N° d'ordre : 03/2015-D/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediène

Faculté deMathématiques

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

THESE

Présentée pour l'obtention du **grade** de **DOCTEUR EN SCIENCES**

En : MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : AIT AMRANE Lyes

Sujet

Etude des périodes de suites récurrentes linéaires sur les courbes elliptiques

Soutenue publiquement, le 12 mars 2015, devant le jury composé de :

M.	B. BENZAGHOU	Prof	USTHB / FMT	Président
M.	K. BETINA	Prof	USTHB / FMT	Directeur de thèse
M.	A. MOKRANE	Prof	U. PARIS 8	Co-directeur de thèse
M.	M. HERNANE	Prof	USTHB / FMT	Examinateur
M.	A. BOUYAKOUB	Prof	U. ORAN	Examinateur
M.	D. BEHLOUL	Prof	USTHB / FEI	Examinateur
Mme.	A. LAOUDI	MCA	USTHB / FMT	Examinatrice
Mme.	F. Z. BELKREDIM	MCA	U. CHLEF	Examinatrice

TABLE DES MATIÈRES

LISTE DES ANNEXES

INTRODUCTION

Plusieurs travaux établissant des liens entre courbes elliptiques et suites récurrentes linéaires ont été réalisés, essentiellement avec des suites de Fibonacci et leurs généralisations. On peut citer le travail de Ribenboim [27] qui détermine les points de coordonnées entières dans certaines courbes elliptiques grâce à l'étude de certaines suites de Lucas. Bugeaud et *al* [11] ont montré, par des techniques modulaires inspirées de la preuve du dernier théorème de Fermat, que les seules puissances parfaites dans la suite de Fibonacci sont $1, 8$ et 144. Plus récemment, Reynolds [26] a démontré qu'il n'y a qu'un nombre fini de puissances parfaites dans les suites de divisibilité elliptiques dont un cas particulier est la suite de Fibonacci. Aussi, il y a eu des études de périodes de suites récurrentes linéaires modulo un entier $m \geq 2$. On peut citer le travail de Brent [10] qui a étudié les périodes de suites de Fibonacci généralisées. Klaška [21–23] a étudié la suite Tribonacci modulo p^t pour un nombre premier p, ainsi que les formules de partition modulo un entier $m \geq 2$. Klaška et Skula [24] ont étudié les périodes de la suite Tribonacci modulo un nombre premier $p \equiv 1$ modulo 3. Wall [37] a étudié les périodes des suites de Fibonacci modulo m et Vinson [35] a étudié la relation entre la période et le rang d'apparition de zéro dans une période de la suite de Fibonacci modulo m. Vince [34] a considéré une suite récurrente linéaire d'ordre N quelconque, définie sur l'anneau des entiers A d'un corps de nombres K et il a étudié les propriétés des périodes de cette suite modulo des idéaux de A.

Le but de ce travail est de faire le lien entre la combinatoire énumérative et la théorie des nombres à travers les courbes elliptiques. Plus précisément, l'étude des périodes de suites récurrentes linéaires sur des courbes elliptiques. Il y a un premier travail qui a été fait par Coleman et *al* [12] qui ont étudié les périodes des suites de Fibonacci sur les courbes elliptiques. Ce travail peut être considéré dans un cadre plus général.

On sait que les nombres de Fibonacci s'expriment comme étant la somme des éléments parcourant les diagonales principales du triangle de Pascal, c'est-à-dire que chaque élément de la suite de Fibonacci $(F_n)_n$ est la somme de coefficients binomiaux $\binom{n-k}{k} : F_{n+1} = \sum_k \binom{n-k}{k}$. Dans ce contexte, il existe deux façons de généraliser les travaux de Coleman et *al* [12]. D'abord, sachant que la suite de Fibonacci est une suite récurrente linéaire d'ordre 2, nous sommes curieux de voir si nous

pouvons reproduire ce travail pour les suites récurrentes linéaires d'ordre $s+1$ définies par :

$$\begin{cases} u_0 = u_1 = \cdots = u_{s-1} = 0 \text{ et } u_s = 1, \\ u_{n+1} = u_n + u_{n-1} + \cdots + u_{n-s}, \ \ (n \geq s). \end{cases} \tag{0.1}$$

Les éléments de cette suite récurrente linéaire sont la somme des éléments des diagonales principales d'un triangle de Pascal généralisé et sont donnés par $u_{n+s} = \sum_k \binom{n-k}{k}_s$, où les $\binom{n}{k}_s$ sont des coefficients qui généralisent les coefficients binomiaux, donnés par la fonction génératrice $(1+x+\cdots+x^s)^n$, voir [6]. Cependant, déterminer des propriétés liées à la divisibilité des nombres premiers pour les suites récurrentes linéaires d'ordre s quelconque n'est pas chose facile. Donc, pour montrer que nous pouvons généraliser ce travail et avoir une première étape vers un programme plus vaste, nous l'avons fait d'abord pour les suites Tribonacci, c'est-à-dire $s = 2$.

Une deuxième façon de prolonger les travaux de Coleman et *al* [12] est de généraliser à la suite récurrente linéaire $(v_n)_n$, associée à différentes directions des transversales finies du triangle de Pascal, définie pour $n, p, q, r \in \mathbb{Z}$ avec $n \geq 0$, $r \geq 1$, $0 \leq p \leq r-1$ et $q+r > 0$, par

$$v_{n+1} = \sum_{k=0}^{\lfloor (n-p)/(q+r) \rfloor} \binom{n-qk}{p+rk} x^{n-p-(q+r)k} y^{p+rk},$$

et qui satisfait la relation de récurrence linéaire [8],

$$v_n - x\binom{r}{1} v_{n-1} + x^2\binom{r}{2} v_{n-2} + \cdots + (-1)^r x^r \binom{r}{r} v_{n-r} = y^r v_{n-r-q}, \tag{0.2}$$

et ayant la fonction génératrice [9]

$$T(z) := \sum_{n \geq 0} T_{n+1}^{(r,q,p)} z^n = \frac{y^p z^{p+1}(1-xz)^{r-p-1}}{(1-xz)^r - y^r z^{q+r}}.$$

Lorsque $q \leq 0$, la suite $(v_n)_n$ est d'ordre r pour tout q ($-r < q \leq 0$), et le coefficient y^r de v_{n-r-q} est soustrait de l'un des coefficients des termes $v_{n-1}, \ldots, v_{n-r}$, de sorte que, pour $-r < q \leq 0$, on obtienne

$$v_n - x\binom{r}{1} v_{n-1} + \cdots + \left((-x)^{r+q} \binom{r}{r+q} - y^r \right) v_{n-r-q} + \cdots + (-x)^r \binom{r}{r} v_{n-r} = 0.$$

Ainsi, le coefficient de ce terme change de statut. C'est ce qu'on appelle *le phénomène Morgan-*

Voyce.

Dans le premier chapitre, nous présentons des préliminaires sur les résidus quadratiques et les courbes elliptiques. Plus précisément, dans la première partie nous introduisons un résultat qui permet de déterminer les nombres premiers p pour lesquels une équation quadratique a des solutions modulo p. Dans la deuxième partie, nous définissons la notion d'une courbe elliptique et nous expliquons comment additionner deux points sur une courbe elliptique donnée par le graphe d'une équation de Weierstrass.

Dans le deuxième chapitre, nous présentons des préliminaire sur les suites récurrentes linéaires d'ordres N et leurs matrices compagnons. Nous définissons la notion d'une suite récurrente linéaire simplement périodique modulo un entier $m \geq 2$ et nous donnons une condition suffisante sur la matrice compagnon pour que la suite soit simplement périodique modulo m. Ensuite, nous rappelons ce qu'est une matrice circulante et nous donnons ses valeurs propres dans le cas général. Nous terminons par le cas Fibonacci où l'on résume les résultats qui nous ont motivé et que nous nous proposons de généraliser à d'autres suites récurrentes linéaires.

Dans le troisième chapitre [4], nous traitons le cas $r = 2$, $q = -1$, $x = 1$ et $y = \sqrt{t}$ dans (0.2), qui coïncide avec la relation de récurrence satisfaite par la suite de Morgan-Voyce. En fait, la suite de Morgan-Voyce classique $(M_n)_n$ est la suite récurrente linéaire d'ordre 2 définie par

$$\begin{cases} M_1 = 1,\ M_2 = 1+t+s, \\ M_n = (2+t)M_{n-1} - M_{n-2}, \ \ (n \geq 3). \end{cases}$$

Toujours en relation avec le triangle de Pascal, on a [8, 9] :

$$M_{n+1} = \sum_{k=0}^{n} M(n,k)t^k \ \text{ avec } \ M(n,k) = \binom{n+k}{2k} + s\binom{n+k}{2k+1}.$$

Pour prendre en charge un travail en relation avec les réseaux électriques, A. M. Morgan-Voyce [25] a défini une famille de polynômes par :

$$\begin{aligned} b_n(t) &= tB_{n-1}(t) + b_{n-1}(t) && (n \geq 1) \\ B_n(t) &= (1+t)B_{n-1}(t) + b_{n-1}(t) && (n \geq 1), \end{aligned}$$

avec $b_0(t) = B_0(t) = 1$. Ces polynômes b_n et B_n ont des propriétés fascinantes et intéressantes. Ils ont été étudiés par plusieurs auteurs, on peut citer, par exemple, Horadam [17], Swamy [32, 33] et

plus récemment Belbachir et *al* [8, 9]. Il n'est pas difficile de voir que ces polynômes vérifient

$$\begin{cases} b_n(t) = (2+t)b_{n-1}(t) - b_{n-2}(t), \ \ (n \geq 2) \\ b_0(t) = 1, \ b_1(t) = 1+t, \end{cases}$$

et

$$\begin{cases} B_n(t) = (2+t)B_{n-1}(t) - B_{n-2}(t), \ \ (n \geq 2) \\ B_0(t) = 1, \ B_1(t) = 2+t. \end{cases}$$

Ces polynômes sont donc un cas particulier de la suite $(M_n)_n$ et sont obtenus pour $s = 0$ et $s = 1$. Dans ces cas là, les coefficients $M(n,k)$ sont bien connus dans l'étude des réseaux électriques. Pour $s = 0$, ces coefficients sont exactement les lignes du triangle DFF donné dans le Tableau 1 ci-dessous [14], alors que pour $s = 1$, ils forment les lignes du triangle DFFz donné dans le Tableau 2 ci-dessous [15].

$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	...
0	1												
1	1	1											
2	1	3	1										
3	1	6	5	1									
4	1	10	15	7	1								
5	1	15	35	28	9	1							
6	1	21	70	84	45	11	1						
7	1	28	126	210	165	66	13	1					
8	1	36	210	462	495	286	91	15	1				
9	1	45	330	924	1287	1001	455	120	17	1			
10	1	55	495	1716	3003	3003	1820	680	153	19	1		
11	1	66	715	3003	6435	8008	6188	3060	969	190	21	1	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Tableau 1 : Le triangle DFF

Dans le quatrième chapitre [2], nous traitons le cas de la suite quasi Morgan-Voyce introduite par Horadam [18] et donnée par

$$\begin{cases} D_1 = 1, \ \ D_2 = 1+t+s, \\ D_n = (2+t)D_{n-1} + D_{n-2}, \quad (n \geq 3). \end{cases}$$

Horadam a posé la question suivante : *pouvons-nous trouver, si elle existe, une formule pour* $D(n,k)$ *comportant des coefficients binomiaux, analogue à celle de* $M(n,k)$*, c'est-à-dire :* $D_n = \sum_{k=0}^{n} D(n,k)t^k$ *?*

$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	...
0	1												
1	2	1											
2	3	4	1										
3	4	10	6	1									
4	5	20	21	8	1								
5	6	35	56	36	10	1							
6	7	56	126	120	55	12	1						
7	8	84	252	330	220	78	14	1					
8	9	120	462	792	715	364	105	16	1				
9	10	165	792	1716	2002	1365	560	136	18	1			
10	11	220	1287	3432	5005	4368	2380	816	171	20	1		
11	12	286	2002	6435	11440	12376	8568	3876	1140	210	22	1	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Tableau 2 : Le triangle DFFz

La réponse a été donnée par Belbachir et *al* [8, 9]. Elle est négative pour les paramètres réels.

Notons que pour $t = -1$ et $s = 1$, la suite quasi Morgan-Voyce donne exactement la suite de Fibonacci $(F_n)_n$.

Dans le cinquième chapitre [3], nous traitons le cas $s = 2$ dans (0.1) qui est la suite Tribonacci donnée par

$$\begin{cases} T_0 = T_1 = 0,\ T_2 = 1, \\ T_{n+1} = T_n + T_{n-1} + T_{n-2}, \quad (n \geq 2). \end{cases}$$

Dans chacun de ces trois derniers chapitres, nous étudions les propriétés des périodes de notre suite modulo un entier $m \geq 2$. Pour les chapitres 3 et 4, nous définissons une relation d'équivalence sur l'ensemble $(\mathbb{Z}/m\mathbb{Z})^2$ et nous donnons un théorème de partition de l'ensemble de toutes les conditions initiales possibles. Nous faisons de même dans le chapitre 5 sur l'ensemble $(\mathbb{Z}/m\mathbb{Z})^3$. Nous obtenons aussi une relation entre les périodes et les matrices circulantes. Finalement, nous définissons notre suite sur une courbe elliptique donnée par le graphe d'une équation de Weierstrass à coefficients dans un corps fini $\mathbb{F}_p(= \mathbb{Z}/p\mathbb{Z})$, où p est un nombre premier différent de 2, et nous étudions quelles sont les propriétés qui restent vérifiées lorsqu'elles sont généralisées aux courbes elliptiques. Il s'avère que la plupart des concepts que nous développons sur les groupes de courbes elliptiques sont vrais sur tout groupe abélien fini. Cependant, nous traitons les propriétés analogues dans le contexte des courbes elliptiques puisque c'est ce qui a motivé notre travail.

En Annexe A [1], nous revenons à l'étude de la suite quasi Morgan-Voyce définie ci-dessus que l'on notera cette fois-ci $\left(Q_n^{(s)}\right)_n$. Si nous écrivons $Q_{n+1}^{(s)} = \sum_{k=0}^{n} Q^{(s)}(n,k)t^k$ pour $n \geq 0$, alors,

dans un premier temps, nous montrons que les coefficients $Q^{(1)}(n,k)$ sont des produits de convolution de suites de Pell. Ensuite, nous montrons que les coefficients $Q^{(s)}(n,k)$ sont des produits de convolution de suites de Pell généralisés.

Enfin, nous terminons notre travail par une conclusion où des perspectives sont données.

Liste des articles réalisés : acceptés ou soumis, relatifs à la thèse.

1. L. Ait-Amrane, H. Belbachir et K. Betina. Periods of Morgan-Voyce sequences and elliptic curves, à paraître : Mathematica Slovaca.

2. L. Ait-Amrane et H. Belbachir. Periods of quasi Morgan-Voyce sequences and elliptic curves, soumis.

3. L. Ait-Amrane et H. Belbachir. Periods of Tribonacci sequences and elliptic curves, soumis.

4. L. Ait-Amrane et H. Belbachir. Quasi Morgan-Voyce sequences as convolutions of iterated generalized Pell sequences, soumis.

CHAPITRE 1

QUELQUES ÉLÉMENTS SUR LES CONGRUENCES DANS $\mathbb{Z}$ ET LES COURBES ELLIPTIQUES

1.1 Réciprocité quadratique

Cette section est largement puisée du livre de K. Ireland et M. Rosen "A Classical introduction to Modern Number Theory" [20].

Dans ce qui suit, on considère $a \in \mathbb{Z}$ et $m \in \mathbb{N}^\star$. Si p est un nombre premier, la résolution de la congruence $x^2 \equiv a \bmod p$ est assez facile. Elle est résoluble si et seulement si $a^{(p-1)/2} \equiv 1 \bmod p$. Toutefois, si la question est inversée, le problème est beaucoup plus difficile. Supposons que a est un nombre entier. Pour quels nombres premiers p la congruence $x^2 \equiv a \mod p$ est-elle résoluble ? La réponse est fournie par la loi de réciprocité quadratique. Cette loi a été formulée par Euler et Legendre, c'est Gauss qui a été le premier à fournir une preuve complète en 1801. Gauss était extrêmement fier de ce résultat qu'il a appelé le Théorème d'or.

1.1.1 Résidus quadratiques

Pour $\text{pgcd}(a,m) = 1$, a est appelé un résidu quadratique modulo m si la congruence $x^2 \equiv a \bmod m$ a une solution. Sinon, a est appelé un non résidu quadratique modulo m.

Dans ce qui suit p désignera un nombre premier impair.

Définition 1.1.1. Le symbole (a/p) aura la valeur 1 si a est un résidu quadratique modulo p, -1 si a est un non résidu quadratique modulo p et 0 si p divise a. Le symbole (a/p) est appelé symbole de Legendre.

Le symbole de Legendre est un outil très pratique pour étudier les résidus quadratiques. Nous allons énumérer quelques-unes de ses propriétés.

Proposition 1.1.1. *[20, Proposition 5.1.2]*

(a) $a^{(p-1)/2} \equiv (a/p) \bmod p$.

(b) $(ab/p) = (a/p)(b/p)$.

(c) *Si* $a \equiv b \bmod p$, *alors* $(a/p) = (b/p)$.

Corollaire 1.1.1.1. *[20, Corollaire 1, p. 51] Il y a autant de résidus quadratiques que de non résidus quadratiques modulo p.*

Corollaire 1.1.1.2. *[20, Corollaire 2, p. 51] Le produit de deux résidus quadratiques est un résidu quadratique, le produit de deux non résidus quadratiques est un résidu quadratique et le produit d'un résidu quadratique avec un non résidu quadratique est un non résidu quadratique.*

Corollaire 1.1.1.3. *[20, Corollaire 3, p. 52]* $(-1)^{(p-1)/2} = (-1/p)$.

Le Corollaire 1.1.1.3 est particulièrement intéressant. Tout entier impair est de la forme $4k+1$ ou $4k+3$, ce qui permet de reformuler le Corollaire 1.1.1.3 comme suit : $x^2 \equiv -1 \bmod p$ a une solution si et seulement si p est de la forme $4k+1$. Ainsi, -1 est un résidu quadratique pour les nombres premiers $5, 13, 17, 29, \ldots$ et p est un non résidu quadratique pour les nombres premiers $3, 7, 11, 19, \ldots$.

Proposition 1.1.2. *[20, Proposition 5.1.3] Le nombre* 2 *est un résidu quadratique pour les nombres premiers de la forme* $8k+1$ *et* $8k+7$. *Le nombre* 2 *est un non résidu quadratique pour les nombres premiers de la forme* $8k+3$ *et* $8k+5$. *Cette information est résumée dans la formule*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

1.1.2 Loi de réciprocité quadratique

Théorème 1.1.3. *[20, Théorème 1, p. 53] Soient p et q des nombres premiers impairs, alors*

(a) $(-1/p) = (-1)^{(p-1)/2}$.

(b) $(2/p) = (-1)^{(p^2-1)/8}$.

(c) $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

Si p ou q est de la forme $4k+1$, alors $((p-1)/2)((q-1)/2) \equiv 0 \bmod 2$. Si p et q sont de la forme $4k+3$, alors $((p-1)/2)((q-1)/2) \equiv 1 \bmod 2$. Cela nous permet de reformuler la partie (c) de la manière suivante :

(1) Si p ou q est de la forme $4k+1$, alors p est un résidu quadratique modulo q si et seulement si q est un résidu quadratique modulo p.

(2) Si p et q sont de la forme $4k+3$, alors p est un résidu quadratique modulo q si et seulement si q est un non résidu quadratique modulo p.

Comme première application de la réciprocité quadratique, on montre comment elle peut être utilisée, à l'aide de la Proposition 1.1.1, dans le calcul numérique du symbole de Legendre. Un exemple devrait suffire pour illustrer la méthode.

On se propose de calculer $(23/41)$. Puisque $41 \equiv 1 \bmod 4$, on a $(23/41) = (41/23) = (18/23)$. La dernière étape découle de $41 \equiv 18 \bmod 23$. En outre, on a $(18/23) = (2/23)(3/23)^2 = (2/23)$. Maintenant, $23 \equiv 7 \bmod 8$, donc $(2/23) = 1$. Par conséquent, $(23/41) = 1$, c'est-à-dire, 23 est un résidu quadratique modulo 41. En effet, $8^2 \equiv 23 \bmod 41$.

La prochaine application est plus importante. Nous avons remarqué précédemment que -1 est un résidu quadratique pour les nombres premiers de la forme $4k+1$ et que 2 est un résidu quadratique pour les nombres premiers qui sont de la forme $8k+1$ ou $8k+7$. Si a est un nombre entier arbitraire, pour quels nombres premiers p a-t-on a un résidu quadratique modulo p ? La réponse, dans le cas où $a = q$ est un nombre premier impair, est donnée dans le théorème suivant.

Théorème 1.1.4. *[20, Théorème 2, p. 54] Soit $q \neq 2$ un nombre premier.*

(a) *Si $q \equiv 1$ mod 4, alors q est un résidu quadratique modulo p si et seulement si $p \equiv r$ mod q, où r est un résidu quadratique modulo q.*

(b) *Si $q \equiv 3$ mod 4, alors q est un résidu quadratique modulo p si et seulement si $p \equiv \pm b^2$ mod $4q$, où b est un entier impair premier avec q.*

Prenons $q = 3$ comme une première illustration. D'après la partie (b) du Théorème 1.1.4, nous devons trouver les résidus modulo 12 des carrés des nombres entiers impairs premiers à 3. Les nombres $1^2, 5^2, 7^2$ et 11^2 sont tous congrus à 1. Ainsi, 3 est un résidu quadratique pour les nombres premiers p congrus à ± 1 modulo 12 et un non résidu quadratique pour les nombres premiers congrus à ± 5 modulo 12.

Considérons maintenant $q = 5$. Puisque $5 \equiv 1 \bmod 4$, nous sommes dans la partie simple (a) du Théorème 1.1.4. Les nombres 1 et 4 sont les résidus quadratiques modulo 5, et 2 et 3 sont les non résidus quadratiques. Ainsi, 5 est un résidu quadratique pour les nombres premiers congrus à 1 ou 4 modulo 5 et un non résidu quadratique pour les nombres premiers congrus à 2 ou 3 modulo 5.

1.2 Courbes elliptiques

Cette section est puisée, en grande partie, du livre de L. C. Washington "Elliptic curves : Number theory and cryptography" [38], pour un complément exhaustif, voir aussi [28–30].

Dans cette section K désignera un corps commutatif.

1.2.1 Equation de Weierstrass

Une courbe elliptique E est une courbe lisse donnée par le graphe d'une équation de la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

où a_1, a_2, a_3, a_4 et a_6 sont des constantes. Cette équation s'appelle *équation de Weierstrass généralisée* d'une courbe elliptique. On aura besoin de préciser à quel ensemble $a_1, a_2, a_3, a_4, a_6, x$ et y appartiennent. En général, ils sont dans un corps commutatif, par exemple, le corps des nombres réels $\mathbb{R}$, le corps des nombres complexes $\mathbb{C}$, le corps des nombres rationnels $\mathbb{Q}$, l'un des corps finis $\mathbb{F}_p(=\mathbb{Z}/p\mathbb{Z})$ pour un nombre premier p, ou l'un des corps finis $\mathbb{F}_q$, où $q = p^k$ avec $k \geq 1$. Si la caractéristique du corps est différente de 2, alors on peut diviser par 2 et compléter le carré

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

ce qui peut être écrit comme suit

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{1.2}$$

avec $y_1 = y + a_1x/2 + a_3/2$ et a_2', a_4', a_6' des constantes. Si la caractéristique est aussi différente de 3, on peut poser $x_1 = x + a_2'/3$ et obtenir

$$y_1^2 = x_1^3 + ax_1 + b,$$

pour a et b des constantes données. On vient de voir que toute courbe elliptique définie sur un corps de caractéristique différente de 2 et de 3 peut être donnée par le graphe d'une équation de la forme :

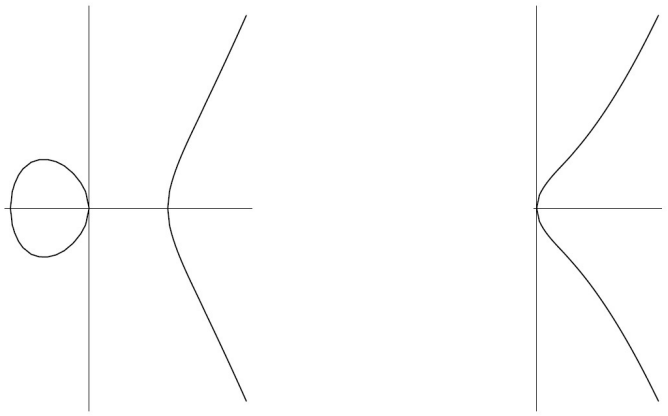
$$y^2 = x^3 + ax + b, \tag{1.3}$$

où a et b sont des constantes. Cette dernière équation s'appelle *équation de Weierstrass* d'une courbe elliptique. Si a et b appartiennent à K, on dit que E *est définie sur* K.

Si on veut considérer des points dont les coordonnées sont dans un certain corps $L \supseteq K$, on écrit $E(L)$. Par définition, cet ensemble contient toujours le point à l'infini, noté O, que l'on définira plus loin dans cette section. On note donc par $E(L)$ l'ensemble

$$E(L) = \{O\} \cup \{(x,y) \in L \times L \mid y^2 = x^3 + ax + b\}.$$

Il n'est pas possible de dessiner des graphes significatifs de courbes elliptiques sur la plupart des corps. Cependant, pour l'intuition, il est utile de penser en termes de graphes dans le plan réel. Ces graphes ont essentiellement deux formes représentées dans la Figure 1 ci-dessous. La cubique $y^2 = x^3 - x$ dans le premier cas a trois racines réelles distinctes. Dans le second cas, la cubique $y^2 = x^3 + x$ a une seule racine réelle. Dans le cas général, il ne peut pas y avoir de racine multiple car par hypothèse, une courbe elliptique est une courbe lisse, on supposera donc que le discriminant $\Delta = -2^4(4a^3 + 27b^2)$ est non nul.



(a) $y^2 = x^3 - x$ (b) $y^2 = x^3 + x$

Figure 1.

On a vu qu'en caractéristique différente de 2 et 3, toute courbe elliptique est donnée par le graphe d'une équation de Weierstrass (1.3). Cependant, en caractéristique 3, il existe aussi des courbes elliptiques qui sont données par une équation de Weierstrass (1.3). Les deux exemples précédents sont des courbes elliptiques sur $\mathbb{F}_3$.

Pour des raisons techniques, il est utile d'ajouter un point à l'infini à une courbe elliptique. Dans la sous-section 2.3, ce concept sera expliqué rigoureusement. Cependant, il est plus facile de le considérer comme un point (∞,∞), généralement noté par O, se trouvant au sommet de l'axe

des ordonnées. Pour des fins de calcul, ce sera un symbole formel répondant à certaines règles de calcul. Par exemple, une droite passe par O exactement lorsque cette droite est verticale (c'est-à-dire $x =$ constante). Le point O peut sembler un peu artificiel, mais on verra que le fait de le rajouter a des conséquences très utiles.

1.2.2 La loi de groupe

Connaissant deux points, ou même un point, sur une courbe elliptique, on peut produire de nouveaux points sur cette courbe.

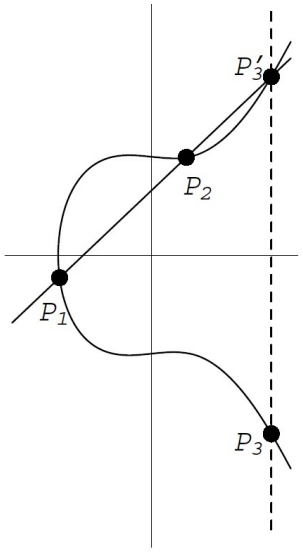


Figure 2.

Sommer des points sur une courbe elliptique

Commençons avec deux points

$$P_1(x_1, y_1), \quad P_2(x_2, y_2)$$

sur une courbe elliptique E donnée par l'équation $y^2 = x^3 + ax + b$, on définit un nouveau point P_3 comme suit : on trace la droite D qui passe par P_1 et P_2, on verra ci-dessous que D intersecte E en un troisième point P_3', on prend le symétrique de P_3' par rapport à l'axe des abscisses pour obtenir le point P_3. On définit

$$P_3 := P_1 + P_2.$$

Supposons d'abord que $P_1 \neq P_2$ et qu'aucun des deux points n'est le point O. On trace la droite

D passant par P_1 et P_2. Si $x_1 = x_2$, la droite D est verticale, on traitera ce cas plus tard. Supposons donc que $x_1 \neq x_2$, alors la pente de D est

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

et son équation est donnée par

$$y = m(x - x_1) + y_1.$$

Pour trouver l'intersection avec E, on remplace y dans l'équation de E et on obtient

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b,$$

ce qu'on peut écrire sous la forme

$$0 = x^3 - m^2x^2 + \cdots.$$

Les trois racines de cette cubique correspondent aux trois points d'intersection de D et E. En règle générale, la résolution d'une cubique n'est pas facile, mais dans le cas présent, on connaît déjà deux des racines, à savoir x_1 et x_2, puisque P_1 et P_2 sont des points de D et E. Par conséquent, on pourrait factoriser la cubique pour obtenir la troisième valeur de x. Mais il y a un moyen plus simple. Si on a un polynôme cubique $x^3 + \alpha x^2 + \beta x + \gamma$ avec des racines r, s, t, alors

$$x^3 + \alpha x^2 + \beta x + \gamma = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \cdots.$$

Si on connaît deux racines r et s, alors la troisième racine est $t = -\alpha - r - s$.

Dans notre cas, on obtient

$$x = m^2 - x_1 - x_2$$

et

$$y = m(x - x_1) + y_1.$$

Maintenant, on prenant le symétrique par rapport à l'axe des x, on obtient le point $P_3 = (x_3, y_3)$:

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1.$$

Dans le cas où $x_1 = x_2$ mais $y_1 \neq y_2$, la droite passant par P_1 et P_2 est une droite verticale, qui intersecte E à l'infini (au point O). En prenant le symétrique de O par rapport à l'axe des x, on

obtient le même point O (c'est pourquoi on met O à la fois en haut et en bas de l'axe des y). Par conséquent, dans ce cas, $P_1 + P_2 = O$.

Considérons maintenant le cas où $P_1 = P_2 = (x_1, y_1)$. Lorsque deux points sur une courbe sont très proches l'un de l'autre, la droite D passant par ces deux points se rapproche d'une droite tangente. Par conséquent, lorsque les deux points coïncident, la droite D est la droite tangente. La différentiation implicite nous permet de trouver la pente m de D :

$$2y\frac{dy}{dx} = 3x^2 + a, \quad \text{donc} \quad m = \frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}.$$

Si $y_1 = 0$, alors la droite D est verticale et on pose $P_1 + P_2 = O$, comme ci-dessus (en fait, comme E est par hypothèse lisse, alors $y_1 = 0$ implique que le numérateur $3x_1^2 + a \neq 0$). C'est pourquoi, on suppose que $y_1 \neq 0$. L'équation de D est

$$y = m(x - x_1) + y_1,$$

comme ci-dessus. On obtient l'équation cubique

$$0 = x^3 - m^2x^2 + \cdots.$$

Cette fois-ci, nous ne connaissons qu'une seule racine, à savoir x_1, mais c'est une racine double puisque D est tangente à E en P_1. Par conséquent, en procédant comme précédemment, on obtient

$$x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1.$$

Enfin, supposons que $P_2 = O$. La droite passant par P_1 et O est une droite verticale qui intersecte E au point P_1' qui est la réflexion de P_1 sur l'axe des x. Lorsqu'on prend le symétrique de P_1' par rapport à l'axe des x pour obtenir $P_3 = P_1 + P_2$, on revient au point P_1, donc

$$P_1 + O = P_1$$

pour tous les points P_1 dans E. Bien sûr, on prolonge ce dernier cas pour avoir $O + O = O$.

Résumons la discussion ci-dessus :

Loi de groupe

Soit E une courbe elliptique définie par (1.3). Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ des points de E avec P_1, $P_2 \neq O$. On définit $P_1 + P_2 = P_3 = (x_3, y_3)$ comme suit :

1. Si $x_1 \neq x_2$, alors

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{où } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2. Si $x_1 = x_2$ et $y_1 \neq y_2$, alors $P_1 + P_2 = O$.

3. Si $P_1 = P_2$ et $y_1 \neq 0$, alors

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{où } m = \frac{3x_1^2 + a}{2y_1}.$$

4. Si $P_1 = P_2$ et $y_1 = 0$, alors $P_1 + P_2 = O$.

5. $P + O = P$, pour tout point P de E.

Notons que si P_1 et P_2 ont leurs coordonnées dans un corps L contenant a et b, alors $P_1 + P_2$ a aussi ses coordonnées dans L. Par conséquent, l'addition de points ci-dessus est une loi de composition interne dans $E(L)$.

Théorème 1.2.1. *[38, Théorème 2.1] L'addition de points sur une courbe elliptique E satisfait les propriétés suivantes :*

1. *(Commutativité) $P_1 + P_2 = P_2 + P_1$ pour tous P_1, P_2 dans E.*
2. *(Existence d'un élément neutre) $P + O = O$ pour tout point P dans E.*
3. *(Existence des inverses) Etant donné P dans E, il existe P' dans E vérifiant $P + P' = O$. Ce point P' sera noté $-P$.*
4. *(Associativité) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ pour tous P_1, P_2, P_3 dans E.*

En d'autres termes, les points de E forment un groupe abélien additif ayant O pour élément neutre.

Remarque 1. Pour l'équation de Weierstrass (1.3), si $P = (x, y)$, alors $-P = (x, -y)$. Pour l'équation de Weierstrass généralisée (1.1), ce n'est plus le cas. Si $P = (x, y)$ est sur la courbe décrite par (1.1), alors $-P = (x, -a_1 x - a_3 - y)$.

Pour $m \in \mathbb{Z}$ et $P \in E$, on pose

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ termes si } m>0}, \quad [m]P = \underbrace{-P - \cdots - P}_{|m| \text{ termes si } m<0}, \quad [0]P = O.$$

Pour calculer $[m]P$ pour un grand nombre entier m, il est inefficace d'ajouter P à lui même de façon répétée. Il est plus rapide d'utiliser la multiplication successive par 2. Par exemple, pour calculer $[19]P$, on calcule

$$[2]P, \ \ [4]P = [2]P + [2]P, \ \ [8]P = [4]P + [4]P,$$

$$[16]P = [8]P + [8]P, \ \ [19]P = [16]P + [2]P + P.$$

Cette méthode nous permet de calculer $[m]P$ pour de très grand m, dire de plusieurs centaines de chiffres, très rapidement. La seule difficulté est que la taille des coordonnées des points augmente très rapidement si on travaille sur les nombres rationnels. Cependant, lorsqu'on travaille sur un corps fini, par exemple $\mathbb{F}_p$, ce n'est pas un problème parce qu'on peut sans cesse réduire modulo p et ainsi garder les nombres relativement petits. Notons que le fait que la loi est associative nous permet de faire ces calculs sans se soucier de de l'ordre qu'on utilise pour combiner ces additions.

1.2.3 Espace projectif et le point à l'infini

On sait tous que les droites parallèles se rencontrent à l'infini. L'espace projectif nous permet de donner un sens à cette assertion, et aussi d'interpréter le point à l'infini sur une courbe elliptique.

L'espace projectif $\mathbf{P}^2_K$ de dimension 2 sur K est donné par des classes d'équivalence de triplets (x,y,z) avec x, y, $z \in K$ et au moins un des x, y, z est non nul. Deux triplets (x_1,y_1,z_1) et (x_2,y_2,z_2) sont dit *équivalent* s'il existe un élément non nul $\lambda \in K$ tel que

$$(x_1,y_1,z_1) = (\lambda x_2, \lambda y_2, \lambda z_2),$$

on écrit $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$. La classe d'équivalence de (x,y,z) est notée $(x : y : z)$.

Si $(x : y : z)$ est un point avec $z \neq 0$, alors $(x : y : z) = (x/z : y/z : 1)$. Ce sont les points "finis" de $\mathbf{P}^2_K$. Cependant, si $z = 0$ alors diviser par z devrait être considéré pour nous comme si on était à l'infini en coordonnée x ou y, et donc les points $(x,y,0)$ sont appelés les "*points à l'infini*" de $\mathbf{P}^2_K$. Le point à l'infini sur une courbe elliptique sera bientôt identifié avec l'un de ces points à l'infini de $\mathbf{P}^2_K$.

Le *plan affine* de dimension 2 sur K est souvent noté par

$$\mathbf{A}_K^2 = \{(x,y) \in K \times K\}.$$

On a l'inclusion canonique

$$\mathbf{A}_K^2 \hookrightarrow \mathbf{P}_K^2$$

donnée par

$$(x,y) \mapsto (x : y : 1).$$

De cette façon, le plan affine est identifié avec les points finis de $\mathbf{P}_K^2$. Ajouter les points à l'infini pour obtenir $\mathbf{P}_K^2$ peut être considéré comme un moyen de "compactifier" le plan.

Un polynôme de trois variables est *homogène* de degré n s'il est la somme de termes de la forme $ax^iy^jz^k$ avec $a \in K$ et $i+j+k=n$. Par exemple, $F(x,y,z) = 2x^3 - 5xyz + 7yz^2$ est un polynôme homogène de degré 3. Si un polynôme est homogène de degré n, alors $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x,y,z)$ pour tout $\lambda \in K$. Il s'ensuit que si F est homogène d'un certain degré et $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$, alors $F(x_1,y_1,z_1) = 0$ si et seulement si $F(x_2,y_2,z_2) = 0$. Par conséquent, un zéro de F dans $\mathbf{P}_K^2$ ne dépend pas du choix du représentant de la classe d'équivalence, donc l'ensemble des zéros de F dans $\mathbf{P}_K^2$ est bien défini.

Si $F(x,y,z)$ est un polynôme arbitraire en x, y, z, alors on ne peut pas parler d'un point de $\mathbf{P}_K^2$ vérifiant $F(x,y,z) = 0$ car cela dépend du représentant (x,y,z) de la classe d'équivalence. Par exemple, soit $F(x,y,z) = x^2 + 2y - 3z$, alors $F(1,1,1) = 0$, donc on serait tenté de dire que F s'annule en $(1:1:1)$. Mais $F(2,2,2) = 2$ et $(1:1:1) = (2:2:2)$. Pour éviter ce problème, on a besoin de travailler avec des polynômes homogènes.

Si $f(x,y)$ est un polynôme en x et y, alors on peut le rendre homogène en insérant une puissance appropriée de z. Par exemple, si $f(x,y) = y^2 - x^3 - ax - b$, alors on obtient le polynôme homogène $F(x,y,z) = y^2z - x^3 - axz^2 - bz^3$.

Si F est homogène de degré n, alors

$$F(x,y,z) = z^n f(x/z, y/z)$$

et

$$f(x,y) = F(x,y,1).$$

On peut maintenant voir ce que signifie deux droites parallèles qui se rencontrent à l'infini. Soient

$$y = mx + b_1 \quad \text{et} \quad y = mx + b_2$$

deux droites parallèles non verticales avec $b_1 \neq b_2$, elles ont les formes homogènes

$$y = mx + b_1 z \quad \text{et} \quad y = mx + b_2 z.$$

Lorsqu'on résout les équations simultanément pour trouver leur intersection, on obtient

$$z = 0 \quad \text{et} \quad y = mx.$$

Puisqu'on ne peut pas avoir $x = y = z = 0$, on doit avoir $x \neq 0$. Par conséquent, en divisant par x on obtient que l'intersection des deux droites est

$$(x : mx : 0) = (1 : m : 0).$$

De même, si $x = c_1$ et $x = c_2$ sont deux droites verticales, elles s'intersectent au point $(0 : 1 : 0)$. Il s'agit d'un des points à l'infini de $\mathbf{P}^2_K$.

Regardons maintenant la courbe elliptique E donnée par $y^2 = x^3 + ax + b$. Sa forme homogène est $y^2 z = x^3 + axz^2 + bz^3$. Les points (x, y) sur la courbe originale correspondent aux points $(x : y : 1)$ sur la version projective. Pour voir quels sont les points sur E qui se situent à l'infini, on pose $z = 0$ et on obtient $0 = x^3$. Par conséquent, $x = 0$ et y peut être n'importe quel nombre non nul. En divisant par y on obtient que $(0 : y : 0) = (0 : 1 : 0)$ est le seul point à l'infini sur E. Comme on l'a vu ci-dessus, le point $(0 : 1 : 0)$ se trouve sur toutes les droites verticales, de sorte que chaque droite verticale intersecte E en ce point à l'infini. De plus, étant donné que $(0 : 1 : 0) = (0 : -1 : 0)$, le "haut" et le "bas" de l'axe des y sont les mêmes.

1.2.4 Points de torsion

Soient E une courbe elliptique définie sur K et n un entier strictement positif. L'ensemble des points de n-torsion est définie par

$$E[n] = \{P \in E(\overline{K}) \mid [n]P = O\},$$

où $\overline{K}$ est une clôture algébrique de K. Soulignons que $E[n]$ contient des points de coordonnées dans $\overline{K}$, et pas seulement dans K.

On s'intéresse au cas de la caractéristique différente de 2. Dans ce cas, on a vu (équation (1.2)) que E peut être mise sous la forme $y^2 =$ une cubique, il est donc facile de déterminer $E[2]$. Soit

$$y^2 = (x-e_1)(x-e_2)(x-e_3),$$

avec e_1, e_2, $e_3 \in \overline{K}$. Un point P satisfait $[2]P = O$ si et seulement si la droite tangente à P est verticale, ce qui veut dire que $y = 0$, donc

$$E[2] = \{O, (e_1,0), (e_2,0), (e_3,0)\}.$$

Proposition 1.2.2. *[38, Proposition 3.1] Soit E une courbe elliptique sur K. Si la caractéristique de K est différente de* 2*, alors*

$$E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Si la caractéristique de K est 2*, alors*

$$E[2] \simeq (0) \quad ou \quad \mathbb{Z}/2\mathbb{Z}.$$

La situation générale est donnée par le théorème suivant.

Théorème 1.2.3. *[38, Théorème 3.2] Soient E une courbe elliptique définie sur K et n un entier strictement positif. Si la caractéristique de K ne divise pas n, ou si elle est égale à* 0*, alors*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Si la caractéristique de K est $p > 0$ et $p|n$, on écrit $n = p^r n'$ avec $p \nmid n'$, alors

$$E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \quad ou \quad E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}.$$

1.2.5 Courbes elliptiques sur un corps fini

Soient F un corps fini et E une courbe elliptique définie sur F. Puisque il n'existe qu'un nombre fini de paires (x,y) avec x, $y \in F$, le groupe $E(F)$ est fini. Plusieurs propriétés de ce groupe, par

exemple, son ordre, se révèlent importantes dans de nombreux contextes. Dans cette section on donnera deux résultats dont on aura besoin dans les chapitres suivants.

Lemme 1.2.1. *[12, Lemme 2.1] Soit R un point d'une courbe elliptique E définie sur le corps fini $\mathbb{F}_p$, où p est un nombre premier différent de 2. Soient m et n des entiers, alors*

$$[m]R = [n]R \iff m \equiv n \ mod \ ord(R).$$

Théorème 1.2.4. *[38, Théorème 4.1] Soient q une puissance d'un nombre premier et E une courbe elliptique définie sur le corps fini $\mathbb{F}_q$, alors*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \quad ou \quad \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

pour un certain entier $n \geq 1$, ou pour certains entiers n_1, $n_2 \geq 1$ avec n_1 divisant n_2.

CHAPITRE 2

QUELQUES ÉLÉMENTS SUR LES SUITES RÉCURRENTES LINÉAIRES, LES MATRICES ET LES PÉRIODES (LE CAS FIBONACCI)

2.1 Suites récurrentes linéaires d'ordre N

Soit $(N, n_0) \in \mathbb{N}^\star \times \mathbb{N}$, une suite récurrente linéaire d'ordre N à valeur dans un corps commutatif K est définie, pour tout $n \geq n_0$, par la relation de récurrence suivante :

$$u_{n+N} = a_{N-1}u_{n+N-1} + \cdots + a_1 u_{n+1} + a_0 u_n, \tag{2.1}$$

où a_0, a_1, …, a_{N-1} sont des scalaires fixés de K avec $a_0 \neq 0$. Une telle suite est entièrement déterminée par la donnée des N premiers termes $u_{n_0}, u_{n_0+1}, \ldots, u_{n_0+N-1}$ de la suite et par la relation de récurrence (2.1). A une telle suite $(u_n)_n$ on associe le polynôme $F(x)$ de degré N suivant :

$$F(x) = x^N - \sum_{i=0}^{N-1} a_i x^i. \tag{2.2}$$

Le polynôme $F(x)$ est appelé *polynôme caractéristique associé à la suite* $(u_n)_n$.

La relation (2.1) peut être écrite sous forme matricielle comme suit :

$$U_{n+1} = TU_n, \qquad (n \geq 0), \tag{2.3}$$

avec

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{N-1} \end{pmatrix}, \qquad U_n = \begin{pmatrix} u_{n_0+n} \\ u_{n_0+n+1} \\ \vdots \\ u_{n_0+n+N-2} \\ u_{n_0+n+N-1} \end{pmatrix}.$$

La matrice T est appelé *matrice compagnon du polynôme* $F(x)$, ou bien, *matrice compagnon de la suite* $(u_n)_n$, et le polynôme $F(x)$ est le polynôme caractéristique de la matrice T qui est aussi son polynôme minimal. En fait, nous avons le théorème suivant :

Théorème 2.1.1. *[19, Théorème 3.3.14] Tout polynôme unitaire est à la fois le polynôme minimal*

et le polynôme caractéristique de sa matrice compagnon.

Supposons maintenant que les scalaires a_0, a_1, …, a_{N-1} ainsi que les N premiers termes de la suites $(u_n)_n$ sont entiers et soit $m \geq 2$ un entier. Puisque l'anneau $\mathbb{Z}/m\mathbb{Z}$ est fini, la suite $(u_n \bmod m)_n$ est périodique à partir d'un certain rang, ce qui revient au même de dire que la suite $(U_n \bmod m)_n$ est périodique à partir d'un certain rang. En fait, comme on vient de voir que les identités (2.1) et (2.3) définissent la même suite, on utilisera, selon notre besoin, l'une ou l'autre de ces deux identités.

On dit que la suite $(u_n)_n$ est *simplement périodique modulo m*, ou que la suite $(u_n \bmod m)_n$ est *simplement périodique*, si elle est périodique et qu'elle revient à son premier terme, c'est-à-dire, s'il existe un entier $k > 0$ tel que :

$$u_{k+i} \equiv u_i \bmod m, \qquad \text{avec } \; n_0 \leq i \leq n_0 + N - 1, \tag{2.4}$$

ou

$$U_k \equiv U_0 \bmod m. \tag{2.5}$$

On note par $k(u_{n_0}, \ldots, u_{n_0+N-1}; m)$ la période de la suite $(u_n \bmod m)_n$, i.e., le plus petit entier strictement positif k vérifiant (2.4). Un entier $k \in \mathbb{N}^\star$ vérifie (2.4) si, et seulement si, k est multiple de $k(u_{n_0}, \ldots, u_{n_0+N-1}; m)$, voir [34].

On aura besoin du lemme suivant dans les prochains chapitres. Pour simplifier les notations, on pose $v = k(u_{n_0}, \ldots, u_{n_0+N-1}; m)$. Notons que la matrice compagnon ne dépend pas des conditions initiales.

Lemme 2.1.1. *Soit $m \geq 2$ un entier. Si $\det T$ est inversible modulo m, alors la suite $(u_n \bmod m)_n$ est simplement périodique.*

Démonstration. Puisque la suite $(u_n \bmod m)_n$ est périodique, alors pour un certain entier l, on aura

$$U_{l+v} \equiv U_l \bmod m,$$

en outre $U_{l+v} = T^l U_v$ et $U_l = T^l U_0$, donc cette dernière congruence devient

$$T^l U_v \equiv T^l U_0 \bmod m.$$

Lorsque $\det T$ est inversible modulo m, on obtient

$$U_v \equiv U_0 \bmod m.$$

□

Vince [34] a étudié les périodes de suites récurrentes linéaires modulo un idéal premier dans le cas général. On donne ici un de ses résultat dont on aura besoin dans les chapitres suivants. Soit p un nombre premier, le polynôme $F(x)$ s'écrit dans le corps fini $\mathbb{F}_p$ comme suit

$$F = F_1^{e_1} F_2^{e_2} \cdots F_\rho^{e_\rho}$$

où chaque F_i est irréductible sur $\mathbb{F}_p$. Soit f_i le degré du polynôme F_i dans cette factorisation et soit b_i le terme constant de F_i. On note par τ_i l'ordre multiplicatif de $(b_i)(-1)^{f_i}$ dans le corps $\mathbb{F}_p$.

Proposition 2.1.2. *[34, Corollaire 3] Soit s l'unique entier vérifiant $p^s \geq \max e_i > p^{s-1}$, alors*

$$k(u_{n_0}, \ldots, u_{n_0+N-1}; p) | p^s ppcm[\tau_i(p^{f_i} - 1)/(p-1)].$$

On aura aussi besoin du lemme suivant qui est un cas particulier du Lemme 2 dans [34], où l'on a posé $v(m) = k(u_{n_0}, \ldots, u_{n_0+N-1}; m)$.

Lemme 2.1.2. *Soit $m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}$ la factorisation de m en produit de nombres premiers, alors*

$$v(m) = \text{ppcm}\left(v\left(p_1^{r_1}\right), v\left(p_2^{r_2}\right), \ldots, v\left(p_s^{r_s}\right)\right).$$

2.2 Matrices circulantes

Dans les prochains chapitres on aura besoins de certaines propriétés des matrices circulantes qu'on va présenter dans cette section, pour plus de détails sur les propriétés de ces matrices, voir [5, 13, 16].

Une *matrice circulante* est une matrice carrée, à coefficients dans le corps des nombres complexes $\mathbb{C}$, dans laquelle on passe d'une ligne à la suivante par permutation circulaire (décalage vers

la droite) des coefficients. C'est donc une matrice de taille n de la forme

$$W_n = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & & & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{pmatrix}.$$

La *matrice circulante standard* π_n est la matrice de taille n suivante

$$\pi_n = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

qui est également appelé la *matrice de permutation vers l'avant*.

Toute matrice circulante s'exprime comme un polynôme en π_n, en effet

$$W_n = \sum_{k=0}^{n-1} c_k \pi_n^k. \tag{2.6}$$

La matrice π_n a des valeurs propres distinctes qui sont les racines n-ième de l'unité $e^{2i\pi k/n}$, pour $k = 0, 1, \ldots, n-1$. Les valeurs propres de W_n sont alors

$$\lambda_j = \sum_{k=0}^{n-1} c_k e^{2i\pi kj/n}, \qquad 0 \leq j \leq n-1. \tag{2.7}$$

Ces valeurs propres ne sont pas nécessairement distinctes.

On note par $w_n = \det W_n$ le déterminant de la matrice circulante W_n, on a alors

$$w_n = \prod_{j=0}^{n-1} \lambda_j. \tag{2.8}$$

2.3 Périodes de Suites de Fibonacci et courbes elliptiques

La suite de Fibonacci modulo un entier $m \geq 2$ a été étudiée par plusieurs auteurs. Nous nous sommes intéressés en particulier aux travaux de Coleman et *al* [12] et à certains résultats des travaux de Vinson [35] et Wall [37] que nous allons résumer dans cette section. Considérons d'abord la suite de Fibonacci $(F_n)_n$ donnée par

$$\begin{cases} F_0 = 0,\ F_1 = 1, \\ F_n = F_{n-1} + F_{n-2}, \ \ (n \geq 2). \end{cases}$$

Cette suite calculée modulo un entier $m \geq 2$ est simplement périodique, comme on peut le voir d'après le Lemme 2.1.1. Le théorème suivant contient quelques-unes des propriétés fondamentales connues sur les périodes de la suite de Fibonacci modulo un entier $m \geq 2$. Dans toute la suite de ce chapitre, on notera par $k(m) = k(0,1;m)$ la période de la suite $(F_n \bmod m)_n$.

Théorème 2.3.1. *[12, Théorème 1]*

(a) *Si p est un nombre premier et $p \equiv \pm 1$ mod 10, alors $k(p)|(p-1)$.*

(b) *Si p est un nombre premier et $p \equiv \pm 3$ mod 10, alors $k(p)|2(p+1)$.*

(c) *Si $m = \prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de m, alors $k(m) = \mathrm{ppcm}\big(k(p_i^{e_i})\big)$.*

(d) *Si $n|m$, alors $k(n)|k(m)$.*

(e) *Si $m > 2$ et n est le plus petit entier strictement positif tel que n est pair et $m|F_n$ ou n est impair et $m|F_{n-1} + F_{n+1}$, alors $k(m) = 2n$.*

Le théorème suivant donne tous les indices n pour lesquels F_n est congru à 0 mod m.

Théorème 2.3.2. *[37, Théorème 3] Les indices des termes F_n pour lesquels $F_n \equiv 0$ mod m forment une progression arithmétique simple. C'est-à-dire, $n = xd$, pour $x = 0,1,2,\ldots$ et un certain nombre entier strictement positif $d = d(m)$, donne tous les n vérifiant $F_n \equiv 0$ mod m.*

D'après le Théorème 2.3.2, on voit que $d(m)$ est le plus petit entier strictement positif k pour lequel $F_k \equiv 0 \bmod m$. On a

$$F_n \equiv 0 \bmod m \iff d(m)|n.$$

En particulier, puisque $F_{k(m)} \equiv F_0 \equiv 0 \bmod m$, on a

$$d(m)|k(m).$$

On définit une fonction $l(m)$ par l'équation $d(m)l(m) = k(m)$. On note que $l(m)$ est un entier pour tout m, c'est le nombre de zéros dans la période de la suite $(F_n)_n$ modulo m.

Théorème 2.3.3. *[35, Théorème 1] Pour $m > 2$, on a*

i) $l(m) = 1$ *ou* 2 *si* $d(m)$ *est pair, et*

ii) $l(m) = 4$ *si* $d(m)$ *est impair.*

De plus, $l(1) = l(2) = 1$. *Inversement,* $l(m) = 4$ *implique* $d(m)$ *est impair,* $l(m) = 2$ *implique* $d(m)$ *est pair, et* $l(m) = 1$ *implique* $d(m)$ *est pair ou* $m = 1$ *ou* 2.

Considérons maintenant la (a,b)-suite de Fibonacci $(G_n)_n$ donnée par

$$\begin{cases} G_0 = a,\ G_1 = b, \\ G_n = G_{n-1} + G_{n-2},\ \ (n \geq 2). \end{cases}$$

La proposition suivante contient quelques propriétés de la suite $(G_n)_n$.

Proposition 2.3.4. *[12, Proposition 2] Soient a, b et m des entiers avec $m \geq 2$.*

(a) *La (a,b)-suite de Fibonacci $(G_n)_n$ satisfait*

$$G_n = aF_{n-1} + bF_n, \quad (n \geq 0).$$

(b) *La (a,b)-suite de Fibonacci modulo m est simplement périodique.*

La proposition suivante contient quelques propriétés des périodes des (a,b)-suites de Fibonacci modulo un entier $m \geq 2$.

Proposition 2.3.5. *[12, Proposition 3] Soit $m \geq 2$ un entier.*

(a) $k(0,b;m) = k(b,0;m)$ *et* $k(0,b;m)|k(m)$.

(b) *Si* $pgcd(b,m) = 1$, *alors* $k(0,b;m) = k(m)$.

(c) $k(a,b;m) | ppcm(k(a,0;m), k(0,b;m))$.

Le théorème suivant nous dit quand et pour quels entiers m on a $k(m) = k(a,b;m)$

Théorème 2.3.6. *[37, Théorème 12] Soient a, b et m des entiers tels que* $\text{pgcd}(a,b,m) = 1$ *et supposons que* $m = p^e$ *pour un nombre premier impair* $p \neq 5$ *et un entier e strictement positif. Si* $k(a,b;m)$ *est pair, alors* $k(a,b;m) = k(m)$.

Soit $m \geq 2$ un entier, on définit une relation d'équivalence sur l'ensemble $(\mathbb{Z}/m\mathbb{Z})^2$ comme suit : on dit que (q,r) est équivalent à (a,b) si q et r (modulo m) apparaissent comme des termes consécutifs dans la (a,b)-suite de Fibonacci modulo m. Puisque deux termes consécutifs déterminent complètement la (a,b)-suite de Fibonacci, il s'agit bien d'une relation d'équivalence sur $(\mathbb{Z}/m\mathbb{Z})^2$.

La taille d'une classe d'équivalence contenant (a,b) est $k(a,b;m)$. On définit $c_d(m)$ comme étant le nombre de classes d'équivalence distinctes de taille d. Les petites classes d'équivalence sont décrites dans la proposition suivante.

Proposition 2.3.7. *[12, Proposition 4] Soit* $m \geq 2$ *un entier.*

(a) $c_1(m) = 1$.

(b) $c_2(m) = 0$.

(c) *Si m est pair, alors* $c_3(m) = 1$, *sinon* $c_3(m) = 0$.

(d) *Si* $5 \nmid m$, *alors* $c_4(m) = 0$. *Si* $5 | m$, *alors* $c_4(m) = 1$, *et* 0 *n'apparaît pas comme un terme dans la période.*

Tandis que la Proposition 2.3.7 donne des informations sur $c_d(m)$ pour des petites valeurs de d, on va considérer d'autres cas, d'une manière générale. Tout d'abord, observons que si $x_1, x_2, \ldots, x_d$ est une période de la (x_1,x_2)-suite de Fibonacci modulo m, alors

$$x_1 + x_2 \equiv x_3 \bmod m, \;\; x_2 + x_3 \equiv x_4 \bmod m, \ldots, \; x_d + x_1 \equiv x_2 \bmod m.$$

Ainsi, on obtient

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & & \vdots & & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{d-1} \\ x_d \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \mod m.$$

On définit la matrice circulante de Fibonacci W_n^{Fib}, par la matrice de taille n suivante :

$$W_n^{Fib} = \begin{pmatrix} 1 & 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & -1 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

On note par $w_n^{Fib} = \det W_n^{Fib}$ le déterminant de la matrice circulante de Fibonacci.

Proposition 2.3.8. *[12, Proposition 5] Soit w_n^{Fib} le déterminant de la matrice circulante de Fibonacci.*

(a) $|w_n^{Fib}| = (-1)^{n-1} \prod_{j=0}^{n-1} \left(1 + e^{(2i\pi j)/n} - e^{(4i\pi j)/n}\right)$.

(b) $|w_n^{Fib}| = (-1)^{n-1} - 1 + F_{n+1} + F_{n-1}$.

(c) *Si n est impair, alors $|w_n^{Fib}| = F_{n+1} + F_{n-1} = L_n$ où L_n est le n-ième nombre de Lucas. De plus, si $n \equiv 0$ mod 4, alors $|w_n^{Fib}| = 5F_{n/2}^2$ et si $n \equiv 2$ mod 4, alors $|w_n^{Fib}| = L_{n/2}^2$.*

On peut maintenant énoncer la pertinence de la suite $\left(|w_n^{Fib}|\right)_n$ sur la période de la suite de Fibonacci modulo m.

Théorème 2.3.9. *[12, Théorème 6] Soient a, b et m des entiers tels que $m \geq 2$ et $(a,b) \not\equiv (0,0)$ mod m. Si $c = k(a,b;m)$, alors pgcd $\left(|w_c^{Fib}|, m\right) > 1$.*

Le théorème suivant compte les éléments de $(\mathbb{Z}/m\mathbb{Z})^2$ correspondant à la partition de cet ensemble en classes d'équivalence.

Théorème 2.3.10. *[12, Théorème 7] Soient $m \geq 2$ un entier et $c_d(m)$ le nombre de classes d'équivalence distinctes de taille d, alors*

$$m^2 = \sum_{d|k(m)} d \cdot c_d(m).$$

La proposition suivante nous donne toutes les valeurs de $c_d(p)$ pour une certaine classe de nombres premiers p.

Proposition 2.3.11. *[12, Proposition 9] Si p est un nombre premier tel que $p \equiv 3$ ou 7 modulo 20 et $k(p) = 2(p+1)$, alors $c_0(p) = 1, c_{2(p+1)} = (p-1)/2$ et $c_d(p) = 0$ pour tous les autres d.*

On va définir maintenant une suite de Fibonacci sur une courbe elliptique E. Dans toute la suite de cette thèse, on désignera par E une courbe elliptique donnée par une équation de la forme $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{F}_p$, où p est un nombre premier différent de 2. On posera

$$E(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + ax + b\} \cup \{O\},$$

et on notera par $h = ord(E(\mathbb{F}_p))$ l'ordre du groupe $E(\mathbb{F}_p)$ et par $h_R = ord(R)$ l'ordre de tout point $R \in E(\mathbb{F}_p)$.

Soient A et B deux points de $E(\mathbb{F}_p)$. On définit la (A,B)-suite de Fibonacci $(H_n)_n$ par :

$$\begin{cases} H_0 = A,\ H_1 = B, \\ H_n = H_{n-1} + H_{n-2}, \quad (n \geq 2). \end{cases}$$

La proposition suivante nous donne quelques propriétés de la suite $(H_n)_n$.

Proposition 2.3.12. *[12, Proposition 10] Soient A et B deux points de $E(\mathbb{F}_p)$.*

(a) *La (A,B)-suite de Fibonacci $(H_n)_n$ est donnée par*

$$H_n = [F_{n-1}]A + [F_n]B, \qquad (n \geq 0).$$

(b) *La (O,B)-suite de Fibonacci est donnée par $H_n = [F_n]B$, avec $n \geq 0$.*

(c) *La (A,B)-suite de Fibonacci $(H_n)_n$ est simplement périodique.*

On note par $K(A,B;E)$ la période de la (A,B)-suite de Fibonacci $(H_n)_n$. La proposition suivante fait le lien entre les périodes de la suite de Fibonacci définie sur une courbe elliptique et les périodes de la suite de Fibonacci ordinaire.

Théorème 2.3.13. *[12, Théorème 12] Soient A et B deux points de $E(\mathbb{F}_p)$, alors*

(a) $K(O,B;E) = K(B,O;E) = k(h_B)$.

(b) $K(A,B;E) | ppcm(K(A,O;E), K(O,B;E))$.

(c) $K(A,B;E) | k(h)$.

Puisqu'on a $k(h_B) = K(O,B;E)$, certaines propriétés de la suite ordinaire de Fibonacci peuvent être transférées à des propriétés analogues pour les (O,B)-suites de Fibonacci sur une courbe elliptique.

Théorème 2.3.14. *[12, Théorème 13] Soient A et B deux point de $E(\mathbb{F}_p)$.*

(a) *Si h_B est un nombre premier tel que $h_B \equiv \pm 1$ mod 10, alors $K(O,B;E) | (h_B - 1)$.*

(b) *Si h_B est un nombre premier tel que $h_B \equiv \pm 3$ mod 10, alors $K(O,B;E) | 2(h_B + 1)$.*

(c) *Si $\prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de h_B, alors on a $K(O,B;E) = \text{ppcm}\big(k(p_i^{e_i})\big)$.*

(d) *Si $h_A | h_B$, alors $K(O,A;E) | K(O,B;E)$.*

On donne maintenant la notion analogue d'une classe d'équivalence pour les suites définies sur les courbes elliptiques. Soient A, A', B et B' des points de $E(\mathbb{F}_p)$. On dit que (A',B') est équivalent à (A,B) si A' et B' apparaissent comme des termes consécutifs dans la (A,B)-suite de Fibonacci. On sait que la taille d'une classe d'équivalence contenant (A,B) est $K(A,B;E)$. On note par $C_d(E)$ le nombre de classes d'équivalence distinctes de taille d.

Théorème 2.3.15. *[12, Théorème 14] Soient A et B des points de $E(\mathbb{F}_p)$ et w_c^{Fib} les déterminants des matrices circulantes de Fibonacci.*

(a) $C_1(E) = 1$.

(b) $C_2(E) = 0$.

(c) *Si* $c = K(A,B;E)$*, alors* $pgcd\left(|w_c^{Fib}|,h\right) > 1$.

Finalement, nous avons un théorème analogue au Théorème 2.3.10.

Théorème 2.3.16. *[12, Théorème 15] Soit* $C_d(E)$ *défini comme ci-dessus, alors*

$$h^2 = \sum_{d|k(h)} d \cdot C_d(E).$$

CHAPITRE 3

PÉRIODES DES SUITES DE MORGAN-VOYCE ET COURBES ELLIPTIQUES

Dans ce chapitre, on étudie la suite de Morgan-Voyce $(M_n)_n$ qui est une suite récurrente linéaire d'ordre 2 définie par

$$\begin{cases} M_1 = 1,\ M_2 = 1+t+s, \\ M_n = (2+t)M_{n-1} - M_{n-2}, \ \ (n \geq 3). \end{cases}$$

Puisqu'on est intéressé par les périodes de la suite de Morgan-Voyce modulo un entier $m \geq 2$, on suppose que s et t sont entiers. La matrice compagnon de la suite de Morgan-Voyce est $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 2+t \end{smallmatrix}\right)$. Cette matrice est de déterminant 1, elle est donc inversible modulo tout entier $m \geq 2$. On en déduit, d'après le Lemme 2.1.1, que la suite $(M_n)_n$ modulo m est simplement périodique.

On commence par le cas $s = 1$. Dans ce cas, les deux premiers termes de notre suite sont $M_1 = 1$ et $M_2 = 2+t$. On peut définir, à partir de la relation de récurrence, le terme $M_0 = (2+t)M_1 - M_2 = 0$. Ainsi, dans ce qui suit, on désignera par $(M_n)_n$ la suite de Morgan-Voyce de valeurs initiales $M_0 = 0$ et $M_1 = 1$. On note par $k(m)$ la période de la suite $(M_n)_n$ modulo m, i.e., le plus petit entier strictement positif k tel que $M_k \equiv 0 \bmod m$ et $M_{k+1} \equiv 1 \bmod m$.

3.1 La suite de Morgan-Voyce

On commence par donner quelques propriétés de la suite $(M_n)_n$ fort utiles pour la suite de notre travail.

Proposition 3.1.1. *On a les identités suivantes*

(a) $M_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n-k-1}{k} (2+t)^{n-2k-1}$, $(n \geq 1)$,

(b) $M_n^2 - M_{n-1}M_{n+1} = 1$, $(n \geq 1)$,

(c) $M_n = \sum_{k=0}^{n-1} \binom{n+k}{2k+1} t^k$, $(n \geq 1)$,

(d) $M_{n-1}M_n - M_{n-2}M_{n+1} = 2+t = M_2$, $(n \geq 2)$,

(e) $M_{n+g} = M_{n+1}M_g - M_nM_{g-1}$, $(g \geq 1, n \geq 0)$,

(f) $M_{2n} = M_n(M_{n+1} - M_{n-1})$, $(n \geq 1)$,

(g) $M_{2n+1} = M_n(M_{n+2} - M_n) + 1, \qquad (n \geq 0),$

(h) $M_{n-1}^2 - (2+t)M_{n-1}M_n + M_n^2 = 1, \qquad (n \geq 1),$

(i) Pour $\alpha = (2+t+\sqrt{\Delta})/2, \beta = (2+t-\sqrt{\Delta})/2$ *où* $\Delta = t^2+4t$, *on a*

$$\alpha\beta = 1 \qquad et \qquad (\alpha-\beta)M_n = (\alpha^n - \beta^n), \quad (n \geq 0),$$

(j) $M_{n+1} - M_{n-1} = \alpha^n + \beta^n, \qquad (n \geq 1),$

(k) $M_{n+1} - M_{n-1} = \sum_{k=0}^{n} \frac{2n}{n+k}\binom{n+k}{n-k}t^k, \qquad (n \geq 1).$

Démonstration. (h) découle de (b), (g) s'obtient par récurrence en utilisant (b) et (f), utiliser (c) pour (k). (d) peut être vérifiée directement à l'aide de (b), en effet

$$\begin{aligned} M_{n-1}M_n &= M_{n-1}\left[(2+t)M_{n-1} - M_{n-2}\right] \\ &= (2+t)M_{n-1}^2 - M_{n-1}M_{n-2} \end{aligned}$$

et

$$\begin{aligned} M_{n-2}M_{n+1} &= M_{n-2}\left[(2+t)M_n - M_{n-1}\right] \\ &= (2+t)M_{n-2}M_n - M_{n-2}M_{n-1}, \end{aligned}$$

d'où

$$\begin{aligned} M_{n-1}M_n - M_{n-2}M_{n+1} &= (2+t)(M_{n-1}^2 - M_{n-2}M_n) \\ &= (2+t). \end{aligned}$$

Pour (a) voir [7], pour (b), (c), (e) et (f), on peut voir [32], pour (i) et (j) on peut voir [17]. □

Remarque 2. Si $t \notin \{0, -4\}$, alors (i) implique

$$M_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad (n \geq 0). \tag{3.1}$$

Si $t = 0$, alors $M_n = n$ pour tout $n \geq 0$ et si $t = -4$, alors $M_n = (-1)^{n+1}n$ pour tout $n \geq 0$.

Soit $F(x) = x^2 - (2+t)x + 1$ le polynôme caractéristique de la suite $(M_n)_n$.

Théorème 3.1.2. *Soit $p \neq 2$ un nombre premier.*

(a) Si $F(x)$ a deux racines distinctes modulo p, alors $k(p)|(p-1)$.

(b) Si $F(x)$ est irréductible modulo p, alors $k(p)|(p+1)$.

(c) Si $F(x)$ a une racine double modulo p, alors $k(p)|2p$[1].

Démonstration. Conséquence de la Proposition 2.1.2, en effet

(a) Si $F(x)$ a deux racines distinctes modulo p, alors on est dans le cas $f_1 = f_2 = e_1 = e_2 = 1$, $s = 0$ et $\tau_i|(p-1)$ pour $i = 1,\ 2$. D'après la Proposition 2.1.2, on obtient $k(p)|(p-1)$.

(b) Si $F(x)$ est irréductible modulo p, alors on est dans le cas $f_1 = 2$, $e_1 = 1$, $s = 0$ et $\tau_1 = 1$, donc, d'après la Proposition 2.1.2, on obtient $k(p)|(p+1)$.

(c) Si $F(x) \equiv (x-b_1)^2 \bmod p$, alors on est dans le cas $f_1 = 1$, $e_1 = 2$, $s = 1$ et puisque $b_1^2 \equiv 1 \bmod p$, alors $\tau_1|2$. D'après la Proposition 2.1.2, on obtient $k(p)|2p$.

□

Lemme 3.1.1. *Soit $p \neq 2$ un nombre premier, alors*

$$F(x) \equiv 0 \ mod\ p \iff (2x-(2+t))^2 \equiv t^2+4t \ mod\ p.$$

Démonstration. Soit $p \neq 2$ un nombre premier, alors

$$\begin{aligned} (2x-(2+t))^2 \equiv t^2+4t \bmod p &\iff 4(x^2-(2+t)x+1) \equiv 0 \bmod p \\ &\iff F(x) \equiv 0 \bmod p. \end{aligned}$$

□

Lemme 3.1.2. *Soit $p \neq 2$ un nombre premier, alors $F(x)$ a une racine double modulo p si et seulement si $t^2+4t \equiv 0\ mod\ p$.*

[1] Dans la référence [4] nous n'avons pas explicité que $k(p)|2p$, on a juste précisé que $k(p)|p(p-1)$.

Démonstration. Soit $p \neq 2$ un nombre premier, alors

$$t^2+4t \equiv 0 \bmod p \iff (t+2)^2 \equiv 4 \bmod p \iff t+2 \equiv \pm 2 \bmod p,$$

dans ce cas, on a

$$F(x) = x^2-(2+t)x+1 \equiv (x \pm 1)^2 \bmod p.$$

□

Théorème 3.1.3. *Soient $p \neq 2$ un nombre premier et $m \geq 2$ un entier.*

(a) Si t^2+4t est un résidu quadratique modulo p, alors $k(p)|(p-1)$.

(b) Si t^2+4t est un non résidu quadratique modulo p, alors $k(p)|(p+1)$.

(c) Si $p|(t^2+4t)$, alors $k(p)|2p$.

(d) Si $m = \prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de m, alors on a $k(m) = \text{ppcm}\left(k\left(p_i^{e_i}\right)\right)$.

(e) Si $n|m$, alors $k(n)|k(m)$.

Démonstration. (a), (b) et (c) sont des conséquences du Théorème 3.1.2 et des Lemmes 3.1.1 et 3.1.2. Pour (d), supposons que $m = \prod p_i^{e_i}$. Puisque les $p_i^{e_i}$ sont deux à deux premiers entre eux, on a

$$\begin{aligned} M_k \equiv 0[m] \text{ et } M_{k+1} \equiv 1[m] &\iff m|M_k \text{ et } m|(M_{k+1}-1) \\ &\iff p_i^{e_i}|M_k \text{ et } p_i^{e_i}|(M_{k+1}-1) \text{ pour tout } i \\ &\iff M_k \equiv 0\left[p_i^{e_i}\right] \text{ et } M_{k+1} \equiv 1\left[p_i^{e_i}\right] \text{ pour tout } i \\ &\iff k\left(p_i^{e_i}\right)|k \text{ pour tout } i, \end{aligned}$$

le plus petit entier k strictement positif qui satisfait à ces conditions est d'une part $k = k(m)$ et d'autre part $k = \text{ppcm}\left(k\left(p_i^{e_i}\right)\right)$. Pour (e), supposons que $n|m$. Puisque $M_{k(m)} \equiv 0 \bmod m$ et $M_{k(m)+1} \equiv 1 \bmod m$, alors $M_{k(m)} \equiv 0 \bmod n$ et $M_{k(m)+1} \equiv 1 \bmod n$, d'où $k(n)|k(m)$. □

On va décrire, pour certaines valeurs de t, les nombres premiers p pour lesquels $k(p)|(p-1)$ et ceux pour lesquels $k(p)|(p+1)$.

(1) Pour $t = 1$, la suite est définie par $M_n = 3M_{n-1} - M_{n-2}$. Cette suite correspond à A001906 dans l'encyclopédie des suites entières de Sloane [31]. Le polynôme caractéristique est $F(x) = x^2 - 3x + 1$. Ce polynôme a une racine double modulo p seulement pour $p = 5$. Pour $p \notin \{2,5\}$, on a $x^2 - 3x + 1 \equiv 0 \bmod p$ si et seulement si $(2x-3)^2 \equiv 5 \bmod p$. On a vu dans le Chapitre 1 que 5 est un résidu quadratique pour les nombres premiers de la forme $p = 10k \pm 1$ et 5 est un non résidu quadratique pour les nombres premiers de la forme $p = 10k \pm 3$. Ainsi, on obtient $k(2) = 3$ et $k(5) = 10$. Si $p = 10k \pm 1$, alors $k(p)|(p-1)$ et si $p = 10k \pm 3$, alors $k(p)|(p+1)$. Dans le Tableau 3.I, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $10k \pm 1$, ainsi que ses périodes. Dans le Tableau 3.II, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $10k \pm 3$ et ses périodes.

p	$(M_n \bmod p)_n$	$k(p)\|(p-1)$
11	$0,1,3,8,10;0,1$	$k(11) = 5$
19	$0,1,3,8,2,17,11,16,18;0,1$	$k(19) = 9$
29	$0,1,3,8,21,26,28;0,1$	$k(29) = 7$
31	$0,1,3,8,21,24,20,5,26,11,7,10,23,28,30;0,1$	$k(31) = 15$

Tableau 3.I – périodes modulo de petits p de la forme $10k \pm 1$.

p	$(M_n \bmod p)_n$	$k(p)\|(p+1)$
3	$0,1,0,2;0,1$	$k(3) = 4$
7	$0,1,3,1,0,6,4,6;0,1$	$k(7) = 8$
13	$0,1,3,8,8,3,1,0,12,10,5,5,10,12;0,1$	$k(13) = 14$
17	$0,1,3,8,4,4,8,3,1,0,16,14,9,13,13,9,14,16;0,1$	$k(17) = 18$
23	$0,1,3,8,21,9,6,9,21,8,3,1,0,22,20,15,2,14,17,14,2,15,20,22;0,1$	$k(23) = 24$

Tableau 3.II – périodes modulo de petits p de la forme $10k \pm 3$.

(2) Pour $t = 2$, la suite $(M_n)_n$ est définie par $M_n = 4M_{n-1} - M_{n-2}$. Cette suite correspond à A001353 dans [31]. Dans ce cas, $t^2 + 4t = 12$ et d'après (b) de la Proposition1.1.1, on a $(12/p) = (2/p)^2(3/p) = (3/p)$. Le calcul nous donne $k(2) = 2$ et $k(3) = 6$ et on a vu dans le Chapitre 1 que 3 est un résidu quadratique pour les nombres premiers de la forme $12k \pm 1$ et 3 est un non résidu quadratique pour les nombres premiers de la forme $12k \pm 5$, on en déduit que si $p = 12k \pm 1$, alors $k(p)|(p-1)$ et si $p = 12k \pm 5$, alors $k(p)|(p+1)$. Dans le Tableau 3.III, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $12k \pm 1$, ainsi que ses périodes. Dans le Tableau 3.IV, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $12k \pm 5$ et ses périodes.

p	$(M_n \bmod p)_n$	$k(p)\|(p-1)$
11	$0,1,4,4,1,0,10,7,7,10;0,1$	$k(11)=10$
13	$0,1,4,2,4,1,0,12,9,11,9,12;0,1$	$k(13)=12$
23	$0,1,4,15,10,2,21,13,8,19,22;0,1$	$k(23)=11$
37	$0,1,4,15,19,24,3,25,23,30,23,25,3,24,19,15,4,1,0,36,33,22,18,$ $13,34,12,14,7,14,12,34,13,18,22,33,36;0,1$	$k(37)=36$

Tableau 3.III – périodes modulo de petits p de la forme $12k\pm1$.

p	$(M_n \bmod p)_n$	$k(p)\|(p+1)$
5	$0,1,4;0,1$	$k(5)=3$
7	$0,1,4,1,0,6,3,6;0,1$	$k(7)=8$
17	$0,1,4,15,5,5,15,4,1,0,16,13,2,12,12,2,13,16;0,1$	$k(17)=18$
19	$0,1,4,15,18;0,1$	$k(19)=5$
29	$0,1,4,15,27,6,26,11,18,3,23,2,14,25,28;0,1$	$k(29)=15$
31	$0,1,4,15,25,23,5,28,14,28,5,23,25,15,4,1,0,30,27,16,6,8,26,3,17,$ $3,26,8,6,16,27,30;0,1$	$k(31)=32$

Tableau 3.IV – périodes modulo de petits p de la forme $12k\pm5$.

(3) Pour $t=3$, la suite $(M_n)_n$ est donnée par $M_n=5M_{n-1}-M_{n-2}$. Cette suite correspond à A004254 dans [31]. Dans ce cas, $t^2+4t=21$ et d'après (c) du Théorème 3.1.3, on obtient $k(3)|6$ et $k(7)|14$. Après calculs, on trouve $k(2)=3, k(3)=3$ et $k(7)=14$. D'après la Proposition 1.1.1 (b), on a $(21/p)=(3/p)(7/p)$ et en utilisant le Théorème 1.1.4 (b), on obtient que si $p=42k\pm1$, $42k\pm5$, $42k\pm17$, alors $k(p)|(p-1)$ et si $p=42k\pm11$, $42k\pm13$, $42k\pm19$, alors $k(p)|(p+1)$. Dans le Tableau 3.V, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $42k\pm1$, $42k\pm5$ et $42k\pm17$, ainsi que ses périodes. Dans le Tableau 3.VI, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $p=42k\pm11$, $42k\pm13$ et $42k\pm19$, ainsi que ses périodes.

p	$(M_n \bmod p)_n$	$k(p)\|(p-1)$
5	$0,1,0,4;0,1$	$k(5)=4$
17	$0,1,5,7,13,7,5,1,0,16,12,10,4,10,12,16;0,1$	$k(17)=16$
37	$0,1,5,24,4,33,13,32,36;0,1$	$k(37)=9$
41	$0,1,5,24,33,18,16,21,7,14,22,14,7,21,16,18,33,24,5,1,0,40,36,$ $17,8,23,25,20,34,27,19,27,34,20,25,23,8,17,36,40;0,1$	$k(41)=40$

Tableau 3.V – périodes modulo de petits p de la forme $42k\pm1$, $42k\pm5$, $42k\pm17$.

(4) Pour $t=4$, la suite $(M_n)_n$ est définie par $M_n=6M_{n-1}-M_{n-2}$. Cette suite correspond à A001109 dans [31]. Dans ce cas, $t^2+4t=32$ et $(32/p)=(2/p)^5=(2/p)$. Le calcul nous donne

p	$(M_n \bmod p)_n$	$k(p)\|(p+1)$
11	$0,1,5,2,5,1,0,10,6,9,6,10;0,1$	$k(11)=12$
13	$0,1,5,11,11,5,1,0,12,8,2,2,8,12;0,1$	$k(13)=14$
19	$0,1,5,5,1,0,18,14,14,18;0,1$	$k(19)=10$
23	$0,1,5,1,0,22,18,22;0,1$	$k(23)=8$
29	$0,1,5,24,28;0,1$	$k(29)=5$
31	$0,1,5,24,22,24,5,1,0,30,26,7,9,7,26,30;0,1$	$k(31)=16$

Tableau 3.VI – périodes modulo de petits p de la forme $p=42k\pm11$, $42k\pm13$, $42k\pm19$.

$k(2)=2$ et on déduit de la Proposition 1.1.2 que si $p=8k\pm1$, alors $k(p)|(p-1)$ et si $p=8k\pm3$, alors $k(p)|(p+1)$. Dans le Tableau 3.VII, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $8k\pm1$, ainsi que ses périodes. Dans le Tableau 3.VIII, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $8k\pm3$ et ses périodes.

p	$(M_n \bmod p)_n$	$k(p)\|(p-1)$
7	$0,1,6;0,1$	$k(7)=3$
17	$0,1,6,1,0,16,11,16;0,1$	$k(17)=8$
23	$0,1,6,12,20,16,7,3,11,17,22;0,1$	$k(23)=11$
31	$0,1,6,4,18,11,17,29,2,14,20,13,27,25,30;0,1$	$k(31)=15$
41	$0,1,6,35,40;0,1$	$k(41)=5$

Tableau 3.VII – périodes modulo de petits p de la forme $8k\pm1$.

p	$(M_n \bmod p)_n$	$k(p)\|(p+1)$
3	$0,1,0,2;0,1$	$k(3)=4$
5	$0,1,1,0,4,4;0,1$	$k(5)=6$
11	$0,1,6,2,6,1,0,10,5,9,5,10;0,1$	$k(11)=12$
13	$0,1,6,9,9,6,1,0,12,7,4,4,7,12;0,1$	$k(13)=14$
19	$0,1,6,16,14,11,14,16,6,1,0,18,13,3,5,8,5,3,13,18;0,1$	$k(19)=20$
29	$0,1,6,6,1,0,28,23,23,28;0,1$	$k(29)=10$
37	$0,1,6,35,19,5,11,24,22,34,34,22,24,11,5,19,35,6,1,0,36,31,2,18,$ $32,26,13,15,3,3,15,13,26,32,18,2,31,36;0,1$	$k(37)=38$

Tableau 3.VIII – périodes modulo de petits p de la forme $8k\pm3$.

(5) Pour $t=5$, la suite $(M_n)_n$ est donnée par $M_n=7M_{n-1}-M_{n-2}$. Cette suite correspond à A004187 dans [31]. Dans ce cas, on a $k(2)=3$. Puisque $t^2+4t=45$, alors d'après (c) du Théorème 3.1.3, on a $k(3)|6$ et $k(5)|10$. D'après (b) de la Proposition 1.1.1, on a $(45/p)=(3/p)^2(5/p)=(5/p)$. Comme pour le cas $t=1$, si $p=10k\pm1$, alors $k(p)|(p-1)$ et si $p=10k\pm3$, alors $k(p)|(p+1)$. Dans le Tableau 3.IX, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p

de la forme $10k \pm 1$, ainsi que ses périodes. Dans le Tableau 3.X, on donne la suite $(M_n)_n$ modulo de petits nombres premiers p de la forme $10k \pm 3$ et ses périodes.

p	$(M_n \bmod p)_n$	$k(p)\|(p-1)$
11	$0,1,7,4,10;0,1$	$k(11)=5$
19	$0,1,7,10,6,13,9,12,18;0,1$	$k(19)=9$
29	$0,1,7,19,10,22,28;0,1$	$k(29)=7$
31	$0,1,7,17,19,23,18,10,21,13,8,12,14,24,30;0,1$	$k(31)=15$
41	$0,1,7,7,1,0,40,34,34,40;0,1$	$k(41)=10$

Tableau 3.IX – périodes modulo de petits p de la forme $10k \pm 1$.

p	$(M_n \bmod p)_n$	$k(p)\|(p+1)$
7	$0,1,0,6;0,1$	$k(7)=4$
13	$0,1,7,9,4,6,12;0,1$	$k(13)=7$
17	$0,1,7,14,6,11,3,10,16;0,1$	$k(17)=9$
23	$0,1,7,2,7,1,0,22,16,21,16,22;0,1$	$k(23)=12$
37	$0,1,7,11,33,35,27,6,15,25,12,22,31,10,2,4,26,30,36;0,1$	$k(37)=19$

Tableau 3.X – périodes modulo de petits p de la forme $10k \pm 3$.

Notons qu'il existe des cas faciles. Par exemple, si $t = 0$, la suite $(M_n)_n$ est définie par $M_n = n$ pour tout $n \geq 0$. Dans ce cas, il est évident que $k(m) = m$ pour tout $m \geq 2$. Si $t = -1$, la suite est donnée par $M_n = M_{n-1} - M_{n-2}$. Dans ce cas, il est facile de voir que $k(2) = 3$ et $k(p) = 6$ pour tout $p \neq 2$. En effet, on a $M_0 = 0$, $M_1 = 1$, $M_2 = 1$, $M_3 = 0$, $M_4 = -1$, $M_5 = -1$, $M_6 = 0$, $M_7 = 1$, …. En fait, en utilisant le Théorème 3.1.3, on obtient $k(3)|6$, si $p = 12k+1$ ou $p = 12k-5$, alors $k(p)|(p-1)$ et si $p = 12k-1$ ou $p = 12k+5$, alors $k(p)|(p+1)$.

Le théorème suivant est un analogue au Théorème 2.3.2 pour le cas Morgan-Voyce.

Théorème 3.1.4. *Les indices des termes M_n pour lesquels $M_n \equiv 0$ mod m forment une progression arithmétique simple. C'est-à-dire, $n = xd$, pour $x = 0,1,2,\ldots$ et un certain nombre entier strictement positif $d = d(m)$, donne tous les n vérifiant $M_n \equiv 0$ mod m.*

Démonstration. La Proposition 3.1.1 (b) nous donne $\text{pgcd}(M_n, M_{n+1}) = 1$. De cette dernière avec la Proposition 3.1.1 (e) on obtient que si $M_i \equiv 0 \bmod m$ et $M_j \equiv 0 \bmod m$ alors

$$M_{i+j} \equiv 0 \bmod m, \tag{3.2}$$

et (avec $i \geq j$)

$$M_{i-j} \equiv 0 \bmod m. \tag{3.3}$$

En effet, la congruence (3.2) est obtenue en posant $n = i$ et $g = j$. En posant $n+g = i$ et $n = j$, on obtient $M_{j+1}M_g = M_i + M_j M_{g-1} \equiv 0 \bmod m$, donc $M_{j+1}M_{i-j} \equiv 0 \bmod m$. Cette dernière congruence avec $\text{pgcd}(M_j, M_{j+1}) = 1$ et $M_j \equiv 0 \bmod m$ donnent la congruence (3.3). Maintenant, l'ensemble S des entiers strictement positifs k satisfaisant $M_k \equiv 0 \bmod m$ n'est pas vide puisqu'il contient $k(m)$. Soit d le plus petit de ces entiers et soit α un autre entier quelconque de S. Supposons que $d \nmid \alpha$, alors il va exister deux entiers positifs β et γ tels que $\alpha = \beta d + \gamma$ avec $0 < \gamma < d$. Des congruences (3.2) et (3.3) on obtient $M_{\alpha-\beta d} \equiv 0 \bmod m$, c'est-à-dire $M_\gamma \equiv 0 \bmod m$, ce qui contredit la minimalité de d. On en déduit que α est un multiple de d. Finalement, la congruence (3.2) nous dit que les indices n qui nous intéressent sont de la forme $n = xd$ avec $x = 0, 1, 2, \ldots$ et $d > 0$. □

Vinson [35] a déterminé le nombre de zéros dans la période de la suite de Fibonacci modulo m. Nous suivons la même méthode pour le cas Morgan-Voyce.

D'après le Théorème 3.1.4, on voit que $d(m)$ est le plus petit entier strictement positif k pour lequel $M_k \equiv 0 \bmod m$. On a

$$M_n \equiv 0 \bmod m \iff d(m) | n. \tag{3.4}$$

En particulier, puisque $M_{k(m)} \equiv M_0 \equiv 0 \bmod m$, on a

$$d(m) | k(m). \tag{3.5}$$

On définit une fonction $l(m)$ par l'équation $d(m)l(m) = k(m)$. On note que $l(m)$ est un entier pour tout m, c'est le nombre de zéros dans la période de la suite $(M_n)_n$ modulo m.

Pour $t \notin \{0, -4\}$, l'identité (3.1) donne un prolongement naturel de la suite $(M_n)_n$ aux valeurs négatives de n. En utilisant l'identité $\alpha^n \beta^n = 1$, on trouve

$$M_{-n} = -M_n. \tag{3.6}$$

Il est facile de voir que l'identité (3.6) est également valable pour $t \in \{0, -4\}$. De cela, on note que la relation de récurrence $M_n = (2+t)M_{n-1} - M_{n-2}$ est valable pour la suite prolongée.

Supposons maintenant que $t \notin \{0,-4\}$. En résolvant le système

$$\begin{cases} \alpha^k - \beta^k &= (\alpha-\beta)M_k \\ \alpha\cdot\alpha^k - \beta\cdot\beta^k &= (\alpha-\beta)M_{k+1} \end{cases}$$

en α^k et β^k, on obtient

$$\begin{cases} \alpha^k = M_{k+1} - \beta M_k = (2+t)M_k - M_{k-1} - \beta M_k = \alpha M_k - M_{k-1} \\ \beta^k = M_{k+1} - \alpha M_k = (2+t)M_k - M_{k-1} - \alpha M_k = \beta M_k - M_{k-1}, \end{cases}$$

on en déduit que

$$(\alpha-\beta)M_{nk+r} = \alpha^{nk+r} - \beta^{nk+r} = (\alpha M_k - M_{k-1})^n \alpha^r - (\beta M_k - M_{k-1})^n \beta^r.$$

En développant et en recombinant, on obtient (pour $n \geq 0$)

$$M_{nk+r} = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} M_k^j M_{k-1}^{n-j} M_{r+j}. \tag{3.7}$$

On déduit de

$$\begin{aligned} \sum_{j=1}^{n} (-1)^{n-j} j \binom{n}{j} k^j (k-1)^{n-j} &= \sum_{j=1}^{n} (-1)^{n-j} nk \binom{n-1}{j-1} k^{j-1} (k-1)^{n-j} \\ &= nk \sum_{l=0}^{n-1} (-1)^{n-1-l} \binom{n-1}{l} k^l (k-1)^{n-1-l} \\ &= nk\big(k-(k-1)\big)^{n-1} \\ &= nk, \end{aligned}$$

que l'égalité (3.7) est aussi vérifiée pour $t \in \{0,-4\}$. En effet, pour $t=0$ on a

$$\begin{aligned} \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} M_k^j M_{k-1}^{n-j} M_{r+j} &= \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} k^j (k-1)^{n-j} (r+j) \\ &= nk + r \\ &= M_{nk+r}. \end{aligned}$$

De la même façon, on trouve pour $t = -4$ que

$$\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} M_k^j M_{k-1}^{n-j} M_{r+j} = (-1)^{nk+r+1}(nk+r) = M_{nk+r}.$$

Maintenant, si on pose $k = d(m)$ dans (3.7), on trouve

$$M_{nd(m)+r} \equiv (-1)^n M_{d(m)-1}^n M_r \bmod m. \tag{3.8}$$

On note que ceci est valable pour les entiers négatifs aussi bien que pour les entiers positifs r.

Lemme 3.1.3. *$l(m)$ est le plus petit entier strictement positif n pour lequel*

$$(-1)^n M_{d(m)-1}^n \equiv 1 \ mod \ m.$$

Démonstration. Supposons que $(-1)^n M_{d(m)-1}^n \equiv 1 \bmod m$, alors de (3.8) on obtient $M_{nd(m)+r} \equiv M_r \bmod m$, pour tout r. On en déduit, d'après la définition de $k(m)$, que $k(m) \leq nd(m)$ et donc $l(m) = k(m)/d(m) \leq n$.

Maintenant, on pose $r = 1$ et $n = l(m)$ dans (3.8) pour obtenir

$$(-1)^{l(m)} M_{d(m)-1}^{l(m)} \equiv M_{l(m)d(m)+1} \equiv M_{k(m)+1} \equiv M_1 \equiv 1 \bmod m.$$

On en déduit que $l(m)$ est le plus petit entier strictement positif n pour lequel on a $(-1)^n M_{d(m)-1}^n \equiv 1 \bmod m$. □

Théorème 3.1.5. *Soient $m > 2$ un entier et $p \neq 2$ un nombre premier.*

(a) $l(2) = 1$ *et* $l(m) = 1$ *ou* 2.

(b) $l(p) = 2$ *si et seulement si* $k(p)$ *est pair, dans ce cas* $d(p) = k(p)/2$.

(c) $l(p) = 1$ *si et seulement si* $k(p)$ *est impair, dans ce cas* $d(p) = k(p) \neq p \pm 1$.

(d) Si $\prod p_i^{e_i}$ *est la factorisation de m en produit de nombres premiers, alors* $d(m) = \text{ppcm}\left(d\left(p_i^{e_i}\right)\right)$.

Démonstration.

(a) $l(2) = 1$ est facile à vérifier. On pose $n = d(m) - 1$ dans l'identité (b) de la Proposition 3.1.1 pour obtenir

$$(-1)^2 M_{d(m)-1}^2 = M_{d(m)-1}^2 = M_{d(m)} M_{d(m)-2} + 1 \equiv 1 \bmod m,$$

et (a) découle du Lemme 3.1.3.

(b) Il est clair que si $l(p) = 2$, alors $k(p) = l(p)d(p)$ est pair. Inversement, si $k(p)$ est pair, alors en mettant $n = k(p)/2$ dans l'identité (f) de la Proposition 3.1.1, on obtient

$$M_{k(p)} = M_{k(p)/2}\left(M_{k(p)/2+1} - M_{k(p)/2-1}\right). \tag{3.9}$$

Supposons maintenant que $M_{k(p)/2+1} - M_{k(p)/2-1} \equiv 0 \bmod p$, alors en mettant $n = k(p)/2 - 1$ dans l'identité (g) de la Proposition 3.1.1, on obtient

$$M_{k(p)-1} = M_{k(p)/2-1}\left(M_{k(p)/2+1} - M_{k(p)/2-1}\right) + 1 \equiv 1 \bmod p.$$

Puisqu'on sait que $M_{k(p)} \equiv 0 \bmod p$, on obtient

$$M_{k(p)+1} = (2+t)M_{k(p)} - M_{k(p)-1} \equiv -1 \bmod p,$$

mais on sait, par définition de $k(p)$, que $M_{k(p)+1} \equiv 1 \bmod p$, donc $-1 \equiv 1 \bmod p$, ce qui est une contradiction pour $p > 2$, d'où $M_{k(p)/2+1} - M_{k(p)/2-1} \not\equiv 0 \bmod p$, et d'après (3.9) on obtient $M_{k(p)/2} \equiv 0 \bmod p$, c'est-à-dire, $l(p) = 2$.

(c) D'après (b) on voit que $k(p)$ est impair, si et seulement si $l(p) \neq 2$, et de (a) on en déduit que $l(p) = 1$.

(d) Puisque les $p_i^{e_i}$ sont deux à deux premiers entre eux, $m|M_k$ est équivalent à $p_i^{e_i}|M_k$ pour tout i, ce qui est équivalent, d'après (A.2), à $d(p_i^{e_i})|k$ pour tout i. Le plus petit entier strictement positif k qui satisfait à ces conditions est $k = \text{ppcm}\left(d\left(p_i^{e_i}\right)\right)$.

□

Par exemple, dans le Tableau 3.IV, $k(5)$, $k(19)$ et $k(29)$ sont impairs et on a bien $l(5) = l(19) = l(29) = 1$, alors que $k(7)$, $k(17)$ et $k(31)$ sont pairs et on a bien $l(7) = l(17) = l(31) = 2$.

3.2 La suite de Morgan-Voyce avec des conditions initiales généralisées

Soient a et b des entiers et considérons la suite $(M_n^{a,b})_n$ définie par

$$M_0^{a,b} = a, \;\; M_1^{a,b} = b \;\text{ et }\; M_n^{a,b} = (2+t)M_{n-1}^{a,b} - M_{n-2}^{a,b} \;\text{ pour } n \geq 2.$$

Puisque la matrice compagnon de la suite $(M_n^{a,b})_n$ est la même que celle de la suite $(M_n)_n$ (elle ne dépend pas des conditions initiales), on en déduit que la suite $(M_n^{a,b} \bmod m)_n$ est simplement périodique, pour tout entier $m \geq 2$. On désigne par $k(a,b;m)$ la période de la suite $(M_n^{a,b} \bmod m)_n$, i.e., le plus petit entier strictement positif k tel que $M_k^{a,b} \equiv a \bmod m$ et $M_{k+1}^{a,b} \equiv b \bmod m$. Notons que la suite de Morgan-Voyce classique est $(M_n^{1-s,1})_n$. La suite $(M_n^{2,2+t})_n$, qui est appelée la suite compagnon de $(M_n)_n$, satisfait plusieurs propriétés [17]. La proposition suivante indique qu'on peut exprimer la suite $(M_n^{a,b})_n$ en fonction de la suite $(M_n)_n$. Notons qu'à partir de la relation de récurrence, on peut définir $M_{-1} = (2+t)M_0 - M_1 = -1$. On peut aussi utiliser la relation (3.6).

Proposition 3.2.1. *La suite $(M_n^{a,b})_n$ satisfait*

$$M_n^{a,b} = bM_n - aM_{n-1}, \qquad (n \geq 0). \tag{3.10}$$

Démonstration. Cela découle d'une simple récurrence. □

Proposition 3.2.2. *Soient a, b et m des entiers avec $m \geq 2$, alors*

(a) $k(a,b;m) | k(m)$.

(b) $k(b,0;m) = k(0,-b;m) = k(0,b;m)$ *et* $k(0,b;m) | k(m)$.

(c) Si $\text{pgcd}(b,m) = 1$, *alors* $k(0,b;m) = k(m)$.

(d) $k(a,b;m) | \text{ppcm}\big(k(a,0;m), k(0,b;m)\big)$.

Démonstration.

(a) La relation (3.10) nous donne

$$\begin{cases} M^{a,b}_{k(m)} = bM_{k(m)} - aM_{k(m)-1} \\ M^{a,b}_{k(m)+1} = bM_{k(m)+1} - aM_{k(m)} \end{cases} \Longrightarrow \begin{cases} M^{a,b}_{k(m)} \equiv bM_0 - aM_{-1} \bmod m \\ M^{a,b}_{k(m)+1} \equiv bM_1 - aM_0 \bmod m \end{cases}$$
$$\Longrightarrow \begin{cases} M^{a,b}_{k(m)} \equiv a \bmod m \\ M^{a,b}_{k(m)+1} \equiv b \bmod m \end{cases}.$$

Il vient que $k(a,b;m)|k(m)$. Remarquons que (a) peut se déduire aussi de (b) et (d).

(b) Il est clair que $M^{b,0}_{n+1} = M^{0,-b}_n$ pour tout $n \geq 0$, il vient que $k(b,0;m) = k(0,-b;m)$. Pour la deuxième égalité, on a $M^{0,-b}_n = -M^{0,b}_n$ pour tout $n \geq 0$. En effet, de la relation (3.10), on a $M^{0,-b}_n = -bM_n$ et $M^{0,b}_n = bM_n$ pour tout $n \geq 0$. Posons maintenant $l = k(0,b;m)$, alors

$$\begin{cases} M^{0,b}_l \equiv 0 \bmod m \\ M^{0,b}_{l+1} \equiv b \bmod m \end{cases} \Longleftrightarrow \begin{cases} -M^{0,b}_l \equiv 0 \bmod m \\ -M^{0,b}_{l+1} \equiv -b \bmod m \end{cases}$$
$$\Longleftrightarrow \begin{cases} M^{0,-b}_l \equiv 0 \bmod m \\ M^{0,-b}_{l+1} \equiv -b \bmod m. \end{cases}$$

Cela montre que $k(0,-b;m) = k(0,b;m)$. Le fait que $k(0,b;m)|k(m)$ est un cas particulier de (a).

(c) Le fait que b est inversible modulo m nous donne que $M_i \equiv M_j \bmod m$, si et seulement si, $bM_i \equiv bM_j \bmod m$, si et seulement si, $M^{0,b}_i \equiv M^{0,b}_j \bmod m$. On en déduit que $k(0,b;m) = k(m)$.

(d) D'après la relation (3.10), on a $M^{0,b}_n = bM_n$ et $M^{a,0}_n = -aM_{n-1}$, pour tout $n \geq 0$. Posons $\sigma = k(a,0;m)$ et $\tau = k(0,b;m)$, alors $M^{a,0}_\sigma \equiv a \bmod m$, $M^{a,0}_{\sigma+1} \equiv 0 \bmod m$ et $M^{0,b}_\tau \equiv 0 \bmod m$, $M^{0,b}_{\tau+1} \equiv b \bmod m$. Soit $\theta = \text{ppcm}(\sigma,\tau)$. Puisque $\sigma|\theta$ et $\tau|\theta$, on a $-aM_{\theta-1} = M^{a,0}_\theta \equiv a \bmod m$, $-aM_\theta = M^{a,0}_{\theta+1} \equiv 0 \bmod m$, $bM_\theta = M^{0,b}_\theta \equiv 0 \bmod m$ et $bM_{\theta+1} = M^{0,b}_{\theta+1} \equiv b \bmod m$. On déduit de ces quatre dernières congruences et de la relation (3.10) que $M^{a,b}_\theta = bM_\theta - aM_{\theta-1} \equiv a \bmod m$ et $M^{a,b}_{\theta+1} = bM_{\theta+1} - aM_\theta \equiv b \bmod m$, i.e., $k(a,b;m)|\theta = \text{ppcm}\big(k(a,0;m),k(0,b;m)\big)$.

□

Proposition 3.2.3. *Nous avons les identités suivantes.*

(a) $(M_n^{a,b})^2 - M_{n-1}^{a,b} M_{n+1}^{a,b} = a^2 + b^2 - (2+t)ab, \qquad (n \geq 1),$

(b) $M_{n+g}^{a,b} = M_{n+1}^{a,b} M_g - M_n^{a,b} M_{g-1} \qquad (g \geq 1 \text{ et } n \geq 0),$

(c) $M_{2n}^{a,b} = M_n^{a,b}(M_{n+1} - M_{n-1}) - a, \qquad (n \geq 0),$

(d) $M_{2n+1}^{a,b} = M_n(M_{n+2}^{a,b} - M_n^{a,b}) + b, \qquad (n \geq 0),$

(e) $(M_{n-1}^{a,b})^2 - (2+t)M_{n-1}^{a,b} M_n^{a,b} + (M_n^{a,b})^2 = a^2 + b^2 - (2+t)ab, \qquad (n \geq 1).$

Démonstration. Utiliser les résultats de la Proposition 3.1.1 avec (3.1). □

Lemme 3.2.1. *Soient a, b et m des entiers tels que* $\text{pgcd}(a,b,m) = 1$ *et supposons que $m = p^e$ pour un nombre premier impair p et un entier strictement positif e, alors $M_g^{2,2+t} \equiv 2 \bmod m$, où $g = k(a,b;m)$.*

Démonstration. Il est facile de voir que $M_n^{2,2+t} = M_{n+1} - M_{n-1}$ pour tout $n \geq 0$. On a

$$\begin{cases} M_g^{a,b} \equiv a \bmod m \\ M_{g+1}^{a,b} \equiv b \bmod m \end{cases} \iff \begin{cases} bM_g - aM_{g-1} \equiv a \bmod m \\ bM_{g+1} - aM_g \equiv b \bmod m \end{cases}$$

$$\iff \begin{cases} bM_g - a(M_{g-1}+1) \equiv 0 \bmod m \\ b(M_{g+1}-1) - aM_g \equiv 0 \bmod m \end{cases}.$$

Puisque $\text{pgcd}(a,b,m) = 1$, on obtient $M_g^2 - (M_{g+1}-1)(M_{g-1}+1) \equiv 0 \bmod m$, qui, à l'aide de la proposition 3.1.1 (b), devient $M_{g+1} - M_{g-1} \equiv 2 \bmod m$, c'est-à-dire, $M_g^{2,2+t} \equiv 2 \bmod m$. □

Le théorème suivant est aussi un analogue au Théorème 2.3.6 pour le cas Morgan-Voyce.

Théorème 3.2.4. *Soit $p > 2$ un nombre premier tel que $p \nmid (t^2+4t)$; soient a et b des entiers tels que* $\text{pgcd}(a,b,p) = 1$*, alors $k(a,b;p) = k(p)$.*

Démonstration. D'après la Proposition 3.1.1 (j), on a $M_n^{2,2+t} = \alpha^n + \beta^n$ pour tout $n \geq 0$; donc, d'après le Lemme 3.2.1, on a

$$\alpha^g + \beta^g - 2 \equiv 0 \bmod p,$$

où $g = k(a,b;p)$. Puisque $\alpha\beta = 1$, on trouve

$$(\alpha^g - \beta^g)^2 = (\alpha^g + \beta^g - 2)^2 + 4(\alpha^g + \beta^g - 2) \equiv 0 \bmod p.$$

Maintenant, puisque $p \nmid (t^2+4t)$, on divise la relation ci-dessus par $(\alpha-\beta)^2 = t^2+4t$ pour obtenir

$$\left(\frac{\alpha^g - \beta^g}{\alpha - \beta}\right)^2 = M_g^2 \equiv 0 \bmod p,$$

d'où $M_g \equiv 0 \bmod p$. Cette dernière congruence et la relation $M_{g+1} = (2+t)M_g - M_{g-1}$ donnent $M_{g+1} \equiv -M_{g-1} \bmod p$. Cette dernière congruence avec $M_{g+1} - M_{g-1} \equiv 2 \bmod p$ impliquent $M_{g+1} \equiv -M_{g-1} \equiv 1 \bmod p$. Ainsi, on obtient $k(p)|g$ et on déduit de la Proposition 3.2.2 (a) que $g = k(p)$. □

Considérons maintenant une relation binaire sur l'ensemble $(\mathbb{Z}/m\mathbb{Z})^2$ définie par $(a,b) \sim (q,r)$, si et seulement si, il existe un indice i tel que $M_i^{a,b} \equiv q \bmod m$ et $M_{i+1}^{a,b} \equiv r \bmod m$. Puisque deux termes consécutifs déterminent complètement la suite $(M_n^{a,b})_n$ modulo m, il s'agit bien d'une relation d'équivalence sur $(\mathbb{Z}/m\mathbb{Z})^2$. Le Tableau 3.XI, où l'on considère $t = 1$, donne toutes les classes d'équivalence modulo 6.

$k(a,b;6)$	(a,b)
1	$(0,0)$
12	$(0,1),(1,3),(3,2),(2,3),(3,1),(1,0),(0,5),(5,3),(3,4),(4,3),(3,5),(5,0)$
4	$(0,2),(2,0),(0,4),(4,0)$
3	$(0,3),(3,3),(3,0)$
12	$(1,1),(1,2),(2,5),(5,1),(1,4),(4,5),(5,5),(5,4),(4,1),(1,5),(5,2),(2,1)$
4	$(2,2),(2,4),(4,4),(4,2)$

Tableau 3.XI – Les (a,b)-classes d'équivalence modulo 6.

Une suite $(M_n^{a,b})_n$ de période d modulo m est de la forme $M_0^{a,b}$, $M_1^{a,b}$, $M_2^{a,b}$, …, $M_{d-1}^{a,b}$, $M_d^{a,b} \equiv M_0^{a,b}$, $M_{d+1}^{a,b} \equiv M_1^{a,b}$, …. Par conséquent, les paires distinctes qui sont composées de deux termes consécutifs dans la suite $(M_n^{a,b} \bmod m)_n$ sont $(M_0^{a,b}, M_1^{a,b})$, $(M_1^{a,b}, M_2^{a,b})$, …, $(M_{d-1}^{a,b}, M_0^{a,b})$. Ainsi, on a d paires, on en déduit que la taille de la classe d'équivalence contenant (a,b) est $d = k(a,b;m)$. Étant donné un entier $m \geq 2$ fixé, on définit $c_d(m)$ comme étant le nombre de classes d'équivalence distinctes de taille d. Ainsi, dans le Tableau 3.XI, on voit que $c_1(6) = 1$, $c_3(6) = 1$, $c_4(6) = 2$, $c_{12}(6) = 2$, et $c_d(6) = 0$ pour tous les autres d.

Le théorème suivant compte les éléments de $(\mathbb{Z}/m\mathbb{Z})^2$ correspondant à la partition de cet ensemble en classes d'équivalence.

Théorème 3.2.5. *Soient $m \geq 2$ et $c_d(m)$ défini comme ci-dessus, alors*

$$m^2 = \sum_{d|k(m)} d \cdot c_d(m).$$

Démonstration. Les classes d'équivalences forment une partition de $(\mathbb{Z}/m\mathbb{Z})^2$ et d'après la Proposition 3.2.2 (a), la taille de chaque classe d'équivalence divise $k(m)$. En additionnant le nombre d'éléments dans chaque classe de taille d pour tout $d|k(m)$, on obtient le nombre de paires possibles, qui est m^2. □

Des résultats partiels pour les petites classes d'équivalence sont décrits par la proposition suivante.

Proposition 3.2.6. *Soit $m \geq 2$ un entier.*

(a) $c_1(m) = \text{pgcd}(t,m)$.

(b) *(i) Si* $\text{pgcd}(t,m) = 1$, *alors* $c_2(m) = (g-1)/2$, *où* $g = \text{pgcd}(4+t,m)$.

(ii) Si $m|t$, alors $c_2(m) = 0$ si m est impair et $c_2(m) = m/2$ si m est pair.

(c) Si $\text{pgcd}(3+t,m) = 1$, *alors* $c_3(m) = 0$.

Démonstration.

(a) Une suite de période 1 est de la forme $a,a,a,\ldots$ modulo m. Ainsi, on a $(2+t)a - a \equiv a \bmod m$, ce qui est équivalent à $ta \equiv 0 \bmod m$. Soit $g = \text{pgcd}(t,m)$, alors $t = gt_1$ et $m = gm_1$ avec $\text{pgcd}(t_1,m_1) = 1$. On a

$$\begin{aligned} ta \equiv 0 \bmod m &\iff gt_1 a \equiv 0 \bmod gm_1 \\ &\iff t_1 a \equiv 0 \bmod m_1 \\ &\iff a \equiv 0 \bmod m_1, \end{aligned}$$

donc, $a = lm_1 = lm/g$, avec $l = 0,1,\ldots,g-1$. En effet, on a

$$(2+t)\frac{lm}{g} - \frac{lm}{g} = \frac{lm}{g} + t_1 lm \equiv \frac{lm}{g} \bmod m.$$

(b) Une suite de période 2 est de la forme $a,b,a,b,\ldots$ modulo m. Ainsi,

$$\begin{cases} (2+t)a-b \equiv b[m] \\ (2+t)b-a \equiv a[m] \end{cases} \iff \begin{cases} t(a+b) & \equiv & 0[m] \\ 2a-2b+ta & \equiv & 0[m] \end{cases}. \tag{3.11}$$

(i) Si $\text{pgcd}(t,m)=1$, alors

$$(3.11) \iff \begin{cases} b & \equiv & -a[m] \\ (4+t)a & \equiv & 0[m] \end{cases}. \tag{3.12}$$

Soit $g=\text{pgcd}(4+t,m)$, alors $4+t=gt_1$ et $m=gm_1$ avec $\text{pgcd}(t_1,m_1)=1$. On a

$$(3.12) \iff \begin{cases} b & \equiv & -a[m] \\ gt_1a & \equiv & 0[gm_1] \end{cases} \iff \begin{cases} b & \equiv & -a[m] \\ a & \equiv & 0[m_1] \end{cases},$$

donc $a=lm/g$ et $b=m-a=m-lm/g$ avec $l=0,1,\ldots,g-1$. En enlevant les cas $a=b$ et où les mêmes suites $a,b,a,b,\ldots$ et $b,a,b,a,\ldots$ sont obtenues, il ne reste que les suites $lm/g, m-lm/g,\ldots$ avec $l=1,2,\ldots,(g-1)/2$, d'où $c_2(m)=(g-1)/2$. Notons que puisque $\text{pgcd}(m,t)=1$, alors g est toujours impair.

(ii) Si $m|t$, alors le système (3.11) est équivalent à $2a\equiv 2b[m]$. Dans ce cas, si m est impair, la dernière congruence est équivalente à $a\equiv b[m]$, ce qui donne $c_2(m)=0$. Si m est pair, alors $2a\equiv 2b[m]$ si et seulement si $a\equiv b[m/2]$, ce qui donne des suites de période 2 qui sont $a,m/2+a,a,m/2+a,\ldots$, avec $a=0,1,\ldots,m/2-1$, d'où $c_2(m)=m/2$.

(c) Une suite de période 3 est de la forme $a,b,c,a,b,c,\ldots$ modulo m. Ainsi,

$$\begin{cases} (2+t)b-a-c \equiv 0[m] \\ (2+t)c-b-a \equiv 0[m] \\ (2+t)a-c-b \equiv 0[m] \end{cases} \iff \begin{cases} (3+t)(b-c) \equiv 0[m] \\ (3+t)(c-a) \equiv 0[m] \\ (2+t)a-c-b \equiv 0[m] \end{cases}. \tag{3.13}$$

Si $\text{pgcd}(3+t,m)=1$, alors (3.13) donne $a\equiv b\equiv c[m]$, d'où $c_3(m)=0$.

□

Par exemple, si $t=8$ et $m=4$, alors $c_1(4)=4, c_2(4)=2$ et $c_3(4)=0$. Puisque $k(4)=4$, on déduit du Théorème 3.2.5 que $c_4(m)=2$ et $c_d(m)=0$ pour tous les autres d.

A l'exception de la suite $(M_n^{0,0})_n$ qui est toujours de longueur 1, on peut avoir toutes les classes de longueur $k(m)$, comme représenté dans le Tableau 3.XII par le cas $t = 2$ et $m = 7$, avec $k(m) = 8$.

Diviseur d	1	2	4	8
$c_d(7)$	1	0	0	6

Tableau 3.XII – Longueurs et nombre de classes d'équivalence modulo 7 pour $t = 2$.

Théorème 3.2.7. *Soient $m \geq 2$ un entier et $p > 2$ un nombre premier.*

(a) Si $m|t$, alors $M_n \equiv n \bmod m$, pour tout $n \geq 0$. Dans ce cas, $k(m) = m$.

(b) Si $m|(2+t)$, alors $M_n \equiv 0 \bmod m$ si $n \equiv 0 \bmod 2$, $M_n \equiv 1 \bmod m$ si $n \equiv 1 \bmod 4$ et $M_n \equiv -1 \bmod m$ si $n \equiv -1 \bmod 4$. Dans ce cas, $k(2) = 2$ et $k(m) = 4$ pour $m > 2$.

(c) Si $p|t$, alors $c_1(p) = p$, $c_p(p) = p-1$ et $c_d(p) = 0$ pour tous les autres d.

(d) Si $p|(2+t)$, alors $c_1(p) = 1$, $c_4(p) = (p^2-1)/4$ et $c_d(p) = 0$ pour tous les autres d.

Démonstration.

(a) Le fait que $k(m) = m$ est une conséquence de la congruence $M_n \equiv n \bmod m$ pour tout $n \geq 0$, qui elle même découle de la Proposition 3.1.1 (c) et du fait que $m|t$.

(b) Le fait que $k(2) = 2$ et $k(m) = 4$ pour $m > 2$ est une conséquence des trois congruences qui elles mêmes découlent de la Proposition 3.1.1 (a) et du fait que $m|(2+t)$.

(c) Si $p|t$, alors d'après (a), on a $k(p) = p$. Ainsi, d'après la Proposition 3.2.2 (a), on obtient que toutes les classes sont de taille 1 ou p ; et d'après le Théorème 3.2.5, on obtient $p^2 = c_1(p) + pc_p(p)$. Maintenant, d'après la Proposition 3.2.6 (a), on a $c_1(p) = p$. On en déduit que $c_p(p) = p-1$.

(d) Si $p|(2+t)$, alors d'après (b), on a $k(p) = 4$. D'après la Proposition 3.2.2(a), on obtient que toutes les classes ont une taille divisant 4. Les conditions $p > 2$ et $p|(2+t)$ impliquent $p \nmid t$ et $p \nmid (4+t)$. Donc, d'après la Proposition 3.2.6 (a), on a $c_1(p) = 1$ et d'après la Proposition 3.2.6 (b) (i), on a $c_2(p) = 0$. Maintenant, d'après le Théorème 3.2.5, on obtient $p^2 - 1 = 4c_4(p)$. D'où $c_1(p) = 1$, $c_4(p) = (p^2-1)/4$ et $c_d(p) = 0$ pour tous les autres d.

□

Théorème 3.2.8. *Si $p > 2$ est un nombre premier tel que $p \nmid (t^2+4t)$, alors $c_1(p) = 1$, $c_{k(p)}(p) = (p^2-1)/k(p)$ et $c_d(p) = 0$ pour tous les autres d. En particulier, si on a $k(p) = p+1$, alors $c_1(p) = 1$, $c_{p+1}(p) = p-1$ et $c_d(p) = 0$ pour tous les autres d. Si $k(p) = p-1$, alors $c_1(p) = 1$, $c_{p-1}(p) = p+1$ et $c_d(p) = 0$ pour tous les autres d.*

Démonstration. D'après le Théorème 3.2.4, on sait que, sauf pour $c_1(p)$ qui est égal à 1, toutes les classes sont de taille $k(p)$. Ainsi, d'après le Théorème 3.2.5, on a $p^2-1 = k(p)c_{k(p)}(p)$. Si $k(p) = p+1$, alors $c_1(p) = 1, c_{p+1}(p) = p-1$ et $c_d(p) = 0$ pour tous les autres d. Si $k(p) = p-1$, alors $c_1(p) = 1, c_{p-1}(p) = p+1$ et $c_d(p) = 0$ pour tous les autres d. □

Notons que, pour $p \neq 2$, puisque $p|(2+t)$ implique $p \nmid (t^2+4t)$, le Théorème 3.2.7 (d) est un cas particulier du Théorème 3.2.8.

En considérant, d'une manière générale, une suite $(M_n^{a,b})_n$ de période d modulo m, on a

$$-M_0^{a,b} + M_2 M_1^{a,b} \equiv M_2^{a,b},\ -M_1^{a,b} + M_2 M_2^{a,b} \equiv M_3^{a,b}, \ldots,\ -M_{d-1}^{a,b} + M_2 M_0^{a,b} \equiv M_1^{a,b},$$

où $M_2 = 2+t$. Ainsi, on obtient

$$\begin{pmatrix} -1 & M_2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & M_2 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & M_2 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & & \vdots & & & \ddots & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & -1 & M_2 & -1 \\ -1 & 0 & 0 & 0 & 0 & \cdots & 0 & -1 & M_2 \\ M_2 & -1 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} M_0^{a,b} \\ M_1^{a,b} \\ M_2^{a,b} \\ \vdots \\ M_{d-3}^{a,b} \\ M_{d-2}^{a,b} \\ M_{d-1}^{a,b} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} \mod m.$$

On définit la matrice circulante de Morgan-Voyce W_n^{MV} par la matrice de taille n suivante :

$$W_n^{MV} := \begin{pmatrix} -1 & M_2 & -1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & M_2 & -1 & \cdots & 0 & 0 \\ 0 & 0 & -1 & M_2 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & \cdots & -1 & M_2 \\ M_2 & -1 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix}.$$

Proposition 3.2.9. *Soit* $w_n^{MV} = \det W_n^{MV}$, *alors*

(a) $w_n^{MV} = \prod_{j=0}^{n-1} \Big(-1 + M_2 e^{2i\pi j/n} - e^{4i\pi j/n} \Big), \qquad (n \geq 3),$

(b) $w_n^{MV} = (-1)^{n-3} \big(M_{n+1} - M_{n-1} - 2 \big), \qquad (n \geq 3),$

(c) $\begin{cases} w_1^{MV} = t, w_2^{MV} = -t^2 - 4t, \\ w_n^{MV} = 2t(-1)^{n-3} - (2+t) w_{n-1}^{MV} - w_{n-2}^{MV}, \qquad (n \geq 3), \end{cases}$

(d) $w_n^{MV} = (-1)^{n-3} \sum_{k=1}^{n} \frac{2n}{n+k} \binom{n+k}{n-k} t^k, \qquad (n \geq 3).$

Démonstration.

(a) D'après l'identité (2.6), on a $W_n^{MV} = -I_n + M_2 \pi_n - \pi_n^2$ et d'après l'identité (2.7), les valeurs propres de W_n^{MV} sont $-1 + M_2 e^{2i\pi j/n} - e^{4i\pi j/n}$, avec $j = 0, 1, \ldots, n-1$. On en déduit que le déterminant est $w_n^{MV} = \prod_{j=0}^{n-1} \Big(-1 + M_2 e^{2i\pi j/n} - e^{4i\pi j/n} \Big)$.

(b) Pour $n = 3$, on peut le vérifier directement. Pour $n \geq 4$, notons par L_i la i-ième ligne de la matrice W_n^{MV}. En remplaçant L_{n-1} par $-\sum_{i=1}^{n-4} M_i L_i + L_{n-1}$ et L_n par $\sum_{i=1}^{n-3} M_{i+1} L_i + L_n$, on obtient

$$\begin{pmatrix} -1 & M_2 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & -1 & M_2 & -1 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & M_2 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & & \vdots & & \ddots & & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & -1 & M_2 & -1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & M_2 & -1 \\ 0 & 0 & 0 & 0 & \cdots & -M_{n-3} & M_{n-4} & -1 & M_2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & M_{n-1} & -M_{n-2} & -1 \end{pmatrix},$$

on en déduit que

$$w_n^{MV} = (-1)^{n-4} \begin{vmatrix} -1 & M_2 & -1 & 0 \\ 0 & -1 & M_2 & -1 \\ -M_{n-3} & M_{n-4} & -1 & M_2 \\ 0 & M_{n-1} & -M_{n-2} & -1 \end{vmatrix}.$$

En développant, par rapport à la première colonne, on trouve

$$\begin{aligned} w_n^{MV} &= (-1)^{n-3}\big[-1-M_{n-2}(M_2M_{n-3}-M_{n-4}) \\ &\quad +M_2(M_2M_{n-1}-M_{n-2})-M_2(M_2M_{n-3}-M_{n-4}) \\ &\quad -M_{n-1}+M_{n-1}M_{n-3}+M_{n-3}\big]. \end{aligned}$$

En utilisant la définition de la suite $(M_n)_n$, on obtient

$$\begin{aligned} w_n^{MV} &= (-1)^{n-3}\big[-1-M_{n-2}^2+M_2M_n-M_2M_{n-2} \\ &\quad -M_{n-1}+M_{n-1}M_{n-3}+M_{n-3}\big] \\ &= (-1)^{n-3}\big[-1+(M_{n-1}M_{n-3}-M_{n-2}^2)+M_{n+1}-M_{n-1}\big], \end{aligned}$$

finalement, de la Proposition 3.1.1 (b), on obtient

$$w_n^{MV} = (-1)^{n-3}\big(M_{n+1}-M_{n-1}-2\big).$$

(c) La relation de récurrence $w_n^{MV} = 2t(-1)^{n-3}-(2+t)w_{n-1}^{MV}-w_{n-2}^{MV}$ résulte de (b), $w_1^{MV}=t$ et $w_2^{MV}=-t^2-4t$ donnent une définition de w_1^{MV} et w_2^{MV} inspirée par (b).

(d) Utiliser (b) et la Proposition 3.1.1 (k).

□

Corollaire 3.2.9.1. *Soient a, b et m des entiers tels que* $\text{pgcd}(a,b,m)=1$ *et supposons que* $m=p^e$ *pour un nombre premier impair p et un entier strictement positif e, alors* $w_g^{MV}\equiv 0$ *mod m, où* $g=k(a,b;m)$.

Démonstration. Découle de la Proposition 3.2.9 (b) et du Lemme 3.2.1. □

Le théorème suivant nous donne une relation entre w_n^{MV} et la période de la suite $(M_n^{a,b})_n$ modulo m. En fait, il nous dit que si $\text{pgcd}\left(w_l^{MV},m\right)=1$, alors l ne peut pas être une période d'une suite $(M_n^{a,b})_n$ modulo m.

Théorème 3.2.10. *Soient a et b des entiers tels que* $(a,b)\not\equiv(0,0)$ *mod m, où* $m\geq 2$ *est un entier. Si* $l=k(a,b;m)$, *alors* $\text{pgcd}\left(w_l^{MV},m\right)\neq 1$.

Démonstration. Supposons par l'absurde que $\text{pgcd}\left(w_l^{MV}, m\right) = 1$. D'une part, on sait que $X = (M_0^{a,b}, M_1^{a,b}, \ldots, M_{l-1}^{a,b})$ est une solution non triviale du système $W_l^{MV} X \equiv 0 \bmod m$. D'autre part, $\text{pgcd}\left(w_l^{MV}, m\right) = 1$ implique que W_l^{MV} est inversible modulo m, donc la seule solution du système $W_l X \equiv 0 \bmod m$ est $X \equiv 0 \bmod m$, ce qui conduit à une contradiction. □

3.3 Suites de Morgan-Voyce sur les courbes elliptiques

Soient A et B deux points de $E(\mathbb{F}_p)$ où $E : y^2 = x^3 + ax + b$ est une courbe elliptique définie sur le corps fini $\mathbb{F}_p$, avec $p > 2$ un nombre premier. On définit la suite de Morgan-Voyce $(M_n^{A,B})_n$ sur la courbe elliptique E par

$$M_0^{A,B} = A,\ M_1^{A,B} = B \ \text{ et } \ M_n^{A,B} = [2+t]M_{n-1}^{A,B} - M_{n-2}^{A,B}, \quad \text{pour } \ n \geq 2.$$

Tout d'abord, on établit quelques propriétés de base relatives à $(M_n^{A,B})_n$.

Proposition 3.3.1. *Soient A et B deux points de $E(\mathbb{F}_p)$.*

(a) La suite $(M_n^{A,B})_n$ est donnée par

$$M_n^{A,B} = [M_n]B - [M_{n-1}]A, \qquad (n \geq 0). \tag{3.14}$$

(b) La suite $(M_n^{A,B})_n$ est simplement périodique.

(c)
$$\begin{cases} M_{2n}^{A,B} &= [M_{n+1} - M_{n-1}]M_n^{A,B} - A \\ M_{2n+1}^{A,B} &= [M_n](M_{n+2}^{A,B} - M_n^{A,B}) + B \end{cases}, \qquad (n \geq 0).$$

Démonstration.

(a) Cela découle d'une simple récurrence.

(b) Si on considère une paire constituée de deux termes consécutifs quelconques de la suite, alors il n'y a que h^2 paires distinctes possibles. Par conséquent, à un certain point de la suite, on aura une paire qui se répète. Supposons qu'on a $M_{\sigma-1}^{A,B} = M_{\tau-1}^{A,B}$ et $M_\sigma^{A,B} = M_\tau^{A,B}$ avec $\tau > \sigma$. Puisque $M_{n-2}^{A,B} = [2+t]M_{n-1}^{A,B} - M_n^{A,B}$, on en déduit que $M_{\sigma-\rho}^{A,B} = M_{\tau-\rho}^{A,B}$ pour $\rho \geq 0$. D'où pour $\rho = \sigma - 1$, on a $M_1^{A,B} = M_{\tau-\sigma+1}^{A,B}$ et pour $\rho = \sigma$ on a $M_0^{A,B} = M_{\tau-\sigma}^{A,B}$. On en déduit que la suite est périodique et qu'elle revient à son point de départ.

(c) Utiliser la relation (3.14) et les relations (f) et (g) de la Proposition 3.1.1.

□

On note par $K(A,B;E)$ la période de la suite $(M_n^{A,B})_n$, c'est-à-dire, le plus petit entier strictement positif k satisfaisant $M_k^{A,B} = A$ et $M_{k+1}^{A,B} = B$.

Le Lemme 1.2.1 nous permet de faire le lien entre les périodes de $(M_n^{A,B})_n$ et les périodes de $(M_n \bmod m)_n$. On va voir que la période de la suite $(M_n^{O,B})_n$ ne dépend que de $h_B = \mathrm{ord}(B)$, de sorte que tous les points R qui ont le même ordre vont engendrer des suites avec exactement la même longueur. Une fois cette connexion établie, on pourra généraliser les propriétés de la suite ordinaire $(M_n)_n$ à des suites $(M_n^{A,B})_n$ sur les courbes elliptiques.

Théorème 3.3.2. *Soient A et B deux points de $E(\mathbb{F}_p)$.*

(a) $K(B,O;E) = K(O,-B;E) = K(O,B;E) = k(h_B)$.

(b) $K(A,B;E) | \mathrm{ppcm}\left(K(A,O;E), K(O,B;E)\right)$.

(c) $K(A,B;E) | k(h)$.

Démonstration.

(a) La preuve des deux premières égalités découle d'arguments analogues à ceux de la preuve de la Proposition 3.2.2(b). D'après la relation (3.14), la suite $(M_n^{O,B})_n$ est de la forme $([M_n]B)_n$. Soit $c = K(O,B;E)$, alors

$$\begin{cases} M_c^{O,B} = M_0^{O,B} \\ M_{c+1}^{O,B} = M_1^{O,B} \end{cases} \iff \begin{cases} [M_c]B = [M_0]B = [0]B \\ [M_{c+1}]B = [M_1]B = [1]B \end{cases}$$
$$\iff \begin{cases} M_c \equiv 0 \bmod h_B \\ M_{c+1} \equiv 1 \bmod h_B \end{cases}.$$

La dernière équivalence résulte du Lemme 1.2.1. Puisque c est le plus petit entier positif vérifiant ce dernier système, on en déduit $c = k(h_B)$.

(b) La preuve est analogue à celle de la Proposition 3.2.2(d).

(c) On sait que $h_A | h$ et $h_B | h$. Par conséquent, d'après le Théorème 3.1.3 (e), on a $k(h_A) | k(h)$ et $k(h_B) | k(h)$, donc $\mathrm{ppcm}\big(k(h_A), k(h_B)\big) | k(h)$. D'après (a), on a $k(h_A) = K(A,O;E)$ et $k(h_B) = K(O,B;E)$. Le résultat découle de (b).

□

Corollaire 3.3.2.1. *Soient A et B deux points de $E(\mathbb{F}_p)$ et supposons qu'on est dans le cas $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, avec n_1, $n_2 \geq 1$ des entiers donnés tels que n_1 divise n_2, alors $K(A,B;E)|k(n_2)$.*

Démonstration. Découle d'une preuve analogue à celle du Théorème 3.3.2 (c) en utilisant le Théorème 1.2.4 et le fait que l'ordre de tout point de $E(\mathbb{F}_p)$ divise n_2. □

Puisqu'on a $k(h_B) = K(O,B;E)$, certaines propriétés de la suite ordinaire $(M_n)_n$ peuvent être transférées à des propriétés analogues pour les suites $(M_n^{O,B})_n$ sur une courbe elliptique.

Théorème 3.3.3. *Soient A et B deux points de $E(\mathbb{F}_p)$.*

(a) Si h_B est un nombre premier impair et t^2+4t est un résidu quadratique modulo h_B, alors $K(O,B;E)|(h_B-1)$.

(b) Si h_B est un nombre premier impair et t^2+4t est un non résidu quadratique modulo h_B, alors $K(O,B;E)|(h_B+1)$.

(c) Si h_B est un nombre premier impair et $h_B|(t^2+4t)$, alors $K(O,B;E)|2{h_B}^2$.

(d) Si $\prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de h_B, alors $K(O,B;E) = \mathrm{ppcm}\big(k(p_i^{e_i})\big)$.

(e) Si $h_A|h_B$, alors $k(h_A)|k(h_B)$.

Démonstration. Utiliser le résultat du Théorème 3.3.2 (a) dans le Théorème 3.1.3. □

On donne maintenant la notion analogue d'une classe d'équivalence pour les suites définies sur les courbes elliptiques. On dit que (A',B') est équivalent à (A,B) s'il existe un indice i tel que $M_i^{A,B} = A'$ et $M_{i+1}^{A,B} = B'$. Comme pour le cas ordinaire, la taille d'une classe d'équivalence contenant (A,B) est $K(A,B;E)$. On définit $C_d(E)$ comme étant le nombre de classes d'équivalence distinctes de taille d.

Des résultats partiels pour les petites classes d'équivalence sont décrits dans la proposition suivante.

[2]Dans la référence [4] nous n'avons pas explicité que $K(O,B;E)|2h_B$, on a juste précisé que $K(O,B;E)|h_B(h_B-1)$.

Proposition 3.3.4. *Soit E une courbe elliptique sur $\mathbb{F}_p$.*

(a) $C_1(E) = \#\{P \in E(\mathbb{F}_p) \mid t \equiv 0 \ mod\ h_P\} \geq 1$.

(b) *(i)* *Soit* $\alpha = \#\{P \in E(\mathbb{F}_p) \mid (4+t) \equiv 0 \ mod\ h_P\}$. *Si* $\text{pgcd}(h,t) = 1$, *alors* $C_2(E) = (\alpha - 1)/2$.

(ii) *Soit* $\beta = \#\{(P,Q) \in E(\mathbb{F}_p)^2 \mid P \neq Q \text{ et } [2]P = [2]Q\}$. *Si* $h|t$, *alors*

$$\begin{cases} C_2(E) = 0, & \text{si } h \text{ est impair}, \\ C_2(E) = \beta/2, & \text{si } h \text{ est pair}. \end{cases} \tag{3.15}$$

Démonstration.

(a) Une suite de période 1 est de la forme $P, P, P, \ldots$. Ainsi, $[2+t]P - P = P$, ce qui est équivalent à $[t]P = O$. Cela équivaut, d'après Lemme 1.2.1, à $t \equiv 0 \bmod h_P$. On note que la suite triviale est toujours de période 1.

(b) Une suite de période 2 est de la forme $P, Q, P, Q, \ldots$. Ainsi, on a

$$\begin{cases} [2+t]Q - P = P \\ [2+t]P - Q = Q \end{cases} \iff \begin{cases} [t](P+Q) = O \\ [2+t]P - [2]Q = O \end{cases} \tag{3.16}$$

$$\iff \begin{cases} t \equiv 0 \bmod h_{P+Q} \\ [2+t]P - [2]Q = O \end{cases}. \tag{3.17}$$

(i) Si $\text{pgcd}(h,t) = 1$, alors (4.3) est équivalent à $h_{P+Q} = 1$, i.e., $Q = -P$, et $[4+t]P = O$. Ainsi, en enlevant les cas où $P = -P$ et où les mêmes suites $P, -P, P, -P, \ldots$ et $-P, P, -P, P, \ldots$ sont obtenues, il ne reste que $(\alpha - 1)/2$ suites différentes de période 2. On note que, puisque $\text{pgcd}(h,t) = 1$, il n'y a aucune contribution de points d'ordre 2 à α. On note aussi que $\alpha - 1$ est toujours pair, puisque $h_P = h_{-P}$ et $P = O$ n'est pas considéré.

(ii) Si $h|t$, alors (4.2) est équivalent à $[2](P - Q) = O$. Si h est impair, il n'y a aucun point d'ordre 2 dans $E(\mathbb{F}_p)$ et $C_2(E) = 0$ (la cas $P = Q$ donne une suite de période 1). Si h est pair, en enlevant les cas où les mêmes suites $P, Q, P, Q, \ldots$ et $Q, P, Q, P, \ldots$ sont obtenues, on obtient $C_2(E) = \beta/2$. On note que β est toujours pair, puisque (P,Q) et (Q,P) satisfont les mêmes conditions.

□

Par exemple, sur la courbe elliptique $E : y^2 = x^3 + x + 1$ considérée sur $\mathbb{F}_5$, on a $E(\mathbb{F}_5) = \{P_j = [j]P_1, 0 \leq j \leq 8\}$, où $P_1 = (0,1)$. Le point P_1 est d'ordre 9 et engendre ce groupe. Ainsi, $E(\mathbb{F}_5) \simeq \mathbb{Z}/9\mathbb{Z}$. Par conséquent, travailler sur $E(\mathbb{F}_5)$ revient à travailler sur les suites de Morgan-Voyce ordinaires modulo 9 et on a $C_d(E) = c_d(9)$ pour tout d. Par exemple, si $t = 3$, alors $C_1(E) = \#\{O, P_3, P_6\} = 3 = \text{pgcd}(3,9) = c_1(9)$. Si $t = 1$, alors $\alpha = 1$, donc $C_2(E) = 0 = c_2(9)$.

Le théorème suivant est analogue au Théorème 3.2.10.

Théorème 3.3.5. *Soient A et B deux points de $E(\mathbb{F}_p)$ tels que $(A,B) \neq (O,O)$ et w_c^{MV} les déterminants des matrices circulantes de Morgan-Voyce définis comme précédemment. Si $c = K(A,B;E)$, alors* $\text{pgcd}(w_c^{MV}, h) \neq 1$.

Démonstration. Découle d'une preuve analogue à celle du Théorème 3.2.10. Notons que la matrice W_n^{MV}, qui intervient dans l'équation matricielle, contient uniquement des multiples entiers de points d'une courbe elliptique et par conséquent, la matrice garde tout son sens. Compte tenu du Lemme 1.2.1 et du fait que chaque point R de $E(\mathbb{F}_p)$ est d'ordre divisant $h = ord(E(\mathbb{F}_p))$, on peut considérer W_n^{MV} modulo h et le système aura des solutions triviales lorsque w_n^{MV} est premier avec h. □

Le théorème suivant est analogue au Théorème 3.2.5.

Théorème 3.3.6. *Soient E une courbe elliptique sur $\mathbb{F}_p$ et $C_d(E)$ défini comme précédemment, alors*

$$h^2 = \sum_{d|k(h)} d \cdot C_d(E).$$

Démonstration. Résulte du fait que les classes d'équivalence forment une partition de $E(\mathbb{F}_p)^2$ et que, d'après le Théorème 3.3.2(c), toutes les classes ont une taille qui divise $k(h)$. □

Corollaire 3.3.6.1. *Supposons qu'on a $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ pour $n_1, n_2 \geq 1$ des entiers donnés tels que n_1 divise n_2, alors*

$$h^2 = \sum_{d|k(n_2)} d \cdot C_d(E).$$

Démonstration. Découle du Théorème 3.3.6 et du Corollaire 3.3.2.1. □

CHAPITRE 4

PÉRIODES DES SUITES QUASI MORGAN-VOYCE ET COURBES ELLIPTIQUES

Dans ce chapitre, on étudie la suite quasi Morgan-Voyce $(D_n)_n$ qui est une suite récurrente linéaire d'ordre 2 définie par

$$\begin{cases} D_1 = 1,\ D_2 = 1+t+s, \\ D_n = (2+t)D_{n-1} + D_{n-2},\ \ (n \geq 3). \end{cases}$$

Comme dans le chapitre précédent, on suppose que s et t sont entiers. La matrice compagnon de la suite quasi Morgan-Voyce est $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 2+t \end{smallmatrix}\right)$. Cette matrice est de déterminant -1, elle est donc inversible modulo tout entier $m \geq 2$. On en déduit, d'après le Lemme 2.1.1, que la suite $(D_n)_n$ modulo m est simplement périodique.

On commence par le cas $s = 1$. Dans ce cas, les deux premiers termes de notre suite sont $D_1 = 1$ et $D_2 = 2+t$. D'après la relation de récurrence, on peut définir $D_0 = D_2 - (2+t)D_1 = 0$. Dans ce qui suit, on note par $(D_n)_n$ la suite quasi Morgan-Voyce avec les valeurs initiales $D_0 = 0$ et $D_1 = 1$. On notera aussi par $k(m)$ la période de la suite $(D_n)_n$ modulo m, i.e., le plus petit entier strictement positif k tel que $D_k \equiv 0 \bmod m$ et $D_{k+1} \equiv 1 \bmod m$. Notons que si $m|(1+t)$, alors $D_n \equiv F_n \bmod m$ pour tout $n \geq 0$, où $(F_n)_n$ est la suite de Fibonacci. De sorte que, dans ce cas, tous les résultats sur la suite de Fibonacci modulo un entier $m \geq 2$ se généralisent à la suite quasi Morgan-Voyce. Cependant, on va voir que la suite quasi Morgan-Voyce vérifie des identités qui sont vérifiées par la suite de Fibonacci, ce qui va nous permettre de généraliser des résultats du cas Fibonacci au cas quasi Morgan-Voyce pour tout entier t. Notons que si $m|t$, alors $D_n \equiv P_n$ pour tout $n \geq 0$, où $(P_n)_n$ est la suite de Pell.

4.1 La suite quasi Morgan-Voyce

Soit $F(x) = x^2 - (2+t)x - 1$ le polynôme caractéristique de la suite $(D_n)_n$.

Théorème 4.1.1. *Soit $p \neq 2$ un nombre premier.*

(a) Si $F(x)$ a deux racines distinctes modulo p, alors $k(p)|(p-1)$.

(b) Si $F(x)$ est irréductible modulo p, alors $k(p)|2(p+1)$.

(c) Si $F(x)$ a une racine double modulo p, alors $k(p)|4p$[1].

Démonstration. Même preuve que pour le Théorème 3.1.2, sauf que dans ce cas on a $\tau_1 = 2$ pour (b) et $\tau_1|4$ pour (c). □

Les deux lemmes suivants découlent du fait que

$$4F(x) = \big(2x-(2+t)\big)^2 - (t^2+4t+8).$$

Lemme 4.1.1. *Soit $p \neq 2$ un nombre premier, alors*

$$F(x) \equiv 0 \ mod\ p \iff \big(2x-(2+t)\big)^2 \equiv t^2+4t+8 \ mod\ p.$$

Lemme 4.1.2. *Soit $p \neq 2$ un nombre premier, alors $F(x)$ a une racine double modulo p, si et seulement si, $t^2+4t+8 \equiv 0$ mod p.*

Théorème 4.1.2. *Soient $p \neq 2$ un nombre premier et $m \geq 2$ un entier.*

(a) Si t^2+4t+8 est un résidu quadratique modulo p, alors $k(p)|(p-1)$.

(b) Si t^2+4t+8 est un non résidu quadratique modulo p, alors $k(p)|2(p+1)$.

(c) Si $p|(t^2+4t+8)$, alors $k(p)|4p$.

(d) Si $m = \prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de m, alors on a $k(m) = \text{ppcm}\big(k(p_i^{e_i})\big)$.

(e) Si $n|m$, alors $k(n)|k(m)$.

Démonstration. (a), (b) et (c) sont des conséquences du Théorème 4.1.1 et des Lemmes 4.1.1 et 4.1.2. Pour (d) voir le Lemme 2.1.2. Pour (e), la même preuve que pour le Théorème 3.1.3 (e) reste valable. □

On va décrire, pour certaines valeurs de t, les nombres premiers p pour lesquels $k(p)|(p-1)$ et ceux pour lesquels $k(p)|2(p+1)$.

(1) Pour $t = -1$, la suite $(D_n)_n$ est définie par $D_n = D_{n-1} + D_{n-2}$, donc on est dans le cas Fibonacci, voir [12].

[1] Dans la référence [2] nous n'avons pas explicité que $k(p)|4p$, on a juste précisé que $k(p)|p(p-1)$.

(2) Pour $t = 0$, la suite $(D_n)_n$ est définie par $D_n = 2D_{n-1} + D_{n-2}$, Cette suite correspond à A000129 dans [31] (Les nombres de Pell). Dans ce cas, $t^2 + 4t + 8 = 8$ et d'après (b) de la Proposition 1.1.1, on a $(8/p) = (2/p)^3 = (2/p)$. On a vu dans la Proposition 1.1.2 que 2 est un résidu quadratique pour les nombres premiers de la forme $8k \pm 1$ et 2 est un non résidu quadratique pour les nombres premiers de la forme $8k \pm 3$. On en déduit que si $p = 8k \pm 1$, alors $k(p)|(p-1)$ et si $p = 8k \pm 3$, alors $k(p)|2(p+1)$. Le calcul nous donne $k(2) = 2$. Dans le Tableau 4.I, on donne la suite $(D_n)_n$ modulo de petits nombres premiers p de la forme $8k \pm 1$, ainsi que ses périodes. Dans le Tableau 4.II, on donne la suite $(D_n)_n$ modulo de petits nombres premiers p de la forme $8k \pm 3$ et ses périodes.

p	$(D_n \bmod p)_n$	$k(p)\|(p-1)$
7	$0,1,2,5,5,1;0,1$	$k(7) = 6$
17	$0,1,2,5,12,12,2,16,0,16,15,12,5,5,15,1;0,1$	$k(17) = 16$
23	$0,1,2,5,12,6,1,8,17,19,9,14,14,19,6,8,22,6,11,5,21,1;0,1$	$k(23) = 22$
31	$0,1,2,5,12,29,8,14,5,24,22,6,3,12,27,4,4,12,28,6,9,24,26,14,$ $23,29,19,5,29,1;0,1$	$k(31) = 30$
41	$0,1,2,5,12,29,29,5,39,1;0,1$	$k(41) = 10$

Tableau 4.I – périodes modulo de petits p de la forme $8k \pm 1$.

p	$(D_n \bmod p)_n$	$k(p)\|2(p+1)$
3	$0,1,2,2,0,2,1,1;0,1$	$k(3) = 8$
5	$0,1,2,0,2,4,0,4,3,0,3,1;0,1$	$k(5) = 12$
11	$0,1,2,5,1,7,4,4,1,6,2,10,0,10,9,6,10,4,7,7,10,5,9,1;0,1$	$k(11) = 24$
13	$0,1,2,5,12,3,5,0,5,10,12,8,2,12,0,12,11,8,1,10,8,0,8,$ $3,1,5,11,1;0,1$	$k(13) = 28$
19	$0,1,2,5,12,10,13,17,9,16,3,3,9,2,13,9,12,14,2,18,0,18,17,14,$ $7,9,6,2,10,3,16,16,10,17,6,10,7,5,17,1;0,1$	$k(19) = 40$
29	$0,1,2,5,12,0,12,24,2,28,0,28,27,24,17,0,17,5,27,1;0,1$	$k(29) = 20$
37	$0,1,2,5,12,29,33,21,1,23,10,6,22,13,11,35,7,12,31,0,31,25,7,2,$ $11,24,22,31,10,14,1,16,33,8,12,32,2,36,0,36,35,32,25,8,4,16,$ $36,14,27,31,15,24,26,2,30,25,6,0,6,12,30,35,26,13,15,6,27,$ $23,36,21,4,29,25,5,35,1;0,1$	$k(37) = 76$

Tableau 4.II – périodes modulo de petits p de la forme $8k \pm 3$.

(3) Pour $t = 1$, la suite $(D_n)_n$ donnée par $D_n = 3D_{n-1} + D_{n-2}$, cette suite correspond à A006190 dans [31]. Dans ce cas, $t^2 + 4t + 8 = 13$. L'assertion (c) nous dit que $k(13)|52$ et le calcul donne $k(13) = 52$. puisque $13 \equiv 1 \bmod 4$, d'après le Théorème 1.1.4 (a), 13 est un résidu quadratique modulo p si et seulement si $p \equiv r \bmod 13$, où r est un résidu quadratique modulo 13. Après calculs,

on obtient que si p est de la forme $26k \pm 1$, $26k \pm 3$, $26k \pm 9$ alors $k(p)|(p-1)$ et si p est de la forme $26k \pm 5$, $26k \pm 7$, $26k \pm 11$ alors $k(p)|2(p+1)$. Dans le Tableau 4.III, on donne la suite $(D_n)_n$ modulo de petits nombres premiers p de la forme $26k \pm 1$, $26k \pm 3$, $26k \pm 9$, ainsi que ses périodes. Dans le Tableau 4.IV, on donne la suite $(D_n)_n$ modulo de petits nombres premiers p de la forme $26k \pm 5$, $26k \pm 7$, $26k \pm 11$ et ses périodes.

p	$(D_n \bmod p)_n$	$k(p)\|(p-1)$
3	$0,1;0,1$	$k(3)=2$
17	$0,1,3,10,16,7,3,16,0,16,14,7,1,10,14,1;0,1$	$k(17)=16$
23	$0,1,3,10,10,17,15,16,17,21,11,8,12,21,6,16,8,17,13,10,20,1;0,1$	$k(23)=22$
29	$0,1,3,10,4,22,12,0,12,7,4,19,3,28,0,28,26,19,25,7,17,0,17,22,$ $25,10,26,1;0,1$	$k(29)=28$
43	$0,1,3,10,33,23,16,28,14,27,9,11,42,8,23,34,39,22,19,36,41,30,2,$ $36,24,22,4,34,20,8,1,11,34,27,29,28,27,23,10,10,40,1;0,1$	$k(43)=42$

Tableau 4.III – périodes modulo de petits p de la forme $26k \pm 1$, $26k \pm 3$, $26k \pm 9$.

p	$(D_n \bmod p)_n$	$k(p)\|2(p+1)$
5	$0,1,3,0,3,4,0,4,2,0,2,1;0,1$	$k(5)=12$
7	$0,1,3,3,5,4,3,6,0,6,4,4,2,3,4,1;0,1$	$k(7)=16$
11	$0,1,3,10,0,10,8,1;0,1$	$k(11)=8$
19	$0,1,3,10,14,14,18,11,13,12,11,7,13,8,18,5,14,9,3,18,0,18,16,$ $9,5,5,1,8,6,7,8,12,6,11,1,14,5,10,16,1;0,1$	$k(19)=40$
31	$0,1,3,10,2,16,19,11,21,12,26,28,17,17,6,4,18,27,6,14,17,3,26,$ $19,21,20,19,15,2,21,3,30,0,30,28,21,29,15,12,20,10,19,5,3,14,$ $14,25,27,13,4,25,17,14,28,5,12,10,11,12,16,29,10,28,1;0,1$	$k(31)=64$
37	$0,1,3,10,33,35,27,5,5,20,28,30,7,14,12,13,14,18,31,0,31,19,14,$ $24,12,23,7,7,28,17,5,32,27,2,33,27,3,36,0,36,34,27,4,2,10,32,$ $32,17,9,7,30,23,25,24,23,19,6,0,6,18,23,13,25,14,30,30,9,$ $20,32,5,10,35,4,10,34,1;0,1$	$k(37)=76$
41	$0,1,3,10,33,27,32,0,32,14,33,31,3,40,0,40,38,31,8,14,9,0,9,27,$ $8,10,38,1;0,1$	$k(41)=28$

Tableau 4.IV – périodes modulo de petits p de la forme $26k \pm 5$, $26k \pm 7$, $26k \pm 11$.

(4) Pour $t=2$, la suite $(D_n)_n$ est définie par $D_n = 4D_{n-1} + D_{n-2}$, cette suite correspond à A001076 dans [31]. Dans ce cas, $t^2+4t+8 = 20$. L'assertion (c) nous dit que $k(5)|20$ et les calculs donnent $k(2)=2$ et $k(5)=20$. D'après (b) de la Proposition 1.1.1, on a $(20/p) = (2/p)^2(5/p) = (5/p)$. On a vu dans le Chapitre 1 que 5 est un résidu quadratique pour les nombres premiers de la forme $10k \pm 1$ et 5 est un non résidu quadratique pour les nombres premiers de la forme $10k \pm 3$. On en déduit que si $p = 10k \pm 1$, alors $k(p)|(p-1)$ et si $p = 10k \pm 3$, alors $k(p)|2(p+1)$. Dans

le Tableau 4.V, on donne la suite $(D_n)_n$ modulo de petits nombres premiers p de la forme $10k \pm 1$, ainsi que ses périodes. Dans le Tableau 4.VI, on donne la suite $(D_n)_n$ modulo de petits nombres premiers p de la forme $10k \pm 3$ et ses périodes.

p	$(D_n \bmod p)_n$	$k(p)\|(p-1)$
11	$0,1,4,6,6,8,5,6,7,1;0,1$	$k(11)=10$
19	$0,1,4,17,15,1;0,1$	$k(19)=6$
29	$0,1,4,17,14,15,16,21,13,15,15,17,25,1;0,1$	$k(29)=14$
31	$0,1,4,17,10,26,21,17,27,1;0,1$	$k(31)=10$
41	$0,1,4,17,31,18,21,20,19,14,34,27,19,21,21,23,31,24,4,40,0,40,$ $37,24,10,23,20,21,22,27,7,14,22,20,20,18,10,17,37,1;0,1$	$k(41)=40$

Tableau 4.V – périodes modulo de petits p de la forme $10k \pm 1$.

p	$(D_n \bmod p)_n$	$k(p)\|2(p+1)$
3	$0,1,1,2,0,2,2,1;0,1$	$k(3)=8$
7	$0,1,4,3,2,4,4,6,0,6,3,4,5,3,3,1;0,1$	$k(7)=16$
13	$0,1,4,4,7,6,5,0,5,7,7,9,4,12,0,12,9,9,6,7,8,0,8,6,6,4,9,1;0,1$	$k(13)=28$
17	$0,1,4,0,4,16,0,16,13,0,13,1;0,1$	$k(17)=12$
23	$0,1,4,17,3,6,4,22,0,22,19,6,20,17,19,1;0,1$	$k(23)=16$
37	$0,1,4,17,35,9,34,34,22,11,29,16,19,18,17,12,28,13,6,0,6,24,28,$ $25,17,19,19,21,29,26,22,3,34,28,35,20,4,36,0,36,33,20,2,28,3,$ $3,15,26,8,21,18,19,20,25,9,24,31,0,31,13,9,12,20,18,18,16,8,$ $11,15,34,40,9,2,17,33,1;0,1$	$k(37)=76$

Tableau 4.VI – périodes modulo de petits p de la forme $10k \pm 3$.

Notons qu'il existe des cas faciles. Par exemple, si $t=-2$ on obtient $F(x)=x^2-1$, donc $F(x)$ a une racine double pour $p=2$ et deux racines distinctes pour $p>2$. Ainsi, on a $k(p)|(p-1)$ pour $p>2$. En fait, la suite $(D_n)_n$ est définie par $D_n=D_{n-2}$, donc on a $D_0=0,D_1=1,D_0=0,D_1=1,\ldots$. Par conséquent, on a $k(m)=2$ pour tout $m\geq 2$.

Soient $\alpha=[(2+t)+\sqrt{\Delta}]/2$ et $\beta=[(2+t)-\sqrt{\Delta}]/2$ les racines complexes du polynôme caractéristique $F(x)$, où $\Delta=(2+t)^2+4$. Ces racines sont distinctes pour tout entier t. On a les identités suivantes

$$D_n^2-D_{n-1}D_{n+1}=(-1)^{n+1}, \qquad (n\geq 1), \tag{4.1}$$

$$D_{n+g}=D_{n+1}D_g+D_nD_{g-1}, \qquad (g\geq 1, n\geq 0), \tag{4.2}$$

$$\alpha^n\beta^n=(-1)^n \qquad (n\geq 0), \tag{4.3}$$

$$D_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}, \qquad (n\geq 0), \tag{4.4}$$

$$D_{n+1} + D_{n-1} = \alpha^n + \beta^n, \qquad (n \geq 1). \tag{4.5}$$

L'identité (4.2) se démontre par récurrence, l'identité (4.3) est évidente. Pour les identités (4.1), (4.4) et (4.5), voir [18].

Etant donné que les identités ci-dessus sont les mêmes que celles vérifiées par la suite de Fibonacci $(F_n)_n$, on a les mêmes résultats suivants.

Théorème 4.1.3. *Les indices des termes D_n pour lesquels $D_n \equiv 0$ mod m forment une progression arithmétique simple. C'est-à-dire, $n = xd$, pour $x = 0, 1, 2, \ldots$ et un certain nombre entier strictement positif $d = d(m)$, donne tous les n vérifiant $D_n \equiv 0$ mod m.*

Démonstration. La même preuve que dans le cas Fibonacci en utilisant les identités (4.1) et (4.2), voir [37, Théorème 3]. Le fait que $\text{pgcd}(D_n, D_{n+1}) = 1$ se déduit de l'identité (4.1). On peut aussi le voir de la façon suivante. Si $d > 0$ est un diviseur de D_n et D_{n+1}, alors d divise aussi le terme précédent puisque $D_{n-1} = D_{n+1} - (2+t)D_n$. En réitérant cette opération, on démontre que tous les termes précédents sont divisibles par d, donc en particulier $d | D_1 = 1$. □

D'après le Théorème 4.1.3, on voit que $d(m)$ est le plus petit entier strictement positif k vérifiant $D_k \equiv 0 \bmod m$. En particulier, on a $d(m) | k(m)$. On définit une fonction $l(m)$ par l'équation $d(m)l(m) = k(m)$. Notons que l(m) est le nombre de zéros dans la période de la suite $(D_n \bmod m)_n$.

Théorème 4.1.4. *Soit $m \geq 2$ un entier, alors*

1. *$l(m)$ est le plus petit entier strictement positif n vérifiant $D^n_{d(m)-1} \equiv 1$ mod m.*
2. *Pour $m > 2$, on a*
   (a) *$l(m) = 1$ ou 2 si $d(m)$ est pair, et*
   (b) *$l(m) = 4$ si $d(m)$ est impair.*
   De plus, $l(1) = l(2) = 1$. Inversement, $l(m) = 4$ implique $d(m)$ est impair, $l(m) = 2$ implique $d(m)$ est pair, et $l(m) = 1$ implique $d(m)$ est pair ou $m = 1$ ou 2.

Démonstration. La même preuve que dans le cas Fibonacci en utilisant les identités (4.1), (4.3) et (4.4). Voir [35, Lemme 1 et Théorème 1]. □

Par exemple, dans le Tableau 4.II, $d(5) = 3$, $d(13) = 7$, $d(29) = 5$, $d(37) = 19$ et on a bien $l(5) = l(13) = l(29) = l(37) = 4$, alors que $d(3) = 4$, $d(11) = 12$, $d(19) = 20$ et on a bien $l(3) =$

$l(11) = l(19) = 2$. Dans le Tableau 4.I, $d(7) = 6$, $d(23) = 22$, $d(31) = 30$, $d(41) = 10$ et on a bien $l(7) = l(23) = l(31) = l(41) = 1$.

Méthode de calcul de $k(m)$: au lieu de calculer tous les M_i mod m jusqu'à obtenir 0 et 1 comme deux termes consécutifs, on commence par calculer les M_i mod m pour $i = 2,3,\ldots$, dés qu'on obtient un M_i qui est congru à 0 modulo m alors $d(m) = i$. Si $d(m)$ est impair, alors $l(m) = 4$ et $k(m) = 4d(m)$. Si $d(m)$ est pair, alors $l(m) = 1$ ou 2. Dans ce cas il suffit de voir $M_{d(m)+1}$ mod m. Si $M_{d(m)+1} \equiv 1 \bmod m$, alors $l(m) = 1$ et $k(m) = d(m)$, si $M_{d(m)+1} \not\equiv 1 \bmod m$, alors $l(m) = 2$ et $k(m) = 2d(m)$.

4.2 La suite quasi Morgan-Voyce avec des conditions initiales généralisées

Soient a et b des entiers et considérons la suite $(D_n^{a,b})_n$ définie par

$$D_0^{a,b} = a,\ \ D_1^{a,b} = b \ \text{ et } \ D_n^{a,b} = (2+t)D_{n-1}^{a,b} + D_{n-2}^{a,b} \ \text{ pour } \ n \geq 2.$$

Puisque la matrice compagnon de la suite $(D_n^{a,b})_n$ est la même que celle de la suite $(D_n)_n$, on en déduit que la suite $(D_n^{a,b} \bmod m)_n$ est simplement périodique, pour tout entier $m \geq 2$. On désigne par $k(a,b;m)$ la période de la suite $(D_n^{a,b} \bmod m)_n$, i.e., le plus petit entier strictement positif k tel que $D_k^{a,b} \equiv a \bmod m$ et $D_{k+1}^{a,b} \equiv b \bmod m$. La suite $(D_n^{2,2+t})_n$, appelée suite compagnon de $(D_n)_n$, satisfait plusieurs propriétés, voir [18]. La proposition suivante indique qu'on peut exprimer la suite $(D_n^{a,b})_n$ en fonction de la suite $(D_n)_n$. Notons qu'à partir de la relation de récurrence, on peut définir $D_{-1} = D_1 - (2+t)D_0 = 1$.

Proposition 4.2.1. *La suite $(D_n^{a,b})_n$ satisfait*

$$D_n^{a,b} = bD_n + aD_{n-1}, \qquad (n \geq 0). \tag{4.6}$$

Démonstration. Cela découle d'une simple récurrence. □

Proposition 4.2.2. *Soient a,b et m des entiers avec $m \geq 2$, alors*

(a) $k(a,b;m) | k(m)$.

(b) $k(b,0;m) = k(0,b;m)$ *et* $k(0,b;m) | k(m)$.

(c) Si $\text{pgcd}(b,m) = 1$, *alors* $k(0,b;m) = k(m)$.

(d) $k(a,b;m)|\text{ppcm}\big(k(a,0;m),k(0,b;m)\big)$.

Démonstration.

(a) La relation (4.6) donne

$$\begin{cases} D^{a,b}_{k(m)} = bD_{k(m)} + aD_{k(m)-1} \\ D^{a,b}_{k(m)+1} = bD_{k(m)+1} + aD_{k(m)} \end{cases} \Longrightarrow \begin{cases} D^{a,b}_{k(m)} \equiv bD_0 + aD_{-1} \bmod m \\ D^{a,b}_{k(m)+1} \equiv bD_1 + aD_0 \bmod m \end{cases}$$
$$\Longrightarrow \begin{cases} D^{a,b}_{k(m)} \equiv a \bmod m \\ D^{a,b}_{k(m)+1} \equiv b \bmod m \end{cases}.$$

Il vient que $k(a,b;m)|k(m)$. Remarquons que (a) peut se déduire aussi de (b) et (d).

(b) Il est clair que $D^{b,0}_{n+1} = D^{0,b}_n$ pour tout $n \geq 0$, il vient que $k(b,0;m) = k(0,b;m)$. Le fait que $k(0,b;m)|k(m)$ est un cas particulier de (a).

(c) Même preuve que dans le cas Morgan-Voyce, voir la Proposition 3.2.2 (c).

(d) D'après la relation (4.6), on a $D^{0,b}_n = bD_n$ et $D^{a,0}_n = aD_{n-1}$, pour tout $n \geq 0$. Posons $\sigma = k(a,0;m)$ et $\tau = k(0,b;m)$, alors $D^{a,0}_\sigma \equiv a \bmod m$, $D^{a,0}_{\sigma+1} \equiv 0 \bmod m$ et $D^{0,b}_\tau \equiv 0 \bmod m$, $D^{0,b}_{\tau+1} \equiv b \bmod m$. Soit $\theta = \text{ppcm}(\sigma,\tau)$. Puisque $\sigma|\theta$ et $\tau|\theta$, on a $aD_{\theta-1} = D^{a,0}_\theta \equiv a \bmod m$, $aD_\theta = D^{a,0}_{\theta+1} \equiv 0 \bmod m$, $bD_\theta = D^{0,b}_\theta \equiv 0 \bmod m$ et $bD_{\theta+1} = D^{0,b}_{\theta+1} \equiv b \bmod m$. On déduit de ces quatre dernières congruences et de la relation (4.6) que $D^{a,b}_\theta = bD_\theta + aD_{\theta-1} \equiv a \bmod m$ et $D^{a,b}_{\theta+1} = bD_{\theta+1} + aD_\theta \equiv b \bmod m$, i.e., $k(a,b;m)|\theta = \text{ppcm}\big(k(a,0;m),k(0,b;m)\big)$.

□

Lemme 4.2.1. *Soient a,b et m des entiers tels que* $\text{pgcd}(a,b,m) = 1$ *et supposons que $m = p^e$ pour un nombre premier impair p et un entier strictement positif e. Si $g = k(a,b;m)$ est pair, alors $D^{2,2+t}_g \equiv 2$ mod m.*

Démonstration. Il est facile de voir que $D^{2,2+t}_n = D_{n+1} + D_{n-1}$ pour tout $n \geq 0$. On a

$$\begin{cases} D^{a,b}_g \equiv a \bmod m \\ D^{a,b}_{g+1} \equiv b \bmod m \end{cases} \Longleftrightarrow \begin{cases} bD_g + aD_{g-1} \equiv a \bmod m \\ bD_{g+1} + aD_g \equiv b \bmod m \end{cases}$$
$$\Longleftrightarrow \begin{cases} bD_g + a(D_{g-1} - 1) \equiv 0 \bmod m \\ b(D_{g+1} - 1) + aD_g \equiv 0 \bmod m \end{cases}.$$

Puisque $\text{pgcd}(a,b,m) = 1$, on obtient $D_g^2 - (D_{g+1} - 1)(D_{g-1} - 1) \equiv 0 \bmod m$, qui, à l'aide de l'identité (4.1), devient $D_{g+1} + D_{g-1} \equiv 2 \bmod m$, c'est-à-dire, $D_g^{2,2+t} \equiv 2 \bmod m$. □

Le théorème suivant est un analogue au Théorème 12 dans [37] pour le cas quasi Morgan-Voyce, que nous énonçons dans le cas $m = p$ un nombre premier différent de 2, alors que dans [37] il est énoncé pour $m = p^e$ une puissance d'un nombre premier impair. Nous pensons que dans l'article de Wall [37], pour une puissance d'un premier, il y a un problème dans la preuve.

Théorème 4.2.3. *Soit $p > 2$ un nombre premier tel que $p \nmid (t^2 + 4t + 8)$; soient a et b des entiers tels que* $\text{pgcd}(a,b,p) = 1$. *Si $g = k(a,b;p)$ est pair, alors $g = k(p)$.*

Démonstration. D'après l'identité (4.5), on a $D_n^{2,2+t} = \alpha^n + \beta^n$ pour $n \geq 0$. Par conséquent, d'après le Lemme 4.2.1, on a

$$\alpha^g + \beta^g - 2 \equiv 0 \bmod p.$$

Puisque $\alpha\beta = -1$, on trouve

$$(\alpha^g - \beta^g)^2 = (\alpha^g + \beta^g - 2)^2 + 4(\alpha^g + \beta^g - 2) \equiv 0 \bmod p.$$

Maintenant, puisque $p \nmid (t^2 + 4t + 8)$, on divise la relation ci-dessus par $(\alpha - \beta)^2 = t^2 + 4t + 8$ pour obtenir

$$\left(\frac{\alpha^g - \beta^g}{\alpha - \beta}\right)^2 = D_g^2 \equiv 0 \bmod p,$$

d'où $D_g \equiv 0 \bmod p$. De l'identité $D_{g+1} = (2+t)D_g + D_{g-1}$, on obtient $D_{g+1} \equiv D_{g-1} \bmod p$. Cette dernière congruence avec $D_{g+1} + D_{g-1} \equiv 2 \bmod p$ impliquent $D_{g+1} \equiv D_{g-1} \equiv 1 \bmod p$. Ainsi, on obtient $k(p) | g$ et on déduit de la Proposition 4.2.2(a) que $g = k(p)$. □

Considérons maintenant une relation binaire sur l'ensemble $(\mathbb{Z}/m\mathbb{Z})^2$ définie par $(a,b) \sim (q,r)$, si et seulement si, il existe un indice i tel que $D_i^{a,b} \equiv q \bmod m$ et $D_{i+1}^{a,b} \equiv r \bmod m$. Puisque deux termes consécutifs déterminent complètement la suite $(D_n^{a,b} \bmod m)_n$, il s'agit bien d'une relation d'équivalence sur $(\mathbb{Z}/m\mathbb{Z})^2$. Le Tableau 4.VII, où l'on a considéré $t = 1$, donne toutes les classes d'équivalence modulo 6.

Une suite $(D_n^{a,b})_n$ de période d modulo m est de la forme $D_0^{a,b}, D_1^{a,b}, D_2^{a,b}, \ldots, D_{d-1}^{a,b}, D_d^{a,b} \equiv D_0^{a,b}$, $D_{d+1}^{a,b} \equiv D_1^{a,b}, \ldots$. Par conséquent, les paires distinctes qui sont composées de deux termes consécutifs dans la suite $(D_n^{a,b} \bmod m)_n$ sont $(D_0^{a,b}, D_1^{a,b})$, $(D_1^{a,b}, D_2^{a,b})$, …, $(D_{d-1}^{a,b}, D_0^{a,b})$. Ainsi, on a d paires et on en déduit que la taille de la classe d'équivalence contenant (a,b) est $d = k(a,b;m)$.

$k(a,b;6)$	(a,b)
1	$(0,0)$
6	$(0,1),(1,3),(3,4),(4,3),(3,1),(1,0)$
2	$(0,2),(2,0)$
3	$(0,3),(3,3),(3,0)$
2	$(0,4),(4,0)$
6	$(0,5),(5,3),(3,2),(2,3),(3,5),(5,0)$
3	$(1,1),(1,4),(4,1)$
1	$(2,2)$
1	$(4,4)$
3	$(5,5),(5,2),(2,5)$
6	$(1,2),(2,1),(1,5),(5,4),(4,5),(5,1)$
2	$(2,4),(4,2)$

Tableau 4.VII – Les (a,b)-classes d'équivalence modulo 6.

Étant donné un entier $m \geq 2$ fixé, on définit $c_d(m)$ comme étant le nombre de classes d'équivalence distinctes de taille d. Ainsi, dans le Tableau 4.VII, on voit que $c_1(6) = c_2(6) = c_3(6) = c_6(6) = 3$ et $c_d(6) = 0$ pour tous les autres d.

Le théorème suivant compte les éléments de $(\mathbb{Z}/m\mathbb{Z})^2$ correspondant à la partition de cet ensemble en classes d'équivalence.

Théorème 4.2.4. *Soient $m \geq 2$ un entier et $c_d(m)$ défini comme ci-dessus, alors*

$$m^2 = \sum_{d|k(m)} d \cdot c_d(m).$$

Démonstration. La même preuve que dans le cas Morgan-Voyce, voir Théorème 3.2.5. □

Les petites classes d'équivalence sont décrites dans la proposition suivante.

Proposition 4.2.5. *Soient $m \geq 2$ un entier et $g = \text{pgcd}(2+t,m)$.*

(a) $c_1(m) = g$.

(b) $c_2(m) = g(g-1)/2$.

(c) Si $m|(2+t)$, alors $k(m) = 2$, $c_1(m) = m$, $c_2(m) = m(m-1)/2$ et $c_d(m) = 0$ pour tous les autres d.

Démonstration. Posons $2+t = gt_1$ et $m = gm_1$ avec $\text{pgcd}(t_1,m_1) = 1$.

(a) Une suite de période 1 est de la forme a, a, a, ... modulo m. Ainsi, d'après la définition de la suite, on a $(2+t)a+a \equiv a \bmod m$, ce qui est équivalent à $a \equiv 0 \bmod m_1$, d'où $a = lm/g$ avec $l = 0, 1, \ldots, g-1$, i.e., $c_1(m) = g$.

(b) Une suite de période 2 est de la forme $a,b,a,b,\ldots$ modulo m. Ainsi, d'après la définition de la suite, on a $(2+t)a+b \equiv b \bmod m$ et $(2+t)b+a \equiv a \bmod m$, lesquelles sont équivalentes à $a \equiv 0 \bmod m_1$ et $b \equiv 0 \bmod m_1$. En enlevant les cas où $a = b$ et où les mêmes suites a, b, a, b, ... et b, a, b, a, ... sont obtenues, on obtient $a = l_1 m/g$ et $b = l_2 m/g$ avec $0 \leq l_1 < l_2 \leq g-1$, d'où $c_2(m) = g(g-1)/2$.

(c) Supposons que $m|(2+t)$. D'après (a) et (b), on a $c_1(m) + 2c_2(m) = m^2$. Par conséquent, d'après le Théorème 4.2.4, $c_d(m) = 0$ pour tous les autres d et $k(m) = 2$.

□

A l'exception de la suite $(D_n^{0,0})_n$ qui est toujours de longueur 1, on peut avoir toutes les classes de longueur $k(m)$, comme représenté dans le Tableau 4.VIII par le cas $t = 1$ et $m = 7$, avec $k(m) = 16$.

Diviseur d	1	2	4	8	16
$c_d(7)$	1	0	0	0	3

Tableau 4.VIII – Longueurs et nombre de classes d'équivalence modulo 7 pour $t = 1$.

En considérant, d'une manière générale, une suite $(D_n^{a,b})_n$ de période d modulo m, on a

$$D_0^{a,b} + D_2 D_1^{a,b} \equiv D_2^{a,b},\ D_1^{a,b} + D_2 D_2^{a,b} \equiv D_3^{a,b}, \ldots,\ D_{d-1}^{a,b} + D_2 D_0^{a,b} \equiv D_1^{a,b},$$

où $D_2 = 2+t$. Ainsi, on obtient

$$\begin{pmatrix} 1 & D_2 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & D_2 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & D_2 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & \cdots & 1 & D_2 \\ D_2 & -1 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} D_0^{a,b} \\ D_1^{a,b} \\ D_2^{a,b} \\ \vdots \\ D_{d-2}^{a,b} \\ D_{d-1}^{a,b} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \bmod m.$$

On définit la matrice circulante quasi Morgan-Voyce W_n^{QMV} par la matrice de taille n suivante

$$W_n^{QMV} := \begin{pmatrix} 1 & D_2 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & D_2 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & D_2 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & \cdots & 1 & D_2 \\ D_2 & -1 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Proposition 4.2.6. *Soit* $w_n^{QMV} = \det W_n^{QMV}$*, alors*

(a) $w_n^{QMV} = \prod_{j=0}^{n-1} \left(1 + D_2 e^{2i\pi j/n} - e^{4i\pi j/n}\right)$, $(n \geq 3)$.

(b) $w_n^{QMV} = (-1)^{n-1}\left((-1)^{n-1} - 1 + D_{n+1} + D_{n-1}\right)$, $(n \geq 3)$.

(c) Si n est impair, alors $w_n^{QMV} = D_{n+1} + D_{n-1} = D_n^{2,2+t}$, $(n \geq 3)$.

(d) $\begin{cases} w_1^{QMV} = 2+t, w_2^{QMV} = -(4+4t+t^2), \\ w_n^{QMV} = \left((-1)^{n-1}+1\right)(2+t) - (2+t)w_{n-1}^{QMV} + w_{n-2}^{QMV}, \end{cases}$ $(n \geq 3)$.

Démonstration. L'assertion (a) découle de l'identité (2.8). Pour avoir (b), on échelonne la matrice W_n^{QMV} exactement comme dans le cas Fibonacci, voir [12, Proposition 5 (b)]. L'assertion (c) découle de (b). Pour montrer (d), soit $n \geq 3$, alors on a d'après (b)

$$\begin{aligned} w_n^{QMV} &= (-1)^{n-1}\left[(-1)^{n-1} - 1 + D_{n+1} + D_{n-1}\right] \\ &= (-1)^{n-1}\left[(-1)^{n-1} - 1 + (2+t)D_n + D_{n-1} + (2+t)D_{n-2} + D_{n-3}\right] \\ &= (-1)^{n-1}(2+t)\left(D_n + D_{n-2}\right) + (-1)^{n-3}\left[(-1)^{n-3} - 1 + D_{n-1} + D_{n-3}\right] \\ &= (-1)^{n-1}(2+t)\left(D_n + D_{n-2} + (-1)^{n-2} - 1 - (-1)^{n-2} + 1\right) + w_{n-2}^{QMV} \\ &= \left((-1)^{n-1}+1\right)(2+t) - (2+t)w_{n-1}^{QMV} + w_{n-2}^{QMV}. \end{aligned}$$

$w_1^{QMV} = 2+t$ et $w_2^{QMV} = -(4+4t+t^2)$ donnent une définition de w_1^{QMV} et w_2^{QMV} inspirée par (b). □

Comme dans les cas Fibonacci et Morgan-Voyce, nous avons un théorème qui nous donne une relation entre w_n^{QMV} et la période de la suite $(D_n^{a,b})_n$ modulo m.

Théorème 4.2.7. *Soient a et b des entiers tels que* $(a,b) \not\equiv (0,0)$ *mod m, où* $m \geq 2$ *est un entier. Si* $l = k(a,b;m)$*, alors* $\text{pgcd}\left(w_l^{QMV}, m\right) \neq 1$.

Démonstration. La même preuve que dans le cas Morgan-Voyce fonctionne, voir Théorème 3.2.10. □

4.3 Suites quasi Morgan-Voyce sur les courbes elliptiques

Soient A et B deux points de $E(\mathbb{F}_p)$ où $E : y^2 = x^3 + ax + b$ est une courbe elliptique définie sur le corps fini $\mathbb{F}_p$, avec $p > 2$ un nombre premier. On définit la suite quasi Morgan-Voyce $(D_n^{A,B})_n$ sur la courbe elliptique E par

$$D_0^{A,B} = A,\ D_1^{A,B} = B \ \text{ et } \ D_n^{A,B} = [2+t]D_{n-1}^{A,B} + D_{n-2}^{A,B}, \quad \text{pour } \ n \geq 2.$$

Proposition 4.3.1. *Soient A et B deux points de* $E(\mathbb{F}_p)$.

(a) La suite $(D_n^{A,B})_n$ *est donnée par*

$$D_n^{A,B} = [D_n]B + [D_{n-1}]A, \quad \textit{pour } \ n \geq 0. \tag{4.7}$$

(b) La suite $(D_n^{A,B})_n$ *est simplement périodique.*

Démonstration. (a) découle d'une simple récurrence et (b) se démontre de la même façon que dans le cas Morgan-Voyce, voir Proposition 3.3.1 (b). □

On note par $K(A,B;E)$ la période de la suite $(D_n^{A,B})_n$, c'est-à-dire, le plus petit entier strictement positif k satisfaisant $D_k^{A,B} = A$ et $D_{k+1}^{A,B} = B$.

Comme dans le cas Morgan-Voyce, le Lemme 1.2.1 nous permet de faire le lien entre les périodes de $(D_n^{A,B})_n$ et les périodes de $(D_n \bmod m)_n$. On va voir que la période de la suite $(D_n^{O,B})_n$ ne dépend que de h_B, de sorte que tous les points R qui ont le même ordre vont engendrer des suites avec exactement la même longueur. Une fois cette connexion établie, on pourra généraliser les propriétés de la suite ordinaire $(D_n)_n$ à des suites $(D_n^{A,B})_n$ sur les courbes elliptiques.

Théorème 4.3.2. *Soient A et B deux points de* $E(\mathbb{F}_p)$.

(a) $K(B,O;E) = K(O,B;E) = k(h_B)$.

(b) $K(A,B;E)|\text{ppcm}\big(K(A,O;E),K(O,B;E)\big)$.

(c) $K(A,B;E)|k(h)$.

Démonstration.

(a) Il est clair que $D_{n+1}^{B,O}=D_n^{O,B}$ pour tout $n\geq 0$, il vient que $K(B,O;E)=K(O,B;E)$. D'après la relation (4.7), la suite $(D_n^{O,B})_n$ est de la forme $([D_n]B)_n$. Soit $c=K(O,B;E)$, alors

$$\begin{cases} D_c^{O,B}=D_0^{O,B} \\ D_{c+1}^{O,B}=D_1^{O,B} \end{cases} \iff \begin{cases} [D_c]B=[D_0]B=[0]B \\ [D_{c+1}]B=[D_1]B=[1]B \end{cases}$$

$$\iff \begin{cases} D_c\equiv 0 \bmod h_B \\ D_{c+1}\equiv 1 \bmod h_B \end{cases}.$$

La dernière équivalence résulte du Lemme 1.2.1. Puisque c est le plus petit entier positif vérifiant ce dernier système, on en déduit $c=k(h_B)$.

(b) La preuve est analogue à celle de la Proposition 4.2.2 (d).

(c) Même preuve que dans le cas Morgan-Voyce, voir Théorème 3.3.2 (c).

□

Corollaire 4.3.2.1. *Soient A et B deux points de $E(\mathbb{F}_p)$ et supposons qu'on est dans le cas $E(\mathbb{F}_p)\simeq \mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$, avec n_1, $n_2\geq 1$ des entiers donnés tels que n_1 divise n_2, alors $K(A,B;E)|k(n_2)$.*

Démonstration. Découle d'une preuve analogue à celle du Théorème 4.3.2 (c) en utilisant le Théorème 1.2.4 et le fait que l'ordre de tout point de $E(\mathbb{F}_p)$ divise n_2. □

Puisqu'on a $k(h_B)=K(O,B;E)$, certaines propriétés de la suite ordinaire $(D_n)_n$ peuvent être transférées à des propriétés analogues pour les suites $(D_n^{O,B})_n$ sur une courbe elliptique.

Théorème 4.3.3. *Soient A et B deux points de $E(\mathbb{F}_p)$.*

(a) Si h_B est un nombre premier impair et t^2+4t+8 est un résidu quadratique modulo h_B, alors $K(O,B;E)|(h_B-1)$.

(b) Si h_B est un nombre premier impair et t^2+4t+8 est un non résidu quadratique modulo h_B, alors $K(O,B;E)|2(h_B+1)$.

(c) Si h_B est un nombre premier impair et $h_B|(t^2+4t+8)$, alors $K(O,B;E)|4{h_B}^2$.

[2]Dans la référence [2] nous n'avons pas explicité que $K(O,B;E)|4h_B$, on a juste précisé que $K(O,B;E)|h_B(h_B-1)$.

(d) Si $\prod p_i^{e_i}$ *est la factorisation en produit de nombres premiers de* h_B*, alors* $K(O,B;E) = \text{ppcm}\big(k(p_i^{e_i})\big)$.

(e) Si $h_A | h_B$*, alors* $k(h_A) | k(h_B)$.

Démonstration. Utiliser le résultat du Théorème 4.3.2(a) dans le Théorème 4.1.2. □

On donne maintenant la notion analogue d'une classe d'équivalence pour les suites définies sur les courbes elliptiques. On dit que (A',B') est équivalent à (A,B) s'il existe un indice i tel que $D_i^{A,B} = A'$ et $D_{i+1}^{A,B} = B'$. Comme pour le cas ordinaire, la taille d'une classe d'équivalence contenant (A,B) est $K(A,B;E)$. On définit $C_d(E)$ comme étant le nombre de classes d'équivalence distinctes de taille d.

Proposition 4.3.4. *Soit* $\alpha = \#\{P \in E(\mathbb{F}_p) \mid h_P | (2+t)\}$*, où E est une courbe elliptique sur* $\mathbb{F}_p$.

(a) $C_1(E) = \alpha$.

(b) $C_2(E) = \alpha(\alpha-1)/2$.

Démonstration.

(a) Une suite de période 1 est de la forme P, P, P, ... Ainsi, $[2+t]P + P = P$, ce qui est équivalent, d'après le Lemme 1.2.1, à $2+t \equiv 0 \bmod h_P$. Notons que la suite triviale est toujours de période 1.

(b) Une suite de période 2 est de la forme P, R, P, R, ... Ainsi, $[2+t]R + P = P$ et $[2+t]P + R = R$, lesquelles sont équivalentes à $2+t \equiv 0 \bmod h_R$ et $2+t \equiv 0 \bmod h_P$. En enlevant les cas où $P = R$ et où les mêmes suites P, R, P, R, ... et R, P, R, P, ... sont obtenues, il ne reste que $\alpha(\alpha-1)/2$ suites différentes de période 2.

□

Par exemple, sur la courbe elliptique $E : y^2 = x^3 + x + 1$ considérée sur $\mathbb{F}_5$, on a $E(\mathbb{F}_5) = \{P_j = [j]P_1, 0 \leq j \leq 8\}$, où $P_1 = (0,1)$. Le point P_1 est d'ordre 9 et engendre ce groupe. Ainsi, $E(\mathbb{F}_5) \simeq \mathbb{Z}/9\mathbb{Z}$. Par conséquent, travailler sur $E(\mathbb{F}_5)$ revient à travailler sur les suites quasi Morgan-Voyce ordinaires modulo 9, et on a $C_d(E) = c_d(9)$ pour tout d. Par exemple, si $2+t \equiv 0 \bmod 9$, alors $\alpha = 9, C_1(E) = c_1(9) = 9$ et $C_2(E) = c_2(9) = 36$. Si $t = 1$, alors $\alpha = \#\{O, P_3, P_6\} = 3, C_1(E) =$

$c_1(9) = 3$ et $C_2(E) = c_2(9) = 3$.

Le théorème suivant est analogue au Théorème 4.2.7.

Théorème 4.3.5. *Soient A et B deux points de $E(\mathbb{F}_p)$ tels que $(A,B) \neq (O,O)$ et w_c^{QMV} les déterminants des matrices circulantes quasi Morgan-Voyce, comme précédemment. Si $c = K(A,B;E)$, alors* pgcd $\left(w_c^{QMV}, h\right) \neq 1$.

Démonstration. La même preuve que dans le cas Morgan-Voyce, voir Théorème 3.3.5. □

Le théorème suivant est analogue au Théorème 4.2.4.

Théorème 4.3.6. *Soient E une courbe elliptique sur $\mathbb{F}_p$ et $C_d(E)$ défini comme précédemment, alors*

$$h^2 = \sum_{d|k(h)} d \cdot C_d(E).$$

Démonstration. La même preuve que dans le cas Morgan-Voyce, voir Théorème 3.3.6. □

Corollaire 4.3.6.1. *Supposons qu'on a $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ pour $n_1, n_2 \geq 1$ des entiers donnés tels que n_1 divise n_2, alors*

$$h^2 = \sum_{d|k(n_2)} d \cdot C_d(E).$$

Démonstration. Découle du Théorème 4.3.6 et du Corollaire 4.3.2.1. □

Par exemple, sur la courbe elliptique $E : y^2 = x^3 + 2$ considérée sur $\mathbb{F}_7$, on a $E(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Si $t = 1$, il est facile de voir que $k(3) = 2$. D'après la Proposition 4.3.4, on a $C_1(E) = 9$ et $C_2(E) = 36$. Ainsi, le Corollaire 4.3.6.1 est vérifié.

CHAPITRE 5

PÉRIODES DES SUITES DE TRIBONACCI ET COURBES ELLIPTIQUES

Dans ce chapitre, on étudie la suite Tribonacci $(T_n)_n$ qui est une suite récurrente linéaire d'ordre 3 définie par

$$\begin{cases} T_0 = 0,\ T_1 = 0,\ T_2 = 1, \\ T_{n+1} = T_n + T_{n-1} + T_{n-2},\ \ (n \geq 2). \end{cases}$$

On sait que $(T_n \bmod m)_n$ est simplement périodique pour tout entier $m \geq 2$ [36, 39]. On peut aussi le voir en utilisant le Lemme 2.1.1 puisque la matrice compagnon de la suite Tribonacci $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$ est de déterminant 1 et est donc inversible modulo tout entier $m \geq 2$. On note par $k(m)$ la période de la suite $(T_n \bmod m)_n$, i.e., le plus petit entier strictement positif k tel que $T_k \equiv T_{k+1} \equiv 0 \bmod m$ et $T_{k+2} \equiv 1 \bmod m$.

5.1 La suite Tribonacci

Soient $F(x) = x^3 - x^2 - x - 1$ le polynôme caractéristique de la suite Tribonacci $(T_n)_n$ et $I = \{3,5,23,31,\ldots\}$ l'ensemble de tous les nombres premiers p pour lesquels $F(x)$ est irréductible sur $\mathbb{F}_p$, $Q = \{7,13,17,19,\ldots\}$ l'ensemble de tous les nombres premiers p pour lesquels $F(x)$ se factorise sur $\mathbb{F}_p$ en produit d'un facteur linéaire et d'un facteur quadratique irréductible et $L = \{2,11,47,53,\ldots\}$ l'ensemble de tous les nombres premiers p pour lesquels $F(x)$ se factorise complètement sur $\mathbb{F}_p$ en facteurs linéaires. Ces ensembles sont donnés dans [24]. Le théorème suivant contient certaines des propriétés fondamentales connues sur les périodes de la suite Tribonacci modulo m.

Théorème 5.1.1. *Soit $p \neq 2,11$ un nombre premier.*

(a) *Si $p \in L$, alors $k(p)|(p-1)$.*

(b) *Si $p \in Q$, alors $k(p)|(p^2-1)$.*

(c) *Si $p \in I$, alors $k(p)|(p^2+p+1)$.*

(d) *Si $\prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de m, alors $k(m) = \operatorname{ppcm}\big(k(p_i^{e_i})\big)$.*

(e) *Si $n|m$, alors $k(n)|k(m)$.*

Démonstration. Pour (a)-(c) voir [24] ou utiliser la Proposition 2.1.2, pour (d) voir [36, 39] ou utiliser le Lemme 2.1.2. Pour (e), Supposons que $n|m$ et soient $\sigma = k(n)$, $\tau = k(m)$, alors σ est le plus petit entier strictement positif satisfaisant $T_\sigma \equiv T_{\sigma+1} \equiv 0 \bmod n$, $T_{\sigma+2} \equiv 1 \bmod n$ et τ est le plus petit entier strictement positif satisfaisant $T_\tau \equiv T_{\tau+1} \equiv 0$ et $T_{\tau+2} \equiv 1 \bmod m$. Par hypothèse, on a $n|m$, d'où l'on déduit que $T_\tau \equiv T_{\tau+1} \equiv 0 \bmod n$, $T_{\tau+2} \equiv 1 \bmod n$ et donc $\sigma|\tau$. □

Par exemple, la suite Tribonacci modulo 3 est donnée par 0, 0, 1, 1, 2, 1, 1, 1, 0, 2, 0, 2, 1, 0, 0, 1, …, ce qui implique $k(3) = 13|(3^2+3+1) = 13$ et donc (c) est vérifiée. La suite Tribonacci modulo 6 est 0, 0, 1, 1, 2, 4, 1, 1, 0, 2, 3, 5, 4, 0, 3, 1, 4, 2, 1, 1, 4, 0, 5, 3, 2, 4, 3, 3, 4, 4, 5, 1, 4, 4, 3, 5, 0, 2, 1, 3, 0, 4, 1, 5, 4, 4, 1, 3, 2, 0, 5, 1, 0, 0, 1, …, et donc $k(6) = 52$. Modulo 2, la suite est 0, 0, 1, 1, 0, 0, 1, …, et donc $k(2) = 4$. Ainsi, la partie (d) est aussi vérifiée puisqu'on a $\text{ppcm}\big(k(2),k(3)\big) = \text{ppcm}(4,13) = 52 = k(6)$. On voit aussi que (e) est vérifiée puisque $2,3|6$ et $k(2),k(3)|k(6)$.

5.2 La (a,b,c)-suite Tribonacci

Soient a, b et c des entier, la (a,b,c)-suite Tribonacci est la suite $(G_n)_n$ définie par

$$\begin{cases} G_0 = a,\ G_1 = b,\ G_2 = c, \\ G_{n+1} = G_n + G_{n-1} + G_{n-2}, \ \ (n \geq 2). \end{cases}$$

Puisque la matrice compagnon de la (a,b,c)-suite Tribonacci $(G_n)_n$ est la même que celle de la suite $(T_n)_n$, on en déduit que la suite $(G_n \bmod m)_n$ est simplement périodique, pour tout entier $m \geq 2$. On désigne par $k(a,b,c;m)$ la période de la suite $(G_n \bmod m)_n$, c'est-à-dire, le plus petit entier strictement positif k tel que $G_k \equiv a \bmod m$, $G_{k+1} \equiv b \bmod m$ et $G_{k+2} \equiv c \bmod m$.

La proposition suivante nous indique qu'on peut exprimer la suite $(G_n)_n$ en fonction de la suite $(T_n)_n$. Notons qu'à partir de la relation de récurrence, on peut définir $T_{-1} = T_2 - T_1 - T_0 = 1$ et $T_{-2} = T_1 - T_0 - T_{-1} = -1$.

Proposition 5.2.1. *Soient a, b, c et m des entiers avec $m \geq 2$. La (a,b,c)-suite Tribonacci satisfait*

$$G_n = aT_{n-1} + b(T_{n-1} + T_{n-2}) + cT_n \quad \textit{pour } n \geq 0. \tag{5.1}$$

Démonstration. Cela découle d'une simple récurrence. □

Proposition 5.2.2. *Soit $(G_n)_n$ la (a,b,c)-suite Tribonacci, où a, b, c et m sont des entiers avec $m \geq 2$.*

(a) $k(a,b,c;m)|k(m)$.

(b) $k(0,0,c;m) = k(c,0,0;m)$ *et* $k(0,0,c;m)|k(m)$.

(c) *Si* $\text{pgcd}(c,m) = 1$, *alors* $k(0,0,c;m) = k(m)$.

(d) $k(a,b,c;m)|\text{ppcm}\big(k(a,0,0;m),k(0,b,0;m),k(0,0,c;m)\big)$.

Démonstration.

(a) La relation (5.1) implique

$$\begin{cases} G_{k(m)} &= aT_{k(m)-1} + b(T_{k(m)-1} + T_{k(m)-2}) + cT_{k(m)}, \\ G_{k(m)+1} &= aT_{k(m)} + b(T_{k(m)} + T_{k(m)-1}) + cT_{k(m)+1}, \\ G_{k(m)+2} &= aT_{k(m)+1} + b(T_{k(m)+1} + T_{k(m)}) + cT_{k(m)+2}, \end{cases}$$

ce qui implique

$$\begin{cases} G_{k(m)} &\equiv aT_{-1} + b(T_{-1} + T_{-2}) + cT_0 \bmod m, \\ G_{k(m)+1} &\equiv aT_0 + b(T_0 + T_{-1}) + cT_1 \bmod m, \\ G_{k(m)+2} &\equiv aT_1 + b(T_1 + T_0) + cT_2 \bmod m, \end{cases}$$

donc on obtient $G_{k(m)} \equiv G_0$, $G_{k(m)+1} \equiv G_1$, $G_{k(m)+2} \equiv G_2 \bmod m$. Il vient que $k(a,b,c;m)|k(m)$.

(b) La première partie découle du fait que la $(c,0,0)$-suite Tribonacci commence par $c,0,0,c$ donnant la même suite que la $(0,0,c)$-suite Tribonacci à l'exception du premier point. La deuxième partie est un cas particulier de (b).

(c) La relation (5.1) implique que le terme général de la $(0,0,c)$-suite Tribonacci est $G_n = cT_n$. Si $\text{pgcd}(c,m) = 1$, alors c est inversible modulo m et donc $cT_i \equiv cT_j \bmod m$ si et seulement si $T_i \equiv T_j \bmod m$. Par conséquent, $k(0,0,c;m) = k(m)$.

(d) Soient $\sigma = k(a,0,0;m)$, $\tau = k(0,b,0;m)$ et $\theta = k(0,0,c;m)$. La relation (5.1) implique, en considérant les termes généraux des $(a,0,0)$, $(0,b,0)$ et $(0,0,c)$-suites, que $aT_{\sigma-1} \equiv a$, $aT_\sigma \equiv 0$, $aT_{\sigma+1} \equiv 0 \bmod m$, $b(T_{\tau-1} + T_{\tau-2}) \equiv 0$, $b(T_\tau + T_{\tau-1}) \equiv b$, $b(T_{\tau+1} + T_\tau) \equiv 0 \bmod m$ et

$cT_\theta \equiv 0$, $cT_{\theta+1} \equiv 0$, $cT_{\theta+2} \equiv c \bmod m$. Soit $\rho = \text{ppcm}(\sigma, \tau, \theta)$. Puisque $\sigma|\rho$, $\tau|\rho$ et $\theta|\rho$, alors $aT_{\rho-1} \equiv a$, $aT_\rho \equiv 0$, $aT_{\rho+1} \equiv 0 \bmod m$, $b(T_{\rho-1}+T_{\rho-2}) \equiv 0$, $b(T_\rho+T_{\rho-1}) \equiv b$, $b(T_{\rho+1}+T_\rho) \equiv 0 \bmod m$ et $cT_\rho \equiv 0$, $cT_{\rho+1} \equiv 0$, $cT_{\rho+2} \equiv c \bmod m$. Ces neuf dernières congruences et la relation (5.1) donnent $G_\rho \equiv a$, $G_{\rho+1} \equiv b$ et $G_{\rho+2} \equiv c \bmod m$, d'où $k(a,b,c;m)|\rho$.

□

Considérons maintenant une relation binaire sur l'ensemble $(\mathbb{Z}/m\mathbb{Z})^3$, définie par $(a,b,c) \sim (q,r,t)$, si et seulement si, dans la (a,b,c)-suite Tribonacci, il existe un indice i tel que $G_i \equiv q \bmod m, G_{i+1} \equiv r \bmod m$ et $G_{i+2} \equiv t \bmod m$. Puisque trois termes consécutifs déterminent complètement la (a,b,c)-suite Tribonacci modulo m, il s'agit bien d'une relation d'équivalence sur $(\mathbb{Z}/m\mathbb{Z})^3$. Le Tableau 5.I donne toutes les classes d'équivalence modulo 6.

Une suite Tribonacci de période d modulo m est de la forme x_1, x_2, x_3, …, x_d, $x_{d+1} \equiv x_1$, $x_{d+2} \equiv x_2$, …. Par conséquent, les triplets distincts qui sont composés de trois termes consécutifs dans cette suite sont (x_1,x_2,x_3), (x_2,x_3,x_4), …, (x_d,x_1,x_2). Ainsi, on a d triplets et on en déduit que la taille de la classe d'équivalence contenant (a,b,c) est $d = k(a,b,c;m)$. Étant donné un module entier $m \geq 2$ fixé, on définit $c_d(m)$ comme étant le nombre de classes d'équivalence distinctes de taille d. Ainsi, dans le Tableau 5.I, on voit que $c_1(6) = 2$, $c_2(6) = 1$, $c_4(6) = 1$, $c_{13}(6) = 4$, $c_{26}(6) = 2$, $c_{52}(6) = 2$ et $c_d(6) = 0$ pour tous les autres d.

Le théorème suivant compte les éléments de $(\mathbb{Z}/m\mathbb{Z})^3$ correspondant à la partition de cet ensemble en classes d'équivalence.

Théorème 5.2.3. *Soient $m \geq 2$ un entier et $c_d(m)$ défini comme ci-dessus, alors*

$$m^3 = \sum_{d|k(m)} d \cdot c_d(m).$$

Démonstration. La même preuve que dans le cas Morgan-Voyce, voir Théorème 3.2.5. □

On a vu dans le Tableau 5.I que modulo 6, il y a des classes qui ont des tailles différentes. Cependant, à l'exception de la $(0,0,0)$-classe qui est toujours de longueur 1, on peut avoir toutes les classes de longueur $k(m)$, comme représenté dans le Tableau 5.II par le cas $m = 5$, avec $k(m) = 31$.

Les petites classes d'équivalence sont décrites dans la proposition suivante.

$k(a,b,c;6)$	classe d'équivalence de (a,b,c)
1	$(0,0,0)$
52	$(0,0,1),(0,1,1),(1,1,2),(1,2,4),(2,4,1),(4,1,1),(1,1,0),(1,0,2),$ $(0,2,3),(2,3,5),(3,5,4),(5,4,0),(4,0,3),(0,3,1),(3,1,4),(1,4,2),$ $(4,2,1),(2,1,1),(1,1,4),(1,4,0),(4,0,5),(0,5,3),(5,3,2),(3,2,4),$ $(2,4,3),(4,3,3),(3,3,4),(3,4,4),(4,4,5),(4,5,1),(5,1,4),(1,4,4),$ $(4,4,3),(4,3,5),(3,5,0),(5,0,2),(0,2,1),(2,1,3),(1,3,0),(3,0,4),$ $(0,4,1),(4,1,5),(1,5,4),(5,4,4),(4,4,1),(4,1,3),(1,3,2),(3,2,0),$ $(2,0,5),(0,5,1),(5,1,0),(1,0,0).$
13	$(0,0,2),(0,2,2),(2,2,4),(2,4,2),(4,2,2),(2,2,2),(2,2,0),(2,0,4),$ $(0,4,0),(4,0,4),(0,4,2),(4,2,0),(2,0,0).$
4	$(0,0,3),(0,3,3),(3,3,0),(3,0,0).$
13	$(0,0,4),(0,4,4),(4,4,2),(4,2,4),(2,4,4),(4,4,4),(4,4,0),(4,0,2),$ $(0,2,0),(2,0,2),(0,2,4),(2,0,4),(4,0,0).$
52	$(0,0,5),(0,5,5),(5,5,4),(5,4,2),(4,2,5),(2,5,5),(5,5,0),(5,0,4),$ $(0,4,3),(4,3,1),(3,1,2),(1,2,0),(2,0,3),(0,3,5),(3,5,2),(5,2,4),$ $(2,4,5),(4,5,5),(5,5,2),(5,2,0),(2,0,1),(0,1,3),(1,3,4),(3,4,2),$ $(4,2,3),(2,3,3),(3,3,2),(3,2,2),(2,2,1),(2,1,5),(1,5,2),(5,2,2),$ $(2,2,3),(2,3,1),(3,1,0),(1,0,4),(0,4,5),(4,5,3),(5,3,0),(3,0,2),$ $(0,2,5),(2,5,1),(5,1,2),(1,2,2),(2,2,5),(2,5,3),(5,3,4),(3,4,0),$ $(4,0,1),(0,1,5),(1,5,0),(5,0,0).$
26	$(1,4,1),(4,1,0),(1,0,5),(0,5,0),(5,0,5),(0,5,4),(5,4,3),(4,3,0),$ $(3,0,1),(0,1,4),(1,4,5),(4,5,4),(5,4,1),(4,1,4),(1,4,3),(4,3,2),$ $(3,2,3),(2,3,2),(3,2,1),(2,1,0),(1,0,3),(0,3,4),(3,4,1),(4,1,2),$ $(1,2,1),(2,1,4).$
2	$(0,3,0),(3,0,3).$
13	$(5,5,5),(5,5,3),(5,3,1),(3,1,3),(1,3,1),(3,1,5),(1,5,3),(5,3,3),$ $(3,3,5),(3,5,5),(5,5,1),(5,1,5),(1,5,5).$
1	$(3,3,3)$
13	$(1,1,1),(1,1,3),(1,3,5),(3,5,3),(5,3,5),(3,5,1),(5,1,3),(1,3,3),$ $(3,3,1),(3,1,1),(1,1,5),(1,5,1),(5,1,1).$
26	$(5,0,3),(0,3,2),(3,2,5),(2,5,4),(5,4,5),(4,5,2),(5,2,5),(2,5,0),$ $(5,0,1),(0,1,0),(1,0,1),(0,1,2),(1,2,3),(2,3,0),(3,0,5),(0,5,2),$ $(5,2,1),(2,1,2),(1,2,5),(2,5,2),(5,2,3),(2,3,4),(3,4,3),(4,3,4),$ $(3,4,5),(4,5,0).$

Tableau 5.I – Les (a,b,c)-classes d'équivalence modulo 6.

Diviseur d	1	31
$c_d(10)$	1	4

Tableau 5.II – Longueurs et nombre de classes d'équivalence modulo 5.

Proposition 5.2.4. *Soit $m \geq 2$ un entier.*

(a) $c_1(m) = 1$ *si m est impair et* $c_1(m) = 2$ *si m est pair.*

(b) $c_2(m) = 0$ *si m est impair et* $c_2(m) = 1$ *si m est pair.*

(c) $c_3(m) = 0$.

(d) $c_4(m) = 0$ *si* $m \equiv 1, 3$ *mod* 4, $c_4(m) = 1$ *si* $m \equiv 2$ *mod* 4 *et* $c_4(m) = 3$ *si* $m \equiv 0$ *mod* 4.

Démonstration.

(a) Une suite de période 1 est de la forme a, a, a, a, ... modulo m. Ainsi, $a+a+a \equiv a \bmod m$, donc $2a \equiv 0 \bmod m$. Si m est impair, on obtient $a \equiv 0 \bmod m$ et la suite est en fait 0, 0, 0, ..., d'où $c_1(m) = 1$. Si m est pair, on obtient $a \equiv 0 \bmod m/2$. Dans ce cas, on a les deux suites 0, 0, 0, ... et $m/2$, $m/2$, $m/2$, ..., d'où $c_1(m) = 2$.

(b) Une suite de période 2 est de la forme a, b, a, b, a, ... mod m. Ainsi, $a+b+a \equiv b \bmod m$ et $b+a+b \equiv a \bmod m$, ce qui donne $2a \equiv 2b \equiv 0 \bmod m$. Si m est impair, on obtient $a \equiv b \equiv 0 \bmod m$. Ceci donne la suite 0, 0, 0, ..., qui est en fait une suite de période 1, d'où $c_2(m) = 0$. Si m est pair, on obtient $a \equiv b \equiv 0 \bmod m/2$. Ceci donne une suite de période 2, qui est (à un ordre près) 0, $m/2$, 0, $m/2$, ... et deux suites de période 1, qui sont 0, 0, 0, ... et $m/2$, $m/2$, $m/2$, ..., d'où $c_2(m) = 1$.

(c) Une suite de période 3 est de la forme $a, b, c, a, b, c, \ldots \bmod m$. Ainsi, on a $a+b+c \equiv a \bmod m$, $b+c+a \equiv b \bmod m$ et $c+a+b \equiv c \bmod m$, ce qui donne $2a \equiv 2b \equiv 2c \equiv 0 \bmod m$. Si m est impair, on obtient $a \equiv b \equiv c \equiv 0 \bmod m$. Ceci donne la suite 0, 0, 0, ... qui est en fait une suite de période 1, d'où $c_3(m) = 0$. Si m est pair, on obtient $a \equiv b \equiv c \equiv 0 \bmod m/2$. Ceci donne une suite de période 2 qui est (à un ordre près) 0, $m/2$, 0, $m/2$, ..., deux suites de période 1 qui sont 0, 0, 0, ... et $m/2$, $m/2$, $m/2$, ..., les autres cas donnent la mêmes suite d'ordre 4 qui est (à un ordre près) $m/2$, $m/2$, 0, 0, $m/2$, $m/2$, ..., d'où $c_3(m) = 0$.

(d) Une suite de période 4 peut s'écrire sous la forme a, b, c, $a+b+c$, $a+2b+2c$, $2a+3b+4c$, $4a+6b+7c$, ... mod m. Ainsi, on a $a+2b+2c \equiv a \bmod m$, $2a+3b+4c \equiv b \bmod m$ et

$4a+6b+7c \equiv c \bmod m$, ce qui implique $2b+2c \equiv 2a+2c \equiv 2a+2b \equiv 0 \bmod m$. Si m est impair, on obtient $b+c \equiv a+c \equiv a+b \equiv 0 \bmod m$, ce qui implique $2a \equiv 2b \equiv 2c \equiv 0 \bmod m$ et donc $a \equiv b \equiv c \equiv 0 \bmod m$. Par conséquent, on a une suite de période 1 qui est 0, 0, 0, ... et $c_4(m) = 0$. Si m est pair, on obtient $b+c \equiv a+c \equiv a+b \equiv 0 \bmod m/2$, ce qui implique $2a \equiv 2b \equiv 2c \equiv 0 \bmod m/2$, ici aussi, on distingue deux cas. Si $m/2$ est impair, alors on a $a \equiv b \equiv c \equiv 0 \bmod m/2$ et on obtient une classe de taille 4 qui est $(0,0,m/2)$, deux classes de taille 1 qui sont $(0,0,0)$, $(m/2,m/2,m/2)$ et une classe de taille 2 qui est $(0,m/2,0)$, d'où $c_4(m) = 1$. Si $m/2$ est pair, alors $a \equiv b \equiv c \equiv 0 \bmod m/4$ et on obtient 2 classes de taille 1 qui sont $(0,0,0,)$, $(m/2,m/2,m/2)$, une classe da taille 2 qui est $(0,m/2,0)$, trois classes de taille 4 qui sont $(0,0,m/2)$, $(m/4,m/4,m/4)$, $(m/4,3m/4,3m/4)$ et six classes de taille 8 qui sont $(0,0,m/4)$, $(0,0,3m/4)$, $(0,m/4,0)$, $(0,m/2,3m/4)$, $(0,m/2,3m/4)$, $(0,3m/4,0)$. On en déduit que $c_4(m) = 3$.

□

On considère maintenant, d'une manière générale, une (x_1,x_2,x_3)-suite Tribonacci de période d modulo m, alors on a $x_1+x_2+x_3 \equiv x_4$, $x_2+x_3+x_4 \equiv x_5$, ... $x_{d-1}+x_d+x_1 \equiv x_2$. Ainsi, on obtient

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & & \vdots & & & & \ddots & & & \vdots \\ -1 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 1 & 1 & -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{d-2} \\ x_{d-1} \\ x_d \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} \bmod m.$$

On définit la matrice circulante Tribonacci W_n^{TRI}, par la matrice de taille n suivante :

$$W_n^{TRI} := \begin{pmatrix} 1 & 1 & 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & & \vdots & & & \ddots & & \vdots \\ 1 & -1 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 1 & -1 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

On note par $w_n^{TRI} = \det\left(W_n^{TRI}\right)$ le déterminant de la matrice circulante Tribonacci. D'après les formules (2.7) et (2.8), on a $w_n^{TRI} = \prod_{j=0}^{n-1}\left(1+e^{2i\pi j/n}+e^{4i\pi j/n}-e^{6i\pi j/n}\right)$. Le théorème suivant nous donne une relation entre w_n^{TRI} et la période de la suite Tribonacci modulo m.

Théorème 5.2.5. *Soient a, b et c des entiers tels que* $(a,b,c) \not\equiv (0,0,0)$ *mod m, où* $m \geq 2$ *est un entier. Si* $l = k(a,b,c;m)$*, alors* $\text{pgcd}\left(w_l^{TRI},m\right) \neq 1$.

Démonstration. La même preuve que dans le cas Morgan-Voyce fonctionne, voir Théorème 3.2.10. □

Le Tableau 5.III donne quelques valeurs de la suite (w_n^{TRI}). Par exemple, si on considère $w_{13}^{TRI} = 2862 = 2\cdot 3^3\cdot 53$, alors le Théorème 5.2.5 nous dit que si une suite a une période de longueur 13 modulo m, alors $2,3$ ou $53|m$. A titre d'exemple, il est facile de voir que $k(2,2,4;6) = 13$ et on a $\text{pgcd}(w_{13}^{TRI},6) = 6$. Ainsi, les facteurs premiers de w_n^{TRI} donnent une liste finie de nombres premiers, si aucun d'eux ne divise m, alors n ne peut pas être une période d'une suite Tribonacci modulo m.

n	w_n^{TRI}	n	w_n^{TRI}
4	$16 = 2^4$	20	$195536 = 2^4\cdot 11^2\cdot 101$
5	$22 = 2\cdot 11$	21	$361286 = 2\cdot 43\cdot 4201$
6	$28 = 2^2\cdot 7$	22	$665372 = 2^2\cdot 397\cdot 419$
7	$86 = 2\cdot 43$	23	$1219462 = 2\cdot 47\cdot 12973$
8	$128 = 2^7$	24	$2248064 = 2^7\cdot 7\cdot 13\cdot 193$
9	$218 = 2\cdot 109$	25	$4134922 = 2\cdot 11\cdot 187951$
10	$484 = 2^2\cdot 11^2$	26	$7595748 = 2^2\cdot 3^3\cdot 53\cdot 1327$
11	$794 = 2\cdot 397$	27	$13985354 = 2\cdot 109\cdot 64153$
12	$1456 = 2^4\cdot 7\cdot 13$	28	$25718128 = 2^4\cdot 29\cdot 43\cdot 1289$
13	$2862 = 2\cdot 3^3\cdot 53$	29	$47283806 = 2\cdot 23641903$
14	$4988 = 2^2\cdot 29\cdot 43$	30	$87007228 = 2^2\cdot 7\cdot 11^2\cdot 61\cdot 421$
15	$9262 = 2\cdot 11\cdot 421$	31	$160006750 = 2\cdot 5^3\cdot 640027$
16	$17408 = 2^10\cdot 17$	32	$294264832 = 2^{13}\cdot 17\cdot 2113$
17	$31282 = 2\cdot 15641$	33	$541334114 = 2\cdot 397\cdot 681781$
18	$57988 = 2^2\cdot 7\cdot 19\cdot 109$	34	$995580932 = 2^2\cdot 15641\cdot 15913$
19	$107314 = 2\cdot 53657$	35	$1831116386 = 2\cdot 11\cdot 43\cdot 1935641$

Tableau 5.III – Les nombres w_n^{TRI} et leurs factorisations en produit de nombres premiers.

5.3 Suites Tribonacci sur les courbes elliptiques

Soient A, B et C trois points de $E(\mathbb{F}_p)$ où $E : y^2 = x^3 + ax + b$ est une courbe elliptique définie sur le corps fini $\mathbb{F}_p$, avec $p > 2$ un nombre premier. On définit la (A,B,C)-suite Tribonacci, notée

par $(H_n)_n$, sur la courbe elliptique E par

$$\begin{cases} H_0 = A,\ H_1 = B,\ H_2 = C, \\ H_{n+1} = H_n + H_{n-1} + H_{n-2}, \ \ (n \geq 2). \end{cases}$$

Tout d'abord, on établit quelques propriétés de base de (H_n).

Proposition 5.3.1. *Soient A, B et C trois points de $E(\mathbb{F}_p)$.*

(a) *La (A,B,C)-suite Tribonacci (H_n) est donnée par*

$$H_n = [T_{n-1}]A + [T_{n-2} + T_{n-1}]B + [T_n]C. \tag{5.2}$$

(b) *La (O,O,C)-suite Tribonacci est $H_n = [T_n]C$.*

(c) *La (O,B,O)-suite Tribonacci est $H_n = [T_{n-2} + T_{n-1}]B$.*

(d) *La (A,B,C)-suite Tribonacci (H_n) est simplement périodique.*

Démonstration. (a) découle d'une simple récurrence. (b) et (c) sont des cas particuliers de (a) avec $A = B = O$ pour (b) et $A = C = O$ pour (c). (d) se démontre de la même façon que dans le cas Morgan-Voyce en considérant cette fois-ci un triplet constitué de trois termes consécutifs, voir Proposition 3.3.1 (b). □

On note par $K(A,B,C;E)$ la période de la (A,B,C)-suite Tribonacci, c'est-à-dire, le plus petit entier strictement positif k satisfaisant $H_k = A, H_{k+1} = B$ et $H_{k+2} = C$.

Comme dans les cas Morgan-Voyce et quasi Morgan-Voyce, le Lemme 1.2.1 nous permet de faire le lien entre les périodes de le suite Tribonacci sur une courbe elliptique et les périodes de la suite Tribonacci ordinaire. On verra que la période de la (O,O,C)-suite ne dépend que de h_C, de sorte que tous les points R qui ont le même ordre vont engendrer des suites Tribonacci avec exactement la même longueur. Une fois cette connexion établie, on pourra généraliser les propriétés de la suite Tribonacci ordinaire à la (O,O,C)-suite Tribonacci sur les courbes elliptiques.

Théorème 5.3.2. *Soient A, B et C des points de $E(\mathbb{F}_p)$, alors*

(a) *$K(O,O,C;E) = K(C,O,O;E) = k(h_C)$. Si h_C est impair, alors $K(O,C,O;E) = k(h_C)$.*

(b) *$K(O,C,O;E) | k(h_C)$.*

(c) $K(A,B,C;E) \mid \text{ppcm}\,(K(A,O,O;E),K(O,B,O;E),K(O,O,C;E))$.

(d) $K(A,B,C;E) \mid k(h)$.

Démonstration.

(a) L'égalité $K(O,O,C;E) = K(C,O,O;E)$ est évidente étant donné que les deux suites sont les mêmes. La Proposition 5.3.1 (b) nous dit que la (O,O,C)-suite est $H_n = [T_n]C$. Soit $c = K(O,O,C;E)$, alors $[0]C = H_c = [T_c]C$, $[0]C = H_{c+1} = [T_{c+1}]C$ et $[1]C = H_{c+2} = [T_{c+2}]C$. D'après le Lemme 1.2.1, cela se produit si et seulement si $T_c \equiv 0$, $T_{c+1} \equiv 0$ et $T_{c+2} \equiv 1 \bmod h_C$. Puisque c est le plus petit entier vérifiant ces congruences, on en déduit que $c = k\,(h_C)$. Supposons maintenant que h_C est impair et soit $c = K(O,C,O;E)$. La Proposition 5.3.1 (c) nous dit que la (O,C,O)-suite est $H_n = [T_{n-2} + T_{n-1}]C$. Ainsi, on a

$$
\begin{cases} H_0 = H_c \\ H_1 = H_{c+1} \\ H_2 = H_{c+2} \end{cases}
\iff
\begin{cases} [0]C = [T_{c-2} + T_{c-1}]C \\ [1]C = [T_{c-1} + T_c]C \\ [0]C = [T_c + T_{c+1}]C \end{cases}
$$

$$
\iff
\begin{cases} T_{c-2} + T_{c-1} \equiv 0 \mod (h_C) \\ T_{c-1} + T_c \equiv 1 \mod (h_C) \\ T_c + T_{c+1} \equiv 0 \mod (h_C) \end{cases}
$$

$$
\iff
\begin{cases} 2T_{c+1} \equiv 0 \mod (h_C) \\ T_{c-1} + T_c \equiv 1 \mod (h_C) \\ T_c + T_{c+1} \equiv 0 \mod (h_C) \end{cases}
$$

$$
\iff
\begin{cases} T_{c+1} \equiv 0 \mod (h_C) \\ T_{c-1} \equiv 1 \mod (h_C) \\ T_c \equiv 0 \mod (h_C) \end{cases}
$$

$$
\iff
\begin{cases} T_{c+1} \equiv 0 \mod (h_C) \\ T_{c+2} \equiv 1 \mod (h_C) \\ T_c \equiv 0 \mod (h_C) \end{cases}
$$

où la deuxième équivalence provient du Lemme 1.2.1. Puisque c est le plus petit entier vérifiant le dernier système, on en déduit que $c = k(h_C)$.

(b) Si h_C est un entier positif quelconque, alors la quatrième équivalence ci-dessus devient une implication puisque

$$T_{c+1} \equiv 0 \bmod (h_C) \Longrightarrow 2T_{c+1} \equiv 0 \bmod (h_C).$$

Ainsi, on en déduit que $K(O,C,O;E)|k(h_C)$.

(c) La preuve est analogue à celle de la Proposition 5.2.2(d).

(d) On sait que $h_A|h$, $h_B|h$ et $h_C|h$. Par conséquent, d'après le Théorème 5.1.1 (e), on a $k(h_A)|k(h)$, $k(h_B)|k(h)$ et $k(h_C)|k(h)$. D'après (a) et (b), on a $K(A,O,O;E) = k(h_A)$, $K(O,B,O;E)|k(h_B)$ et $K(O,O,C;E) = k(h_C)$, on en déduit que les trois périodes $K(A,O,O;E)$, $K(O,B,O;E)$ et $K(O,O,C;E)$ divisent $k(h)$, donc $\text{ppcm}(K(A,O,O;E),K(O,B,O;E),K(O,O,C;E))|k(h)$ et le résultat découle de (c).

□

Corollaire 5.3.2.1. *Soient A, B et C trois points de $E(\mathbb{F}_p)$ et supposons qu'on a $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ pour n_1, $n_2 \geq 1$ des entiers donnés tels que n_1 divise n_2, alors $K(A,B,C;E)|k(n_2)$.*

Démonstration. Découle d'une preuve analogue à celle du Théorème 5.3.2(d) en utilisant le Théorème 1.2.4 et le fait que l'ordre de tout point de $E(\mathbb{F}_p)$ divise n_2. □

Puisqu'on a $k(h_C) = K(O,O,C;E)$, certaines propriétés de la suite Tribonacci ordinaire peuvent être transférées à des propriétés analogues pour les (O,O,C)-suites Tribonacci sur une courbe elliptique.

Théorème 5.3.3. *Soient A, B et C trois points de $E(\mathbb{F}_p)$.*

(a) *Si $h_C \in L \setminus \{2,11\}$, alors $K(O,O,C;E)|(h_C - 1)$.*

(b) *Si $h_C \in Q$, alors $K(O,O,C;E)|(h_C^2 - 1)$.*

(c) *Si $h_C \in I$, alors $K(O,O,C;E)|(h_C^2 + h_C + 1)$.*

(d) *Si $\prod p_i^{e_i}$ est la factorisation en produit de nombres premiers de h_C, alors on a $K(O,O,C;E) = \text{ppcm}\left(k(p_i^{e_i})\right)$.*

(e) *Si $h_A|h_C$, alors $k(h_A)|k(h_C)$.*

Démonstration. Utiliser le résultat du Théorème 5.3.2(a) dans le Théorème 5.1.1. □

On définit maintenant, comme pour les suites Tribonacci ordinaires, une relation d'équivalence sur les suites Tribonacci définies sur les courbes elliptiques. On dit que (A',B',C') est équivalent à (A,B,C) si, dans la (A,B,C)-suite Tribonacci, il existe un indice i tel que $H_i = A'$, $H_{i+1} = B'$ et $H_{i+2} = C'$. Comme pour le cas ordinaire, la taille d'une classe d'équivalence contenant (A,B,C) est $K(A,B,C;E)$. On définit $C_d(E)$ comme étant le nombre de classes d'équivalence distinctes de taille d.

On va voir dans le théorème suivant que nous ne pouvons pas toujours avoir les mêmes résultats que pour la suite Tribonacci ordinaire modulo m.

Théorème 5.3.4. *Soient A, B et C trois points de $E(\mathbb{F}_p)$ et w_c^{TRI} les déterminants des matrices circulantes Tribonacci comme précédemment, alors*

(a) $C_1(E) = \begin{cases} 1, & \text{si la cubique n'a pas de racine dans } \mathbb{F}_p, \\ 2, & \text{si la cubique n'a qu'une racine dans } \mathbb{F}_p, \\ 4, & \text{si la cubique a trois racine dans } \mathbb{F}_p. \end{cases}$

(b) $C_2(E) = \begin{cases} 0, & \text{si la cubique n'a pas de racine dans } \mathbb{F}_p, \\ 1, & \text{si la cubique n'a qu'une racine dans } \mathbb{F}_p, \\ 6, & \text{si la cubique a trois racine dans } \mathbb{F}_p. \end{cases}$

(c) *Si $c = K(A,B,C;E)$, alors* $\text{pgcd}\left(w_c^{TRI}, h\right) \neq 1$.

Démonstration. (a) et (b) découlent d'arguments analogues à ceux de la preuve de la Proposition 5.2.4. En effet, si la cubique n'a pas de racine dans $\mathbb{F}_p$ et par conséquent, n'a pas de point d'ordre 2 dans $E(\mathbb{F}_p)$, alors on aura une suite de période 1 qui est (O,O,O) et pas de suite de période 2. S'il n'y a qu'un point P d'ordre 2 dans $E(\mathbb{F}_p)$, alors on aura deux suites de période 1 qui sont (O,O,O) et (P,P,P), une suite de période 2 qui est (O,P,O). S'il y a trois points P_i, avec $i = 1,2,3$, d'ordre 2 dans $E(\mathbb{F}_p)$, alors on aura quatre suites de période 1 qui sont (O,O,O) et (P_i,P_i,P_i) avec $i = 1,2,3$, six suites de période 2 qui sont (O,P_i,O) et (P_i,P_j,P_i) avec $i,j = 1,2,3$ et $i < j$. Pour (c), la même preuve que dans le cas Morgan-Voyce fonctionne, voir Théorème 3.3.5. □

Le théorème suivant est analogue au Théorème 5.2.3.

Théorème 5.3.5. *Soient E une courbe elliptique sur $\mathbb{F}_p$ et $C_d(E)$ défini comme précédemment, alors*

$$h^3 = \sum_{d|k(h)} d \cdot C_d(E).$$

Démonstration. Découle du fait que les classes d'équivalence forment une partition de $E(\mathbb{F}_p)^3$ et que, d'après le Théorème 5.3.2(d), toutes les classes ont une taille qui divise $k(h)$. □

Corollaire 5.3.5.1. *Supposons qu'on a $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ pour $n_1, n_2 \geq 1$ des entiers donnés tels que n_1 divise n_2, alors*

$$h^3 = \sum_{d|k(n_2)} d \cdot C_d(E).$$

Démonstration. Découle du Théorème 5.3.5 et du Corollaire 5.3.2.1. □

Le Tableau 5.IV illustre le Corollaire 5.3.5.1 pour la courbe elliptique $y^2 = x^3 + 2$ sur $\mathbb{F}_7$. On a $E(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, h = ord(E(\mathbb{F}_7)) = 9, k(3) = 13$ et $k(9) = 39$.

Diviseur d	1	3	13	39
$C_d(E)$	1	0	56	0

Tableau 5.IV – Longueurs et nombre de classes d'équivalence pour $y^2 = x^3 + 2$ sur $\mathbb{F}_7$.

Exemple 1. Sur la courbe elliptique $E : y^2 = x^3 + x + 1$ considérée sur le corps $\mathbb{F}_5$, on a $E(\mathbb{F}_5) = \{O, P_i, 1 \leq i \leq 8\}$, où $P_1 = (0,1)$, $P_2 = (4,2)$, $P_3 = (2,1)$, $P_4 = (3,4)$, $P_5 = (3,1)$, $P_6 = (2,4)$, $P_7 = (7,3)$ et $P_8 = (0,4)$. Le point P_1 est d'ordre 9 et engendre ce groupe. On a $P_j = [j]P_1$ avec $1 \leq j \leq 8$. Ainsi, $E(\mathbb{F}_5) \simeq \mathbb{Z}/9\mathbb{Z}$. Par conséquent, travailler sur $E(\mathbb{F}_5)$ revient à travailler sur les suites Tribonacci ordinaires modulo 9. Ce groupe n'a pas de point d'ordre 2, donc $C_1(E) = 1 = c_1(9)$, $C_2(E) = 0 = c_2(9)$.

Exemple 2. Sur la courbe elliptique $E : y^2 = x^3 + x$ considérée sur $\mathbb{F}_3$, la cubique n'a qu'une racine dans $\mathbb{F}_3$ qui est $x = 0$, donc il n'y a qu'un point d'ordre 2 dans $E(\mathbb{F}_3)$ qui est $(0,0)$. Les autres points non triviaux sont $(2,1)$ et $(2,2)$ qui sont d'ordre 4, on en déduit que $E(\mathbb{F}_3) \simeq \mathbb{Z}/4\mathbb{Z}$. Par conséquent, travailler sur $E(\mathbb{F}_3)$ revient à travailler sur les suites Tribonacci ordinaires modulo 4 et on a $C_1(E) = 2 = c_1(4)$, $C_2(E) = 1 = c_2(4)$. Le Tableau 5.V illustre le Théorème 5.3.5 pour cette courbe elliptique. On a $ord(E(\mathbb{F}_3)) = 4$ et $k(4) = 8$.

Diviseur d	1	2	4	8
$C_d(E)$	2	1	3	6

Tableau 5.V – Longueurs et nombre de classes d'équivalence pour $y^2 = x^3 + x$ sur $\mathbb{F}_3$.

Exemple 3. Sur la courbe elliptique $E : y^2 = x^3 - x$ considérée sur $\mathbb{F}_3$, la cubique a trois racines dans $\mathbb{F}_3$, donc on a trois points d'ordre 2 dans $E(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans ce cas, on a $C_1(E) = 4$ et $C_2(E) = 6$, ce qui ne se produit pas sur une suite Tribonacci ordinaire modulo m.

Annexe A

Les suites quasi Morgan-Voyce comme convolutions itérées de suites de Pell généralisées

Horadam [18] a introduit la *suite quasi Morgan-Voyce* définie par (Il nous a semblé utile de changer les notations vu que c'est une annexe indépendante, on fait juste appel à ces résultats)

$$\begin{cases} Q_1^{(s)} = 1, \;\; Q_2^{(s)} = 1+t+s, \\ Q_n^{(s)} = (2+t)Q_{n-1}^{(s)} + Q_{n-2}^{(s)}, \quad (n \geq 3). \end{cases} \tag{A.1}$$

Si nous écrivons $Q_{n+1}^{(s)} = \sum_{k=0}^{n} Q^{(s)}(n,k)t^k$ pour $n \geq 0$, alors, dans un premier temps, nous montrons que les coefficients $Q^{(1)}(n,k)$ sont des produits de convolution de la suite de Pell $(P_n)_n$, définie ci-dessous, avec elle même. Ensuite, nous montrons que les coefficients $Q^{(s)}(n,k)$ sont des produits de convolutions de suites de Pell généralisés.

A.1 Cas $s = 1$

On commence par le cas $s = 1$. Dans ce cas, notre suite est donnée par

$$\begin{cases} Q_1^{(1)} = 1, \;\; Q_2^{(1)} = 2+t, \\ Q_n^{(1)} = (2+t)Q_{n-1}^{(1)} + Q_{n-2}^{(1)}, \quad (n \geq 3). \end{cases} \tag{A.2}$$

On va montrer que les coefficients $Q^{(1)}(n,k)$ sont exactement les lignes du triangle de convolution de la suite de Pell donné ci-dessous, ce triangle correspond à A054456 dans [31]. On rappelle que la suite de Pell $(P_n)_n$ est définie par

$$\begin{cases} P_1 = 1, \; P_2 = 2, \\ P_n = 2P_{n-1} + P_{n-2}, \;\; (n \geq 3). \end{cases} \tag{A.3}$$

Le triangle de convolution des suites de Pell est défini comme suit : la première colonne est constituée des nombres de Pell, la deuxième colonne est constituée de la convolution de la colonne des nombres de Pell avec elle-même, la troisième colonne est constituée de la colonne des nombres de Pell convolée deux fois avec elle-même et ainsi de suite. Les 0 dans le Tableau A.I sont représentés par un vide.

$n\backslash k$	0	1	2	3	4	5	6	7	8	9	…
0	1										
1	2	1									
2	5	4	1								
3	12	14	6	1							
4	29	44	27	8	1						
5	70	131	104	44	10	1					
6	169	376	366	200	65	12	1				
7	408	1052	1212	810	340	90	14	1			
8	985	2888	3842	3032	1555	532	119	16	1		
9	2378	7813	11784	10716	6482	2709	784	152	18	1	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Tableau A.I – Triangle de convolution de la suite de Pell.

Si on note par $D(n,k)$ les éléments de ce triangle, alors on a

$$D(n,k) = 0, \qquad (n < k), \tag{A.4}$$

$$D(n,n) = 1 \qquad (n \geq 0), \tag{A.5}$$

$$D(n,0) = P_{n+1}, \qquad (n \geq 0), \tag{A.6}$$

et pour tout $j \in \{0,1,\ldots,k-1\}$

$$D(n,k) = \sum_{i=0}^{n-1} D(i,j)D(n-1-i,k-1-j), \qquad (k,n \geq 1). \tag{A.7}$$

Lemme A.1.1. *Soient $n \geq 1$ et $k \geq 1$ des entiers, alors on a*

$$D(n+1,k) = D(n,k-1) + 2D(n,k) + D(n-1,k). \tag{A.8}$$

Démonstration. Soient $n \geq 1$ et $k \geq 1$ des entiers, alors

$$\begin{aligned} D(n+1,k) &= \sum_{i=0}^{n} D(i,k-1)D(n-i,0) \\ &= D(n,k-1)D(0,0) + D(n-1,k-1)D(1,0) + \sum_{i=0}^{n-2} D(i,k-1)D(n-i,0) \end{aligned}$$

$$
\begin{aligned}
&= D(n,k-1)+2D(n-1,k-1)\\
&\quad +\sum_{i=0}^{n-2} D(i,k-1)\left[2D(n-1-i,0)+D(n-2-i,0)\right]\\
&= D(n,k-1)+2D(n-1,k-1)+2\sum_{i=0}^{n-2} D(i,k-1)D(n-1-i,0)\\
&\quad +\sum_{i=0}^{n-2} D(i,k-1)D(n-2-i,0)\\
&= D(n,k-1)+2\sum_{i=0}^{n-1} D(i,k-1)D(n-1-i,0)\\
&\quad +\sum_{i=0}^{n-2} D(i,k-1)D(n-2-i,0)\\
&= D(n,k-1)+2D(n,k)+D(n-1,k).
\end{aligned}
$$

□

Théorème A.1.1. *Le terme général de la suite* $\left(Q_n^{(1)}\right)_n$ *est*

$$
Q_{n+1}^{(1)} = \sum_{k=0}^{n} D(n,k)t^k, \qquad (n \geq 0). \tag{A.9}
$$

Démonstration. Par récurrence sur n. Pour $n = 0$ et 1, l'identité (A.9) est facile à vérifiée. Supposons que (A.9) est vraie jusqu'à l'ordre n, alors

$$
\begin{aligned}
Q_{n+2}^{(1)} &= (2+t)Q_{n+1}^{(1)} + Q_n^{(1)}\\
&= (2+t)\sum_{k=0}^{n} D(n,k)t^k + \sum_{k=0}^{n-1} D(n-1,k)t^k\\
&= 2\sum_{k=0}^{n} D(n,k)t^k + \sum_{k=0}^{n} D(n,k)t^{k+1} + \sum_{k=0}^{n-1} D(n-1,k)t^k\\
&= 2\sum_{k=0}^{n} D(n,k)t^k + \sum_{k=1}^{n+1} D(n,k-1)t^k + \sum_{k=0}^{n-1} D(n-1,k)t^k\\
&= 2D(n,0) + \sum_{k=1}^{n-1} 2D(n,k)t^k + 2D(n,n)t^n + \sum_{k=1}^{n-1} D(n,k-1)t^k\\
&\quad + D(n,n-1)t^n + D(n,n)t^{n+1} + D(n-1,0) + \sum_{k=1}^{n-1} D(n-1,k)t^k
\end{aligned}
$$

$$
\begin{aligned}
&= [2D(n,0)+D(n-1,0)]+\sum_{k=1}^{n-1}[D(n,k-1)+2D(n,k)+D(n-1,k)]\,t^k \\
&\quad +[2D(n,n)+D(n,n-1)]\,t^n+D(n,n)t^{n+1},
\end{aligned}
$$

d'après le Lemme A.1.1 et les relations (A.4), (A.5), (A.6) et (A.8) on obtient

$$
\begin{aligned}
Q^{(1)}_{n+2} &= D(n+1,0)+\sum_{k=1}^{n-1}D(n+1,k)t^k+D(n+1,n)t^n+D(n+1,n+1)t^{n+1} \\
&= \sum_{k=0}^{n+1}D(n+1,k)t^k.
\end{aligned}
$$

□

Proposition A.1.2. *Avec les mêmes notations que précédemment, on a*

$$
D(n,k)=\sum_{j=0}^{\lfloor (n-k)/2\rfloor}\binom{n-j}{j}\binom{n-2j}{k}2^{n-2j-k}, \qquad 0\le k\le n. \tag{A.10}
$$

Démonstration. D'après [7, Corollaire 1], on a

$$
\begin{aligned}
Q^{(1)}_{n+1} &= \sum_{j=0}^{\lfloor n/2\rfloor}\binom{n-j}{j}(2+t)^{n-2j} \\
&= \sum_{j=0}^{\lfloor n/2\rfloor}\left(\binom{n-j}{j}\sum_{k=0}^{n-2j}\binom{n-2j}{k}2^{n-2j-k}t^k\right) \\
&= \sum_{\substack{j,k\\ 0\le k\le n-2j\le n}}\binom{n-j}{j}\binom{n-2j}{k}2^{n-2j-k}t^k \\
&= \sum_{k=0}^{n}\left(\sum_{j=0}^{\lfloor (n-k)/2\rfloor}\binom{n-j}{j}\binom{n-2j}{k}2^{n-2j-k}\right)t^k,
\end{aligned}
$$

et le résultat découle en identifiant cela avec (A.9). □

A.2 Cas s entier quelconque

Nous traitons maintenant le cas général (s entier quelconque). Supposons donc que notre suite quasi Morgan-Voyce est donnée par (A.1) et soit $(G_n)_n$ la suite de Pell avec des conditions initiales

généralisées, donnée par

$$\begin{cases} G_1 = 1, \;\; G_2 = 1+s, \\ G_n = 2G_{n-1} + G_{n-2}, \quad (n \geq 3). \end{cases} \tag{A.11}$$

On définit le triangle de convolution des suites de Pell généralisées comme suit : la première colonne est constituée des nombres de Pell avec les conditions initiales 1 et $1+s$, la deuxième colonne est constituée de la convolution de la suite $(G_n)_n$ avec la suite $(P_n)_n$, la troisième colonne est constituée de la suite $(G_n)_n$ convolée deux fois avec la suite $(P_n)_n$ et ainsi de suite. C'est-à-dire, chaque colonne est la convolution de la colonne précédente avec la suite $(P_n)_n$. On va montrer que les coefficients $Q^{(s)}(n,k)$ sont exactement les lignes du triangle de convolution des suites de Pell généralisées donné ci-dessous.

$n\backslash k$	0	1	2	3	4	5	6	…
0	1							
1	$1+s$	1						
2	$3+2s$	$3+s$	1					
3	$7+5s$	$10+4s$	$5+s$	1				
4	$17+12s$	$30+14s$	$21+6s$	$7+s$	1			
5	$41+29s$	$87+44s$	$77+27s$	$36+8s$	$9+s$	1		
6	$99+70s$	$245+131s$	$262+104s$	$156+44s$	$55+10s$	$11+s$	1	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Tableau A.II – Triangle de convolution des suites de Pell généralisées

Si on note par $B(n,k)$ les éléments de ce triangle, alors on a

$$B(n,k) = 0, \qquad (n < k), \tag{A.12}$$

$$B(n,n) = 1 \qquad (n \geq 0), \tag{A.13}$$

$$B(n,0) = G_{n+1}, \qquad (n \geq 0), \tag{A.14}$$

et pour tout $j \in \{0,1,\ldots,k-1\}$

$$B(n,k) = \sum_{i=0}^{n-1} D(i,j)B(n-1-i,k-1-j), \qquad (k,n \geq 1). \tag{A.15}$$

Lemme A.2.1. *Soient $n \geq 1$ et $k \geq 1$ des entiers, alors on a*

$$B(n+1,k) = B(n,k-1) + 2B(n,k) + B(n-1,k). \tag{A.16}$$

Démonstration. Soient $n \geq 1$ et $k \geq 1$ des entiers, alors

$$\begin{aligned}
D(n+1,k) &= \sum_{i=0}^{n} D(i,0)B(n-i,k-1) \\
&= D(0,0)B(n,k-1) + D(1,0)B(n-1,k-1) + \sum_{i=2}^{n} D(i,0)B(n-i,k-1) \\
&= B(n,k-1) + 2B(n-1,k-1) \\
&\quad + \sum_{i=2}^{n} \left[2D(i-1,0) + D(i-2,0)\right] B(n-i,k-1) \\
&= B(n,k-1) + 2B(n-1,k-1) + 2\sum_{i=2}^{n} D(i-1,0)B(n-i,k-1) \\
&\quad + \sum_{i=2}^{n} D(i-2,0)B(n-i,k-1) \\
&= B(n,k-1) + 2\sum_{i=1}^{n} D(i-1,0)B(n-i,k-1) \\
&\quad + \sum_{i=2}^{n} D(i-2,0)B(n-i,k-1) \\
&= B(n,k-1) + 2\sum_{i=0}^{n-1} D(i,0)B(n-1-i,k-1) + \sum_{i=0}^{n-2} D(i,0)B(n-2-i,k-1) \\
&= B(n,k-1) + 2B(n,k) + B(n-1,k).
\end{aligned}$$

□

Théorème A.2.1. *Le terme général de la suite* $\left(Q_n^{(s)}\right)_n$ *est*

$$Q_{n+1}^{(s)} = \sum_{k=0}^{n} B(n,k)t^k, \qquad (n \geq 0). \tag{A.17}$$

Démonstration. Par récurrence sur n. Pour $n = 0$ et 1, l'identité (A.17) est facile à vérifiée. Supposons que (A.17) est vraie jusqu'à l'ordre n, alors

$$\begin{aligned}
Q_{n+2}^{(s)} &= (2+t)Q_{n+1}^{(s)} + Q_n^{(s)} \\
&= (2+t)\sum_{k=0}^{n} B(n,k)t^k + \sum_{k=0}^{n-1} B(n-1,k)t^k \\
&= 2\sum_{k=0}^{n} B(n,k)t^k + \sum_{k=0}^{n} B(n,k)t^{k+1} + \sum_{k=0}^{n-1} B(n-1,k)t^k
\end{aligned}$$

$$
\begin{aligned}
&= 2\sum_{k=0}^{n} B(n,k)t^k + \sum_{k=1}^{n+1} B(n,k-1)t^k + \sum_{k=0}^{n-1} B(n-1,k)t^k \\
&= 2B(n,0) + \sum_{k=1}^{n-1} 2B(n,k)t^k + 2B(n,n)t^n + \sum_{k=1}^{n-1} B(n,k-1)t^k \\
&\quad + B(n,n-1)t^n + B(n,n)t^{n+1} + B(n-1,0) + \sum_{k=1}^{n-1} B(n-1,k)t^k \\
&= [2B(n,0) + B(n-1,0)] + \sum_{k=1}^{n-1} [B(n,k-1) + 2B(n,k) + B(n-1,k)]\,t^k \\
&\quad + [2B(n,n) + B(n,n-1)]\,t^n + B(n,n)t^{n+1},
\end{aligned}
$$

d'après le Lemme A.2.1 et les relations (A.12), (A.13), (A.14) et (A.15) on obtient

$$
\begin{aligned}
Q_{n+2}^{(S)} &= B(n+1,0) + \sum_{k=1}^{n-1} B(n+1,k)t^k + B(n+1,n)t^n + B(n+1,n+1)t^{n+1} \\
&= \sum_{k=0}^{n+1} B(n+1,k)t^k.
\end{aligned}
$$

□

CONCLUSION ET PERSPECTIVES

Plusieurs propriétés des périodes des suites de Fibonacci se généralisent aux suites de Morgan-Voyce et quasi Morgan-Voyce qui sont des suites récurrentes linéaires d'ordre 2. Certaines de ces propriétés s'étendent aussi aux suites Tribonacci qui sont des suites récurrentes linaires d'ordre 3.

Le fait que certaines identités satisfaites par la suite quasi Morgan-Voyce sont les mêmes que celles satisfaites par la suite de Fibonacci fait que l'on obtient, parfois, exactement les mêmes résultats, ce qui n'est pas le cas pour la suite de Morgan-Voyce qui satisfait des identités qui ressemblent à celles satisfaites par la suite de Fibonacci.

Notre première perspective est de faire l'étude des périodes des suites de Morgan-Voyce d'ordre 3. Ces suites sont obtenues en posant $r = 3$ et $q \leq 0$ dans la relation (0.2). Dans ce cas, on obtient la relation de récurrence

$$v_n - 3xv_{n-1} + 3x^2v_{n-2} - x^3v_{n-3} = y^3v_{n-3-q}.$$

Comme par hypothèse on a $q + r > 0$, on en déduit qu'on a trois cas qui sont $q = 0$, -1 ou -2. Nous allons d'abord nous intéresser aux trois cas $(q, p) = (0,0)$, $(-1,0)$ et $(-2,0)$.

Par exemple, dans le premier cas, on obtient la suite

$$\begin{cases} v_1 = 1,\ v_2 = x,\ v_3 = x^2, \\ v_n = 3xv_{n-1} - 3x^2v_{n-2} + (x^3 + y^3)v_{n-3},\ \ (n \geq 4). \end{cases}$$

La matrice compagnon de cette suite est $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ x^3+y^3 & -3x^2 & 3x \end{pmatrix}$ qui est de déterminant $x^3 + y^3$. On en déduit que si $x^3 + y^3$ est inversible modulo un entier $m \geq 2$, alors cette suite modulo m est simplement périodique. Il est raisonnable de commencer l'étude pour certaines valeurs de x et y.

Notre deuxième perspective est de s'intéresser à l'étude des périodes de la suite *Multibonacci* donné par (0.1). Cette suite a une matrice compagnon de déterminant 1, elle est donc simplement périodique modulo m, pour tout $m \geq 2$.

Notre troisième perspective est d'étudier les périodes de suites récurrentes linéaires sur un groupe abélien fini quelconque.

BIBLIOGRAPHIE

[1] **L. Ait-Amrane** et H. Belbachir. Les suites quasi Morgan-Voyce comme convolutions itérées de suites de Pell généralisées. *Soumis*, .

[2] **L. Ait-Amrane** et H. Belbachir. Periods of quasi Morgan-Voyce sequences and elliptic curves. *Soumis*, .

[3] **L. Ait-Amrane** et H. Belbachir. Periods of Tribonacci sequences and elliptic curves. *Soumis*, .

[4] **L. Ait-Amrane**, H. Belbachir et K. Betina. Periods of Morgan-Voyce sequences and elliptic curves. *A paraître : Mathematica Slovaca.*

[5] R. Aldrovandi. *Special matrices of mathematical physics*. World Scientific Publishing Co., Inc., River Edge, NJ, 2001. ISBN 981-02-4708-7. Stochastic, circulant and Bell matrices.

[6] H. Belbachir. Determining the mode for convolution powers of discrete uniform distribution. *Probab. Engrg. Inform. Sci.*, 25(4):469–475, 2011. ISSN 0269-9648.

[7] H. Belbachir et F. Bencherif. Linear recurrence sequences and powers of a square matrix. *Integers*, 6, A12:17 pp, 2006.

[8] H. Belbachir, T. Komatsu et L. Szalay. Characterization of linear recurrences associated to rays in Pascal's triangle. Dans *Diophantine analysis and related fields 2010*, volume 1264 de *AIP Conf. Proc.*, pages 90–99. Amer. Inst. Phys., Melville, NY, 2010.

[9] H. Belbachir, T. Komatsu et L. Szalay. Linear recurrences associated to rays in Pascal's triangle and combinatorial identities. *Math. Slovaca*, 64(2):287–300, 2014. ISSN 0139-9918.

[10] R. P. Brent. On the periods of generalized Fibonacci recurrences. *Math. Comp.*, 63(207): 389–401, 1994. ISSN 0025-5718.

[11] Y. Bugeaud, M. Mignotte et S. Siksek. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163(3): 969–1018, 2006. ISSN 0003-486X.

[12] D. A. Coleman, C. J. Dugan, R. A. McEwen, C. A. Reiter et T. T. Tang. Periods of (q,r)-Fibonacci sequences and elliptic curves. *Fibonacci Quart.*, 44(1):59–70, 2006. ISSN 0015-0517.

[13] P. J. Davis. *Circulant matrices*. John Wiley & Sons, New York-Chichester-Brisbane, 1979. ISBN 0-471-05771-1. A Wiley-Interscience Publication, Pure and Applied Mathematics.

[14] G. Ferri, M. Faccio et A. D'Amico. A new numerical triangle showing links with Fibonacci numbers. *Fibonacci Quart.*, 29(4):316–321, 1991. ISSN 0015-0517.

[15] G. Ferri, M. Faccio et A. D'Amico. Fibonacci numbers and ladder network impedance. *Fibonacci Quart.*, 30(1):62–67, 1992. ISSN 0015-0517.

[16] R. M. Gray. Toeplitz and circulant matrices : A review, 2006. URL `http://ee.stanford.edu/~gray/toeplitz.pdf`.

[17] A. F. Horadam. New aspects of Morgan-Voyce polynomials. Dans *Applications of Fibonacci numbers, Vol. 7 (Graz, 1996)*, pages 161–176. Kluwer Acad. Publ., Dordrecht, 1998.

[18] A. F. Horadam. Quasi Morgan-Voyce polynomials and Pell convolutions. Dans *Applications of Fibonacci numbers, Vol. 8 (Rochester, NY, 1998)*, pages 179–193. Kluwer Acad. Publ., Dordrecht, 1999.

[19] R. A. Horn et C. R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, 1985. ISBN 0-521-30586-1.

[20] K. Ireland et M. Rosen. *A classical introduction to modern number theory*, volume 84 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1990. ISBN 0-387-97329-X.

[21] J. Klaška. Tribonacci modulo 2^t and 11^t. *Math. Bohem.*, 133(4):377–387, 2008. ISSN 0862-7959.

[22] J. Klaška. Tribonacci modulo p^t. *Math. Bohem.*, 133(3):267–288, 2008. ISSN 0862-7959.

[23] J. Klaška. Tribonacci partition formulas modulo m. *Acta Math. Sin. (Engl. Ser.)*, 26(3):465–476, 2010. ISSN 1439-8516.

[24] J. Klaška et L. Skula. Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$. *Fibonacci Quart.*, 48(3):228–235, 2010. ISSN 0015-0517.

[25] A. M. Morgan-Voyce. Ladder network analysis using Fibonacci numbers. *IRE. Trans. on Circuit Theory*, 6:321–322, 1959.

[26] J. Reynolds. Perfect powers in elliptic divisibility sequences. *J. Number Theory*, 132(5): 998–1015, 2012. ISSN 0022-314X.

[27] P. Ribenboim. An algorithm to determine the points with integral coordinates in certain elliptic curves. *J. Number Theory*, 74(1):19–38, 1999. ISSN 0022-314X.

[28] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ISBN 0-387-94328-5.

[29] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 de *Graduate Texts in Mathematics*. Springer, Dordrecht, second édition, 2009. ISBN 978-0-387-09493-9.

[30] J. H. Silverman et J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. ISBN 0-387-97825-9.

[31] N. J. A. Sloane. The on-line encyclopedia of integer sequences, 2014. URL `http://www.oeis.org`.

[32] M. N. S. Swamy. Properties of the polynomials defined by Morgan-Voyce. *Fibonacci Quart.*, 4(1):73–81, 1966.

[33] M. N. S. Swamy. Further properties of Morgan-Voyce polynomials. *Fibonacci Quart.*, 6(2): 167–175, 1968. ISSN 0015-0517.

[34] A. Vince. Period of a linear recurrence. *Acta Arith.*, 39(4):303–311, 1981. ISSN 0065-1036.

[35] J. Vinson. The relation of the period modulo to the rank of apparition of m in the Fibonacci sequence. *Fibonacci Q.*, 1(2):37–46, 1963. ISSN 0015-0517.

[36] M. E. Waddill. Some properties of a generalized Fibonacci sequence modulo m. *Fibonacci Quart.*, 16(4):344–353, 1978. ISSN 0015-0517.

[37] D. D. Wall. Fibonacci series modulo *m*. *Amer. Math. Monthly*, 67:525–532, 1960. ISSN 0002-9890.

[38] L. C. Washington. *Elliptic curves. Number theory and cryptography. 2nd ed.* 2nd ed. édition, 2008. ISBN 978-1-4200-7146-7/hbk.

[39] C. C. Yalavigi. Properties of Tribonacci numbers. *Fibonacci Quart.*, 10(3):231–246, 1972.