Graphes de Steinhaus réguliers et triangles de Steinhaus dans les groupes cycliques

Jonathan Chappelon

Université du Littoral Côte d'Opale
École Doctorale Sciences Pour l'Ingénieur N° 72

Thèse en vue de l'obtention du grade de
Docteur de l'Université du Littoral Côte d'Opale
Discipline : Mathématiques

Directeur de thèse : Shalom Eliahou

GRAPHES DE STEINHAUS RÉGULIERS ET TRIANGLES DE STEINHAUS DANS LES GROUPES CYCLIQUES

Jonathan Chappelon

<chappelon@lmpa.univ-littoral.fr>

Cette thèse a été soutenue le vendredi 21 novembre 2008 à Calais.
Le Jury était constitué de

M. Allouche Jean-Paul	Université Paris Sud	Rapporteur
M. Dymacek Wayne	Washington and Lee University, USA	Rapporteur
M. von Below Joachim	Université du Littoral Côte d'Opale	Président de Jury
M. Eliahou Shalom	Université du Littoral Côte d'Opale	Directeur de Thèse
M. Harborth Heiko	Technische Universität Braunschweig	Examinateur
M. Lecouvey Cédric	Université du Littoral Côte d'Opale	Examinateur
M. Ramirez Alfonsin Jorge Luis	Université Pierre et Marie Curie	Examinateur

La soutenance de cette thèse a reçu l'accord de la Commission des Thèses de Mathématiques des Universités de Lille I, Valenciennes, Artois et Littoral le vendredi 19 septembre 2008.

Remerciements

Je remercie chaleureusement Shalom Eliahou d'avoir encadré ce travail de thèse, avec beaucoup de compétence, d'enthousiasme et de disponibilité. Merci Shalom pour tes conseils, ton optimisme et la confiance que tu as su m'accorder au cours de ces années.

Je remercie les rapporteurs de cette thèse Jean-Paul Allouche et Wayne Dymacek pour la rapidité avec laquelle ils ont lu mon mémoire et l'intérêt qu'ils ont porté à mon travail. Merci également aux autres membres du jury qui ont accepté de juger ce travail : Joachim von Below, Heiko Harborth, Cédric Lecouvey et Jorge Luis Ramirez Alfonsin.

Merci à tous les membres du Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville de Calais. Je tiens à remercier plus particulièrement mon collègue et ami Simon Rénier pour ses conseils et les diverses conversations que nous avons pu avoir durant ces trois années.

Merci enfin à toute ma famille, en particulier Audrey, de m'avoir soutenu et aidé.

Table des matières

Conventions **11**

Introduction **13**

1 Triangles de Steinhaus binaires **15**

1.1 Le problème de Steinhaus 15

1.1.1 Enoncé élémentaire 15

1.1.2 Définitions et premières propriétés 16

1.2 Le nombre de 1 dans un triangle de Steinhaus 21

1.3 Solutions du Problème de Steinhaus 28

1.3.1 Solution de Harborth 28

1.3.2 Solution de Eliahou-Hachez 36

1.3.3 Suites binaires balancées symétriques et antisymétriques 39

1.3.4 Suites binaires balancées de poids moyen 42

2 Graphes de Steinhaus pairs et impairs **43**

2.1 Définitions et premières propriétés 43

2.2 Une nouvelle preuve du théorème de Dymacek 47

2.3 Graphes de Steinhaus pairs 50

2.4 Graphes de Steinhaus impairs 54

3 Graphes de Steinhaus réguliers **57**

3.1 Graphes de Steinhaus réguliers 57
3.2 Matrices de Steinhaus multisymétriques 61
3.3 Degrés des sommets des graphes associés aux matrices de Steinhaus multisymétriques 63
3.4 Matrices de Steinhaus multisymétriques associées à des graphes de Steinhaus réguliers modulo 4 66

4 Triangles de Steinhaus dans les groupes cycliques 71

4.1 Triangles de Steinhaus et Problème de Molluzzo 72
4.1.1 Triangles de Steinhaus 72
4.1.2 Le Problème de Molluzzo 74
4.2 Généralités sur les suites balancées 75
4.2.1 Longueur d'une suite balancée 75
4.2.2 Projections de suites balancées 77
4.3 Triangles de Steinhaus de suites arithmétiques 78
4.4 Suites arithmétiques balancées dans les groupes cycliques d'ordre impair . . 79
4.5 Le cas antisymétrique 92
4.6 Solutions du Problème de Molluzzo 97
4.7 Suites arithmétiques balancées dans les groupes cycliques d'ordre pair 99

5 L'ordre multiplicatif de a^n modulo n 101

5.1 La fonction arithmétique α_n 101
5.2 La fonction arithmétique β_n 109

Conclusion et perspectives 113

Bibliographie 116

A Suites balancées dans les groupes cycliques d'ordre 3, 5 et 7 117

A.1 Suites fortement balancées 117

A.1.1 Suites fortement balancées à droite 118
A.1.2 Suites à dérivation fortement balancée 119
A.2 Solutions du Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$ 122
A.2.1 Suites balancées antisymétriques et périodiques 122
A.2.2 Suites arithmétiques et primitives 122
A.3 Solution du Problème de Molluzzo dans $\mathbb{Z}/7\mathbb{Z}$ 123
A.3.1 Suites arithmétiques et primitives 123
A.3.2 Suites arithmétiques entrelacées 125

B English summary **129**

B.1 Binary Steinhaus triangles 129
B.1.1 The Steinhaus Problem 129
B.1.2 The number of 1's in a Steinhaus triangle 130
B.1.3 Solutions of Steinhaus's Problem 131
B.2 Even and odd Steinhaus graphs 131
B.3 Regular Steinhaus graphs 134
B.4 Steinhaus triangles in finite cyclic groups 136
B.5 Multiplicative order of a^n modulo n 139

Conventions

On note $\mathbb{N}$ l'ensemble des entiers naturels et $\mathbb{Z}$ l'ensemble des entiers relatifs.

On note $\mathbb{Z}/n\mathbb{Z}$ le groupe cyclique à $n \in \mathbb{N}^*$ éléments.

Pour tout nombre réel x, on note $\lfloor x \rfloor$ sa partie entière inférieure et $\lceil x \rceil$ sa partie entière supérieure.

On note $|E|$ le cardinal d'un ensemble E et, de même, on note $|M|$ le cardinal d'un multiensemble M.

On note $E_1 \cap E_2$ et $E_1 \cup E_2$ l'intersection et la réunion de deux ensembles E_1 et E_2.

On note $M_1 \cap M_2$ et $M_1 \cup M_2$ l'intersection et la réunion de deux multiensembles M_1 et M_2.

On note $\mathcal{P}$ l'ensemble des nombres premiers.

Pour tout entier n et tout p dans $\mathcal{P}$, on note $v_p(n)$ la valuation p-adique de l'entier n, c'est-à-dire, le plus grand exposant $e \in \mathbb{N}$ tel que p^e divise n.

On note $\mathrm{rad}(n)$ le radical de l'entier n, c'est-à-dire, le plus grand facteur sans carré de n.

On note $\omega(n)$ le nombre de facteurs premiers distincts de l'entier n.

On note φ la fonction indicatrice d'Euler et, pour tout entier n, on note $\varphi(n)$ l'image de n par φ.

On note $n_1 \wedge n_2$ le plus grand commun diviseur des entiers n_1 et n_2.

On note $n_1 \vee n_2$ le plus petit commun multiple des entiers n_1 et n_2.

On note $S_1 S_2$ ou $S_1 \cdot S_2$ la concaténation des suites de longueur finies S_1 et S_2.

Pour tout $k \in \mathbb{N} \cup \{\infty\}$ et toute suite S finie, on note S^k la suite S concaténée k fois.

Pour toute suite $S = (a_1, \ldots, a_n)$ de longueur $n \in \mathbb{N} \cup \{\infty\}$, on note $S[m]$ la sous-suite initiale de S de longueur $m \leqslant n$, c'est-à-dire, $S[m] = (a_1, \ldots, a_m)$.

Enfin, on utilise les notations usuelles de la théorie des graphes du livre de Diestel [7].

Introduction

Depuis leur apparition, les nombres entiers et leurs propriétés n'ont cessé de fasciner les Hommes. En mathématiques, la théorie des nombres occupe une place particulière, à la fois par ses connexions avec de nombreux autres domaines et par la fascination qu'exercent ses énoncés. En théorie des nombres et en arithmétique, il existe de nombreux problèmes encore ouverts portant sur les nombres entiers et dont l'énoncé est facilement compréhensible, même par un non mathématicien. Par exemple, on peut citer la conjecture de Goldbach qui stipule que tout nombre pair supérieur à 2 peut être écrit comme la somme de deux nombres premiers. Dans ce mémoire, plusieurs problèmes à énoncé simple de théorie combinatoire des nombres et de théorie des graphes sont examinés. Plus précisément, on s'intéresse à des constructions basées sur des suites de longueur finie dans les groupes cycliques.

Tout d'abord, au Chapitre 1, on étudie les triangles de Steinhaus binaires. A partir d'une suite S de longueur $n \geqslant 2$ dans $\mathbb{Z}/2\mathbb{Z}$, on peut construire la suite dérivée ∂S de S qui est la suite de longueur $n-1$ obtenue en sommant chaque paire d'éléments consécutifs de S. Le triangle de Steinhaus ΔS est la collection des suites dérivées successives de S, c'est-à-dire $\Delta S = \{S, \partial S, \partial^2 S, \ldots, \partial^{n-1} S\}$, où la $i$ème dérivée $\partial^i S$ de S est définie de manière récursive par $\partial^i S = \partial(\partial^{i-1} S)$ pour $i \geqslant 2$. Chaque triangle de Steinhaus d'ordre n, c'est-à-dire associé à une suite de longueur n, peut alors être considéré comme un multiensemble composé de $\binom{n+1}{2}$ éléments de $\mathbb{Z}/2\mathbb{Z}$, comptés avec multiplicité. Cette construction est apparue en 1963 [23]. Steinhaus pose le problème de savoir s'il existe, pour tout entier $n \equiv 0$ ou $3 \pmod 4$, un triangle de Steinhaus d'ordre n comportant autant de 0 que de 1. Après avoir rappelé certaines propriétés sur les triangles de Steinhaus binaires, on détaille plusieurs solutions connues du Problème de Steinhaus, toutes indépendantes les unes des autres.

Ensuite, au Chapitre 2, on s'intéresse aux matrices et aux graphes de Steinhaus. Une matrice de Steinhaus de taille $n \geqslant 1$ est une matrice carrée, composée de 0 et de 1, qui est symétrique, de diagonale nulle et dont la partie triangulaire supérieure est un triangle de Steinhaus binaire. Un graphe de Steinhaus à $n \geqslant 1$ sommets est un graphe simple dont la matrice d'adjacence est une matrice de Steinhaus de taille n. Un problème classique sur ce type de graphes est de déterminer ceux possédant une propriété graphique donnée. Par exemple, les graphes de Steinhaus bipartis sont déterminés dans [4, 9, 10, 12] et ceux planaires dans [11]. Dans ce chapitre, on étudie les graphes de Steinhaus pairs et impairs, c'est-à-dire ceux dont tous les sommets sont de degrés de même parité. Les résultats obtenus sont basés sur un théorème dû à Dymacek et dont on fournit une nouvelle preuve dans ce mémoire. On

prouve en fait un résultat plus général qui établit certaines relations fortes entre les degrés des sommets d'un graphe de Steinhaus et les éléments de l'antidiagonale de sa matrice associée. On rappelle ensuite des résultats sur ces graphes de Steinhaus pairs et impairs qui ont été établis par Dymacek en 1979 [8].

Les graphes de Steinhaus réguliers, qui sont un cas particulier des graphes de Steinhaus pairs et impairs, sont étudiés au Chapitre 3. En 1979 [8], Dymacek a conjecturé que les graphes de Steinhaus réguliers sont les graphes sans arête à n sommets, les graphes à $n = 3m+1$ sommets dont la première ligne de la matrice associée est de la forme $0110110\ldots110$ et le graphe complet à deux sommets K_2. On s'intéresse surtout au cas impair de cette conjecture. On rappelle un résultat qui caractérise les suites binaires associées aux graphes de Steinhaus réguliers de degré impair. Cette structure conduit à l'étude des matrices de Steinhaus multisymétriques et, plus particulièrement, celles dont le graphe associé est régulier modulo 4, c'est-à-dire où tous les sommets sont de même degré modulo 4. Les résultats obtenus sur ces matrices de Steinhaus multisymétriques permettent de pousser la vérification de la conjecture de Dymacek, dans le cas impair, jusqu'à 1500 sommets, améliorant ainsi d'un facteur 12 la borne précédente connue (117 sommets).

Au Chapitre 4, on étudie la structure de triangle de Steinhaus dans tout groupe cyclique. On présente le Problème de Molluzzo qui est une généralisation du Problème de Steinhaus à tout groupe cyclique et qui consiste à déterminer l'existence de suites balancées, c'est-à-dire de suites finies dont le triangle de Steinhaus associé contient chaque élément du groupe avec la même multiplicité. Jusqu'à ce jour, aucune solution de ce problème n'était connue. Tout d'abord, on montre, en exhibant deux contre-exemples, que le Problème de Molluzzo n'admet pas toujours de solution positive. Ensuite, on conjecture que ce problème est vrai dans tout groupe cyclique d'ordre une puissance de premier. Dans ce chapitre, on répond positivement et complètement au Problème de Molluzzo dans tout groupe cyclique d'ordre une puissance de 3. Cette preuve est basée sur l'étude des suites arithmétiques. Les résultats obtenus permettent de prouver que, dans tout groupe cyclique d'ordre impair n, les suites arithmétiques de raison inversible sont balancées pour toutes les longueurs $m \equiv 0$ ou $-1 \pmod{\varphi(n)n}$. On prouve également que, contrairement aux groupes cycliques d'ordre impair, presqu'aucune suite arithmétique n'est balancée dans les groupes cycliques d'ordre pair. Ces résultats sur les suites arithmétiques balancées font apparaître deux fonctions arithmétiques particulières, qui sont étudiées en détail au Chapitre 5. Enfin, en annexe, sont présentés des résultats obtenus de manière expérimentale sur le Problème de Molluzzo dans les groupes cycliques d'ordre 3, 5 et 7. On y retrouve la résolution de ce Problème dans $\mathbb{Z}/3\mathbb{Z}$ par les suites arithmétiques balancées du Chapitre 4. Ces dernières permettent également de répondre partiellement au Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$. On complète alors ces solutions de manière expérimentale, ce qui permet de mettre en évidence toute la complexité du Problème de Molluzzo.

Chapitre 1

Triangles de Steinhaus binaires

Dans ce chapitre, on étudie les triangles de Steinhaus binaires. Cette construction, basée sur des suites binaires de longueur finie, est présentée à la Section 1.1, d'abord de manière élémentaire puis de manière plus rigoureuse, en définissant des outils de base qui sont utilisés par la suite. On énonce ensuite le Problème de Steinhaus, qui est un problème portant sur l'existence de triangles de Steinhaus possédant autant de 0 que de 1. A la Section 1.2, on s'intéresse à des résultats concernant la détermination du nombre d'éléments égaux à 1 dans ces triangles de Steinhaus. Enfin, à la Section 1.3, on présente quatre solutions connues et indépendantes du Problème de Steinhaus.

1.1 Le problème de Steinhaus

1.1.1 Enoncé élémentaire

En 1963, Hugo Steinhaus [23] propose la construction illustrée à la Figure 1.1 : soient 14 signes + et 14 signes − arrangés de telle sorte que sous chaque paire de signes égaux on place un signe + et sous chaque paire de signes opposés on place un signe −.

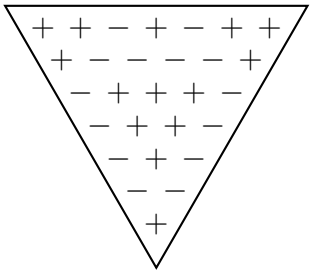


FIG. 1.1 – Un exemple de triangle de Steinhaus

Dans un tel triangle, si la première ligne comporte n signes, alors le triangle entier est composé de $\binom{n+1}{2}$ signes. Le triangle de la Figure 1.1 correspond au cas $n = 7$. Comme le coefficient binomial $\binom{n+1}{2}$ est pair si, et seulement si, $n \equiv 0$ ou $3 \pmod 4$, on peut se demander s'il est possible de construire un triangle analogue à celui de la Figure 1.1, i.e. comportant autant de signes $+$ que de signes $-$, et dont la première ligne est composée de n signes pour tout entier $n \equiv 0$ ou $3 \pmod 4$. On appelle ce problème "Problème de Steinhaus" et on verra, dans les sections suivantes, qu'il en existe de multiples solutions. Steinhaus propose la solution de la Figure 1.1 pour $n = 7$ ainsi que celles de la Figure 1.2 pour $n = 12$ et $n = 20$ à partir desquelles, en supprimant la premire ligne des triangles respectifs, on obtient des solutions pour $n = 11$ et $n = 19$.

1.1.2 Définitions et premières propriétés

Dans la suite de ce chapitre, on remplace les signes $+$ et les signes $-$ par les éléments 0 et 1 de $\mathbb{Z}/2\mathbb{Z}$, le groupe cyclique à 2 éléments. Ainsi, la relation liant deux éléments consécutifs dans une même ligne des triangles présentés à la Sous-Section 1.1.1 correspond avec la somme dans le groupe $\mathbb{Z}/2\mathbb{Z}$. On va commencer par s'intéresser aux suites de longueur finie dans $\mathbb{Z}/2\mathbb{Z}$. On introduit une opération de dérivation et une opération d'intégration sur ces suites.

Définition 1.1.1. Soit $S = (a_1, \ldots, a_n)$ une suite de longueur finie $n \geqslant 2$ dans $\mathbb{Z}/2\mathbb{Z}$. La *suite dérivée* de S est la suite ∂S définie par

$$\partial S = (a_1 + a_2, \ldots, a_{n-1} + a_n)\,,$$

où $+$ désigne la somme dans $\mathbb{Z}/2\mathbb{Z}$. C'est une suite de longueur $n-1$ dans $\mathbb{Z}/2\mathbb{Z}$. Par convention, on admet que $\partial S = \emptyset$ si la suite S est de longueur $n \leqslant 1$, où $\emptyset$ désigne la suite vide de longueur $n = 0$. Par itération du procédé de dérivation, on peut également définir récursivement la $i$ème dérivée $\partial^i S$ de la suite S par $\partial^0 S = S$ et $\partial^i S = \partial\left(\partial^{i-1} S\right)$ pour tout $i \geqslant 1$.

Les éléments de la $i$ème dérivée d'une suite S peuvent alors être exprimés en fonction des éléments de la suite S de départ.

Proposition 1.1.2. *Soit $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors, pour tout i, $0 \leqslant i \leqslant n-1$, on a*

$$\partial^i S = \left(\sum_{k=0}^{i} \binom{i}{k} a_{1+k} \;,\; \sum_{k=0}^{i} \binom{i}{k} a_{2+k} \;,\; \ldots\ldots \;,\; \sum_{k=0}^{i} \binom{i}{k} a_{n-i+k} \right).$$

Preuve. Par récurrence sur i avec la Définition 1.1.1. □

Définition 1.1.3. Soit S une suite de longueur $n \geqslant 0$ dans $\mathbb{Z}/2\mathbb{Z}$. On appelle *suite primitive* de S toute suite T de longueur $n+1$ telle que S soit sa suite dérivée, c'est-à-dire $\partial T = S$.

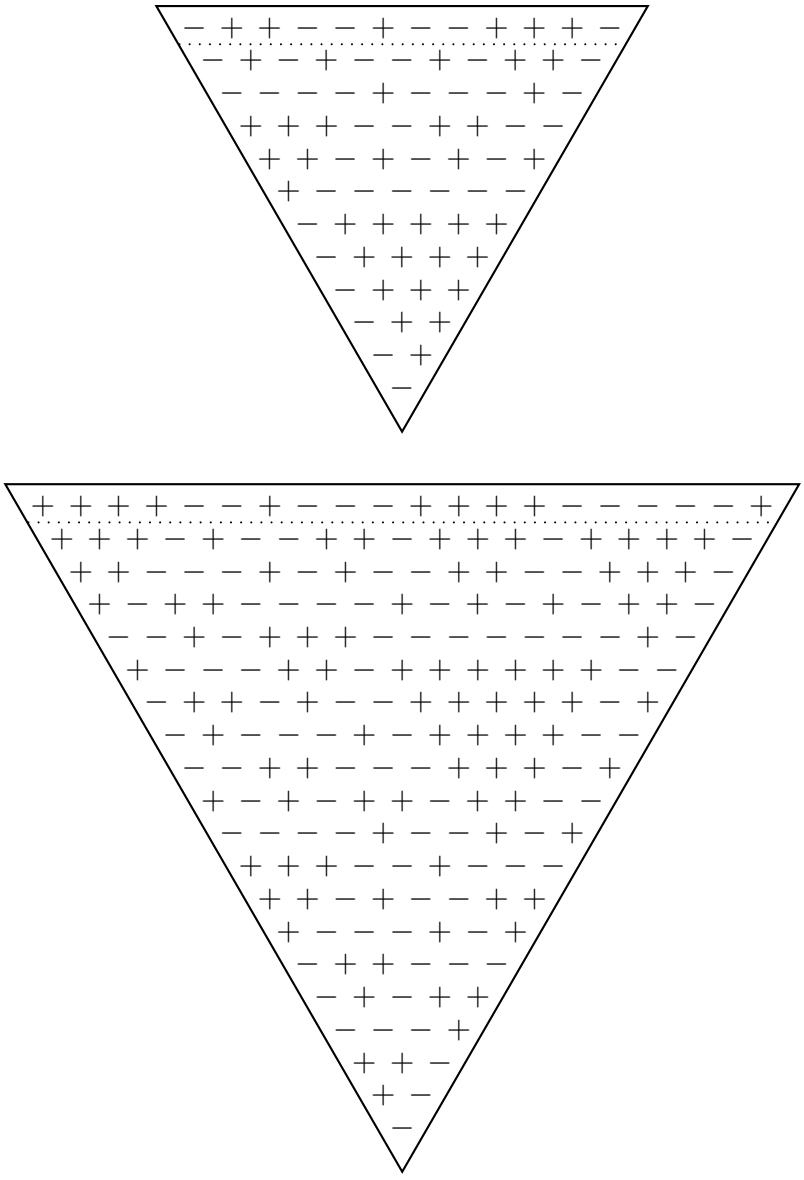


FIG. 1.2 – Solutions de Steinhaus pour $n = 11, 12, 19, 20$

Proposition 1.1.4. *Pour toute suite de longueur $n \geqslant 0$ dans $\mathbb{Z}/2\mathbb{Z}$, il existe exactement deux suites primitives. De plus, ces deux suites sont complémentaires, c'est-à-dire leur somme terme à terme est la suite constante égale à 1. On note $P_0(S)$ et $P_1(S)$ les suites primitives de S selon que le premier élément de la suite primitive soit égal à 0 ou à 1.*

Preuve. Soit $S = (a_1, \ldots, a_n)$ une suite binaire de longueur n. Si $n = 0$, alors $S = \emptyset$ et les suites (0) et (1) sont bien les primitives de S. Supposons maintenant $n \geqslant 1$ et que $T = (b_1, \ldots, b_{n+1})$ soit une suite primitive de S. Alors, pour tout j, $2 \leqslant j \leqslant n+1$, on a

$$b_1 + b_j = \sum_{k=1}^{j-1} (b_k + b_{k+1}) = \sum_{k=1}^{j-1} a_k.$$

Ainsi, on peut définir chaque b_j en fonction de b_1 et des éléments de S. Il existe donc deux suites primitives de la suite S qui sont définies par

$$P_0(S) = \left(0, a_1, a_1 + a_2, \ldots, \sum_{k=1}^{n} a_k\right),$$

$$P_1(S) = \left(1, 1 + a_1, 1 + a_1 + a_2, \ldots, 1 + \sum_{k=1}^{n} a_k\right).$$

Enfin, ces deux suites sont bien complémentaires. □

Ces deux opérations sont, en quelque sorte, réciproques. En effet, on obtient un théorème fondamental de l'analyse pour les suites binaires de longueur finie.

Proposition 1.1.5 (Théorème fondamental de l'analyse)**.** *Soient $S = (a_1, \ldots, a_n)$ une suite binaire de longueur $n \geqslant 1$ et $i \in \{0, 1\}$. Alors,*

$$\partial P_i(S) = S,$$

$$P_i(\partial S) = S + (i + a_1)_{j=1}^{n},$$

où $(i + a_1)_{j=1}^{n}$ est la suite constante égale à $i + a_1$ et de longueur n.

Preuve. Posons $P_i(S) = (b_1, \ldots, b_{n+1})$ et $\partial P_i(S) = (c_1, \ldots, c_n)$. Alors,

$$c_1 = b_1 + b_2 = i + (i + a_1) = a_1,$$

et pour tout entier j, $2 \leqslant j \leqslant n$, on a

$$c_j = b_j + b_{j+1} = \left(i + \sum_{k=1}^{j-1} a_k\right) + \left(i + \sum_{k=1}^{j} a_k\right) = a_j.$$

On obtient donc bien que $\partial P_i(S) = S$.

Posons maintenant $\partial S = (b_1, \ldots, b_{n-1})$ et $P_i(\partial S) = (c_1, \ldots, c_n)$. Alors,

$$c_1 = i = a_1 + (i + a_1),$$

et pour tout entier j, $2 \leqslant j \leqslant n$, on obtient

$$c_j = i + \sum_{k=1}^{j-1} b_k = i + \sum_{k=1}^{j-1} (a_k + a_{k+1}) = i + \sum_{k=1}^{j-1} a_k + \sum_{k=2}^{j} a_k = a_j + (i + a_1).$$

Ainsi, on a $P_i(\partial S) = S + (i + a_1)_{j=1}^{n}$. □

Ces opérations sur les suites binaires apparaissent également dans le cadre de l'étude des suites binaires pseudo-périodiques de longueur infinie [16, 20, 21].

On peut maintenant définir les triangles de Steinhaus qui ont été brièvement présentés à la Sous-Section 1.1.1.

Définition 1.1.6. Soit S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Le *triangle de Steinhaus* associé à la suite S est la collection ΔS de ses suites dérivées successives, c'est-à-dire

$$\Delta S = \left\{ \partial^i S \;\middle|\; 0 \leqslant i \leqslant n-1 \right\}.$$

On appelle *ordre* du triangle ΔS la longueur de sa suite associée S. Un triangle de Steinhaus d'ordre $n \geqslant 1$ peut alors être considéré comme un multiensemble composé de $\binom{n+1}{2}$ éléments de $\mathbb{Z}/2\mathbb{Z}$, comptés avec multiplicité.

Cette définition des triangles de Steinhaus binaires apparaît également dans [14, 17]. Par exemple, le triangle de Steinhaus ΔS d'ordre 7, associé à la suite binaire $S = (0010100)$, est représenté à la Figure 1.3.

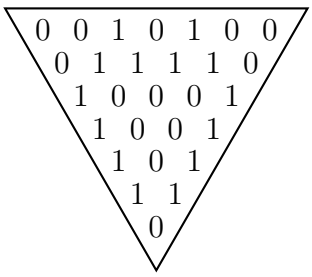


FIG. 1.3 – Le triangle de Steinhaus ΔS

Chaque triangle de Steinhaus d'ordre n étant associé bijectivement à une suite binaire de longueur n, on en déduit qu'il existe exactement 2^n triangles de Steinhaus d'ordre n distincts, pour tout entier $n \geqslant 0$.

Notation. Soit $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Pour tout i, $1 \leqslant i \leqslant n$, et tout j, $1 \leqslant j \leqslant n - i + 1$, on note $a_{i,j}$ le $j$ème élément de la $i$ème ligne du triangle ΔS d'ordre n associé à la suite S, i.e. le $j$ème de la suite dérivée $\partial^{i-1} S$. Par exemple, pour tout j, $1 \leqslant j \leqslant n$, l'élément $a_{1,j}$ correspond avec a_j, le $j$ème élément de la suite S.

Chaque élément d'un triangle de Steinhaus peut être exprimé en fonction des éléments de sa suite associée mais également en fonction des éléments du côté gauche ou du côté droit du triangle.

Proposition 1.1.7. *Soient S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$ et $\Delta S = (a_{i,j})$ son triangle de Steinhaus associé. Alors, pour tout i, $1 \leqslant i \leqslant n$, et tout j, $1 \leqslant j \leqslant n-i+1$, chaque élément $a_{i,j}$ s'exprime en fonction des éléments de la première ligne $(a_{1,1}, a_{1,2}, \ldots, a_{1,n})$, du côté gauche $(a_{1,1}, a_{2,1}, \ldots, a_{n,1})$ ou du côté droit $(a_{1,n}, a_{2,n-1}, \ldots, a_{n,1})$ du triangle ΔS de la manière suivante :*

$$a_{i,j} = \sum_{k=0}^{i-1} \binom{i-1}{k} a_{1,j+k} = \sum_{k=0}^{j-1} \binom{j-1}{k} a_{i+k,1} = \sum_{k=0}^{n-i-j+1} \binom{n-i-j+1}{k} a_{i+k,n-i-k+1}.$$

Preuve. Par récurrence. En utilisant la relation :

$$a_{i,j} + a_{i,j+1} = a_{i+1,j},$$

pour tout i, $1 \leqslant i \leqslant n-1$, et tout j, $1 \leqslant j \leqslant n-i$, provenant de la définition de ΔS. □

On s'intéresse maintenant aux suites binaires dont le triangle de Steinhaus associé possède autant de 0 que de 1.

Définition 1.1.8. Soient S une suite de longueur $n \geqslant 0$ dans $\mathbb{Z}/2\mathbb{Z}$ et ΔS son triangle de Steinhaus associé. La suite S est dite *balancée* si ΔS contient autant de 0 que de 1.

Par exemple, la suite $S = (0010100)$ de longueur $n = 7$ est balancée. En effet, comme on peut le voir à la Figure 1.3, son triangle de Steinhaus ΔS est composé de 14 éléments 0 et de 14 éléments 1.

Comme le cardinal d'un triangle de Steinhaus d'ordre n est égal à $\binom{n+1}{2}$, il clair qu'il ne peut y avoir de suite binaire balancée de longueur $n \equiv 1$ ou $2 \pmod 4$. Cela provient du fait que

$$\binom{n+1}{2} \equiv 0 \pmod 2 \iff n(n+1) \equiv 0 \pmod 4 \iff n \equiv 0 \text{ ou } 3 \pmod 4.$$

Il est alors légitime de se poser la question de savoir si cette condition nécessaire sur la longueur d'une suite binaire balancée est également suffisante.

Problème 1.1.9 (Steinhaus, 1963)**.** *Pour tout entier $n \equiv 0$ ou $3 \pmod 4$, existe-t-il une suite balancée de longueur n dans $\mathbb{Z}/2\mathbb{Z}$?*

Dans la section suivante, on s'intéresse à la détermination du nombre d'éléments égaux à 1 dans un triangle de Steinhaus. Ce qui permet, à la Section 1.3, d'expliciter plus facilement différentes solutions du Problème de Steinhaus.

1.2 Le nombre de 1 dans un triangle de Steinhaus

Notation. Soient $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$ et $\Delta S = (a_{i,j})$ son triangle de Steinhaus associé. On notera $\nu(S) = \nu(a_1, \ldots, a_n)$ le nombre d'éléments égaux à 1 dans ΔS, c'est-à-dire,

$$\nu(S) = \nu(a_1, \ldots, a_n) = \sum_{i=1}^{n} \sum_{j=1}^{n-i+1} a_{i,j},$$

où $a_{i,j}$ n'est pas considéré comme un élément de $\mathbb{Z}/2\mathbb{Z}$ mais comme un entier de $\{0, 1\}$.

Soient $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$ et $\Delta S = (a_{i,j})$ son triangle de Steinhaus associé. Tout d'abord, on peut voir que la commutativité de la somme dans $\mathbb{Z}/2\mathbb{Z}$ et la Proposition 1.1.7 entraînent une bijection entre les triangles de Steinhaus engendrés par les suites suivantes :

$$(a_{1,1}, a_{1,2}, \ldots, a_{1,n}), \quad (a_{1,1}, a_{2,1}, \ldots, a_{n,1}), \quad (a_{1,n}, a_{2,n-1}, \ldots, a_{n,1}),$$

$$(a_{1,n}, a_{1,n-1}, \ldots, a_{1,1}), \quad (a_{n,1}, a_{n-1,1}, \ldots, a_{1,1}), \quad (a_{n,1}, a_{n-1,2}, \ldots, a_{1,n}),$$

c'est-à-dire, les suites qui correspondent, selon le sens de lecture, à la première ligne, au côté gauche et au côté droit du triangle ΔS. Ceci prouve donc le résultat suivant :

Proposition 1.2.1. *Soient S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$ et $\Delta S = (a_{i,j})$ son triangle de Steinhaus associé. Alors,*

$$\begin{aligned}
\nu(S) &= \nu(a_{1,n}, a_{1,n-1}, \ldots, a_{1,1}) \\
&= \nu(a_{1,1}, a_{2,1}, \ldots, a_{n,1}) \\
&= \nu(a_{n,1}, a_{n-1,1}, \ldots, a_{1,1}) \\
&= \nu(a_{1,n}, a_{2,n-1}, \ldots, a_{n,1}) \\
&= \nu(a_{n,1}, a_{n-1,2}, \ldots, a_{1,n})
\end{aligned}$$

Pour toute suite binaire S, les éléments du triangle de Steinhaus ΔS étant construits modulo 2, il est possible d'obtenir une formule reliant la parité de $\nu(S)$ aux éléments de la suite S. Cette formule est détaillée dans le résultat suivant qui correspond au Théorème 1 de [3].

Théorème 1.2.2. *Soit $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors,*

$$\nu(S) \equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \pmod 2.$$

De plus, le nombre $\nu(S)$ est pair pour toute suite S de longueur n si, et seulement si, $n = 2^k - 2$ pour un certain $k \geqslant 2$.

La preuve qui est donnée dans ce mémoire est inspirée de [17] et utilise le théorème de Lucas dont l'énoncé est rappelé ci-dessous.

Théorème 1.2.3 (Lucas, 1878)**.** *Soient m et n deux entiers positifs et p un nombre premier. Soit*

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0, \text{ et}$$
$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0,$$

l'écriture en base p des entiers m et n. Alors,

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Preuve du Théorème 1.2.2. L'équivalence se prouve par récurrence sur n. Pour $n = 1$, il est évident que $\nu(a_1) \equiv a_1 \pmod 2$. Soit $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. On suppose le résultat prouvé pour toute suite de longueur $n-1$. On obtient alors

$$\begin{aligned}
\nu(S) &= \sum_{j=1}^{n} a_j + \nu(\partial S) = \sum_{j=1}^{n} a_j + \nu(a_1 + a_2, \ldots, a_{n-1} + a_n) \\
&\equiv \sum_{j=1}^{n} a_j + \sum_{j=1}^{n-1} \left(\binom{n}{j} - 1 \right) (a_j + a_{j+1}) \\
&\equiv \sum_{j=1}^{n} a_j + \sum_{j=1}^{n-1} \left(\binom{n}{j} - 1 \right) a_j + \sum_{j=2}^{n} \left(\binom{n}{j-1} - 1 \right) a_j \\
&\equiv n a_1 + \sum_{j=2}^{n-1} \left(\binom{n}{j} + \binom{n}{j-1} - 1 \right) a_j + n a_n \\
&\equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \pmod 2.
\end{aligned}$$

Le résultat est donc bien prouvé pour toute longueur $n \geqslant 1$. Supposons que $n = 2^k - 2$ pour un certain entier $k \geqslant 2$. Comme

$$n + 1 = 2^k - 1 = \sum_{i=0}^{k-1} 2^i,$$

on en déduit par le théorème de Lucas que

$$\binom{n+1}{j} \equiv \prod_{i=0}^{k-1} \binom{1}{j_i} \equiv 1 \pmod 2,$$

pour tout entier $j = \sum_{i=0}^{k-1} j_i 2^i \in [\![1, n]\!]$. Ainsi pour toute suite binaire $S = (a_1, \ldots, a_n)$, on obtient

$$\nu(a_1, \ldots, a_n) \equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \equiv 0 \pmod 2.$$

Supposons maintenant que $n \neq 2^k - 2$ pour tout $k \geqslant 2$. On construit une suite binaire de longueur n dont le triangle associé contient un nombre impair de 1. Considérons

$$n+1 = \sum_{i=0}^{l} n_i 2^i$$

l'écriture en base 2 de $n+1$. Comme $n+1 \neq \sum_{i=0}^{k} 2^i$ pour tout $k \geqslant 1$, alors il existe m, $0 \leqslant m \leqslant l-1$, tel que $n_m = 0$ et $n_{m+1} = 1$. Ainsi, par le théorème de Lucas, on a

$$\binom{n+1}{2^m} \equiv \left(\prod_{\substack{i=0 \\ i \neq m}}^{l} \binom{n_i}{0} \right) \binom{0}{1} \equiv 0 \pmod 2.$$

Soit $S = (a_1, \ldots, a_n)$ la suite binaire de longueur n définie par $a_j = 0$ si $j \neq 2^m$ et $a_{2^m} = 1$. Alors,

$$\nu(S) \equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \equiv \binom{n+1}{2^m} - 1 \equiv 1 \pmod 2.$$

Ce qui complète la preuve. □

Notations.

- Soient $S_1 = (a_1, \ldots, a_{n_1})$ et $S_2 = (b_1, \ldots, b_{n_2})$ deux suites binaires de longueurs n_1 et n_2 respectivement. On note

$$S_1 \cdot S_2 = S_1 S_2 = (a_1, \ldots, a_{n_1}, b_1, \ldots, b_{n_2})$$

  la concaténation des suites S_1 et S_2 qui est une suite binaire de longueur $n_1 + n_2$.
- Pour tout $k \in \mathbb{N} \cup \{\infty\}$ et toute suite S de longueur finie, on note S^k la suite S concaténée k fois, c'est-à-dire

$$S^k = \underbrace{S \cdot S \cdot S \cdots S}_{k \text{ fois}}.$$

- Pour toute suite $S = (a_1, \ldots, a_n)$, de longueur $n \in \mathbb{N} \cup \{\infty\}$, on note $S[m]$ la sous-suite initiale de S de longueur $m \leqslant n$, c'est-à-dire, $S[m] = (a_1, \ldots, a_m)$.

On rappelle maintenant un résultat de [3] et [17] qui détermine, pour tout entier $n \geqslant 1$, le plus petit et le plus grand nombre possibles d'éléments égaux à 1 dans tout triangle de Steinhaus d'ordre n.

Proposition 1.2.4. *Soit S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors,*

$$0 \leqslant \nu(S) \leqslant \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor.$$

On détaille ici la preuve de ce résultat.

Preuve. La première inégalité est évidente. En effet, par définition, pour toute suite binaire de longueur $n \geqslant 1$, on a $\nu(S) \geqslant 0$ et l'égalité est obtenue pour la suite nulle $S = (0 \dots 0)$ de longueur n.

Afin de démontrer l'autre inégalité, considérons tout d'abord, comme représenté à la Figure 1.4, les différents triangles de Steinhaus d'ordre 2. Ces triangles contiennent soit 2 éléments égaux à 1, soit aucun.

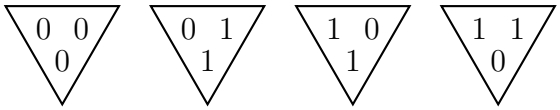


FIG. 1.4 – Triangles de Steinhaus d'ordre 2

Il est alors évident que s'il est possible de construire une suite de longueur n dont le triangle de Steinhaus d'ordre n est composé uniquement de sous-triangles d'ordre 2 qui contiennent 2 éléments égaux à 1 à chaque fois, alors le nombre maximal d'éléments égaux à 1 sera obtenu dans ce triangle.

On détaille maintenant la construction de cette suite. Posons $S = (a_1, \dots, a_n)$ une telle suite et $\Delta S = (a_{i,j})$ son triangle associé. Comme ΔS ne peut pas contenir que des éléments 1, on a $a_{i,j} = 0$ pour un certain i, $1 \leqslant i \leqslant n$, et un certain j, $1 \leqslant j \leqslant n - i + 1$. Les conditions posées sur les éléments du triangle impliquent, entre autre, qu'il ne peut y avoir deux éléments 0 voisins. On obtient donc successivement les égalités suivantes, représentées à la Figure 1.5 :

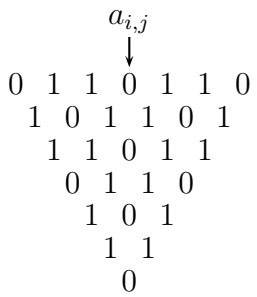


FIG. 1.5 – Structure de ΔS

$$a_{i,j} = 0 \implies a_{i,j-1} = a_{i,j+1} = 1 \implies a_{i+2,j-1} = 0 \implies a_{i+2,j-2} = a_{i+2,j} = 1$$

$$\implies \begin{cases} a_{i,j-2} = a_{i,j+2} = 1 \\ a_{i+1,j-2} = a_{i+1,j+1} = 0 \end{cases} \implies \begin{cases} a_{i+1,j-3} = a_{i+1,j+2} = 1 \\ a_{i,j-3} = a_{i,j+3} = 0 \end{cases}$$

On en déduit que $S = (\dots 0110110 \dots)$. Posons $S = (110)^\infty[n]$ de longueur $n \geqslant 1$. Calculons $\nu(S)$. On commence par déterminer explicitement chaque élément du triangle ΔS. Pour tout

i, $1 \leqslant i \leqslant n$, et tout j, $1 \leqslant j \leqslant n-i+1$, on a

$$a_{i,j} = \begin{cases} 0 \text{ pour } (i,j) \equiv (0,2),(1,0),(2,1) \pmod 3, \\ 1 \text{ pour } (i,j) \equiv (0,0),(0,1),(1,1),(1,2),(2,0),(2,2) \pmod 3. \end{cases}$$

Ce résultat se vérifie rapidement grâce à la relation :

$$a_{i,j} + a_{i,j+1} = a_{i+1,j},\ \forall 1 \leqslant i \leqslant n-1,\ \forall 1 \leqslant j \leqslant n-i.$$

De plus, on peut remarquer que, dans le triangle ΔS, trois éléments consécutifs d'une même ligne sont composés exactement de deux 1 et de un 0 :

$$(a_{i,j}, a_{i,j+1}, a_{i,j+2}) \in \{(110),(101),(011)\},\ \forall 1 \leqslant i \leqslant n-2,\ \forall 1 \leqslant j \leqslant n-i-1.$$

Si $n = 3m$, alors on a

$$\begin{aligned} \nu(S) &= \sum_{k=0}^{m-1} \left(\sum_{j=1}^{3(m-k)} a_{3k+1,j} + \sum_{j=1}^{3(m-k)-1} a_{3k+2,j} + \sum_{j=1}^{3(m-k)-2} a_{3k+3,j} \right) \\ &= \sum_{k=0}^{m-1} \big(2(m-k) + 2(m-k-1) + a_{3k+2,3(m-k)-2} + a_{3k+2,3(m-k)-1} \\ &\quad + 2(m-k-1) + a_{3k+3,3(m-k)-2} \big) \\ &= \sum_{k=1}^{m} (6k-2) = m(3m+1) = \frac{n(n+1)}{3}. \end{aligned}$$

Si $n = 3m+1$, on obtient

$$\begin{aligned} \nu(S) &= \sum_{k=0}^{m-1} \left(\sum_{j=1}^{3(m-k)+1} a_{3k+1,j} + \sum_{j=1}^{3(m-k)} a_{3k+2,j} + \sum_{j=1}^{3(m-k)-1} a_{3k+3,j} \right) + a_{3m+1,1} \\ &= \sum_{k=0}^{m-1} \big(2(m-k) + a_{3k+1,3(m-k)+1} + 2(m-k) + 2(m-k-1) \\ &\quad + a_{3k+3,3(m-k)-2} + a_{3k+3,3(m-k)-1} \big) + a_{3m+1,1} \\ &= \sum_{k=1}^{m} 6k+1 = 3m(m+1)+1 = \frac{n(n+1)+1}{3}. \end{aligned}$$

Si $n = 3m+2$, on a alors

$$\begin{aligned} \nu(S) &= \sum_{k=0}^{m-1} \left(\sum_{j=1}^{3(m-k)+2} a_{3k+1,j} + \sum_{j=1}^{3(m-k)+1} a_{3k+2,j} + \sum_{j=1}^{3(m-k)} a_{3k+3,j} \right) + a_{3m+1,1} + a_{3m+1,2} + a_{3m+2,1} \\ &= \sum_{k=0}^{m-1} \big(2(m-k) + a_{3k+1,3(m-k)+1} + a_{3k+1,3(m-k)+2} + 2(m-k) + a_{3k+2,3(m-k)+1} \\ &\quad + 2(m-k) \big) + a_{3m+1,1} + a_{3m+1,2} + a_{3m+2,1} \\ &= \sum_{k=1}^{m} 6k + 2m + 2 = (3m+2)(m+1) = \frac{n(n+1)}{3}. \end{aligned}$$

Finalement, on a bien prouvé que

$$\nu(S) = \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor.$$

De la même manière, on peut montrer que

$$\nu\left((101)^\infty[n]\right) = \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor,$$

$$\nu\left((011)^\infty[n]\right) = \begin{cases} \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor & \text{si } n \equiv 0, 2 \pmod 3, \\ \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor - 1 & \text{si } n \equiv 1 \pmod 3. \end{cases}$$

Ce qui achève la preuve. □

Déterminer toutes les valeurs possibles de $\nu(a_1, \ldots, a_n)$ pour tout entier $n \geqslant 1$ n'est pas envisageable. Cependant, Chang [3] parvient à établir les résultats qui suivent. Tout d'abord, il détermine les quatre plus petites valeurs possibles de $\nu(a_1, \ldots, a_n)$ et les suites correspondantes.

Proposition 1.2.5. *Soit S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Si $\nu(S) > 0$, alors $\nu(S) \geqslant n$. De plus, $\nu(S) = n$ si, et seulement si, S est l'une des suites suivantes :*

- $(1 \ldots 1)$,
- $(10 \ldots 0)$,
- $(0 \ldots 01)$,
- (101) *pour* $n = 3$.

Proposition 1.2.6. *Soit S une suite de longueur $n \geqslant 4$ dans $\mathbb{Z}/2\mathbb{Z}$. Si $\nu(S) > n$, alors $\nu(S) \geqslant n - 1 + \lfloor \frac{n}{2} \rfloor$. De plus, $\nu(S) = n - 1 + \lfloor \frac{n}{2} \rfloor$ si, et seulement si, S est l'une des suites suivantes :*

- $(010 \ldots 0)$ *et* $(0 \ldots 010)$,
- $(0 \ldots 011)$ *et* $(110 \ldots 0)$,
- $(01)^{\frac{n}{2}}$ *pour n pair et* $0(10)^{\frac{n-1}{2}}$ *pour n impair,*
- (001100), (001000) *et* (000100) *pour* $n = 6$,
- (0001000) *pour* $n = 7$.

Proposition 1.2.7. *Soit S une suite de longueur impaire $n > 3$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors, $\nu(S) = n - 1 + \lfloor \frac{n+1}{2} \rfloor$ si, et seulement si, S est l'une des suites suivantes :*

- $1(01)^{\frac{n-1}{2}}$,
- $(0 \ldots 011)$ *et* $(110 \ldots 0)$,
- (00100), (01100) *et* (00110) *pour* $n = 5$.

Proposition 1.2.8. *Soit S une suite de longueur $n \geqslant 7$ dans $\mathbb{Z}/2\mathbb{Z}$. Si $\nu(S) > n - 1 + \lfloor \frac{n+1}{2} \rfloor$, alors*

$$\nu(S) \geqslant \begin{cases} 2n - 4 \text{ si } n \equiv 2 \pmod 4 \text{ ou } n = 11, \\ 2n - 3 \text{ sinon.} \end{cases}$$

Chang parvient également à déterminer les deux plus grandes valeurs possibles de $\nu(a_1, \ldots, a_n)$ et les suites correspondantes.

Proposition 1.2.9. *Soit S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors $\nu(S) = \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor$ si, et seulement si, S est l'une des suites suivantes :*
- $(110)^{\frac{n}{3}}$, $(101)^{\frac{n}{3}}$ *et* $(011)^{\frac{n}{3}}$ *pour* $n \equiv 0 \pmod 3$,
- $1(101)^{\frac{n-1}{3}}$ *et* $1(011)^{\frac{n-1}{3}}$ *pour* $n \equiv 1 \pmod 3$,
- $11(011)^{\frac{n-2}{3}}$, $10(110)^{\frac{n-2}{3}}$ *et* $01(101)^{\frac{n-2}{3}}$ *pour* $n \equiv 2 \pmod 3$.

Proposition 1.2.10. *Soit S une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors $\nu(S) = \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor - 1$ si, et seulement si, S est l'une des suites suivantes :*
- (0) *pour* $n = 1$,
- (111), (010), (100) *et* (001) *pour* $n = 3$,
- (0110), (1001), (1110) *et* (0111) *pour* $n = 4$,
- (01110), (01011), (11010), (11101), (10111), (01001) *et* (10010) *pour* $n = 5$,
- $0(110)^{\frac{n-1}{3}}$ *pour* $n \equiv 1 \pmod 3$.

Proposition 1.2.11. *Soit S une suite de longueur $n \geqslant 6$ dans $\mathbb{Z}/2\mathbb{Z}$. Si $\nu(S) < \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor - 1$, alors $\nu(S) \leqslant \left\lfloor \frac{n^2+1}{3} \right\rfloor$. De plus, si $\nu(S) = \left\lfloor \frac{n^2+1}{3} \right\rfloor$, alors il ne peut y avoir trois 0 consécutifs dans la suite S, à l'exception des suites (110001) et (100011) pour $n = 6$ et des suites (110001110) et (011100011) pour $n = 9$.*

La fin de cette section est consacrée à la détermination du nombre moyen d'éléments égaux à 1 dans un triangle de Steinhaus d'ordre n.

Notation. On note $\mathfrak{m}(n)$ le nombre moyen d'éléments égaux à 1 dans un triangle de Steinhaus d'ordre $n \geqslant 1$, c'est-à-dire le rapport entre le nombre total d'éléments égaux à 1 dans l'ensemble des triangles de Steinhaus d'ordre n et le nombre de triangles d'ordre n.

Proposition 1.2.12. *Pour tout entier $n \geqslant 1$, on a*

$$\mathfrak{m}(n) = \frac{1}{2}\binom{n+1}{2}.$$

Preuve. Montrons, par récurrence sur n, que le nombre total d'éléments égaux à 1 dans l'ensemble des triangles d'ordre n est égal à $2^{n-1}\binom{n+1}{2}$. Pour $n = 1$, il n'y a que deux triangles de Steinhaus, qui sont (0) et (1). On obtient bien que $\mathfrak{m}(1) = \frac{1}{2}$. Supposons maintenant que le résultat soit vrai pour $n-1$ et montrons le pour n. Par la Proposition 1.1.4, chaque suite binaire S de longueur $n-1$ admet 2 suites primitives $P_0(S)$ et $P_1(S)$ complémentaires. Comme l'ensemble des 2 suites complémentaires comporte n fois l'élément 1, on en déduit que

$$\nu\left(P_0(S)\right) + \nu\left(P_1(S)\right) = n + 2\nu(S),$$

et donc, par l'hypothèse de récurrence, le nombre de 1 dans l'ensemble des triangles d'ordre n est égal à

$$2^{n-1}n + 2 \times 2^{n-2}\binom{n}{2} = 2^{n-1}\binom{n+1}{2}.$$

Comme il existe 2^n triangles d'ordre n, on en conclut que

$$\mathfrak{m}(n) = \frac{1}{2}\binom{n+1}{2}.$$

□

Le Problème de Steinhaus peut alors être reformulé de la manière suivante : pour tout entier $n \equiv 0$ ou $3 \pmod 4$, existe-t-il une suite binaire de longueur n dont le triangle de Steinhaus associé contienne un nombre moyen d'éléments égaux à 1 ?

1.3 Solutions du Problème de Steinhaus

Dans cette section, quatre solutions complètes et indépendantes du Problème de Steinhaus sont présentées. On s'attarde surtout sur celle de Harborth [17] qui, historiquement, fut la première à paraître. La seconde, due à Eliahou et Hachez [14], est obtenue grâce à la considération de suites binaires fortement balancées. Enfin, les deux dernières solutions sont basées sur l'étude de suites binaires possédant des propriétés supplémentaires telles que la symétrie, l'antisymétrie ou le fait d'être de poids moyen [13, 15].

1.3.1 Solution de Harborth

Cette solution, parue en 1972, est basée sur la construction ingénieuse de suites binaires balancées de nature pseudo-périodiques. Dans cette sous-section, la preuve de la solution de Harborth est réécrite afin d'utiliser les résultats de la Section 1.2 mais en conservant les idées de base.

On procède par étapes :

1ère étape : Soit p un entier positif multiple de 4. On commence par déterminer l'ensemble E_1^p défini par

$$E_1^p = \left\{ (a_1, \ldots, a_p) \in (\mathbb{Z}/2\mathbb{Z})^p \;\middle|\; \partial^p(a_1, \ldots, a_p)^k = (a_1, \ldots, a_p)^{k-1},\ \forall k \geqslant 1 \right\},$$

pour les premières valeurs de p. Tout d'abord, par définition de l'opération de dérivation, il est clair que

$$\left(\partial^p(a_1, \ldots, a_p)^k = (a_1, \ldots, a_p)^{k-1},\ \forall k \geqslant 1 \right) \iff \left(\partial^p(a_1, \ldots, a_p)^2 = (a_1, \ldots, a_p) \right)$$

Soit $S = (a_1, \ldots, a_{2p}) = (a_1, \ldots, a_p)^2$ une suite binaire de longueur $2p$ telle que

$$\partial^p S = (a_1, \ldots, a_p).$$

Par la Proposition 1.1.2, cette équation est équivalente à

$$\sum_{k=0}^{p-1} \binom{p}{k} a_{j+k} = 0, \ \forall 1 \leqslant j \leqslant p.$$

Pour $p = 4$ et $p = 8$, on obtient que $a_j = 0$ pour tout j, $1 \leqslant j \leqslant p$. La suite S est alors la suite nulle et donc

$$E_1^4 = \{(0000)\},$$
$$E_1^8 = \{(00000000)\}.$$

Pour $p = 12$, on obtient le système suivant :

$$\begin{cases} a_1 + a_5 + a_9 = 0 \\ a_2 + a_6 + a_{10} = 0 \\ a_3 + a_7 + a_{11} = 0 \\ a_4 + a_8 + a_{12} = 0 \end{cases}$$

Chacune de ces équations possède 4 solutions dans $\mathbb{Z}/2\mathbb{Z}$. Ainsi,

$$E_1^{12} = \{(a_1, \ldots, a_{12}) \mid \{a_j, a_{j+4}, a_{j+8}\} \in \{\{0,0,0\}, \{0,1,1\}, \{1,0,1\}, \{1,1,0\}\}, \ \forall 1 \leqslant j \leqslant 4\}.$$

L'ensemble E_1^{12} est donc composé de $4^4 = 256$ 12-uplets distincts. Dans la suite de cette sous-section, on pose $p = 12$ et $E_1 = E_1^{12}$.

2ème étape : On cherche s'il existe des 12-uplets de E_1 qui engendrent des suites périodiques balancées, c'est-à-dire, les 12-uplets $(a_1, \ldots, a_{12})$ de E_1 tel que la suite $(a_1, \ldots, a_{12})^k$ soit balancée pour tout entier $k \geqslant 1$. Commençons par examiner le cas $k = 1$.

Proposition 1.3.1. *Soit $S = (a_1, \ldots, a_{12})$ dans E_1. Alors, la suite S n'est pas balancée.*

Preuve. Soit $S = (a_1, \ldots, a_{12})$ dans E_1. Par le Théorème 1.2.2, on a

$$\nu(S) \equiv \sum_{j=1}^{12} \left(\binom{13}{j} - 1 \right) a_j \equiv a_2 + a_3 + a_6 + a_7 + a_{10} + a_{11} \pmod 2.$$

Par définition des éléments de E_1, on sait que $a_2 + a_6 + a_{10} \equiv 0 \pmod 2$ et $a_3 + a_7 + a_{11} \equiv 0 \pmod 2$, donc $\nu(S)$ est pair. De plus, si la suite S est balancée, alors $\nu(S) = \mathfrak{m}(12) = \frac{1}{2}\binom{13}{2} = 39$, ce qui contredit la parité de $\nu(S)$. On en conclut qu'aucune des 256 suites de E_1 ne peut être balancée. □

3ème étape : Soit $S = (a_1, \ldots, a_{12})^k$ avec $(a_1, \ldots, a_{12})$ un 12-uplet de E_1 et $k \geqslant 1$ un entier. Soient a et b les entiers définis par

$$a = \nu((a_1, \ldots, a_{12})),$$
$$b = \nu((a_1, \ldots, a_{12})^2) - 3\nu((a_1, \ldots, a_{12})).$$

On considère alors le découpage du triangle de Steinhaus ΔS représenté à la Figure 1.6.

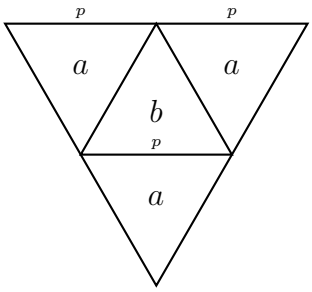


FIG. 1.6 – Structure de ΔS

Le nombre de 1 dans ΔS peut ainsi être exprimé en fonction des quantités a et b de la manière suivante :

$$\begin{aligned}\nu(S) &= (a+b)\binom{k}{2} + ka = (a+b)\left(\frac{1}{144}\binom{12k+1}{2} - \frac{13}{24}k\right) + ka \\ &= \frac{a+b}{144}\binom{12k+1}{2} + \frac{11a-13b}{24}k\end{aligned}$$

Si

$$\frac{a+b}{144} = \frac{1}{2},$$

alors le nombre de 1 dans ΔS ne diffère du nombre moyen de 1 dans un triangle d'ordre $12k$ que d'un seul terme, linéaire en k, à savoir

$$\nu((a_1,\ldots,a_{12})^k) = \mathfrak{m}(12k) + \frac{11a-13b}{24}k.$$

On pose

$$E_2 = \left\{(a_1,\ldots,a_{12}) \in E_1 \;\middle|\; \frac{a+b}{144} = \frac{1}{2}\right\}.$$

L'ensemble E_2 est constitué des 60 12-uplets de E_1 suivants :

(000001110111)	(001101010110)	(011001000010)	(100110010000)	(110011110011)
(000010011001)	(001110111000)	(011010101100)	(100111100111)	(110100101111)
(000011101110)	(001111001111)	(011100000111)	(101000101000)	(110101011000)
(000100110010)	(010000100110)	(011101110000)	(101001011111)	(110111000001)
(000101000101)	(010001010001)	(011110011110)	(101010110001)	(111000001110)
(000110101011)	(010010111111)	(011111101001)	(101011000110)	(111001111001)
(000111011100)	(010011001000)	(100000111011)	(101100011010)	(111010010111)
(001000010011)	(010100010100)	(100001001100)	(101110000011)	(111011100000)
(001001100100)	(010101100011)	(100010100010)	(101111110100)	(111100111100)
(001010001010)	(010110001101)	(100011010101)	(110000011101)	(111101001011)
(001011111101)	(010111111010)	(100100001001)	(110001101010)	(111110100101)
(001100100001)	(011000110101)	(100101111110)	(110010000100)	(111111010010)

4ème étape : On va maintenant corriger ce terme linéaire en k pour au moins une des 60 suites de E_2 afin d'obtenir des suites balancées pour toutes les longueurs admissibles.

Pour tout entier positif $r \in \{3, 4, 7, 8, 11, 12\}$, on pose

$$E_3^r = \left\{ (a_1, \ldots, a_{12}, a_{13}, \ldots, a_{12+r}) \;\middle|\; \begin{array}{l} (a_1, \ldots, a_{12}) \in E_2 \\ \partial^{12}(a_1, \ldots, a_{12+r}) = (a_{13}, \ldots, a_{12+r}) \\ (a_1, \ldots, a_{12+r}) \text{ et } (a_{13}, \ldots, a_{12+r}) \text{ balancées} \end{array} \right\}.$$

Proposition 1.3.2. *Si* $(a_1, \ldots, a_{12}, a_{13}, \ldots, a_{12+r}) \in E_3^r$, *alors* $(a_1, \ldots, a_{12})^k \cdot (a_{13}, \ldots, a_{12+r})$ *est balancée pour tout* $k \geqslant 0$.

Preuve. Par récurrence sur k. Par définition de l'ensemble E_3^r, le résultat est vrai pour $k = 0$ et $k = 1$. Soit maintenant $k \geqslant 2$ et $S = (a_1, \ldots, a_{12})^k \cdot (a_{13}, \ldots, a_{12+r})$ avec $(a_1, \ldots, a_{12+r}) \in E_3^r$. On considère le découpage du triangle de Steinhaus ΔS représenté à la Figure 1.7, où les entiers a, b, c et d sont définis par

$$\begin{array}{l} a = \nu((a_1, \ldots, a_{12})), \\ b = \nu((a_1, \ldots, a_{12})^2) - 3\nu((a_1, \ldots, a_{12})), \\ c = \nu((a_{13}, \ldots, a_{12+r})), \\ d = \nu((a_1, \ldots, a_{12+r})) - \nu((a_1, \ldots, a_{12})) - \nu((a_{13}, \ldots, a_{12+r})). \end{array}$$

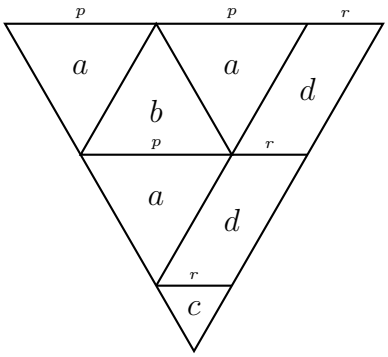


FIG. 1.7 – Structure de ΔS

De plus, on a

$$\begin{array}{rcl} (a_1, \ldots, a_{12}) \in E_2 & \Longrightarrow & a + b = 72, \\ (a_{13}, \ldots, a_{12+r}) \text{ balancée} & \Longleftrightarrow & c = \frac{1}{2}\binom{r+1}{2}, \\ (a_1, \ldots, a_{12+r}) \text{ balancée} & \Longleftrightarrow & a + d + c = \frac{1}{2}\binom{r+13}{2}. \end{array}$$

Supposons que le résultat soit vrai pour $k - 1$. Alors, on obtient

$$\begin{aligned} \nu(S) &= \frac{1}{2}\binom{12(k-1)+r+1}{2} + (k-1)(a+b) + (a+d) \\ &= \frac{1}{2}\binom{12(k-1)+r+1}{2} + 72(k-1) + \frac{1}{2}\binom{r+13}{2} - \frac{1}{2}\binom{r+1}{2} \\ &= \frac{1}{2}\binom{12k+r+1}{2}. \end{aligned}$$

Ce qui conclut la preuve. □

Soient $(a_1, \ldots, a_{12})$ l'un des 60 éléments de E_2 et $(a_{13}, \ldots, a_{12+r})$ une suite balancée de longueur r. Soient a, b, c et d les entiers définis précédemment. Afin de déterminer l'ensemble E_3^r, il suffit donc de vérifier $60 \times b(r)$ fois l'égalité

$$a + c + d = \frac{1}{2}\binom{13+r}{2},$$

où $b(r)$ est le nombre de suites balancées de longueur r. Ce nombre de tests peut être réduit dans certains cas. Tout d'abord, pour $r \geqslant 5$, on obtient la proposition suivante.

Proposition 1.3.3. *Soit $(a_1, \ldots, a_{12}, a_{13}, \ldots, a_{12+r})$ dans E_3^r avec $r \geqslant 5$. Alors,*

$$a_{j+12} = a_j, \ \forall 1 \leqslant j \leqslant r-4.$$

Preuve. De l'égalité

$$\partial^{12}(a_1, \ldots, a_{12+r}) = (a_{13}, \ldots, a_{12+r}),$$

on déduit que

$$a_j + a_{j+4} + a_{j+8} = 0, \forall 1 \leqslant j \leqslant r.$$

Pour tout j, $1 \leqslant j \leqslant r-4$, on obtient alors

$$a_{j+12} = a_{j+8} + a_{j+4} = a_j.$$

□

Enfin, en comparant le nombre de 1 dans les triangles associés aux suites $(a_1, \ldots, a_{12+r})$ et $(a_{13}, \ldots, a_{12+r})$ pour $(a_1, \ldots, a_{12+r})$ dans E_3^r, on obtient la relation suivante.

Proposition 1.3.4. *Soit $(a_1, \ldots, a_{12+r})$ un élément de E_3^r. Alors,*

$$\sum_{j=1}^{12}\binom{13+r}{j}a_j + \sum_{j=13}^{12+r}\left(\binom{13+r}{j} + \binom{r+1}{j-12}\right)a_j \equiv 1 \pmod 2.$$

Preuve. Tout d'abord, comme $r \equiv 0$ ou $3 \pmod 4$, on a

$$\frac{1}{2}\binom{r+13}{2} = \frac{1}{2}\binom{r+1}{2} + 3(r+1) + 3(r+12),$$

ce qui entraîne que

$$\nu(a_1, \ldots, a_{12+r}) + \nu(a_{13}, \ldots, a_{12+r}) = \frac{1}{2}\binom{r+13}{2} + \frac{1}{2}\binom{r+1}{2} \equiv 1 \pmod 2.$$

De plus, par le Théorème 1.2.2, on obtient

$$\begin{aligned}\nu(a_1, \ldots, a_{12+r}) + \nu(a_{13}, \ldots, a_{12+r}) &\equiv \sum_{j=1}^{12+r}\left(\binom{13+r}{j} - 1\right)a_j + \sum_{j=13}^{12+r}\left(\binom{r+1}{j-12} - 1\right)a_j \\ &\equiv \sum_{j=1}^{12}\left(\binom{13+r}{j} - 1\right)a_j + \sum_{j=13}^{12+r}\left(\binom{13+r}{j} + \binom{r+1}{j-12}\right)a_j \pmod 2.\end{aligned}$$

Enfin, comme $(a_1, \ldots, a_{12}) \in E_1$, on a $\sum_{j=1}^{12} a_j \equiv 0 \pmod 2$ et la relation recherchée s'ensuit.

□

5ème étape : On va déterminer l'ensemble E_3^r pour les différentes valeurs de r.

r = 4 : Il y a $b(4) = 6$ suites balancées de longueur 4. Soit $S = (a_1, \ldots, a_{16})$ un élément de E_3^4. La Proposition 1.3.4 implique la relation

$$1 \equiv \sum_{j=1}^{12} \binom{17}{j} a_j + \sum_{j=13}^{16} \left(\binom{17}{j} + \binom{5}{j-12} \right) a_j \equiv a_1 + a_{13} \pmod 2.$$

Il y a alors 38 éléments distincts dans E_3^4. Ainsi, les suites pseudo-périodiques de période 12 et de longueur $n \equiv 4 \pmod{12}$ suivantes sont balancées :

$(000001110111)^k \cdot (1010)$	$(010111111010)^k \cdot (1100)$	$(101111110100)^k \cdot (0100)$
$(000001110111)^k \cdot (1100)$	$(011000110101)^k \cdot (1100)$	$(110000011101)^k \cdot (0100)$
$(000101000101)^k \cdot (1010)$	$(100001001100)^k \cdot (0011)$	$(110010000100)^k \cdot (0101)$
$(000101000101)^k \cdot (1100)$	$(100001001100)^k \cdot (0101)$	$(110011110011)^k \cdot (0101)$
$(001000010011)^k \cdot (1100)$	$(100010100010)^k \cdot (0101)$	$(110100101111)^k \cdot (0010)$
$(001010001010)^k \cdot (1100)$	$(100011010101)^k \cdot (0010)$	$(110101011000)^k \cdot (0010)$
$(001100100001)^k \cdot (1010)$	$(101000101000)^k \cdot (0100)$	$(110101011000)^k \cdot (0101)$
$(001111001111)^k \cdot (1010)$	$(101010110001)^k \cdot (0101)$	$(110111000001)^k \cdot (0101)$
$(010001010001)^k \cdot (1010)$	$(101100011010)^k \cdot (0100)$	$(111100111100)^k \cdot (0100)$
$(010010111111)^k \cdot (1010)$	$(101101001111)^k \cdot (0011)$	$(111101001011)^k \cdot (0011)$
$(010010111111)^k \cdot (1100)$	$(101101001111)^k \cdot (0100)$	$(111110100101)^k \cdot (0010)$
$(010100010100)^k \cdot (1100)$	$(101110000011)^k \cdot (0011)$	$(111110100101)^k \cdot (0100)$
$(010110001101)^k \cdot (1010)$	$(101111110100)^k \cdot (0011)$	

r = 3 : Il y a $b(3) = 4$ suites balancées de longueur 3. Soit $S = (a_1, \ldots, a_{15})$ dans E_3^3. La Proposition 1.3.4 entraîne la contradiction

$$1 \equiv \sum_{j=1}^{12} \binom{16}{j} a_j + \sum_{j=13}^{15} \left(\binom{16}{j} + \binom{4}{j-12} \right) a_j \equiv 0 \pmod 2.$$

On en déduit que

$$E_3^3 = \emptyset.$$

On peut alors rechercher des suites balancées de longueur $n \equiv 3 \pmod{12}$ parmi les suites dérivées des suites balancées de longueur $n \equiv 4 \pmod{12}$. En effet, si S est une suite balancée de longueur $n \geqslant 2$ et qui, de plus, contient le même nombre de 0 que de 1, alors sa suite dérivée ∂S est une suite balancée de longueur $n - 1$. On obtient ainsi 8 suites balancées de longueur $n \equiv 3 \pmod{12}$:

$(000010011001)^k \cdot (000010011000010)$	$(101001011111)^k \cdot (101001011110010)$
$(000010011001)^k \cdot (000010011000111)$	$(110010000100)^k \cdot (110010000101010)$
$(011001000010)^k \cdot (011001000011111)$	$(111010010111)^k \cdot (111010010110111)$
$(011111101001)^k \cdot (011111101000111)$	$(111111010010)^k \cdot (111111010011111)$

Ces solutions sont de la forme représentée à la Figure 1.7 avec $r = 15$ mais avec un chevauchement. En effet, il faut que $\nu(a_{25}, a_{26}, a_{27}) = 3$. On peut alors, en rajoutant cette condition, construire l'ensemble que l'on notera E_3^{15} et qui détermine 26 suites balancées de longueur $n \equiv 3 \pmod{12}$ de plus :

$$\begin{array}{ll}
(000001110111)^k \cdot (000001110110001) & (011100000111)^k \cdot (011100000110010) \\
(000011101110)^k \cdot (000011101111010) & (011101110000)^k \cdot (011101110001010) \\
(000011101110)^k \cdot (000011101111100) & (011111101001)^k \cdot (011111101000100) \\
(000101000101)^k \cdot (000101000100100) & (100000111011)^k \cdot (100000111010100) \\
(000101000101)^k \cdot (000101000100111) & (100101111110)^k \cdot (100101111111100) \\
(000110101011)^k \cdot (000110101010001) & (101010110001)^k \cdot (101010110000100) \\
(000111011100)^k \cdot (000111011101001) & (101011000110)^k \cdot (101011000111100) \\
(001011111101)^k \cdot (001011111100001) & (101100011010)^k \cdot (101100011011100) \\
(001110111000)^k \cdot (001110111001001) & (101110000011)^k \cdot (101110000010001) \\
(011000110101)^k \cdot (011000110100001) & (110000011101)^k \cdot (110000011100111) \\
(011000110101)^k \cdot (011000110100100) & (110001101010)^k \cdot (110001101011111) \\
(011001000010)^k \cdot (011001000011001) & (110100101111)^k \cdot (110100101110001) \\
(011010101100)^k \cdot (011010101101010) & (110111000001)^k \cdot (110111000000111)
\end{array}$$

r = 7 : Il y a $b(7) = 12$ suites balancées de longueur 7. Soit $S = (a_1, \ldots, a_{19})$ dans E_3^7. La Proposition 1.3.4 implique la relation

$$1 \equiv \sum_{j=1}^{12} \binom{20}{j} a_j + \sum_{j=13}^{19} \left(\binom{20}{j} + \binom{8}{j-12} \right) a_j \equiv a_4 + a_{16} \pmod{2},$$

et la Proposition 1.3.3 entraîne les égalités

$$a_{12+j} = a_j, \ \forall 1 \leqslant j \leqslant 3.$$

Il y a alors 7 éléments distincts dans E_3^7. Ainsi, les suites pseudo-périodiques de période 12 et de longueur $n \equiv 7 \pmod{12}$ suivantes sont balancées :

$$\begin{array}{ll}
(010000100110)^k \cdot (0101011) & (101011000110)^k \cdot (1011111) \\
(010101100011)^k \cdot (0100001) & (110001101010)^k \cdot (1101010) \\
(011010101100)^k \cdot (0111100) & (111011100000)^k \cdot (1111101) \\
(100100001001)^k \cdot (1000010) &
\end{array}$$

r = 8 : Il y a $b(8) = 40$ suites balancées de longueur 8. Soit $S = (a_1, \ldots, a_{20})$ dans E_3^8. La Proposition 1.3.4 implique la relation

$$1 \equiv \sum_{j=1}^{12} \binom{21}{j} a_j + \sum_{j=13}^{20} \left(\binom{21}{j} + \binom{9}{j-12} \right) a_j \equiv a_1 + a_4 + a_5 + a_{13} + a_{16} + a_{17} \pmod{2},$$

et la Proposition 1.3.3 entraîne les égalités

$$a_{12+j} = a_j, \ \forall 1 \leqslant j \leqslant 4.$$

En combinant les deux, on obtient

$$a_5 + a_{17} = 1.$$

Il y a alors 20 éléments distincts dans E_3^8. Ainsi, les suites pseudo-périodiques de période 12 et de longueur $n \equiv 8 \pmod{12}$ suivantes sont balancées :

$$\begin{array}{ll}
(000001110111)^k \cdot (00001011) & (100001001100)^k \cdot (10001010) \\
(000001110111)^k \cdot (00001101) & (101000101000)^k \cdot (10101111) \\
(010001010001)^k \cdot (01001000) & (101100011010)^k \cdot (10111011) \\
(010010111111)^k \cdot (01000011) & (101110000011)^k \cdot (10110000) \\
(010011001000)^k \cdot (01000010) & (101111110100)^k \cdot (10110000) \\
(010011001000)^k \cdot (01000101) & (110011110011)^k \cdot (11000100) \\
(010100010100)^k \cdot (01011010) & (110100101111)^k \cdot (11011101) \\
(010110001101)^k \cdot (01010111) & (110101011000)^k \cdot (11011101) \\
(010111111010)^k \cdot (01010001) & (110111000001)^k \cdot (11010000) \\
(010111111010)^k \cdot (01010110) & (111110100101)^k \cdot (11110011)
\end{array}$$

Aucune des suites dérivées de ces solutions ne fournit de suite balancée de longueur $n \equiv 7 \pmod{12}$.

r = 11 : Il y a $b(11) = 171$ suites balancées de longueur 11. Soit $S = (a_1, \ldots, a_{23})$ dans E_3^{11}. La Proposition 1.3.4 implique la relation

$$1 \equiv \sum_{j=1}^{12} \binom{24}{j} a_j + \sum_{j=13}^{23} \left(\binom{24}{j} + \binom{12}{j-12} \right) a_j \equiv a_8 + a_{20} \pmod{2},$$

et la Proposition 1.3.3 entraîne les égalités

$$a_{12+j} = a_j, \ \forall 1 \leqslant j \leqslant 7.$$

Il y a alors 18 éléments distincts dans E_3^{11}. Ainsi, les suites pseudo-périodiques de période 12 et de longueur $n \equiv 11 \pmod{12}$ suivantes sont balancées :

$$\begin{array}{ll}
(001001100100)^k \cdot (00100111000) & (011010101100)^k \cdot (01101011111) \\
(001011111101)^k \cdot (00101110001) & (100101111110)^k \cdot (10010110000) \\
(001101010110)^k \cdot (00110100001) & (100101111110)^k \cdot (10010110011) \\
(001110111000)^k \cdot (00111010000) & (100110010000)^k \cdot (10011000010) \\
(010000100110)^k \cdot (01000011001) & (101011000110)^k \cdot (10101101010) \\
(010001010001)^k \cdot (01000100100) & (110001101010)^k \cdot (11000111100) \\
(010100010100)^k \cdot (01010000101) & (111000001110)^k \cdot (11100001101) \\
(010100010100)^k \cdot (01010000110) & (111010010111)^k \cdot (11101000100) \\
(010101100011)^k \cdot (01010111011) & (111010010111)^k \cdot (11101000111)
\end{array}$$

r = 12 : Il y a $b(12) = 410$ suites balancées de longueur 12. Soit $S = (a_1, \ldots, a_{24})$ dans E_3^{12}. La Proposition 1.3.4 implique la relation

$$1 \equiv \sum_{j=1}^{12} \binom{25}{j} a_j + \sum_{j=13}^{24} \left(\binom{25}{j} + \binom{13}{j-12} \right) a_j \equiv a_1 + a_8 + a_9 + a_{13} + a_{20} + a_{21} \pmod{2},$$

et la Proposition 1.3.3 entraîne les égalités

$$a_{12+j} = a_j, \ \forall 1 \leqslant j \leqslant 8.$$

En combinant les deux, on obtient

$$a_9 + a_{21} = 1.$$

Il y a alors 18 éléments distincts dans E_3^{12}. Ainsi, les suites pseudo-périodiques de période 12 et de longueur $n \equiv 0 \pmod{12}$ suivantes sont balancées :

$$\begin{array}{ll}
(000101000101)^k \cdot (000101001000) & (010111111010)^k \cdot (010111110111) \\
(000101000101)^k \cdot (000101001110) & (011000110101)^k \cdot (011000111111) \\
(010001010001)^k \cdot (010001011010) & (011001000010)^k \cdot (011001001110) \\
(010001010001)^k \cdot (010001011100) & (101000101000)^k \cdot (101000100101) \\
(010010111111)^k \cdot (010010110011) & (101001011111)^k \cdot (101001010100) \\
(010011001000)^k \cdot (010011000011) & (101100011010)^k \cdot (101100010000) \\
(010100010100)^k \cdot (010100010100) & (110010000100)^k \cdot (110010001001) \\
(010100010100)^k \cdot (010100011111) & (110011110011)^k \cdot (110011111000) \\
(010110001101)^k \cdot (010110000111) & (110111000001)^k \cdot (110111000001)
\end{array}$$

Parmi les suites dérivées de ces solutions, il y a une suite balancée de longueur $n \equiv 11 \pmod{12}$.

On vient donc bien de prouver que pour tout entier $n \equiv 0$ ou $3 \pmod 4$, il existe au moins 4 suites balancées de longueur n.

1.3.2 Solution de Eliahou-Hachez

Cette seconde solution, parue en 2004 [14], est basée sur l'étude des suites binaires fortement balancées. Les principaux résultats sont rappelés ici.

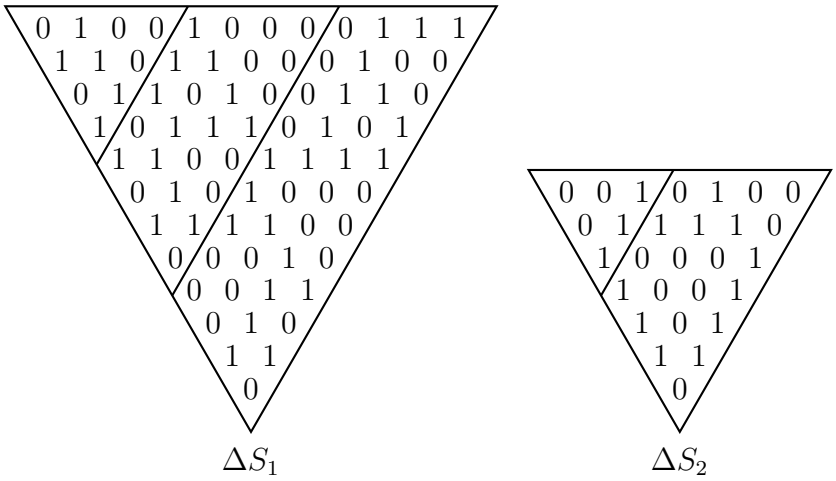
Définition 1.3.5. Une suite $(a_1, \ldots, a_n)$ de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$ est dite *fortement balancée* si la sous-suite initiale $(a_1, \ldots, a_{n-4t})$ est balancée pour tout entier t, $0 \leqslant t < \frac{n}{4}$.

Les suites binaires balancées de longueur $n = 3$ ou 4 sont donc, par définition, des suites fortement balancées. Pour $n \geqslant 7$, on peut alors définir de manière récursive la notion de suite fortement balancée grâce au résultat suivant.

Proposition 1.3.6. *Soit $(a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 7$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors,*

$$(a_1, \ldots, a_n) \text{ fortement balancée} \iff \begin{cases} (a_1, \ldots, a_n) \text{ balancée,} \\ (a_1, \ldots, a_{n-4}) \text{ fortement balancée.} \end{cases}$$

Par exemple, comme illustré à la Figure 1.8, les suites $S_1 = (010010000111)$ et $S_2 = (0010100)$ sont fortement balancées. En effet, les sous-suites initiales de S_1 et S_2, c'est-à-dire les suites (0100), (01001000), S_1 et (001), S_2 respectivement, sont des suites binaires balancées.



ΔS_1 ΔS_2

FIG. 1.8 – Triangles associés à des suites fortement balancées

Notation. Pour tout entier $n \geqslant 0$, on note $fb(n)$ le nombre de suites fortement balancées de longueur n dans $\mathbb{Z}/2\mathbb{Z}$.

Il est clair que $fb(n) = 0$ pour tout entier $n \equiv 1$ ou $2 \pmod 4$ puisqu'il n'existe pas de suite balancée pour ces longueurs. Rien ne permet de prévoir l'existence de telles suites pour toutes les longueurs n possibles, c'est-à-dire pour tout $n \equiv 0$ ou $3 \pmod 4$. Cependant, à l'aide de l'algorithme suggéré par la Proposition 1.3.6, on peut déterminer [14] la fonction génératrice $g(t) = \sum_{n=0}^{+\infty} fb(n)t^n$ du nombre $fb(n)$ de suites binaires fortement balancées de longueur n.

Théorème 1.3.7. *La fonction génératrice $g(t) = \sum_{n=0}^{+\infty} fb(n)t^n$ du nombre $fb(n)$ de suites binaires fortement balancées de longueur n est la fonction rationnelle suivante :*

$$g(t) = \frac{4t^{92}}{1-t^4} + f_0(t) + \left(14 + 12t^4 + 14t^8\right)\frac{t^{27}}{1-t^{12}} + f_3(t),$$

où $f_0(t)$ et $f_3(t)$ sont les fonctions polynomiales suivantes :

$$\begin{aligned} f_0(t) = \; & 1 + 6t^4 + 18t^8 + 30t^{12} + 52t^{16} + 80t^{20} + 88t^{24} + 106t^{28} + 116t^{32} \\ & + 124t^{36} + 106t^{40} + 92t^{44} + 92t^{48} + 90t^{52} + 64t^{56} + 44t^{60} \\ & + 38t^{64} + 32t^{68} + 20t^{72} + 20t^{76} + 8t^{80} + 8t^{84} + 6t^{88}, \end{aligned}$$

$$\begin{aligned} f_3(t) = \; & 4t^3 + 8t^7 + 16t^{11} + 26t^{15} + 36t^{19} + 48t^{23} + 48t^{27} + 66t^{31} + 88t^{35} \\ & + 108t^{39} + 114t^{43} + 90t^{47} + 88t^{51} + 104t^{55} + 92t^{59} + 60t^{63} \\ & + 48t^{67} + 28t^{71} + 26t^{75} + 26t^{79} + 20t^{83} + 16t^{87} + 18t^{91} + 14t^{95} \\ & + 14t^{99} + 14t^{103} + 14t^{107} + 16t^{111} + 14t^{115} + 14t^{119} + 16t^{123}. \end{aligned}$$

Remarque. La pseudo-périodicité des valeurs $fb(n)$ se retrouve dans le caractère rationnel de la fonction génératrice g.

On va maintenant présenter de manière explicite l'ensemble des suites fortement balancées de longueur $n \geqslant 92$ pour $n \equiv 0 \pmod 4$, et $n \geqslant 127$ pour $n \equiv 3 \pmod 4$. Commençons par les suites de longueur $n \equiv 0 \pmod 4$.

Théorème 1.3.8. *Soient Q_1, Q_2, Q_3 et Q_4 les suites binaires infinies, pseudo-périodiques de période 12, définies par*

$$\begin{aligned} Q_1 &= (0100) \cdot (001001011100)^\infty, \\ Q_2 &= (010010000111)^\infty, \\ Q_3 &= (0101) \cdot (011000011000)^\infty, \\ Q_4 &= (0101) \cdot (101000101000)^\infty. \end{aligned}$$

Alors, pour tout entier $n \equiv 0 \pmod 4$, les suites $Q_1[n]$, $Q_2[n]$, $Q_3[n]$ et $Q_4[n]$ sont fortement balancées. De plus, pour tout entier $n \equiv 0 \pmod 4$ et $n \geqslant 92$, toute suite fortement balancée de longueur n est une de ces 4 sous-suites $Q_1[n]$, $Q_2[n]$, $Q_3[n]$ ou $Q_4[n]$.

On continue avec les suites fortement balancées de longueur $n \geqslant 127$ pour $n \equiv 3 \pmod 4$.

Théorème 1.3.9. *Soient $R_1, \ldots, R_{12}$ les suites binaires infinies, pseudo-périodiques de période 12 ou 24, définies par*

$$\begin{aligned} R_1 &= (001) \cdot (010000100001)^\infty, \\ R_2 &= (0011110) \cdot (001101010110)^\infty, \\ R_3 &= (101) \cdot (000101000010)^\infty, \\ R_4 &= (0100001) \cdot (010010111100001010111111)^\infty, \\ R_5 &= (0100001) \cdot (100100001001)^\infty, \\ R_6 &= (0101011) \cdot (010101100011)^\infty, \\ R_7 &= (0101011) \cdot (010111111101011010011101)^\infty, \\ R_8 &= (010) \cdot (101110110010)^\infty, \\ R_9 &= (100) \cdot (001000010100)^\infty, \\ R_{10} &= (1000010) \cdot (110001101010)^\infty, \\ R_{11} &= (1111101) \cdot (011000110101)^\infty, \\ R_{12} &= (111) \cdot (110110000111)^\infty. \end{aligned}$$

Alors, pour tout entier $n \equiv 3 \pmod 4$, les suites $R_1[n], \ldots, R_{12}[n]$ sont fortement balancées. De plus, pour tout entier $n \equiv 3 \pmod 4$ et $n \geqslant 127$, toute suite fortement balancée de longueur n est une de ces 12 sous-suites $R_1[n], \ldots, R_{12}[n]$, avec les exceptions suivantes :

- *si $n \equiv 3 \pmod{12}$, alors il y a deux suites fortement balancées de longueur n de plus, qui sont les suites $R_5[n-4] \cdot (0101)$ et $R_8[n-4] \cdot (0100)$,*
- *si $n \equiv 7 \pmod{12}$, alors il y a deux suites fortement balancées de longueur n de plus, qui sont les suites $R_8[n-8] \cdot (01001000)$, et soit $R_5[n-8] \cdot (01011111)$ pour $n \equiv 7 \pmod{24}$, soit $R_5[n-8] \cdot (01011010)$ pour $n \equiv 19 \pmod{24}$.*

Corollaire 1.3.10. *Pour tout entier $n \equiv 0$ ou $3 \pmod 4$, il existe au moins 4 suites fortement balancées de longueur n.*

1.3.3 Suites binaires balancées symétriques et antisymétriques

Définition 1.3.11. Soit $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$.
- La suite S est dite *symétrique* si

$$a_j = a_{n-j+1}, \ \forall 1 \leqslant j \leqslant n.$$

  Par exemple, la suite (01010) est une suite binaire symétrique de longueur n=5.
- La suite S est dite *antisymétrique* si

$$a_j = a_{n-j+1} + 1, \ \forall 1 \leqslant j \leqslant n.$$

  Par exemple, la suite (110100) est une suite binaire antisymétrique de longueur $n = 6$.

Remarque. Par définition il n'y a pas de suite binaire antisymétrique de longueur impaire.

Les résultats qui vont suivre et qui portent sur l'existence de suites binaires balancées symétriques ou antisymétriques apparaissent dans [15].

Théorème 1.3.12. *Il existe une suite binaire balancée symétrique de longueur $n \geqslant 1$ si, et seulement si, $n \equiv 0, 3, 7 \pmod 8$.*

Théorème 1.3.13. *Il existe une suite binaire balancée antisymétrique de longueur $n \geqslant 1$ si, et seulement si, $n \equiv 4 \pmod 8$.*

Conditions nécessaires :

On obtient, à l'aide des résultats de la Section 1.2, les conditions nécessaires sur les longueurs des suites balancées symétriques ou antisymétriques. Cette preuve est sensiblement plus courte que celle donnée dans [15].

Soit $S = (a_1, \ldots, a_n)$ une suite binaire balancée de longueur $n \geqslant 1$. Supposons que n soit pair. Alors, le Théorème 1.2.2 conduit à la relation suivante :

$$\frac{n(n+1)}{4} = \nu(S) \equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \equiv \sum_{j=1}^{n/2} \left(\binom{n+1}{j} - 1 \right) (a_j + a_{n-j+1}) \pmod 2.$$

Si la suite S est symétrique, alors on a

$$\frac{n(n+1)}{4} \equiv 0 \pmod 2,$$

et donc $n \equiv 0 \pmod 8$. Si la suite S est antisymétrique, alors on a

$$\frac{n(n+1)}{4} \equiv \sum_{j=1}^{n/2} \left(\binom{n+1}{j} - 1 \right) = 2^n - 1 - \frac{n}{2} \equiv \frac{n}{2} + 1 \pmod 2.$$

Ce qui entraîne

$$n(n-1) \equiv 4 \pmod 8,$$

et donc $n \equiv 4 \pmod 8$. Supposons maintenant que n soit impair et S une suite balancée symétrique de longueur n. Alors le Théorème 1.2.2 implique

$$\begin{aligned}\frac{n(n+1)}{4} &\equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \\ &= \left(\binom{n+1}{\frac{n+1}{2}} - 1 \right) a_{\frac{n+1}{2}} + \sum_{j=1}^{\frac{n-1}{2}} \left(\binom{n+1}{j} - 1 \right) (a_j + a_{n-j+1}) \\ &\equiv \left(2\binom{n}{\frac{n-1}{2}} - 1 \right) a_{\frac{n+1}{2}} \equiv a_{\frac{n+1}{2}} \pmod 2.\end{aligned}$$

On en conclut que

$$a_{\frac{n+1}{2}} = 0 \implies n(n+1) \equiv 0 \pmod 8 \implies n \equiv 7 \pmod 8,$$

ou

$$a_{\frac{n+1}{2}} = 1 \implies n(n+1) \equiv 4 \pmod 8 \implies n \equiv 3 \pmod 8.$$

Conditions suffisantes :

On s'intéresse tout d'abord aux liens entre les suites binaires symétriques ou antisymétriques et leurs suites dérivées respectives. On obtient alors le résultat suivant qui est une version particulière d'un théorème plus général sur les suites antisymétriques dans un groupe cyclique quelconque. Cette généralisation est étudiée au Chapitre 4.

Proposition 1.3.14. *Soit $S = (a_1, \ldots, a_n)$ une suite de longueur $n \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors,*

$$S \text{ symétrique} \iff \begin{cases} \partial S \text{ symétrique,} \\ a_{\lfloor n/2 \rfloor} + a_{\lfloor n/2 \rfloor + 1} = 0. \end{cases}$$

De même,

$$S \text{ antisymétrique} \iff \begin{cases} \partial S \text{ symétrique,} \\ a_{\lfloor n/2 \rfloor} + a_{\lfloor n/2 \rfloor + 1} = 1. \end{cases}$$

Preuve. Soient $S = (a_1, \ldots, a_n)$ et $\partial S = (b_1, \ldots, b_{n-1})$ sa suite dérivée. Supposons que la suite S soit symétrique. Alors,

$$b_j + b_{n-j} = a_j + a_{j+1} + a_{n-j} + a_{n-j+1} = 0, \ \forall 1 \leqslant j \leqslant n-1,$$

donc ∂S est également symétrique. Réciproquement, supposons que la suite ∂S soit symétrique et que $a_{\lfloor n/2 \rfloor} + a_{\lfloor n/2 \rfloor + 1} = 0$. Si n est pair, alors

$$a_j + a_{n-j+1} = \sum_{k=j}^{n-j} b_k = \sum_{k=j}^{n/2-1} (b_k + b_{n-k}) + b_{n/2} = a_{n/2} + a_{n/2+1} = 0, \ \forall 1 \leqslant j \leqslant n.$$

Sinon, si n est impair, alors

$$a_j + a_{n-j+1} = \sum_{k=j}^{n-j} b_k = \sum_{k=j}^{(n-1)/2} (b_k + b_{n-k}) = 0, \ \forall 1 \leqslant j \leqslant n.$$

L'autre équivalence se démontre de la même manière. □

Dans [15], des suites binaires balancées et symétriques de longueur $n \geqslant 1$, pour tout $n \equiv 0, 3$ ou $7 \pmod 8$, et des suites binaires balancées et antisymétriques de longueur n, pour tout $n \equiv 4 \pmod 8$, sont construites. On rappelle rapidement ci-dessous cette construction.

Pour $\mathbf{n \equiv 0, 7}$ (mod 8) : Soit S la suite binaire symétrique de longueur 24 définie par

$$S = (011111000001100000111110).$$

Alors, les suites suivantes sont des suites binaires balancées et symétriques de longueur n, pour tout $n \equiv 0 \pmod 8$:

$$\begin{array}{lcc} n = 24k & : & S^k, \\ n = 24k + 8 & : & (0100) \cdot S^k \cdot (0010), \\ n = 24k + 16 & : & (11000100) \cdot S^k \cdot (00100011). \end{array}$$

Par la Proposition 1.3.14, la suite $\partial(S^k)$ est symétrique pour tout $k \geqslant 1$. Les suites suivantes sont donc balancées et symétriques de longueur n, pour tout $n \equiv 7 \pmod 8$:

$$\begin{array}{lcc} n = 24k - 1 (k \geqslant 1) & : & \partial(S^k), \\ n = 24k + 7 & : & (0010) \cdot \partial(S^k) \cdot (0100), \\ n = 24k + 15 & : & (01000010) \cdot \partial(S^k) \cdot (01000010). \end{array}$$

Pour $\mathbf{n \equiv 3}$ (mod 8) : On commence par définir une suite $w = (w_j)_{j \in \mathbb{Z}}$ doublement infinie et périodique de période 12. Soit $\pi : \mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/12\mathbb{Z}$ la surjection canonique et

$$p = (p_0, p_1, \ldots, p_{11}) = (100001010000)$$

la suite de longueur 12 que l'on considère indexée sur $\mathbb{Z}/12\mathbb{Z}$. On peut remarquer que

$$p_{\pi(j)} = p_{\pi(-j)}, \ \forall j \in \mathbb{Z}.$$

Soit w la suite définie par $w = (w_j)_{j \in \mathbb{Z}} = (p_{\pi(j)})_{j \in \mathbb{Z}}$. Alors, pour tout $k \geqslant 0$, la suite

$$v_k = w[-4k - 1, 4k + 1] = (w_{-4k-1}, w_{-4k}, \ldots, w_{4k}, w_{4k+1})$$

est une suite binaire balancée et symétrique de longueur $8k + 3$. Les suites v_0, v_1, v_2, v_3 et v_4 sont illustrées ci-dessous :

$$\begin{array}{c} 010 \\ 10000100001 \\ 00101000010000010100 \\ 01000010100001000010100001 0 \\ 10000100001010000100001010000100001 \end{array}$$

Pour $\mathbf{n \equiv 4}$ (mod 8) : On construit une suite binaire balancée et antisymétrique de longueur n, pour tout $n \equiv 4 \pmod 8$.

Proposition 1.3.15. *Pour tout entier $k \geqslant 0$, les suites $P_0(v_k)$ et $P_1(v_k)$ sont des suites binaires balancées et antisymétriques de longueur $8k+4$.*

Preuve. Par la Proposition 1.3.14, on sait que les suites $P_0(v_k)$ et $P_1(vk)$ sont antisymétriques car la suite v_k est symétrique et $p_0 = 1$. De plus, ces suites sont balancées car, par antisymétrie, elles contiennent $4k+2$ fois l'élément 1. Par conséquent, on obtient

$$\nu(P_i(v_k)) = 4k + 2 + \nu(v_k) = 4k + 2 + \frac{1}{2}\binom{8k+4}{2} = \frac{1}{2}\binom{8k+5}{2},$$

pour $i \in \{0, 1\}$. Ce qui achève la preuve. □

1.3.4 Suites binaires balancées de poids moyen

Définition 1.3.16. Soit S une suite de longueur finie dans $\mathbb{Z}/2\mathbb{Z}$. La suite S est dite *de poids moyen* si elle contient autant d'éléments 1 que d'éléments 0.

Par exemple, toute suite binaire de longueur finie et antisymétrique est une suite de poids moyen. Il est clair que si S est une suite binaire balancée de longueur $n \equiv 0 \pmod 4$ et de poids moyen, alors sa suite dérivée ∂S est également balancée et de longueur $n \equiv 3 \pmod 4$. Ainsi, montrer qu'il existe au moins une suite binaire balancée de poids moyen pour toute longueur $n \equiv 0 \pmod 4$ permet de répondre positivement au Problème de Steinhaus. Ce résultat apparaît dans [13] où les auteurs construisent explicitement une telle suite.

Théorème 1.3.17. *Soient S_0 et S_4 les deux suites binaires infinies et pseudo-périodiques de période 24 suivantes :*

$$S_0 = (01101010) \cdot (111010001101010000111100)^\infty,$$
$$S_4 = (11000011) \cdot (101001111000110101001001)^\infty.$$

Alors les suites de poids moyen $S_0[8k]$ et $S_4[8k+4]$, de longueurs respectives $8k$ et $8k+4$, sont balancées pour tout entier $k \geqslant 0$.

Chapitre 2

Graphes de Steinhaus pairs et impairs

Dans ce chapitre, on présente les graphes de Steinhaus qui sont des graphes simples dont la matrice d'adjacence est une matrice de Steinhaus, c'est-à-dire une matrice carrée, composée de 0 et de 1, symétrique, à diagonale nulle et dont le triangle supérieur est un triangle de Steinhaus, comme défini au Chapitre 1. Après avoir rappelé, à la Section 2.1, certaines propriétés sur ces graphes, on s'intéresse au cas particulier des graphes pairs et impairs, à savoir les graphes dont tous les sommets sont de degrés de même parité. On commence par donner une nouvelle preuve, à la Section 2.2, d'un théorème de Dymacek qui établit que tout graphe de Steinhaus pair possède une matrice d'adjacence bisymétrique. Ce résultat est ensuite utilisé afin d'étudier les graphes de Steinhaus pairs à la Section 2.3 et les impairs à la Section 2.4.

2.1 Définitions et premières propriétés

Définition 2.1.1. Soit $s = (a_1, \ldots, a_{n-1})$ une suite de longueur $n-1 \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. La *matrice de Steinhaus* associée à la suite s est la matrice carrée de taille n, symétrique, à diagonale nulle et dont le triangle supérieur est constitué des éléments du triangle de Steinhaus Δs, i.e. la matrice carrée $M(s) = (a_{i,j})_{1 \leqslant i,j \leqslant n}$ définie par :

- $a_{i,i} = 0$ pour $1 \leqslant i \leqslant n$,
- $a_{1,j} = a_{j-1}$ pour $2 \leqslant j \leqslant n$,
- $a_{i,j} = a_{i-1,j-1} + a_{i-1,j}$ pour $2 \leqslant i < j \leqslant n$,
- $a_{i,j} = a_{j,i}$ pour $1 \leqslant i, j \leqslant n$.

Par convention $M(\emptyset) = (0)$ est la matrice de Steinhaus de taille $n = 1$ associée à la suite vide.

Par exemple, la matrice $M(s)$ de $\mathcal{M}_5(\mathbb{Z}/2\mathbb{Z})$ suivante est la matrice de Steinhaus associée

à la suite binaire $s = (1100)$ de longueur 4.

$$M(s) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Notation. Pour tout entier $n \geqslant 1$, l'ensemble des matrices de Steinhaus de taille n sera noté $\mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$. Il est évident que l'ensemble $\mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$ comporte 2^{n-1} éléments distincts.

On a vu, au Chapitre 1, que dans un triangle de Steinhaus binaire, chaque élément du triangle peut être exprimé en fonction des éléments de la première ligne, du côté gauche ou du côté droit du triangle. De la même manière, dans une matrice de Steinhaus, chaque élément du triangle supérieur peut être exprimé en fonction de la première ligne, de la dernière colonne ou de la surdiagonale de la matrice.

Proposition 2.1.2. *Soit $M = (a_{i,j})$ une matrice de Steinhaus de taille $n \geqslant 2$. Alors, pour tout i et tout j, $1 \leqslant i < j \leqslant n$, on a*

$$a_{i,j} = \sum_{k=0}^{i-1} \binom{i-1}{k} a_{1,j-k} = \sum_{k=0}^{n-j} \binom{n-j}{k} a_{i+k,n} = \sum_{k=0}^{j-i-1} \binom{j-i-1}{k} a_{i+k,i+k+1}.$$

Preuve. Ce n'est qu'une réécriture de la Proposition 1.1.7. □

Le vocabulaire de la théorie des graphes utilisé dans ce chapitre et le suivant est issu du livre de Diestel [7].

Définition 2.1.3. Soit s une suite de longueur $n-1 \geqslant 0$ dans $\mathbb{Z}/2\mathbb{Z}$. Le *graphe de Steinhaus* associé à la suite s est le graphe simple $G(s)$ à n sommets dont la matrice d'adjacence $\mathcal{A}(G(s))$ est la matrice de Steinhaus $M(s)$, i.e.

$$\mathcal{A}(G(s)) = M(s).$$

Chaque sommet d'un graphe de Steinhaus $G(s)$ est numéroté selon l'ordre des lignes dans la matrice $M(s)$ et le $i$ème sommet de $G(s)$ est noté V_i pour tout i, $1 \leqslant i \leqslant n$.

Par exemple, le graphe simple à 5 sommets de la Figure 2.1 est le graphe de Steinhaus $G(s)$ associé à la suite $s = (1100)$. Pour tout entier $n \geqslant 1$, le graphe sans arête à n sommets est le graphe de Steinhaus associé à la suite nulle de longueur $n-1$.

Les graphes de Steinhaus ont été introduits en 1978 par Molluzzo [19]. Sa définition des graphes de Steinhaus correspond avec le complémentaire des graphes que l'on considère dans ce chapitre. La définition utilisée ici a été donnée pour la première fois par Dymacek [8].

Une des premières propriétés que l'on peut observer est que, pour tout graphe de Steinhaus G, si l'on efface les premier ou dernier sommets et leurs arêtes incidentes, on obtient un nouveau graphe de Steinhaus.

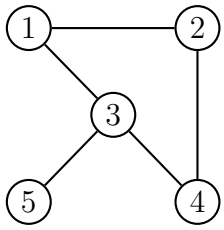


FIG. 2.1 – Exemple de graphe de Steinhaus

Notation. Soit G un graphe de Steinhaus à $n \geqslant 1$ sommets. Alors, pour tout entier i, $1 \leqslant i \leqslant n$, on note $G \setminus \{V_i\}$ le graphe, à $n-1$ sommets, obtenu de G en supprimant le $i$ème sommet V_i et ses arêtes incidentes dans G.

Proposition 2.1.4. *Soit $s = (a_1, \ldots, a_{n-1})$ une suite de longueur $n-1 \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors les graphes $G(s) \setminus \{V_1\}$, $G(s) \setminus \{V_n\}$ et $G(s) \setminus \{V_1, V_n\} = (G(s) \setminus \{V_1\}) \setminus \{V_n\} = (G(s) \setminus \{V_n\}) \setminus \{V_1\}$ sont les graphes de Steinhaus suivants :*

$$G(s) \setminus \{V_1\} = G(\partial s),$$
$$G(s) \setminus \{V_n\} = G((a_1, \ldots, a_{n-2})),$$
$$G(s) \setminus \{V_1, V_n\} = G((a_1 + a_2, \ldots, a_{n-3} + a_{n-2})).$$

Preuve. La matrice d'adjacence du graphe $G(s) \setminus \{V_1\}$ est la matrice de Steinhaus $M(s)$ dont on a tronqué la première ligne et la première colonne. Elle est donc égale à

$$M(a_1 + a_2, \ldots, a_{n-2} + a_{n-1}) = M(\partial s)$$

et le résultat s'ensuit. La matrice d'adjacence du graphe $G(s) \setminus \{V_n\}$ est la matrice de Steinhaus $M(s)$ dont on a tronqué la dernière ligne et la dernière colonne. Elle correspond donc à

$$M(a_1, \ldots, a_{n-2}).$$

En combinant ces deux résultats, on obtient que la matrice d'adjacence du graphe $G(s) \setminus \{V_1, V_n\}$ est la matrice de Steinhaus

$$M((a_1 + a_2, \ldots, a_{n-3} + a_{n-2})).$$

Ce qui conclut la preuve. □

On peut également montrer que les graphes de Steinhaus sont presque tous connexes. Ce résultat et sa preuve sont issus de [8].

Théorème 2.1.5. *Soit s une suite de longueur $n-1 \geqslant 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors, le graphe de Steinhaus $G(s)$ est connexe si, et seulement si, $s \neq (0 \ldots 0)$.*

Preuve. Par récurrence sur n. Pour $n = 2$, il n'existe que deux matrices de Steinhaus qui sont

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Les graphes de Steinhaus à 2 sommets sont donc soit le graphe sans arête à 2 sommets qui est totalement disconnexe, soit le graphe complet K_2 à 2 sommets qui est bien connexe. Supposons maintenant que le résultat soit vrai pour les graphes de Steinhaus à $n-1$ sommets et prouvons le pour ceux à n sommets. Soit $s = (a_1, \ldots, a_{n-1})$ une suite de longueur $n-1$ dans $\mathbb{Z}/2\mathbb{Z}$. Comme $G' = G((a_1, \ldots, a_{n-2}))$ est un graphe de Steinhaus à $n-1$ sommets, on sait, par hypothèse de récurrence, que G' est connexe si, et seulement si, $(a_1, \ldots, a_{n-2}) \neq (0 \ldots 0)$. Distinguons les différents cas :

- Si $s = (0 \ldots 0)$, alors la matrice de Steinhaus $M(s)$ est la matrice nulle de taille $n \times n$ par définition et donc le graphe de Steinhaus $G(s)$ est le graphe totalement disconnexe à n sommets.
- Si $s = (0 \ldots 01)$, alors la matrice de Steinhaus $M(s) = (a_{i,j})_{1 \leqslant i,j \leqslant n}$ est définie par

  $$\begin{cases} a_{i,j} = 0 & \text{pour } 1 \leqslant i < j \leqslant n-1, \\ a_{i,n} = 1 & \text{pour } 1 \leqslant i \leqslant n-1. \end{cases}$$

  Le graphe de Steinhaus $G(s)$ est donc le graphe étoile à n sommets qui est un graphe connexe.
- Si $(a_1, \ldots, a_{n-2}) \neq (0 \ldots 0)$ alors par hypothèse de récurrence le graphe G' est connexe. La seule possibilité pour que $G(s)$ ne soit pas connexe est donc que V_n soit un sommet isolé, soit

  $$a_{i,n} = 0, \ \forall 1 \leqslant i \leqslant n.$$

  Ce qui implique, par la Proposition 2.1.2, que $s = (0 \ldots 0)$. On obtient donc une contradiction.

□

Un problème général sur les graphes de Steinhaus est celui de caractériser ceux qui possèdent une propriété graphique donnée. Les graphes de Steinhaus bipartis [4, 9, 12] et ceux planaires [11] ont été caractérisés.

Définition 2.1.6. On appelle *graphe pair* un graphe pour lequel tous ses sommets sont de degrés pairs, et *graphe impair* un graphe pour lequel tous ses sommets sont de degrés impairs.

Dans la suite de ce chapitre, on étudie les graphes de Steinhaus pairs et impairs. Ces résultats sont en partie issus de [8] mais souvent reformulés. Cependant, à la section suivante, on donne une nouvelle preuve du théorème principal utilisé dans l'étude de ce type de graphes de Steinhaus. On s'intéresse à la notion plus forte de graphes de Steinhaus réguliers, c'est-à-dire où tous les sommets ont le même degré, au Chapitre 3.

2.2 Une nouvelle preuve du théorème de Dymacek

Définition 2.2.1. Soit $M = (a_{i,j})$ une matrice carrée de taille $n \geqslant 1$. La matrice M est dite *bisymétrique* si les éléments de M sont symétriques par rapport à sa diagonale et à son antidiagonale, i.e.

$$a_{i,j} = a_{j,i} = a_{n-j+1,n-i+1},\ \forall 1 \leqslant i, j \leqslant n.$$

Par exemple, la matrice suivante est une matrice bisymétrique de taille $n = 5$.

$$\begin{pmatrix} 1 & 0 & 1 & 3 & 7 \\ 0 & 2 & 8 & 4 & 3 \\ 1 & 8 & 0 & 8 & 1 \\ 3 & 4 & 8 & 2 & 0 \\ 7 & 3 & 1 & 0 & 1 \end{pmatrix}$$

Théorème 2.2.2 (Dymacek,1979)**.** *La matrice d'adjacence d'un graphe de Steinhaus pair est bisymétrique.*

Ce théorème, qui est la pierre angulaire de l'étude des graphes de Steinhaus pairs et impairs, apparaît ici comme un corollaire du théorème suivant, où l'on prouve que tout élément de l'antidiagonale d'une matrice de Steinhaus peut être exprimé en fonction des degrés des sommets de son graphe associé.

Notation. Soit G un graphe de Steinhaus à $n \geqslant 1$ sommets et $M = (a_{i,j})$ sa matrice de Steinhaus associée. Pour tout entier i, $1 \leqslant i \leqslant n$, on note $\deg_G(V_i)$ le degré du sommet V_i dans G, i.e.

$$\deg_G(V_i) = \sum_{j=1}^{n} a_{i,j},$$

où $a_{i,j}$ est considéré comme un élément de $\{0, 1\}$. Lorsqu'il n'y a pas d'ambiguïté sur le graphe G concerné, on note simplement $\deg(V_i)$.

Théorème 2.2.3 (Chappelon,[6])**.** *Soit G un graphe de Steinhaus à $n \geqslant 2$ sommets et $M = (a_{i,j})$ sa matrice de Steinhaus associée. Alors, chaque élément de l'antidiagonale de M peut être exprimé en fonction des degrés des sommets de G, à savoir, pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n}{2} \right\rfloor$, on a*

$$a_{i,n-i+1} \equiv \sum_{k=0}^{i-1} \binom{i-1}{k} \deg\left(V_{i+k+1}\right) \equiv \sum_{k=0}^{i-1} \binom{i-1}{k} \deg\left(V_{n-i-k}\right) \pmod 2.$$

Preuve. On commence par exprimer le degré de chaque sommet du graphe G en fonction des éléments de la première ligne, de la dernière colonne et de la surdiagonale de M. On

considère ici les éléments $a_{i,j}$ comme des entiers de $\{0,1\}$. Pour tout i, $2 \leqslant i \leqslant n-1$, on obtient

$$\begin{aligned}
\deg(V_i) &= \sum_{j=1}^{n} a_{i,j} = \sum_{j=1}^{i-1} a_{j,i} + \sum_{j=i+1}^{n} a_{i,j} \\
&\equiv \sum_{j=1}^{i-1} (a_{j,i+1} + a_{j+1,i+1}) + \sum_{j=i+1}^{n} (a_{i-1,j-1} + a_{i-1,j}) \\
&\equiv \sum_{j=1}^{i-1} a_{j,i+1} + \sum_{j=2}^{i} a_{j,i+1} + \sum_{j=i}^{n-1} a_{i-1,j} + \sum_{j=i+1}^{n} a_{i-1,j} \\
&\equiv a_{1,i+1} + a_{i,i+1} + a_{i-1,i} + a_{i-1,n} \pmod 2.
\end{aligned}$$

Ceci entraîne, par la Proposition 2.1.2, que

$$\begin{aligned}
\sum_{k=0}^{i-1} \binom{i-1}{k} \deg(V_{i+k+1}) &\equiv \sum_{k=0}^{i-1} \binom{i-1}{k} (a_{1,i+k+2} + a_{i+k+1,i+k+2} + a_{i+k,i+k+1} + a_{i+k,n}) \\
&\equiv \sum_{k=0}^{i-1} \binom{i-1}{k} a_{1,2i-k+1} + \sum_{k=0}^{i-1} \binom{i-1}{k} a_{i+k+1,i+k+2} \\
&+ \sum_{k=0}^{i-1} \binom{i-1}{k} a_{i+k,i+k+1} + \sum_{k=0}^{i-1} \binom{i-1}{k} a_{i+k,n} \\
&\equiv a_{i,2i+1} + a_{i+1,2i+1} + a_{i,2i} + a_{i,n-i+1} \equiv a_{i,n-i+1} \pmod 2,
\end{aligned}$$

pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n}{2} \right\rfloor$. La seconde équivalence peut être traitée de la même manière. □

Remarque. On déduit du Théorème 2.2.3 une condition nécessaire sur les degrés des sommets pour qu'un graphe donné soit un graphe de Steinhaus. En effet, les degrés d'un graphe de Steinhaus à n sommets doivent satisfaire les équations suivantes dans $\mathbb{Z}/2\mathbb{Z}$:

$$\sum_{k=0}^{i-1} \binom{i-1}{k} \deg(V_{i+k+1}) \equiv \sum_{k=0}^{i-1} \binom{i-1}{k} \deg(V_{n-i-k}) \pmod 2, \ \forall 1 \leqslant i \leqslant \left\lfloor \frac{n}{2} \right\rfloor.$$

Plus généralement, un problème ouvert (Question 3 de [10]) est de déterminer si un graphe arbitraire, pas nécessairement labellé, est isomorphe à un graphe de Steinhaus.

On continue par la caractérisation des matrices de Steinhaus bisymétriques qui apparaît dans [8].

Proposition 2.2.4. *Soit $M = (a_{i,j})$ une matrice de Steinhaus de taille $n \geqslant 3$. Alors les assertions suivantes sont équivalentes :*

(i) la matrice M est bisymétrique,

(ii) la surdiagonale de M est une suite symétrique,

(iii) les éléments $a_{i,n-i+1}$ de l'antidiagonale de M s'annulent pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$.

Preuve.

(**i**) $\Longrightarrow$ (**ii**) : Evident.

(**ii**) $\Longrightarrow$ (**iii**) : Supposons la surdiagonale de M symétrique, i.e.

$$a_{i,i+1} = a_{n-i,n-i+1},$$

pour tout i, $1 \leqslant i \leqslant n-1$. Si n est impair, alors on a

$$a_{i,n-i+1} = \sum_{k=0}^{n-2i} \binom{n-2i}{k} a_{i+k,i+k+1} = \sum_{k=0}^{\frac{n-2i+1}{2}} \binom{n-2i}{k} (a_{i+k,i+k+1} + a_{n-i-k,n-i-k+1}) = 0,$$

pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$. Sinon, si n est pair, alors on obtient

$$a_{i,n-i+1} = \sum_{k=0}^{\frac{n}{2}-i-1} \binom{n-2i}{k} (a_{i+k,i+k+1} + a_{n-i-k,n-i-k+1}) + 2\binom{n-2i-1}{\frac{n}{2}-i} a_{\frac{n}{2},\frac{n}{2}+1} = 0,$$

pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$.

(**iii**) $\Longrightarrow$ (**i**) : Par induction sur n. On considère la sous-matrice $N = (a_{i,j})_{2 \leqslant i,j \leqslant n-1}$ qui est une matrice de Steinhaus de taille $n-2$. Par hypothèse d'induction, la matrice N est bisymétrique. Il reste alors à prouver que $a_{1,j} = a_{n-j+1,n}$ pour tout j, $2 \leqslant j \leqslant n$. Comme $a_{1,n} = 0$, il s'ensuit que $a_{1,n-1} = a_{1,n} + a_{2,n} = a_{2,n}$ et pour tout j, $2 \leqslant j \leqslant n-2$, on a

$$a_{1,j} = \sum_{k=j+1}^{n-1} a_{2,k} + a_{1,n-1} = \sum_{k=2}^{n-j} a_{k,n-1} + a_{2,n} = a_{n-j+1,n}.$$

□

Corollaire 2.2.5 (Dymacek,[8])**.** *Pour tout entier $n \geqslant 1$, il y a exactement $2^{\left\lfloor \frac{n}{2} \right\rfloor}$ matrices de Steinhaus de taille n bisymétriques.*

Preuve. Soit $n \geqslant 1$ un entier. Par la Proposition 2.1.2, toute matrice de Steinhaus est entièrement définie par sa surdiagonale. On en déduit, par la Proposition 2.2.4, qu'il existe une bijection entre les matrices de Steinhaus de taille n bisymétriques et les suites binaires de longueur $n-1$ symétriques. Il existe $2^{\left\lceil \frac{n-1}{2} \right\rceil}$ suites binaires symétriques de longueur $n-1$. Ce qui conclut la preuve. □

On peut maintenant prouver le théorème de Dymacek.

Preuve du Théorème 2.2.2. Soient G un graphe de Steinhaus pair à n sommets et $M = (a_{i,j})$ sa matrice de Steinhaus. Si $n = 1$, alors $M = (0)$ qui est bien une matrice bisymétrique. Sinon, pour $n \geqslant 2$, le Théorème 2.2.3 implique l'égalité suivante

$$a_{i,n-i+1} \equiv \sum_{k=0}^{i-1} \binom{i-1}{k} \deg(V_{i+k+1}) \equiv 0 \pmod 2,$$

pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n}{2} \right\rfloor$. Finalement, la matrice M est bisymétrique par la Proposition 2.2.4. □

2.3 Graphes de Steinhaus pairs

Les résultats de cette section et de la suivante sont principalement issus de [8].

Définition 2.3.1. Soit G un graphe à $n \geqslant 1$ sommets $\{V_1, \ldots, V_n\}$. Le graphe G est dit symétrique si

$$\deg(V_i) = \deg(V_{n-i+1}),\ \forall 1 \leqslant i \leqslant n.$$

Proposition 2.3.2. *Soit G un graphe à $n \geqslant 1$ sommets et $M = \mathcal{A}(G) = (a_{i,j})$ sa matrice d'adjacence. Si la matrice M est bisymétrique, alors le graphe G est symétrique.*

Preuve. Pour tout i, $1 \leqslant i \leqslant n$, on obtient

$$\deg(V_i) = \sum_{j=1}^{n} a_{i,j} = \sum_{j=1}^{n} a_{n-j+1,n-i+1} = \sum_{j=1}^{n} a_{j,n-i+1} = \deg(V_{n-i+1}).$$

□

Ainsi, par le théorème de Dymacek, tout graphe de Steinhaus pair est symétrique.

Définition 2.3.3. Soit T l'opérateur

$$T : \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathcal{SM}_{n-3}(\mathbb{Z}/2\mathbb{Z})$$

qui à toute matrice $M = (a_{i,j})$ de $\mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$ associe la matrice $T(M) = (b_{i,j})$ de $\mathcal{SM}_{n-3}(\mathbb{Z}/2\mathbb{Z})$ définie par $b_{i,j} = a_{i+1,j+2}$ pour tout i et tout j, $1 \leqslant i < j \leqslant n$. Le triangle supérieur (resp. inférieur) de la matrice $T(M)$ est donc inscrit dans le triangle supérieur (resp. inférieur) de la matrice M comme on peut le voir dans la représentation de la matrice M ci-dessous :

$$\begin{pmatrix}
0 & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & \cdots & \cdots & a_{1,n-4} & a_{1,n-3} & a_{1,n-2} & a_{1,n-1} & a_{1,n} \\
 & 0 & a_{2,3} & \mathbf{b_{1,2}} & \mathbf{b_{1,3}} & \mathbf{b_{1,4}} & & & & \mathbf{b_{1,n-5}} & \mathbf{b_{1,n-4}} & \mathbf{b_{1,n-3}} & a_{2,n} \\
 & & 0 & a_{3,4} & \mathbf{b_{2,3}} & \mathbf{b_{2,4}} & & & & & \mathbf{b_{2,n-4}} & \mathbf{b_{2,n-3}} & a_{3,n} \\
 & & & 0 & a_{4,5} & \mathbf{b_{3,4}} & & & & & & \mathbf{b_{3,n-3}} & a_{4,n} \\
 & & & & 0 & a_{5,6} & & & & & & & a_{5,n} \\
 & & & & & 0 & \ddots & & & & & & \vdots \\
 & & & & & & \ddots & \ddots & & & & & \vdots \\
 & & & & & & & 0 & a_{n-5,n-4} & \mathbf{b_{n-6,n-5}} & \mathbf{b_{n-6,n-4}} & \mathbf{b_{n-6,n-3}} & a_{n-5,n} \\
 & & & & & & & & 0 & a_{n-4,n-3} & \mathbf{b_{n-5,n-4}} & \mathbf{b_{n-5,n-3}} & a_{n-4,n} \\
 & & & & & & & & & 0 & a_{n-3,n-2} & \mathbf{b_{n-4,n-3}} & a_{n-3,n} \\
 & & & & & & & & & & 0 & a_{n-2,n-1} & a_{n-2,n} \\
 & & & & & & & & & & & 0 & a_{n-1,n} \\
 & & & & & & & & & & & & 0
\end{pmatrix}$$

Proposition 2.3.4. *Soit $M = (a_{i,j})$ une matrice de Steinhaus de taille $n \geqslant 1$. Alors,*

$$M \text{ bisymétrique} \iff \begin{cases} T(M) \text{ bisymétrique,} \\ a_{1,n} = 0. \end{cases}$$

Preuve. Provient directement de la Proposition 2.2.4. □

Notation. Soit G un graphe de Steinhaus à $n \geqslant 4$ sommets. Par abus de langage, on note $T(G)$ le graphe de Steinhaus à $n-3$ sommets dont la matrice d'adjacence est l'image par l'opérateur T de la matrice d'adjacence du graphe G, soit

$$\mathcal{A}(T(G)) := T(\mathcal{A}(G)).$$

Proposition 2.3.5. *Soit G un graphe de Steinhaus à $n \geqslant 4$ sommets. Alors, on obtient la relation suivante entre les degrés des sommets de G et ceux des sommets de $T(G)$:*

$$\deg_{T(G)}(V_i) \equiv \deg_G(V_{i+1}) + \deg_G(V_{i+2}) \pmod 2, \ \forall 1 \leqslant i \leqslant n-3.$$

Preuve. Notons $\mathcal{A}(G) = (a_{i,j})$ et $\mathcal{A}(T(G)) = (b_{i,j})$ les matrices de Steinhaus associées aux graphes G et $T(G)$ respectivement. Alors, pour tout entier i, $2 \leqslant i \leqslant n-4$, on a

$$\begin{aligned}
\deg_G(V_{i+1}) + \deg_G(V_{i+2}) &= \sum_{j=1}^{i} a_{j,i+1} + \sum_{j=i+2}^{n} a_{i+1,j} + \sum_{j=1}^{i+1} a_{j,i+2} + \sum_{j=i+3}^{n} a_{i+2,j} \\
&= \sum_{j=1}^{i} (a_{j,i+1} + a_{j,i+2}) + 2a_{i+1,i+2} + \sum_{j=i+3}^{n} (a_{i+1,j} + a_{i+2,j}) \\
&\equiv \sum_{j=2}^{i} a_{j,i+2} + \sum_{j=i+3}^{n-1} a_{i+1,j} \equiv \sum_{j=1}^{i-1} b_{j,i} + \sum_{j=i+1}^{n-3} b_{i,j} \\
&\equiv \deg_{T(G)}(V_i) \pmod 2.
\end{aligned}$$

De même, pour $i = 1$ et $i = n-3$, on obtient

$$\begin{aligned}
\deg_G(V_2) + \deg_G(V_3) &= a_{1,2} + \sum_{j=3}^{n} a_{2,j} + a_{1,3} + a_{2,3} + \sum_{j=4}^{n} a_{3,j} \\
&\equiv \sum_{j=4}^{n-1} a_{2,j} \equiv \sum_{j=2}^{n-3} b_{1,j} \equiv \deg_{T(G)}(V_1) \pmod 2,
\end{aligned}$$

$$\begin{aligned}
\deg_G(V_{n-2}) + \deg_G(V_{n-1}) &= \sum_{j=1}^{n-3} a_{j,n-2} + a_{n-2,n-1} + a_{n-2,n} + \sum_{j=1}^{n-2} a_{j,n-1} + a_{n-1,n} \\
&\equiv \sum_{j=2}^{n-3} a_{j,n-1} \equiv \sum_{j=1}^{n-4} b_{j,n-3} \equiv \deg_{T(G)}(V_{n-3}) \pmod 2.
\end{aligned}$$

□

Théorème 2.3.6 (Dymacek,[8])**.** *Soit G un graphe de Steinhaus à $n \geqslant 4$ sommets. Alors,*

$$G \text{ pair} \implies T(G) \text{ pair}.$$

De même,

$$G \text{ impair} \implies T(G) \text{ pair}.$$

Preuve. Par la proposition 2.3.5, on a

$$\deg_{T(G)}(V_i) \equiv \deg_G(V_{i+1}) + \deg_G(V_{i+2}) \equiv 0 \pmod 2,$$

pour tout i, $1 \leqslant i \leqslant n-3$. □

On construit maintenant un opérateur "inverse" de T. Soit $N = (b_{i,j})$ une matrice de Steinhaus de taille $n \geqslant 1$ fixée. On détermine les matrices de Steinhaus $M = (a_{i,j})$ de taille $n+3$ telles que $T(M) = N$. Tout d'abord, on sait, par définition de T, que la suite $(a_{1,3}, \ldots, a_{1,n+2})$ est une suite primitive de la suite $(b_{1,2}, \ldots, b_{1,n})$. Toute matrice de Steinhaus étant entièrement déterminée par sa première ligne, on en déduit que la matrice M ne dépend que du choix des éléments $a_{1,2}$ et $a_{1,n+3}$ et du choix de la primitive $(a_{1,3}, \ldots, a_{1,n-1})$. Ainsi, il existe 8 matrices de Steinhaus M distinctes de taille $n+3$ telles que $T(M) = N$. De plus, si la matrice N est bisymétrique, alors la Proposition 2.2.4 entraîne qu'il existe exactement 4 matrices de Steinhaus M de taille $n+3$ et bisymétriques telles que $T(M) = N$. Ce sont celles où $a_{1,n+3} = 0$. Enfin, si le graphe associé à la matrice N est pair et que l'on souhaite que le graphe associé à la matrice M le soit également, alors il faut de plus que $\sum_{j=1}^{n+3} a_{1,j} \equiv 0 \pmod 2$, soit que

$$a_{1,2} \equiv \sum_{j=3}^{n-1} a_{1,j} \pmod 2.$$

Il ne peut donc y avoir plus de 2 graphes pairs à $n+3$ sommets dont l'image par T soit le graphe pair associé à la matrice N. On définit maintenant ces deux opérateurs inverses et on montre que les graphes de Steinhaus pairs sont stables par eux.

Définition 2.3.7. Soit $k \in \{0,1\}$ et $n \geqslant 1$. Soit U_k l'opérateur

$$U_k : \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathcal{SM}_{n+3}(\mathbb{Z}/2\mathbb{Z})$$

qui à toute matrice $M = (b_{i,j})$ de $\mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$ associe la matrice $U_k(M) = (a_{i,j})$ de $\mathcal{SM}_{n+3}(\mathbb{Z}/2\mathbb{Z})$ définie par

$$\begin{cases} a_{1,n+3} = 0, \\ (a_{1,3}, \ldots, a_{1,n+2}) = P_k((b_{1,2}, \ldots, b_{1,n})), \\ a_{1,2} = \sum_{j=3}^{n+2} a_{1,j}, \end{cases}$$

où $P_k((b_{1,2}, \ldots, b_{1,n}))$ est la suite primitive de $(b_{1,2}, \ldots, b_{1,n})$ définie à la Proposition 1.1.4.

Proposition 2.3.8. *Soit $k \in \{0,1\}$. Pour toute matrice de Steinhaus M de taille $n \geqslant 1$, on a*

$$T(U_k(M)) = M.$$

Preuve. Ce résultat provient de la Proposition 1.1.5, en particulier du fait que pour toute suite binaire s de longueur n, on a $\partial P_k(s) = s$. □

Notation. Soit $k \in \{0,1\}$. Soit G un graphe de Steinhaus à $n \geqslant 1$ sommets. Par abus de langage, on note $U_k(G)$ le graphe de Steinhaus à $n+3$ sommets dont la matrice d'adjacence est l'image par l'opérateur U_k de la matrice d'adjacence du graphe G, soit

$$\mathcal{A}(U_k(G)) := U_k(\mathcal{A}(G)).$$

On peut alors maintenant énoncer le théorème qui permet l'étude des graphes de Steinhaus pairs.

Théorème 2.3.9 (Dymacek,[8])**.** *Soit G un graphe de Steinhaus à $n \geqslant 1$ sommets. Alors, le graphe G est pair si, et seulement si, les deux graphes $U_0(G)$ et $U_1(G)$ sont des graphes pairs à $n+3$ sommets.*

Preuve. Par le Théorème 2.3.6, si $U_k(G)$ est un graphe de Steinhaus pair à $n+3$ sommets pour $k = 0$ ou 1, alors le graphe $T(U_k(G)) = G$ est un graphe de Steinhaus pair à n sommets. Réciproquement, supposons que le graphe G soit un graphe de Steinhaus pair à n sommets. Soit $k \in \{0,1\}$. On note $M = \mathcal{A}(U_k(G)) = (a_{i,j})$. Par le Théorème 2.2.2, la matrice de Steinhaus associée au graphe G est bisymétrique donc, par définition de U_k, on en déduit que la matrice M est également bisymétrique. Le graphe $U_k(G)$ est donc symétrique par la Proposition 2.3.2. On obtient alors

$$\deg_{U_k(G)}(V_1) = \deg_{U_k(G)}(V_n) = \sum_{j=2}^{n} a_{1,j} = a_{1,2} + \sum_{j=3}^{n} a_{1,j} \equiv 2\sum_{j=3}^{n} a_{1,j} \equiv 0 \pmod 2.$$

De plus, par le Théorème 2.2.3, on a

$$\deg_{U_k(G)}(V_2) = \deg_{U_k(G)}(V_{n-1}) \equiv a_{1,n} \equiv 0 \pmod 2.$$

Enfin, par la proposition 2.3.5, on obtient, pour tout j, $3 \leqslant j \leqslant n-2$, l'équivalence suivante :

$$\begin{aligned}\deg_{U_k(G)}(V_j) &\equiv \deg_{U_k(G)}(V_2) + \deg_{U_k(G)}(V_j) \equiv \sum_{l=2}^{j-1} \left(\deg_{U_k(G)}(V_l) + \deg_{U_k(G)}(V_{l+1})\right) \\ &\equiv \sum_{l=2}^{j-1} \deg_{T(U_k(G))}(V_{l-1}) \equiv \sum_{l=1}^{j-2} \deg_G(V_l) \equiv 0 \pmod 2.\end{aligned}$$

□

Théorème 2.3.10 (Dymacek,[8])**.** *Soit $n \geqslant 1$ un entier. Si on note $P(n)$ le nombre de graphes de Steinhaus pairs à n sommets, alors*

$$P(n) = 2^{\lfloor \frac{n}{3} \rfloor}.$$

Preuve. On déduit du Théorème 2.3.9 que, pour tout entier $n \geqslant 4$, on a

$$P(n) = 2 \times P(n-3).$$

On conclut la preuve en observant que pour $n \in \{1,2,3\}$, il n'y a qu'un seul graphe de Steinhaus pair à n sommets qui est le graphe totalement disconnexe, le graphe sans arête à n sommets. □

2.4 Graphes de Steinhaus impairs

On commence par rappeler que tout graphe simple possède un nombre pair de sommets de degrés impairs.

Proposition 2.4.1. *Soit G un graphe simple. Alors, le graphe G possède un nombre pair de sommets de degré impair.*

Preuve. Notons V l'ensemble des sommets et E l'ensemble des arêtes de G. Alors, comme chaque arête possède deux extrémités, on a

$$\sum_{v \in V} \deg(v) = 2 \times |E|.$$

En écrivant cette somme modulo 2, on obtient bien que le nombre de sommet de degré impair est pair. □

On en déduit immédiatement :

Proposition 2.4.2. *Il n'existe pas de graphe simple impair avec un nombre impair de sommets.*

On construit maintenant l'opérateur I qui permet la caractérisation des graphes de Steinhaus impairs à partir des graphes de Steinhaus pairs.

Définition 2.4.3. Soit I l'opérateur

$$I : \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$$

qui à toute matrice de Steinhaus $M(a_1, \ldots, a_{n-1})$ de taille $n \geqslant 1$ associe la matrice de Steinhaus $M(a_1, \ldots, a_{n-2}, a_{n-1} + 1)$.

Par exemple si $s = (1100)$, alors $I(M(1100)) = M(1101)$.

$$M(1100) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad M(1101) = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Proposition 2.4.4. *Pour toute matrice de Steinhaus M de taille $n \geqslant 1$, on a $I(I(M)) = M$.*

Preuve. Evident. □

Notation. Pour tout graphe de Steinhaus G à $n \geqslant 1$ sommets, on note $I(G)$ le graphe de Steinhaus à n sommets dont la matrice d'adjacence est l'image de celle du graphe G par l'opérateur I, i.e.

$$\mathcal{A}(I(G)) := I(\mathcal{A}(G)).$$

Proposition 2.4.5. *Soit G un graphe de Steinhaus à $n \geqslant 1$ sommets. Alors*

$$\deg_{I(G)}(V_i) \equiv \deg_G(V_i) + 1 \pmod 2,$$

pour tout i, $1 \leqslant i \leqslant n-1$. De plus, pour $i = n$,

$$\deg_{I(G)}(V_n) \equiv \deg_G(V_n) + n - 1 \pmod 2.$$

Preuve. Soient $M = \mathcal{A}(G) = (a_{i,j})$ et $I(M) = \mathcal{A}(I(G)) = (b_{i,j})$. Tout d'abord, examinons la structure de $I(M)$ en fonction de M. Par la Proposition 2.1.2, on a

$$b_{i,j} = \sum_{k=0}^{i-1} \binom{i-1}{k} b_{1,j-k} = \sum_{k=0}^{i-1} \binom{i-1}{k} a_{1,j-k} = a_{i,j}, \ \forall 1 \leqslant i < j \leqslant n-1,$$

et pour tout i, $2 \leqslant i \leqslant n-1$,

$$b_{i,n} = \sum_{k=0}^{i-1} \binom{i-1}{k} b_{1,n-k} = b_{1,n} + \sum_{k=1}^{i-1} \binom{i-1}{k} b_{1,n-k} = a_{1,n} + 1 + \sum_{k=1}^{i-1} \binom{i-1}{k} a_{1,n-k} = a_{i,n} + 1.$$

Pour tout i, $1 \leqslant i \leqslant n-1$, on obtient alors

$$\deg_{I(G)}(V_i) = \sum_{j=1}^{n-1} b_{i,j} + b_{i,n} \equiv \sum_{j=1}^{n-1} a_{i,j} + a_{i,n} + 1 \equiv \deg_G(V_i) + 1 \pmod 2.$$

De plus, pour $i = n$, on a

$$\deg_{I(G)}(V_n) = \sum_{j=1}^{n-1} b_{j,n} \equiv \sum_{j=1}^{n-1} (a_{j,n} + 1) \equiv \deg_G(V_n) + n - 1 \pmod 2.$$

□

Les graphes de Steinhaus impairs à $2n$ sommets peuvent alors être associés aux graphes de Steinhaus pairs à $2n$ sommets.

Théorème 2.4.6 (Dymacek,[8])**.** *Soit G un graphe de Steinhaus à $2n \geqslant 1$ sommets. Alors, le graphe G est pair si, et seulement si, le graphe $I(G)$ est impair.*

Preuve. Immédiat par la Proposition 2.4.5. □

Théorème 2.4.7 (Dymacek,[8]). *Soit $n \geqslant 1$ un entier. Si on note $Imp(n)$ le nombre de graphes de Steinhaus impairs à n sommets, alors*

$$Imp(n) = \begin{cases} 2^{\lfloor \frac{n}{3} \rfloor} & \text{si } n \text{ pair,} \\ 0 & \text{si } n \text{ impair.} \end{cases}$$

Preuve. Par la Proposition 2.4.2 dans le cas où n est impair et le Théorème 2.4.6 dans le cas où n est pair. □

Chapitre 3

Graphes de Steinhaus réguliers

Dans ce chapitre, on s'intéresse aux graphes de Steinhaus réguliers et en particulier à ceux de degré impair. Des résultats sur ces graphes réguliers sont conjecturés dans [2, 8]. On rappelle ces conjectures à la Section 3.1 et on prouve que les suites de la forme $(110)^m$ engendrent une famille de graphes de Steinhaus réguliers de degré pair. On rappelle également un théorème énoncé dans [8] et prouvé dans [2] qui donne la structure de la matrice de Steinhaus associée à un graphe régulier de degré impair. A la Section 3.2, ce théorème est raffiné et on introduit la notion de matrices de Steinhaus multisymétriques. A la Section 3.3, on détermine les relations liant les degrés d'un graphe de Steinhaus aux éléments de sa matrice associée si celle-ci est multisymétrique. Ces résultats permettent alors, à la Section 3.4, d'étudier les graphes de Steinhaus réguliers modulo 4 dont la matrice de Steinhaus est multisymétrique. On détermine une borne supérieure du nombre de ces graphes et on prouve qu'il n'existe pas de graphe de Steinhaus régulier à n sommets dont la matrice associée est multisymétrique pour tout entier n impair, à l'exception du graphe sans arête. Enfin, les divers résultats de ce chapitre, qui apparaissent dans [6], permettent de pousser la vérification jusqu'à 1500 sommets que K_2, le graphe complet à 2 sommets, est le seul graphe de Steinhaus régulier de degré impair, améliorant ainsi d'un facteur 12 la borne précédente connue (117 sommets).

3.1 Graphes de Steinhaus réguliers

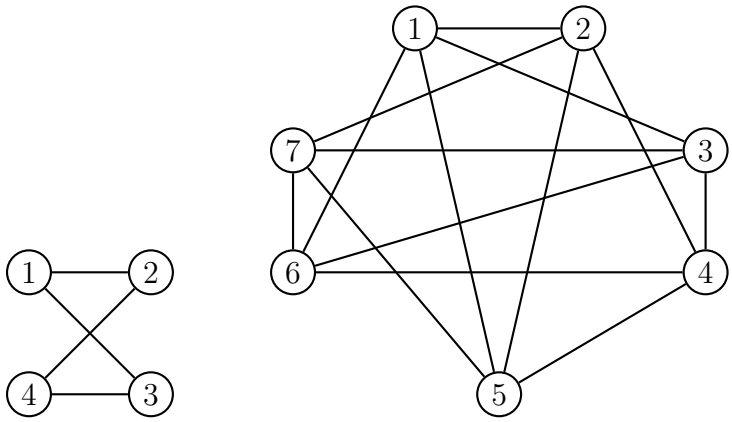
On commence par énoncer les conjectures faites en 1979 par Dymacek [8] et portant sur les graphes de Steinhaus réguliers.

Conjecture 3.1.1. Les graphes de Steinhaus réguliers de degré pair sont le graphe sans arête à n sommets, pour tout entier $n \geqslant 1$, et le graphe $G(s)$ à $n = 3m + 1$ sommets engendré par la suite périodique $s = (110)^m$ de longueur $3m$, pour tout entier $m \geqslant 1$.

Conjecture 3.1.2. Le graphe complet à deux sommets K_2 est le seul graphe de Steinhaus régulier de degré impair.

Une première vérification de ces conjectures a été faite jusqu'à 25 sommets en 1988 [2]. Plus récemment, en 2007, la vérification a été poussée jusqu'à 117 sommets [1]. Ce progrès a été réalisé en recherchant les graphes réguliers parmi les graphes de Steinhaus pairs et impairs. Grâce à leur étude présentée au Chapitre 2, il est évident qu'il est plus rapide de rechercher parmi $2^{\lfloor \frac{n}{3} \rfloor + 1}$ graphes paires et impairs, pour n pair, ou parmi $2^{\lfloor \frac{n}{3} \rfloor}$ graphes paires et impairs, pour n impair, que parmi l'ensemble des 2^{n-1} graphes de Steinhaus à n sommets. Les résultats obtenus au cours de ce chapitre vont permettre de vérifier, par ordinateur, la Conjecture 3.1.2 jusqu'à 1500 sommets, améliorant ainsi d'un facteur 12 la borne précédente connue.

On commence par vérifier que les suites de la forme $(110)^m$ engendrent bien des graphes de Steinhaus réguliers de degré pair. A la Figure 3.1 sont représentés les graphes de Steinhaus $G(110)$ et $G(110110)$ qui sont réguliers de degré 2 et 4 respectivement.



$G(110)$ $G(110110)$

FIG. 3.1 – Les premiers graphes de Steinhaus réguliers de degré pair

Théorème 3.1.3. *Pour tout entier $m \geqslant 1$, le graphe de Steinhaus $G((110)^m)$ à $3m+1$ sommets est régulier de degré $2m$.*

Ce résultat est souvent cité mais n'est jamais prouvé explicitement dans la littérature. La preuve donnée ici est basée sur une détermination explicite des éléments de la matrice de Steinhaus associée à la suite $(110)^m$, pour tout entier $m \geqslant 1$.

Preuve. Soit $m \geqslant 1$ un entier. Posons $M = M((110)^m) = (a_{i,j})$ la matrice de Steinhaus de taille $3m+1$ associée au graphe $G((110)^m)$. On commence par déterminer explicitement chaque élément du triangle supérieur de la matrice M. Pour tout i et tout j, $1 \leqslant i < j \leqslant 3m+1$, on a

$$a_{i,j} = \begin{cases} 0 \text{ pour } (i,j) \equiv (0,2),(1,1),(2,0) \pmod 3, \\ 1 \text{ pour } (i,j) \equiv (0,0),(0,1),(1,0),(1,2),(2,1),(2,2) \pmod 3. \end{cases}$$

Ce résultat se vérifie rapidement grâce à la relation :

$$a_{i,j} = a_{i-1,j-1} + a_{i-1,j}, \ \forall 2 \leqslant i < j \leqslant 3m+1.$$

De plus, on peut remarquer que, dans le triangle supérieur de M, trois éléments consécutifs dans une même ligne ou une même colonne sont composés exactement de deux 1 et de un 0, à savoir,

$$(a_{i,j}, a_{i,j+1}, a_{i,j+2}) \in \{(110), (101), (011)\},\ \forall 1 \leqslant i < j \leqslant 3m-1,$$

$$(a_{i-2,j}, a_{i-1,j}, a_{i,j}) \in \{(110), (101), (011)\},\ \forall 3 \leqslant i < j \leqslant 3m+1.$$

On obtient alors

$$\deg(V_1) = \sum_{j=2}^{3m+1} a_{1,j} = \sum_{k=0}^{m-1} (a_{1,3k+2} + a_{1,3k+3} + a_{1,3k+4}) = 2m,$$
$$\deg(V_{3m+1}) = \sum_{i=1}^{3m} a_{i,3m+1} = \sum_{k=0}^{m-1} (a_{3k+1,3m+1} + a_{3k+2,3m+1} + a_{3k+3,3m+1}) = 2m.$$

De plus, pour tout l, $1 \leqslant l \leqslant m$, on a

$$\deg(V_{3l}) = \sum_{i=1}^{3l-1} a_{i,3l} + \sum_{j=3l+1}^{3m+1} a_{3l,j} = \sum_{k=0}^{l-2} (a_{3k+1,3l} + a_{3k+2,3l} + a_{3k+3,3l}) + a_{3l-2,3l} + a_{3l-1,3l}$$
$$+a_{3l,3l+1} + \sum_{k=l}^{m-1} (a_{3l,3k+2} + a_{3l,3k+3} + a_{3l,3k+4}) = 2(l-1) + 1 + 0 + 1 + 2(m-l) = 2m.$$

De même, pour tout l, $1 \leqslant l \leqslant m-1$, on a

$$\deg(V_{3l+1}) = \sum_{i=1}^{3l} a_{i,3l+1} + \sum_{j=3l+2}^{3m+1} a_{3l+1,j} = \sum_{k=0}^{l-1} (a_{3k+1,3l+1} + a_{3k+2,3l+1} + a_{3k+3,3l+1})$$
$$+ \sum_{k=l}^{m-1} (a_{3l+1,3k+2} + a_{3l+1,3k+3} + a_{3l+1,3k+4}) = 2l + 2(m-l) = 2m.$$

Enfin, pour tout l, $0 \leqslant l \leqslant m-1$, on obtient

$$\deg(V_{3l+2}) = \sum_{i=1}^{3l+1} a_{i,3l+2} + \sum_{j=3l+3}^{3m+1} a_{3l+2,j} = \sum_{k=0}^{l-1} (a_{3k+1,3l+2} + a_{3k+2,3l+2} + a_{3k+3,3l+2})$$
$$+a_{3l+1,3l+2} + a_{3l+2,3l+3} + a_{3l+2,3l+4} + \sum_{k=l+1}^{m-1} (a_{3l+2,3k+2} + a_{3l+2,3k+3} + a_{3l+2,3k+4})$$
$$= 2l + 1 + 0 + 1 + 2(m-l-1) = 2m.$$

Le graphe $G((110)^m)$ est donc bien régulier de degré pair $2m$. □

Dans la suite de ce chapitre, on s'intéresse uniquement à la conjecture dans le cas impair. On termine cette section avec le théorème suivant, qui permet d'obtenir une première idée de la forme d'une matrice de Steinhaus associée à un graphe régulier de degré impair.

Théorème 3.1.4 (Dymacek,[8]). *Soit G un graphe de Steinhaus à $2n$ sommets et régulier de degré impair k. Soit $\mathcal{A}(G) = (a_{i,j})$ sa matrice de Steinhaus associée. Alors,*

– $k = n$,
– $G \setminus \{V_1, V_{2n}\}$ *est un graphe de Steinhaus régulier de degré pair* $n-1$,
– $a_{1,j} = a_{1,2n-j+1}$ *pour tout* j, $2 \leqslant j \leqslant 2n-1$.

La preuve de ce théorème est basée sur le Théorème 2.2.2.

Preuve. On pose

$$M = \mathcal{A}(G) = (a_{i,j})_{1 \leqslant i,j \leqslant 2n},$$

$$G' = G \setminus \{V_1, V_{2n}\},$$

$$N = \mathcal{A}(G') = (a_{i,j})_{2 \leqslant i,j \leqslant 2n-1}.$$

Comme le graphe G est impair à $2n$ sommets, on en déduit que le graphe $I(G)$ est pair par la Proposition 2.4.5. Par conséquent, $I(M)$ est une matrice de Steinhaus bisymétrique par le Théorème 2.2.2. Par définition d'une matrice bisymétrique et de l'opérateur I, on obtient

$$a_{1,j} \equiv a_{2n-j+1,2n} + 1 \pmod 2, \ \forall 2 \leqslant j \leqslant 2n-1.$$

De plus, comme $I(M)$ est bisymétrique, la sous-matrice N est également une matrice de Steinhaus bisymétrique et donc son graphe G' est symétrique par la Proposition 2.3.2, soit

$$\deg_{G'}(V_i) = \deg_{G'}(V_{2n-i-1}), \ \forall 1 \leqslant i \leqslant 2n-2.$$

Pour tout entier i, $2 \leqslant i \leqslant 2n-1$, on obtient l'égalité suivante

$$\deg_G(V_i) = \sum_{j=1}^{i-1} a_{j,i} + \sum_{j=i+1}^{2n} a_{i,j} = a_{1,i} + a_{i,2n} + \deg_{G'}(V_{i-1}).$$

On en déduit que

$$a_{1,i} + a_{i,2n} = \deg_G(V_i) - \deg_{G'}(V_{i-1}) = \deg_G(V_{2n-i+1}) - \deg_{G'}(V_{2n-i}) = a_{1,2n-i+1} + a_{2n-i+1,2n}.$$

Comme les éléments de la matrice M sont dans $\{0,1\}$, on a $a_{1,i} = a_{1,2n-i+1}$ pour tout i, $2 \leqslant i \leqslant 2n-1$, et $a_{1,i} + a_{i,2n} = 1$. Par conséquent, on obtient l'égalité

$$\deg_{G'}(V_i) = \deg_G(V_{i+1}) - 1, \ \forall 1 \leqslant i \leqslant 2n-2.$$

Le graphe de Steinhaus G' est donc régulier de degré pair $k-1$. Enfin, on détermine k de la manière suivante :

$$2k = \deg_G(V_1) + \deg_G(V_{2n}) = \sum_{i=2}^{2n} a_{1,i} + \sum_{i=1}^{2n-1} a_{i,2n} = 2a_{1,n} + \sum_{i=2}^{2n-1} (a_{1,i} + a_{i,2n}) = 2 + 2n - 2 = 2n,$$

soit $k = n$. Ce qui conclut la preuve de ce théorème. □

3.2 Matrices de Steinhaus multisymétriques

Définition 3.2.1. Soit $M = (a_{i,j})$ une matrice carrée de taille $n \geqslant 1$. La matrice M est dite *multisymétrique* si elle est bisymétrique et si chaque ligne de son triangle supérieur est une suite symétrique, i.e., pour tout i et tout j, $1 \leqslant i < j \leqslant n$, on a

$$a_{i,j} = a_{i,n-j+i+1}.$$

Par exemple, la matrice M ci-dessous est une matrice multisymétrique de taille $n = 5$.

$$M = \begin{pmatrix} 1 & 2 & 0 & 0 & 2 \\ 2 & 3 & 0 & 3 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 3 & 0 & 3 & 2 \\ 2 & 0 & 0 & 2 & 1 \end{pmatrix}$$

Tout d'abord, il est facile de voir que chaque colonne de la partie triangulaire supérieure d'une matrice multisymétrique est également symétrique.

Proposition 3.2.2. *Soit $M = (a_{i,j})$ une matrice multisymétrique de taille n. Alors, chaque colonne de la partie triangulaire supérieure de M est une suite symétrique, c'est-à-dire $a_{i,j} = a_{j-i,j}$ pour tout i et tout j, $1 \leqslant i < j \leqslant n$.*

Preuve. Provient de la relation : $a_{i,j} = a_{i,n-j+i+1} = a_{j-i,n-i+1} = a_{j-i,j}$ pour tout i et tout j, $1 \leqslant i < j \leqslant n$. □

Le résultat suivant caractérise les matrices de Steinhaus multisymétriques.

Proposition 3.2.3. *Soit $M = (a_{i,j})$ une matrice de Steinhaus de taille $n \geqslant 3$. Alors les assertions suivantes sont équivalentes :*

(i) la matrice M est multisymétrique,

(ii) la première ligne, la dernière colonne et la surdiagonale de M sont symétriques,

(iii) les éléments $a_{i,n-i+1}$, $a_{n-2i+1,n-i+1}$ et $a_{i,2i}$ s'annulent pour tout i et tout j, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$.

Preuve. Similaire à la preuve de la Proposition 2.2.4 en utilisant la Proposition 2.1.2 et la Proposition 3.2.2. □

On peut maintenant raffiner le Théorème 3.1.4.

Théorème 3.2.4. *Soit G un graphe de Steinhaus à $2n \geqslant 4$ sommets et régulier de degré impair n. Alors $G \setminus \{V_1, V_{2n}\}$ est un graphe de Steinhaus régulier de degré pair $n-1$ dont la matrice de Steinhaus associée est multisymétrique.*

Preuve. On note $M = \mathcal{A}(G) = (a_{i,j})_{1 \leqslant i,j \leqslant 2n}$ la matrice de Steinhaus associée au graphe G. Par le Théorème 3.1.4, on sait que le graphe de Steinhaus $G \setminus \{V_1, V_{2n}\}$ est régulier de degré pair $n-1$ et que l'on a

$$a_{1,j} = a_{1,2n-j+1},$$

pour tout j, $2 \leqslant j \leqslant 2n-1$. Alors, pour tout j, $3 \leqslant j \leqslant 2n-1$, on obtient

$$\begin{aligned} a_{2,j} + a_{2,2n-j+2} &= (a_{1,j-1} + a_{1,j}) + (a_{1,2n-j+1} + a_{1,2n-j+2}) \\ &= (a_{1,j-1} + a_{1,2n-j+2}) + (a_{1,j} + a_{1,2n-j+1}) = 0. \end{aligned}$$

Donc la première ligne du triangle supérieur de la matrice $N = (a_{i,j})_{2 \leqslant i,j \leqslant 2n-1}$, la matrice de Steinhaus associée au graphe $G \setminus \{V_1, V_{2n}\}$, est une suite symétrique. De plus, par le Théorème 2.2.2, la matrice N est bisymétrique. Finalement, par la Proposition 3.2.3 et la Proposition 2.2.4, la matrice N est multisymétrique. □

Remarque. A l'aide du Théorème 3.2.4, il est facile de voir que la Conjecture 3.1.1 entraîne la Conjecture 3.1.2. En effet, si la Conjecture 3.1.1 est vraie, alors le graphe totalement disconnexe à n sommets, i.e. le graphe de Steinhaus associé à la suite nulle $(0 \ldots 0)$, est le seul graphe de Steinhaus régulier de degré pair dont la matrice associée soit multisymétrique. Il s'ensuit, par le Théorème 3.2.4, que si $G(s)$ est un graphe de Steinhaus régulier de degré impair à $n+2$ sommets, alors $s = (0 \ldots 01)$ ou $s = (1 \ldots 1)$. Ainsi le graphe de Steinhaus $G(s)$ est le graphe étoile à $n+2$ sommets S_{n+2}, qui n'est pas un graphe régulier.

Dans la suite de ce chapitre, les matrices de Steinhaus multisymétriques sont étudiées en détail. Tout d'abord, on détermine le nombre de ces matrices à l'aide de l'opérateur T défini page 50.

Proposition 3.2.5. *Soit $M = (a_{i,j})$ une matrice de Steinhaus de taille $n \geqslant 4$. Alors l'extension M de $T(M)$ dépend uniquement des paramètres $a_{1,2}$, a_{1,j_0} et $a_{1,n}$, pour j_0 dans $\{3, \ldots, n-1\}$.*

Preuve. Soit $3 \leqslant j_0 \leqslant n-1$. Chaque élément $a_{1,j}$, pour tout j, $3 \leqslant j \leqslant n-1$, peut être exprimé en fonction de a_{1,j_0} et des éléments de la matrice $T(M) = (b_{i,j})$. En effet, on a

$$(*) \begin{cases} a_{1,j} = a_{1,j_0} + \displaystyle\sum_{k=j-1}^{j_0-2} b_{1,k}, & \text{pour } 3 \leqslant j < j_0, \\ a_{1,j} = a_{1,j_0} + \displaystyle\sum_{k=j_0-1}^{j-2} b_{1,k}, & \text{pour } j_0 < j \leqslant n-1. \end{cases}$$

Alors les éléments $a_{1,2}$, a_{1,j_0} et $a_{1,n}$ déterminent l'extension M de $T(M)$. □

C'est pourquoi, pour toute matrice de Steinhaus N de taille $n-3 \geqslant 1$, il existe 8 matrices de Steinhaus distinctes M de taille n telles que $T(M) = N$. L'opérateur T peut également être utilisé afin de paramétrer les matrices de Steinhaus multisymétriques.

Proposition 3.2.6. *Soit $M = (a_{i,j})$ une matrice de Steinhaus multisymétrique de taille n. Soit j_i un entier de l'ensemble $\{2i+1, \ldots, n-i\}$ pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{3} \right\rfloor$. Alors la matrice M dépend uniquement des paramètres suivants :*

- a_{1,j_1} *et* $\left\{ a_{2i,j_{2i}} \;\middle|\; 1 \leqslant i \leqslant \left\lceil \frac{n}{6} \right\rceil - 1 \right\}$, *pour n pair,*
- $\left\{ a_{2i+1,j_{2i+1}} \;\middle|\; 0 \leqslant i \leqslant \left\lceil \frac{n-3}{6} \right\rceil - 1 \right\}$, *pour n impair.*

Preuve. Soit $M = (a_{i,j})$ une matrice de Steinhaus multisymétrique de taille n. On considère les sous-matrices $T(M)$, $T^2(M) = T(T(M))$, $T^3(M)$, $T^4(M)$, ... Par applications successives de la Proposition 3.2.5 à l'extension $T^{i-1}(M)$ de $T^i(M)$ et comme les éléments $a_{i,n-i+1}$, $a_{n-2i+1,n-i+1}$ et $a_{i,2i}$ s'annulent pour tout i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$ par la Proposition 3.2.3, on en déduit les dépendances de la matrice multisymétrique M. □

Remarque. Des paramétrisations explicites d'une matrice de Steinhaus multisymétrique peuvent être obtenues par applications successives de $(*)$.

Le nombre de matrices de Steinhaus multisymétriques de taille $n \geqslant 1$ se déduit immédiatement de ce résultat.

Théorème 3.2.7. *Soit $n \geqslant 1$ un entier. Si l'on note $MS(n)$ le nombre de matrices de Steinhaus multisymétriques de taille n, alors on obtient*

$$MS(n) = \begin{cases} 2^{\left\lceil \frac{n}{6} \right\rceil} & , \text{ pour } n \text{ pair}, \\ 2^{\left\lceil \frac{n-3}{6} \right\rceil} & , \text{ pour } n \text{ impair}. \end{cases}$$

3.3 Degrés des sommets des graphes associés aux matrices de Steinhaus multisymétriques

Dans cette section, on analyse les degrés des sommets des graphes associés aux matrices de Steinhaus multisymétriques de taille $n \geqslant 1$. On voit que, pour de tels graphes, la connaissance des degrés des sommets modulo 4 impose de fortes conditions sur leur matrice associée. Afin de prouver ce résultat, on distingue différents cas selon la parité de n.

Proposition 3.3.1. *Soit n un nombre pair et G un graphe de Steinhaus à n sommets dont la matrice de Steinhaus associée $M = (a_{i,j})$ est multisymétrique. Alors, on a*

$$\deg(V_1) = \deg(V_n) \equiv a_{1,\frac{n}{2}+1} \pmod 2,$$

$$\deg(V_2) = \deg(V_{n-1}) \equiv 2a_{1,\frac{n}{2}+1} \pmod 4,$$

$$\deg(V_3) = \deg(V_{n-2}) \equiv 2a_{2,\frac{n}{2}+1} \pmod 4,$$

$$\deg(V_{2i}) = \deg(V_{n-2i+1}) \equiv 2a_{2,2i+1} + 2a_{i,2i+1} \pmod 4, \ \forall 2 \leqslant i \leqslant \tfrac{n}{2} - 2.$$

Preuve. Tout d'abord, la Proposition 3.2.3 implique que les éléments $a_{i,2i}$ et $a_{2i+1,\frac{n}{2}+i+1}$ s'annulent pour tout i, $1 \leqslant i \leqslant \frac{n}{2}-1$. Ceci conduit à

$$\deg(V_1) = \sum_{j=2}^{n} a_{1,j} = \sum_{j=2}^{\frac{n}{2}} (a_{1,j} + a_{1,n-j+2}) + a_{1,\frac{n}{2}+1} \equiv a_{1,\frac{n}{2}+1} \pmod 2,$$

$$\deg(V_2) = a_{1,2} + 2\sum_{j=3}^{\frac{n}{2}+1} (a_{2,j} + a_{2,n-j+3}) = 2\sum_{j=3}^{\frac{n}{2}+1} a_{2,j} \equiv 2a_{1,2} + 2a_{1,\frac{n}{2}+1} \equiv 2a_{1,\frac{n}{2}+1} \pmod 4,$$

$$\deg(V_3) = (a_{1,3} + a_{2,3}) + \sum_{j=4}^{\frac{n}{2}+1} (a_{3,j} + a_{3,n-j+4}) + a_{3,\frac{n}{2}+2} = 2a_{2,3} + 2\sum_{j=4}^{\frac{n}{2}+1} a_{3,j} \equiv 2a_{2,\frac{n}{2}+1} \pmod 4,$$

et, pour tout i, $2 \leqslant i \leqslant \frac{n}{2}-2$, on a

$$\begin{aligned}
\deg(V_{2i}) &= \sum_{j=i+1}^{2i-1} (a_{j,2i} + a_{2i-j,2i}) + a_{i,2i} + \sum_{j=2i+1}^{\frac{n}{2}+i} (a_{2i,j} + a_{2i,n-j+2i+1}) \\
&= 2\sum_{j=i+1}^{2i-1} a_{j,2i} + 2\sum_{j=2i+1}^{\frac{n}{2}+i} a_{2i,j} \\
&\equiv 2\sum_{k=i+1}^{2i-1} a_{j,2i+1} + 2\sum_{j=i+2}^{2i} a_{j,2i+1} + 2\sum_{j=2i}^{\frac{n}{2}+i-1} a_{2i-1,j} + 2\sum_{j=2i+1}^{\frac{n}{2}+i} a_{2i-1,j} \\
&\equiv 2a_{i+1,2i+1} + 2a_{2i,2i+1} + 2a_{2i-1,2i} + 2a_{2i-1,\frac{n}{2}+i} \\
&\equiv 2a_{i+1,2i+1} + 2a_{2i-1,2i+1} \equiv 2a_{2,2i+1} + 2a_{i,2i+1} \pmod 4.
\end{aligned}$$

Enfin, on complète la preuve par la Proposition 2.3.2. □

Remarque. Soit n un nombre pair. Dans chaque graphe de Steinhaus à n sommets dont la matrice de Steinhaus est multisymétrique, le 4ème sommet V_4 est de degré divisible par 4.

Proposition 3.3.2. *Soit n un nombre impair et G un graphe de Steinhaus à n sommets dont la matrice de Steinhaus associée $M = (a_{i,j})$ est multisymétrique. Alors, on a*

$$\deg(V_1) = \deg(V_n) \equiv 0 \pmod 2,$$

$$\deg(V_2) = \deg(V_{n-1}) \equiv 2a_{1,\frac{n+1}{2}} \pmod 4,$$

$$\deg(V_{2i}) \equiv 2a_{i+1,2i+1} + 2a_{2i-1,2i+1} + 2a_{2i-1,\frac{n-1}{2}+i} \pmod 4,\ \forall 2 \leqslant i \leqslant \tfrac{n-3}{2},$$

$$\deg(V_{2i+1}) \equiv 2a_{2,2i+2} \pmod 4,\ \forall 1 \leqslant i \leqslant \tfrac{n-3}{2}.$$

Preuve. La Proposition 3.2.3 implique que les éléments $a_{i,2i}$ et $a_{2i,\frac{n+1}{2}+i}$ s'annulent pour tout

i, $1 \leqslant i \leqslant \frac{n-1}{2}$. Ceci entraîne

$$\begin{aligned}
\deg(V_1) &= \sum_{j=2}^{\frac{n+1}{2}} (a_{1,j} + a_{1,n-j+2}) = 2\sum_{j=2}^{\frac{n+1}{2}} a_{1,j} \equiv 0 \pmod 2,\\
\deg(V_2) &= a_{1,2} + \sum_{j=3}^{\frac{n+1}{2}} (a_{2,j} + a_{2,n-j+3}) + a_{2,\frac{n+3}{2}}\\
&= 2\sum_{j=3}^{\frac{n+1}{2}} a_{2,j} \equiv 2a_{1,2} + 2a_{1,\frac{n+1}{2}} \equiv 2a_{1,\frac{n+1}{2}} \pmod 4.
\end{aligned}$$

De même, pour tout i, $2 \leqslant i \leqslant \frac{n-3}{2}$, on a

$$\begin{aligned}
\deg(V_{2i}) &= \sum_{j=i+1}^{2i-1} (a_{j,2i} + a_{2i-j,2i}) + a_{i,2i} + \sum_{j=2i+1}^{\frac{n-1}{2}+i} (a_{2i,j} + a_{2i,n-j+2i+1}) + a_{2i,\frac{n+1}{2}+i}\\
&= 2\sum_{j=i+1}^{2i-1} a_{j,2i} + 2\sum_{j=2i+1}^{\frac{n-1}{2}+i} a_{2i,j}\\
&\equiv 2\sum_{j=i+1}^{2i-1} a_{j,2i+1} + 2\sum_{j=i+2}^{2i} a_{j,2i+1} + 2\sum_{j=2i}^{\frac{n-3}{2}+i} a_{2i-1,j} + 2\sum_{j=2i+1}^{\frac{n-1}{2}+i} a_{2i-1,j}\\
&\equiv 2a_{i+1,2i+1} + 2a_{2i,2i+1} + 2a_{2i-1,2i} + 2a_{2i-1,\frac{n-1}{2}+i}\\
&\equiv 2a_{i+1,2i+1} + 2a_{2i-1,2i+1} + 2a_{2i-1,\frac{n-1}{2}+i} \pmod 4,
\end{aligned}$$

et pour tout i, $1 \leqslant i \leqslant \frac{n-3}{2}$, on obtient

$$\begin{aligned}
\deg(V_{2i+1}) &= \sum_{j=i+1}^{2i} (a_{j,2i+1} + a_{2i-j+1,2i+1}) + \sum_{j=2i+2}^{\frac{n+1}{2}+i} (a_{2i+1,j} + a_{2i+1,n-j+2i+2})\\
&= 2\sum_{j=i+1}^{2i} a_{j,2i+1} + 2\sum_{j=2i+2}^{\frac{n+1}{2}+i} a_{2i+1,j}\\
&\equiv 2\sum_{j=i+1}^{2i} a_{j,2i+2} + 2\sum_{j=i+2}^{2i+1} a_{j,2i+2} + 2\sum_{j=2i+1}^{\frac{n-1}{2}+i} a_{2i,j} + 2\sum_{j=2i+2}^{\frac{n+1}{2}+i} a_{2i,j}\\
&\equiv 2a_{i+1,2i+2} + 2a_{2i+1,2i+2} + 2a_{2i,2i+1} + 2a_{2i,\frac{n+1}{2}+i}\\
&\equiv 2a_{2i,2i+2} \equiv 2a_{2,2i+2} \pmod 4.
\end{aligned}$$

Enfin, on complète la preuve par la Proposition 2.3.2. □

Remarque. Soit n un nombre impair. Dans chaque graphe de Steinhaus à n sommets dont la matrice de Steinhaus associée est multisymétrique, le 3ème sommet V_3 est de degré divisible par 4.

3.4 Matrices de Steinhaus multisymétriques associées à des graphes de Steinhaus réguliers modulo 4

Dans cette section, on considère les matrices de Steinhaus multisymétriques de taille $n \geqslant 1$ associées à des graphes de Steinhaus réguliers modulo 4, i.e. où tous les sommets sont de même degré modulo 4. Tout d'abord, on peut déterminer une borne supérieure du nombre de ces matrices. Deux cas sont distingués, suivant la parité de n.

Théorème 3.4.1. *Pour tout nombre pair n, il y a au plus $2^{\lceil \frac{n}{24} \rceil}$ matrices de Steinhaus multisymétriques de taille n dont le graphe de Steinhaus associé soit régulier modulo 4.*

Preuve. Soit n un nombre pair et $M = (a_{i,j})$ une matrice de Steinhaus multisymétrique de taille n. Par la Proposition 3.2.6, la matrice M peut être paramétrée par

$$a_{1,\frac{n}{2}+1} \text{ et } \{a_{2i,4i+1} \mid 1 \leqslant i \leqslant m-1\},$$

avec

$$m = \left\lceil \frac{n}{6} \right\rceil.$$

Supposons que l'on connaisse les p paramètres de

$$P = \{a_{2i,4i+1} \mid m-p \leqslant i \leqslant m-1\}.$$

Alors, par la Proposition 3.2.6, la matrice de Steinhaus multisymétrique $T^{2(m-p-1)}(M)$ peut être paramétrée par P. Donc les éléments

$$\left\{ a_{i,2i+1} \;\middle|\; 2(m-p)-1 \leqslant i \leqslant \frac{n}{2} - (m-p) \right\}$$

dans $T^{2(m-p-1)}(M)$ ne dépendent que des paramètres de P. De plus, si le graphe de Steinhaus associé à M est régulier modulo 4, alors la Proposition 3.3.1 implique que $a_{1,\frac{n}{2}+1} = 0$ et

$$a_{2,2i+1} = a_{i,2i+1},$$

pour tout i, $2 \leqslant i \leqslant \frac{n}{2} - 1$. Il s'ensuit que les éléments

$$a_{2i,n-2(m-p)+1} = \sum_{k=0}^{i-1} \binom{i-1}{k} a_{2,2(\frac{n}{2}-(m-p)-k)+1} = \sum_{k=0}^{i-1} \binom{i-1}{k} a_{\frac{n}{2}-(m-p)-k,2(\frac{n}{2}-(m-p)-k)+1}$$

dépendent seulement des paramètres de P pour tout i, $1 \leqslant i \leqslant \frac{n}{2} - 3(m-p) + 2$. Supposons maintenant que p soit solution de l'inégalité suivante :

$$\frac{n}{2} - 3(m-p) + 2 \geqslant m - p - 1.$$

Alors, comme dans la preuve de la Proposition 3.2.6, on peut voir que l'extension M de $T^{2(m-p-1)}(M)$ dépend uniquement des éléments $a_{2i,n-2(m-p)+1}$ pour tout i, $1 \leqslant i \leqslant m-p-1$,

et donc tous les éléments de la matrice M peuvent être exprimés en fonction des p paramètres de P. Finalement une solution de cette inégalité est obtenue pour

$$p = \left\lceil \frac{n}{24} \right\rceil \geqslant \left\lceil \frac{n}{6} \right\rceil - \frac{n+6}{8}.$$

□

Théorème 3.4.2. *Pour tout nombre impair n, il y a au plus $2^{\lceil \frac{n}{30} \rceil}$ matrices de Steinhaus multisymétriques de taille n dont le graphe de Steinhaus associé est régulier modulo 4.*

Preuve. Soit n un nombre impair et $M = (a_{i,j})$ une matrice de Steinhaus multisymétrique de taille n. Par la Proposition 3.2.6, la matrice M dépend uniquement des paramètres $a_{2i+1,\frac{n+1}{2}+i}$ pour tout i, $0 \leqslant i \leqslant \left\lceil \frac{n-3}{6} \right\rceil - 1$. Si le graphe de Steinhaus associé à M est régulier modulo 4, alors la Proposition 3.3.2 implique que $a_{2,2j} = 0$ pour tout j, $2 \leqslant j \leqslant \frac{n-1}{2}$, et donc

$$a_{2i,2j} = \sum_{k=0}^{i-1} a_{2,2j-2k} = 0,$$

pour tout i et tout j, $1 \leqslant i < j \leqslant \frac{n-1}{2}$.

Si $n \equiv 1 \pmod 4$, alors $\frac{n+1}{2}$ est impair et

$$a_{4i+1,\frac{n+1}{2}+2i} = a_{4i,\frac{n-1}{2}+2i} + a_{4i,\frac{n+1}{2}+2i} = 0,$$

pour tout i, $0 \leqslant i \leqslant \left\lfloor \frac{\lceil \frac{n-3}{6} \rceil - 1}{2} \right\rfloor$. Par conséquent, la matrice M peut être paramétrée par

$$\left\{ a_{4i+3,\frac{n+3}{2}+2i} \;\middle|\; 0 \leqslant i \leqslant m-1 \right\},$$

avec

$$m = \left\lceil \frac{\lceil \frac{n-3}{6} \rceil - 1}{2} \right\rceil.$$

Supposons que l'on connaisse les p paramètres de

$$P = \left\{ a_{4i+3,\frac{n+3}{2}+2i} \;\middle|\; m-p \leqslant i \leqslant m-1 \right\}.$$

Alors, par la Proposition 3.2.6, la matrice multisymétrique $T^{4(m-p)-1}(M)$ peut être paramétrée par P. Par conséquent les éléments

$$\left\{ a_{i,2i+1} \;\middle|\; 4(m-p) \leqslant i \leqslant \frac{n-1}{2} - 2(m-p) \right\}$$

dans $T^{4(m-p)-1}(M)$ dépendent uniquement des paramètres de P. De plus, si le graphe de Steinhaus associé à M est régulier modulo 4, alors la Proposition 3.3.2 implique que

$$a_{2,2i+1} = a_{2i-1,2i+1} \equiv a_{i+1,2i+1} + a_{2i-1,\frac{n-1}{2}+i} \equiv a_{i+1,2i+1} + a_{\left(\frac{n+1}{2}-i\right)+1,2\left(\frac{n+1}{2}-i\right)+1} \pmod 2,$$

pour tout i, $1 \leqslant i \leqslant \frac{n-1}{2}$. Si l'inégalité

$$\frac{n+1}{2} - 4(m-p) \geqslant 4(m-p)$$

est vérifiée, alors les éléments $a_{2,2i+1}$ dépendent uniquement des paramètres de P pour tout i, $4(m-p) \leqslant i \leqslant \frac{n+1}{2} - 4(m-p)$. Comme $a_{2,2i} = 0$ pour tout i, $4(m-p) \leqslant i \leqslant \frac{n+3}{2} - 4(m-p)$, il s'ensuit que les éléments

$$\left\{ a_{i,j} \;\middle|\; \begin{array}{c} 2 \leqslant i \leqslant n+5-16(m-p) \\ 8(m-p)+i-1 \leqslant j \leqslant n+3-8(m-p) \end{array} \right\}$$

dépendent uniquement des paramètres de P. Supposons maintenant que p soit solution de l'inégalité suivante :

$$n + 5 - 16(m-p) \geqslant 4(m-p) - 1.$$

Alors, l'extension M de $T^{(4(m-p)-1)}(M)$ dépend uniquement des éléments $a_{i,n+3-8(m-p)}$ pour tout i, $2 \leqslant i \leqslant 4(m-p)-1$, et $a_{1,\frac{n+1}{2}}$ qui s'annule par la Proposition 3.3.2. Donc, tous les éléments de la matrice M dépendent uniquement des p paramètres de P. Finalement, une solution de l'inégalité est obtenue pour

$$p = \left\lceil \frac{n}{30} \right\rceil \geqslant \left\lceil \frac{\left\lceil \frac{n-3}{6} \right\rceil - 1}{2} \right\rceil - \frac{n+6}{20}.$$

Si $n \equiv 3 \pmod 4$, alors $\frac{n+1}{2}$ est pair et

$$a_{4i+3,\frac{n+3}{2}+2i} = a_{4i+2,\frac{n+1}{2}+2i} + a_{4i+2,\frac{n+3}{2}+2i} = 0,$$

pour tout i, $0 \leqslant i \leqslant \left\lceil \frac{\left\lceil \frac{n-3}{6} \right\rceil - 1}{2} \right\rceil - 1$. Par conséquent la matrice M peut être paramétrée par

$$\left\{ a_{4i+1,\frac{n+1}{2}+2i} \;\middle|\; 0 \leqslant i \leqslant m \right\}$$

avec

$$m = \left\lfloor \frac{\left\lceil \frac{n-3}{6} \right\rceil - 1}{2} \right\rfloor.$$

Comme précédemment, dans le cas $n \equiv 1 \pmod 4$, on peut prouver que tous les éléments de la matrice M dépendent uniquement des p paramètres de

$$\left\{ a_{4i+1,\frac{n+1}{2}+2i} \;\middle|\; m-p+1 \leqslant i \leqslant m \right\}$$

si p est solution de l'inégalité suivante

$$n - 16(m-p) - 4 \geqslant 4(m-p) + 1.$$

Une solution est obtenue pour

$$p = \left\lceil \frac{n}{30} \right\rceil \geqslant \left\lfloor \frac{\left\lceil \frac{n-3}{6} \right\rceil - 1}{2} \right\rfloor - \frac{n-5}{20}.$$

□

Par la Proposition 3.2.6, en utilisant des paramétrisations explicites de matrices de Steinhaus multisymétriques dont le graphe associé est régulier modulo 4, on obtient le résultat suivant à l'aide d'une recherche par ordinateur :

Résultat calculatoire 3.4.3. *Pour tout entier $n \leqslant 1500$, le graphe sans arête à n sommets est le seul graphe de Steinhaus à n sommets avec une matrice de Steinhaus multisymétrique et qui soit régulier modulo 4.*

Ce résultat peut être rapidement prouvé pour tout nombre impair dans le cas spécial des graphes de Steinhaus réguliers à n sommets dont la matrice de Steinhaus est multisymétrique.

Théorème 3.4.4. *Pour tout nombre impair n, il n'y a pas de graphe de Steinhaus régulier à n sommets dont la matrice de Steinhaus est multisymétrique, à l'exception du graphe sans arête à n sommets.*

Preuve. Soit n un nombre impair. Soit G un graphe de Steinhaus régulier à n sommets et $M = (a_{i,j})$ sa matrice de Steinhaus associée. Alors la Proposition 3.3.2 implique que

$$\deg(V_i) \equiv 0 \pmod 4,$$

pour tout i, $1 \leqslant i \leqslant n$ et

$$a_{2,2i+2} = 0,$$

pour tout i, $1 \leqslant i \leqslant \frac{n-3}{2}$. Si l'on note par $\oplus$ la somme dans $\mathbb{Z}/2\mathbb{Z}$ et $+$ la somme dans les entiers, alors on obtient

$$\begin{aligned}
\deg(V_3) &= a_{1,3} + a_{2,3} + \sum_{j=4}^{n} a_{3,j} = (a_{1,2} \oplus a_{2,3} + a_{2,3}) + \sum_{j=2}^{\frac{n-3}{2}} (a_{3,2j+1} + a_{3,2j+2}) + 2a_{3,n} \\
&= 2a_{2,3} + \sum_{j=2}^{\frac{n-3}{2}} (a_{2,2j} \oplus a_{2,2j+1} + a_{2,2j+1} \oplus a_{2,2j+2}) + 2a_{2,n-1} \oplus a_{2,n} \\
&= 2\sum_{j=1}^{\frac{n-1}{2}} a_{2,2j+1} = 2(a_{1,2} + \sum_{j=3}^{n} a_{2,j}) = 2 \times \deg(V_2).
\end{aligned}$$

Ceci entraîne que $\deg(V_i) = 0$ pour tout i, $1 \leqslant i \leqslant n$, et donc G est le graphe sans arête à n sommets. □

Finalement, le résultat calculatoire précédent permet d'étendre la vérification de la Conjecture 3.1.2 jusqu'à $n \leqslant 1500$ sommets. En effet, comme prouvé dans une remarque de la Section 3.2, pour un graphe de Steinhaus G à $2n$ sommets, si $G \setminus \{V_1, V_{2n}\}$ est le graphe sans arête à $2n-2$ sommets, alors G est le graphe étoile à $2n$ sommets S_{2n} qui n'est pas un graphe régulier. Par conséquent, par le Théorème 3.2.4, on obtient

Théorème 3.4.5. *Il n'y a pas de graphe de Steinhaus régulier de degré impair à $2 < n \leqslant 1500$ sommets.*

Chapitre 4

Triangles de Steinhaus dans les groupes cycliques

Dans ce chapitre, on étudie les triangles de Steinhaus dans les groupes cycliques. Les résultats obtenus sont publiés dans [5]. A la Section 4.1, on définit la structure combinatoire de triangles de Steinhaus et on présente le Problème de Molluzzo qui est une généralisation, à tout groupe cyclique, du Problème de Steinhaus du Chapitre 1. Ce problème consiste à déterminer l'existence de suites balancées, c'est-à-dire de suites finies dont le triangle de Steinhaus associé contient chaque élément du groupe cyclique avec la même multiplicité. Jusqu'à ce jour, aucune solution n'était connue. On montre, tout d'abord, que ce problème n'admet pas toujours de solution positive en exhibant deux contre-exemples et on conjecture ensuite qu'il est vrai dans tout groupe cyclique d'ordre une puissance de premier. Le résultat principal de ce chapitre est la preuve que le Problème de Molluzzo est vrai dans tout groupe cyclique d'ordre une puissance de 3. Cette preuve est basée sur l'étude des suites arithmétiques dans les groupes cycliques. Après avoir étudié les longueurs admissibles des suites balancées et la projection de suites balancées à la Section 4.2, on s'intéresse, à la Section 4.3, aux triangles de Steinhaus associés aux suites arithmétiques. Les résultats obtenus permettent de prouver, aux Sections 4.4 et 4.5, que dans tout groupe cyclique d'ordre impair n, les suites arithmétiques de raison inversible sont balancées pour toutes les longueurs $m \equiv 0$ ou $-1 \pmod{\varphi(n)n}$. On récapitule alors, à la Section 4.6, ce que l'on sait maintenant à propos du Problème de Molluzzo et en particulier qu'il est vrai dans tout groupe cyclique d'ordre une puissance de 3. Enfin, à la Section 4.7, on prouve que, contrairement aux groupes cycliques d'ordre impair, presqu'aucune suite arithmétique n'est balancée dans les groupes cycliques d'ordre pair.

4.1 Triangles de Steinhaus et Problème de Molluzzo

4.1.1 Triangles de Steinhaus

Soit $\mathbb{Z}/n\mathbb{Z}$ le groupe cyclique d'ordre $n \geqslant 1$. Comme dans le cas des suites finies de $\mathbb{Z}/2\mathbb{Z}$ présenté au Chapitre 1, on peut définir des opérations de dérivation et d'intégration sur les suites finies de $\mathbb{Z}/n\mathbb{Z}$.

Définition 4.1.1. Soit $S = (a_1, \ldots, a_m)$ une suite de longueur finie $m \geqslant 2$ dans $\mathbb{Z}/n\mathbb{Z}$. La *suite dérivée* de S est la suite ∂S définie par

$$\partial S = (a_1 + a_2, \ldots, a_{m-1} + a_m),$$

où $+$ désigne la somme dans $\mathbb{Z}/n\mathbb{Z}$. C'est une suite de longueur $m-1$ dans $\mathbb{Z}/n\mathbb{Z}$. Par convention, on admet que $\partial S = \emptyset$ si la suite S est de longueur $m \leqslant 1$, où $\emptyset$ désigne la suite vide de longueur $m = 0$. Par itération du procédé de dérivation, on peut également définir récursivement la $i$ème dérivée $\partial^i S$ de la suite S par $\partial^0 S = S$ et $\partial^i S = \partial\left(\partial^{i-1} S\right)$ pour tout $i \geqslant 1$.

Proposition 4.1.2. *Soit $S = (a_1, \ldots, a_m)$ une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Alors pour tout i, $0 \leqslant i \leqslant m-1$, la $i$ème dérivée de S peut être exprimée en fonction des éléments de S de la manière suivante :*

$$\partial^i S = \left(\sum_{k=0}^{i} \binom{i}{k} a_{1+k} \ , \ \sum_{k=0}^{i} \binom{i}{k} a_{2+k} \ , \ \ldots\ldots \ , \ \sum_{k=0}^{i} \binom{i}{k} a_{m-i+k} \right).$$

Preuve. Par récurrence sur i avec la Définition 4.1.1. □

Définition 4.1.3. Soit S une suite de longueur $m \geqslant 0$ dans $\mathbb{Z}/n\mathbb{Z}$. On appelle *suite primitive* de S toute suite T de longueur $m+1$ telle que S soit sa suite dérivée, c'est-à-dire $\partial T = S$.

Proposition 4.1.4. *Pour toute suite $S = (a_1, \ldots, a_m)$ de longueur $m \geqslant 0$ dans $\mathbb{Z}/n\mathbb{Z}$, il existe exactement n suites primitives dans $\mathbb{Z}/n\mathbb{Z}$, chacune ayant un premier élément distinct. Pour tout i dans $\mathbb{Z}/n\mathbb{Z}$, on note $P_i(S)$ la suite primitive de S commençant par i. Alors,*

$$P_i(S) = \left(i, a_1 - i, a_2 - a_1 + i, \ldots\ldots, \sum_{k=1}^{m} (-1)^{m-k} a_k + (-1)^m i \right).$$

Preuve. Soit $S = (a_1, \ldots, a_m)$ une suite de longueur m dans $\mathbb{Z}/n\mathbb{Z}$. Si $m = 0$, alors $S = \emptyset$ et la suite (i) est bien une primitive de S, pour tout i de $\mathbb{Z}/n\mathbb{Z}$. Supposons maintenant que $m \geqslant 1$ et que $T = (b_1, \ldots, b_{m+1})$ soit une suite primitive de S. Alors, par récurrence sur j, on peut montrer que chaque élément b_j de T peut s'exprimer en fonction des éléments de S et de b_1, le premier élément de la suite T. Pour tout j, $2 \leqslant j \leqslant m+1$, on obtient

$$b_j = \sum_{k=1}^{j-1} (-1)^{j-k-1} a_k + (-1)^{j-1} b_1.$$

Il existe donc exactement n suites primitives de la suite S qui sont les suites $P_i(S)$ définies précédemment. □

De la même manière que dans $\mathbb{Z}/2\mathbb{Z}$, ces opérations sont, en quelque sorte, réciproques.

Proposition 4.1.5 (Théorème fondamental de l'analyse)**.** *Soient $S = (a_1, \ldots, a_m)$ une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$ et i un élément de $\mathbb{Z}/n\mathbb{Z}$. Alors,*

$$\partial P_i(S) = S,$$

$$P_i\left(\partial S\right) = S + \left((-1)^j(a_1 - i)\right)_{j=1}^{m},$$

où

$$\left((-1)^j(a_1 - i)\right)_{j=1}^{m} = (i - a_1, a_1 - i, i - a_1, a_1 - i, \ldots)$$

est la suite périodique de période 2 et de longueur m.

Preuve. Posons $P_i(S) = (b_1, \ldots, b_{m+1})$ et $\partial P_i(S) = (c_1, \ldots, c_m)$. Alors,

$$c_1 = b_1 + b_2 = i + (a_1 - i) = a_1,$$

et pour tout entier j, $2 \leqslant j \leqslant m$, on a

$$c_j = b_j + b_{j+1} = \left(\sum_{k=1}^{j-1} (-1)^{j-k-1} a_k + (-1)^{j-1} i\right) + \left(\sum_{k=1}^{j} (-1)^{j-k} a_k + (-1)^j i\right) = a_j.$$

On obtient donc bien que $\partial P_i(S) = S$.

Posons maintenant $\partial S = (b_1, \ldots, b_{m-1})$ et $P_i\left(\partial S\right) = (c_1, \ldots, c_m)$. Alors,

$$c_1 = i = a_1 + (i - a_1),$$

et pour tout entier j, $2 \leqslant j \leqslant m$, on obtient

$$\begin{aligned} c_j &= \sum_{k=1}^{j-1} (-1)^{j-k-1} b_k + (-1)^{j-1} i = \sum_{k=1}^{j-1} (-1)^{j-k-1} (a_k + a_{k+1}) + (-1)^{j-1} i \\ &= \sum_{k=1}^{j-1} (-1)^{j-k-1} a_k + \sum_{k=2}^{j} (-1)^{j-k} a_k + (-1)^{j-1} i = a_j + (-1)^j (a_1 - i). \end{aligned}$$

Ainsi $P_i\left(\partial S\right) = S + \left((-1)^j(a_1 - i)\right)_{j=1}^{m}$. Ce qui achève la preuve. □

Dans la suite de ce chapitre, on s'intéresse aux triangles de Steinhaus dans $\mathbb{Z}/n\mathbb{Z}$.

Définition 4.1.6. Soit $S = (a_1, \ldots, a_m)$ une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Le *triangle de Steinhaus* ΔS engendré par la suite S est l'union multiensembliste, i.e. où toutes les multiplicités sont ajoutées, des suites dérivées successives de S, c'est-à-dire,

$$\Delta S = \bigcup_{i=0}^{m-1} \partial^i S = \left\{ \sum_{k=0}^{i} \binom{i}{k} a_{j+k} \;\middle|\; 0 \leqslant i \leqslant m-1,\ 1 \leqslant j \leqslant m-i \right\}.$$

Remarque. Le triangle de Steinhaus engendré par une suite de longueur $m \geqslant 1$ est constitué de $\binom{m+1}{2}$ éléments de $\mathbb{Z}/n\mathbb{Z}$, comptés avec multiplicité.

Par exemple, le triangle de Steinhaus ΔS associé à la suite $S = (0122)$ de $\mathbb{Z}/3\mathbb{Z}$ peut être représenté comme à la Figure 4.1, où la $i$ème ligne du triangle correspond à la $(i-1)$ème suite dérivée $\partial^{i-1}S$ de S.

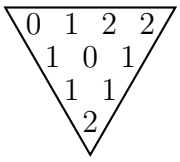


FIG. 4.1 – Un triangle de Steinhaus dans $\mathbb{Z}/3\mathbb{Z}$

Définition 4.1.7. Une suite finie S dans $\mathbb{Z}/n\mathbb{Z}$ est dite *balancée* si chaque élément de $\mathbb{Z}/n\mathbb{Z}$ apparaît avec la même multiplicité dans son triangle de Steinhaus ΔS.

Par exemple, la suite (2233) est balancée dans $\mathbb{Z}/5\mathbb{Z}$. En effet, comme représenté Figure 4.2, chaque élément de $\mathbb{Z}/5\mathbb{Z}$ apparaît deux fois dans son triangle de Steinhaus.

Remarque. Pour une suite S de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$, une condition nécessaire afin d'être balancée est que l'entier n divise le coefficient binomial $\binom{m+1}{2}$, i.e. le cardinal du triangle de Steinhaus ΔS.

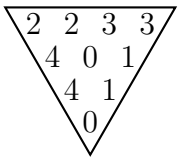


FIG. 4.2 – Le triangle de Steinhaus d'une suite balancée dans $\mathbb{Z}/5\mathbb{Z}$

Cette construction est due à John C. Molluzzo en 1976 [19].

4.1.2 Le Problème de Molluzzo

Molluzzo propose également une généralisation du problème de Steinhaus à tous les groupes cycliques.

Problème 4.1.8 (Molluzzo, 1976)**.** *Soit $n \geqslant 1$ un entier. Pour un entier $m \geqslant 1$ donné, est-il vrai qu'il existe une suite balancée de longueur m dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, le coefficient binomial $\binom{m+1}{2}$ est divisible par n ?*

Cette généralisation du Problème de Steinhaus correspond à la Question 8 de [10]. Jusqu'à ce jour, aucune solution de ce problème n'était connue pour $n \geqslant 3$.

Tout d'abord, on montre que le Problème de Molluzzo n'admet pas toujours de solution positive. En effet, cherchons, pour m petit, s'il existe une suite balancée de longueur m dans $\mathbb{Z}/n\mathbb{Z}$ telle que son triangle de Steinhaus associé soit constitué de chaque élément du groupe avec une multiplicité égale à 1. Pour $n = 1$ et $m = 1$, le résultat est évident ; pour $n = 3$ et $m = 2$, la suite (12) est balancée ; pour $n = 6$ et $m = 3$, la suite (135) est balancée ; pour $n = 10$ et $m = 4$, la suite (1694) est balancée. Ces suites et leurs triangles associés sont représentés à la Figure 4.3. Cependant, pour $m = 5$ et $m = 6$, une recherche exhaustive montre qu'il n'existe pas de telle suite de longueur m, fournissant ainsi les premiers contre-exemples au Problème de Molluzzo.

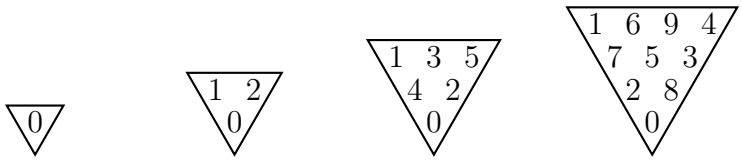


FIG. 4.3 – Triangles de Steinhaus où chaque élément du groupe a une multiplicité égale à 1

Résultat calculatoire 4.1.9 (contre-exemples au Problème de Molluzzo)**.**

1. *Il n'existe pas de suite balancée de longueur* $m = 5$ *dans* $\mathbb{Z}/15\mathbb{Z}$.
2. *Il n'existe pas de suite balancée de longueur* $m = 6$ *dans* $\mathbb{Z}/21\mathbb{Z}$.

Dans la suite de ce chapitre, les résultats obtenus permettent de répondre positivement et complètement au Problème de Molluzzo dans tout groupe cyclique d'ordre une puissance de 3. Plus généralement, il est prouvé que, dans chaque groupe cyclique d'ordre impair, il existe des suites balancées pour toutes les longueurs $m \equiv 0$ ou $-1 \pmod{\varphi(n)n}$. De ces résultats, on peut conjecturer que le Problème de Molluzzo est vrai dans tout groupe cyclique d'ordre une puissance de premier. Si cette conjecture s'avère être vraie, alors, grâce aux contre-exemples précédents, il ne peut exister aucune manière formelle de déduire une réponse positive au Problème de Molluzzo dans tout groupe cyclique d'ordre n, de la seule validité de ce problème dans tous les groupes cycliques d'ordre une puissance de premier.

4.2 Généralités sur les suites balancées

Dans cette section, on établit les longueurs admissibles pour les suites balancées dans $\mathbb{Z}/n\mathbb{Z}$ et on étudie le comportement de ces suites balancées et de leurs projections.

4.2.1 Longueur d'une suite balancée

Notations.

– L'ensemble des nombres premiers est noté $\mathcal{P}$.

– Pour tout nombre premier p, on note $v_p(n)$ la valuation p-adique de n, i.e. le plus grand exposant $e \geqslant 0$ pour lequel p^e divise n. Ainsi, la factorisation de n en éléments premiers peut s'écrire

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

– Le nombre de facteurs premiers distincts de n est noté $\omega(n)$, i.e. le nombre de premiers p pour lesquels $v_p(n) \geqslant 1$.

On a vu, à la Section 4.1, que pour une suite S de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$, une condition nécessaire afin d'être balancée est que n divise le coefficient binomial $\binom{m+1}{2}$, le cardinal du triangle de Steinhaus ΔS. L'ensemble des entiers $m \geqslant 1$ satisfaisant cette condition de divisibilité est décrit dans le théorème qui suit.

Théorème 4.2.1. *Soit $n \geqslant 1$ un entier. L'ensemble de tous les entiers $m \geqslant 1$ tels que le coefficient binomial $\binom{m+1}{2}$ soit un multiple de n est une réunion disjointe de $2^{\omega(n)}$ classes distinctes modulo $2n$ si n est pair, et du même nombre de classes distinctes modulo n si n est impair. De plus, cet ensemble comprend les classes $2n\mathbb{N}$ et $(2n-1)+2n\mathbb{N}$ si n est pair, et les classes $n\mathbb{N}$ et $(n-1)+n\mathbb{N}$ si n est impair.*

Preuve. Soient n et m deux entiers positifs. Alors,

$$\begin{aligned}\binom{m+1}{2} \equiv 0 \pmod{n} &\iff m(m+1) \equiv 0 \pmod{2n} \\ &\iff \begin{cases} m(m+1) \equiv 0 \pmod{2^{v_2(n)+1}} \\ m(m+1) \equiv 0 \pmod{p^{v_p(n)}},\ \forall p \in \mathcal{P} \setminus \{2\} \end{cases} \\ &\iff \begin{cases} m \equiv a_2 \pmod{2^{v_2(n)+1}} \\ m \equiv a_p \pmod{p^{v_p(n)}},\ \forall p \in \mathcal{P} \setminus \{2\} \end{cases}\end{aligned}$$

avec $a_p \in \{-1, 0\}$ pour tout nombre premier p. Chaque élément m de l'ensemble apparaît donc comme une solution d'un système de congruences composé de $\omega(n)$ équations non-triviales. Alors, le théorème des restes chinois montre qu'il existe une unique solution modulo n ou modulo $2n$, selon la parité de n. On en déduit qu'il existe $2^{\omega(n)}$ classes modulo $2n$ (resp. modulo n) pour tout nombre n pair (resp. impair). En particulier, si n est pair (resp. impair) et $a_p = 0$ pour chaque nombre premier p, alors les entiers m, pour qui le coefficient binomial $\binom{m+1}{2}$ est un multiple de n, constituent la classe $2n\mathbb{N}$ (resp. la classe $n\mathbb{N}$). De manière analogue, si n est pair (resp. impair) et $a_p = -1$ pour chaque nombre premier p, alors de tels entiers m forment la classe $(2n-1)+2n\mathbb{N}$ (resp. la classe $(n-1)+n\mathbb{N}$). □

Corollaire 4.2.2. *Soient p un nombre premier impair et $k \geqslant 1$ un entier. Alors, pour tout entier $m \geqslant 1$, on a*

$$\binom{m+1}{2} \equiv 0 \pmod{p^k} \iff m \equiv 0 \text{ ou } -1 \pmod{p^k}.$$

De même, pour tout entier $m \geqslant 1$, on a

$$\binom{m+1}{2} \equiv 0 \pmod{2^k} \iff m \equiv 0 \text{ ou } -1 \pmod{2^{k+1}}.$$

Par exemple, pour $n = 825 = 3 \cdot 5^2 \cdot 11$, l'ensemble des entiers $m \geqslant 1$ tels que le coefficient binomial $\binom{m+1}{2}$ soit divisible par 825 est la réunion disjointe des 8 classes $a + 825\mathbb{N}$ où $a \in \{0, 99, 275, 374, 450, 549, 725, 824\}$.

4.2.2 Projections de suites balancées

Pour tout multiensemble fini M de $\mathbb{Z}/n\mathbb{Z}$, on note $\mathfrak{m}_M$ la fonction de multiplicité de M, c'est-à-dire la fonction

$$\mathfrak{m}_M : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{N}$$

qui à chaque élément x de $\mathbb{Z}/n\mathbb{Z}$ associe le nombre d'occurrence $\mathfrak{m}_M(x)$ de x dans le multiensemble M. On convient que la fonction de multiplicité $\mathfrak{m}_M$ s'annule sur tout élément x qui n'est pas dans M.

Comme d'accoutumée, le cardinal $|M|$ d'un multiensemble fini M correspond au nombre total des éléments de M, comptés avec multiplicité, c'est-à-dire,

$$|M| = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \mathfrak{m}_M(x).$$

Soit S une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Comme le triangle de Steinhaus ΔS est un multiensemble de cardinal $\binom{m+1}{2}$, il s'ensuit que la suite S est balancée si, et seulement si, la fonction de multiplicité $\mathfrak{m}_{\Delta S}$, associée au multiensemble ΔS, est constante égale à $\frac{1}{n}\binom{m+1}{2}$.

Pour tout facteur q de l'entier $n \geqslant 1$, on note π_q le morphisme canonique et surjectif $\pi_q : \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/q\mathbb{Z}$. Pour une suite finie $S = (a_1, a_2, \ldots, a_m)$ de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$, on note

$$\pi_q(S) = (\pi_q(a_1), \pi_q(a_2), \ldots, \pi_q(a_m)),$$

sa suite projetée dans $\mathbb{Z}/q\mathbb{Z}$. On étudie maintenant le comportement des suites balancées de $\mathbb{Z}/n\mathbb{Z}$ sous l'action de la projection $\pi_q : \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/q\mathbb{Z}$.

Théorème 4.2.3 (Théorème de projection)**.** *Soient q un diviseur de n et S une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Alors, la suite S est balancée si, et seulement si, sa suite projetée $\pi_q(S)$ est aussi balancée et la fonction de multiplicité $\mathfrak{m}_{\Delta S} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{N}$ est constante sur chaque coset du sous-groupe $q\mathbb{Z}/n\mathbb{Z}$.*

Preuve. Pour tout x dans $\mathbb{Z}/n\mathbb{Z}$, il est clair que la multiplicité de $\pi_q(x)$ dans $\Delta\pi_q(S)$ est la somme des multiplicités dans ΔS de tous les éléments du coset $x + q\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire,

$$\mathfrak{m}_{\Delta\pi_q(S)}(\pi_q(x)) = \sum_{k=0}^{\frac{n}{q}-1} \mathfrak{m}_{\Delta S}(x + kq), \ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Ce qui complète la preuve. □

4.3 Triangles de Steinhaus de suites arithmétiques

Dans cette section, on décrit la structure du triangle de Steinhaus associé à une suite arithmétique de $\mathbb{Z}/n\mathbb{Z}$.

Notation. Soient a et d des éléments de $\mathbb{Z}/n\mathbb{Z}$ et $m \geqslant 1$ un entier. On note

$$PA(a,d,m) = (a, a+d, a+2d, \ldots, a+(m-1)d)$$

la suite arithmétique de longueur $m \geqslant 1$ commençant par a et de raison d.

On commence par analyser les suites dérivées successives d'une suite à progression arithmétique dans $\mathbb{Z}/n\mathbb{Z}$. Tout d'abord, sa suite dérivée est aussi une suite arithmétique de $\mathbb{Z}/n\mathbb{Z}$. Plus précisément, on a

Proposition 4.3.1. *Soit $n \geqslant 1$ un entier et soient a et d dans $\mathbb{Z}/n\mathbb{Z}$. Alors, la $i$ème suite dérivée de la suite arithmétique $PA(a,d,m)$ est la suite à progression arithmétique*

$$\partial^i PA(a,d,m) = PA\left(2^i a + 2^{i-1} id, 2^i d, m-i\right),$$

pour tout i, $0 \leqslant i \leqslant m-1$.

Preuve. Posons $S = PA(a,d,m) = (a_1, a_2, \ldots, a_m)$ et $\partial^i S = (b_1, b_2, \ldots, b_{m-i})$. Alors, on a

$$\begin{aligned} b_j &= \sum_{k=0}^{i} \binom{i}{k} a_{j+k} = \sum_{k=0}^{i} \binom{i}{k} (a + (j+k-1)d) = \sum_{k=0}^{i} \binom{i}{k} (a + (j-1)d) + \sum_{k=0}^{i} \binom{i}{k} kd \\ &= 2^i (a + (j-1)d) + 2^{i-1} id = (2^i a + 2^{i-1} id) + (j-1)2^i d, \end{aligned}$$

pour tout j, $1 \leqslant j \leqslant m-i$. □

Notation. Soit S une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. On note $\Delta S(i,j)$ le $j$ème élément de la $i$ème ligne du triangle de Steinhaus ΔS, i.e. le $j$ème élément de la $(i-1)$ème suite dérivée $\partial^{i-1} S$ de S, pour tout i, $1 \leqslant i \leqslant m$, et tout j, $1 \leqslant j \leqslant m-i+1$. Par exemple, avec cette notation, le $j$ème élément de la suite S correspond à $\Delta S(1,j)$.

On décrit maintenant les coefficients du triangle de Steinhaus engendré par une suite arithmétique dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 4.3.2. *Soit $n \geqslant 1$ un entier. Soient a et d dans $\mathbb{Z}/n\mathbb{Z}$ et $S = PA(a,d,m)$ une suite arithmétique dans $\mathbb{Z}/n\mathbb{Z}$. Alors, on a*

$$\begin{cases} \Delta S(1,j) = a + (j-1)d & , \ \forall 1 \leqslant j \leqslant m, \\ \Delta S(i,j) = 2^{i-1} a + 2^{i-2}(2j+i-3)d & , \ \forall 2 \leqslant i \leqslant m, \ \forall 1 \leqslant j \leqslant m-i+1. \end{cases}$$

Preuve. Il s'agit simplement d'une reformulation de la Proposition 4.3.1 en utilisant la notation $\Delta S(i,j)$ introduite auparavant. □

On a vu à la Proposition 4.1.4 que toute suite finie de $\mathbb{Z}/n\mathbb{Z}$ admet exactement n suites primitives. Cependant, pour n impair, si S est une suite arithmétique de $\mathbb{Z}/n\mathbb{Z}$, alors il n'y a qu'une seule primitive de S qui soit aussi une suite à progression arithmétique dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 4.3.3. *Soit n un nombre impair et soient a et d dans $\mathbb{Z}/n\mathbb{Z}$. Alors, la suite $PA(2^{-1}a-2^{-2}d, 2^{-1}d, m+1)$ est l'unique suite primitive de la suite arithmétique $PA(a,d,m)$ qui soit également une suite à progression arithmétique dans $\mathbb{Z}/n\mathbb{Z}$.*

Preuve. On sait, par la Proposition 4.3.1, que la suite dérivée de la suite $PA(2^{-1}a - 2^{-2}d, 2^{-1}d, m+1)$ est la suite arithmétique $PA(a,d,m)$, c'est-à-dire,

$$\partial PA(2^{-1}a - 2^{-2}d, 2^{-1}d, m+1) = PA(a,d,m).$$

Supposons maintenant que les suites à progression arithmétique $PA(a_1,d_1,m+1)$ et $PA(a_2,d_2,m+1)$ aient la même suite dérivée, c'est-à-dire,

$$\partial PA(a_1,d_1,m+1) = \partial PA(a_2,d_2,m+1).$$

Alors, par la Proposition 4.3.1, on a

$$PA(2a_1+d_1, 2d_1, m) = PA(2a_2+d_2, 2d_2, m).$$

Il s'ensuit que $2a_1 + d_1 = 2a_2 + d_2$ et $2d_1 = 2d_2$. Comme 2 est inversible dans $\mathbb{Z}/n\mathbb{Z}$, cela conduit aux égalités $a_1 = a_2$ et $d_1 = d_2$ et donc l'unicité du résultat est prouvé. □

A contrario, pour n pair, il n'y a pas d'unicité. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, les suites arithmétiques (37373) et (11111) sont distinctes mais ont la même suite dérivée (2222).

4.4 Suites arithmétiques balancées dans les groupes cycliques d'ordre impair

Dans toute cette section, l'entier n est supposé être impair. On commence par montrer que la raison d'une suite arithmétique balancée de $\mathbb{Z}/n\mathbb{Z}$ doit être inversible.

Théorème 4.4.1. *Soit n un nombre impair et soient a et d dans $\mathbb{Z}/n\mathbb{Z}$. Si d est non-inversible, alors, pour tout entier $m \geqslant 1$, la suite à progression arithmétique $PA(a,d,m)$ n'est pas balancée.*

Preuve. Supposons, par l'absurde, qu'il existe une suite arithmétique balancée

$$S = PA(a, d, m)$$

dont la raison d est non-inversible dans $\mathbb{Z}/n\mathbb{Z}$. On pose

$$q = n \wedge d_0 \neq 1$$

où d_0 est un entier dont d est la classe de résidu modulo n. On considère le morphisme canonique surjectif $\pi_q : \mathbb{Z}/n\mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/q\mathbb{Z}$ et la suite arithmétique

$$\pi_q(S) = PA(\pi_q(a), \pi_q(d), m) = PA(\pi_q(a), 0, m),$$

qui est une suite constante dans $\mathbb{Z}/q\mathbb{Z}$. Le Théorème 4.2.3 implique alors que la suite $\pi_q(S)$ est balancée. Par conséquent, il existe au moins un élément égal à 0 dans le triangle $\Delta\pi_q(S)$, disons $\Delta\pi_q(S)(i, j) = 0$. On obtient alors $2^{i-1}\pi_q(a) = 0$ par la Proposition 4.3.2. Comme 2 est inversible dans $\mathbb{Z}/q\mathbb{Z}$, il s'ensuit que $\pi_q(a) = 0$ et donc $\pi_q(X)$ est la suite nulle de longueur m dans $\mathbb{Z}/q\mathbb{Z}$, en contradiction avec le fait que $\pi_q(S)$ soit balancée. □

Dans la suite de cette section, on étudie les suites arithmétiques dont la raison est inversible.

Notations. Soit n un nombre impair. On note $\alpha(n)$ l'*ordre multiplicatif* de 2^n modulo n, i.e. le plus petit exposant $e \geqslant 1$ tel que $2^{en} \equiv 1 \pmod{n}$, à savoir,

$$\alpha(n) = \min\left\{e \in \mathbb{N}^* \mid 2^{en} \equiv 1 \pmod{n}\right\}.$$

On remarque alors que, pour tout n impair, l'entier $\alpha(n)$ divise $\varphi(n)$.

A l'inverse du Théorème 4.4.1, le résultat suivant établit que, pour tout a et d dans $\mathbb{Z}/n\mathbb{Z}$ avec d inversible, il existe une infinité de longueur $m \geqslant 1$ pour lesquelles la suite arithmétique $PA(a, d, m)$ est balancée.

Théorème 4.4.2. *Soit n un nombre impair. Soient a et d dans $\mathbb{Z}/n\mathbb{Z}$ avec d inversible. Alors, la suite arithmtique $PA(a, d, m)$ est balancée pour tout entier positif $m \equiv 0$ ou $-1 \pmod{\alpha(n)n}$.*

Ce théorème est prouvé à la fin de cette section.

L'entier $\alpha(n)$ semble être difficile à déterminer. En effet, il n'existe pas de formule générale afin de calculer l'ordre multiplicatif d'un entier modulo n. Cependant, on obtient les propositions suivantes qui sont d'une grande utilité dans la suite.

Notation. Soit $n \geqslant 1$ un entier. On note $\mathrm{rad}(n)$ *le radical de* n, le produit des facteurs premiers distincts de n, c'est-à-dire,

$$\mathrm{rad}(n) = \prod_{\substack{p \in \mathcal{P} \\ p|n}} p.$$

Le radical de n est aussi le plus grand diviseur sans carré de n.

Proposition 4.4.3. *Soit n un nombre impair. Alors $\alpha(n)$ divise $\alpha(\mathrm{rad}(n))$.*

Preuve. Soit p un facteur premier de n tel que p^2 divise n. On montre que $\alpha(n)$ divise $\alpha(\frac{n}{p})$. Tout d'abord, il existe un entier positif u tel que

$$2^{\alpha(\frac{n}{p})\frac{n}{p}} = 1 + u\frac{n}{p}.$$

Le théorème du binôme implique alors que

$$2^{\alpha(\frac{n}{p})n} = \left(2^{\alpha(\frac{n}{p})\frac{n}{p}}\right)^p = \left(1 + u\frac{n}{p}\right)^p = 1 + \sum_{k=1}^{p-1}\binom{p}{k}u^k\left(\frac{n}{p}\right)^k + u^p\left(\frac{n}{p}\right)^p \equiv 1 \pmod{n},$$

et donc $\alpha(n)$ divise $\alpha(\frac{n}{p})$. On conclut par induction que $\alpha(n)$ divise $\alpha(\mathrm{rad}(n))$. □

Proposition 4.4.4. *Soit p un nombre premier impair. Alors,*

$$\alpha(p^k) = \alpha(p),$$

pour tout entier $k \geqslant 1$.

Preuve. L'entier $\alpha(p^k)$ divise $\alpha(p)$ par la Proposition 4.4.3. Il reste à prouver que $\alpha(p)$ divise $\alpha(p^k)$. La congruence

$$2^{\alpha(p^k)p^k} \equiv 1 \pmod{p^k}$$

implique que

$$2^{\alpha(p^k)p^k} \equiv 1 \pmod{p},$$

et donc, par le petit théorème de Fermat, il suit que

$$2^{\alpha(p^k)p} \equiv 2^{\alpha(p^k)p^k} \equiv 1 \pmod{p}.$$

Par conséquent, l'entier $\alpha(p)$ divise $\alpha(p^k)$. Ce qui complète la preuve. □

Proposition 4.4.5. *Soient n_1 et n_2 deux nombres impairs et premiers entre eux. Alors, l'entier $\alpha(n_1n_2)$ divise $\alpha(n_1) \vee \alpha(n_2)$.*

Preuve. Soit $i \in \{1, 2\}$. Les congruences

$$2^{\alpha(n_i)n_i} \equiv 1 \pmod{n_i}$$

impliquent que

$$2^{(\alpha(n_1)\vee\alpha(n_2))n_1n_2} \equiv 1 \pmod{n_i}.$$

On conclut par le théorème des restes chinois. □

n	rad(n)	$\alpha(n)$
1	1	1
3	3	2
5	5	4
7	7	3
9	3	2
11	11	10
13	13	12
15	$5 \cdot 3$	4
17	17	8
19	19	18
21	$7 \cdot 3$	2
23	23	11
25	5	4

n	rad(n)	$\alpha(n)$
27	3	2
29	29	28
31	31	5
33	$11 \cdot 3$	10
35	$7 \cdot 5$	12
37	37	36
39	$13 \cdot 3$	4
41	41	20
43	43	14
45	$5 \cdot 3$	4
47	47	23
49	7	3
51	$17 \cdot 3$	8

n	rad(n)	$\alpha(n)$
53	53	52
55	$11 \cdot 5$	4
57	$19 \cdot 3$	6
59	59	58
61	61	60
63	$7 \cdot 3$	2
65	$13 \cdot 5$	12
67	67	66
69	$23 \cdot 3$	22
71	71	35
73	73	9
75	$5 \cdot 3$	4
77	$11 \cdot 7$	30

n	rad(n)	$\alpha(n)$
79	79	39
81	3	2
83	83	82
85	$17 \cdot 5$	8
87	$29 \cdot 3$	28
89	89	11
91	$13 \cdot 7$	12
93	$31 \cdot 3$	10
95	$19 \cdot 5$	36
97	97	48
99	$11 \cdot 3$	10
101	101	100
103	103	51

FIG. 4.4 – Les premières valeurs de $\alpha(n)$ pour n impair

Par exemple, pour $n_1 = 5$ et $n_2 = 3$, on a l'égalité $\alpha(15) = 4 = 4 \vee 2 = \alpha(5) \vee \alpha(3)$. Cependant, $\alpha(n_1 n_2)$ peut être un facteur strict de $\alpha(n_1) \vee \alpha(n_2)$, par exemple pour $n = 21$: $\alpha(21) = 2$ et $\alpha(7) \vee \alpha(3) = 3 \vee 2 = 6$. Le tableau représenté Figure 4.4 montre les premières valeurs de $\alpha(n)$ pour n impair.

On termine cette section par la preuve du Théorème 4.4.2, qui est basée sur les deux lemmes suivants.

Lemme 4.4.6. *Soit $n \geqslant 1$ un entier. Soit $PA(a, d, m) = (a_1, a_2, \ldots, a_m)$ une suite arithmétique commençant par $a \in \mathbb{Z}/n\mathbb{Z}$ et de raison inversible $d \in \mathbb{Z}/n\mathbb{Z}$. Alors, n éléments consécutifs de $PA(a, d, m)$ sont distincts. En d'autres termes, pour tout i, $1 \leqslant i \leqslant m - n + 1$, on a*

$$\{a_i, a_{i+1}, \ldots, a_{i+n-1}\} = \mathbb{Z}/n\mathbb{Z}.$$

Preuve. Comme la raison d est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il s'ensuit que, pour tous entiers positifs i_1 et i_2, on a

$$a_{i_1} = a_{i_2} \iff a+(i_1-1)d = a+(i_2-1)d \iff (i_1-1)d = (i_2-1)d \iff i_1 \equiv i_2 \pmod{n}.$$

Ce qui complète la preuve. □

Lemme 4.4.7. *Soit n un nombre impair et $k \geqslant 1$ un entier. Soient a et d dans $\mathbb{Z}/n\mathbb{Z}$ avec d inversible. Alors, la suite arithmétique $PA(a, d, k\alpha(n)n)$ est balancée si, et seulement si, sa sous-suite initiale $PA(a, d, \alpha(n)n)$ est aussi balancée.*

Preuve. On montre qu'il existe une relation entre la fonction de multiplicité du triangle de Steinhaus $\Delta PA(a, d, k\alpha(n)n)$ et celle de $\Delta PA(a, d, \alpha(n)n)$. On pose

$$S = PA(a, d, k\alpha(n)n).$$

On considère maintenant la structure du triangle de Steinhaus ΔS représentée à la Figure 4.5. Rappelons que $\Delta S(i,j)$ désigne le $j$ème élément de la $i$ème ligne de ΔS, pour tout entier i, $1 \leqslant i \leqslant k\alpha(n)n$, et tout entier j, $1 \leqslant j \leqslant k\alpha(n)n - i + 1$.

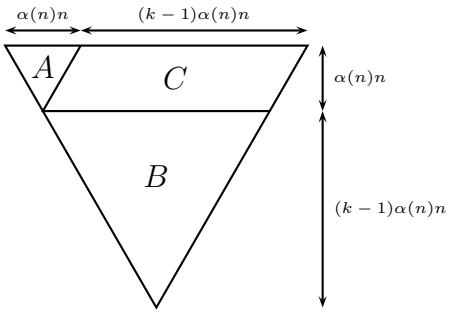


FIG. 4.5 – Structure de ΔS

Le sous-triangle A est défini par

$$A = \{\Delta S(i,j) \mid 1 \leqslant i \leqslant \alpha(n)n \ , \ 1 \leqslant j \leqslant \alpha(n)n - i + 1\}.$$

Alors A est le triangle de Steinhaus engendré par la sous-suite initiale $PA(a,d,\alpha(n)n)$ de la suite S, c'est-à-dire,

$$A = \Delta PA(a,d,\alpha(n)n).$$

Le sous-triangle B est défini par

$$B = \{\Delta S(i,j) \mid \alpha(n)n + 1 \leqslant i \leqslant k\alpha(n)n \ , \ 1 \leqslant j \leqslant k\alpha(n)n - i + 1\}.$$

Alors B est le triangle de Steinhaus engendré par la suite dérivée $\partial^{\alpha(n)n}S$, c'est-à-dire,

$$B = \Delta\partial^{\alpha(n)n}S.$$

En appliquant la Proposition 4.3.1, on obtient que

$$\partial^{\alpha(n)n}PA\left(a,d,k\alpha(n)n\right) = PA\left(2^{\alpha(n)n}a + 2^{\alpha(n)n-1}\alpha(n)nd, 2^{\alpha(n)n}d, (k-1)\alpha(n)n\right).$$

Comme $2^{\alpha(n)n} = 1$, il suit immédiatement que

$$B = \Delta PA(a,d,(k-1)\alpha(n)n).$$

Enfin, le multiensemble C est défini par

$$C = \{\Delta S(i,j) \mid 1 \leqslant i \leqslant \alpha(n)n \ , \ \alpha(n)n - i + 2 \leqslant j \leqslant k\alpha(n)n - i + 1\}.$$

Alors chaque ligne de C est composée de $(k-1)\alpha(n)n$ termes consécutifs d'une suite dérivée de S. Comme, pour tout i, $0 \leqslant i \leqslant k\alpha(n)n - 1$, la suite dérivée $\partial^i S$ de S est une suite arithmétique de raison inversible $2^i d$ par la Proposition 4.3.1, cela entraîne, par le Lemme 4.4.6, que chaque élément de $\mathbb{Z}/n\mathbb{Z}$ apparaît $(k-1)\alpha(n)$ fois dans chaque ligne de C. Par conséquent, la fonction de multiplicité de C est la fonction constante définie par

$$\mathfrak{m}_C(x) = (k-1)\alpha(n)^2 n, \ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

En combinant ces résultats sur les multiensembles A, B et C, on a

$$\begin{aligned}\mathfrak{m}_{\Delta PA(a,d,k\alpha(n)n)}(x) &= \mathfrak{m}_A(x) + \mathfrak{m}_B(x) + \mathfrak{m}_C(x) \\ &= \mathfrak{m}_{\Delta PA(a,d,\alpha(n)n)}(x) + \mathfrak{m}_{\Delta PA(a,d,(k-1)\alpha_n n)}(x) + (k-1)\alpha(n)^2 n,\end{aligned}$$

pour tout x dans $\mathbb{Z}/n\mathbb{Z}$. Alors, par induction sur k, on obtient

$$\mathfrak{m}_{\Delta PA(a,d,k\alpha(n)n)}(x) = k \cdot \mathfrak{m}_{\Delta PA(a,d,\alpha(n)n)}(x) + \binom{k}{2}\alpha(n)^2 n, \ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Ce qui complète la preuve. □

On est maintenant prêt à prouver le théorème principal de cette section.

Preuve du Théorème 4.4.2.

1er Cas : $\mathbf{m \equiv -1}$ (mod $\alpha(\mathbf{n})\mathbf{n}$).
Tout d'abord, on montre que l'on peut déduire le cas $m \equiv -1 \pmod{\alpha(n)n}$ du cas $m \equiv 0 \pmod{\alpha(n)n}$. Soit $k \geqslant 1$ un entier et

$$S = PA\left(a, d, k\alpha(n)n - 1\right).$$

Par la Proposition 4.3.3, la suite arithmétique

$$T = PA\left(2^{-1}a - 2^{-2}d, 2^{-1}d, k\alpha(n)n\right)$$

est une suite primitive de S. Comme T est une suite arithmétique de raison inversible $2^{-1}d$ et de longueur $k\alpha(n)n$, il suit du Lemme 4.4.6 que chaque élément du groupe $\mathbb{Z}/n\mathbb{Z}$ apparaît $k\alpha(n)$ fois dans la suite T. Comme S est la suite dérivée de T, on a

$$\mathfrak{m}_{\Delta S}(x) = \mathfrak{m}_{\Delta\partial T}(x) = \mathfrak{m}_{\Delta T}(x) - \mathfrak{m}_T(x) = \mathfrak{m}_{\Delta T}(x) - k\alpha(n),$$

pour tout x dans $\mathbb{Z}/n\mathbb{Z}$. Par conséquent, la suite S est balancée si, et seulement si, la suite T est aussi balancée. Ceci prouve bien que l'on déduit le cas $m \equiv -1 \pmod{\alpha(n)n}$ du cas $m \equiv 0 \pmod{\alpha(n)n}$.

2ème Cas : $\mathbf{m \equiv 0}$ (mod $\alpha(\mathbf{n})\mathbf{n}$).
On prouve ce cas par induction sur n. Pour $n = 1$, il est clair que toute suite finie de $\mathbb{Z}/n\mathbb{Z} = \{0\}$ est balancée et donc l'assertion du théorème est vraie pour $n = 1$. Soit maintenant $n > 1$ et soit p son plus grand facteur premier. Supposons que l'énoncé soit vrai pour $q = \frac{n}{p}$, i.e. toute suite arithmétique de raison inversible et de longueur $m \equiv 0 \pmod{\alpha(q)q}$ dans $\mathbb{Z}/q\mathbb{Z}$ est balancée. Soient a et d dans $\mathbb{Z}/n\mathbb{Z}$ avec d inversible. On montre que la suite $PA(a, d, m)$ est balancée pour tout entier positif $m \equiv 0 \pmod{\alpha(n)n}$. On sait, par le Lemme 4.4.7, qu'il est suffisant de montrer que la suite $PA(a, d, m)$ est balancée pour une seule longueur m multiple de $\alpha(n)n$.

On pose

$$\lambda = \varphi\left(\frac{\mathrm{rad}(n)}{p}\right).$$

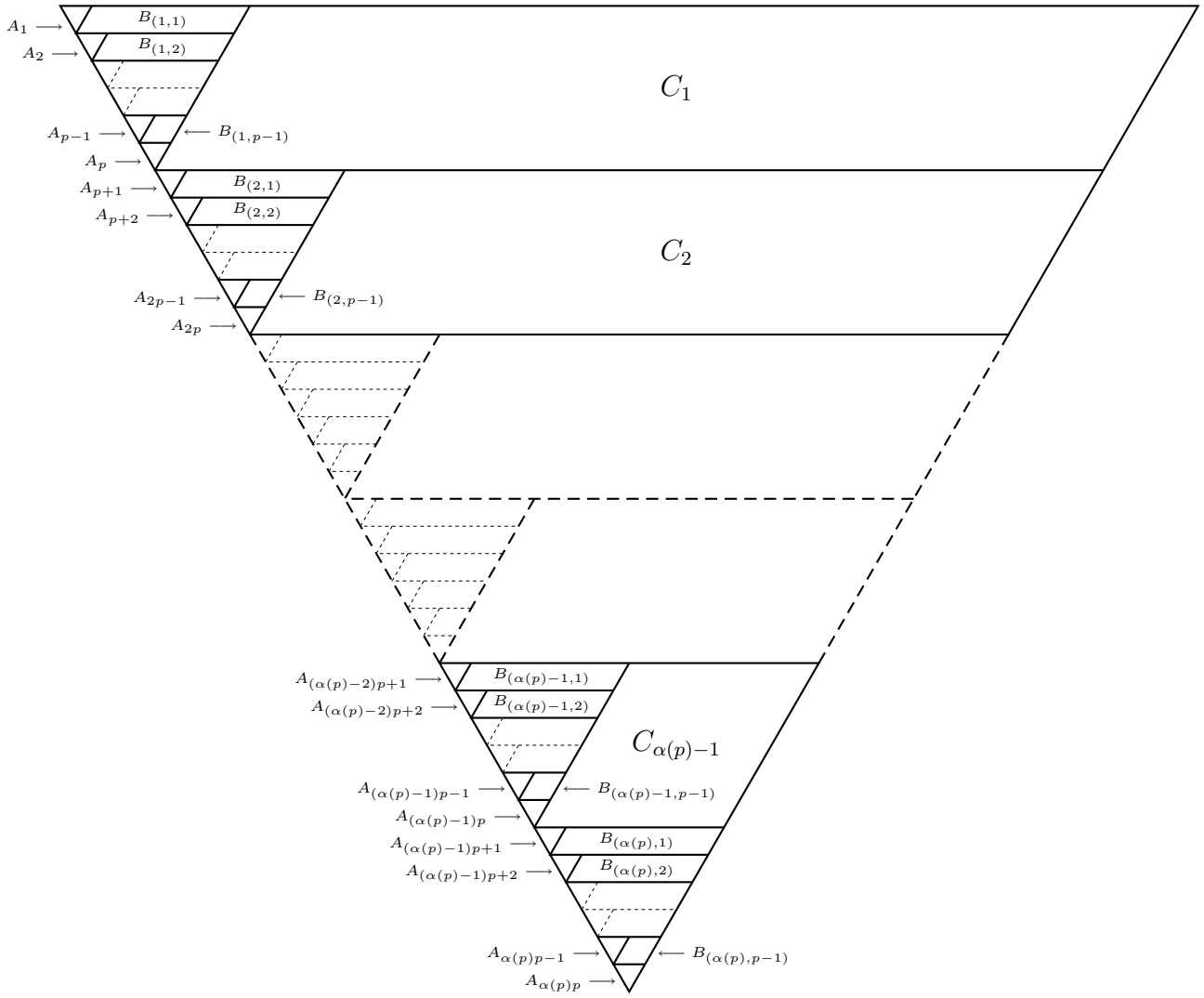


FIG. 4.6 – Structure de ΔS

Alors l'entier $\lambda\alpha(p)$ est un multiple de $\alpha(n)$. En effet, l'entier $\alpha(n)$ divise $\alpha(\mathrm{rad}(n))$ par la Proposition 4.4.3, lequel divise $\alpha\left(\frac{\mathrm{rad}(n)}{p}\right)\alpha(p)$ par la Proposition 4.4.5, qui enfin divise l'entier $\varphi\left(\frac{\mathrm{rad}(n)}{p}\right)\alpha(p)$ par définition de la fonction α.

On prouve que la suite $S = PA(a, d, \lambda\alpha(p)n)$ est balancée. On commence par montrer que la fonction de multiplicité de ΔS est constante sur chaque coset du sous-groupe $q\mathbb{Z}/n\mathbb{Z}$. Pour ce faire, on considère la structure du triangle de Steinhaus ΔS représenté à la Figure 4.6 où ΔS est constitué par les multiensembles A_r, $B_{(s,t)}$ et C_u. On établit successivement que (**1**) la fonction de multiplicité $\mathfrak{m}_{C_u}$ est constante pour chaque C_u, (**2**) la fonction de multiplicité de la réunion des $B_{(s,t)}$ est constante, et (**3**) la fonction de multiplicité de la réunion des A_r est constante sur chaque coset du sous-groupe $q\mathbb{Z}/n\mathbb{Z}$.

Etape (1) : La fonction de multiplicité $\mathfrak{m}_{C_u}$ est constante pour tout u, $1 \leqslant u \leqslant \alpha(p) - 1$.

Pour tout entier u, $1 \leqslant u \leqslant \alpha(p) - 1$, le multiensemble C_u est défini par

$$C_u = \{\Delta S(i, j) \mid (u-1)\lambda n + 1 \leqslant i \leqslant u\lambda n \ , \ u\lambda n - i + 2 \leqslant j \leqslant \lambda\alpha(p)n - i + 1\},$$

où $\Delta S(i, j)$ correspond au $j$ème élément de la $i$ème ligne de ΔS, pour tout entier i, $1 \leqslant i \leqslant \lambda\alpha(p)n$, et tout entier j, $1 \leqslant j \leqslant \lambda\alpha(p)n - i + 1$. Comme représenté à la Figure 4.7, chaque multiensemble C_u est un parallélogramme avec λn lignes et $(\alpha(p) - u)\lambda n$ colonnes.

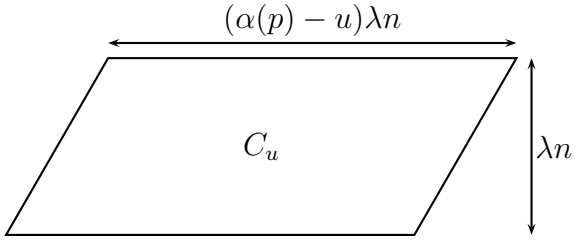


FIG. 4.7 – Structure de C_u

Soit u un entier tel que $1 \leqslant u \leqslant \alpha(p)-1$. Chaque ligne de C_u est composée de $(\alpha(p)-u)\lambda n$ termes consécutifs d'une suite dérivée de S. Pour tout i, $0 \leqslant i \leqslant \lambda\alpha(p)n - 1$, la suite dérivée $\partial^i S$ de S est une suite à progression arithmétique de raison inversible $2^i d$ par la Proposition 4.3.1. Il suit du Lemme 4.4.6 que chaque élément du groupe $\mathbb{Z}/n\mathbb{Z}$ apparaît $(\alpha(p) - u)\lambda$ fois dans chaque ligne de C_u. Par conséquent, la fonction de multiplicité de C_u est la fonction constante définie par

$$\mathfrak{m}_{C_u}(x) = (\alpha(p) - u)\lambda^2 n, \ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Etape (2) : La fonction de multiplicité de la réunion de tous les multiensembles $B_{(s,t)}$ est constante.

Pour tout entier s, $1 \leqslant s \leqslant \alpha(p)$, et tout entier t, $1 \leqslant t \leqslant p - 1$, le multiensemble $B_{(s,t)}$ est défini par

$$B_{(s,t)} = \left\{ \Delta SX(i, j) \;\middle|\; \begin{array}{l} ((s-1)p + t - 1)\lambda\frac{n}{p} + 1 \leqslant i \leqslant ((s-1)p + t)\lambda\frac{n}{p} \\ ((s-1)p + t)\lambda\frac{n}{p} - i + 2 \leqslant j \leqslant s\lambda n - i + 1 \end{array} \right\}.$$

Comme représenté à la Figure 4.8, chaque multiensemble $B_{(s,t)}$ est un parallélogramme avec $\lambda\frac{n}{p}$ lignes et $(p-t)\lambda\frac{n}{p}$ colonnes.

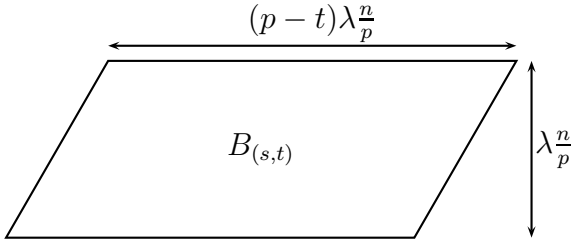


FIG. 4.8 – Structure de $B_{(s,t)}$

On construit une involution sans point fixe Ψ sur l'ensemble des paires (s,t) telle que la fonction de multiplicité de la réunion multiensembliste $B_{(s,t)} \cup B_{\Psi(s,t)}$ soit constante pour chaque paire d'éléments (s,t). Soit

$$\Psi : \left\{ \begin{array}{ccc} [\![1,\alpha(p)]\!] \times [\![1,p-1]\!] & \longrightarrow & [\![1,\alpha(p)]\!] \times [\![1,p-1]\!] \\ (s,t) & \longmapsto & (\psi(s,t),p-t) \end{array} \right. ,$$

où $\psi : [\![1,\alpha(p)]\!] \times [\![1,p-1]\!] \longrightarrow [\![1,\alpha(p)]\!]$ est la fonction qui à chaque paire (s,t) associe l'entier positif $\psi(s,t)$ de $[\![1,\alpha(p)]\!]$ qui est équivalent à $s+2t-1$ modulo $\alpha(p)$, c'est-à-dire,

$$\psi(s,t) \equiv s+2t-1 \pmod{\alpha(p)},\ \forall 1 \leqslant s \leqslant \alpha(p),\ \forall 1 \leqslant t \leqslant p-1.$$

Comme $\alpha(p)$ divise $\varphi(p) = p-1$, il s'ensuit que

$$\psi(\psi(s,t),p-t) \equiv \psi(s,t) + 2p - 2t - 1 \equiv s + 2(p-1) \equiv s \pmod{\alpha(p)}$$

et donc, on obtient

$$\Psi\left(\Psi(s,t)\right) = \Psi(\psi(s,t),p-t) = (\psi(\psi(s,t),p-t),t) = (s,t),$$

pour toute paire (s,t) dans $[\![1,\alpha(p)]\!] \times [\![1,p-1]\!]$. De plus, cette involution est sans point fixe. En effet, si (s,t) est un point fixe de Ψ, alors

$$(s,t) = \Psi(s,t) = (\psi(s,t),p-t),$$

ce qui implique que $p = 2t$, en contradiction avec la parité de p. On a donc bien prouvé que Ψ est une involution sans point fixe sur l'ensemble $[\![1,\alpha(p)]\!] \times [\![1,p-1]\!]$.

Soient s et t des entiers tels que $1 \leqslant s \leqslant \alpha(p)$ et $1 \leqslant t \leqslant p-1$. Si l'on note $B^{(v)}_{(s,t)}$ la $v$ème ligne de $B_{(s,t)}$, c'est-à-dire,

$$B^{(v)}_{(s,t)} = \left\{ \Delta S\left(((s-1)p+t-1)\lambda\frac{n}{p} + v, j \right) \;\middle|\; \lambda\frac{n}{p} - v + 2 \leqslant j \leqslant (p-t+1)\lambda\frac{n}{p} - v + 1 \right\},$$

pour tout v, $1 \leqslant v \leqslant \lambda\frac{n}{p}$, alors

$$B_{(s,t)} = \bigcup_{v=1}^{\lambda\frac{n}{p}} B^{(v)}_{(s,t)}.$$

Soit v un entier tel que $1 \leqslant v \leqslant \lambda\frac{n}{p}$. La suite $B^{(v)}_{(s,t)}$ est composée de $(p-t)\lambda\frac{n}{p}$ termes consécutifs de la suite dérivée

$$\partial^{((s-1)p+t-1)\lambda\frac{n}{p}+v-1}S,$$

qui est une suite arithmétique de raison

$$2^{((s-1)p+t-1)\lambda\frac{n}{p}+v-1}d$$

par la Proposition 4.3.1. On en déduit que

$$B^{(v)}_{(s,t)} = PA\left(b^{(v)}_{(s,t)}\ ,\ 2^{((s-1)p+t-1)\lambda\frac{n}{p}+v-1}d\ ,\ (p-t)\lambda\frac{n}{p}\right),$$

avec

$$b^{(v)}_{(s,t)} = \Delta S\left(((s-1)p+t-1)\lambda\frac{n}{p}+v, \lambda\frac{n}{p}-v+2\right).$$

On montre que la suite $B^{(v)}_{(s,t)} \circ B^{(v)}_{\Psi(s,t)}$, *la concaténation des suites* $B^{(v)}_{(s,t)}$ *et* $B^{(v)}_{\Psi(s,t)}$, est une suite à progression arithmétique de raison inversible et de longueur λn. La congruence $p \equiv 1 \pmod{\alpha(p)}$ implique que

$$(s-1)p+t-1 \equiv s+t-2 \pmod{\alpha(p)},$$

et

$$(\psi(s,t)-1)p+(p-t)-1 \equiv \psi(s,t)-1-t \equiv s+t-2 \pmod{\alpha(p)}.$$

Comme $\alpha(n)$ divise $\lambda\alpha(p)$, il suit que

$$2^{((\psi(s,t)-1)p+(p-t)-1)\lambda} \equiv 2^{((s-1)p+t-1)\lambda} \equiv 2^{(s+t-2)\lambda} \pmod{n},$$

et donc,

$$2^{((\psi(s,t)-1)p+(p-t)-1)\lambda\frac{n}{p}+v-1}d = 2^{((s-1)p+t-1)\lambda\frac{n}{p}+v-1}d = 2^{(s+t-2)\lambda\frac{n}{p}+v-1}d.$$

Par conséquent, les suites $B^{(v)}_{(s,t)}$ et $B^{(v)}_{\Psi(s,t)}$ sont toutes les deux des suites arithmétiques de raison

$$2^{(s+t-2)\lambda\frac{n}{p}+v-1}d.$$

Il reste à prouver que $b^{(v)}_{\Psi(s,t)}$ peut être exprimé comme l'élément suivant de la suite arithmétique $B^{(v)}_{(s,t)}$. Comme

$$\begin{aligned}
b^{(v)}_{\Psi(s,t)} &= \Delta S\left(((\Psi(s,t)-1)p+(p-t)-1)\lambda\tfrac{n}{p}+v, \lambda\tfrac{n}{p}-v+2\right)\\
&= 2^{((\psi(s,t)-1)p+(p-t)-1)\lambda\frac{n}{p}+v-2}\left(2a+\left(2\left(\lambda\tfrac{n}{p}-v+2\right)+\right.\right.\\
&\quad \left.\left.+\left(((\psi(s,t)-1)p+(p-t)-1)\lambda\tfrac{n}{p}+v\right)-3\right)d\right)\\
&= 2^{(s+t-2)\lambda\frac{n}{p}+v-2}\left(2a+\left(((p-t)+1)\lambda\tfrac{n}{p}-v+1\right)d\right)\\
&= 2^{(s+t-2)\lambda\frac{n}{p}+v-2}\left(2a+\left((t+1)\lambda\tfrac{n}{p}-v+1\right)d\right)+(p-2t)\lambda\tfrac{n}{p}\left(2^{(s+t-2)\lambda\frac{n}{p}+v-2}d\right)\\
&= b^{(v)}_{(s,t)}+(p-t)\lambda\tfrac{n}{p}\left(2^{(s+t-2)\lambda\frac{n}{p}+v-2}d\right),
\end{aligned}$$

il suit que

$$B^{(v)}_{(s,t)} \circ B^{(v)}_{\Psi(s,t)} = PA\left(b^{(v)}_{(s,t)}\ ,\ 2^{(s+t-2)\lambda\frac{n}{p}+v-1}d\ ,\ \lambda n\right),$$

et ainsi, chaque élément du groupe $\mathbb{Z}/n\mathbb{Z}$ apparaît λ fois dans $B^{(v)}_{(s,t)} \circ B^{(v)}_{\Psi(s,t)}$ pour tout v, $1 \leqslant v \leqslant \lambda\frac{n}{p}$. Alors, la fonction de multiplicité de la réunion $B_{(s,t)} \cup B_{\Psi(s,t)}$ est la fonction constante définie par

$$\mathfrak{m}_{B_{(s,t)}\cup B_{\Psi(s,t)}}(x) = \lambda^2\frac{n}{p},\ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Si l'on note B la réunion de tous les multiensembles $B_{(s,t)}$, alors

$$\mathfrak{m}_B(x) = \sum_{s=1}^{\alpha(p)}\sum_{t=1}^{p-1}\mathfrak{m}_{B_{(s,t)}}(x) = \frac{1}{2}\sum_{s=1}^{\alpha(p)}\sum_{t=1}^{p-1}\mathfrak{m}_{B_{(s,t)}\cup B_{\Psi(s,t)}}(x) = \frac{1}{2}\sum_{s=1}^{\alpha(p)}\sum_{t=1}^{p-1}\lambda^2\frac{n}{p} = \alpha(p)\lambda^2\frac{(p-1)n}{2p},$$

pour tout x dans $\mathbb{Z}/n\mathbb{Z}$, puisque Ψ est une involution sans point fixe sur $[\![1,\alpha(p)]\!]\times[\![1,p-1]\!]$.

Etape (3) : La fonction de multiplicité de la réunion de tous les multiensembles A_r est constante sur chaque coset du sous-groupe $\frac{n}{p}\mathbb{Z}/n\mathbb{Z}$.

Pour tout entier r, $1 \leqslant r \leqslant \alpha(p)p$, le multiensemble A_r est défini par

$$A_r = \left\{\Delta S(i,j)\ \middle|\ (r-1)\lambda\frac{n}{p}+1 \leqslant i \leqslant r\lambda\frac{n}{p}\ ,\ 1 \leqslant j \leqslant r\lambda\frac{n}{p}-i+1\right\}.$$

Comme représenté à la Figure 4.9, chaque multiensemble A_r est un triangle associé à une suite de longueur $\lambda\frac{n}{p}$.

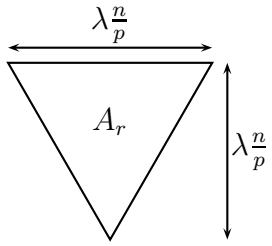


FIG. 4.9 – Structure de A_r

Si l'on note S_r la suite des $\lambda\frac{n}{p}$ premiers termes de la suite dérivée $\partial^{(r-1)\lambda\frac{n}{p}}S$, alors A_r est le triangle de Steinhaus engendré par S_r, pour tout r, $1 \leqslant r \leqslant \alpha(p)p$. Il est clair qu'il existe une correspondance entre A_r et le triangle de Steinhaus entier ΔS. En effet, pour tout entier i, $1 \leqslant i \leqslant \lambda\frac{n}{p}$, et tout entier j, $1 \leqslant j \leqslant \lambda\frac{n}{p}-i+1$, on a

$$\Delta S_r(i,j) = \Delta S\left((r-1)\lambda\frac{n}{p}+i, j\right).$$

Soient l, i et j des entiers tels que $1 \leqslant l \leqslant \alpha(p)$, $1 \leqslant i \leqslant \lambda\frac{n}{p}$ et $1 \leqslant j \leqslant \lambda\frac{n}{p}-i+1$. On prouve alors que chaque élément du coset

$$\Delta S_l(i,j) + \frac{n}{p}\mathbb{Z}/n\mathbb{Z}$$

apparaît exactement une fois dans le multiensemble

$$\left\{\Delta S_{l+k\alpha(p)}(i,j) \;\middle|\; k \in [\![0, p-1]\!]\right\}.$$

Tout d'abord, l'égalité

$$\lambda n - \lambda\frac{n}{p} = \lambda(p-1)\frac{n}{p} = \varphi\left(\frac{\mathrm{rad}(n)}{p}\right)(p-1)\frac{n}{p} = \varphi(\mathrm{rad}(n))\frac{n}{p} = \varphi(n)\frac{\mathrm{rad}(n)}{p}$$

implique que

$$2^{\lambda n} \equiv 2^{\lambda\frac{n}{p}} \pmod{n},$$

et ainsi,

$$2^{\alpha(p)\lambda\frac{n}{p}} \equiv 2^{\alpha(p)\lambda n} \equiv 1 \pmod{n},$$

comme $\alpha(n)$ divise $\lambda\alpha(p)$. Cela conduit à

$$\begin{aligned}
\Delta S_{l+k\alpha(p)}(i,j) &= \Delta S\left((k\alpha(p)+l-1)\lambda\tfrac{n}{p}+i, j\right)\\
&= 2^{(k\alpha(p)+l-1)\lambda\frac{n}{p}+i-1}\left(2a+\left(2j+(k\alpha(p)+l-1)\lambda\tfrac{n}{p}+i-3\right)d\right)\\
&= 2^{k\alpha(p)\lambda\frac{n}{p}}2^{(l-1)\lambda\frac{n}{p}+i-1}\left(2a+\left(2j+(k\alpha(p)+l-1)\lambda\tfrac{n}{p}+i-3\right)d\right)\\
&= 2^{(l-1)\lambda\frac{n}{p}+i-1}\left(2a+\left(2j+(l-1)\lambda\tfrac{n}{p}+i-3\right)d\right)+k\left(2^{(l-1)\lambda\frac{n}{p}+i-1}\lambda\alpha(p)d\right)\tfrac{n}{p}\\
&= \Delta S\left((l-1)\lambda\tfrac{n}{p}+i, j\right)+k\left(2^{(l-1)\lambda\frac{n}{p}+i-1}\lambda\alpha(p)d\right)\tfrac{n}{p}\\
&= \Delta S_l(i,j)+k\left(2^{(l-1)\lambda\frac{n}{p}+i-1}\lambda\alpha(p)d\right)\tfrac{n}{p},
\end{aligned}$$

pour tout entier k, $0 \leqslant k \leqslant p-1$. La congruence $p \equiv 1 \pmod{\alpha(p)}$ implique que $\alpha(p)$ n'est pas divisible par p. De plus, comme p est le plus grand facteur premier de n, il s'ensuit que $\lambda = \varphi\left(\frac{\mathrm{rad}(n)}{p}\right)$ est premier avec p et alors, l'entier $\lambda\alpha(p)$ n'est pas divisible par p. Par conséquent, on obtient l'égalité suivante, portant sur des multiensembles,

$$\left\{\Delta S_{l+k\alpha(p)}(i,j) \;\middle|\; k \in [\![0, p-1]\!]\right\} = \left\{\Delta S_l(i,j), \Delta S_l(i,j)+\frac{n}{p}, \ldots, \Delta S_l(i,j)+\frac{(p-1)n}{p}\right\},$$

pour tout entier l, $1 \leqslant l \leqslant \alpha(p)$, tout entier i, $1 \leqslant i \leqslant \lambda\frac{n}{p}$, et tout entier j, $1 \leqslant j \leqslant \lambda\frac{n}{p}-i+1$. Si l'on note A la réunion de tous les multiensembles A_r, alors la fonction de multiplicité de A est constante sur chaque coset du sous-groupe $\frac{n}{p}\mathbb{Z}/n\mathbb{Z}$.

On rassemble maintenant les résultats obtenus auparavant. Par les Etapes 1 et 2, on a

$$\begin{aligned}
\mathfrak{m}_{\Delta S}(x) &= \mathfrak{m}_A(x)+\mathfrak{m}_B(x)+\sum_{u=1}^{\alpha(p)-1}\mathfrak{m}_{C_u}(x)\\
&= \mathfrak{m}_A(x)+\alpha(p)\lambda^2\tfrac{(p-1)n}{2p}+\sum_{u=1}^{\alpha(p)-1}(\alpha(p)-u)\lambda^2 n\\
&= \mathfrak{m}_A(x)+\alpha(p)\lambda^2\tfrac{(p-1)n}{2p}+\binom{\alpha(p)}{2}\lambda^2 n,
\end{aligned}$$

pour tout x dans $\mathbb{Z}/n\mathbb{Z}$ et ainsi, par l'Etape 3, la fonction de multiplicité $\mathfrak{m}_{\Delta S}$ est constante sur chaque coset du sous-groupe $\frac{n}{p}\mathbb{Z}/n\mathbb{Z} = q\mathbb{Z}/n\mathbb{Z}$.

On termine la preuve en montrant que $\pi_q(S)$, l'image de la suite S par le morphisme surjectif $\pi_q : \mathbb{Z}/n\mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/q\mathbb{Z}$ avec $q = \frac{n}{p}$, est une suite balancée. Tout d'abord, la suite $\pi_q(S)$ est la suite arithmétique commençant par $\pi_q(a) \in \mathbb{Z}/q\mathbb{Z}$, de raison $\pi_q(d) \in \mathbb{Z}/q\mathbb{Z}$ et de longueur $\lambda\alpha(p)n$, c'est-à-dire,

$$\pi_q\left(S\right) = \pi_q\left(PA(a, d, \lambda\alpha(p)n)\right) = PA\left(\pi_q(a), \pi_q(d), \lambda\alpha(p)n\right).$$

Ensuite, l'entier $\lambda\alpha(p)$ est divisible par $\alpha(q)$. En effet, si $v_p(n) \geqslant 2$, alors $\mathrm{rad}(q) = \mathrm{rad}(n)$ et donc $\alpha(q)$ divise $\alpha(\mathrm{rad}(q)) = \alpha(\mathrm{rad}(n))$ par la Proposition 4.4.3. Comme déjà vu auparavant, l'entier $\lambda\alpha(p)$ est divisible par $\alpha(\mathrm{rad}(n))$ et alors, $\alpha(q)$ divise $\lambda\alpha(p)$. Sinon, si $v_p(n) = 1$, alors $\mathrm{rad}(q) = \frac{\mathrm{rad}(n)}{p}$ et donc $\alpha(q)$ divise $\alpha(\mathrm{rad}(q)) = \alpha\left(\frac{\mathrm{rad}(n)}{p}\right)$ par la Proposition 4.4.3. Comme $\lambda = \varphi\left(\frac{\mathrm{rad}(n)}{p}\right)$ est divisible par $\alpha\left(\frac{\mathrm{rad}(n)}{p}\right)$, il suit que $\alpha(q)$ divise λ. Dans tous les cas, on a

$$\lambda\alpha(p) \equiv 0 \pmod{\alpha(q)}.$$

Par conséquent, l'hypothèse d'induction implique que la suite $\pi_q(S)$ est balancée, comme c'est une suite arithmétique de raison $\pi_q(d)$ et de longueur $\lambda\alpha(p)n$ divisible par $\alpha(q)q$.

On conclut alors que la suite S est balancée par le Théorème 4.2.3. Ce qui complète la preuve du Théorème 4.4.2. □

Par exemple, dans $\mathbb{Z}/7\mathbb{Z}$, la suite arithmétique $PA(1, 3, 20)$ est balancée puisque $\alpha(7) = 3$ et 3 est un élément inversible de $\mathbb{Z}/7\mathbb{Z}$. En effet, comme représenté à la Figure 4.10, chaque élément de $\mathbb{Z}/7\mathbb{Z}$ apparaît 30 fois dans ce triangle de Steinhaus.

On peut, dans un premier temps, voir le Théorème 4.4.2 comme une solution partielle du Problème de Molluzzo.

Corollaire 4.4.8. *Soit n un nombre impair. Alors, il existe au moins $\varphi(n)n$ suites balancées pour toute longueur $m \equiv 0$ ou $-1 \pmod{\varphi(\mathrm{rad}(n))n}$.*

Preuve. Puisqu'il y a n éléments distincts a dans $\mathbb{Z}/n\mathbb{Z}$ et $\varphi(n)$ éléments inversibles distincts d dans $\mathbb{Z}/n\mathbb{Z}$, il suit que, pour chaque entier positif m, il existe exactement $\varphi(n)n$ suites arithmétiques distinctes $PA(a, d, m)$ de raison inversible dans $\mathbb{Z}/n\mathbb{Z}$ et de longueur m. De plus, pour n impair, l'entier $\alpha(n)$ divise $\alpha(\mathrm{rad}(n))$ par la Proposition 4.4.3, qui divise $\varphi(\mathrm{rad}(n))$ par définition de la fonction α. Par conséquent, pour n impair, le Théorème 4.4.2 implique qu'il existe au moins $\varphi(n)n$ suites balancées pour toute longueur $m \equiv 0$ ou $-1 \pmod{\varphi(\mathrm{rad}(n))n}$. □

Cependant, le Théorème 4.4.2 n'est pas suffisant pour complètement résoudre le Problème de Molluzzo, comme le montre la proposition suivante. Cette lacune est en partie surmontée dans la section qui suit.

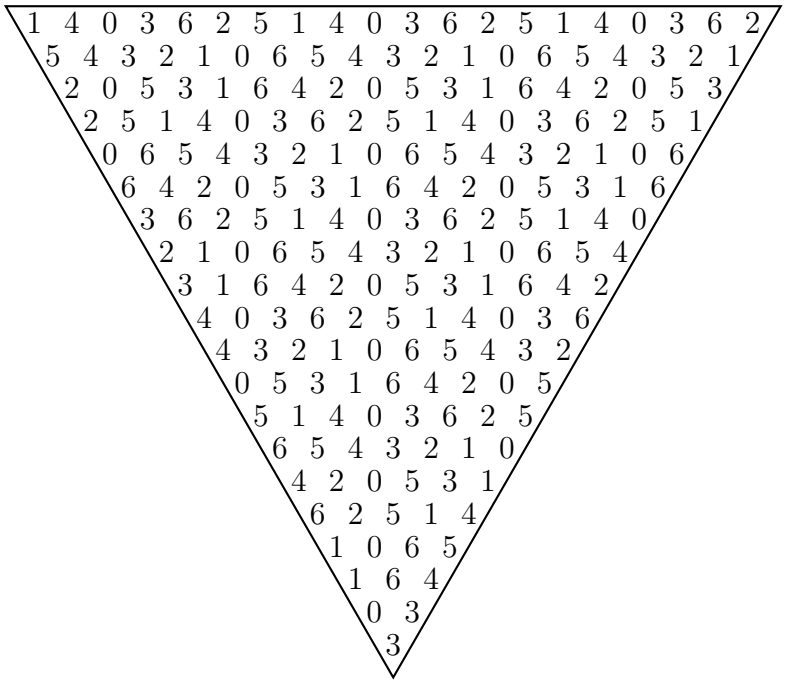


FIG. 4.10 – Le triangle de Steinhaus $\Delta PA(1, 3, 20)$

Proposition 4.4.9. *Soit $n > 1$ un nombre impair. Alors*

$$\alpha(n) \geqslant 2.$$

Preuve. Soit

$$n = {p_1}^{r_1} \cdots {p_k}^{r_k}$$

la factorisation en nombres premiers du nombre impair $n > 1$. Si $\alpha(n) = 1$, alors

$$2^n \equiv 1 \pmod{n}.$$

Soit p_j le plus petit facteur premier de n. Puisque

$$2^n \equiv 1 \pmod{p_j},$$

il s'ensuit que $\mathcal{O}_{p_j}(2)$ divise n, en contradiction avec le fait que $\mathcal{O}_{p_j}(2)$ divise $p_j - 1$ qui est premier avec n. □

4.5 Le cas antisymétrique

A la Section 4.4, on a vu qu'il existe une infinité de suites balancées dans $\mathbb{Z}/n\mathbb{Z}$, pour n impair. Plus précisément, le Théorème 4.4.2 établit que toutes les suites arithmétiques de raison inversible et de longueur $m \equiv 0$ ou $-1 \pmod{\alpha(n)n}$ sont balancées. Dans cette section, on raffine ce résultat en considérant les suites antisymétriques dans $\mathbb{Z}/n\mathbb{Z}$. Ceci est

suffisant pour répondre positivement au Problème de Molluzzo dans le cas où $n = 3^k$, pour tout entier $k \geqslant 1$.

Définition 4.5.1. Soit $S = (a_1, a_2, \ldots, a_m)$ une suite finie de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. La suite S est dite *antisymétrique* si $a_{m-i+1} = -a_i$, pour tout entier i, $1 \leqslant i \leqslant m$.

Remarque. Dans $\mathbb{Z}/2\mathbb{Z}$, cette définition de suite antisymétrique diffère de la définition que l'on a donnée au Chapitre 1 mais elle correspond à la définition de suite symétrique.

On commence par montrer que l'antisymétrie est préservée par l'opération de dérivation. Elle l'est également par l'opération d'intégration mais sous certaines conditions.

Proposition 4.5.2. *Soit $S = (a_1, a_2, \ldots, a_m)$ une suite finie de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Alors, la suite S est antisymétrique si, et seulement si, sa suite dérivée ∂S est aussi antisymétrique et $a_{\lceil \frac{m}{2} \rceil} + a_{m-\lceil \frac{m}{2} \rceil+1} = 0$, où $\lceil \frac{m}{2} \rceil$ est la partie entière supérieure de $\frac{m}{2}$.*

Preuve. On pose $S = (a_1, a_2, \ldots, a_m)$ et $\partial S = T = (b_1, b_2, \ldots, b_{m-1})$ sa suite dérivée.

$\Longrightarrow$ Pour tout entier i, $1 \leqslant i \leqslant m-1$, on a

$$b_{m-i} + b_i = (a_{m-i} + a_{m-i+1}) + (a_i + a_{i+1}) = (a_{m-i+1} + a_i) + (a_{m-i} + a_{i+1}) = 0.$$

$\Longleftarrow$ Par induction, on peut prouver que

$$\begin{aligned} a_i &= (-1)^{j-i} a_j + \sum_{k=i}^{j-1} (-1)^{k-i} b_k, \\ a_j &= (-1)^{j-i} a_i + \sum_{k=i}^{j-1} (-1)^{j-k-1} b_k, \end{aligned}$$

pour tout entier i et tout entier j, $1 \leqslant i < j \leqslant m$. Ceci entraîne que

$$a_{m-i+1} + a_i = (-1)^{\lceil \frac{m}{2} \rceil - i} a_{m-\lceil \frac{m}{2} \rceil+1} + \sum_{k=m-\lceil \frac{m}{2} \rceil+1}^{m-i} (-1)^{m-k-i} b_k + (-1)^{\lceil \frac{m}{2} \rceil - i} a_{\lceil \frac{m}{2} \rceil}$$
$$+ \sum_{k=i}^{\lceil \frac{m}{2} \rceil - 1} (-1)^{k-i} b_k = (-1)^{\lceil \frac{m}{2} \rceil - i} \underbrace{\left(a_{\lceil \frac{m}{2} \rceil} + a_{m-\lceil \frac{m}{2} \rceil+1} \right)}_{=0} + \sum_{k=i}^{\lceil \frac{m}{2} \rceil - 1} (-1)^{k-i} (\underbrace{b_k + b_{m-k}}_{=0}) = 0,$$

pour tout entier i, $1 \leqslant i \leqslant \lceil \frac{m}{2} \rceil - 1$.

Ce qui complète la preuve. □

Proposition 4.5.3. *Soit n un nombre impair. Soient a et d dans $\mathbb{Z}/n\mathbb{Z}$. Alors, la suite arithmétique $PA(a, d, m)$ de longueur $m \geqslant 2$ est antisymétrique si, et seulement si, sa suite dérivée $PA(2a + d, 2d, m - 1)$ est également antisymétrique.*

Preuve. On pose $S = PA(a, d, m) = (a_1, a_2, \ldots, a_m)$ et $\partial S = PA(2a + d, 2d, m - 1) = (b_1, b_2, \ldots, b_{m-1})$. Il suit que

$$\begin{aligned} b_{m-i} + b_i &= (2a + d) + (m - i - 1)2d + (2a + d) + (i - 1)2d = 2(2a + (m - 1)d) \\ &= 2(a + (m - j)d + a + (j - 1)d) = 2(a_{m-j+1} + a_j), \end{aligned}$$

pour tout entier i, $1 \leqslant i \leqslant m - 1$, et tout entier j, $1 \leqslant j \leqslant m$. □

A contrario, pour n pair, cette proposition n'est pas vraie. Par exemple, pour $n = 8$, la suite arithmétique $S = (01234)$ n'est pas antisymétrique alors que sa suite dérivée $\partial S = (1357)$ l'est.

On détermine maintenant les suites arithmétiques qui sont antisymétriques dans $\mathbb{Z}/n\mathbb{Z}$ pour n impair.

Proposition 4.5.4. *Soit n un nombre impair. Soient d dans $\mathbb{Z}/n\mathbb{Z}$ et $m \geqslant 1$ un entier. Alors, il existe une unique suite arithmétique et antisymétrique de raison d et de longueur m. De plus, pour $m \equiv 0 \pmod{n}$, il s'agit de la suite $PA(2^{-1}d, d, m)$ et pour $m \equiv -1 \pmod{n}$, il s'agit de la suite $PA(d, d, m)$.*

Preuve. On pose $S = PA(a, d, m) = (a_1, a_2, \ldots, a_m)$. Si la suite S est antisymétrique, alors

$$a_{m-i+1} + a_i = 0$$

pour tout entier i, $1 \leqslant i \leqslant m$. Puisque

$$a_{m-i+1} + a_i = a + (m-i)d + a + (i-1)d = 2a + (m-1)d$$

pour chaque entier i, $1 \leqslant i \leqslant m$, il suit que la suite arithmétique S est antisymétrique si, et seulement si, les entiers a, d et m sont tels que $2a + (m-1)d = 0$. Par conséquent, la suite

$$PA\left(2^{-1}(1-m)d, d, m\right)$$

est la seule suite arithmétique de longueur $m \geqslant 1$ et de raison $d \in \mathbb{Z}/n\mathbb{Z}$ qui soit antisymétrique. Ceci complète la preuve. □

Pour n pair, l'unicité précédente n'est plus valable en générale. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, les suites antisymétriques (02460) et (46024) sont toutes deux des suites arithmétiques de longueur $m = 5$ et de raison $d = 2$.

Notation. Pour tout nombre impair n, on note $\beta(n)$ *l'ordre multiplicatif projectif de* 2^n *modulo* n, i.e. le plus petit entier positif e tel que $2^{en} \equiv \pm 1 \pmod{n}$, à savoir,

$$\beta(n) = \min\left\{e \in \mathbb{N}^* \mid 2^{en} \equiv \pm 1 \pmod{n}\right\}.$$

On peut remarquer que l'on a soit $\alpha(n) = \beta(n)$, soit $\alpha(n) = 2\beta(n)$. De plus, $\alpha(n) = 2\beta(n)$ si, et seulement si, il existe une puissance e de 2^n telle que $2^{en} \equiv -1 \pmod{n}$. Si n est une puissance de premier, alors $\beta(n) = \beta(\mathrm{rad}(n))$, en analogie avec la Proposition 4.4.4 pour $\alpha(n)$.

Proposition 4.5.5. *Soit p un nombre premier impair. Alors,*

$$\beta\left(p^k\right) = \beta\left(p\right),$$

pour tout entier $k \geqslant 1$.

Preuve. Le résultat se déduit de l'affirmation que $\alpha(p^k) = 2\beta(p^k)$ si, et seulement si, $\alpha(p) = 2\beta(p)$.

En effet, si $\alpha(p^k) = 2\beta(p^k)$, alors on a $2^{\beta(p^k)p^k} \equiv -1 \pmod{p^k}$. Ce qui implique que $2^{\beta(p^k)p^k} \equiv -1 \pmod{p}$ et donc $2^{\beta(p^k)p} \equiv -1 \pmod{p}$ par le petit théorème de Fermat. Il suit que $\alpha(p) = 2\beta(p)$.

Réciproquement, si $\alpha(p) = 2\beta(p)$, alors $2^{\beta(p)p} \equiv -1 \pmod{p}$. Par induction sur k, il suit du théorème du binôme qu'il existe un entier positif u_k tel que $2^{\beta(p)p^k} = -1 + u_k p^k$. Cela conduit à la congruence $2^{\beta(p)p^k} \equiv -1 \pmod{p^k}$ et donc on a $\alpha(p^k) = 2\beta(p^k)$.

Dans les deux cas, $\alpha(p^k) = 2\beta(p^k)$ ou $\alpha(p^k) = \beta(p^k)$, le résultat se déduit de la Proposition 4.4.4. □

On peut maintenant raffiner le Théorème 4.4.2 en considérant les suites arithmétiques et antisymétriques de raison inversible. Par la Proposition 4.5.4, il y a exactement $\varphi(n)$ telles suites, pour toutes les longueurs.

Théorème 4.5.6. *Soient n un nombre impair et d un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Alors*
- *pour tout $m \equiv 0 \pmod{\beta(n)n}$, la suite arithmétique $PA(2^{-1}d, d, m)$ est balancée,*
- *pour tout $m \equiv -1 \pmod{\beta(n)n}$, la suite arithmétique $PA(d, d, m)$ est balancée.*

La preuve est basée sur le Théorème 4.4.2 et sur le lemme suivant.

Lemme 4.5.7. *Soient $n \geqslant 1$ un entier et S une suite antisymétrique de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Alors on a*

$$\mathfrak{m}_{\Delta S}(x) = \mathfrak{m}_{\Delta S}(-x), \ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Preuve. Par la Proposition 4.5.3, toutes les suites dérivées successives de S sont antisymétriques. Ceci conduit à l'égalité suivante

$$\mathfrak{m}_{\Delta S}(x) = \sum_{i=0}^{m-1} \mathfrak{m}_{\partial^i S}(x) = \sum_{i=0}^{m-1} \mathfrak{m}_{\partial^i S}(-x) = \mathfrak{m}_{\Delta S}(-x), \ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

□

On est maintenant prêt à prouver notre raffinement du Théorème 4.4.2.

Preuve du Théorème 4.5.6. Comme pour la preuve du Théorème 4.4.2, on commence par montrer que le cas $m \equiv -1 \pmod{\beta(n)n}$ dérive du cas $m \equiv 0 \pmod{\beta(n)n}$. Soit $k \geqslant 1$ un entier. On pose $m = k\beta(n)n - 1$ et $S = PA(d, d, m)$. Par la Proposition 4.3.3, la suite arithmétique

$$T = PA(2^{-2}d, 2^{-1}d, k\beta(n)n)$$

est une primitive de la suite S. Comme T est une suite arithmétique de raison inversible $2^{-1}d$ et de longueur $k\beta(n)n$, il suit du Lemme 4.4.6 que chaque élément du groupe $\mathbb{Z}/n\mathbb{Z}$ apparaît $k\beta(n)$ fois dans la suite T. Puisque S est la suite dérivée de T, on a

$$\mathfrak{m}_{\Delta S}(x) = \mathfrak{m}_{\Delta\partial T}(x) = \mathfrak{m}_{\Delta T}(x) - \mathfrak{m}_T(x) = \mathfrak{m}_{\Delta T}(x) - k\beta(n),$$

pour tout x dans $\mathbb{Z}/n\mathbb{Z}$. Par conséquent, la suite S est balancée si, et seulement si, la suite T l'est aussi. Ce qui complète la preuve du cas $m \equiv -1 \pmod{\beta(n)n}$ à partir du cas $m \equiv 0 \pmod{\beta(n)n}$.

On va maintenant s'occuper du cas où $m \equiv 0 \pmod{\beta(n)n}$. Si $\alpha(n) = \beta(n)$, alors ce résultat est un cas particulier du Théorème 4.4.2. Supposons que $\alpha(n) = 2\beta(n)$ et donc que $2^{\beta(n)n} \equiv -1 \pmod{n}$. Soit $k \geqslant 1$ un entier. On montre que la suite

$$PA\left(2^{-1}d, d, k\beta(n)n\right)$$

est balancée. Tout d'abord, on pose

$$S = PA(2^{-1}d, d, 2k\beta(n)n).$$

On considère alors la structure du triangle de Steinhaus ΔS représentée à la Figure 4.11. Rappelons que $\Delta S(i,j)$ désigne le $j$ème élément de la $i$ème ligne de ΔS, pour tout entier i, $1 \leqslant i \leqslant 2k\beta(n)n$, et tout entier j, $1 \leqslant j \leqslant 2k\beta(n)n - i + 1$.

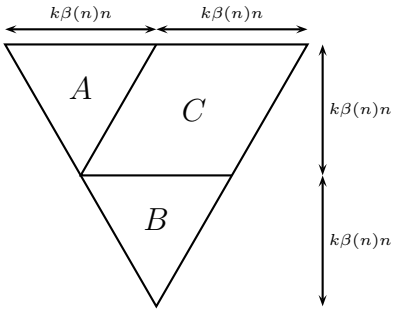


FIG. 4.11 – Structure de ΔS

Le sous-triangle A est défini par

$$A = \{\Delta S(i,j) \mid 1 \leqslant i \leqslant k\beta(n)n \ , \ 1 \leqslant j \leqslant k\beta(n)n - i + 1\}\,.$$

Alors A est le triangle de Steinhaus engendré par les $k\beta(n)n$ premiers éléments de la suite S, c'est-à-dire,

$$A = \Delta PA\left(2^{-1}d, d, k\beta(n)n\right).$$

Le sous-triangle B est défini par

$$B = \{\Delta S(i,j) \mid k\beta(n)n + 1 \leqslant i \leqslant 2k\beta(n)n \ , \ 1 \leqslant j \leqslant 2k\beta(n)n - i + 1\}\,.$$

Alors B est le triangle de Steinhaus engendré par la suite dérivée $\partial^{k\beta(n)n}S$, c'est-à-dire,

$$B = \Delta\partial^{k\beta(n)n}S.$$

La Proposition 4.3.1 entraîne que

$$\begin{aligned}\partial^{k\beta(n)n}S &= \partial^{k\beta(n)n}PA\left(2^{-1}d, d, 2k\beta(n)n\right)\\ &= PA\left(2^{k\beta(n)n-1}d + 2^{k\beta(n)n-1}k\beta(n)nd, 2^{k\beta(n)n}d, k\beta(n)n\right).\end{aligned}$$

Puisque $2^{\beta(n)n} \equiv -1 \pmod{n}$, il s'ensuit que

$$\partial^{k\beta(n)n}S = PA\left((-1)^k 2^{-1}d, (-1)^k d, k\beta(n)n\right).$$

Si k est pair, alors $\partial^{k\beta(n)n}S = PA\left(2^{-1}d, d, k\beta(n)n\right)$ et donc $A = B$. Si k est impair, alors $\partial^{k\beta(n)n}S = PA\left(-2^{-1}d, -d, k\beta(n)n\right)$. Comme c'est une suite arithmétique et antisymétrique par la Proposition 4.5.4, le Lemme 4.5.7 entraîne que $\mathfrak{m}_B(x) = \mathfrak{m}_B(-x)$ pour tout x dans $\mathbb{Z}/n\mathbb{Z}$. Par conséquent, on obtient

$$\mathfrak{m}_B(x) = \mathfrak{m}_B(-x) = \mathfrak{m}_{\Delta PA(-2^{-1}d,-d,k\beta(n)n)}(-x) = \mathfrak{m}_{\Delta PA(2^{-1}d,d,k\beta(n)n)}(x) = \mathfrak{m}_A(x)$$

pour tout $x \in \mathbb{Z}/n\mathbb{Z}$. Dans tous les cas, on a

$$\mathfrak{m}_B(x) = \mathfrak{m}_A(x),\ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Enfin, le multiensemble C est défini par

$$C = \left\{\Delta S(i,j) \mid 1 \leqslant i \leqslant k\beta(n)n\ ,\ k\beta(n)n - i + 2 \leqslant j \leqslant 2k\beta(n)n - i + 1\right\}.$$

Alors chaque ligne de C est composée de $k\beta(n)n$ termes consécutifs d'une suite dérivée de S. Comme, pour tout entier i, $0 \leqslant i \leqslant 2k\beta(n)n - 1$, la suite dérivée $\partial^i S$ de S est une suite arithmétique de raison inversible $2^i d$ par la Proposition 4.3.1, il suit du Lemme 4.4.6 que chaque élément du groupe $\mathbb{Z}/n\mathbb{Z}$ apparaît $k\beta(n)$ fois dans chaque ligne de C. Par conséquent, la fonction de multiplicité de C est la fonction constante définie par

$$\mathfrak{m}_C(x) = k^2\beta(n)^2 n,\ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

En combinant les résultats précédents, on obtient

$$\mathfrak{m}_{\Delta S}(x) = \mathfrak{m}_A(x) + \mathfrak{m}_B(x) + \mathfrak{m}_C(x) = 2\mathfrak{m}_A(x) + k^2\beta(n)^2 n$$

pour tout x dans $\mathbb{Z}/n\mathbb{Z}$.

On en conclut que la suite $PA(2^{-1}d, d, k\beta(n)n)$ est balancée si, et seulement si, la suite $S = PA(2^{-1}d, d, 2k\beta(n)n) = PA(2^{-1}d, d, k\alpha(n)n)$ est aussi balancée. Ce qui complète la preuve du Théorème 4.5.6. □

4.6 Solutions du Problème de Molluzzo

Tout d'abord, le Théorème 4.5.6 permet de répondre positivement et complètement au Problème de Molluzzo dans tout groupe cyclique d'ordre une puissance de 3.

Corollaire 4.6.1. *Il existe une suite balancée de longueur m dans $\mathbb{Z}/3^k\mathbb{Z}$ si, et seulement si, $\binom{m+1}{2}$ est divisible par 3^k.*

Preuve. Soit $k \geqslant 1$ un entier. Par la Proposition 4.5.5, on a

$$\beta(3^k) = \beta(3) = 1.$$

Soit d un élément inversible de $\mathbb{Z}/3^k\mathbb{Z}$. Alors, le Théorème 4.5.6 dit que
- $PA(2^{-1}d, d, m)$ est balancée pour tout entier positif $m \equiv 0 \pmod{3^k}$,
- $PA(d, d, m)$ est balancée pour tout entier positif $m \equiv -1 \pmod{3^k}$.

Enfin, du Corollaire 4.2.2, on sait que 3^k divise le coefficient binomial $\binom{m+1}{2}$ si, et seulement si, l'entier m est congru à 0 ou à -1 modulo 3^k. Par conséquent, on a bien construit des suites balancées pour toutes les longueurs admissibles dans $\mathbb{Z}/3^k\mathbb{Z}$. □

Les résultats précédents permettent également de répondre partiellement au Problème de Molluzzo dans chaque groupe cyclique d'ordre impair.

Notations. On note $N(n)$ l'ensemble des longueurs admissibles pour une suite balancée dans $\mathbb{Z}/n\mathbb{Z}$, c'est à dire l'ensemble des entiers positifs m tels que que $\binom{m+1}{2}$ est un multiple de n, et $B(n)$ l'ensemble des longueurs des suites balancées dans $\mathbb{Z}/n\mathbb{Z}$, à savoir,

$$N(n) = \left\{ m \in \mathbb{N} \;\middle|\; \binom{m+1}{2} \equiv 0 \pmod{n} \right\},$$

et

$$B(n) = \{ m \in \mathbb{N} \mid \exists \text{ une suite balancée dans } \mathbb{Z}/n\mathbb{Z} \text{ de longueur } m \},$$

Comme déjà remarqué dans les Sections 4.1 et 4.2, on a clairement $B(n) \subset N(n)$. De plus, le Problème de Molluzzo peut être reformulé sous la question de savoir si $B(n) = N(n)$ pour tout $n > 1$. On a vu qu'il existe des valeurs de n pour lesquelles cette égalité n'est pas vraie, par exemple pour $n = 15$ ou $n = 21$, et on a conjecturé que $B(p^k) = N(p^k)$ pour tout p premier. Néanmoins, les résultats des sections précédentes, plus particulièrement les Théorèmes 4.2.1 et 4.5.6, impliquent la minoration suivante.

Proposition 4.6.2. *Soit n un nombre impair. Alors,*

$$\frac{|B(n) \cap [\![0, k]\!]|}{|N(n) \cap [\![0, k]\!]|} \geqslant \frac{1}{2^{\omega(n)-1}\beta(n)},$$

pour tout $k \geqslant \beta(n)n$.

Puisque $2^{\omega(n)-1}\beta(n) \geqslant 2$ pour tout nombre impair $n \neq 3^k$, il s'ensuit que la méthode décrite ici ne donne une solution complète au Problème de Molluzzo que pour les puissances de 3. Par exemple, pour $n = 5^k$, on a $2^{\omega(n)-1}\beta(n) = 2$, et donc nos résultats fournissent des suites balancées pour la moitié des longueurs admissibles dans ce cas.

4.7 Suites arithmétiques balancées dans les groupes cycliques d'ordre pair

Dans les sections précédentes, on a vu que, pour tout nombre impair n et tout élément inversible d de $\mathbb{Z}/n\mathbb{Z}$, les suites arithmétiques $PA(a,d,m)$, pour $m \equiv 0$ ou $-1 \pmod{\alpha(n)n}$, constituent une famille infinie de suites balancées. Dans cette section, on étudie le cas où n est pair et on montre que, contrairement au cas impair, presqu'aucune suite arithmétique n'est balancée dans les groupes cycliques d'ordre pair.

Théorème 4.7.1. *Soit n un nombre pair et soient a et d dans $\mathbb{Z}/n\mathbb{Z}$. Alors la suite arithmétique $S = PA(a,d,m)$ est balancée si, et seulement si, on a*

$$\begin{cases} n = 2 \quad et \quad S \in \{(010),(111),(0101),(1010)\}, \\ \quad ou \\ n = 6 \quad et \quad S \in \{(135),(234),(432),(531)\}. \end{cases}$$

Preuve. Supposons que la suite arithmétique $S = PA(a,d,m)$ soit balancée. Tout d'abord, on considère la projection $\pi_2 : \mathbb{Z}/n\mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/2\mathbb{Z}$ et la suite projetée $\pi_2(S) = PA(\pi_2(a), \pi_2(d), m)$ dans $\mathbb{Z}/2\mathbb{Z}$ qui est aussi balancée par le Théorème 4.2.3. Si l'on note par $\Delta\pi_2(S)(i,j)$ le $j$ème élément de la $i$ème ligne du triangle $\Delta\pi_2(S)$, alors la Proposition 4.3.2 implique que

$$\Delta\pi_2(S)(i,j) = 2^{i-2}(2\pi_2(a) + (2j+i-3)\pi_2(d)) = 0 \in \mathbb{Z}/2\mathbb{Z},$$

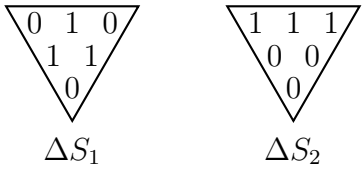
pour tout $i \geqslant 3$. Par conséquent, pour tout $i \geqslant 3$, la suite dérivée $\partial^i S$ est la suite nulle, c'est-à-dire, la suite contenant uniquement des zéros. Puisque la suite $\pi_2(S)$ est balancée, il suit que son triangle $\Delta\pi_2(S)$ doit contenir au moins deux fois plus d'éléments que $\pi_2(S)$ et sa suite dérivée $\partial\pi_2(S)$. Par conséquent, l'entier $m \geqslant 1$ est solution de l'inégalité suivante :

$$2\binom{m-1}{2} \leqslant \binom{m+1}{2}.$$

Par conséquent, $m \in [\![1,6]\!]$. De plus, la condition nécessaire que le coefficient binomial $\binom{m+1}{2}$, le cardinal du triangle de Steinhaus $\Delta\pi_2(S)$, doit être pair implique que $m = 3$ ou $m = 4$. On distingue maintenant les différents cas.

m = 3 : Puisque n divise $\binom{m+1}{2} = 6$, il suit que $n = 2$ ou $n = 6$.

n = 2 : Il existe quatre suites arithmétiques de longueur $m = 3$ dans $\mathbb{Z}/2\mathbb{Z}$ dont deux sont balancées. Ce sont les suites $S_1 = (010)$ et $S_2 = (111)$.



ΔS_1 ΔS_2

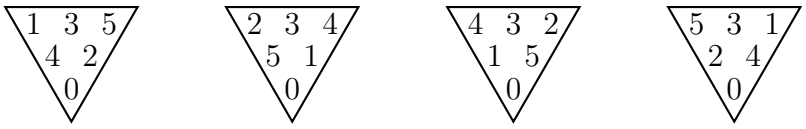
n = 6 : On recherche un triangle de Steinhaus ΔS contenant chaque élément de $\mathbb{Z}/6\mathbb{Z}$ exactement une fois. Comme l'égalité $\Delta S\,(i,j) = 0$ implique $\Delta S(i, j-1) = \Delta S(i+1, j-1)$ ou $\Delta S(i, j+1) = \Delta S(i+1, j)$, il suit que $\Delta S(3,1) = 0$ et donc, on a

$$0 = \Delta S(3,1) = 4(a+d) = 4\Delta S(1,2).$$

Par conséquent, $\Delta S(1,2) = 3$ et on cherche alors une suite arithmétique balancée de la forme

$$S = (a, 3, -a),$$

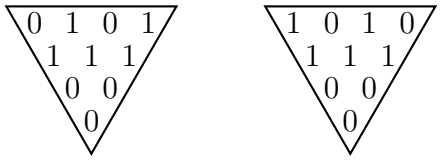
avec $a \in \{1, 2, 4, 5\}$. On trouve les quatre suites arithmétiques suivantes : $S_3 = (135)$, $S_4 = (234)$, $S_5 = (432)$ et $S_6 = (531)$.



ΔS_3 ΔS_4 ΔS_5 ΔS_6

m = 4 : Puisque n divise $\binom{m+1}{2} = 10$, il suit que $n = 2$ ou $n = 10$.

n = 2 : Il existe quatre suites arithmétiques de longueur $m = 4$ dans $\mathbb{Z}/2\mathbb{Z}$ dont deux sont balancées. Ce sont les suites $S_7 = (0101)$ et $S_8 = (1010)$.



ΔS_7 ΔS_8

n = 10 : On recherche un triangle de Steinhaus ΔS contenant chaque élément de $\mathbb{Z}/10\mathbb{Z}$ exactement une fois. Comme l'égalité $\Delta S\,(i,j) = 0$ implique $\Delta S(i, j-1) = \Delta S(i+1, j-1)$ ou $\Delta S(i, j+1) = \Delta S(i+1, j)$, il suit que $\Delta S(4,1) = 0$ et donc, on a

$$0 = \Delta S(4,1) = 4(2a+3d) = 4\Delta S(2,2).$$

Par conséquent, $\Delta S(2,2) = 5$. De plus, si $2a + 3d = 5$, alors

$$d = 3^{-1}(5-2a) = 7(5-2a) = 5-4a.$$

On cherche donc une suite arithmétique balancée de la forme

$$S = (a, 5-3a, 3a, 5-a)$$

avec $a \in \{1, 2, 3, 4, 6, 7, 8, 9\}$. Enfin, il n'existe pas de telle suite dans $\mathbb{Z}/10\mathbb{Z}$.

□

Chapitre 5

L'ordre multiplicatif de a^n modulo n

Au chapitre précédent, on a vu que, dans tout groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ d'ordre n impair, les suites arithmétiques $PA(a, d, m)$ de raison inversible d sont balancées pour toute longueur $m \equiv 0$ ou $-1 \pmod{\alpha(n)n}$, où $\alpha(n)$ correspond à l'ordre multiplicatif de 2^n modulo n. On s'intéresse ici à la fonction arithmétique α_n qui à tout élément a premier avec n associe l'ordre multiplicatif de a^n modulo n. La fonction α_n est donc une extension de la fonction α utilisée dans le chapitre précédent. Dans un premier temps, on prouve quelques résultats basiques qui sont des généralisations de ceux obtenus sur $\alpha(n)$. On montre ensuite qu'il existe une relation exacte entre les fonctions $\alpha_{\mathrm{rad}(n)}$ et α_n, pour tout entier n. Enfin, on s'intéresse à la fonction β_n qui est une extension de la fonction β introduite précédemment. Les résultats obtenus dans ce chapitre font l'objet d'un article qui sera soumis prochainement.

5.1 La fonction arithmétique α_n

Notation. Pour tout entier $n \geqslant 1$ et tout entier a premier avec n, on note $\mathcal{O}_n(a)$ *l'ordre multiplicatif de a modulo n*, i.e. le plus petit exposant e tel que $a^e \equiv 1 \pmod{n}$, à savoir

$$\mathcal{O}_n(a) = \min\left\{e \in \mathbb{N}^* \mid a^e \equiv 1 \pmod{n}\right\}.$$

L'ordre multiplicatif de a modulo n correspond également avec l'ordre de l'élément $\pi_n(a)$ dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, le groupe des unités de $\mathbb{Z}/n\mathbb{Z}$, et où $\pi_n : \mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/n\mathbb{Z}$ est le morphisme surjectif canonique. On peut remarquer que $\mathcal{O}_n(a)$ divise $\varphi(n)$.

Dans cette section, on s'intéresse à la fonction arithmétique α_n.

Définition 5.1.1. Soit $n \geqslant 1$ un entier. Soit α_n la fonction

$$\begin{array}{rccl} \alpha_n : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \left\{ \begin{array}{cl} \mathcal{O}_n\left(a^n\right) & \text{pour } a \wedge n = 1, \\ 0 & \text{sinon,} \end{array} \right. \end{array}$$

où $a \wedge n$ est le plus grand diviseur commun des entiers a et n, avec la convention que $0 \wedge n = n$ pour tout entier positif n.

Remarque. Comme $\mathcal{O}_n(a)$ divise $\varphi(n)$ et que l'on a l'égalité $\alpha_n(a) = \mathcal{O}_n(a^n) = \frac{\mathcal{O}_n(a)}{\mathcal{O}_n(a) \wedge n}$, on en déduit que l'entier $\alpha_n(a)$ divise $\frac{\varphi(n)}{\varphi(n) \wedge n}$, pour tout entier a premier avec n.

Proposition 5.1.2. *Soient n un entier positif et a un entier. Alors,*

$$a \wedge n = 1 \Longleftrightarrow a \wedge \mathrm{rad}(n) = 1.$$

Preuve. Evident. □

L'entier $\alpha_n(a)$ semble être difficile à déterminer. En effet, comme déjà remarqué dans le chapitre précédent, il n'existe pas de formule générale permettant de calculer directement l'ordre multiplicatif d'un entier modulo n. On peut néanmoins obtenir les résultats qui vont suivre.

Proposition 5.1.3. *Soient n un entier positif et a un entier. Alors l'entier $\alpha_n(a)$ divise $\alpha_{\mathrm{rad}(n)}(a)$.*

Preuve. Si $a \wedge n \neq 1$, alors, par définition des fonctions α_n et $\alpha_{\mathrm{rad}(n)}$ et par la Proposition 5.1.2, on obtient

$$\alpha_n(a) = \alpha_{\mathrm{rad}(n)}(a) = 0.$$

Supposons maintenant que $a \wedge n = 1$ et soit p un facteur premier de n tel que $v_p(n) \geqslant 2$. On montre que $\alpha_n(a)$ divise $\alpha_{\frac{n}{p}}(a)$. Par définition de $\alpha_{\frac{n}{p}}(a)$, il existe un entier positif u tel que

$$a^{\alpha_{\frac{n}{p}}(a)\frac{n}{p}} = 1 + u\frac{n}{p}.$$

Par conséquent, par le théorème du binôme, on a

$$a^{\alpha_{\frac{n}{p}}(a)n} = \left(a^{\alpha_{\frac{n}{p}}(a)\frac{n}{p}}\right)^p = \left(1 + u\frac{n}{p}\right)^p = 1 + un + \sum_{k=2}^{p} \binom{p}{k} u^k \left(\frac{n}{p}\right)^k.$$

Puisque $v_p(n) \geqslant 2$, il suit que $\left(\frac{n}{p}\right)^k$ est divisible par n pour tout entier $k \geqslant 2$ et donc

$$a^{\alpha_{\frac{n}{p}}(a)n} \equiv 1 \pmod{n}.$$

Alors $\alpha_n(a)$ divise $\alpha_{\frac{n}{p}}(a)$. Par induction, on obtient que $\alpha_n(a)$ divise $\alpha_{\mathrm{rad}(n)}(a)$. □

Une relation exacte entre $\alpha_n(a)$ et $\alpha_{\mathrm{rad}(n)}(a)$ est déterminée à la fin de cette section. Cependant, on peut facilement régler le cas où n est une puissance de nombre premier.

Proposition 5.1.4. *Soient p un nombre premier et a un entier. Alors, on a*

$$\alpha_{p^k}(a) = \alpha_p(a)$$

pour tout entier $k \geqslant 1$.

Preuve. Si $a \wedge n \neq 1$, alors $\alpha_n(a) = \alpha_{\mathrm{rad}(n)}(a) = 0$. Supposons maintenant que l'entier a est premier avec n. Par la Proposition 5.1.3, l'entier $\alpha_{p^k}(a)$ divise $\alpha_p(a)$. Il reste donc à prouver que $\alpha_p(a)$ divise bien $\alpha_{p^k}(a)$. La congruence

$$a^{\alpha_{p^k}(a)p^k} \equiv 1 \pmod{p^k}$$

implique que

$$a^{\alpha_{p^k}(a)p^k} \equiv 1 \pmod{p},$$

et donc, par le petit théorème de Fermat, il suit que

$$a^{\alpha_{p^k}(a)p} \equiv a^{\alpha_{p^k}(a)p^k} \equiv 1 \pmod{p}.$$

Par conséquent $\alpha_p(a)$ divise $\alpha_{p^k}(a)$. Ce qui complète la preuve. □

Remarque. Si $p = 2$, alors, pour tout entier positif k, on obtient que $\alpha_{2^k}(a) = \alpha_2(a) = 1$ pour tout entier a premier avec n.

Proposition 5.1.5. *Soient n_1 et n_2 deux nombres premiers entre eux et a un entier. Alors, l'entier $\alpha_{n_1n_2}(a)$ divise $\alpha_{n_1}(a) \vee \alpha_{n_2}(a)$.*

Preuve. Si $a \wedge n_1n_2 \neq 1$, alors $a \wedge n_1 \neq 1$ ou $a \wedge n_2 \neq 1$ et donc

$$\alpha_{n_1n_2}(a) = \alpha_{n_1}(a) \vee \alpha_{n_2}(a) = 0.$$

Supposons maintenant que $a \wedge n_1n_2 = 1$ et donc que les entiers a, n_1 et n_2 soient premiers entre eux deux par deux. Soit $i \in \{1, 2\}$. Les congruences

$$a^{\alpha_{n_i}(a)n_i} \equiv 1 \pmod{n_i}$$

impliquent que

$$a^{\left(\alpha_{n_1}(a)\vee\alpha_{n_2}(a)\right)n_1n_2} \equiv 1 \pmod{n_i}.$$

Par conséquent, le théorème des restes chinois implique que l'entier $\alpha_{n_1n_2}(a)$ divise $\alpha_{n_1}(a) \vee \alpha_{n_2}(a)$. □

Le tableau et le graphique représentés à la Figure 5.1 donnent les premières valeurs de $\alpha_n(a)$ pour tout entier $n \in [\![1, 20]\!]$ et tout entier $a \in [\![-20, 20]\!]$.

Par définition, on sait que $\alpha_n(a) = \alpha_{\mathrm{rad}(n)}(a) = 0$ pour tout entier a non premier avec n. Le reste de cette section est consacré à la détermination de la relation exacte qui lie $\alpha_n(a)$ et $\alpha_{\mathrm{rad}(n)}(a)$ pour tout entier a premier avec n. Ce résultat est un corollaire du théorème suivant.

$n\backslash a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
4	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
5	1	4	4	2	0	1	4	4	2	0	1	4	4	2	0	1	4	4	2	0
6	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
7	1	3	6	3	6	2	0	1	3	6	3	6	2	0	1	3	6	3	6	2
8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
9	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
10	1	0	2	0	0	0	2	0	1	0	1	0	2	0	0	0	2	0	1	0
11	1	10	5	5	5	10	10	10	5	2	0	1	10	5	5	5	10	10	10	5
12	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
13	1	12	3	6	4	12	12	4	3	6	12	2	0	1	12	3	6	4	12	12
14	1	0	3	0	3	0	0	0	3	0	3	0	1	0	1	0	3	0	3	0
15	1	4	0	2	0	0	4	4	0	0	2	0	4	2	0	1	4	0	2	0
16	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
17	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2	0	1	8	16
18	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
19	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2	0	1
20	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0

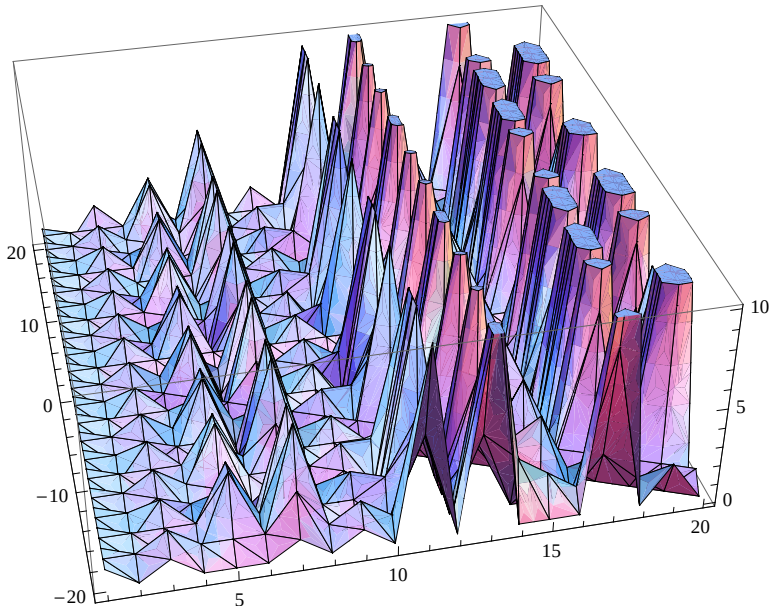


FIG. 5.1 – Les premières valeurs de $\alpha_n(a)$

Notation. Soit $\delta : \mathbb{N}^* \longrightarrow \{1, 2\}$ la fonction définie par

$$\delta(n) = \begin{cases} 2 & \text{si } n = 2, \\ 1 & \text{sinon.} \end{cases}$$

Théorème 5.1.6. *Soit*

$$n = {p_1}^{r_1} \cdots {p_k}^{r_k}$$

la factorisation en nombres premiers de l'entier positif n et soit $a \neq \pm 1$ un entier relativement premier avec n. Soient $s_1, \ldots, s_k$ les plus grands entiers tels que

$$a^{\mathcal{O}_{{p_i}^{\delta(p_i)}}(a)} \equiv 1 \pmod{{p_i}^{s_i}},$$

i.e. $s_i = v_{p_i}\left(a^{\mathcal{O}_{{p_i}^{\delta(p_i)}}(a)} - 1\right)$ pour tout i, $1 \leqslant i \leqslant k$. Si $v_2(n) \leqslant 1$, alors on a

$$\mathcal{O}_n(a) = \mathcal{O}_{\mathrm{rad}(n)}(a) \prod_{i=1}^{k} {p_i}^{\max\{0, r_i - s_i\}}.$$

Sinon, si $v_2(n) \geqslant 2$, alors on a

$$\mathcal{O}_n(a) = \mathcal{O}_{2\,\mathrm{rad}(n)}(a) \prod_{i=1}^{k} {p_i}^{\max\{0, r_i - s_i\}}.$$

La preuve de ce théorème est basée sur les deux lemmes suivants.

Lemme 5.1.7. *Soient p un nombre premier et $a \neq \pm 1$ un entier premier avec p. Soit s le plus grand entier tel que*

$$a^{\mathcal{O}_{p^{\delta(p)}}(a)} \equiv 1 \pmod{p^s}.$$

Alors, pour tout entier $l \geqslant 0$, il existe un entier u_l, premier avec p, tel que

$$a^{\mathcal{O}_{p^{\delta(p)}}(a)p^l} = 1 + u_l p^{s+l}.$$

Preuve. Par induction sur l. Si $l = 0$, alors, par définition du coefficient s, il existe un entier u_0 premier avec p tel que

$$a^{\mathcal{O}_{p^{\delta(p)}}(a)} = 1 + u_0 p^s.$$

Par conséquent, l'assertion est vraie pour $l = 0$. Supposons maintenant que l'assertion soit vraie pour un entier positif l donné. Alors, par le théorème binomial, on a

$$a^{\mathcal{O}_{p^{\delta(p)}}(a)p^{l+1}} = \left(1 + u_l p^{s+l}\right)^p = 1 + u_l p^{s+l+1} + \sum_{k=2}^{p} \binom{p}{k} {u_l}^k p^{(s+l)k}.$$

Si $p = 2$, alors $s \geqslant 2$ car

$$a^{\mathcal{O}_4(a)} = a^{\mathcal{O}_{p^{\delta(p)}}(a)} \equiv 1 \pmod{2^s}.$$

Par conséquent

$$\sum_{k=2}^{p} \binom{p}{k} {u_l}^k p^{(s+l)k} = {u_l}^2 2^{2(s+l)}$$

est divisible par 2^{s+l+2}. Sinon, si $p \geqslant 3$, alors $s \geqslant 1$ car

$$a^{\mathcal{O}_p(a)} = a^{\mathcal{O}_{p^{\delta(p)}}(a)} \equiv 1 \pmod{p^s}.$$

De plus, comme le coefficient binomial $\binom{p}{k}$ est divisible par p pour tout entier k, $2 \leqslant k \leqslant p-1$, il suit que

$$\sum_{k=2}^{p} \binom{p}{k} {u_l}^k p^{(s+l)k} = \sum_{k=2}^{p-1} \binom{p}{k} {u_l}^k p^{(s+l)k} + {u_l}^p p^{(s+l)p}$$

est divisible par p^{s+l+2}. Ainsi, dans tous les cas, il existe un entier $\tilde{u}$ tel que

$$a^{\mathcal{O}_{p^{\delta(p)}}(a)p^{l+1}} = 1 + u_l p^{s+l+1} + \tilde{u} p^{s+l+2} = 1 + (u_l + \tilde{u}p)p^{s+l+1}$$

et l'entier $u_l + \tilde{u}p$ est premier avec p. Ce qui complète la preuve. □

Lemme 5.1.8. *Soient p un nombre premier et $a \neq \pm 1$ un entier premier avec p. Soit s le plus grand entier tel que*

$$a^{\mathcal{O}_{p^{\delta(p)}}(a)} \equiv 1 \pmod{p^s}.$$

Alors, pour tout entier $r \geqslant \delta(p)$, on a

$$\mathcal{O}_{p^r}(a) = \mathcal{O}_{p^{\delta(p)}}(a) p^{\max\{0, r-s\}}.$$

Le cas impair de ce lemme correspond au Théorème 3.6 de [22]. Cependant, pour le confort du lecteur, la preuve suivante est autonome.

Preuve. Par induction sur l'entier r. Si $r = \delta(p)$, alors

$$s = v_p\left(a^{\mathcal{O}_{p^{\delta(p)}}(a)} - 1\right) = v_p\left(a^{\mathcal{O}_{p^r}(a)} - 1\right) \geqslant r.$$

Par conséquent $\max\{0, r-s\} = 0$ et l'assertion est vraie pour $r = \delta(p)$. Supposons maintenant que l'assertion soit vraie pour un entier $r \geqslant \delta(p)$. Tout d'abord, la congruence

$$a^{\mathcal{O}_{p^{r+1}}(a)} \equiv 1 \pmod{p^{r+1}}$$

implique que

$$a^{\mathcal{O}_{p^{r+1}}(a)} \equiv 1 \pmod{p^r}$$

et donc $\mathcal{O}_{p^r}(a)$ divise $\mathcal{O}_{p^{r+1}}(a)$. Comme

$$\mathcal{O}_{p^r}(a) = \mathcal{O}_{p^{\delta(p)}}(a) p^{\max\{0, r-s\}}$$

par hypothèse d'induction, il suit du Lemme 5.1.7 qu'il existe un entier u, premier avec p, tel que

$$a^{\mathcal{O}_{p^r}(a)} = a^{\mathcal{O}_{p^{\delta(p)}}(a)p^{\max\{0,r-s\}}} = 1 + up^{s+\max\{0,r-s\}} = 1 + up^{\max\{s,r\}}.$$

Si $r \leqslant s-1$, alors

$$a^{\mathcal{O}_{p^r}(a)} = 1 + up^s \equiv 1 \pmod{p^{r+1}},$$

et donc on obtient que $\mathcal{O}_{p^{r+1}}(a) = \mathcal{O}_{p^r}(a)$. Sinon, si $r \geqslant s$, alors

$$a^{\mathcal{O}_{p^r}(a)} = 1 + up^r \not\equiv 1 \pmod{p^{r+1}},$$

et donc $\mathcal{O}_{p^r}(a)$ est un diviseur propre de $\mathcal{O}_{p^{r+1}}(a)$. De plus, par le Lemme 5.1.7, il existe un entier v, premier avec p, tel que

$$a^{\mathcal{O}_{p^r}(a)p} = a^{\mathcal{O}_{p^{\delta(p)}}(a)p^{\max\{0,r-s\}+1}} = 1 + vp^{\max\{s,r\}+1} = 1 + vp^{r+1} \equiv 1 \pmod{p^{r+1}}.$$

Il s'ensuit que $\mathcal{O}_{p^{r+1}}(a) = \mathcal{O}_{p^r}(a)p$. Dans tous les cas, on obtient

$$\mathcal{O}_{p^{r+1}}(a) = \mathcal{O}_{p^{\delta(p)}}(a)p^{\max\{0,(r+1)-s\}}.$$

Ce qui complète la preuve. □

Preuve du Théorème 5.1.6. Tout d'abord, par le théorème des restes chinois, on obtient

$$\mathcal{O}_n(a) = \mathcal{O}_{\prod_{i=1}^k p_i{}^{r_i}}(a) = \bigvee_{i=1}^k \mathcal{O}_{p_i{}^{r_i}}(a).$$

Si $v_2(n) = 0$, alors, par le Lemme 5.1.8, on a

$$\begin{aligned}\mathcal{O}_n(a) &= \bigvee_{i=1}^k \mathcal{O}_{p_i{}^{r_i}}(a) = \bigvee_{i=1}^k \mathcal{O}_{p_i}(a)p_i{}^{\max\{0,r_i-s_i\}} = \left(\bigvee_{i=1}^k \mathcal{O}_{p_i}(a)\right)\prod_{i=1}^k p_i{}^{\max\{0,r_i-s_i\}} \\ &= \mathcal{O}_{\prod_{i=1}^k p_i}(a)\prod_{i=1}^k p_i{}^{\max\{0,r_i-s_i\}} = \mathcal{O}_{\mathrm{rad}(n)}(a)\prod_{i=1}^k p_i{}^{\max\{0,r_i-s_i\}}.\end{aligned}$$

Si $v_2(n) = 1$, alors on peut supposer, sans perte de généralité, que $p_1 = 2$ et $r_1 = 1$. Par conséquent, par le Lemme 5.1.8, on obtient

$$\begin{aligned}\mathcal{O}_n(a) &= \mathcal{O}_2(a) \vee \left(\bigvee_{i=2}^k \mathcal{O}_{p_i}(a)p_i{}^{\max\{0,r_i-s_i\}}\right) = \left(\bigvee_{i=1}^k \mathcal{O}_{p_i}(a)\right)\prod_{i=2}^k p_i{}^{\max\{0,r_i-s_i\}} \\ &= \mathcal{O}_{\prod_{i=1}^k p_i}(a)\prod_{i=2}^k p_i{}^{\max\{0,r_i-s_i\}} = \mathcal{O}_{\mathrm{rad}(n)}(a)\prod_{i=2}^k p_i{}^{\max\{0,r_i-s_i\}}.\end{aligned}$$

De plus, comme $s_1 = v_2\left(a^{\mathcal{O}_4(a)} - 1\right) \geqslant 2$, il suit que $\max\{0, r_1 - s_1\} = 0$ et donc

$$\mathcal{O}_n(a) = \mathcal{O}_{\mathrm{rad}(n)}(a)\prod_{i=1}^k p_i{}^{\max\{0,r_i-s_i\}}.$$

Enfin, si $v_2(n) \geqslant 2$, alors on peut supposer, sans perte de généralité, que $p_1 = 2$ et $r_1 \geqslant 2$. Par conséquent, par le Lemme 5.1.8, on obtient

$$\begin{aligned}\mathcal{O}_n(a) &= \mathcal{O}_{{p_1}^2}(a){p_1}^{\max\{0,r_1-s_1\}} \vee \left(\bigvee_{i=2}^{k} \mathcal{O}_{p_i}(a){p_i}^{\max\{0,r_i-s_i\}}\right) \\ &= \left(\mathcal{O}_{{p_1}^2}(a) \vee \left(\bigvee_{i=2}^{k} \mathcal{O}_{p_i}(a)\right)\right) \prod_{i=1}^{k} {p_i}^{\max\{0,r_i-s_i\}} = \mathcal{O}_{2\,\mathrm{rad}(n)}(a) \prod_{i=1}^{k} {p_i}^{\max\{0,r_i-s_i\}}.\end{aligned}$$

□

On est maintenant prêt à déterminer la relation exacte entre $\alpha_n(a)$ et $\alpha_{\mathrm{rad}(n)}(a)$ pour tout entier a premier avec n.

Théorème 5.1.9. *Soit*

$$n = {p_1}^{r_1} \cdots {p_k}^{r_k}$$

la factorisation en nombres premiers de l'entier positif n et soit a un entier premier avec n. Soient $s_1, \ldots, s_k$ les plus grand entiers tels que

$$a^{\mathcal{O}_{{p_i}^{\delta(p_i)}(a)}} \equiv 1 \pmod{{p_i}^{s_i}},$$

i.e. $s_i = v_{p_i}\left(a^{\mathcal{O}_{{p_i}^{\delta(p_i)}(a)}} - 1\right)$ pour tout i, $1 \leqslant i \leqslant k$. Si $v_2(n) \leqslant 1$, alors on a

$$\alpha_n(a) = \frac{\alpha_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i,s_i\}}}{\mathrm{rad}(n)}}.$$

Sinon, si $v_2(n) \geqslant 2$, alors on a

$$\alpha_n(a) = \frac{\alpha_{2\,\mathrm{rad}(n)}(a)}{\alpha_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i,s_i\}}}{2\,\mathrm{rad}(n)}}.$$

Preuve. Supposons que $v_2(n) \leqslant 1$. Le Théorème 5.1.6 amène à

$$\begin{aligned}\alpha_n(a) &= \alpha_n(a) = \mathcal{O}_n\left(a^n\right) = \frac{\mathcal{O}_n\left(a\right)}{\mathcal{O}_n\left(a\right) \wedge n} = \frac{\mathcal{O}_{\mathrm{rad}(n)}\left(a\right) \prod_{i=1}^{k} {p_i}^{\max\{0,r_i-s_i\}}}{\mathcal{O}_{\mathrm{rad}(n)}\left(a\right) \prod_{i=1}^{k} {p_i}^{\max\{0,r_i-s_i\}} \wedge \prod_{i=1}^{k} {p_i}^{r_i}} \\ &= \frac{\mathcal{O}_{\mathrm{rad}(n)}\left(a\right)}{\mathcal{O}_{\mathrm{rad}(n)}\left(a\right) \wedge \prod_{i=1}^{k} {p_i}^{\min\{s_i,r_i\}}}.\end{aligned}$$

On pose

$$I = \left\{ i \in [\![1,k]\!] \;\middle|\; p_i \text{ divise } \mathcal{O}_{\mathrm{rad}(n)}(a) \right\}.$$

Alors

$$\prod_{i \in I} p_i = \mathcal{O}_{\mathrm{rad}(n)}(a) \wedge \mathrm{rad}(n)$$

et donc

$$\alpha_n(a) = \frac{\mathcal{O}_{\mathrm{rad}(n)}(a)}{\mathcal{O}_{\mathrm{rad}(n)}(a) \wedge \prod_{i\in I} {p_i}^{\min\{s_i,r_i\}}} = \frac{\frac{\mathcal{O}_{\mathrm{rad}(n)}(a)}{\mathcal{O}_{\mathrm{rad}(n)}(a)\wedge\mathrm{rad}(n)}}{\frac{\mathcal{O}_{\mathrm{rad}(n)}(a)}{\mathcal{O}_{\mathrm{rad}(n)}(a)\wedge\mathrm{rad}(n)} \wedge \frac{\prod_{i\in I} {p_i}^{\min\{s_i,r_i\}}}{\prod_{i\in I} p_i}}$$

$$= \frac{\alpha_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i\in I} {p_i}^{\min\{s_i,r_i\}}}{\prod_{i\in I} p_i}} = \frac{\alpha_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i,s_i\}}}{\mathrm{rad}(n)}}.$$

De la même manière, si $v_2(n) \geqslant 2$, alors le Théorème 5.1.6 conduit à

$$\alpha_n(a) = \frac{\mathcal{O}_{2\,\mathrm{rad}(n)}(a)}{\mathcal{O}_{2\,\mathrm{rad}(n)}(a) \wedge \prod_{i\in I} {p_i}^{\min\{r_i,s_i\}}},$$

où $I = \left\{ i \in [\![1,k]\!] \;\middle|\; p_i \text{ divise } \mathcal{O}_{\mathrm{rad}(n)}(a) \right\}$. Si $v_2\left(\mathcal{O}_{2\,\mathrm{rad}(n)}(a)\right) \geqslant 2$, alors on a

$$2\prod_{i\in I} p_i = \mathcal{O}_{2\,\mathrm{rad}(n)}(a) \wedge 2\,\mathrm{rad}(n)$$

et donc

$$\alpha_n(a) = \frac{\alpha_{2\,\mathrm{rad}(n)}(a)}{\alpha_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i\in I} {p_i}^{\min\{s_i,r_i\}}}{2\prod_{i\in I} p_i}} = \frac{\alpha_{2\,\mathrm{rad}(n)}(a)}{\alpha_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{s_i,r_i\}}}{2\,\mathrm{rad}(n)}}.$$

Sinon, si $v_2\left(\mathcal{O}_{2\,\mathrm{rad}(n)}(a)\right) \leqslant 1$, alors on a

$$\prod_{i\in I} p_i = \mathcal{O}_{2\,\mathrm{rad}(n)}(a) \wedge 2\,\mathrm{rad}(n)$$

et donc

$$\alpha_n(a) = \frac{\alpha_{2\,\mathrm{rad}(n)}(a)}{\alpha_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i\in I} {p_i}^{\min\{s_i,r_i\}}}{\prod_{i\in I} p_i}} = \frac{\alpha_{2\,\mathrm{rad}(n)}(a)}{\alpha_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{s_i,r_i\}}}{2\,\mathrm{rad}(n)}}.$$

Ce qui complète la preuve. □

5.2 La fonction arithmétique β_n

Notation. Pour tout entier $n \geqslant 1$ et tout entier a premier avec n, on note $\mathcal{PO}_n(a)$ *l'ordre multiplicatif projectif de a modulo n*, i.e. le plus petit exposant e tel que $a^e \equiv \pm 1 \pmod{n}$, à savoir

$$\mathcal{PO}_n(a) = \min\left\{ e \in \mathbb{N}^* \mid a^e \equiv \pm 1 \pmod{n} \right\}.$$

L'ordre multiplicatif projectif de a modulo n correspond aussi avec l'ordre de l'élément $\overline{\pi_n(a)}$ dans le groupe multiplicatif quotient $(\mathbb{Z}/n\mathbb{Z})^*/\{-1,1\}$. De plus, on peut remarquer que l'on a soit $\mathcal{O}_n(a) = \mathcal{PO}_n(a)$, soit $\mathcal{O}_n(a) = 2\mathcal{PO}_n(a)$.

Dans cette section, on s'intéresse à la fonction arithmétique β_n.

Définition 5.2.1. Soit $n \geqslant 1$ un entier. Soit β_n la fonction

$$\begin{array}{rccl} \beta_n : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \begin{cases} \mathcal{PO}_n(a^n) & \text{pour } a \wedge n = 1, \\ 0 & \text{sinon.} \end{cases} \end{array}$$

Tout d'abord, on peut observer que, par définition des fonctions α_n et β_n, on a

$$\alpha_n(a) = \beta_n(a) = 0$$

pour tout entier a non premier avec n et

$$\frac{\alpha_n(a)}{\beta_n(a)} \in \{1, 2\}$$

pour tout entier a premier avec n. Il n'y pas de formule générale afin de calculer $\frac{\alpha_n(a)}{\beta_n(a)}$ mais, cependant, on obtient quand même les résultats suivants.

Proposition 5.2.2. *Soient n un entier positif et a un entier premier avec n. Si $v_2(n) \leqslant 1$, alors on a*

$$\frac{\alpha_n(a)}{\beta_n(a)} = \frac{\alpha_{\mathrm{rad}(n)}(a)}{\beta_{\mathrm{rad}(n)}(a)}.$$

Si $v_2(n) \geqslant 2$, alors on a

$$\alpha_n(a) = \beta_n(a).$$

Preuve. Soit n un entier positif tel que $v_2(n) \leqslant 1$ et soit p un facteur premier impair de n tel que $v_p(n) \geqslant 2$. On va prouver que

$$\frac{\alpha_n(a)}{\beta_n(a)} = \frac{\alpha_{\frac{n}{p}}(a)}{\beta_{\frac{n}{p}}(a)}.$$

Si $\alpha_n(a) = 2\beta_n(a)$, alors

$$a^{\beta_n(a)} n \equiv -1 \pmod{n}$$

et donc

$$a^{(\beta_n(a)p)\frac{n}{p}} \equiv -1 \pmod{\frac{n}{p}}.$$

Ce qui implique que $\alpha_{\frac{n}{p}}(a) = 2\beta_{\frac{n}{p}}(a)$. Réciproquement, si $\alpha_{\frac{n}{p}}(a) = 2\beta_{\frac{n}{p}}(a)$, alors on a

$$a^{\beta_{\frac{n}{p}}(a)\frac{n}{p}} \equiv -1 \pmod{\frac{n}{p}}.$$

Puisque $v_p(n) \geqslant 2$, il suit que

$$a^{\beta_{\frac{n}{p}}(a)\frac{n}{p}} \equiv -1 \pmod{p}$$

et donc

$$a^{\beta_{\frac{n}{p}}(a)n} + 1 = 1 - \left(-a^{\beta_{\frac{n}{p}}(a)\frac{n}{p}}\right)^p = \left(1 + a^{\beta_{\frac{n}{p}}(a)\frac{n}{p}}\right) \sum_{k=0}^{p-1} \left(-a^{\beta_{\frac{n}{p}}(a)\frac{n}{p}}\right)^k \equiv 0 \pmod{n}.$$

Ceci implique que $\alpha_n(a) = 2\beta_n(a)$. Par conséquent, par induction, on obtient que

$$\frac{\alpha_n(a)}{\beta_n(a)} = \frac{\alpha_{\mathrm{rad}(n)}(a)}{\beta_{\mathrm{rad}(n)}(a)}.$$

Maintenant, soit n un entier positif tel que $v_2(n) \geqslant 2$ et soit a un entier non nul. Supposons que l'on ait $\alpha_n(a) = 2\beta_n(a)$. Comme

$$a^{\beta_n(a)n} \equiv -1 \pmod{n}$$

il suit que

$$\left(a^{\beta_n(a)\frac{n}{4}}\right)^4 \equiv -1 \pmod{4}$$

en contradiction avec

$$\left(a^{\beta_n(a)\frac{n}{4}}\right)^4 \equiv 1 \pmod{4}.$$

□

Si n est une puissance de premier, alors $\beta_n = \beta_{\mathrm{rad}(n)}$, en analogie avec la Proposition 5.1.4 pour la fonction α_n.

Proposition 5.2.3. *Soient p un nombre premier et a un entier. Alors, on a*

$$\beta_{p^k}(a) = \beta_p(a)$$

pour tout entier $k \geqslant 1$.

Preuve. Pour un entier a non premier avec n, ce résultat est évident. Supposons maintenant que a soit premier avec n. Si $p = 2$, alors par la Proposition 5.2.2, on a

$$\beta_{2^k}(a) = \alpha_{2^k}(a) = 1$$

pour tout entier $k \geqslant 1$. Si p est un nombre premier impair, alors les Propositions 5.2.2 et 5.1.4 entraînent que

$$\beta_{p^k}(a) = \frac{\alpha_{p^k}(a)}{\alpha_p(a)}\beta_p(a) = \beta_p(a)$$

pour tout entier $k \geqslant 1$. Ce qui complète la preuve. □

Comme pour la fonction α_n, il suit immédiatement que $\beta_n(a) = \beta_{\mathrm{rad}(n)}(a) = 0$ pour tout entier a non premier avec n. Enfin, on détermine la relation exact qui lie $\beta_n(a)$ à $\beta_{\mathrm{rad}(n)}(a)$ pour tout entier a premier avec n.

Théorème 5.2.4. *Soit*

$$n = {p_1}^{r_1} \cdots {p_k}^{r_k}$$

la factorisation en nombres premiers de l'entier positif n et soit a un entier premier avec n. Soient $s_1, \ldots, s_k$ les plus grands entiers tels que

$$a^{\mathcal{O}_{p_i^{\delta(p_i)}(a)}} \equiv 1 \pmod{{p_i}^{s_i}},$$

i.e. $s_i = v_{p_i}\left(a^{\mathcal{O}_{p_i^{\delta(p_i)}(a)}} - 1\right)$ pour tout i, $1 \leqslant i \leqslant k$. Si $v_2(n) \leqslant 1$, alors on a

$$\beta_n(a) = \frac{\beta_{\mathrm{rad}(n)}(a)}{\beta_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^k {p_i}^{\min\{r_i,s_i\}}}{\mathrm{rad}(n)}}.$$

Sinon, si $v_2(n) \geqslant 2$, alors on a

$$\beta_n(a) = \frac{\beta_{2\,\mathrm{rad}(n)}(a)}{\beta_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^k {p_i}^{\min\{r_i,s_i\}}}{2\,\mathrm{rad}(n)}}.$$

Preuve. Si $v_2(n) \leqslant 1$, alors le Théorème 5.1.9 et la Proposition 5.2.2 conduisent à

$$\beta_n(a) = \frac{\beta_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a)}\alpha_n(a) = \frac{\beta_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a)} \frac{\alpha_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^k {p_i}^{\min\{s_i,r_i\}}}{\mathrm{rad}(n)}} = \frac{\beta_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^k {p_i}^{\min\{s_i,r_i\}}}{\mathrm{rad}(n)}}.$$

Comme $\frac{\prod_{i=1}^k {p_i}^{\min\{s_i,r_i\}}}{\mathrm{rad}(n)}$ est impair, il s'ensuit que

$$\beta_n(a) = \frac{\beta_{\mathrm{rad}(n)}(a)}{\beta_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^k {p_i}^{\min\{r_i,s_i\}}}{\mathrm{rad}(n)}}.$$

Si $v_2(n) \geqslant 2$, alors $\beta_n(a) = \alpha_n(a)$ et $\beta_{\mathrm{rad}(n)}(a) = \alpha_{\mathrm{rad}(n)}(a)$ par la Proposition 5.2.2 , ce qui entraîne le résultat. □

Conclusion et perspectives

La structure combinatoire de triangle de Steinhaus associée à une suite binaire de longueur finie a été présentée au Chapitre 1. Même si les plus petites et plus grandes valeurs possibles du nombre de 1 dans un triangle de Steinhaus sont connues, la détermination complète de ces valeurs apparaît très ardue. De plus, le Problème de Steinhaus est apparu comme étant à la fois simple par le nombre important de suites balancées qu'il semble exister et complexe par la difficulté sous-jacente de réussir à déterminer explicitement une famille complète de ces suites. On a vu qu'il existe des familles de solutions possédant chacune une propriété supplémentaire telles que les suites pseudo-périodiques, les suites fortement balancées, les suites symétriques et antisymétriques ou encore les suites de poids moyen. Enfin, le Problème de Steinhaus étant résolu, il pourrait être intéressant de rechercher une formule asymptotique du nombre de suites balancées de longueur n pour n grand.

Les matrices et les graphes de Steinhaus sont présentés au Chapitre 2. Ce sont des objets construits à partir des triangles de Steinhaus binaires du Chapitre 1. Dans ce second chapitre, les graphes de Steinhaus pairs et impairs sont étudiés. Cette étude est basée sur un théorème dû à Dymacek qui stipule que tout graphe de Steinhaus pair est associé à une matrice de Steinhaus bisymétrique. Une nouvelle preuve de ce résultat est fournie dans ce mémoire. En fait, un résultat plus général est prouvé. On montre que les éléments de l'antidiagonale d'une matrice de Steinhaus peuvent être exprimés en fonction des degrés des sommets de son graphe de Steinhaus associé. Ce théorème fournit une première relation liant un graphe de Steinhaus à la suite des degrés de ses sommets. On rappelle enfin des résultats sur ces graphes de Steinhaus pairs et impairs qui ont été établis par Dymacek en 1979.

On rappelle, au Chapitre 3, la structure des graphes de Steinhaus réguliers qui a été conjecturée en 1979 par Dymacek. Peu de choses sont connues sur le cas pair mais on prouve tout de même que, pour tout entier $m \geqslant 1$, la suite binaire $s = (110)^m$ engendre un graphe de Steinhaus à $3m + 1$ sommets et régulier de degré $2m$. La conjecture paire annonce que cette famille de graphes de Steinhaus non-triviaux et les graphes totalement disconnexes constituent les seuls graphes de Steinhaus réguliers de degré pair. Dans la suite de ce chapitre, on s'intéresse à la conjecture dans le cas impair qui stipule que K_2, le graphe complet à deux sommets, est l'unique graphe de Steinhaus régulier de degré impair. On reformule un résultat de Dymacek et on prouve alors que si G est un graphe de Steinhaus à $2n$ sommets et régulier de degré impair k, alors $k = n$ et $G \backslash \{V_1, V_{2n}\}$ est un graphe de Steinhaus régulier de degré pair $n - 1$ dont la matrice de Steinhaus associée est multisymétrique. De plus, on prouve que les

matrices de Steinhaus multisymétriques de taille n dont le graphe associé est régulier modulo 4 ne dépendent que de $\lceil \frac{n}{24} \rceil$ paramètres pour n pair et de $\lceil \frac{n}{30} \rceil$ paramètres pour n impair. Ce résultat permet de vérifier la conjecture impaire jusqu'à 1500 sommets, améliorant ainsi d'un facteur 12 la borne précédente connue (117 sommets). Enfin, on conjecture que, pour tout entier n, le graphe totalement disconnexe à n sommets est le seul graphe de Steinhaus régulier modulo 4 dont la matrice de Steinhaus associée est multisymétrique. Cette conjecture entraîne celle de Dymacek dans le cas impair.

La construction des triangles de Steinhaus a été généralisée à tout groupe cyclique d'ordre n par Molluzzo en 1978 [19]. Il pose alors la généralisation du Problème de Steinhaus qui consiste à savoir s'il existe une suite balancée pour toutes les tailles m admissibles. Dans un premier temps, on montre qu'il existe des contre-exemples au Problème de Molluzzo, c'est-à-dire qu'il y a, dans certains groupes cycliques, des longueurs pour lesquelles il n'existe pas de suite balancée. On conjecture ensuite que le Problème de Molluzzo est vrai pour tous les groupes cycliques d'ordre une puissance de premier. On s'intéresse à ce Problème de Molluzzo tout au long du Chapitre 4. Tout d'abord, on détermine les tailles possibles pour une suite balancée et on établit un théorème de projection des suites balancées dans les groupes cycliques. On continue par l'étude des suites à progression arithmétique et de leur triangle de Steinhaus associé. On se pose alors la question de savoir quand est-ce qu'une suite à progression arithmétique est balancée dans $\mathbb{Z}/n\mathbb{Z}$ avec n impair. On montre qu'il faut déjà que la raison d soit inversible, et que si c'est le cas, il suffit que la longueur m soit congrue à 0 ou $-1 \pmod{\alpha(n)n}$, où $\alpha(n)$ est l'ordre multiplicatif de 2^n modulo n. De plus, en considérant la propriété supplémentaire d'antisymétrie, on prouve que, pour tout élément d inversible dans $\mathbb{Z}/n\mathbb{Z}$, les suites arithmétiques $PA(2^{-1}d, d, k\beta(n)n)$ et $PA(d, d, k\beta(n)n - 1)$ sont balancées pour tout $k \geqslant 1$ et où $\beta(n)$ est l'ordre multiplicatif projectif de 2^n modulo n. Les suites arithmétiques permettent donc de répondre complètement et positivement au Problème de Molluzzo dans le cas des groupes cycliques d'ordre une puissance de 3 et, plus généralement, de montrer qu'il existe une infinité de suites balancées dans tout groupe cyclique d'ordre n impair. A la fin de Chapitre 4, on prouve également que, contrairement aux groupes cycliques d'ordre impair, presqu'aucune suite arithmétique n'est balancée dans les groupes cycliques d'ordre pair. Enfin, au cours de cette analyse des suites arithmétiques, il a été nécessaire d'étudier l'ordre multiplicatif de a^n modulo n pour tout entier a premier avec n. Ceci a conduit à la construction des fonctions α_n et β_n dont une description détaillée est fournie au Chapitre 5. Pour terminer, il est possible de s'apercevoir, de manière expérimentale, que la considération de suites arithmétiques entrelacées ou suites arithmétiques multidimensionnelles devrait permettre de construire un plus grand nombre de suites balancées. Cela semble être un objectif atteignable dans les mois à venir.

Bibliographie

[1] Maxime Augier and Shalom Eliahou. Parity-regular Steinhaus graphs. *Mathematics of Computation*, 77 :1831–1839, 2008.

[2] Craig Bailey and Wayne M. Dymacek. Regular Steinhaus graphs. In *Proc. 19th southeast. Conf. Combinatorics, Graph Theory and Computing, Baton Rouge 1988, Congr. Numerantium 66*, pages 45–47, 1988.

[3] Gerard J. Chang. Binary triangles. *Bull. Inst. Math., Acad. Sin.*, 11 :209–225, 1983.

[4] Gerard J. Chang, Bhaskar DasGupta, Wayne M. Dymacek, Martin Fürer, Matthew Koerlin, Yueh-Shin Lee, and Tom Whaley. Characterizations of bipartite Steinhaus graphs. *Discrete Mathematics*, 199(1–3) :11–25, 1999.

[5] Jonathan Chappelon. On a problem of Molluzzo concerning Steinhaus triangles in finite cyclic groups. *INTEGERS : Electronic Journal of Combinatorial Number Theory*, 8(1) :# A37, 2008.

[6] Jonathan Chappelon. Regular Steinhaus graphs of odd degree. *http ://arxiv.org/abs/0806.2779*, 2008.

[7] Reinhard Diestel. *Graph Theory, Third Edition*. Springer, 2006.

[8] Wayne M. Dymacek. Steinhaus graphs. Proc. 10th southeast. Conf. Combinatorics, graph theory and computing, Boca Raton 1979, Vol. I, Congr. Numerantium 23, 399-412, 1979.

[9] Wayne M. Dymacek. Bipartite Steinhaus graphs. *Discrete Mathematics*, 59(1–2) :9–20, 1986.

[10] Wayne M. Dymacek, Matthew Koerlin, and Tom Whaley. A survey of Steinhaus graphs. In *Proc. 8th Quadrennial International Conf. on Graph Theory, Combinatorics, Algorithms and Application, Kalamazoo, Mich. 1996*, volume I, pages 313–323, 1996.

[11] Wayne M. Dymacek, Jean-Guy Speton, and Tom Whalley. Planar Steinhaus graphs. In *Congressus Numerantium 144*, pages 193–206, 2000.

[12] Wayne M. Dymacek and Tom Whaley. Generating strings for bipartite Steinhaus graphs. *Discrete Mathematics*, 141 :95–107, 1995.

[13] S. Eliahou, J.M. Marín, and M.P. Revuelta. Zero-sum balanced binary sequences. *INTEGERS : Electronic Journal of Combinatorial Number Theory*, 7(2) :# A11, 2007.

[14] Shalom Eliahou and Delphine Hachez. On a problem of Steinhaus concerning binary sequences. *Exp. Math.*, 13(2) :215–229, 2004.

[15] Shalom Eliahou and Delphine Hachez. On symmetric and antisymmetric balanced binary sequences. *INTEGERS : Electronic Journal of Combinatorial Number Theory*, 5 :# A06, 2005.

[16] T. Goka. An operator on binary sequences. *SIAM Rev.*, 12 :264–266, 1970.

[17] Heiko Harborth. Solution of Steinhaus's problem with plus and minus signs. *J. Comb. Theory, Ser. A*, 12 :253–259, 1972.

[18] John Milnor. An experiment in mental generation of random numbers. Technical report, Rand Rep. RM-936, Rand Corporation, Santa Monica, California, 1952.

[19] John C. Molluzzo. Steinhaus graphs. Theor. Appl. Graphs, Proc. Kalamazoo 1976, Lect. Notes Math. 642, 394-402, 1978.

[20] Melvyn B. Nathanson. Derivatives of binary sequences. *SIAM J. appl. Math.*, 21 :407–412, 1971.

[21] Melvyn B. Nathanson. Integrals of binary sequences. *SIAM J. Appl. Math.*, 23 :84–86, 1972.

[22] Melvyn B. Nathanson. *Elementary Methods in Number Theory*, pages 92–93. New York, Springer edition, 2000.

[23] Hugo Steinhaus. *One hundred problems in elementary mathematics*, pages 47–48. Pergamon, Elinsford, N.Y., 1963.

Annexe A

Suites balancées dans les groupes cycliques d'ordre 3, 5 et 7

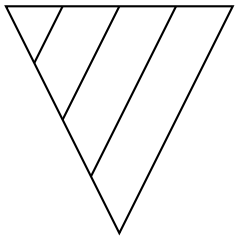
Dans cette annexe, on répond positivement et complètement au Problème de Molluzzo dans les groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ d'ordre $n = 3$, 5 et 7. Ces solutions sont obtenues de manière expérimentale et leurs preuves, souvent longues et répétitives, ne seront pas données ici. La plupart du temps, ces preuves consistent en un découpage astucieux d'un triangle de Steinhaus en blocs élémentaires dans lesquels on contrôle la multiplicité de chaque élément du groupe $\mathbb{Z}/n\mathbb{Z}$ concerné. Les programmes, réalisés en Mathematica, qui ont servi à mettre en évidence ces suites balancées seront prochainement disponibles à l'adresse : `http://www-lmpa.univ-littoral.fr/~chappelo`.

A.1 Suites fortement balancées

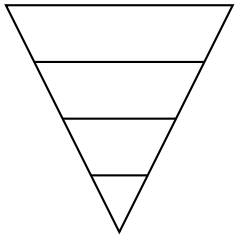
On a vu, au Chapitre 1, que les suites binaires fortement balancées permettent de répondre au Problème de Steinhaus dans $\mathbb{Z}/2\mathbb{Z}$. Dans cette section, on définit deux types différents de suites fortement balancées qui permettent d'obtenir une réponse complète au Problème de Molluzzo dans $\mathbb{Z}/3\mathbb{Z}$ et une réponse partielle dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$. La réponse dans $\mathbb{Z}/3\mathbb{Z}$ coïncide avec les suites arithmétiques balancées qui sont étudiées en détail au Chapitre 4. Les réponses partielles obtenues dans les groupes $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$ sont complétées plus loin par d'autres constructions.

Définition A.1.1. Soit $S = (a_1, \ldots, a_m)$ une suite de longueur $m \geqslant 1$ dans $\mathbb{Z}/n\mathbb{Z}$ avec n impair. Alors, la suite S est dite

– *fortement balancée à droite*, si la sous-suite initiale $S[m - kn]$ de longueur $m - kn$ est balancée pour tout k, $0 \leqslant k \leqslant \frac{m}{n}$.



– *à dérivation fortement balancée*, si la suite dérivée $\partial^{kn}S$ de longueur $m-kn$ est balancée pour tout k, $0 \leqslant k \leqslant \frac{m}{n}$.



On détermine, dans la suite de cette section, l'ensemble des suites fortement balancées à droite et l'ensemble des suites à dérivation fortement balancée dans chacun des groupes $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.

A.1.1 Suites fortement balancées à droite

Notation. Soit $n \in \{3, 5, 7\}$. Pour tout entier $m \geqslant 0$, on note $FBD_n(m)$ l'ensemble des suites fortement balancées à droite et de longueur m dans $\mathbb{Z}/n\mathbb{Z}$. Lorsque cet ensemble est fini, on note $fbd_n(m)$ son cardinal.

Le théorème suivant détermine explicitement, pour tout entier $m \equiv 0$ ou $2 \pmod 3$, l'ensemble des suites fortement balancées à droite et de longueur m dans $\mathbb{Z}/3\mathbb{Z}$.

Théorème A.1.2. *A multiplication par un inversible de $\mathbb{Z}/3\mathbb{Z}$ près, on a*
- pour les longueurs $m \equiv 0 \pmod 3$:

$$\begin{aligned}
FBD_3(0) &= \{\emptyset\}, \\
FBD_3(3) &= \{(102)\}, \\
FBD_3(6) &= \{(102022), (102100), (102101), (102102)\}, \\
FBD_3(9) &= \{(102100210), (102101020), (102102102)\}, \\
FBD_3(12) &= \{(102100210202), (102101020002), (102101020102), (102102102100), \\
&\quad (102102102101), (102102102102)\}, \\
FBD_3(6k+3) &= \left\{(102)^{2k+1}\right\} \text{ pour } k \geqslant 2, \\
FBD_3(6k) &= \left\{(102)^{2k-1}\cdot(100), (102)^{2k-1}\cdot(101), (102)^{2k}\right\} \text{ pour } k \geqslant 3,
\end{aligned}$$

- *pour les longueurs* $m \equiv 2 \pmod 3$ *:*

$$\begin{aligned}
FBD_3(2) &= \{(12)\}, \\
FBD_3(5) &= \{(12012), (12110)\}, \\
FBD_3(8) &= \{(12012012), (12110022), (12110121), (12110202)\}, \\
FBD_3(11) &= \{(12012012012), (12012012221), (12110022110), (12110022201), \\
&\quad (12110121010), (12110202210)\}, \\
FBD_3(14) &= \{(12012012012012), (12110022110010), (12110022110022), (12110022201200), \\
&\quad (12110121010002), (12110121010121), (12110202210202)\}, \\
FBD_3(17) &= \{(12012012012012012), (12110022110022110), (12110121010121010), \\
&\quad (12110202210202000), (12110202210202210)\}, \\
FBD_3(3k+2) &= \{s_1[3k+2], s_2[3k+2], s_3[3k+2], s_4[3k+2]\} \text{ pour } k \geqslant 6, \text{ où } s_1, s_2, s_3 \\
&\quad \text{et } s_4 \text{ est une des suites suivantes} \\
&\quad\quad s_1 = (12) \cdot (012)^\infty \\
&\quad\quad s_2 = (12) \cdot (110022)^\infty \\
&\quad\quad s_3 = (12110) \cdot (121010)^\infty \\
&\quad\quad s_4 = (12110) \cdot (202210)^\infty
\end{aligned}$$

Théorème A.1.3. *La fonction génératrice* $f_3(t) = \sum_{m\in\mathbb{N}} fbd_3(m)t^m$ *du nombre de suites fortement balancées à droite dans* $\mathbb{Z}/3\mathbb{Z}$ *est donné par l'expression*

$$\begin{aligned}
f_3(t) &= 1 + 2\left(t^3 + 4t^6 + 3t^9 + 6t^{12} + \tfrac{(1+3t^3)t^{15}}{1-t^6}\right) \\
&\quad +2\left(t^2 + 2t^5 + 4t^8 + 6t^{11} + 7t^{14} + 5t^{17} + \tfrac{4t^{20}}{1-t^3}\right).
\end{aligned}$$

Le Problème de Molluzzo est donc entièrement résolu dans $\mathbb{Z}/3\mathbb{Z}$ grâce aux suites fortement balancées à droite. Par contre, dans les groupes $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$, il n'y a qu'un nombre fini de suites fortement balancées à droite.

Théorème A.1.4. *La fonction génératrice* $f_5(t) = \sum_{m\in\mathbb{N}} fbd_5(m)t^m$ *du nombre de suites fortement balancées à droite dans* $\mathbb{Z}/5\mathbb{Z}$ *est donné par l'expression*

$$\begin{aligned}
f_5(t) &= 1 + 4\left(3t^5 + 8t^{10} + 8t^{15} + 4t^{20} + t^{25}\right) \\
&\quad +4\left(t^4 + 6t^9 + 6t^{14} + 2t^{19} + t^{24}\right).
\end{aligned}$$

Théorème A.1.5. *La fonction génératrice* $f_7(t) = \sum_{m\in\mathbb{N}} fbd_7(m)t^m$ *du nombre de suites fortement balancées à droite dans* $\mathbb{Z}/7\mathbb{Z}$ *est donné par l'expression*

$$\begin{aligned}
f_7(t) &= 1 + 6\left(13t^7 + 77t^{14} + 105t^{21} + 57t^{28} + 20t^{35} + t^{42}\right) \\
&\quad +6\left(2t^6 + 12t^{13} + 18t^{20} + 11t^{27} + 2t^{34}\right).
\end{aligned}$$

A.1.2 Suites à dérivation fortement balancée

Notation. Soit $n \in \{3, 5, 7\}$. Pour tout entier $m \geqslant 0$, on note $DFB_n(m)$ l'ensemble des suites à dérivation fortement balancée et de longueur m dans $\mathbb{Z}/n\mathbb{Z}$. Lorsque cet ensemble est fini, on note $dfb_n(m)$ son cardinal.

Dans $\mathbb{Z}/3\mathbb{Z}$, le nombre de suites à dérivation fortement balancée de longueur $m \leqslant 50$, avec $m \equiv 0$ ou $2 \pmod 3$, est donné par le tableau suivant.

$\mathbf{m}$	$\mathbf{dfb_3(m)}$	$\mathbf{m}$	$\mathbf{dfb_3(m)}$
0	1	2	2
3	2	5	4
6	10	8	18
9	10	11	18
12	34	14	56
15	56	17	78
18	128	20	168
21	102	23	244
24	302	26	484
27	252	29	462
30	750	32	1270
33	784	35	1612
36	2074	38	3908
39	1814	41	4886
42	5688	44	11110
45	5106	47	9920
48	16582	50	31056

Ces résultats suggèrent que le nombre de suites à dérivation fortement balancée et de longueur $m \equiv 0, 2 \pmod 3$ explose avec m. On continue par l'étude de ces suites dans les groupes $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.

Le théorème suivant détermine explicitement, pour tout entier $m \equiv 0$ ou $4 \pmod 5$, l'ensemble des suites à dérivation fortement balancée et de longueur m dans $\mathbb{Z}/5\mathbb{Z}$.

Théorème A.1.6. *A multiplication par un inversible de $\mathbb{Z}/5\mathbb{Z}$ près, on a*
- pour les longueurs $m \equiv 0 \pmod 5$:

$$\begin{aligned}
DFB_5(30k+15) &= \left\{(023311104442230)^{2k+1}\right\} \text{ pour } k \geqslant 2,\\
DFB_5(30k) &= \left\{(023311104442230)^{2k}, (123103042022411441330310204234)^k,\right.\\
&\quad (132031344243001400213112420324)^k,\\
&\quad (100342443130231423024211312004)^k,\\
&\quad \left.(114220240301321432402013033144)^k\right\} \text{ pour } k \geqslant 3,\\
DFB_5(15k+5) &= \left\{(11044)\cdot(422300233111044)^k\right\} \text{ pour } k \geqslant 5,\\
DFB_5(15k+10) &= \left\{(4223002331)\cdot(110444223002331)^k\right\} \text{ pour } k \geqslant 5,
\end{aligned}$$

- pour les longueurs $m \equiv 4 \pmod 5$:

$$DFB_5(5k+4) = \emptyset \quad \text{pour} \quad k \geqslant 2.$$

Théorème A.1.7. *La fonction génératrice $g_5(t) = \sum_{m\in\mathbb{N}} dfb_5(m)t^m$ du nombre de suites à dérivation fortement balancée dans $\mathbb{Z}/5\mathbb{Z}$ est donné par l'expression*

$$\begin{aligned} g_5(t) &= 1 + 4\,(3t^5 + 12t^{10} + 33t^{15} + 20t^{20} + 15t^{25} + 19t^{30} + 9t^{35} + 7t^{40} + t^{45} + 4t^{50} + t^{55} + \\ &\quad +5t^{60} + 2t^{65} + 3t^{70} + \frac{(1 + t^5 + t^{10} + 5t^{15} + t^{20} + t^{25})t^{75}}{1 - t^{30}}\Big) + 4t^4 \end{aligned}$$

On a donc des suites balancées dans $\mathbb{Z}/5\mathbb{Z}$ pour toutes les longueurs $m \equiv 0 \pmod 5$. De plus, pour tout entier $k \geqslant 1$, la suite $S = (023311104442230)^k$ est une suite balancée de longueur $15k$ et qui contient $3k$ fois chaque élément du groupe $\mathbb{Z}/5\mathbb{Z}$. On en déduit que sa suite dérivée est également balancée et donc la suite

$$(201422143314030) \cdot (020142214331403)^k$$

est une suite balancée de longueur $15k + 14$ pour tout entier $k \geqslant 0$. Les suites à dérivation fortement balancée ne permettent donc pas de répondre complètement au Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$. En effet, il manque encore la preuve qu'il existe des suites balancées pour toutes les longueurs $m \equiv 4$ et $9 \pmod{15}$.

Le théorème suivant détermine explicitement, pour tout entier $m \equiv 0$ ou $6 \pmod 7$, l'ensemble des suites à dérivation fortement balancée et de longueur m dans $\mathbb{Z}/7\mathbb{Z}$.

Théorème A.1.8. *A multiplication par un inversible de $\mathbb{Z}/7\mathbb{Z}$ près, on a*
- pour les longueurs $m \equiv 0 \pmod 7$:

$$\begin{aligned} DFB_7(42k+21) &= \left\{(0433566622055111244 30)^{2k+1}\right\} \text{ pour } k \geqslant 3, \\ DFB_7(42k) &= \left\{(0433566622055111244 30)^{2k},\right. \\ &\quad (13426505311460203352165244050136642021 5346)^k, \\ &\quad (22510414402306364261256153141045033630 6255)^k, \\ &\quad (31601323563215455100340062232654124546 0164)^k, \\ &\quad (35426023111445423354343244532336664501 5324)^k, \\ &\quad (40062232654124546016431601323563215455 1003)^k, \\ &\quad (56153141045033630625522510414402306364 2612)^k, \\ &\quad \left.(65244050136642021534613426505311460203352 1)^k\right\} \text{ pour } k \geqslant 3, \\ DFB_7(21k+7) &= \left\{(6220551) \cdot (1124430043356662205 51)^k\right\} \text{ pour } k \geqslant 5, \\ DFB_7(21k+14) &= \left\{(11244300433566) \cdot (6220551112443004335 66)^k\right\} \text{ pour } k \geqslant 5, \end{aligned}$$

- pour les longueurs $m \equiv 6 \pmod 7$:

$$DFB_7(7k+6) = \emptyset \quad \text{pour} \quad k \geqslant 9.$$

Théorème A.1.9. *La fonction génératrice $g_7(t) = \sum_{m\in\mathbb{N}} dfb_7(m)t^m$ du nombre de suites à dérivation fortement balancée dans $\mathbb{Z}/7\mathbb{Z}$ est donné par l'expression*

$$\begin{aligned} g_7(t) &= 1 + 6\,(13t^7 + 92t^{14} + 136t^{21} + 112t^{28} + 47t^{35} + 33t^{42} + 4t^{49} + 5t^{56} + 2t^{63} + t^{70} + t^{77} + \\ &\quad +8t^{84} + t^{91} + t^{98} + t^{105} + 2t^{112} + \frac{(1 + 8t^7 + t^{14} + t^{21} + t^{28} + t^{35})t^{119}}{1 - t^{42}}\Big) + \\ &\quad +6(2t^6 + 23t^{13} + 45t^{20} + 46t^{27} + 54t^{34} + 12t^{41} + 13t^{48} + 5t^{55} + 3t^{62}). \end{aligned}$$

On a donc des suites balancées dans $\mathbb{Z}/7\mathbb{Z}$ pour toutes les longueurs $m \equiv 0 \pmod 7$. De plus, pour tout entier $k \geqslant 1$, la suite $S = (043356662205511124430)^k$ est une suite balancée de longueur $21k$ et qui contient $3k$ fois chaque élément du groupe $\mathbb{Z}/7\mathbb{Z}$. On en déduit que sa suite dérivée est également balancée et la suite

$$(40614551425362236103) \cdot (040614551425362236103)^k$$

est une suite balancée de longueur $21k + 20$ pour tout entier $k \geqslant 0$. Les suites à dérivation fortement balancée ne permettent donc pas de répondre complètement au Problème de Molluzzo dans $\mathbb{Z}/7\mathbb{Z}$. En effet, il manque encore la preuve qu'il existe des suites balancées pour toutes les longueurs $m \equiv 6$ et $13 \pmod{21}$.

A.2 Solutions du Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$

Dans cette section, on donne deux solutions de nature différente au Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$.

A.2.1 Suites balancées antisymétriques et périodiques

On répertorie ici toutes les suites balancées antisymétriques et périodiques de période 10 dans $\mathbb{Z}/5\mathbb{Z}$.

Théorème A.2.1. *Soit $k \geqslant 0$ un entier. Alors, il existe des suites balancées antisymétriques et périodiques de période 10 dans $\mathbb{Z}/5\mathbb{Z}$*

- *de longueur* $10k$ *:* $\begin{cases} (0112233440)^k, \\ (1133002244)^k, \\ (1240230134)^k, \\ (1302413024)^k. \end{cases}$
- *de longueur* $10k+5$ *:* $\begin{cases} (11044) \cdot (0203011044)^k, \\ (11044) \cdot (2302311044)^k. \end{cases}$
- *de longueur* $10k+4$ *:* $(1144) \cdot (2200331144)^k$.
- *de longueur* $10k+9$ *:* $\begin{cases} (123401234) \cdot (0123401234)^k, \\ (143302214) \cdot (0143302214)^k. \end{cases}$

On a ainsi répondu positivement et complètement au Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$.

A.2.2 Suites arithmétiques et primitives

Comme $\beta(5) = 2$, on sait, par le Théorème 4.5.6, que les suites arithmétiques et antisymétriques $PA(2^{-1}d, d, 10k)$ et $PA(d, d, 10k-1)$, de raison inversible d, sont balancées

pour tout entier $k \geqslant 1$. On connaît donc des suites balancées pour la moitié des longueurs admissibles. Pour les longueurs restantes, c'est à dire $m \equiv 4$ et $5 \pmod{10}$, on recherche des suites balancées parmi les primitives des suites arithmétiques.

$\mathbf{m = 10k + 4}$

Parmi les primitives des suites arithmétiques de longueur $10k + 3$, il existe une suite balancée qui est

$$P_2(PA(4, 1, 10k + 3)) = (2233) \cdot (4400112233)^k,$$

pour tout entier $k \geqslant 0$.

$\mathbf{m = 10k + 5}$

Parmi les primitives secondes des suites arithmétiques de longueur $10k + 3$, il existe une suite balancée qui est

$$P_3(P_1(PA(4, 1, 10k + 3))) = (33022) \cdot (1401433022)^k,$$

pour tout entier $k \geqslant 0$.

On obtient ainsi une seconde solution au Problème de Molluzzo dans $\mathbb{Z}/5\mathbb{Z}$.

A.3 Solution du Problème de Molluzzo dans $\mathbb{Z}/7\mathbb{Z}$

Dans cette section, on répond positivement et complètement au Problème de Molluzzo dans $\mathbb{Z}/7\mathbb{Z}$ en combinant des résultats obtenus par deux méthodes distinctes.

A.3.1 Suites arithmétiques et primitives

Comme $\beta(7) = \alpha(7) = 3$, on sait, par le Théorème 4.5.6, que les suites arithmétiques de raison inversible d sont balancées pour toute longueur $m \equiv 0$ ou $20 \pmod{21}$. Comme précédemment, afin de compléter les longueurs manquantes, on recherche des suites balancées parmi les suites primitives des suites arithmétiques.

$\mathbf{m = 42k + 7}$

Parmi les primitives secondes des suites arithmétiques de longueur $42k + 5$, il existe une suite balancée qui est

$$P_6(P_1(PA(5, 1, 42k + 5))) = (6220551) \cdot (34106346220551)^{3k},$$

pour tout entier $k \geqslant 0$.

m = 42k + 14

Parmi les primitives troisièmes des suites arithmétiques de longueur $42k + 11$, il existe deux suites balancées qui sont

$$P_6(P_2(P_6(PA(1, 1, 42k + 11)))) = (63145340521260)^{3k+1},$$
$$P_0(P_1(P_0(PA(3, 1, 42k + 11)))) = (01565203423641)^{3k+1},$$

pour tout entier $k \geqslant 0$.

m = 42k + 28

Parmi les primitives secondes des suites arithmétiques de longueur $42k + 26$, il existe 14 suites balancées qui sont

$$P_0(P_4(PA(4, 1, 42k + 26))) = (04326025531146)^{3k+2},$$
$$P_1(P_4(PA(4, 1, 42k + 26))) = (13410634622055)^{3k+2},$$
$$P_2(P_4(PA(4, 1, 42k + 26))) = (22501543013664)^{3k+2},$$
$$P_3(P_4(PA(4, 1, 42k + 26))) = (31662452104503)^{3k+2},$$
$$P_4(P_4(PA(4, 1, 42k + 26))) = (40053361265412)^{3k+2},$$
$$P_5(P_4(PA(4, 1, 42k + 26))) = (56144200356321)^{3k+2},$$
$$P_6(P_4(PA(4, 1, 42k + 26))) = (65235116440230)^{3k+2},$$
$$P_0(P_4(PA(6, 1, 42k + 26))) = (04503316624521)^{3k+2},$$
$$P_1(P_4(PA(6, 1, 42k + 26))) = (13664225015430)^{3k+2},$$
$$P_2(P_4(PA(6, 1, 42k + 26))) = (22055134106346)^{3k+2},$$
$$P_3(P_4(PA(6, 1, 42k + 26))) = (31146043260255)^{3k+2},$$
$$P_4(P_4(PA(6, 1, 42k + 26))) = (40230652351164)^{3k+2},$$
$$P_5(P_4(PA(6, 1, 42k + 26))) = (56321561442003)^{3k+2},$$
$$P_6(P_4(PA(6, 1, 42k + 26))) = (65412400533612)^{3k+2},$$

pour tout entier $k \geqslant 0$.

m = 42k + 35

Parmi les primitives secondes des suites arithmétiques de longueur $42k + 33$, il existe deux suites balancées qui sont

$$P_0(P_1(PA(4, 1, 42k + 33))) = (0120466) \cdot (51433520120466)^{3k+2},$$
$$P_1(P_2(PA(6, 1, 42k + 33))) = (1130560) \cdot (52443621130560)^{3k+2},$$

pour tout entier $k \geqslant 0$.

m = 42k + 6

Parmi les primitives troisièmes des suites arithmétiques de longueur $42k+3$, il existe une suite balancée qui est

$$P_2(P_5(P_2(PA(6,1,42k+3)))) = (231645)\cdot(40152603231645)^{3k},$$

pour tout entier $k \geqslant 0$.

m = 42k + 13

Parmi les primitives des suites arithmétiques de longueur $42k+3$, il existe deux suites balancées qui sont

$$P_5(PA(4,1,42k+12)) = (5660011223344)\cdot(55660011223344)^{3k},$$
$$P_3(PA(6,1,42k+12)) = (3344556600112)\cdot(23344556600112)^{3k},$$

pour tout entier $k \geqslant 0$.

m = 42k + 27

Parmi les primitives des suites arithmétiques de longueur $42k+26$, il existe deux suites balancées qui sont

$$P_4(PA(4,1,42k+26)) = (4051620314253)\cdot(64051620314253)^{3k+1},$$
$$P_4(PA(6,1,42k+26)) = (4253640516203)\cdot(14253640516203)^{3k+1},$$

pour tout entier $k \geqslant 0$.

m = 42k + 34

Il n'y a pas de primitive de suites arithmétiques qui fournisse une famille de suites balancées de longueur $m = 42k+34$.

A.3.2 Suites arithmétiques entrelacées

Dans cette sous-section, on met en évidence des suites balancées qui sont des suites arithmétiques entrelacées ou, plus précisément, l'entrelacement de trois suites arithmétiques, c'est-à-dire, des suites de la forme

$$(a_1, a_2, a_3, a_1+d_1, a_2+d_2, a_3+d_3, a_1+2d_1, a_2+2d_2, a_3+2d_3, \ldots\ldots)$$

dans $\mathbb{Z}/7\mathbb{Z}$.

$\mathbf{m = 21k + 7}$

Il y a une suite arithmétique entrelacée de longueur $m = 21k + 7$ et balancée

$$(2330445) \cdot (553661006114222330445)^k,$$

pour tout entier $k \geqslant 0$.

$\mathbf{m = 21k + 14}$

Il y a une suite arithmétique entrelacée de longueur $m = 21k + 14$ et balancée

$$(55366100611422) \cdot (2330445553661006114 22)^k,$$

pour tout entier $k \geqslant 0$.

$\mathbf{m = 21k}$

Il y a 60 suites arithmétiques entrelacées de longueur $m = 21k$ et balancées dont

$$(0611422233044555366 10)^k,$$

pour tout entier $k \geqslant 0$.

$\mathbf{m = 21k + 6}$

Il n'y a pas de suite arithmétique entrelacée et balancée pour toute longueur $m = 21k+6$.

$\mathbf{m = 21k + 13}$

Il y a une suite arithmétique entrelacée de longueur $m = 21k + 13$ et balancée

$$(1264410633156) \cdot (302525041264410633156)^k,$$

pour tout entier $k \geqslant 0$.

$\mathbf{m = 21k + 20}$

Il y a 60 suites arithmétiques entrelacées de longueur $m = 21k$ et balancées dont

$$(66555044233422611100) \cdot (3665550442334226 11100)^k,$$

pour tout entier $k \geqslant 0$.

En combinant les résultats obtenus dans cette section, on a donc prouvé l'existence de suites balancées pour toutes les longueurs admissibles $m \equiv 0$ et $6 \pmod 7$. Ainsi, le Problème de Molluzzo est entièrement résolu dans $\mathbb{Z}/7\mathbb{Z}$.

Appendix B

English summary

Regular Steinhaus graphs and Steinhaus triangles in finite cyclic groups

B.1 Binary Steinhaus triangles

B.1.1 The Steinhaus Problem

First, we define an operation of derivation on finite binary sequences.

Definition B.1.1. Let $S = (a_1, \ldots, a_n)$ be a finite sequence of length $n \geqslant 2$ in $\mathbb{Z}/2\mathbb{Z}$. The *derived sequence* of S is the sequence ∂S defined by

$$\partial S = (a_1 + a_2, \ldots, a_{n-1} + a_n),$$

where $+$ is the sum in $\mathbb{Z}/2\mathbb{Z}$. It is a sequence of length $n-1$ in $\mathbb{Z}/2\mathbb{Z}$. By convention, $\partial S = \emptyset$ if $n \leqslant 1$, where $\emptyset$ stands for the empty sequence of length 0. Iterating the derivation process, we denote by $\partial^i S$ the ith derived sequence of S, defined recursively as usual by $\partial^0 S = S$ and $\partial^i S = \partial(\partial^{i-1} S)$ for $i \geqslant 1$.

We also define an operation of integration.

Proposition B.1.2. *Let S be a finite sequence of length $n \geqslant 0$ in $\mathbb{Z}/2\mathbb{Z}$. Then, there exist two complementary sequences T of length $n+1$ such that $\partial T = S$.*

Definition B.1.3. Let S be a finite sequence of length $n \geqslant 0$ in $\mathbb{Z}/2\mathbb{Z}$. Then, the two complementary sequences T of length $n+1$ such that $\partial T = S$ are called *primitive sequences* of S and we denote by $P_i(S)$ the primitive sequence of S whose first element is equal to i, for $i \in \{0, 1\}$.

Then, we obtain a fundamental theorem of calculus on finite sequences in $\mathbb{Z}/2\mathbb{Z}$.

Proposition B.1.4 (Fundamental theorem of calculus)**.** *Let $S = (a_1, \ldots, a_n)$ be a sequence of length $n \geqslant 1$ in $\mathbb{Z}/2\mathbb{Z}$ and $i \in \{0, 1\}$. Then,*

$$\begin{aligned} \partial P_i(S) &= S, \\ P_i(\partial S) &= S + (i + a_1)_{j=1}^{n}, \end{aligned}$$

where $(i + a_1)_{j=1}^{n}$ is the constant sequence equal to $i + a_1$ and of length n.

Using the derivation process, we define the Steinhaus triangle associated to a finite binary sequence.

Definition B.1.5. The *Steinhaus triangle* of S is the collection $\Delta S = \{S, \partial S, \ldots, \partial^{n-1} S\}$ of iterated derived sequences of S. A Steinhaus triangle of *order* n is a Steinhaus triangle associated to a finite sequence of length n.

We are interested in the binary sequences whose Steinhaus triangle contains as many 0's as 1's.

Definition B.1.6. A finite sequence S in $\mathbb{Z}/2\mathbb{Z}$ is said to be *balanced* if its Steinhaus triangle ΔS contains as many 0's as 1's.

Since a binary Steinhaus triangle of order n contains $\binom{n+1}{2}$ elements of $\mathbb{Z}/2\mathbb{Z}$, counted with multiplicity, the length of a balanced sequence must be an integer n such that $\binom{n+1}{2}$ is even, that is, $n \equiv 0$ or $3 \pmod 4$. In 1963, Hugo Steinhaus posed the following problem.

Problem B.1.7. *Does there exist a balanced binary sequence of length n, for every $n \equiv 0$ or $3 \pmod 4$?*

B.1.2 The number of 1's in a Steinhaus triangle

Notation. Let $S = (a_1, \ldots, a_n)$ be a sequence of length $n \geqslant 1$ in $\mathbb{Z}/2\mathbb{Z}$ and $\Delta S = (a_{i,j})$ its Steinhaus triangle, where $a_{i,j}$ denotes the jth element of the ith row of ΔS. We denote by $\nu(S) = \nu(a_1, \ldots, a_n)$ the number of 1's in ΔS, that is,

$$\nu(S) = \nu(a_1, \ldots, a_n) = \sum_{i=1}^{n} \sum_{j=1}^{n-i+1} a_{i,j},$$

where here $a_{i,j}$ is considered as an *integer* in $\{0, 1\}$.

First, we recall a result of [3].

Theorem B.1.8. *Let $S = (a_1, \ldots, a_n)$ be a sequence of length $n \geqslant 1$ in $\mathbb{Z}/2\mathbb{Z}$. Then,*

$$\nu(S) \equiv \sum_{j=1}^{n} \left(\binom{n+1}{j} - 1 \right) a_j \pmod 2.$$

Moreover, the number $\nu(S)$ is even for every sequence S of length n if, and only if, $n = 2^k - 2$ for a certain $k \geqslant 2$.

The proof is by recurrence on n and using Lucas's theorem. The least and the greatest possible values of $\nu(S)$ are determined.

Proposition B.1.9. *Let S be a sequence of length $n \geqslant 1$ in $\mathbb{Z}/2\mathbb{Z}$. Then,*

$$0 \leqslant \nu(S) \leqslant \left\lfloor \frac{n(n+1)+1}{3} \right\rfloor.$$

We recall the four least and the two greatest possible values of $\nu(S)$ determined by Chang [3].

B.1.3 Solutions of Steinhaus's Problem

We present in detail four different solutions of the Problem of Steinhaus. These solutions are based on pseudo-periodic balanced sequences [17], strongly balanced sequences [14], symmetric and antisymmetric balanced sequences [15] and zerosum balanced sequences [13].

B.2 Even and odd Steinhaus graphs

Definition B.2.1. Let $s = (a_1, \ldots, a_n)$ be a finite sequence of length $n - 1 \geqslant 1$ in $\mathbb{Z}/2\mathbb{Z}$. The *Steinhaus matrix* associated to s is the square matrix $M(s) = (a_{i,j})$ of size n defined by:

- $a_{i,i} = 0$ for $1 \leqslant i \leqslant n$,
- $a_{1,j} = a_{j-1}$ for $2 \leqslant j \leqslant n$,
- $a_{i,j} = a_{i-1,j-1} + a_{i-1,j}$ for $2 \leqslant i < j \leqslant n$,
- $a_{i,j} = a_{j,i}$ for $1 \leqslant i, j \leqslant n$.

By convention, $M(\emptyset) = (0)$ is the Steinhaus matrix of size $n = 1$ associated to the empty sequence. The set of all Steinhaus matrices of size n is denoted by $\mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$.

Definition B.2.2. Let s be a sequence of length $n-1 \geqslant 0$ in $\mathbb{Z}/2\mathbb{Z}$. The *Steinhaus graph* associated to s is the simple graph $G(s)$ whose adjacency matrix is the Steinhaus matrix $M(s)$ associated to s.

We study the even and odd Steinhaus graphs, i.e. those with all vertex degrees of the same parity. First, we give a new proof of a theorem of Dymacek which states that the Steinhaus matrix of an even Steinhaus graph is a doubly-symmetric matrix. This new proof is based on a result which shows that the anti-diagonal entries of a Steinhaus matrix are determined by the vertex degrees of its associated Steinhaus graph.

Theorem B.2.3. *Let G be a Steinhaus graph on $n \geqslant 2$ vertices and $M = (a_{i,j})$ its associated Steinhaus matrix. Then every anti-diagonal entry of M can be expressed by means of the vertex degrees of G. If we denote by $\deg(V_i)$ the degree of the vertex V_i in G, then for every i, $1 \leqslant i \leqslant \left\lfloor \frac{n}{2} \right\rfloor$, we have*

$$a_{i,n-i+1} \equiv \sum_{k=0}^{i-1} \binom{i-1}{k} \deg(V_{i+k+1}) \equiv \sum_{k=0}^{i-1} \binom{i-1}{k} \deg(V_{n-i-k}) \pmod 2.$$

We continue by characterizing doubly-symmetric Steinhaus matrices.

Proposition B.2.4. *Let $M = (a_{i,j})$ be a Steinhaus matrix of size $n \geqslant 3$. Then the following assertions are equivalent:*

(i) the matrix M is doubly-symmetric,

(ii) the over-diagonal of M is a symmetric sequence,

(iii) the entries $a_{i,n-i+1}$ of the anti-diagonal of M vanish for all i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$.

We now obtain Dymacek's theorem [8].

Theorem B.2.5. *The Steinhaus matrix of an even Steinhaus graph is doubly-symmetric.*

We use this result in order to study even Steinhaus graphs as follows. This results appear in [8].

Definition B.2.6. Let $k \in \{0,1\}$ and $n \geqslant 1$. Let U_k be the operator

$$U_k : \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathcal{SM}_{n+3}(\mathbb{Z}/2\mathbb{Z})$$

which assigns to each matrix $M = (b_{i,j})$ in $\mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$ the matrix $U_k(M) = (a_{i,j})$ in $\mathcal{SM}_{n+3}(\mathbb{Z}/2\mathbb{Z})$ defined by

$$\begin{cases} a_{1,n+3} = 0, \\ (a_{1,3}, \ldots, a_{1,n+2}) = P_k((b_{1,2}, \ldots, b_{1,n})), \\ a_{1,2} = \sum_{j=3}^{n+2} a_{1,j}, \end{cases}$$

where $P_k((b_{1,2}, \ldots, b_{1,n}))$ is the primitive sequence of $(b_{1,2}, \ldots, b_{1,n})$ defined above.

Notation. Let G be a Steinhaus graph on $n \geqslant 1$ vertices and $k \in \{0, 1\}$. We denote by $U_k(G)$ the Steinhaus graph on $n + 3$ vertices whose Steinhaus matrix is the image of the Steinhaus matrix of G by the operator U_k, that is,

$$\mathcal{A}(U_k(G)) := U_k(\mathcal{A}(G)),$$

where $\mathcal{A}(G)$ denotes the adjacency matrix of the graph G.

Dymacek obtained the two following theorems [8].

Theorem B.2.7. *Let G be a Steinhaus graph on $n \geqslant 1$ vertices. Then, the graph G is even if, and only if, the graphs $U_0(G)$ and $U_1(G)$ are both even graphs on $n + 3$ vertices.*

Theorem B.2.8. *Let n be a positive integer. If we denote by $P(n)$ the number of even Steinhaus graphs on n vertices, then, we have*

$$P(n) = 2^{\lfloor \frac{n}{3} \rfloor}.$$

In the same manner, we study the odd Steinhaus graphs.

Definition B.2.9. Let I be the operator

$$I : \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathcal{SM}_n(\mathbb{Z}/2\mathbb{Z})$$

which assigns to each Steinhaus matrix $M(a_1, \ldots, a_{n-1})$ the Steinhaus matrix $M(a_1, \ldots, a_{n-2}, a_{n-1}+1)$.

Notation. Let G be a Steinhaus graph on $n \geqslant 1$ vertices. We denote by $I(G)$ the Steinhaus graph on n vertices whose Steinhaus matrix is defined by

$$\mathcal{A}(I(G)) := I(\mathcal{A}(G)),$$

where $\mathcal{A}(G)$ denotes the adjacency matrix of the graph G.

Dymacek obtained the two following theorems [8].

Theorem B.2.10. *Let G be a Steinhaus graph on $2n \geqslant 1$ vertices. Then, the graph G is even if, and only if, the graph $I(G)$ is odd.*

Remark. Since the number of vertices of odd degree is even for every simple graph, it follows that there is no odd graph on an odd number of vertices.

Theorem B.2.11. *Let n be a positive integer. If we denote by $Imp(n)$ the number of odd Steinhaus graphs on n vertices, then*

$$Imp(n) = \begin{cases} 2^{\lfloor \frac{n}{3} \rfloor} & \text{for } n \text{ even}, \\ 0 & \text{for } n \text{ odd}. \end{cases}$$

B.3 Regular Steinhaus graphs

In [8], the following conjectures were made:

Conjecture B.3.1. The regular Steinhaus graphs of even degree are the zero-edge graph on n vertices, for every positive integer n, and the Steinhaus graph $G(s)$ on $n = 3m+1$ vertices generated by the periodic sequence $s = (110)^m$ of length $3m$, for every positive integer m.

Conjecture B.3.2. The complete graph on two vertices K_2 is the only regular Steinhaus graph of odd degree.

First, we give a proof that the sequence $(110)^m$ is indeed associated to a regular Steinhaus graph of even degree. This result is stated without proof in [2, 8].

Proposition B.3.3. *For every positive integer m, the Steinhaus graph $G((110)^m)$ on $3m+1$ vertices is regular of degree $2m$.*

In the sequel of the chapter, we are interested in the conjecture in the odd case. We introduce multi-symmetric matrices.

Definition B.3.4. Let $M = (a_{i,j})$ be a square matrix of size $n \geqslant 1$. The matrix M is said to be *multi-symmetric* if it is doubly-symmetric and each row of its upper-triangular part is a symmetric sequence, that is

$$a_{i,j} = a_{i,n-j+i+1}, \ \forall 1 \leqslant i < j \leqslant n.$$

We characterize the multi-symmetric Steinhaus matrices.

Proposition B.3.5. *Let $M = (a_{i,j})$ be a Steinhaus matrix of size $n \geqslant 3$. Then the following assertions are equivalent:*

(i) the matrix M is multi-symmetric,

(ii) the first row, the last column and the over-diagonal of M are symmetric sequences,

(iii) the entries $a_{i,n-i+1}$, $a_{n-2i+1,n-i+1}$ and $a_{i,2i}$ vanish for all i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor$.

The interest of these multi-symmetric Steinhaus matrices is given in the following theorem which is a refinement of a statement of Dymacek [8] proved in [2].

Theorem B.3.6. *Let G be a regular Steinhaus graph of odd degree k on $2n \geqslant 4$ vertices. Then $k = n$ and $G \setminus \{V_1, V_{2n}\}$ is a regular Steinhaus graph of even degree $n-1$ whose associated Steinhaus matrix is multi-symmetric.*

We begin by parametrizing the multi-symmetric Steinhaus matrices.

Proposition B.3.7. *Let $M = (a_{i,j})$ be a multi-symmetric Steinhaus matrix of size n. Let j_i be an element of the set $\{2i+1, \ldots, n-i\}$ for every i, $1 \leqslant i \leqslant \left\lfloor \frac{n-1}{3} \right\rfloor$. Then the matrix M only depends on the following parameters:*

- a_{1,j_1} *and* $\left\{ a_{2i,j_{2i}} \;\middle|\; 1 \leqslant i \leqslant \left\lceil \frac{n}{6} \right\rceil - 1 \right\}$, *for n even,*
- $\left\{ a_{2i+1,j_{2i+1}} \;\middle|\; 0 \leqslant i \leqslant \left\lceil \frac{n-3}{6} \right\rceil - 1 \right\}$, *for n odd.*

Theorem B.3.8. *Let n be a positive integer. If we denote by $MS(n)$ the number of multi-symmetric Steinhaus matrices of size n, then we have*

$$MS(n) = \begin{cases} 2^{\left\lceil \frac{n}{6} \right\rceil} & , \text{ for } n \text{ even,} \\ 2^{\left\lceil \frac{n-3}{6} \right\rceil} & , \text{ for } n \text{ odd.} \end{cases}$$

For a Steinhaus graph associated to a multi-symmetric matrix, the knowledge of the vertex degrees modulo 4 imposes strong conditions on the entries of its Steinhaus matrix. We distinguish different cases depending on the parity of the number of vertices.

Proposition B.3.9. *Let n be an even number and G be a Steinhaus graph on n vertices whose Steinhaus matrix $M = (a_{i,j})$ is multi-symmetric. Then, we have*

$$\begin{aligned} &\deg(V_1) = \deg(V_n) \equiv a_{1,\frac{n}{2}+1} \pmod 2, \\ &\deg(V_2) = \deg(V_{n-1}) \equiv 2a_{1,\frac{n}{2}+1} \pmod 4, \\ &\deg(V_3) = \deg(V_{n-2}) \equiv 2a_{2,\frac{n}{2}+1} \pmod 4, \\ &\deg(V_{2i}) = \deg(V_{n-2i+1}) \equiv 2a_{2,2i+1} + 2a_{i,2i+1} \pmod 4, \ \forall 2 \leqslant i \leqslant \tfrac{n}{2} - 2. \end{aligned}$$

Thus, for n even, in every Steinhaus graph on n vertices whose Steinhaus matrix is multi-symmetric, the 4th vertex V_4 has a degree divisible by 4.

Proposition B.3.10. *Let n be an odd number and G be a Steinhaus graph on n vertices whose Steinhaus matrix $M = (a_{i,j})$ is multi-symmetric. Then, we have*

$$\begin{aligned} &\deg(V_1) = \deg(V_n) \equiv 0 \pmod 2, \\ &\deg(V_2) = \deg(V_{n-1}) \equiv 2a_{1,\frac{n+1}{2}} \pmod 4, \\ &\deg(V_{2i}) \equiv 2a_{i+1,2i+1} + 2a_{2i-1,2i+1} + 2a_{2i-1,\frac{n-1}{2}+i} \pmod 4, \ \forall 2 \leqslant i \leqslant \tfrac{n-3}{2}, \\ &\deg(V_{2i+1}) \equiv 2a_{2,2i+2} \pmod 4, \ \forall 1 \leqslant i \leqslant \tfrac{n-3}{2}. \end{aligned}$$

Thus, for n odd, in every Steinhaus graph on n vertices whose Steinhaus matrix is multi-symmetric the 3rd vertex V_3 has a degree divisible by 4.

The end of the chapter is devoted to the multi-symmetric Steinhaus matrices associated to Steinhaus graphs which are regular modulo 4. An upper bound of the number of these matrices is given.

Theorem B.3.11. *For every even number n, there are at most $2^{\left\lceil \frac{n}{24} \right\rceil}$ multi-symmetric Steinhaus matrices of size n whose associated Steinhaus graphs are regular modulo 4.*

Theorem B.3.12. *For every odd number n, there are at most $2^{\lceil \frac{n}{30} \rceil}$ multi-symmetric Steinhaus matrices of size n whose associated Steinhaus graphs are regular modulo 4.*

Using these results on the multi-symmetric Steinhaus matrices whose Steinhaus graphs are regular modulo 4, we obtain the following statement by computer search:

Computational Result B.3.13. *For every positive integer $n \leqslant 1500$, the zero-edge graph on n vertices is the only Steinhaus graph on n vertices with a multi-symmetric Steinhaus matrix and which is regular modulo 4.*

This result can be easily proved for every odd number in the special case of regular Steinhaus graphs on n vertices whose Steinhaus matrices are multi-symmetric.

Theorem B.3.14. *For every odd number n, there is no regular Steinhaus graph on n vertices whose Steinhaus matrix is multi-symmetric, except the zero-edge graph on n vertices.*

Finally, the above computational result permits us to extend the verification of Conjecture B.3.2 up to $n \leqslant 1500$ vertices.

Theorem B.3.15. *There is no regular Steinhaus graph of odd degree on $2 < n \leqslant 1500$ vertices.*

B.4 Steinhaus triangles in finite cyclic groups

Steinhaus triangles can be defined in any finite cyclic group. In 1976, Molluzzo posed the following generalization of Steinhaus's original problem [19].

Problem B.4.1 (Molluzzo, 1976)**.** *Let n be a positive integer. Given a positive integer m, is it true that there exists a balanced sequence of length m in $\mathbb{Z}/n\mathbb{Z}$ if and only if the binomial coefficient $\binom{m+1}{2}$ is divisible by n?*

Our first observation is that there exist finite cyclic groups where the Problem of Molluzzo can not be answered positively.

Computational Result B.4.2.

1. *There is no balanced sequence of length $m = 5$ in $\mathbb{Z}/15\mathbb{Z}$.*
2. *There is no balanced sequence of length $m = 6$ in $\mathbb{Z}/21\mathbb{Z}$.*

However, we conjecture that the Problem of Molluzzo is true in any finite cyclic group of prime power order. In this chapter, we prove the case of powers of 3. This proof is obtained by studing the arithmetic progressions.

First, we analyse the admissible lengths of balanced sequences in $\mathbb{Z}/n\mathbb{Z}$ and study the behaviour of balanced sequences under projection maps.

Definition B.4.3. For every finite multiset M of $\mathbb{Z}/n\mathbb{Z}$, we define and denote by $\mathfrak{m}_M$ the multiplicity function of M as the function

$$\mathfrak{m}_M : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{N}$$

which assigns to each element x in $\mathbb{Z}/n\mathbb{Z}$ the number of occurrence $\mathfrak{m}_M(x)$ of x in the multiset M. We agree that the multiplicity function $\mathfrak{m}_M$ vanishes at every x not in M.

Definition B.4.4. For every factor q of the positive integer n, we denote by π_q the canonical surjective morphism $\pi_q : \mathbb{Z}/n\mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/q\mathbb{Z}$. For a finite sequence $S = (a_1, a_2, \ldots, a_m)$ of length $m \geqslant 1$ in $\mathbb{Z}/n\mathbb{Z}$, we define, and denote by

$$\pi_q(S) = (\pi_q(a_1), \pi_q(a_2), \ldots, \pi_q(a_m))\,,$$

its projected sequence in $\mathbb{Z}/q\mathbb{Z}$.

We obtain a projection theorem.

Theorem B.4.5. *Let q be a divisor of n and S be a sequence of length $m \geqslant 1$ in $\mathbb{Z}/n\mathbb{Z}$. Then, the sequence S is balanced if, and only if, its projected sequence $\pi_q(S)$ is also balanced and the multiplicity function $\mathfrak{m}_{\Delta S} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{N}$ is constant on each coset of the subgroup $q\mathbb{Z}/n\mathbb{Z}$.*

In the sequel of this chapter, we study in detail the arithmetic progressions

$$AP(a, d, m) = (a, a + d, a + 2d, \ldots\ldots, a + (m - 1)d)$$

in $\mathbb{Z}/n\mathbb{Z}$ and their associated Steinhaus triangles. This permits us to prove that there exist infinitely many balanced sequences in each finite cyclic group of odd order. We obtain the following results.

Theorem B.4.6. *Let n be an odd number and let a and d be in $\mathbb{Z}/n\mathbb{Z}$. If d is non-invertible, then the arithmetic progression $AP(a, d, m)$ is not balanced for every positive integer m.*

Notation. For every odd number n, we denote by $\alpha(n)$ *the multiplicative order of* 2^n *modulo* n, i.e. the smallest positive integer e such that $2^{en} \equiv 1 \pmod{n}$, namely

$$\alpha(n) = \min\left\{e \in \mathbb{N}^* \mid 2^{en} \equiv 1 \pmod{n}\right\}.$$

Theorem B.4.7. *Let n be an odd number. Let a and d be in $\mathbb{Z}/n\mathbb{Z}$ with d invertible. Then, the arithmetic progression $AP(a, d, m)$ is balanced for every positive integer $m \equiv 0$ or $-1 \pmod{\alpha(n)n}$.*

We prove this theorem by induction on n and using the projection theorem. This result can be refined by considering the antisymmetric sequences in $\mathbb{Z}/n\mathbb{Z}$.

Definition B.4.8. Let $S = (a_1, a_2, \ldots, a_m)$ be a finite sequence of length $m \geqslant 1$ in $\mathbb{Z}/n\mathbb{Z}$. The sequence S is said to be *antisymmetric* if $a_{m-i+1} = -a_i$, for every integer i, $1 \leqslant i \leqslant m$.

Then, we determine the arithmetic progressions which are antisymmetric in a finite cyclic group of odd order.

Proposition B.4.9. *Let n be an odd number. Let d be in $\mathbb{Z}/n\mathbb{Z}$ and m be a positive integer. Then, there exists a unique antisymmetric arithmetic progression of length m and with common difference d. Moreover, if m is a multiple of n, then the unique antisymmetric arithmetic progression with common difference d and of length m is the sequence $AP(2^{-1}d, d, m)$. If $m \equiv -1 \pmod{n}$, then the unique antisymmetric arithmetic progression with common difference d and of length m is the sequence $AP(d, d, m)$.*

Notation. For every odd number n, we denote by $\beta(n)$ *the projective multiplicative order of* 2^n *modulo* n, i.e. the smallest positive integer e such that $2^{en} \equiv \pm 1 \pmod{n}$, namely

$$\beta(n) = \min\left\{e \in \mathbb{N}^* \mid 2^{en} \equiv \pm 1 \pmod{n}\right\}.$$

Observe that we have the alternative $\alpha(n) = \beta(n)$ or $\alpha(n) = 2\beta(n)$.

We obtain the following refinement.

Theorem B.4.10. *Let n be an odd number and d be an invertible element in $\mathbb{Z}/n\mathbb{Z}$. Then*

- *for every $m \equiv 0 \pmod{\beta(n)n}$, the arithmetic progression $AP(2^{-1}d, d, m)$ is balanced,*
- *for every $m \equiv -1 \pmod{\beta(n)n}$, the arithmetic progression $AP(d, d, m)$ is balanced.*

Since $\beta(3^k) = 1$ for every $k \geqslant 1$, we obtain, from the preceding theorem, a complete settlement of Molluzzo's Problem in every finite cyclic group of order 3^k for every $k \geqslant 1$. More generally, if we consider the sets

$$N(n) = \left\{m \in \mathbb{N} \;\middle|\; \binom{m+1}{2} \equiv 0 \pmod{n}\right\},$$

and

$$B(n) = \{m \in \mathbb{N} \mid \exists \text{ a balanced sequence in } \mathbb{Z}/n\mathbb{Z} \text{ of length } m\},$$

then clearly $B(n) \subset N(n)$. Moreover, Molluzzo's problem can be reformulated as the question whether $B(n) = N(n)$ for all $n > 1$. It follows from Theorem B.4.10 that

$$\frac{|B(n) \cap [\![0, k]\!]|}{|N(n) \cap [\![0, k]\!]|} \geqslant \frac{1}{2^{\omega(n)-1}\beta(n)},$$

for all $k \geqslant \beta(n)n$, where $\omega(n)$ is the number of distinct prime factors of n. Finally, we study the case where n is even and show that, in contrast, arithmetic progressions are almost never balanced.

Theorem B.4.11. *Let n be an even number and a and d be in $\mathbb{Z}/n\mathbb{Z}$. Then the arithmetic progression $S = AP(a, d, m)$ is balanced if, and only if, we have*

$$\begin{cases} n = 2 \quad \textit{and} \quad S \in \{(0,1,0), (1,1,1), (0,1,0,1), (1,0,1,0)\}, \\ \quad \textit{or} \\ n = 6 \quad \textit{and} \quad S \in \{(1,3,5), (2,3,4), (4,3,2), (5,3,1)\}. \end{cases}$$

B.5 Multiplicative order of a^n modulo n

We present a study of two arithmetic functions which generalize the functions α and β of Chapter 4. We begin with the function α_n.

Notation. For every positive integer n and every integer a coprime to n, we denote by $\mathcal{O}_n(a)$ *the multiplicative order of* a *modulo* n, i.e. the smallest positive integer e such that $a^e \equiv 1 \pmod{n}$, namely

$$\mathcal{O}_n(a) = \min\left\{e \in \mathbb{N}^* \mid a^e \equiv 1 \pmod{n}\right\}.$$

Definition B.5.1. For every positive integer n, we define and denote by α_n the function

$$\begin{array}{rccl} \alpha_n : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \left\{ \begin{array}{cl} \mathcal{O}_n\left(a^n\right) & \text{for } a \wedge n = 1, \\ 0 & \text{otherwise,} \end{array} \right. \end{array}$$

where $a \wedge n$ denotes the greatest common divisor of the integers a and n, with the convention that $0 \wedge n = n$ for every positive integer n.

The main result on the function α_n is the determination of the relationship between $\alpha_n(a)$ and $\alpha_{\mathrm{rad}(n)}(a)$ for every integer a coprime to n and where $\mathrm{rad}(n)$ is the radical of n, i.e. the largest square-free divisor of n.

Notation. For every prime number p, we denote by $v_p(n)$ the p-adic valuation of n, i.e. the greatest exponent $e \geqslant 0$ for which p^e divides n.

Notation. Let $\delta : \mathbb{N}^* \longrightarrow \{1, 2\}$ be the function defined by

$$\delta(n) = \left\{ \begin{array}{ll} 2 & \text{if } n = 2, \\ 1 & \text{otherwise.} \end{array} \right.$$

Theorem B.5.2. *Let*

$$n = {p_1}^{r_1} \cdots {p_k}^{r_k}$$

be the prime factorization of the positive integer n *and* a *be an integer coprime to* n. *Let* s_1, $\ldots$, s_k *be the largest integers such that*

$$a^{\mathcal{O}_{{p_i}^{\delta(p_i)}}(a)} \equiv 1 \pmod{{p_i}^{s_i}},$$

i.e. $s_i = v_{p_i}\left(a^{\mathcal{O}_{{p_i}^{\delta(p_i)}}(a)} - 1\right)$ *for all* i, $1 \leqslant i \leqslant k$. *If* $v_2(n) \leqslant 1$, *then we have*

$$\alpha_n(a) = \frac{\alpha_{\mathrm{rad}(n)}(a)}{\alpha_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i, s_i\}}}{\mathrm{rad}(n)}}.$$

Otherwise, if $v_2(n) \geqslant 2$, *then we have*

$$\alpha_n(a) = \frac{\alpha_{2\,\mathrm{rad}(n)}(a)}{\alpha_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i, s_i\}}}{2\,\mathrm{rad}(n)}}.$$

We continue with the function β_n.

Notation. For every positive integer n and every integer a coprime to n, we denote by $\mathcal{PO}_n(a)$ *the projective multiplicative order of* a *modulo* n, i.e. the smallest positive integer e such that $a^e \equiv \pm 1 \pmod{n}$, namely

$$\mathcal{PO}_n(a) = \min\left\{e \in \mathbb{N}^* \mid a^e \equiv \pm 1 \pmod{n}\right\}.$$

Definition B.5.3. For every positive integer n, we define and denote by β_n the function

$$\begin{array}{rccl} \beta_n : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \left\{ \begin{array}{cl} \mathcal{PO}_n\left(a^n\right) & \text{for } a \wedge n = 1, \\ 0 & \text{otherwise.} \end{array} \right. \end{array}$$

First, we get the useful following proposition.

Proposition B.5.4. *Let* n *be a positive integer and* a *be an integer coprime to* n. *If* $v_2(n) \leqslant 1$, *then we have*

$$\frac{\alpha_n(a)}{\beta_n(a)} = \frac{\alpha_{\mathrm{rad}(n)}(a)}{\beta_{\mathrm{rad}(n)}(a)}.$$

If $v_2(n) \geqslant 2$, *then we have*

$$\alpha_n(a) = \beta_n(a).$$

Finally, we determine the relationship between $\beta_n(a)$ and $\beta_{\mathrm{rad}(n)}(a)$ for every a coprime to n.

Theorem B.5.5. *Let*

$$n = {p_1}^{r_1} \cdots {p_k}^{r_k}$$

be the prime factorization of the positive integer n *and* a *be an integer coprime to* n. *Let* s_1, $\ldots$, s_k *be the largest integers such that*

$$a^{\mathcal{O}_{{p_i}^{\delta(p_i)}(a)}} \equiv 1 \pmod{{p_i}^{s_i}},$$

i.e. $s_i = v_{p_i}\left(a^{\mathcal{O}_{{p_i}^{\delta(p_i)}(a)}} - 1\right)$ *for all* i, $1 \leqslant i \leqslant k$. *If* $v_2(n) \leqslant 1$, *then we have*

$$\beta_n(a) = \frac{\beta_{\mathrm{rad}(n)}(a)}{\beta_{\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i, s_i\}}}{\mathrm{rad}(n)}}.$$

Otherwise, if $v_2(n) \geqslant 2$, *then we have*

$$\beta_n(a) = \frac{\beta_{2\,\mathrm{rad}(n)}(a)}{\beta_{2\,\mathrm{rad}(n)}(a) \wedge \frac{\prod_{i=1}^{k} {p_i}^{\min\{r_i, s_i\}}}{2\,\mathrm{rad}(n)}}.$$