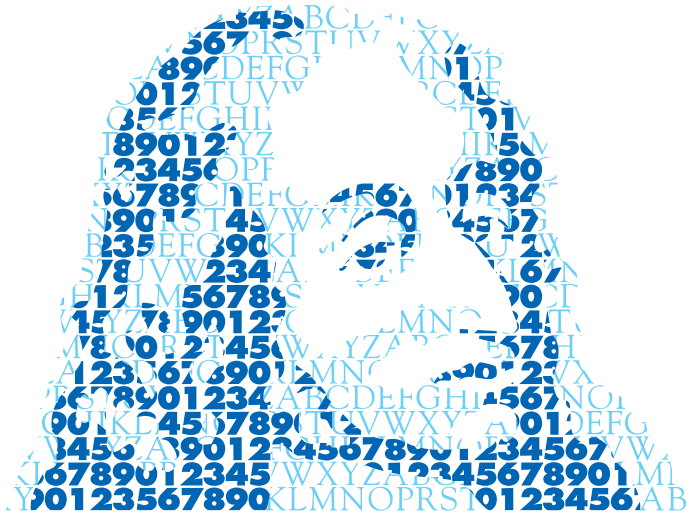
ANNALES MATHÉMATIQUES



BLAISE PASCAL

Flavien Mabilat

Combinatoire des sous-groupes de congruence du groupe modulaire II

Volume 28, n° 2 (2021), p. 199-229.

<http://ambp.centre-mersenne.org/item?id=AMBP_2021__28_2_199_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**, 199-229 (2021)

Combinatoire des sous-groupes de congruence du groupe modulaire II

Flavien Mabilat

Résumé

Dans cet article, on souhaite étudier la combinatoire des sous-groupes de congruence du groupe modulaire. Pour cela, on considère une équation matricielle liée à celle qui apparaît lors de l'étude des frises de Coxeter et on étudie ces solutions irréductibles. En particulier, on donne de nouvelles propriétés des solutions monomiales minimales. De plus, on introduit la notion de solutions dynomiales minimales et on donne des conditions suffisantes d'irréductibilité pour celles-ci.

Combinatorics of congruence subgroups of the modular group II

Abstract

In this paper, we study combinatorics of congruence subgroups of the modular group. More precisely, we consider the matrix equation that naturally arises in the theory of Coxeter friezes and investigate its irreducible solutions. We give new properties for minimal monomial solutions. Furthermore, we introduce the notion of minimal dynomial solutions and study their irreducibility.

« *Il est très difficile d'imaginer quelque chose de simple* »
Pierre MacOrlan, *Villes*

1. Introduction

L'une des propriétés les plus intéressantes 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'existence de parties génératrices à deux éléments. On peut, en particulier, prendre les deux matrices suivantes (voir par exemple [1]) :

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

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

À partir de ce choix, on peut montrer que pour toute matrice A de $\mathrm{SL}_2(\mathbb{Z})$ il existe un entier strictement positif n et des entiers strictement positifs $a_1, \dots, a_n$ tels que

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

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

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

Notons que dans la suite les a_i ne sont pas nécessairement des entiers (on considérera plutôt des éléments appartenant à des anneaux $\mathbb{Z}/N\mathbb{Z}$).

Ces matrices interviennent également dans la théorie des frises de Coxeter (voir par exemple [6, 8] pour la définition des frises de Coxeter). En effet, les solutions de l'équation $M_n(a_1, \dots, a_n) = -\mathrm{Id}$ permettent de construire des frises de Coxeter, et, à partir d'une telle frise, on peut obtenir une solution de cette équation (voir [2] et [8, proposition 2.4]). Les frises de Coxeter possèdent par ailleurs des connections avec de nombreux autres domaines mathématiques (voir par exemple [14]).

Ceci amène naturellement à l'étude de l'équation généralisée suivante :

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

V. Ovsienko (voir [17, théorèmes 1 et 2]) a résolu celle-ci sur $\mathbb{N}^*$ et donné une description combinatoire des solutions en terme de découpages de polygones (généralisant par ailleurs un théorème antérieur dû à Conway et Coxeter, voir [5, 6]). On dispose également des solutions de cette équation sur $\mathbb{N}$ (voir [7, théorème 3.1]), sur $\mathbb{Z}$ (voir [7, théorème 3.2]) et sur $\mathbb{Z}[\alpha]$ avec α un nombre complexe transcendant (voir [13, théorème 2.7]). On peut aussi étudier l'équation (1.1) en remplaçant $\pm\mathrm{Id}$ par $\pm M$ avec M une matrice du groupe modulaire, notamment pour $M = S$ et $M = T$ (voir [12]).

On va s'intéresser ici aux cas des anneaux $\mathbb{Z}/N\mathbb{Z}$, c'est-à-dire à la résolution sur $\mathbb{Z}/N\mathbb{Z}$ de l'équation :

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

On dira, en particulier, qu'une solution de (E_N) est de taille n si cette solution est un n-uplet d'éléments de $\mathbb{Z}/N\mathbb{Z}$. L'étude de l'équation ci-dessus permet notamment de chercher toutes les écritures des éléments des sous-groupes de congruence ci-dessous :

$$\widehat{\Gamma}(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A = \pm \mathrm{Id}\ [N]\}$$

sous la forme $M_n(a_1, \dots, a_n)$ avec les a_i des entiers strictement positifs.

L'équation (E_N) a déjà été étudiée dans des travaux précédents (voir [10, 11]). Pour mener à bien cette étude on avait utilisé une notion de solutions irréductibles à partir de

laquelle on peut construire l'ensemble des solutions (voir section suivante). Ceci nous avait permis de résoudre complètement (E_N) pour $N \leq 6$ (voir [11, section 4]). On avait également obtenu des résultats généraux d'irréductibilité en définissant notamment la notion de solutions monomiales minimales (voir [11, section 3.3 et section 4]). D'autres éléments pouvant être reliés aux cas des anneaux $\mathbb{Z}/N\mathbb{Z}$, avec N premier, peuvent également être trouvés dans [15].

L'objectif ici est de poursuivre cette étude en obtenant des résultats sur la taille et l'irréductibilité des solutions monomiales minimales (voir section 3) et d'obtenir des résultats d'irréductibilité pour d'autres solutions (voir section 4).

Remerciements

Je remercie Valentin Ovsienko pour son aide précieuse.

2. Définitions et résultats principaux

L'objectif de cette section est de rappeler les définitions introduites notamment dans [7] et [11] utiles à l'étude de l'équation (E_N) et d'énoncer les résultats principaux de ce texte. 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 ([18, 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 ci-dessous :

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

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 sommes pour $N > 7$:

- $(\bar{1}, \bar{2}, \bar{3}) \oplus (\bar{4}, \bar{1}, \bar{3}, \bar{2}) = (\bar{3}, \bar{2}, \bar{7}, \bar{1}, \bar{3})$;
- $(\bar{4}, \bar{0}, \bar{1}, \bar{2}) \oplus (\overline{-1}, \bar{0}, \bar{1}) = (\bar{5}, \bar{0}, \bar{1}, \bar{1}, \bar{0})$;
- $n \geq 2$, $(\overline{a_1}, \dots, \overline{a_n}) \oplus (\bar{0}, \bar{0}) = (\bar{0}, \bar{0}) \oplus (\overline{a_1}, \dots, \overline{a_n}) = (\overline{a_1}, \dots, \overline{a_n})$.

En particulier, si $(\overline{b_1}, \dots, \overline{b_m})$ est une solution de (E_N) et $(\overline{a_1}, \dots, \overline{a_n})$ un n-uplet d'éléments de $\mathbb{Z}/N\mathbb{Z}$ 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) (voir [7, 18] et [11, proposition 3.9]). En revanche, l'opération $\oplus$ n'est ni commutative ni associative (voir [18, exemple 2.1]).

Définition 2.3 ([18, définition 1.5])**.** Soient $(\overline{a_1}, \dots, \overline{a_n})$ et $(\overline{b_1}, \dots, \overline{b_n})$ deux n-uplets d'éléments de $\mathbb{Z}/N\mathbb{Z}$. 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 montre facilement que $\sim$ est une relation d'équivalence sur les n-uplets d'éléments de $\mathbb{Z}/N\mathbb{Z}$ (voir [18, lemme 1.7]). De plus, 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) (voir [7, proposition 2.6]).

Définition 2.4 ([7, 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 une solution de (E_N) $(\overline{b_1}, \dots, \overline{b_l})$ et un m-uplet $(\overline{a_1}, \dots, \overline{a_m})$ d'éléments de $\mathbb{Z}/N\mathbb{Z}$ tels 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 2.5. On ne considère pas $(\bar{0}, \bar{0})$ comme étant une solution irréductible de (E_N).

L'un de nos objectifs principaux est de trouver des solutions irréductibles de l'équation (E_N). En particulier, on a introduit dans [11] la notion de solutions monomiales rappelée ci-dessous :

Définition 2.6.

(i) 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).

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

(iii) 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.

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

Si $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$ alors la solution $\overline{k}$-monomiale minimale de (E_N) existe toujours (puisque $M_1(\overline{k})$ est d'ordre fini dans $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$). On connaît déjà un certain nombre de propriétés d'irréductibilité pour ces solutions. Celles-ci seront évoquées dans la section suivante où on démontrera également le résultat ci-dessous :

Théorème 2.7. *Soit N un entier pair supérieur à 4. On a deux cas :*

(i) *Si $4 \mid N$ alors la solution $\overline{\frac{N}{2}}$-monomiale minimale de (E_N) est de taille 4 ;*

(ii) *Si $4 \nmid N$ alors la solution $\overline{\frac{N}{2}}$-monomiale minimale de (E_N) est de taille 6.*

De plus, celle-ci est irréductible dans les deux cas.

Pour obtenir de nouveaux résultats d'irréductibilité on définit une nouvelle classe de solutions de (E_N).

Définition 2.8.

(i) Soient $n \in \mathbb{N}^*$ pair et $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$. On appelle solution $(n, \overline{k})$-dynomiale une solution de taille n de (E_N) de la forme $(\overline{k}, \overline{-k}, \ldots, \overline{k}, \overline{-k})$.

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

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

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

Remarque 2.9. Les propriétés suivantes des solutions dynomiales sont immédiates :

- La solution $\overline{k}$-dynomiale minimale de (E_N) existe toujours.
- Une solution dynomiale est toujours de taille paire.
- Une solution $(n, \overline{k})$-dynomiale est équivalente à une solution $(n, \overline{-k})$-dynomiale.
- Si $\overline{2k} = \overline{0}$ alors une solution $(n, \overline{k})$-dynomiale est une solution $(n, \overline{k})$-monomiale.

On dispose pour cette classe de solutions du résultat d'irréductibilité suivant démontré dans la section 4 :

Théorème 2.10. *Soient N un nombre premier supérieur à 5 et $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$. On suppose que les deux conditions suivantes sont vérifiées :*

- $\overline{k} \neq \overline{0}$;

- $\overline{k}^2 + \overline{8}$ *n'est pas un carré dans* $\mathbb{Z}/N\mathbb{Z}$.

La solution $\overline{k}$*-dynomiale minimale de* (E_N) *est irréductible.*

Ce théorème permet d'obtenir plusieurs résultats d'irréductibilité intéressants exposés dans la section 4.3. On montre notamment dans celle-ci que la solution $\overline{2}$-dynomiale minimale de (E_N) est irréductible lorsque N est un nombre premier supérieur à 5 vérifiant $N \not\equiv \pm 1$ [12].

3. **Propriétés des solutions monomiales minimales**

Comme nous venons de l'évoquer, les solutions monomiales minimales possèdent un certain nombre de propriétés intéressantes (voir [11, section 3.3]). On dispose notamment des deux résultats d'irréductibilité énoncés ci-dessous :

Théorème 3.1. *Soit N un entier naturel supérieur à 2.*

(i) ([11, théorème 3.23]) *Si N est premier alors les solutions monomiales minimales de* (E_N) *différentes de* $(\overline{0}, \overline{0})$ *sont irréductibles.*

(ii) ([11, théorème 2.9]) *Si* $N \geq 3$, $(\overline{2}, \ldots, \overline{2}) \in (\mathbb{Z}/N\mathbb{Z})^N$ *est une solution monomiale minimale irréductible de* (E_N).

L'objectif de cette section est d'approfondir l'étude de ces solutions en obtenant notamment des éléments sur leur taille et de nouveaux résultats d'irréductibilité. Dans cette partie, N est un entier naturel supérieur ou égal à 2.

3.1. **Taille des solutions monomiales minimales**

L'un des problèmes soulevés lors de l'étude de ces solutions (voir [11, problème 1]) était d'avoir des informations sur la taille des solutions monomiales minimales. Notre objectif ici est de fournir des éléments de réponse à ce problème.

Par le théorème 3.1, on sait que la solution $\overline{2}$-monomiale minimale de (E_N) est de taille N. L'étude des solutions de (E_N) pour les petites valeurs de n permet également de répondre précisément à notre question pour certaines valeurs de $\overline{k}$.

Proposition 3.2 ([11, section 3.1])**.**

(i) *L'équation* (E_N) *n'a pas de solution de taille 1.*

(ii) $(\overline{0}, \overline{0})$ *est l'unique solution de* (E_N) *de taille 2.*

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

(iv) *Les solutions de* (E_N) *de taille 4 sont de la forme* $(\overline{-a}, \bar{b}, \bar{a}, \overline{-b})$ *avec* $\overline{ab} = \bar{0}$ *et* $(\bar{a}, \bar{b}, \bar{a}, \bar{b})$ *avec* $\overline{ab} = \bar{2}$.

On en déduit que la solution $\bar{0}$-monomiale minimale est de taille 2 et que les solutions $\pm\bar{1}$-monomiales minimales sont de taille 3.

De plus, pour tout $\bar{k} \in \mathbb{Z}/N\mathbb{Z}$, la solution $\bar{k}$-monomiale minimale et la solution $\overline{-k}$-monomiale minimale ont la même taille. Un simple calcul permet de montrer que la solution $\bar{3}$-monomiale minimale de (E_6) est de taille 6 et que la solution $\bar{3}$-monomiale minimale de (E_7) est de taille 4. Tout ceci nous permet de connaître précisément les tailles des solutions monomiales minimales pour $N \in \{2, 3, 4, 5, 6, 7\}$.

Pour le cas général on dispose du théorème ci-dessous qui donne une majoration de la taille :

Théorème 3.3 ([3, p. 216])**.** *Soit N un entier naturel supérieur à 2. L'ordre des éléments de* $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ *est inférieur à* $3N$.

Dans le cas où N est premier, on peut avoir des informations plus précises sur la taille des solutions monomiales minimales. La preuve qui suit est une adaptation à notre situation de la preuve du cas N premier du théorème précédent fournie dans [3].

Proposition 3.4. *Soient N un nombre premier et* $\bar{k} \in \mathbb{Z}/N\mathbb{Z}$*. On a deux cas :*

- *si* $\bar{k} = \pm\bar{2}$ *alors la solution* $\bar{k}$*-monomiale minimale est de taille N ;*
- *si* $\bar{k} \neq \pm\bar{2}$ *alors la taille de la solution* $\bar{k}$*-monomiale minimale divise* $\frac{N-1}{2}$ *ou* $\frac{N+1}{2}$.

Démonstration. On montre, par récurrence, que pour tout n dans $\mathbb{N}^*$ on a

$$M_n(2, \ldots, 2) = \begin{pmatrix} n+1 & -n \\ n & -n+1 \end{pmatrix}.$$

Donc, $M_N(\bar{2}, \ldots, \bar{2}) = \left(\begin{smallmatrix} \overline{N+1} & \overline{-N} \\ \overline{N} & \overline{-N+1} \end{smallmatrix}\right) = \mathrm{Id}$ ce qui implique que la taille de la solution $\bar{2}$-monomiale minimale de (E_N) divise N. De plus, (E_N) n'a pas de solution de taille 1 et N est premier. Donc, la taille de la solution $\bar{2}$-monomiale minimale de (E_N) est égale à N. Celle de la solution $\overline{-2}$-monomiale minimale de (E_N) est par conséquent aussi égale à N.

On suppose maintenant $\bar{k} \neq \pm\bar{2}$. Le polynôme caractéristique de $M_1(\bar{k})$ est

$$\chi(X) = X^2 - \bar{k}X + \bar{1}.$$

Ce polynôme a pour discriminant $\Delta = \bar{k}^2 - \bar{4} = (\bar{k} - \bar{2})(\bar{k} + \bar{2}) \neq \bar{0}$ (car $\mathbb{Z}/N\mathbb{Z}$ est intègre). On a donc deux cas :

Cas 1 : Δ est un carré dans $\mathbb{Z}/N\mathbb{Z}$. Dans ce cas, $M_1(\bar{k})$ a deux valeurs propres distinctes et donc est diagonalisable dans $\mathbb{Z}/N\mathbb{Z}$. Notons $\bar{a}$ et $\bar{b}$ ses valeurs propres. Il existe $P \in GL_2(\mathbb{Z}/N\mathbb{Z})$ tel que

$$M_1(\bar{k}) = P \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{b} \end{pmatrix} P^{-1}.$$

De plus, $\mathbb{Z}/N\mathbb{Z} - \{\bar{0}\}$ est un groupe de cardinal $N-1$. Ainsi, $\bar{a}^{N-1} = \bar{1}$ ($\bar{a} \neq \bar{0}$ puisque $\overline{ab} = \bar{1}$). Donc, $(\bar{a}^{\frac{N-1}{2}} - \bar{1})(\bar{a}^{\frac{N-1}{2}} + \bar{1}) = \bar{0}$. On en déduit que $\bar{a}^{\frac{N-1}{2}} = \pm\bar{1}$ (puisque $\mathbb{Z}/N\mathbb{Z}$ est intègre). De même, $\bar{b}^{\frac{N-1}{2}} = \pm\bar{1}$. Or, $\overline{ab} = \bar{1}$ donc $\bar{a}^{\frac{N-1}{2}} = \bar{b}^{\frac{N-1}{2}} = \pm\bar{1}$. Il en découle

$$M_1(\bar{k})^{\frac{N-1}{2}} = P \begin{pmatrix} \bar{a}^{\frac{N-1}{2}} & \bar{0} \\ \bar{0} & \bar{b}^{\frac{N-1}{2}} \end{pmatrix} P^{-1} = \pm \mathrm{Id}\,.$$

Par conséquent, l'ordre de $M_1(\bar{k})$ dans $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, c'est-à-dire la taille de la solution $\bar{k}$-monomiale minimale de (E_N), divise $\frac{N-1}{2}$.

Cas 2 : Δ n'est pas un carré dans $\mathbb{Z}/N\mathbb{Z}$. Soit K un corps de décomposition de χ (voir [9, théorème V.18]). χ a deux racines distinctes dans K. Notons les x et y. On a

$$\begin{aligned}
(X - x^N)(X - y^N) &= X^2 - (x^N + y^N)X + x^N y^N \\
&= X^2 - (x+y)^N X + x^N y^N && \text{(morphisme de Frobenius)} \\
&= X^2 - (x+y)^N X + (xy)^N && \text{(commutativité de } K\text{)} \\
&= X^2 - \bar{k}^N X + \bar{1} && (x \text{ et } y \text{ racines de } \chi) \\
&= X^2 - \bar{k}X + \bar{1}.
\end{aligned}$$

Donc, x^N et y^N sont des racines de χ. De plus, $x^N \neq x$. En effet, supposons par l'absurde que $x^N = x$. Dans ce cas, $x^{N-1} = \bar{1}$ ($x \neq \bar{0}$ car $xy = \bar{1}$). Or, le polynôme $Q(X) = X^{N-1} - \bar{1}$ a au plus $N-1$ racines dans K et les éléments non nuls de $\mathbb{Z}/N\mathbb{Z}$ sont des racines. Donc, les seules racines de Q sont les éléments non nuls de $\mathbb{Z}/N\mathbb{Z}$. On a donc, $x \in \mathbb{Z}/N\mathbb{Z}$. Ceci est absurde puisque χ n'a pas de racine dans ce corps.

Ainsi, $x^N = y$ et donc $x^{N+1} = xy = \bar{1}$. En procédant comme dans le cas précédent, on obtient $\bar{x}^{\frac{N+1}{2}} = \bar{y}^{\frac{N+1}{2}} = \pm\bar{1}$ ce qui implique que la taille de la solution $\bar{k}$-monomiale minimale de (E_N) divise $\frac{N+1}{2}$. □

On donne en annexe (voir annexe A) les valeurs des tailles des solutions monomiales minimales pour les nombres premiers compris entre 11 et 47.

Remarque 3.5. Il existe des cas où la taille des solutions monomiales minimales est égale à $\frac{N-1}{2}$ ou $\frac{N+1}{2}$ (voir annexe A).

On peut également obtenir la taille précise de certaines solutions monomiales minimales lorsque N et $\overline{k}$ vérifient certaines propriétés (voir sous-partie suivante).

3.2. Solutions $\overline{\frac{N}{l}}$-monomiales minimales

3.2.1. Preuve du théorème 2.7

On suppose que N est un entier pair supérieur à 4.

(i). Si $4 \mid N$, alors $\overline{\frac{N}{2}}\,\overline{\frac{N}{2}} = \overline{\frac{N^2}{4}} = \overline{N\frac{N}{4}} = \overline{0}$ et donc $\left(\overline{-\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{-\frac{N}{2}}\right) = \left(\overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}\right)$ est solution de (E_N) (voir proposition 3.2). La taille de la solution $\overline{\frac{N}{2}}$-monomiale minimale divise 4 (puisque c'est l'ordre de $M_1\left(\overline{\frac{N}{2}}\right)$ dans le groupe $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$). L'équation (E_N) n'a pas de solution de taille 1. Comme $\overline{\frac{N}{2}} \neq \overline{0}$, $\left(\overline{\frac{N}{2}}, \overline{\frac{N}{2}}\right)$ n'est pas solution et donc la solution $\overline{\frac{N}{2}}$-monomiale minimale est de taille 4. Comme, $\overline{\frac{N}{2}} \neq \overline{\pm 1}$, la solution $\overline{\frac{N}{2}}$-monomiale minimale est irréductible. En effet, une solution réductible de taille 4 est la somme de deux solutions de taille 3 et donc contient forcément $\pm\overline{1}$.

(ii). Si $4 \nmid N$, on note $K = \frac{N}{2}$. En particulier, on a K impair et $\overline{2K} = \overline{0}$. On a

$$M_6(\overline{K}, \overline{K}, \overline{K}, \overline{K}, \overline{K}, \overline{K}) = \begin{pmatrix} \overline{K^6 - 5K^4 + 6K^2 - 1} & \overline{-K^5 + 4K^3 - 3K} \\ \overline{K^5 - 4K^3 + 3K} & \overline{-K^4 + 3K^2 - 1} \end{pmatrix}.$$

Or,

$$\begin{aligned} \overline{K^6 - 5K^4 + 6K^2} &= \overline{K^6 - K^4 - 4K^4 + 3 \times 2K^2} \\ &= \overline{K^6 - K^4} \\ &= \overline{K^4(K^2 - 1)}. \end{aligned}$$

De plus, K^2 est impair (produit de deux entiers impairs) donc $(K^2 - 1)$ est pair. Ainsi, il existe un entier j tel que $(K^2 - 1) = 2j$. Donc,

$$\overline{K^6 - 5K^4 + 6K^2} = \overline{2jK^4} = \overline{jK^3(2K)} = \overline{0}.$$

De même, on a

$$\begin{aligned} \overline{-K^5 + 4K^3 - 3K} &= \overline{-K^5 + 2K(2K^2) - K - 2K} \\ &= \overline{-K^5 - K} \\ &= \overline{-K(1 + K^4)}. \end{aligned}$$

Or, K^4 est impair (produit de quatre entiers impairs) donc $1 + K^4$ est pair. Il existe un entier j' tel que $1 + K^4 = 2j'$. Ainsi,

$$\overline{-K^5 + 4K^3 - 3K} = \overline{-K(1 + K^4)} = \overline{-j'N} = \bar{0}.$$

On procède de façon analogue pour $\overline{-K^4 + 3K^2}$. On a $\overline{-K^4 + 3K^2} = \overline{K^2(1 - K^2)}$. Or, K^2 est impair (produit de deux entiers impairs) donc $(1 - K^2)$ est pair. Il existe un entier j'' tel que $(1 - K^2) = 2j''$. Donc,

$$\overline{-K^4 + 3K^2} = \overline{K^2(1 - K^2)} = \overline{2j''K^2} = \overline{Nj''K} = \bar{0}.$$

Ainsi, $M_6\left(\overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}\right) = -\mathrm{Id}$. Il en découle que la taille de la solution $\overline{\frac{N}{2}}$-monomiale minimale divise 6 (puisque c'est l'ordre de $M_1\left(\overline{\frac{N}{2}}\right)$ dans le groupe $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$) c'est-à-dire que celle-ci est égale à 1, 2, 3 ou 6.

L'équation (E_N) n'a pas de solution de taille 1. $\overline{\frac{N}{2}} \neq \bar{0}$, donc, $\left(\overline{\frac{N}{2}}, \overline{\frac{N}{2}}\right)$ n'est pas solution. $\overline{\frac{N}{2}} \neq \overline{\pm 1}$, donc, $\left(\overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}\right)$ n'est pas solution. On en déduit que la solution $\overline{\frac{N}{2}}$-monomiale minimale de (E_N) est de taille 6.

Si celle-ci est réductible alors elle est la somme de deux solutions de taille 4 (puisqu'elle ne contient pas $\pm\bar{1}$). Dans ce cas, (E_N) a une solution de la forme $\left(\bar{a}, \overline{\frac{N}{2}}, \overline{\frac{N}{2}}, \bar{a}\right)$ avec $\bar{a} \neq \overline{\frac{N}{2}}$ (sinon la solution minimale serait de taille 4). Donc, on a $\overline{\frac{N^2}{4}} = \bar{0}$ et $\bar{a} = \overline{-\frac{N}{2}}$. Ainsi, Il existe un entier l tel que $K^2 = 2lK$. Donc, K^2 est pair ce qui implique K pair. Ce qui est absurde.

Donc, la solution $\overline{\frac{N}{2}}$-monomiale minimale est irréductible de taille 6. □

Remarque 3.6. Si $N = 2$, alors la solution $\overline{\frac{N}{2}}$-monomiale minimale est la solution $\bar{1}$-monomiale minimale qui est irréductible de taille 3.

3.2.2. **Généralisations partielles**

On cherche à généraliser le théorème 2.7 pour des diviseurs de N différents de 2. On commence par le résultat suivant :

Proposition 3.7. *Si $l^2 \mid N$ avec $l \geq 2$ alors $\left(\overline{\frac{N}{l}}, \ldots, \overline{\frac{N}{l}}\right) \in (\mathbb{Z}/N\mathbb{Z})^{2l}$ est solution de (E_N).*

Démonstration. On a

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

L'avant dernière égalité est valide car $\frac{N}{l^2}$ et $\frac{N^{k-2}}{l^{k-2}}$ sont des entiers puisque $l^2 \mid N$ et $l^{k-2} \mid N^{k-2}$. □

Remarque 3.8. Si $l = 1$ alors $\left(\overline{\frac{N}{l}},\dots,\overline{\frac{N}{l}}\right) = (\bar{0},\bar{0}) \in (\mathbb{Z}/N\mathbb{Z})^2$ est aussi solution de (E_N).

Le résultat ci-dessous résout la question de l'irréductibilité de ces solutions.

Proposition 3.9. *Soit $l^2 \mid N$ avec $l \geq 2$. $\left(\overline{\frac{N}{l}},\dots,\overline{\frac{N}{l}}\right) \in (\mathbb{Z}/N\mathbb{Z})^{2l}$ est une solution irréductible de (E_N) si et seulement si $l = 2$.*

Démonstration. Si $l = 2$ alors la solution est irréductible (voir théorème 2.7). Si $l \geq 3$ alors la solution n'est pas irréductible car $\left(\overline{-\frac{N}{l}}, \overline{\frac{N}{l}}, \overline{\frac{N}{l}}, \overline{-\frac{N}{l}}\right)$ est solution de (E_N) puisque

$\overline{\frac{N^2}{l^2}} = N\overline{\frac{N}{l^2}} = \bar{0}$ (voir proposition 3.2) et

$$\left(\overline{\frac{N}{l}}, \dots, \overline{\frac{N}{l}}\right) = \left(2\overline{\frac{N}{l}}, \overline{\frac{N}{l}}, \dots, \overline{\frac{N}{l}}, 2\overline{\frac{N}{l}}\right) \oplus \left(\overline{-\frac{N}{l}}, \overline{\frac{N}{l}}, \overline{\frac{N}{l}}, \overline{-\frac{N}{l}}\right).$$

$\left(2\overline{\frac{N}{l}}, \overline{\frac{N}{l}}, \dots, \overline{\frac{N}{l}}, 2\overline{\frac{N}{l}}\right)$ est de taille $2l - 2 \geq 4 > 3$. □

Remarque 3.10. Ces propositions généralisent les propriétés 3.15 et 3.16 de [11].

Avant de continuer, on a besoin des résultats suivants qui permettent d'obtenir une expression de $M_n(a_1, \dots, a_n)$:

On pose $K_{-1} = 0$, $K_0 = 1$ et on note pour $i \geq 1$

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

$K_i(a_1, \dots, a_i)$ est le continuant de $a_1, \dots, a_i$. On dispose de l'égalité suivante (voir [4, 16]) :

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

De plus, on dispose de l'expression classique ci-dessous :

Lemme 3.11. *Soit $n \geq 0$, $K_n(x, \dots, x) = \sum_{k=0}^{E[\frac{n}{2}]} (-1)^k \binom{n-k}{k} x^{n-2k}$.*

Démonstration. Cela se prouve par récurrence sur n. En effet, la formule est vraie pour $n = 0$ et pour $n = 1$. Supposons qu'il existe un entier positif n tel que la formule est vraie pour n et $n - 1$. On suppose n pair. En développant le déterminant définissant $K_{n+1}(x, \dots, x)$ suivant la première colonne, on obtient :

$$\begin{aligned} K_{n+1}(x, \dots, x) &= xK_n(x, \dots, x) - K_{n-1}(x, \dots, x) \\ &= \sum_{k=0}^{E[\frac{n}{2}]} (-1)^k \binom{n-k}{k} x^{n+1-2k} - \sum_{k=0}^{E[\frac{n-1}{2}]} (-1)^k \binom{n-1-k}{k} x^{n-1-2k} \\ &= \sum_{k=0}^{\frac{n}{2}} (-1)^k \binom{n-k}{k} x^{n+1-2k} - \sum_{k=0}^{\frac{n}{2}-1} (-1)^k \binom{n-1-k}{k} x^{n-1-2k} \quad (n \text{ est pair}) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=0}^{\frac{n}{2}} (-1)^k \binom{n-k}{k} x^{n+1-2k} - \sum_{l=1}^{\frac{n}{2}} (-1)^{l-1} \binom{n-l}{l-1} x^{n+1-2l} \\
&= \sum_{k=0}^{\frac{n}{2}} (-1)^k \binom{n-k}{k} x^{n+1-2k} + \sum_{l=1}^{\frac{n}{2}} (-1)^{l} \binom{n-l}{l-1} x^{n+1-2l} \\
&= x^{n+1} + \sum_{k=1}^{\frac{n}{2}} (-1)^k \left(\binom{n-k}{k} + \binom{n-k}{k-1} \right) x^{n+1-2k} \\
&= x^{n+1} + \sum_{k=1}^{\frac{n}{2}} (-1)^k \binom{n+1-k}{k} x^{n+1-2k} \quad \text{(triangle de Pascal)} \\
&= \sum_{k=0}^{\frac{n}{2}} (-1)^k \binom{n+1-k}{k} x^{n+1-2k}.
\end{aligned}
$$

On procède de façon analogue si n est impair. Cela prouve la formule par récurrence. □

Proposition 3.12. *Si $p^2 \mid N$ avec p premier alors $(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) \in (\mathbb{Z}/N\mathbb{Z})^{2p}$ est une solution monomiale minimale de (E_N).*

Démonstration. Si $p = 2$ alors le résultat est vrai (voir théorème 2.7). On suppose maintenant $p \geq 3$. Par ce qui précède, $(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) \in (\mathbb{Z}/N\mathbb{Z})^{2p}$ est une solution monomiale de (E_N). Ainsi, la taille de la solution $\overline{\frac{N}{p}}$-monomiale minimale divise $2p$. Donc, celle-ci est égale à 1, 2, p ou $2p$. L'équation (E_N) n'a pas de solution de taille 1, et $\overline{\frac{N}{p}} \neq \bar{0}$ (sinon $N \mid \frac{N}{p}$ et donc $\frac{N}{p} \geq N$) donc la solution $\overline{\frac{N}{p}}$-monomiale minimale n'est pas de taille 2. Supposons par l'absurde que la solution $\overline{\frac{N}{p}}$-monomiale minimale est de taille p.

Il existe ϵ dans $\{\pm 1\}$ tel que

$$
\bar{\epsilon}\,\mathrm{Id} = M_p\left(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}\right) = \begin{pmatrix} K_p(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) & -K_{p-1}(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) \\ K_{p-1}(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) & -K_{p-2}(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) \end{pmatrix}.
$$

Donc, $K_{p-1}(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}}) = \bar{0}$. Notons $K = K_{p-1}(\overline{\frac{N}{p}}, \dots, \overline{\frac{N}{p}})$. On a, par le lemme précédent,

$$
K = \overline{\sum_{k=0}^{E[\frac{p-1}{2}]} (-1)^k \binom{p-1-k}{k} \left(\frac{N}{p}\right)^{p-1-2k}}
$$

$$
\begin{aligned}
&= \overline{\sum_{k=0}^{\frac{p-1}{2}} (-1)^k \binom{p-1-k}{k} \left(\frac{N}{p}\right)^{p-1-2k}} \qquad (\text{car } p-1 \text{ est pair}) \\
&= \overline{\sum_{k=0}^{\frac{p-1}{2}-1} (-1)^k \binom{p-1-k}{k} \frac{N^{p-1-2k}}{p^{p-1-2k}} + (-1)^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\frac{p-1}{2}}} \\
&= \overline{(-1)^{\frac{p-1}{2}} + \sum_{k=0}^{\frac{p-1}{2}-1} (-1)^k \binom{p-1-k}{k} N \frac{N}{p^2} \frac{N^{p-1-2k-2}}{p^{p-1-2k-2}}} \quad (p-1-2k-2 \geq 0,\ p^2 \mid N) \\
&= \overline{(-1)^{\frac{p-1}{2}}} \\
&\neq \bar{0}.
\end{aligned}
$$

Ceci est absurde. Donc, la solution $\frac{\overline{N}}{p}$-monomiale minimale est de taille $2p$. □

3.3. **Réductibilité dans le cas** $N = l^n$

On se place dans le cas où $N = l^n$ avec n et l supérieurs à 2. On sait que le $2l^{n-1}$-uplet $(\bar{l}, \dots, \bar{l})$ d'éléments de $\mathbb{Z}/N\mathbb{Z}$ est une solution de (E_N) (voir [11, proposition 3.20]). Cependant, la question de l'irréductibilité potentielle de cette solution reste ouverte. On se propose ici de répondre à cette dernière en démontrant le résultat suivant :

Théorème 3.13. *Si $N = l^n$ avec $l, n \geq 2$ alors $(\bar{l}, \dots, \bar{l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}}$ est une solution irréductible de (E_N) si et seulement si $l = 2$.*

Pour cela on a besoin de plusieurs résultats intermédiaires. On commence par le résultat classique suivant :

Lemme 3.14. *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 $\binom{n}{k}$. □

Lemme 3.15. *Soient $(n, l) \in (\mathbb{N}^*)^2$, $n \geq 3$, $l \geq 2$ et $j \in [\![2; n-1]\!]$. On a l^{n-j} divise $\binom{2l^{n-2}}{j}$.*

Démonstration. Si $j = 2$ alors

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

et donc le résultat est vrai. On peut ainsi supposer $n \geq 4$ et $j \geq 3$. On a par le lemme précédent

$$\frac{2l^{n-2}}{\text{pgcd}(2l^{n-2}, j)} \text{ divise } \binom{2l^{n-2}}{j}.$$

Notons $l = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de l en facteurs premiers. On a deux cas :

Cas 1 : l est impair. Dans ce cas, pour tout i appartenant à $[\![1; r]\!]$, $p_i \neq 2$. Il existe $(\beta_1, \dots, \beta_r, a) \in \mathbb{N}^{r+1}$ tels que $\text{pgcd}(2l^{n-2}, j) = 2^a p_1^{\beta_1} \dots p_r^{\beta_r}$. Si j est pair alors $a = 1$ et si j est impair alors $a = 0$.

Montrons que pour tout i dans $[\![1; r]\!]$, $\beta_i \leq \alpha_i(j-2)$. Supposons par l'absurde qu'il existe i dans $[\![1; r]\!]$ tel que $\beta_i > \alpha_i(j-2)$. Par récurrence, on montre que si $j \geq 3$ on a $p_i^{j-2} \geq j$ (car $p_i > 2$). On a

$$p_i^{\beta_i} > p_i^{\alpha_i(j-2)} \geq p_i^{j-2} \geq j.$$

Donc, $\text{pgcd}(2l^{n-2}, j) > j$ ce qui est absurde.

Ainsi, pour tout i appartenant à $[\![1; r]\!]$, $\beta_i \leq \alpha_i(j-2)$. De plus, on a $a = 1$ si j est pair et $a = 0$ si j est impair. On en déduit que l^{n-j} divise $\frac{2l^{n-2}}{\text{pgcd}(2l^{n-2}, j)}$. Donc, l^{n-j} divise $\binom{2l^{n-2}}{j}$.

Cas 2 : l est pair. Dans ce cas, on peut supposer $p_1 = 2$, et donc $p_j > 2$ pour j dans $[\![2; r]\!]$. Il existe $(\beta_1, \dots, \beta_r) \in \mathbb{N}^r$ tels que $\text{pgcd}(2l^{n-2}, j) = p_1^{\beta_1} \dots p_r^{\beta_r}$.

On montre, en procédant comme dans le premier cas, que pour tout i dans $[\![2; r]\!]$, $\beta_i \leq \alpha_i(j-2)$. Montrons que $\beta_1 \leq \alpha_1(j-2)+1$. Si $\beta_1 > \alpha_1(j-2)+1$ alors

$$p_1^{\beta_1} > p_1^{\alpha_1(j-2)+1} \geq p_1^{j-1} \geq j.$$

Donc, $\text{pgcd}(2l^{n-2}, j) > j$ ce qui est absurde.

On en déduit que pour tout i dans $[\![2; r]\!]$, $\beta_i \leq \alpha_i(j-2)$ et $\beta_1 \leq \alpha_1(j-2)+1$. Ainsi, l^{n-j} divise $\frac{2l^{n-2}}{\text{pgcd}(2l^{n-2}, j)}$. Donc, l^{n-j} divise $\binom{2l^{n-2}}{j}$.

Donc, le résultat est vrai. □

Lemme 3.16. *Soit $N = l^n$, $l > 2$ et $n \geq 3$. $(\overline{2l^{n-1}}, \bar{l}, \dots, \bar{l}, \overline{2l^{n-1}}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}-4l^{n-2}+2}$ est une solution de (E_N).*

Démonstration. On a $2l^{n-1} - 4l^{n-2} + 2 = 2l^{n-2}(l-2) + 2 \geq 2l^{n-2} + 2 \geq 2l + 2 \geq 8$.

$(\overline{2l^{n-1}}, \bar{l}, \dots, \bar{l}, \overline{2l^{n-1}}) \sim (\overline{2l^{n-1}}, \overline{2l^{n-1}}, \bar{l}, \dots, \bar{l})$. Donc, $(\overline{2l^{n-1}}, \bar{l}, \dots, \bar{l}, \overline{2l^{n-1}})$ est solution de (E_N) si et seulement si $(\overline{2l^{n-1}}, \overline{2l^{n-1}}, \bar{l}, \dots, \bar{l})$ l'est aussi. On a

$$\begin{aligned} M &= M_{2l^{n-1}-4l^{n-2}+2}(\overline{2l^{n-1}}, \overline{2l^{n-1}}, \bar{l}, \dots, \bar{l}) \\ &= M_{2l^{n-1}-4l^{n-2}}(\bar{l}, \dots, \bar{l}) M_2(\overline{2l^{n-1}}, \overline{2l^{n-1}}). \end{aligned}$$

$$\begin{aligned} M_{2l^{n-1}-4l^{n-2}}(\bar{l}, \dots, \bar{l}) &= M_{2l^{n-1}}(\bar{l}, \dots, \bar{l}) M_{4l^{n-2}}(\bar{l}, \dots, \bar{l})^{-1} \\ &= \overline{(-1)^{l^{n-1}}} M_{4l^{n-2}}(\bar{l}, \dots, \bar{l})^{-1} \\ &= \overline{(-1)^{l^{n-1}}} \left(\begin{pmatrix} \bar{0} & \bar{1} \\ \overline{-1} & \bar{l} \end{pmatrix} \right)^{4l^{n-2}} \\ &= \overline{(-1)^{l^{n-1}}} \left(\begin{pmatrix} \bar{0} & \bar{1} \\ \overline{-1} & \bar{l} \end{pmatrix}^2 \right)^{2l^{n-2}} \end{aligned}$$

$$\begin{aligned} M_{2l^{n-1}-4l^{n-2}}(\bar{l}, \dots, \bar{l}) &= \overline{(-1)^{l^{n-1}}} \begin{pmatrix} \overline{-1} & \bar{l} \\ \overline{-l} & \overline{-1+l^2} \end{pmatrix}^{2l^{n-2}} \\ &= \overline{(-1)^{l^{n-1}}} \overline{\left(-\mathrm{Id} + l \begin{pmatrix} 0 & 1 \\ -1 & l \end{pmatrix} \right)^{2l^{n-2}}} \\ &= \overline{\sum_{k=0}^{2l^{n-2}} \binom{2l^{n-2}}{k} (-1)^{l^{n-2}(l+2)-k} l^k \begin{pmatrix} 0 & 1 \\ -1 & l \end{pmatrix}^k} \quad \text{(binôme de Newton)} \\ &= \overline{\sum_{k=0}^{n-1} \binom{2l^{n-2}}{k} (-1)^{l^{n-2}(l+2)-k} l^k \begin{pmatrix} 0 & 1 \\ -1 & l \end{pmatrix}^k} \\ &= \overline{(-1)^{l^{n-2}(l+2)} \mathrm{Id} + (-1)^{l^{n-2}(l+2)-1} (2l^{n-2}) l \begin{pmatrix} 0 & 1 \\ -1 & l \end{pmatrix}}. \end{aligned}$$

La dernière égalité est valide car, par le lemme précédent, l^{n-k} divise $\binom{2l^{n-2}}{k}$ pour $2 \leq k \leq n-1$.

De plus, $M_2(\overline{2l^{n-1}}, \overline{2l^{n-1}}) = \begin{pmatrix} \overline{-1} & \overline{-2l^{n-1}} \\ \overline{2l^{n-1}} & \overline{-1} \end{pmatrix}$.

Donc, on a

$$M = M_{2l^{n-1}-4l^{n-2}}(\bar{l}, \dots, \bar{l}) M_2(\overline{2l^{n-1}}, \overline{2l^{n-1}})$$

$$= \left(\overline{(-1)^{l^{n-2}(l+2)}\,\mathrm{Id}} + \overline{(-1)^{l^{n-2}(l+2)-1}(2l^{n-2})l}\begin{pmatrix}\bar{0} & \bar{1}\\ \overline{-1} & \bar{l}\end{pmatrix}\right)\begin{pmatrix}\overline{-1} & \overline{-2l^{n-1}}\\ \overline{2l^{n-1}} & \overline{-1}\end{pmatrix}$$

$$= \overline{(-1)^{l^{n-2}(l+2)}}\begin{pmatrix}\overline{-1} & \overline{-2l^{n-1}}\\ \overline{2l^{n-1}} & \overline{-1}\end{pmatrix} + \overline{(-1)^{l^{n-2}(l+2)-1}(2l^{n-1})}\begin{pmatrix}\overline{2l^{n-1}} & \overline{-1}\\ \bar{1} & \overline{2l^{n-1}-l}\end{pmatrix}$$

$$= \overline{(-1)^{l^{n-2}(l+2)}}\left(\begin{pmatrix}\overline{-1} & \overline{-2l^{n-1}}\\ \overline{2l^{n-1}} & \overline{-1}\end{pmatrix} - \begin{pmatrix}\bar{0} & \overline{-2l^{n-1}}\\ \overline{2l^{n-1}} & \bar{0}\end{pmatrix}\right)$$

$$= \overline{(-1)^{l^{n-2}(l+2)-1}\,\mathrm{Id}}.$$

□

On peut maintenant démontrer le résultat principal de la section.

Démonstration du théorème 3.13. Soit $N = l^n$ avec $l \geq 2$ et $n \geq 2$.

$(\bar{l}, \ldots, \bar{l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}}$ est solution de (E_N) (voir [11, proposition 3.20]).

Si $n = 2$ alors le résultat est vrai (voir proposition 3.9).

Supposons $n \geq 3$. Si $l = 2$ alors la solution est irréductible (voir théorème 3.1). Supposons $l > 2$. On a

$$(\bar{l}, \ldots, \bar{l}) = (\overline{l - 2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{l - 2l^{n-1}}) \oplus (\overline{2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{2l^{n-1}})$$

avec $(\overline{2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{2l^{n-1}}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}-4l^{n-2}+2}$. On a $(\overline{l - 2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{l - 2l^{n-1}}) \in (\mathbb{Z}/N\mathbb{Z})^{4l^{n-2}}$.

De plus, par le lemme précédent, $(\overline{2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{2l^{n-1}}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}-4l^{n-2}+2}$ est une solution de (E_N) de taille supérieure à 3. $(\overline{l - 2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{l - 2l^{n-1}}) \in (\mathbb{Z}/N\mathbb{Z})^{4l^{n-2}}$ est de taille supérieure à 4. Donc, $(\bar{l}, \ldots, \bar{l}) \in (\mathbb{Z}/N\mathbb{Z})^{2l^{n-1}}$ est une solution réductible de (E_N). □

Remarque 3.17. Notons que $(\overline{l - 2l^{n-1}}, \bar{l}, \ldots, \bar{l}, \overline{l - 2l^{n-1}}) \in (\mathbb{Z}/N\mathbb{Z})^{4l^{n-2}}$ est aussi une solution de (E_N).

4. **Solutions dynomiales minimales**

On s'intéresse dans cette section au concept de solutions dynomiales minimales défini dans la section 2 en démontrant notamment le théorème 2.10.

4.1. **Résultats préliminaires**

Pour effectuer la preuve du théorème 2.10, on a besoin de plusieurs résultats intermédiaires. On commence par le lemme ci-dessous :

Lemme 4.1. *Soit $n \in \mathbb{N} \cup \{-1\}$, $K_n(x_1, \ldots, x_n) = (-1)^n K_n(-x_1, \ldots, -x_n)$.*

Démonstration. On raisonne par récurrence sur n.

$K_0 = 1$ et $K_{-1} = 0$ donc le résultat est vrai pour $n = -1$ et pour $n = 0$.

Supposons qu'il existe $n \in \mathbb{N}$ tel que la formule est vraie au rang n et $n-1$. On a :

$$\begin{aligned} K_{n+1}(x_1, \dots, x_{n+1}) &= x_1 K_n(x_2, \dots, x_{n+1}) - K_{n-1}(x_3, \dots, x_{n+1}) \\ &= (-1)^n x_1 K_n(-x_2, \dots, -x_{n+1}) - (-1)^{n-1} K_{n-1}(-x_3, \dots, -x_{n+1}) \\ &= (-1)^{n-1}(-x_1 K_n(-x_2, \dots, -x_{n+1}) - K_{n-1}(-x_3, \dots, -x_{n+1})) \\ &= (-1)^{n+1}(-x_1 K_n(-x_2, \dots, -x_{n+1}) - K_{n-1}(-x_3, \dots, -x_{n+1})) \\ &= (-1)^{n+1} K_{n+1}(-x_1, \dots, -x_{n+1}). \end{aligned}$$

Par récurrence, le résultat est vrai. □

On a également besoin du résultat suivant qui est l'analogue de la proposition 3.21 de [11] pour les solutions dynomiales.

Lemme 4.2. *Soient $n \in \mathbb{N}^*$, $n \geq 4$ et $(\bar{a}, \bar{b}, \bar{k}) \in (\mathbb{Z}/N\mathbb{Z})^3$. Soit $\alpha \in \{\pm 1\}$.*

(i) *Si $(\bar{a}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \bar{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N) alors $\bar{a} = \overline{-b}$ et on a*

$$\bar{0} = \bar{a}(\overline{\alpha k} + \bar{a}).$$

(ii) *Si $(\bar{a}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{\alpha k}, \bar{b}) \in (\mathbb{Z}/N\mathbb{Z})^n$ est solution de (E_N) alors $\bar{a} = \bar{b}$ et on a*

$$\bar{2} = \bar{a}(\overline{\alpha k} + \bar{a}).$$

Démonstration. (i). Supposons que n est pair. Comme $(\bar{a}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \bar{b})$ est solution de (E_N), il existe ϵ dans $\{-1, 1\}$ tel que

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

Ainsi,

$$K_{n-1}(\bar{a}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}) = -K_{n-1}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \bar{b}) = \bar{0}$$

et

$$K_{n-2}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}) = -\bar{\epsilon}.$$

Or,

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

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

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

De même, on a

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

Il en découle

$$\begin{aligned}\bar{b} &= \overline{-\epsilon}K_{n-3}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k},\overline{\alpha k})\\ &= \overline{(-\epsilon)}\,\overline{(-1)^{n-3}}K_{n-3}(\overline{-\alpha k},\overline{\alpha k},\dots,\overline{-\alpha k},\overline{\alpha k},\overline{-\alpha k})\\ &= \overline{-a} \text{ car } n \text{ est pair.}\end{aligned}$$

De plus, on dispose des égalités ci-dessous :

$$\begin{aligned}\overline{-\epsilon} &= K_{n-2}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k})\\ &= \overline{\alpha k}K_{n-3}(\overline{-\alpha k},\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k}) - K_{n-4}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k})\end{aligned}$$

et

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

On en déduit l'égalité suivante :

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

Or, comme $K_{n-2}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}) = \overline{-\epsilon}$, on a

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

c'est-à-dire

$$\begin{aligned} K_{n-4}(\overline{-\alpha k}, \overline{\alpha k}, \dots, \overline{-\alpha k}, \overline{\alpha k}) &= K_{n-4}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}) \quad \text{car } n-4 \text{ est pair} \\ &= \bar{\epsilon}(\bar{1} + K_{n-3}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{\alpha k})^2). \end{aligned}$$

Ainsi, on a

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

Donc, $\bar{0} = \overline{-\alpha \epsilon k a} - \overline{\epsilon a^2} = -\bar{\epsilon}\bar{a}(\overline{\alpha k} + \bar{a})$ et donc $\bar{0} = \bar{a}(\overline{\alpha k} + \bar{a})$.

(ii). Supposons que n est impair. Comme $(\bar{a}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{\alpha k}, \bar{b})$ est solution de (E_N), il existe ϵ dans $\{-1, 1\}$ tel que

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

Donc,

$$K_{n-1}(\bar{a}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{\alpha k}) = -K_{n-1}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{\alpha k}, \bar{b}) = \bar{0}$$

et

$$K_{n-2}(\overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{\alpha k}) = -\bar{\epsilon}.$$

Or,

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

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

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

De même, on a

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

Donc,

$$\begin{aligned}\bar{b} &= \overline{-\epsilon}K_{n-3}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k})\\ &= \overline{(-\epsilon)}\overline{(-1)^{n-3}}K_{n-3}(\overline{-\alpha k},\overline{\alpha k},\dots,\overline{-\alpha k},\overline{\alpha k})\\ &= \overline{(-\epsilon)}K_{n-3}(\overline{-\alpha k},\overline{\alpha k},\dots,\overline{-\alpha k},\overline{\alpha k}) \quad \text{car } n-3 \text{ pair}\\ &= \bar{a}.\end{aligned}$$

De plus, on a

$$\begin{aligned}\overline{-\epsilon} &= K_{n-2}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k},\overline{\alpha k})\\ &= \overline{\alpha k}K_{n-3}(\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k},\overline{\alpha k}) - K_{n-4}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k},\overline{\alpha k})\end{aligned}$$

et

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

Ainsi,

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

Or, comme $K_{n-2}(\overline{\alpha k},\overline{-\alpha k},\dots,\overline{\alpha k},\overline{-\alpha k},\overline{\alpha k}) = \overline{-\epsilon}$, on a

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

c'est-à-dire

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

Donc, on a

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

Donc, $\overline{-2\epsilon} = \overline{-\alpha\epsilon k a} - \overline{\epsilon a^2} = -\bar{\epsilon}\bar{a}(\overline{\alpha k} + \bar{a})$ et donc $\bar{2} = \bar{a}(\overline{\alpha k} + \bar{a})$. □

Remarque 4.3. Dans le cas où n est pair, il est possible que $\bar{a} \neq \bar{0}$ et $\bar{a} \neq \pm\bar{k}$. Par exemple, si on pose $N = 14$, le 18-uplet $(\bar{7}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{3}, \overline{11}, \bar{7})$ est solution de (E_N).

4.2. **Preuve du théorème d'irréductibilité**

On peut maintenant démontrer le résultat principal.

Démonstration du théorème 2.10. Soient $\bar{k} \in \mathbb{Z}/N\mathbb{Z}$, $\bar{k} \neq \bar{0}$, et $n \in \mathbb{N}^*$ tels que le n-uplet $(\bar{k}, \overline{-k}, \dots, \bar{k}, \overline{-k})$ d'éléments de $\mathbb{Z}/N\mathbb{Z}$ est une solution dynomiale minimale de (E_N). On suppose que $\bar{k}^2 + \bar{8}$ n'est pas un carré dans $\mathbb{Z}/N\mathbb{Z}$. On suppose par l'absurde que cette solution peut s'écrire comme une somme de deux solutions non triviales.

$\bar{k} \neq \pm\bar{1}$ car $(\pm\bar{1})^2 + \bar{8} = \bar{9} = \bar{3}^2$. Donc, si $n = 4$, $(\bar{k}, \overline{-k}, \dots, \bar{k}, \overline{-k})$ est irréductible, puisque les solutions réductibles de (E_N) de taille 4 contiennent toujours $\pm\bar{1}$. On suppose maintenant $n \geq 6$.

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 $l, l' \geq 3$ tels que

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

De plus, $\bar{k} \notin \{\bar{0}, \overline{-1}, \bar{1}\}$ donc $l, l' > 3$. Il existe α dans $\{\pm 1\}$ tel que

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

On a deux cas :

Cas 1 : Si l est pair alors $l' = n + 2 - l$ est pair. On a donc

$$(\overline{a_1}, \dots, \overline{a_l}) = (\overline{a_1}, \overline{\alpha k}, \overline{-\alpha k}, \dots, \overline{\alpha k}, \overline{-\alpha k}, \overline{a_l}).$$

Comme $(\overline{a_1}, \dots, \overline{a_l})$ est solution de (E_N), on a, par le lemme 4.2, $\overline{a_1} = \bar{a} = \overline{-a_l}$ et $\bar{0} = \bar{a}(\bar{a} + \overline{\alpha k})$. Comme N est premier, $\mathbb{Z}/N\mathbb{Z}$ est intègre et donc l'équation $\bar{0} = \bar{a}(\bar{a} + \overline{\alpha k})$ a pour solutions $\bar{a} = \bar{0}$ et $\bar{a} = \overline{-\alpha k}$.

Si $\bar{a} = \bar{0}$ alors $(\overline{a_2}, \ldots, \overline{a_{l-1}}) = (\overline{\alpha k}, \overline{-\alpha k}, \ldots, \overline{\alpha k}, \overline{-\alpha k}) \in (\mathbb{Z}/N\mathbb{Z})^{l-2}$ est encore solution de (E_N) ce qui contredit la minimalité de la solution (si $\alpha = -1$ alors $(\overline{-a_2}, \ldots, \overline{-a_{l-1}}) = (\bar{k}, \overline{-k}, \ldots, \bar{k}, \overline{-k})$ est encore solution). Donc, $\bar{a} = \overline{-\alpha k}$ et par minimalité de la solution on a $l \geq n$ ce qui implique $l' \leq 2$. Donc, $l' = 2$ et $(\overline{b_1}, \ldots, \overline{b_{l'}}) = (\bar{0}, \bar{0})$ ce qui est absurde.

Cas 2 : Si l est impair alors $l' = n + 2 - l$ est impair. On a donc

$$(\overline{a_1}, \ldots, \overline{a_l}) = (\overline{a_1}, \overline{-\alpha k}, \overline{\alpha k}, \ldots, \overline{-\alpha k}, \overline{\alpha k}, \overline{-\alpha k}, \overline{a_l})$$

et

$$(\overline{b_1}, \ldots, \overline{b_{l'}}) = (\overline{b_1}, \overline{-\alpha k}, \overline{\alpha k}, \ldots, \overline{-\alpha k}, \overline{\alpha k}, \overline{-\alpha k}, \overline{b_{l'}}).$$

Comme $(\overline{a_1}, \ldots, \overline{a_l})$ et $(\overline{b_1}, \ldots, \overline{b_{l'}})$ sont solutions de (E_N), on a par le lemme 4.2 :

- $\overline{a_1} = \bar{a} = \overline{a_l}$ et $\bar{2} = \bar{a}(\bar{a} - \overline{\alpha k})$;
- $\overline{b_1} = \bar{b} = \overline{b_{l'}}$ et $\bar{2} = \bar{b}(\bar{b} - \overline{\alpha k})$.

$\bar{a}$ et $\bar{b}$ sont des racines de $P(X) = X(X - \overline{\alpha k}) - \bar{2} = X^2 - \overline{\alpha k}X - \bar{2}$. Comme N est premier différent de 2, $\mathbb{Z}/N\mathbb{Z}$ est un corps de caractéristique différente de 2 et le discriminant de P est $\Delta = (-\overline{\alpha k})^2 - 4 \times \overline{-2} = \overline{k}^2 + \bar{8}$. Comme $\overline{k}^2 + \bar{8}$ n'est pas un carré dans $\mathbb{Z}/N\mathbb{Z}$, P n'a pas de racine dans $\mathbb{Z}/N\mathbb{Z}$ ce qui est absurde.

Ainsi, on arrive à une absurdité dans les deux cas et donc $(\bar{k}, \overline{-k}, \ldots, \bar{k}, \overline{-k})$ est irréductible. □

Remarques 4.4.

(i) Il existe des solutions dynomiales minimales réductibles. Par exemple, posons $N = 11$. La solution $\bar{2}$-dynomiale minimale (qui est de taille 12) est réductible. En effet, $(\bar{6}, \bar{9}, \bar{2}, \bar{9}, \bar{6})$ est solution de (E_{11}) et

$$(\bar{2}, \bar{9}, \bar{2}, \bar{9}, \bar{2}, \bar{9}, \bar{2}, \bar{9}, \bar{2}, \bar{9}, \bar{2}, \bar{9}) = (\bar{7}, \bar{9}, \bar{2}, \bar{9}, \bar{2}, \bar{9}, \bar{2}, \bar{9}, \bar{7}) \oplus (\bar{6}, \bar{9}, \bar{2}, \bar{9}, \bar{6}).$$

Cet exemple montre que, contrairement aux solutions monomiales minimales, il existe des solutions dynomiales minimales réductibles même si N est premier. De même, contrairement aux solutions monomiales minimales, il existe des solutions $\bar{2}$-dynomiales minimales réductibles.

(ii) La condition $\overline{k}^2 + \bar{8}$ n'est pas un carré dans $\mathbb{Z}/N\mathbb{Z}$ n'est pas une condition nécessaire. Par exemple, $(\bar{6}, \overline{-6}, \bar{6}, \overline{-6})$ est une solution dynomiale minimale irréductible pour $N = 19$ et $\bar{6}^2 + \bar{8} = \overline{36} + \bar{8} = \bar{6} = \bar{5}^2$.

4.3. **Applications**

La condition $\overline{k}^2 + \overline{8}$ n'est pas un carré dans $\mathbb{Z}/N\mathbb{Z}$ peut être vérifiée à l'aide la loi de réciprocité quadratique de Gauss (puisque N est premier). Si p est un nombre premier impair et si a est un entier premier avec p, on note $(\frac{a}{p})$ le symbole de Legendre c'est-à-dire :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } \overline{a} \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z}; \\ -1 & \text{sinon.} \end{cases}$$

Le symbole de Legendre vérifie les propriétés suivantes :

Lemme 4.5 ([9, proposition XII.20])**.** *Soient p un nombre premier impair et a et b deux entiers premiers avec p. On a :*

(1) *(critère d'Euler)* $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}\ [p]$ *;*

(2) *(multiplicativité)* $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ *;*

(3) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Théorème 4.6 (Loi de réciprocité quadratique de Gauss ; [9, théorème XII.25])**.** *Soient p et q deux nombres premiers impairs distincts. On a*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Par exemple, si $\overline{k} = \overline{3}$, on a $\overline{k^2 + 8} = \overline{17}$. Comme 17 est premier, on peut utiliser la loi de réciprocité quadratique de Gauss pour savoir si $\overline{k^2 + 8}$ est un carré modulo N (avec N un entier premier supérieur à 5). On a alors par exemple :

Proposition 4.7. *La solution $\overline{3}$-dynomiale minimale de (E_{97}) est irréductible.*

Démonstration. 97 est premier et $\overline{3} \notin \{\overline{0}, \overline{1}, \overline{-1}\}$. De plus, $97 = 5 \times 17 + 12$ et les carrés modulo 17 sont :

$$\{\overline{0}, \overline{1}, \overline{4}, \overline{9}, \overline{-1}, \overline{8}, \overline{2}, \overline{15}, \overline{13}\}.$$

Donc, d'après la loi de réciprocité quadratique de Gauss, on a :

$$\left(\frac{17}{97}\right) = \left(\frac{97}{17}\right)(-1)^{\frac{17-1}{2}\frac{97-1}{2}} = \left(\frac{12}{17}\right)(-1)^{8\times 48} = -1.$$

Donc, $\overline{3^2 + 8}$ n'est pas un carré modulo 97. Donc, par le théorème 2.10, la solution $\overline{3}$-dynomiale minimale de (E_{97}) est irréductible. □

On va maintenant s'intéresser au cas de la solution $\overline{2}$-dynomiale minimale de (E_N) où N est un entier premier supérieur à 5. On commence par le résultat intermédiaire ci-dessous :

Lemme 4.8. *Soit p un nombre premier.*

$$\overline{3} \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \iff \begin{cases} p = 2; \\ p = 3; \\ p \equiv \pm 1 \ [12]. \end{cases}$$

Démonstration. Si $p = 2$ alors $\overline{3} = \overline{1} = \overline{1}^2$ et si $p = 3$ alors $\overline{3} = \overline{0} = \overline{0}^2$. On suppose maintenant p supérieur à 5. D'après la loi de réciprocité quadratique de Gauss on a

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Comme p est premier, $p \equiv 1 \ [3]$ ou $p \equiv -1 \ [3]$. De plus, on a $(\frac{1}{3}) = 1$ et $(\frac{-1}{3}) = -1$. On distingue les deux cas :

- Si $p = 3k + 1$ avec k un entier naturel pair

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{1}{3}\right)(-1)^{\frac{3k}{2}} = 1 \iff (-1)^{\frac{3k}{2}} = 1 \iff 4 \text{ divise } k \iff p \equiv 1 \ [12].$$

- Si $p = 3k - 1$ avec k un entier naturel pair

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{-1}{3}\right)(-1)^{\frac{3k-2}{2}} = 1 \iff (-1)^{\frac{3k}{2}} = 1 \iff 4 \text{ divise } k \iff p \equiv -1 \ [12].$$

□

Proposition 4.9. *Si N est un entier premier supérieur à 5 tel que $N \not\equiv \pm 1[12]$ alors la solution $\overline{2}$-dynomiale minimale de (E_N) est irréductible.*

Démonstration. Par le lemme précédent, $\overline{3}$ est un carré modulo N si et seulement si $N \equiv \pm 1[12]$.

N est premier. De plus, on a $\overline{2^2 + 8} = \overline{12}$ et donc par multiplicativité du symbole de Legendre :

$$\left(\frac{12}{N}\right) = \left(\frac{2^2 \times 3}{N}\right) = \left(\frac{2^2}{N}\right)\left(\frac{3}{N}\right) = \left(\frac{2}{N}\right)^2\left(\frac{3}{N}\right) = \left(\frac{3}{N}\right) = -1.$$

Donc, par le théorème 2.10, la solution $\overline{2}$-dynomiale minimale de (E_N) est irréductible. □

Remarque 4.10. Par le théorème faible de la progression arithmétique de Dirichlet (voir [9, proposition VII.13]), il existe une infinité de nombres premiers supérieurs à 5 congrus à 1 modulo 12.

La condition de la proposition précédente n'est pas nécessaire. Par exemple, si $N = 59 \equiv -1\ [12]$ alors la solution $\bar{2}$-dynomiale minimale de (E_N) est irréductible. En effet, celle-ci est de taille 20 et la seule façon de la réduire est de trouver une solution de (E_N) de la forme $(\bar{a}, \overline{-2}, \bar{2}, \overline{-2}, \ldots, \bar{2}, \overline{-2}, \bar{a})$ de taille inférieure à 19 (car les éléments donnés dans le cas 1 de la preuve du théorème 2.10 sont toujours valides). Par le lemme 4.2, les seules valeurs de $\bar{a}$ possibles sont $\overline{12}$ et $\overline{-10}$. Or, en calculant toutes les possibilités on ne trouve aucune solution de (E_N), ce qui implique l'irréductibilité de la solution $\bar{2}$-dynomiale minimale de (E_{59}). Ceci nous amène au problème ouvert suivant :

Problème. Soit N un nombre premier. Trouver des conditions nécessaires et suffisantes sur N pour l'irréductibilité de la solution $\bar{2}$-dynomiale minimale de (E_N).

On donne en annexe B les éléments concernant la réductibilité ou l'irréductibilité des solutions $\bar{2}$-dynomiales minimales de (E_N) pour les nombres premiers congrus à ± 1 modulo 12 et inférieurs à 500.

Annexe A. Taille des solutions $\overline{k}$-monomiales minimales pour les nombres premiers entre 11 et 47

$\overline{k}$ \ N	11	13	17	19	23	29	31	37	41	43	47
$\overline{0}$	2	2	2	2	2	2	2	2	2	2	2
$\overline{1}$	3	3	3	3	3	3	3	3	3	3	3
$\overline{2}$	11	13	17	19	23	29	31	37	41	43	47
$\overline{3}$	5	7	9	9	12	7	15	19	10	22	8
$\overline{4}$	5	6	9	5	11	15	16	18	7	11	23
$\overline{5}$	6	7	8	5	4	5	8	9	20	21	23
$\overline{6}$	6	7	4	10	11	5	15	19	5	22	23
$\overline{7}$	5	7	9	9	6	7	15	19	5	11	4
$\overline{8}$	5	7	8	10	12	15	4	19	21	7	24
$\overline{9}$	11	6	8	9	11	15	16	9	20	11	24
$\overline{10}$	3	7	9	9	11	14	16	19	21	21	23
$\overline{11}$	2	13	4	10	11	7	16	19	7	21	24
$\overline{12}$	3	3	8	9	11	14	5	19	21	21	6
$\overline{13}$	11	2	9	10	11	14	5	19	20	21	23
$\overline{14}$	5	3	9	5	11	15	8	9	7	11	23
$\overline{15}$	5	13	17	5	12	15	15	6	20	7	12
$\overline{16}$	6	7	3	9	6	14	15	18	21	22	23
$\overline{17}$	6	6	2	19	11	14	8	18	4	22	23
$\overline{18}$	5	7	3	3	4	7	5	19	10	22	8
$\overline{19}$	5	7	17	2	11	14	5	19	21	7	23
$\overline{20}$	11	7	9	3	12	15	16	18	21	21	24
$\overline{21}$	3	7	9	19	23	15	16	18	21	11	23
$\overline{22}$	2	6	8	9	3	7	16	6	21	11	12
$\overline{23}$	3	7	4	5	2	5	4	9	10	21	23

Annexe B. Éléments sur la réductibilité des solutions $\overline{2}$-dynomiales minimales de (E_N) pour les nombres premiers congrus à ± 1 modulo 12 et inférieurs à 500

N	taille	réductibilité	solutions de $X(X-\overline{2})=\overline{2}$	exemple de solution permettant de réduire
11	12	réductible	$\overline{6}, \overline{7}$	$(\overline{6}, \overline{-2}, \overline{2}, \overline{-2}, \overline{6})$
13	14	réductible	$\overline{5}, \overline{10}$	$(\overline{5}, \overline{-2}, \overline{2}, \overline{-2}, \overline{5})$
23	22	réductible	$\overline{8}, \overline{17}$	$(\overline{17}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{17})$
37	38	réductible	$\overline{16}, \overline{23}$	$(\overline{16}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{16})$
47	46	réductible	$\overline{13}, \overline{36}$	$(\overline{36}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{36})$, taille : 21
59	20	irréductible	$\overline{12}, \overline{49}$	
61	62	réductible	$\overline{9}, \overline{54}$	$(\overline{9}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{9})$
71	70	réductible	$\overline{29}, \overline{44}$	$(\overline{29}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{29})$
73	36	irréductible	$\overline{22}, \overline{53}$	
83	84	réductible	$\overline{-12}, \overline{14}$	$(\overline{14}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{2}, \overline{-2}, \overline{14})$
97	48	réductible	$\overline{-9}, \overline{11}$	$(\overline{11}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{11})$, taille : 29
107	108	réductible	$\overline{-17}, \overline{19}$	$(\overline{19}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{19})$, taille : 23
109	110	réductible	$\overline{-59}, \overline{61}$	$(\overline{61}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{61})$, taille : 23
131	132	réductible	$\overline{-92}, \overline{94}$	$(\overline{94}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{94})$, taille : 31
157	158	réductible	$\overline{-84}, \overline{86}$	$(\overline{-84}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{-84})$, taille : 59
167	166	réductible	$\overline{-104}, \overline{106}$	$(\overline{-104}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{-104})$, taille : 13
179	36	irréductible	$\overline{-18}, \overline{20}$	
181	182	réductible	$\overline{-32}, \overline{34}$	$(\overline{34}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{34})$, taille : 21
191	190	réductible	$\overline{-23}, \overline{25}$	$(\overline{25}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{25})$, taille : 69
193	96	irréductible	$\overline{-13}, \overline{15}$	
227	76	irréductible	$\overline{-49}, \overline{51}$	
229	46	irréductible	$\overline{-157}, \overline{159}$	
239	14	irréductible	$\overline{-132}, \overline{134}$	
241	40	irréductible	$\overline{-55}, \overline{57}$	
251	84	irréductible	$\overline{-174}, \overline{176}$	

N	taille	réductibilité	solutions de $X(X-\overline{2})=\overline{2}$	exemple de solution permettant de réduire
263	262	réductible	$\overline{-22}, \overline{24}$	$(\overline{24}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{24})$, taille : 85
277	278	réductible	$\overline{-146}, \overline{148}$	$(\overline{148}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{148})$, taille : 83
311	310	réductible	$\overline{-24}, \overline{26}$	$(\overline{26}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{26})$, taille : 31
313	78	irréductible	$\overline{-229}, \overline{231}$	
337	28	irréductible	$\overline{-44}, \overline{46}$	
347	348	réductible	$\overline{-251}, \overline{253}$	$(\overline{-251}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{-251})$, taille : 165
349	350	réductible	$\overline{-183}, \overline{185}$	$(\overline{-183}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{-183})$ taille : 147
359	358	réductible	$\overline{-195}, \overline{197}$	$(\overline{-195}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{-195})$, taille : 103
373	374	réductible	$\overline{-241}, \overline{243}$	$(\overline{-241}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{-241})$, taille : 111
383	382	réductible	$\overline{-223}, \overline{225}$	$(\overline{225}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{225})$, taille : 111
397	398	réductible	$\overline{-19}, \overline{21}$	$(\overline{21}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{21})$ taille : 131
409	102	réductible	$\overline{-240}, \overline{242}$	$(\overline{242}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{242})$, taille : 95
419	140	réductible	$\overline{-28}, \overline{30}$	$(\overline{30}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{30})$ taille : 45
421	422	réductible	$\overline{-73}, \overline{75}$	$(\overline{75}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{75})$ taille : 207
431	430	réductible	$\overline{-35}, \overline{37}$	$(\overline{37}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{37})$, taille : 25
433	216	réductible	$\overline{-50}, \overline{52}$	$(\overline{52}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{52})$, taille : 123
443	148	irréductible	$\overline{-271}, \overline{273}$	
457	114	irréductible	$\overline{-311}, \overline{313}$	
467	468	réductible	$\overline{-300}, \overline{302}$	$(\overline{302}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{302})$, taille : 65
479	478	réductible	$\overline{-30}, \overline{32}$	$(\overline{32}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{32})$, taille : 269
491	492	réductible	$\overline{-112}, \overline{114}$	$(\overline{114}, \overline{-2}, \overline{2}, \overline{-2}, \ldots, \overline{2}, \overline{-2}, \overline{114})$, taille : 323

Références

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

[2] François Bergeron and Christophe Reutenauer. SL_k-tilings of the plane. *Ill. J. Math.*, 54(1) :263–300, 2010.

[3] Éric Charpentier, Étienne Ghys, and Annick Lesne, editors. *L'héritage scientifique de Poincaré*. Belin, 2006.

[4] Charles Conley and Valentin Ovsienko. Rotundus : triangulations, Chebyshev polynomials, and Pfaffians. *Math. Intell.*, 40(3) :45–50, 2018.

[5] John H. Conway and Harold S. M. Coxeter. Triangulated polygons and frieze patterns. *Math. Gaz.*, 57(400-401) :87–94 et 175–183, 1973.

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

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

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

[9] Ivan Gozard. *Théorie de Galois - niveau L3-M1 - 2e édition*. Ellipses, 2009.

[10] Flavien Mabilat. Combinatorial description of the principal congruence subgroup γ (2) in $SL_2(Z)$. `https://arxiv.org/abs/1911.06717`, à paraître dans Commun. Math., 2020.

[11] Flavien Mabilat. Combinatoire des sous-groupes de congruence du groupe modulaire. *Ann. Math. Blaise Pascal*, 28(1) :7–43, 2021.

[12] Flavien Mabilat. Quelques éléments de combinatoire des matrices de $SL_2(Z)$. *Bull. Sci. Math.*, 167 : article no. 102958 (18 pages), 2021.

[13] Flavien Mabilat. λ-quiddité sur $Z[\alpha]$ avec α transcendant. *Math. Scand.*, 128(1) :5–13, 2022.

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

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

[16] 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.

[17] 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.

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

Combinatoire des sous-groupes de congruence du groupe modulaire II

Flavien Mabilat
Laboratoire de Mathématiques de Reims,
UMR9008 CNRS
et Université de Reims Champagne-Ardenne,
U.F.R. Sciences Exactes et Naturelles Moulin de la
Housse
BP 1039 51687 Reims cedex 2, France
flavien.mabilat@univ-reims.fr