns. *Rev. Unión Mat. Argent.*, 60(2) :407–415, 2019.

Flavien Mabilat
Laboratoire de Mathématiques U.F.R. Sciences
Exactes et Naturelles Moulin de la Housse - BP 1039
51687 Reims cedex 2, France
flavien.mabilat@univ-reims.fr